Finite Fields and Their Applications 80 (2022) 102014

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

A transform approach to polycyclic and serial codes over rings

Maryam Bajalan [a,1], Edgar Martínez-Moro [b,*,2], Steve Szabo [c]

[a] *Department of Mathematics, Malayer University, Hamedan, Iran*
[b] *Institute of Mathematics, University of Valladolid, Castilla, Spain*
[c] *Department of Mathematics & Statistics, Eastern Kentucky University, United States of America*

ARTICLE INFO

Article history:
Received 11 May 2021
Received in revised form 22 January 2022
Accepted 9 February 2022
Available online 24 February 2022
Communicated by Qiang Wang

MSC:
94B15
13M10
15B33

Keywords:
Polycyclic code
Duality
Finite local ring
Mattson-Solomon transform
Serial codes

ABSTRACT

In this paper, a transform approach is used for polycyclic and serial codes over finite local rings in the case that the defining polynomials have no multiple roots. This allows us to study them in terms of linear algebra and invariant subspaces as well as understand the duality in terms of the transform domain. We also make a characterization of when two polycyclic ambient spaces are Hamming-isometric.

* Corresponding author.
E-mail addresses: mar.bajalan@gmail.com (M. Bajalan), edgar.martinez@uva.es (E. Martínez-Moro), Steve.Szabo@eku.edu (S. Szabo).

[1] This work was completed while this author visited the Institute of Mathematics of University of Valladolid (IMUVa) during Nov. 2020 – June 2021. She thanks the IMUVa for their kind hospitality.

[2] Second author was supported in part by Grant PGC2018-096446-B-C21 funded by MCIN/AEI/10.13039/501100011033 and by "ERDF A way of making Europe".

https://doi.org/10.1016/j.ffa.2022.102014

0. Introduction

Polycyclic codes over a local ring R can be described as ideals on the ring $R[x]/\langle f(x)\rangle$ where f is a polynomial in $R[x]$. They were introduced in [18] and are a generalization of cyclic and constacyclic codes which have been extensively studied in the literature. Polycyclic codes over finite fields have been studied from several points of view, see for example [1,26], they have been also studied over Galois rings [17] and recently over chain rings in [9]. Note that codes over chain rings have gathered a great importance, see [29,27] and the references there in. In [26] the authors pointed out that it was worth to generalize their results from finite fields alphabets to chain rings. In this paper we will make this generalization to finite local rings in the case that the polynomial defining the ambient space has simple roots (see Section 1 for a definition). We will propose a transform approach that generalizes the classical Mattson-Solomon (Fourier) transform to finite fields, moreover, we show the relationship between the transform and the annihilator duality for polycyclic codes introduced in [1]. Note that this approach can be easily translated to the multivariable case as it is pointed out in the last section of this paper.

The outline of the paper is as follows. In Section 1 we show those results on finite local rings, circulant matrices over rings and matrix diagonalization needed for our work. In Section 2 we review the discrete Fourier Transform over rings as well as some facts on Vandermonde matrices over rings. Section 3 is devoted to the description on the Mattson-Solomon transforms and its relationship with several inner products both in the original space and its transform image. The main result is Theorem 3.3 that shows that all of them generate the same dual code. The generalization to finite local rings of the results in [26] can be found in Section 4. In Section 5 we investigate when two different polycyclic definitions provide isomorphic and isometric coding ambient spaces. Finally in Section 6 we show how all the previous result can be generalized in the case of serial codes.

1. Preliminaries

1.1. Finite local rings

We will show here selected results about local rings needed in the paper, for a complete account see [10]. In this 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 $\bar{\cdot} : R \mapsto (R/\mathfrak{m})$ and abusing notation we will use it also for polynomial rings acting on the coefficients $\bar{\cdot} : R[x] \mapsto (R/\mathfrak{m})[x] = \mathbb{F}_q[x]$.

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 if and only if f is an irreducible polynomial in $\mathcal{J}$, and the polynomials in $\mathcal{J}$ admit unique factorizations into irreducible polynomials and a polynomial in $\mathcal{J}$ has no multiple roots in any local extension of R. **Throughout the paper we will restrict to polynomials in $\mathcal{J}$ unless otherwise stated.** The following two lemmas will be helpful during the paper.

Lemma 1.1 *(Azumaya's lemma). Let f be a monic polynomial in $R[x]$. Then $\mathcal{R}_f = I_1 \bigoplus I_2$ where I_1 and I_2 are ideals in $\mathcal{R}_f$ if and only if there exist monic coprime polynomials h and g in $R[x]$ with $f = gh$ and $I_1 = \langle g\rangle/\langle f\rangle$, $I_2 = \langle h\rangle/\langle f\rangle$.*

An element e of the ring $\mathcal{R}_f$ is called an idempotent if $e^2 = e$; two idempotents e_1, e_2 are said to be orthogonal if $e_1e_2 = 0$ and an idempotent is said to be primitive if it is non-zero and cannot be written as the sum of non-zero orthogonal idempotents. A set $\{e_1, ..., e_r\}$ of elements of $\mathcal{R}_f$ is called a complete set of idempotents if $\sum_{i=1}^{r} e_i = 1$. If $\{e_1, ..., e_r\}$ is a complete set of pairwise orthogonal idempotents, we have that $\mathcal{R}_f = \bigoplus_{i=1}^{r} \mathcal{R}_f e_i$.

Lemma 1.2 *(Theorem 3.2 in [6]). Let R be a finite local commutative ring and f be a monic polynomial in $R[x]$ such that $f = \prod_{i=1}^{r} f_i$ is the unique factorization of f into a product of monic primary pairwise coprime polynomials. The ring $\mathcal{R}_f$ admits a unique complete set of primitive pairwise orthogonal idempotents $\{e_1, e_2, ..., e_r\}$ given by*

$$e_i = v_i(x)\hat{f}_i(x), \text{ where } v_i(x) \in \mathcal{R}_f \text{ and } \hat{f}_i = \frac{f}{f_i}. \tag{1}$$

Moreover $e_iR[x] \cong \frac{R[X]}{\langle f_i\rangle}$ and $\mathcal{R}_f = \bigoplus_{i=1}^{r} e_iR[x]$.

1.2. Circulant matrices

We will denote by $\mathcal{M}_n(R)$ the set of $n \times n$ matrices over the local ring R. If $\deg f(x) = n$, $E_f \in \mathcal{M}_n(R)$ will be the companion matrix associated with $f(x) = x^n - \sum_{i=0}^{n-1} f_i x^i$,

$$E_f = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ f_0 & f_1 & f_2 & \cdots & f_{n-1} \end{pmatrix}. \tag{2}$$

Consider the usual matrix multiplication in $\mathcal{M}_n(R)$ and the ordinary product in $\mathcal{R}_f$. Consider the basis $\mathcal{B} = \{1, x, x^2, \ldots, x^{n-1}\}$ for $\mathcal{R}_f$ and let the map $\rho_f : \mathcal{R}_f \to R^n$ send a polynomial to coefficients of x^i. The map $M : \mathcal{R}_f \to \mathcal{M}_n(R)$ defined by

$$M(g(x)) = \begin{bmatrix} \rho_f(g(x)) \\ \rho_f(xg(x)) \\ \vdots \\ \rho_f(x^{n-1}g(x)) \end{bmatrix}$$

is the regular representation of elements $\mathcal{R}_f$. If we denote the image of M by $\mathcal{M}_n(R, f)$, then $M : \mathcal{R}_f \to \mathcal{M}_n(R, f)$ is a ring isomorphism. Clearly $M(x) = E_f$ and hence set $\{\mathrm{Id}, E_f, E_f^2, \ldots, E_f^{n-1}\}$ is a basis for $\mathcal{M}_n(R, f)$, in fact the elements of $\mathcal{M}_n(R, f)$ are linear combination of powers of the companion matrix E_f. This isomorphism has been extensively studied in [30]. Note that elements $\mathcal{M}_n(R, f)$ are called Barnett matrices in [30], $f(x)$-circulants in [7] or polycirculant matrices in [28]. The following characterization of the subrings of $\mathcal{M}_n(R)$ being images of such an isomorphism can be found in [30].

Lemma 1.3 *(Theorem 2.1 [30]). A subring S of $\mathcal{M}_n(R)$ is of the form $\mathcal{M}_n(R, f)$ if and only if $S = C_{\mathcal{M}_n(R)}(E_f)$, the centralizer of the matrix E_f in $\mathcal{M}_n(R)$.*

This fact plays a central role for the diagonalization of commuting matrices in the field case [7]. We will denote by $\mathcal{M}_{1,n}(R, f)$ the set of all $1 \times n$ matrices $[a_0, a_1 \ldots a_{n-1}]$ endowed with the following multiplication

$$[a_0, a_1 \ldots a_{n-1}] \cdot [b_0, b_1 \ldots b_{n-1}] = [a_0, a_1 \ldots a_{n-1}]M(b), \tag{3}$$

where $b = b_0 + b_1x + \ldots + b_{n-1}x^{n-1}$. Since every element of $\mathcal{M}_n(R, f)$ is determined by its first row and polynomial $f(x)$, the map $\varphi : \mathcal{M}_n(R, f) \to (\mathcal{M}_{1,n}(R, f), \cdot)$, which sends every matrix to the first row is a ring isomorphism.

2. The Discrete Fourier Transform over commutative rings

We assume that the reader is familiar with the Discrete Fourier Transform (DFT) over finite fields and its applications to cyclic codes (see [19] for example). Suppose that ξ is a primitive N^{th} root of unity in a field $\mathbb{F}$, i.e., $\xi^N = 1$ and $\xi \neq 1$ for $i = 1, \ldots, N-1$. For any integer j,

$$\sum_{i=0}^{N-1} \xi^{ij} = \begin{cases} N, & j = 0(\mathrm{mod\ N}), \\ 0, & \text{otherwise}, \end{cases} \tag{4}$$

and the DFT of length N generated by ξ is the mapping DFT_ξ from $\mathbb{F}^N$ to $\mathbb{F}^N$ defined by $B = DFT_\xi(b)$, where $B_i = \sum_{n=0}^{N-1} b_n\xi^{in}$ for $i = 0, 1, \ldots, N-1$ or equivalently $B = bM_\xi$, where

$$M_\xi = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \xi & \xi^2 & \dots & \xi^{N-1} \\ 1 & \xi^2 & \xi^{2\cdot 2} & \dots & \xi^{2(N-1)} \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 1 & \xi^{N-1} & \xi^{(N-1)2} & \dots & \xi^{(N-1)(N-1)} \end{bmatrix}.$$

Thus M_ξ is a Vandermonde matrix with determinant $\prod_{j=1}^{N-1}\prod_{i=1}^{j-1}(\xi^j - \xi^i)$ which is non-zero and hence M_ξ is non-singular and the DFT is always invertible. The inverse transform of DFT is given by

$$b_n = \frac{1}{N}\sum_{i=0}^{N-1} B_i \xi^{-in}, \quad \text{for} \quad n = 0, 1, \dots, N-1. \tag{5}$$

Note that a matrix over a ring is non-singular if and only if its determinant is a unit in the ring [3]. Moreover, a product of elements of a ring is unit if and only if each element is unit. Therefore the following theorem holds.

Theorem 2.1. *(DFT over rings [22, Theorem 10]) If ξ is a primitive N^{th} root of unity in a commutative ring R. Then the DFT from R^N to R^N defines an invertible mapping whose inverse is given by the Equation (5) if and only if $\xi^k - 1$ is a unit of R for $k = 1, 2, \dots, N-1$.*

For example, $\xi = 2$ is a primitive 4^{th} root of unity in $\mathbb{Z}_{15}$ but $\xi^2 - 1$ is not unit. So for $\xi = 2$, DFT of length $N = 4$ is not invertible. There are some results for DFT over $\mathbb{Z}_m$, (Number Theory Transform in [23]). It follows from above theorem that if ξ generates an invertible DFT of length N in ring R and $L(>1)$ is a divisor N, then $\xi^{\frac{N}{L}}$ also generates an invertible DFT of length L in R (see [23]).

2.1. Vandermonde matrices over commutative rings

Let R be the local ring with extension R' and R-algebra morphism $\gamma : R \to R'$. A matrix $M \in \mathcal{M}_n(R)$ is diagonalizable over R' if there are matrices $V, D \in \mathcal{M}_n(R')$ such that D is diagonal and $V^{-1}\gamma(M)V = D$, see [15]. From now on, for convenience we simply write $V^{-1}MV = D$. Consider $f(x) \in R[x]$ such that $f(x) = \prod_{i=1}^{n}(x - \alpha_i) \in R'[x]$, i.e. $f(x)$ splits in R'. Also consider the following Vandermonde matrix

$$V = V(\alpha_1, \dots, \alpha_n) = \begin{bmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \dots & \alpha_n^2 \\ \vdots & \vdots & \dots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \dots & \alpha_n^{n-1} \end{bmatrix}.$$

For $i = 1, \ldots, n$, denote i^{th} column of V as V_i and for $j = 1, \ldots, n$, and given $g \in \mathcal{R}_f$ denote j^{th} row of $M = M(g)$ by M_j. We know that entries of M_j are the coefficients of $x^{j-1}g(x)(\mod f)$ and henceforth $M_jV_i = \alpha_i^{j-1}g(\alpha_i)$. Therefore $MV_i = g(\alpha_i)V_i$, that is V_i is the eigenvector and $g(\alpha_i)$ is the eigenvalue of M in R'. So $MV = \mathrm{diag}[g(\alpha_1), g(\alpha_2), \ldots, g(\alpha_n)]V$. Now If V is non-singular then $V^{-1}MV = \mathrm{diag}[g(\alpha_1), g(\alpha_2), \ldots, g(\alpha_n)]$, and hence M is diagonalized by V. We know that $\det V = \prod_{j=1}^{n-1}\prod_{i=1}^{j-1}(\alpha_j - \alpha_i)$ is in local ring R'. It is well-known that for a local ring $\alpha_j - \alpha_i (i \neq j)$ is a unit if and only if $\bar{\alpha}_j \neq \bar{\alpha}_i$, see [24]. So V is non-singular if and only if $\bar{\alpha}_j \neq \bar{\alpha}_i$, for all $i \neq j$. Note that if $f(x) \in \mathcal{J} \subseteq R[x]$ then V is non-singular. Moreover, if A is a non-singular matrix over a local ring, then the homogeneous system $Ax = 0$ has a unique solution [24, Lemma 2.1]. The following result provides us V^{-1}.

Lemma 2.2 *([25]). If V^T is non-singular, then $(V^T)^{-1} = (w_{ij})$ is given by*

$$(w_{ij}) = (-1)^{i+j}\frac{S_{n-i,j}}{\prod\limits_{l<k}^{n}(\alpha_k - \alpha_l)}$$

with $l = j$ or $k = j$ and $S_k = S_k(\alpha_1, \ldots, \alpha_n) = \sum\limits_{1 \leqslant i_1 < \ldots < i_k \leqslant n} \alpha_{i_1} \ldots \alpha_{i_k}$, and $S_0(\alpha_1, \alpha_2, \ldots, \alpha_n) = 1$ and $S_{k,j} = S_k(\alpha_1, \ldots, \alpha_{j-1}, \alpha_{j+1}, \ldots, \alpha_n)$.

Example 2.3. Let $n = 3$ and $f(x) = x^3 + 5x + 3 \in \mathbb{Z}_9[x]$. Then $f(x) = (x-1)(x-12)(x-23) \in \mathbb{Z}_{27}[x]$. Moreover $\det(V) = 16$ is unit in $\mathbb{Z}_{27}$. We have

$$V^{-1} = \begin{bmatrix} 21 & 8 & 26 \\ 19 & 6 & 2 \\ 15 & 13 & 26 \end{bmatrix}.$$

3. Mattson-Solomon transform and polycyclic codes over rings

From now on we will be concerned with univariate polycyclic codes defined as ideals of the ambient space $\mathcal{R}_f$, where $f(x)$ a monic polynomial in $\mathcal{J} \subseteq R[x]$. For a local ring the diagonalizing of M is unique up to permutation of diagonal entries. So let $\{\alpha_1, \ldots, \alpha_n\}$ be a fixed ordering of roots of $f(x)$ in extension ring R' of R. The map

$$\begin{array}{rccc} MS_f: & (\mathcal{R}_f, \cdot) & \longrightarrow & (R'[x]/\langle f(x)\rangle, \star) \\ & g(x) & \mapsto & \sum\limits_{i=1}^{n} g(\alpha_i)x^{i-1}, \end{array} \tag{6}$$

is a ring homomorphism, where $\cdot$ denotes ordinary polynomial multiplication modulo $f(x)$ and $\star$ denotes the component-wise multiplication or Schur product. We will call the map in (6) the *Mattson-Solomon transform* with respect to the polynomial $f(x)$. Indeed in the case $f(x) = x^n - 1$ we recover the Fourier transform in the previous section. Since

$f(x) \in \mathcal{J}$, the Vandermonde matrix V is non-singular and hence the homomorphism MS_f is injective. Take $V^{-1} = (u_{ij})$ and $g(x) = g_0 + g_1x + \ldots + g_{n-1}x^{n-1} \in \mathcal{R}_f$ and denote $g = (g_0, g_1, \ldots, g_{n-1})$. If we denoted by $B = MS_f(g)$, then $B_i = g(\alpha_i)$ and the inverse formula is given by

$$g_{j-1} = \sum_{k=1}^{n} B_{k-1}u_{kj}, \quad 1 \leqslant j \leqslant n,$$

i.e. $g(x) = \sum\limits_{j=1}^{n}\sum\limits_{k=1}^{n} B_{k-1}u_{kj}x^{j-1}$.

Example 3.1 *(Example 2.3 Cont.).* Let $g(x) = g_0 + g_1x + g_2x^2 \in \mathbb{Z}_9[x]$ and $MS_f(g) = (B_0, B_1, B_2)$ then the inverse of the Mattson-Solomon transform is

$$g_0 = 21B_0 + 19B_1 + 15B_2,\ g_1 = 8B_0 + 6B_1 + 13B_2,\ g_2 = 26B_0 + 2B_1 + 26B_2.$$

Given two polynomials $g_1(x), g_2(x) \in \frac{R'[x]}{\langle f(x)\rangle} = \mathcal{R}'_f$, we define the $\star$ inner product as

$$\langle g_1(x), g_2(x)\rangle_\star = (g_1)_0(g_2)_0 + \ldots + (g_1)_{n-1}(g_2)_{n-1} = (g_1 \star g_2)(1). \tag{7}$$

Since $\langle g(x), x^i\rangle_\star = g_i$ for $i = 1, \ldots, n$, the inner product is non-degenerate. Let $\mathcal{C} \subseteq \mathcal{R}_f$ be a polycyclic code. The dual of $\mathcal{C}$ w.r.t. $\star$, denoted by $\mathcal{C}^{\perp_\star}$, is defined as

$$\mathcal{C}^{\perp_\star} = \{h(x) \in \mathcal{R}_f \mid \langle MS(g), MS(h)\rangle_\star = 0 \text{ for all } g(x) \in \mathcal{C}\}. \tag{8}$$

We also define an inner-product on $\mathcal{R}_f$ by

$$\langle g_1(x), g_2(x)\rangle_{\mathrm{tr}} = \mathrm{trace}\,(M(g_1g_2)), \quad g_1(x), g_2(x) \in \mathcal{R}_f, \tag{9}$$

and denote $\mathcal{C}^{\perp_{tr}} = \{g \in \mathcal{C} \mid \langle g(x), h(x)\rangle_{tr} = 0 \quad \text{for all} \quad h \in \mathcal{C}\}$. Let $k(x) \in \mathcal{R}_f$ and $\langle k(x), x^i\rangle_{tr} = 0$ for all $i = 0, 1, \ldots, n-1$. Then $\langle MS_f(k(x), MS_f(x^i))\rangle_\star = 0$. Thus $\alpha_1^i k(\alpha_1) + \ldots + \alpha_n^i k(\alpha_n) = 0$ and hence $(k(\alpha_1), \ldots, k(\alpha_n))V = 0$. Since V is non-singular, then the linear homogeneous system has the unique solution $k(\alpha_1) = \ldots = k(\alpha_n) = 0$. So $MS_f(k(x)) = 0$, i.e. $k(x) = 0$. Henceforth the trace inner product is non-degenerate.

Let π_i denote the projection of $\mathcal{R}_f$ onto the coefficient of x^i for $i = 0, \ldots, n-1$, the trace map is defined in [10] as $\mathrm{tr} : \mathcal{R}_f \to R$ is given by $\mathrm{tr}(g) = \sum \pi_i(x^i g)$. It is clear that the trace inner product of g_1, g_2 is equal to the trace map of g_1g_2.

Proposition 3.2. *Let $g_1(x), g_2(x) \in \mathcal{R}_f$, then*

$$\langle g_1(x), g_2(x)\rangle_{\mathrm{tr}} = 0 \iff \langle MS_f(g_1),\, MS_f(g_2)\rangle_\star = 0$$

Proof. We know $\gamma(M(g_1g_2))$ is similar to $\text{diag}[(g_1g_2)(\alpha_1), \ldots, (g_1g_2)(\alpha_n)]$. So

$$\begin{aligned}\gamma(\text{trace}(M(g_1g_2))) &= \text{trace}(\gamma(M(g_1g_2))) \\ &= (g_1g_2)(\alpha_1) + \ldots + (g_1g_2)(\alpha_n) \\ &= \langle MS_f(g_1),\, MS_f(g_2)\rangle_\star. \quad \square\end{aligned}$$

Now consider the following inner product on $\mathcal{R}_f$,

$$\langle g_1(x), g_2(x)\rangle_{(0)} = g_1g_2(0), \quad g_1(x), g_2(x) \in \mathcal{R}_f, \tag{10}$$

it is a non-degenerate symmetric bilinear form if $f_0 \neq 0$. The dual $\mathcal{C}^{\perp_0}$ of code $\mathcal{C}$ is just its annihilator dual in [1,9]. Since the matrix V is non-singular the Mattson-Solomon transform is an injective morphism and thus it is clear that for any ideal $\mathcal{C}$ we have

$$\text{Ann}(\mathcal{C}) = \mathcal{C}^{\perp_{MS}} = \{g \in \mathcal{R}_f \mid MS(g) \star MS(c) = 0 \text{ for all } c \in \mathcal{C}\}.$$

We have this result that identifies the dualities in the transform domain.

Theorem 3.3. *Let R be a finite local ring. If $f \in \mathcal{J} \subseteq R[x]$ and $\mathcal{C}$ is a code in $\mathcal{R}_f$ we have that*

$$\mathcal{C}^{\perp_{\text{tr}}} = \mathcal{C}^{\perp_\star} = C^{\perp_0} = \mathcal{C}^{\perp_{MS}} = \text{Ann}(\mathcal{C}).$$

Proof. From the discussion above it is clear that $\mathcal{C}^{\perp_{\text{tr}}} = \mathcal{C}^{\perp_\star}$ and $C^{\perp_0} = \mathcal{C}^{\perp_{MS}} = \text{Ann}(\mathcal{C})$. Moreover $\text{Ann}(\mathcal{C}) \subseteq \mathcal{C}^{\perp_{\text{tr}}}$ is straightforward. Let's prove the other direction. Suppose there exists an element $g \in \mathcal{C}^{\perp_{\text{tr}}}$ such that $g \notin \text{Ann}(\mathcal{C}) = \mathcal{C}^c$, thus $g \in \mathcal{C} \cap \mathcal{C}^{\perp_{\text{tr}}}$ and hence $g = r \cdot \sum_{j=1}^{k} e_{i_j}$ where $\sum_{j=1}^{k} e_{i_j}$ is the idempotent generating $\mathcal{C}$. Consider now any other element $s \in \mathcal{R}_f$, then $s = \sum_{i=1}^{t} s_i e_i$ and $g \cdot s = \sum_{j=1}^{k} r s_{i_j} e_{i_j}$. Hence $0 = \langle g, s\rangle_{\text{tr}} = \langle r, s\rangle_{\text{tr}}$ for all s in $\mathcal{R}_f$, thus $r = 0$ since the trace inner product is non-degenerate and therefore $g = 0$. $\square$

4. Polycyclic codes as invariant spaces

Let $f_1, f_2, \ldots f_r$ be pairwise coprime monic polynomials over R, $f = f_1 f_2 \ldots f_r$ and $\hat{f}_i = \frac{f}{f_i}$. There exists $a_i, b_i \in R$ such that $a_i f_i + b_i \hat{f}_i = 1$. Let $e_i = b_i \hat{f}_i + \langle f(x)\rangle$ as in Lemma 1.2. Let us define the set $U_i \subseteq \mathcal{M}_{1,n}(R, f)$ as $U_i = ker f_i(E_f)$.

Proposition 4.1.

1. $R_f e_i = Ann_{\mathcal{R}_f}(f_i)$.
2. $c \in \mathcal{R}_f e_i$ *if and only if* $e_i c = c$.
3. *The matrix* $M(e_i) = e_i(E_f)$ *is the generator matrix of the polycyclic code* $\mathcal{R}_f e_i$.

4. $M(e_i)$ *is invariant under multiplication by the companion matrix* E_f *for all* $i = 1, \dots r$ *and they are pairwise orthogonal idempotent matrices.*
5. *The image of a polycyclic code under* M *is an invariant ideal under multiplication by* E_f*.*
6. $U_i \cong \mathcal{R}_f e_i$*.*

Proof.

1. It follows from the annihilator definition.
2. It follows from $a_i f_i + b_i \hat{f}_i = 1$ and Part 1.
3. The rows of $M(e_i)$ are the coefficients of $e_i(x)$, $xe_i(x), \dots, x^{n-1}e_i(x)$.
4. $M(\mathcal{R}_f e_i)$ is an ideal in $\mathcal{M}_n(R, f)$ and we know that $\{\mathrm{Id}, E_f, E_f^2, \dots, E_f^{n-1}\}$ is a basis for $\mathcal{M}_n(R, f)$. Moreover, since M is an isomorphism, for all $i \neq j$ we have $M(e_i) \neq M(e_j)$, $M(e_i)M(e_i) = M(e_i^2) = M(e_i)$, and $M(e_i)M(e_j) = M(0) = 0$.
5. It is clear.
6. It is enough to prove that for a fixed i, $\rho_f(\mathcal{R}_f e_i) = U_i$. Let $k = re_i \in \mathcal{R}_f e_i$ for some $r \in \mathcal{R}_f$. Since $e_i f_i = 0$, we have $k(E_f)f_i(E_f) = 0$, and hence $\varphi(k(E_f))f_i(E_f) = 0$, i.e. $\rho_f(k) \in U_i$. Conversely, let $[a_0 \dots a_{n-1}] \in U_i$. Denote $f_i(x) = b_0 + b_1 x + \dots + b_{n-1}x^{n-1}$. Applying definition (3), we have $[a_0 \dots a_{n-1}].[b_0 \dots b_{n-1}] = 0$. If we denote $a(x) = a_0 + a_1 x + \dots + a_{n-1}x^{n-1}$,

$$a(x)f_i(x) = \rho_f^{-1}([a_0 \dots a_{n-1}].[b_0 \dots b_{n-1}]) = 0.$$

Therefore $a(x) \in Ann(f_i)$, i.e. $\rho_f^{-1}[a_0 \dots a_{n-1}] \in \mathcal{R}_f e_i$ and the proof is complete. □

Taking into account the previous proposition and since the ring $\mathcal{R}_f$ admits a unique complete set of primitive pairwise orthogonal idempotents $\{e_1, e_2, ..., e_r\}$, polycyclic codes over rings decompose into some minimal polycyclic codes corresponding to each one of them and the following result follows.

Theorem 4.2. *Let* E_f *be companion matrix with minimal polynomial* f *and* $f = f_1 \dots f_r$ *decomposes in to pairwise coprime monic irreducible polynomials. Then*

$$\mathcal{R}_f \cong U_1 \oplus \dots \oplus U_r,$$

where $U_i = Ker f_i(E_f) \subseteq \mathcal{M}_{1,n}(R, f)$*.*

1. *Each of the above summands is an indecomposible polycyclic code with* E_f*-invariant image in* $\mathcal{M}_n(R, f)$*.*
2. *Each polycyclic code* $\mathcal{C} \subseteq \mathcal{R}_f$ *can be seen as a direct sum of* U_i *for some indices* i*.*

3. *If a polycyclic code* $\mathcal{C}$ *decomposes as* $\mathcal{C} \cong \bigoplus_{i\in I} U_i$ *then*

$$\mathcal{C}^{\perp_{tr}} \cong \left(\bigoplus_{i\in I} U_i\right)^c = \bigoplus_{i\notin I} U_i$$

Note that this result generalizes the decomposition in [26] based on the Primary Decomposition Theorem in linear algebra over finite fields.

Remark 4.3 *(BCH-like bounds).* Mattson-Solomon transform can be a great tool for understanding BCH-like bounds that have been established for different types of (chain) rings (see for example [11,16]) or based on invariant spaces for polycyclic codes over fields [26]. Note that the minimum distance of a linear general code over R is the same as the one of its socle [14, Proposition 5]. Note that in general, we can not state that the minimum distance of a code $\mathcal{C}$ is equal to the minimum distance of the code $\bar{\mathcal{C}}$, since in general $d(\mathcal{C}) \leq d(\bar{\mathcal{C}})$. However, if they are Hensel's lifts of codes over $\mathbb{F}_q$ (see [21] for a characterization) we have the equality and therefore all classical bounds on distances for codes over fields (Bose–Ray-Chaudhuri–Hocquenghem, Hartmann–Tzeng, Roos, etc.) also apply to their Hensel's lifts.

5. Isometric ambient spaces

Assume that a finite ring R is equipped with a weight w. Linear codes $\mathcal{C}, \mathcal{D} \subseteq R^n$ are called isometric if there exists an R-linear isomorphism $\phi : C \to D$ which $w(\phi(c)) = w(c)$ for all $c \in C$. In the literature, codes $\mathcal{C}, \mathcal{D}$ are called isometrically equivalent. The MacWilliams Extension Theorem, one of the most powerful theorems, states that the map $\phi : \mathcal{C} \to \mathcal{D}$ between linear codes over R is the Hamming-isometry if and only if it is a monomial transformation, i.e. for every $c \in \mathcal{C}$ there is a monomial matrix M_c such that $\phi(c) = cM_c$. Notice that every Hamming-isometry is a homogeneous-isometry and vice versa, [12].

Theorem 5.1. *([30] Theorem 3.1) Let* $h(x) = x^n - h_{n-1}x^{n-1} - \cdots - h_1 x - h_0$ *be a polynomial in* $R[x]$ *of the same degree of* f*. If there exists a polynomial* $\omega \in \mathcal{R}_f$ *such that* $h(\omega) = 0 \in \mathcal{R}_f$*, and* $\det(W)$ *is a unit in* R*, where* $W = \begin{bmatrix} \rho_f(\omega^0) \\ \rho_f(\omega^1) \\ \rho_f(\omega^2) \\ \vdots \\ \rho_f(\omega^{n-1}) \end{bmatrix}$ *then*

$$\begin{array}{rccc} \theta: & \mathcal{M}_{1,n}(R,h) & \longrightarrow & \mathcal{M}_{1,n}(R,f) \\ & \rho_h(x) & \mapsto & \rho_f(\omega), \end{array} \tag{11}$$

is an isomorphism which is the identity in R (where R is identify with $\rho_h(r)$, $r \in \mathcal{R}_f$ a constant polynomial).

Remark 5.2. To construct such a polynomial $h(x)$ as described in the first statement of Theorem 5.1, choose $\rho_f(\omega) \in \mathcal{M}_{1,n}(R, f)$ such that $\det W$ is a unit element in R. Now assume $[h_0\, h_1 \dots h_{n-1}] = \rho_f(\omega^n)W^{-1}$.

Example 5.3.

1. Let $R = \mathbb{Z}_4$, $f(x) = x^3 - 2x^2 - x - 1$ and $h(x) = x^3 - x^2 - 1$ are polynomials in $R[x]$. If $\omega = 1 + x^2 \in \frac{R[x]}{\langle f(x)\rangle}$ then $\theta : \frac{R[x]}{\langle h(x)\rangle} \to \frac{R[x]}{\langle f(x)\rangle}$ is an isomorphism since $h(\omega) = 0$ and $\det W = 1$. Note that it is not a Hamming isometry, because $\theta(x^2 + x + 1) = 3x + 1$.
2. Let $R = \mathbb{Z}_4$, $f(x) = x^4 - 3x - 1$ and $h(x) = x^4 - 2x^2 - x - 3$ are polynomials in $R[x]$. If $\omega = 3x + 1 \in \frac{R[x]}{\langle f(x)\rangle}$ then $\theta : \frac{R[x]}{\langle h(x)\rangle} \to \frac{R[x]}{\langle f(x)\rangle}$ is an isomorphism since $h(\omega) = 0$ and $\det W = 1$. Note that this one is not isometry, because $\theta(x^2) = x^2 + 2x + 1$.

We know that isometrically equivalent linear codes have both the same algebraic structure and distance properties thus it will be nice to know when two polycyclic ambient spaces are isometric or not. In [8], Dinh and Li classify all isometrically equivalent classes of constacyclic codes and only study representatives of equivalent classes. The previous example shows that $\mathcal{R}_f$ and $\mathcal{R}_h$ are not necessarily isometrically equivalent for different polynomials f, h of the same degree even if they are isomorphic. In the rest of this section we will describe when a polycyclic ambient space $\mathcal{R}_f$ is isometrically equivalent to another one. Notice that the isomorphism θ is an isometry if and only if W is a monomial matrix.

Proposition 5.4. *With the notation above, W is a monomial matrix if and only if either $f(x) = x^n - f_0$ and $\omega_i x^i$, where $f_0, \omega_i \in R^*$ and $(n, i) = 1$ or $f(x) = x^n - f_1 x$ and $\omega = \omega_j x^j$, where $f_1, \omega_j \in R^*$ and $(n - 1, j) = 1$*

Proof. We know that W is monomial if and only if

$$\{\omega^k \,:\, 1 \leqslant k \leqslant n-1\} = \{a_i x^i \,:\, 1 \leqslant i \leqslant n-1, a_i \in R^*\}. \tag{12}$$

Suppose that W is monomial. Let $w = w_0 + w_1 x + \dots w_{n-1}x^{n-1}$ and $f(x) = x^n - \lambda(x)$. Since W is monomial, w can not be the sum of two terms or more. So there is $i, 1 \leqslant i \leqslant n-1$, such that $\omega = \omega_i x^i$ and $\omega_i \in R^*$. Moreover, if $\lambda(x)$ is the sum of two terms or more, then there is $k, 1 \leqslant k \leqslant n-1$, such that ω^k is the sum of two terms, a contradiction. So $\lambda(x) = f_0$, $f_0 \in R^*$ or $\lambda(x) = f_1 x$, $f_1 \in R^*$. Notice that if $\lambda(x) = f_t x^t, t \geqslant 2$, then $f(x)$ is not in $\mathcal{J}$. In the case $f(x) = x^n - f_1 x$, let $(n-1, j) = k > 1$. Then there is t_1, $t_2 < n-2$ such that $kt_1 = j$ and $kt_2 = n-1$. We obtain $\omega^{t_2} = x^{jt_2} = x^{kt_1 t_2} = x^{nt_1} x^{-t_1} = 1$, a contradiction with (12). With a similar discussion in the other case, we prove $(n, i) = 1$.

Conversely, let $f(x) = x^n - f_1 x$ and $\omega = \omega_j x^j$. The left side of inclusion in (12) is trivial. For the other direction, by contradiction assume that there are k_1, $k_2 < n$ such that $k_1 \neq k_2$ and $\omega^{k_1} = \omega^{k_2}$. So $x^{k_1 j} = x^{(n-1)+k_2 j}$ and hence $(k_1 - k_2)j = n - 1$. A similar discussion occurs for the case $f(x) = x^n - f_0$. □

Corollary 5.5.

1. *Let $f(x) = x^n - f_0$ and $\omega = \omega_i x^i$, where $(n, i) = 1$ and $f_0, \omega_i \in R^*$. Then $\mathcal{M}_{1,n}(R, f)$ and $\mathcal{M}_{1,n}(R, x^n - \omega_i^n f_0)$ are isometric.*
2. *Let $f(x) = x^n - f_1 x$ and $\omega = \omega_j x^j$, where $(n-1, j) = 1$ and $f_1, \omega_j \in R^*$. Then $\mathcal{M}_{1,n}(R, f)$ and $\mathcal{M}_{1,n}(R, x^n - \omega_j^{n-1} f_1^j x)$ are isometric.*

As a corollary we can recover the result [2, Theorem 4.3] as follows.

Corollary 5.6. *Let n be an integer and there is $\lambda \in R^*$ such that n^{th} root of λ is an element in R^*. Then λ-constacyclic code of length n is isometrically equivalent to the cyclic code of length n.*

Proof. Choose an integer $i < n$ such that $(n, i) = 1$. We know there is an element $\omega_i \in R^*$ such that $\omega_i^n = \lambda$. Then $\mathcal{M}_{1,n}(R, x^n - \lambda)$ and $\mathcal{M}_{1,n}(R, x^n - 1)$ are isometric. □

Example 5.7. Let $f(x) = x^6 - f_1 x$ and $\omega = \omega_4 x^4$, where $f_1, \omega_4 \in R^*$. Then

$$W = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \omega_4 & 0 \\ 0 & 0 & 0 & \omega_4^2 f_1 & 0 & 0 \\ 0 & 0 & \omega_4^3 f_1^2 & 0 & 0 & 0 \\ 0 & \omega_4^4 f_1^3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \omega_4^5 f_1^3 \end{bmatrix}.$$

We have $\omega^6 = \omega_4^6 f_1^4 x^4$ and hence by Remark 5.2

$$[h_0 \ h_1 \ \dots \ h_6] = [0 \ 0 \ 0 \ 0 \ \omega_4^6 f_1^4 \ 0] W^{-1} = [0 \ \omega_4^5 f_1^4 \ 0 \ 0 \ 0 \ 0].$$

Then $h(x) = x^6 - \omega_4^5 f_1^4 x$.

6. Multivariable serial codes and transform domain

From now on we will assume that R is a chain ring. A multivariable serial code over R is an ideal of the ring $R[x_1, \dots, x_r]/\langle f_1(x), \dots, f_r(x_r)\rangle$, where $f_i(x) \in \mathcal{J}$ for all $i = 1, \dots, r$, for an account on serial codes see [21]. In this section we will propose a transform approach to those codes defining it duality. For the sake of simplicity all results in this section will be proved for $r = 2$ and can be straightforward worked out for $r > 2$. Let $f_1(x), f_2(x)$ be polynomials in $R[x]$ of degree n_1, n_2, respectively, we will

denote the multivariable ring $R[x_1, x_2]/\langle f_1(x_1), f_2(x_2)\rangle$ by $\mathcal{R}_{f_1,f_2}$. There is an extension R' of R such that f_1 and f_2 splits over R'. Let $\{\alpha_1, \ldots, \alpha_{n_1}\}$ be a fixed ordering of roots of f_1 in R' and $\{\beta_1, \ldots, \beta_{n_2}\}$ be that of f_2 in R'.

The tensor product of two R-modules A, B is an R-module denoted by $A \otimes B$ with multiplication $(a \otimes b)(c \otimes d) = ac \otimes db$. If A, B are free R-modules with basis X_1, X_2, respectively, then $\{x_1 \otimes x_2 : x_1 \in X_1, x_2 \in X_2\}$ is a basis of $A \otimes B$. If A, B are free R-modules and I be a submodule of free R-module $A \otimes B$, then there are submodules $I_1 \in A$ and $I_2 \in B$ such that $I = I_1 \otimes I_2$. If $f : A \to B$ and $g : A' \to B'$ be R-module isomorphisms, then $f \otimes g : A \otimes B \to A' \otimes B'$ defended as $(f \otimes g)(x \otimes y) = f(x) \otimes g(y)$ is an R-module isomorphism. Tensor product over direct sum of modules is distributive.

Recall that the tensor product of matrices A of size $m \times n$ and B of size $p \times q$ (denote by $\otimes$) is $mp \times nq$ matrix $A \otimes B = (a_{i,j}B)$. If A and B are square matrices, then $\det(A \otimes B) = (\det A)^m (\det B)^p$ and $\operatorname{tr}(A \otimes B) = (\operatorname{tr} A)(\operatorname{tr} B)$. Also for matrices A, A', B, B' we have that $(A \otimes B)(A' \otimes B') = (AA') \otimes (BB')$ mixes the ordinary matrix product and tensor product (mixed-product property). For more information on the tensor product of modules and matrices the reader can refer to [13].

Example 6.1. This example is for clarifying the influence of the basis one can choose. Let the polynomials $f(x) = f_1 + f_2 x$ in $R[x]$ and $g(y) = g_0 + g_1 y + g_2 y^2$ in $R[y]$ and also consider the basis $\beta = \{1, y, y^2, x, xy, xy^2\}$ on $\mathcal{R}_{f,g}$. By computing the representation matrix of elements of $\mathcal{R}_{f,g}$ we see that they are related to companion matrices E_f and E_f as follows:

1. the representation matrix x is $E_f \otimes \mathrm{Id}_3$
2. the representation matrix y is $\mathrm{Id}_2 \otimes E_g$
3. the representation matrix xy is $E_f \otimes E_g$
4. the representation matrix xy^2 is $E_f \otimes E_g^2$
5. the representation matrix y^2 is $\mathrm{Id}_2 \otimes E_g^2$

Thus $\beta' = \{\mathrm{Id}_2 \otimes \mathrm{Id}_3, \mathrm{Id}_2 \otimes E_g, \mathrm{Id}_2 \otimes E_g^2, E_f \otimes \mathrm{Id}_3, E_f \otimes E_g, E_f \otimes E_g^2\}$ is its associated basis for the representation matrices. Note that if we choose now another basis $\beta = \{1, x, y, y^2, xy, xy^2\}$, the representation matrix of elements is not equal to tensor product of E_f, E_g, like above, but after permutation on rows of the representation matrix we see that both will be equal.

Consider basis $\theta = \{\theta_1, \ldots, \theta_{n_1 n_2}\}$ for the multivariable ring $\mathcal{R}_{f_1,f_2}$ described in above example. A matrix representation of each element of $\mathcal{R}_{f_1,f_2}$ can be computed with respect to the basis θ. Recall that notations $\mathcal{M}_{n_1}(R, f_1), \mathcal{M}_{n_2}(R, f_2)$ are used for matrix representations of rings $R[x_1]/f_1(x_1), R[x_2]/f_2(x_2)$, respectively. By Theorem 1.3 and mixed-product property, it is obvious that $\mathcal{M}_{n_1}(R, f_1) \otimes \mathcal{M}_{n_1}(R, f_2)$ is commutative. Let ρ denote a map from $\mathcal{R}_{f_1 f_2}$ onto coefficients $x_1^i x_2^j$. Then the map $M : \mathcal{R}_{f_1 f_2} \to \mathcal{M}_{n_1}(R, f_1) \otimes \mathcal{M}_{n_1}(R, f_2)$ is defined by

$$M(k(x_1,x_2)) = \begin{bmatrix} \rho(\theta_1 k(x_1,x_2)) \\ \rho(\theta_2 k(x_1,x_2)) \\ \vdots \\ \rho(\theta_{n_1 n_2} k(x_1,x_2)) \end{bmatrix}$$

is the regular representation of $\mathcal{R}_{f_1,f_2}$ with respect to θ. In fact M maps element $k(x,y) = \sum_i^{n_1-1}\sum_j^{n_2-1} k_{ij}x_1^i x_2^j$ to $\sum_i^{n_1-1}\sum_j^{n_2-1} k_{ij}E_{f_1}^i \otimes E_{f_2}^j$. Clearly M is an isomorphism. Note also that this fact arises from the fact that $R[x_1,x_2]/\langle f_1(x_1), f_2(x_2)\rangle \cong R[x_1]/\langle f_1(x_1)\rangle \otimes R[x_2]/\langle f_2(x_2)\rangle$, see [5], moreover it is a principal ideal ring if both $\mathcal{R}_f$ and $\mathcal{R}_f$ are principal ideal rings, see [4].

Let $V_{f_1} = V(\alpha_1,\ldots,\alpha_{n_1})$ and $V_{f_2} = V(\beta_1,\ldots,\beta_{n_1})$ be the Vandermonde matrices associated to f and g respectively. We know that the image of the companion matrices E_{f_1}, E_{f_2} by γ is diagonalizable by V_{f_1}, V_{f_2}, respectively. Denote $V = V_{f_1} \otimes V_{f_2}$ and suppose that $k(x_1,x_2) \in \mathcal{R}_{f_1,f_2}$ is an arbitrary element. For simplicity we take $M(K(x_1,x_2)) = \gamma(M(K(x_1,x_2)))$, then

$$\begin{aligned}
M(K(x_1,x_2))V &= \sum_i^{n_1-1}\sum_j^{n_2-1} k_{ij}(E_{f_1}^i \otimes E_{f_2}^j)(V_{f_1} \otimes V_{f_2}) \\
&= \sum_i^{n_1-1}\sum_j^{n_2-1} k_{ij}(E_{f_1}^i V_{f_1}) \otimes (E_{f_2}^j V_{f_2}) \\
&= \sum_i^{n_1-1}\sum_j^{n_2-1} k_{ij}(V_{f_1}\,\mathrm{diag}[\alpha_1,\ldots,\alpha_{n_1}]) \otimes (V_{f_2}\mathrm{diag}[\beta_1,\ldots,\beta_{n_2}]) \\
&= \sum_i^{n_1-1}\sum_j^{n_2-1} k_{ij}(V_f \otimes V_g)(\mathrm{diag}[\alpha_1,\ldots,\alpha_{n_1}] \otimes \mathrm{diag}[\beta_1,\ldots,\beta_{n_2}]) \\
&= V\sum_i^{n_1-1}\sum_j^{n_2-1} k_{ij}\mathrm{diag}[\alpha_1,\ldots,\alpha_{n_1}] \otimes \mathrm{diag}[\beta_1,\ldots,\beta_{n_2}] \\
&= V(\mathrm{diag}[k(\alpha_1,\beta_1),\ldots,k(\alpha_1,\beta_{n_2}),\ldots,k(\alpha_{n_1},\beta_1),\ldots,k(\alpha_{n_1},\beta_{n_2})]).
\end{aligned}$$

Recall that since $f_1, f_2 \in \mathcal{J}$ then V_{f_1} and V_{f_2} are non-singular. Therefore, since $\det(V) = (\det V_{f_1})^{n_1}(\det V_{f_2})^{n_2}$ then V is non-singular. Hence $M(K(x_1,x_2))$ is diagonalized by V and its eigenvalues are related to the roots of f and g as above.

Now we are able to define multivariable Mattson-Solomon transform for serial codes as follows.

$$\begin{array}{rccc}
MS_{f_1,f_2}: & (\mathcal{R}_{f_1,f_2},\cdot) & \longrightarrow & (R'[x_1,x_2]/\langle f_1(x_1), f_2(x_2)\rangle, \star) \\
& k(x_1,k_2) & \mapsto & \displaystyle\sum_i^{n_1}\sum_j^{n_2} k(\alpha_i,\beta_j)x_1^{i-1}x_2^{j-1},
\end{array} \tag{13}$$

where . denotes ordinary polynomial multiplication modulo $f_1(x_1), f_2(x_2)$ and $\star$ denotes the component-wise multiplication. We define the inner product $\langle , \rangle_\star$ over $R'[x_1, x_2]/\langle f_1(x_1), f_2(x_2)\rangle$ as in (7). The dual of the polycyclic code $\mathcal{C}$ with respect to this inner product is denoted by $\mathcal{C}^{\perp_\star}$, and furthermore, we define trace inner product on $\mathcal{R}_{f_1,f_2}$ as

$$\langle k_1(x_1,x_2), k_2(x_1,x_2)\rangle_{tr} = \mathrm{trace}(M(k_1(x_1,x_2)k_2(x_1,x_2))). \tag{14}$$

Since V is non-singular, then trace inner product is non-degenerate. Denote the trace dual of the multivariable code $\mathcal{C}$ by $\mathcal{C}^{\perp_{tr}}$. The following result is proven as Proposition 3.2.

Proposition 6.2. *Let $k_1(x_1,x_2), k_2(x_1,x_2) \in \mathcal{R}_{f_1,f_2}$, then*

$$\langle k_1(x_1,x_2), k_2(x_1,x_2)\rangle_{tr} = 0 \iff \langle MS_{f_1,f_2}(k_1(x_1,x_2),),\ MS_{f_1,f_2}(k_2(x_1,x_2),)\rangle_\star = 0$$

Lemma 6.3 *([21]). There is a complete set of central orthogonal idempotents in $\mathcal{R}_{f_1,f_2}$.*

The proof of the result follows from Proposition 3.7 and Remark 5 in [21] where an explicit construction of such idempotents is made.

Taking into account the previous result and the proof of Theorem 3.3 it is easy to proof the following theorem.

Theorem 6.4. *Let R be a finite chain ring. If $\mathcal{C}$ is a multivariable code in $\mathcal{R}_{f_1f_2}$ we have*

$$\mathcal{C}^{\perp_{\mathrm{tr}}} = \mathcal{C}^{\perp_\star} = \mathrm{Ann}(\mathcal{C}).$$

Assume that $\{e_k\}_{k\in K}$ is the complete set of centrally orthogonal idempotents in $\mathcal{R}_{f_1,f_2}$. Also assume that $f_1 = \prod_{i\in I} p_i$ and $f_2 = \prod_{j\in J} q_j$ are pairwise coprime decompositions of f_1, f_2 and $\{e_i\}_{i\in I}$ and $\{e_j\}_{j\in J}$ are the complete set of centrally orthogonal idempotents in $\mathcal{R}_{f_1}$ and $\mathcal{R}_{f_2}$, respectively. Let us set $U_i \subseteq \mathcal{M}_{1,n_1}(R, f_1)$ as $U_i = \ker p_i(E_{f_1})$ and $U_j \subseteq \mathcal{M}_{1,n_2}(R, f_2)$ as $U_j = \ker q_j(E_{f_2})$. We know that $\mathcal{R}_{f_1f_2} \cong \mathcal{R}_{f_1} \otimes \mathcal{R}_{f_2}$, thus by CRT theorem, Proposition 4.1 and the distributivity of tensor product over direct sum we have

$$\begin{aligned}\bigoplus_{k\in K} \mathcal{R}_{f_1,f_2}e_k &\cong \mathcal{R}_{f_1,f_2}\\ &\cong (\bigoplus_{i\in I} \mathcal{R}_{f_1}e_i) \otimes (\bigoplus_{j\in J} \mathcal{R}_{f_2}e_j)\\ &= \bigoplus_{i\in I}\bigoplus_{j\in J} (R_{f_1}e_i \otimes R_{f_2}e_j).\end{aligned}$$

Note that a primitive central idempotent in $A \otimes B$ is the tensor product of primitive central idempotents of A and B, and therefore with above notations, we have following results similar to Proposition 4.1 and Theorem 4.2.

Proposition 6.5.

1. *For e_k there is p_i and q_j such that $\mathcal{R}_{f_1,f_2}e_k \cong Ann(p_i) \otimes Ann(q_j)$.*
2. *$c \in \mathcal{R}_{f_1,f_2}e_k$ if and only if $e_k c = c$.*
3. *$M(e_k)$ is the generator matrix of the multivariable serial code $\mathcal{R}_{f_1,f_2}e_k$.*
4. *$M(e_k)$ is invariant under multiplication by matrices $E^n_{f_1} \otimes E^m_{f_2}$, where $0 \leqslant n \leqslant n_1 - 1$ and $0 \leqslant m \leqslant n_2 - 1$. Moreover $\{M(e_k)\}_{k\in K}$ are idempotent matrices and pairwise orthogonal.*
5. *The image of a multivariable serial code under M is an invariant ideal under multiplication by all $E^n_{f_1} \otimes E^m_{f_2}$, where $0 \leqslant n \leqslant n_1 - 1$ and $0 \leqslant m \leqslant n_2 - 1$.*
6. *$U_i \otimes U_j \cong \mathcal{R}_{f_1,f_2}e_k$ for some i, j.*

Theorem 6.6. *We have*

$$\mathcal{R}_{f_1,f_2} \cong \bigoplus_{i\in I} \bigoplus_{j\in J} (U_i \otimes U_j)$$

1. *Each of the above summands is an indecomposable multivariable serial code with $E^n_{f_1} \otimes E^m_{f_2}$-invariant image in $\mathcal{M}_{n_1}(R, f_1) \otimes M_{n_2}(R, f_2)$ for all $0 \leqslant n \leqslant n_1 - 1, 0 \leqslant m \leqslant n_2 - 1$.*
2. *Each multivariable serial code $\mathcal{C} \subseteq \mathcal{R}_{f_1,f_2}$ can be seen as a direct sum of $U_i \otimes U_j$ for some indices i, j.*
3. *If a serial code $\mathcal{C}$ decomposes as $\mathcal{C} \cong \bigoplus_{i\in I_1} \bigoplus_{j\in J_1} U_i \otimes U_j$, for $I_1 \subseteq I, J_2 \subseteq J$, then*

$$\mathcal{C}^{\perp_{tr}} \cong \left(\bigoplus_{i\in I_1} \bigoplus_{j\in J_1} U_i \otimes U_j \right)^c = \bigoplus_{i\notin I_1} \bigoplus_{j\notin J_1} U_i \otimes U_j$$

Remark 6.7. Note that during this section we only needed the ring R to be a chain ring in those parts where those results of the construction of the idempotents in [21] where needed.

Now we return to the general case where R is local ring. Assume that polynomials $f_1(x_1), h_1(x_1) \in R[x_1]$ have the same degree of n_1 and $f_2(x_2), h_2(x_2) \in R[x_2]$ have the same degree of n_2. The main question is that when multivariable codes over rings $\mathcal{R}_{f_1,f_2}$ and $\mathcal{R}_{h_1,h_2}$ are isometric. We know that

$$\mathcal{R}_{f_1,f_2} \cong \mathcal{M}_{n_1}(R, f_1) \otimes \mathcal{M}_{n_2}(R, f_2) \cong \mathcal{M}_{1,n_1}(R, f_1) \otimes \mathcal{M}_{1,n_2}(R, f_2).$$

Moreover, we know that the tensor product of two submodules of free modules $\mathcal{M}_{1,n_1}(R, f_1), \mathcal{M}_{1,n_2}(R, f_2)$, is a submodule of their tensor product. Now applying Corollary 5.5, we conclude that

Proposition 6.8.

1. *Let* $f_1(x_1) = x_1^{n_1} - \lambda_1$ *and* $\omega_1 = \omega_i x_1^i$ *where* $(n_1, i) = 1$, $\lambda_1, \omega_i \in R^*$.
   Also let $f_2(x_2) = x_2^{n_2} - \lambda_2$ *and* $\omega_2 = \omega_j x_2^j$ *where* $(n_2, j) = 1$, $\lambda_2, \omega_j \in R^*$. *Then* $R[x_1, x_2]/\langle f_1(x_1), f_2(x_1)\rangle$ *and* $R[x_1, x_2]/\langle x_1^{n_1} - \omega_i^{n_1}\lambda_1, x_2^{n_2} - \omega_j^{n_2}\lambda_2\rangle$ *are isometric.*
2. *Let* $f_1(x_1) = x_1^{n_1} - \lambda_1$ *and* $\omega_1 = \omega_i x_1^i$ *where* $(n_1, i) = 1$, $\lambda_1, \omega_i \in R^*$.
   Also let $f_2(x_2) = x_2^{n_2} - \lambda_2 x_2$ *and* $\omega_2 = \omega_j x_2^j$ *where* $(n_2 - 1, j) = 1$, $\lambda_2, \omega_j \in R^*$. *Then* $R[x_1, x_2]/\langle f_1(x_1), f_2(x_1)\rangle$ *and* $R[x_1, x_2]/\langle x_1^{n_1} - \omega_i^{n_1}\lambda_1, x_2^{n_2} - \omega_j^{n_2-1}\lambda_2^j x_2\rangle$ *are isometric.*
3. *Let* $f_1(x_1) = x_1^{n_1} - \lambda_1 x_1$ *and* $\omega_1 = \omega_i x_1^i$ *where* $(n_1 - 1, i) = 1$, $\lambda_1, \omega_i \in R^*$.
   Also let $f_2(x_2) = x_2^{n_2} - \lambda_2 x_2$ *and* $\omega_2 = \omega_j x_2^j$ *where* $(n_2 - 1, j) = 1$, $\lambda_2, \omega_j \in R^*$. *Then* $R[x_1, x_2]/\langle f_1(x_1), f_2(x_1)\rangle$ *and* $R[x_1, x_2]/\langle x_1^{n_1} - \omega_i^{n_1-1}\lambda_1^i x_1, x_2^{n_2} - \omega_j^{n_2-1}\lambda_2^j x_2\rangle$ *are isometric.*

7. Conclusions

In the present paper, we have developed a transform approach to polycyclic codes under the hypothesis that the polynomial defining the ambient space is multiplicity free which is equivalent, in the cyclic codes case, to the coprimality of the length and the alphabet size. We have also extended that approach to multivariable serial codes under an equivalent hypothesis. The main open problem is to derive a similar approach for the repeated root case, at least for the case when the ambient space is a principal ideal ring [20].

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] Aicha Batoul, Kenza Guenda, T. Aaron Gulliver, Some constacyclic codes over finite chain rings, Adv. Math. Commun. 10 (4) (2016) 683–694.
[3] William C. Brown, Matrices over Commutative Rings, Monographs and Textbooks in Pure and Applied Mathematics, vol. 169, Marcel Dekker, Inc., New York, 1993.
[4] J. Cazaran, A.V. Kelarev, On finite principal ideal rings, Acta Math. Univ. Comen. 68 (1) (1999) 77–84.
[5] Jilyana Cazaran, Tensor products and quotient rings which are finite commutative principal ideal rings, Math. J. Okayama Univ. 41 (1999) 1–14.
[6] Mohammed Elhassani Charkani, Joël Kabore, Primitive idempotents and constacyclic codes over finite chain rings, Gulf J. Math. 8 (2) (2020) 55–67.
[7] David Chillag, Regular representations of semisimple algebras, separable field extensions, group characters, generalized circulants, and generalized cyclic codes, Linear Algebra Appl. 218 (1995) 147–183.
[8] Hai Q. Dinh, Chengju Li, Qin Yue, Recent progress on weight distributions of cyclic codes over finite fields, J. Algebra Comb. Discrete Struct. Appl. 2 (1) (2015) 39–63.
[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 (1973) 521–540.
[11] Jian Gao, Linzhi Shen, Fang-Wei Fu, Bounds on quasi-cyclic codes over finite chain rings, J. Appl. Math. Comput. 50 (1–2) (2016) 577–587.

[12] Marcus Greferath, Thomas Honold, Cathy Mc Fadden, Jay A. Wood, Jens Zumbrägel, MacWilliams' extension theorem for bi-invariant weights over finite principal ideal rings, J. Comb. Theory, Ser. A 125 (2014) 177–193.
[13] Nathan Jacobson, Basic Algebra. II, second edition, W. H. Freeman and Company, New York, 1989.
[14] V.L. Kurakin, A.S. Kuzmin, V.T. Markov, A.V. Mikhalev, A.A. Nechaev, Linear codes and polylinear recurrences over finite rings and modules (a survey), in: Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Honolulu, HI, 1999, in: Lecture Notes in Comput. Sci., vol. 1719, Springer, Berlin, 1999, pp. 365–391.
[15] D. Laksov, Diagonalization of matrices over rings, J. Algebra 376 (2013) 123–138.
[16] Shuxing Li, Maosheng Xiong, Gennian Ge, Pseudo-cyclic codes and the construction of quantum MDS codes, IEEE Trans. Inf. Theory 62 (4) (2016) 1703–1710.
[17] 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.
[18] 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.
[19] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes. II, North-Holland Mathematical Library, vol. 16, North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977.
[20] 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.
[21] E. Martínez-Moro, I.F. Rúa, Multivariable codes over finite chain rings: serial codes, SIAM J. Discrete Math. 20 (4) (2006) 947–959.
[22] James L. Massey, Codes and ciphers: Fourier and Blahut, in: Codes, curves, and signals, Urbana, IL, 1997, in: Kluwer Internat. Ser. Engrg. Comput. Sci., vol. 485, Kluwer Acad. Publ., Boston, MA, 1998, pp. 105–119.
[23] James L. Massey, The discrete Fourier transform in coding and cryptography, in: IEEE Inform. Theory Workshop, ITW 98, 1998, pp. 9–11.
[24] Graham H. Norton, Ana Salagean-Mandache, On the key equation over a commutative ring, Des. Codes Cryptogr. 20 (2) (2000) 125–141.
[25] E. Rawashdeh, A Simple Method for Finding the Inverse Matrix of a Vandermonde Matrix, 2019.
[26] Minjia Shi, Xiaoxiao Li, Zahra Sepasdar, Patrick Solé, Polycyclic codes as invariant subspaces, Finite Fields Appl. 68 (14) (2020), Id/No 101760.
[27] 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.
[28] Minjia Shi, Li Xu, Patrick Solé, Construction of isodual codes from polycirculant matrices, Des. Codes Cryptogr. 88 (12) (2020) 2547–2560.
[29] 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.
[30] S. Veldsman, Rings of matrices generated by a companion matrix, Acta Math. Hung. 140 (1–2) (2013) 12–33.