Filomat 35:10 (2021), 3407–3421
https://doi.org/10.2298/FIL2110407O

Published by Faculty of Sciences and Mathematics,
University of Niš, Serbia
Available at: http://www.pmf.ni.ac.rs/filomat

On the Algebraic Structure of Polycyclic Codes

Hassan Ou-Azzou[a], Mustapha Najmeddine[a]

[a] *Department of mathematics, ENSAM–Meknes, Moulay Ismail university*

Abstract. In this paper, we are interested in the study of the right polycyclic codes as invariant subspaces of $\mathbb{F}_q^n$ by a fixed operator T_R. This approach has helped in one hand to connect them to the ideals of the polynomials ring $\mathbb{F}_q[x]/\langle f(X)\rangle$, where $f(x)$ is the minimal polynomial of T_R. On the other hand, it allows to prove that the dual of a right polycyclic code is invariant by the adjoint operator of T_R. Hence, when T_R is normal we prove that the dual code of a right polycyclic code is also a right polycyclic code. However, when T_R isn't normal the dual code is equivalent to a right polycyclic code. Finally, as in the cyclic case, the BCH-like and Hartmann-Tzeng-like bounds for the right polycyclic codes on Hamming distance are derived.

1. Introduction

Polycyclic codes (known under name pseudo-cyclic [10]) of length n over a finite field $\mathbb{F}_q$ with $q-$elements, are an important subclass of linear codes. As they can be described by the ideals of the polynomials ring $\mathbb{F}_q[x]/\langle f(x)\rangle$, where $f(x)$ id a non zero polynomial in $\mathbb{F}_q[x]$. They are better studied under that name in [1] over $\mathbb{F}_q$. A generalization over a finite ring alphabet is presented in [11, 12]. Over finite fields, these codes generalize constacyclic codes when $f = x^n - \lambda$, for some non-zero λ in $\mathbb{F}_q$, and its derivatives cyclic codes ($\lambda = 1$) and negacyclic codes ($\lambda = -1$).

A linear code $C \subseteq \mathbb{F}_q^n$ is said to be right polycyclic code with associate vector $R = (r_0, r_1, \ldots, r_{n-1})$ if for each codeword $c = (c_0, c_1, \ldots, c_{n-1})$ of C the codeword $(0, c_0, \ldots, c_{n-2}) + c_{n-1}(r_0, r_1, \ldots, r_{n-1})$ is also in C [1]. Based on the algebraic approach developed in [2] to constacyclic codes we observe that the right polycyclic codes are the invariant subspaces of $\mathbb{F}_q^n$ by the operator T_R defined by $T_R(a_0, a_1, \ldots, a_{n-1}) = (a_{n-1}r_0, a_0 + a_{n-1}r_1, \ldots, a_{n-2} + a_{n-1}r_{n-1})$, where the minimal polynomial of T_R is $f(x) = x^n - R(x)$, such that $R(x) = r_0 + r_1x + r_2x^2 + \cdots + r_{n-1}x^{n-1}$. A similar idea is developed in [13] for polycyclic codes, where the authors use the characteristic polynomial of the same operator to investigate the algebraic structure of polycylic codes by the invariant subspaces of $\mathbb{F}_q^n$.

In this paper we observe that the operator T_R is a cyclic i.e the minimal polynomial and characteristic polynomial are same. based on this observation we start by proving the one to one correspondence between the invariant subspaces of $\mathbb{F}_q^n$ by a cyclic operator T and the ideals of the polynomials ring $\mathbb{F}_q[x]/\langle \pi_T(x)\rangle$, where $\pi_T(x)$ is the minimal polynomial of T. As application, this permits to connect the right polycyclic codes to the ideals of $\mathbb{F}_q[x]/\langle f(x)\rangle$. In the same way as in [2, 13], the notion of the minimal invariant subspaces is

2020 *Mathematics Subject Classification*. Primary 11T60
Keywords. Cyclic code, polycyclic code, cyclic operator, invariant subspace, BCH and Hartmann-Tzeng bound
Received: 29 December 2020; Accepted: 03 February 2021
Communicated by Paola Bonacin
Email addresses: hassanpfe24@gmail.com (Hassan Ou-Azzou), m.najmeddine@umi.ac.ma (Mustapha Najmeddine)

introduced, driven from the irreducible factorization of $f(x)$ over $\mathbb{F}_q$, which asserts when the polynomial order of $f(x)$ is coprime with the size of $\mathbb{F}_q$, we decompose any right polycyclic code as a direct sum of minimal right polycyclic codes. Next, we give some important results on duality of these codes, where we show that the dual of a right polycyclic code is also polycyclic, when T_R is a normal operator. However, when T_R isn't normal the dual code is equivalent to a right polycyclic code. Finally, we use the polynomial order of $f(x)$ over $\mathbb{F}_q$ to derive the BCH-like and Hartmann-Tzeng-like bounds for right polycyclic codes on Hamming distance like as in the cyclic case.

In this paper, we start with necessary backgrounds on the right polycyclic codes and on the order of polynomials over $\mathbb{F}_q$. Secondly, we prove the one to one correspondence between the $T-$invariant subspaces of $\mathbb{F}_q^n$ and the ideals of the principal polynomials ring $\mathbb{F}_q[x]/\langle \pi_T(x)\rangle$, where T is a cyclic operator with minimal polynomial $\pi_T(x)$ [Theorem1]. As consequence, the right polycyclic codes with associate vector $R = (r_0, r_1, \ldots, r_{n-1}) \in \mathbb{F}_q^n$ are seen as the ideals of $\mathbb{F}_q[x]/\langle f(x)\rangle$. Some algebraic properties of these codes are discussed in [Theorem3 , Theorem4]. Also, some results on the duality of the right polycyclic codes with respect to the standard inner product on $\mathbb{F}_q^n$ are surveyed. Finally, we prove in [Theorem8, Theorem9] the BCH-like and Hartmann-Tzeng-like bounds on Hamming distance of these codes using the order of $f(x)$ over $\mathbb{F}_q$.

2. Preliminaries

This section is devoted to recall the necessary background that we need throughout this paper.

Definition 1 ([1], Definition 2.1.)
Let $C \subseteq \mathbb{F}_q^n$ be a linear code of length n over $\mathbb{F}_q$.

1. C is called a right polycyclic code with associate vector $R = (r_0, r_1, \ldots, r_{n-1}) \in \mathbb{F}_q^n$ if for each $c = (c_0, c_1, \ldots, c_{n-1}) \in C$ we have $(0, c_0, \ldots, c_{n-2}) + c_{n-1}(r_0, r_1, \ldots, r_{n-1}) \in C$.
2. C is called a left polycyclic code with associate vector $L = (l_0, l_1, \ldots, l_{n-1}) \in \mathbb{F}_q^n$ if for each $c = (c_0, c_1, \ldots, c_{n-1}) \in C$ we have $(c_1, \ldots, c_{n-1}, 0) + c_0(l_0, l_1, \ldots, l_{n-1}) \in C$.

Example 1
Let us recall that a linear code $C \subseteq \mathbb{F}_q^n$ of length n over $\mathbb{F}_q$ is called $\lambda-$constacyclic code if for each $(v_0, v_1, \ldots, v_{n-1}) \in C$ we have $(\lambda v_{n-1}, v_0, \ldots, v_{n-2})$ is also in C, where λ is a non-zero element of $\mathbb{F}_q$. Hence C is a right polycyclic code with associate vector $R_\lambda = (\lambda, 0, \ldots, 0)$. Also, cyclic codes ($\lambda = 1$) and negacyclic codes ($\lambda = -1$) are right polycyclic codes.

Associate to $R = (r_0, r_1, \ldots, r_{n-1}) \in \mathbb{F}_q^n$ the polynomial $R(x) = r_0 + r_1 x + r_2 x^2 + \cdots + r_{n-1}x^{n-1}$, and consider the realization φ_R defined by

$$\begin{array}{rccc} \varphi_R & : & \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q[x]/\langle x^n - R(x)\rangle \\ & & (a_0, a_1, \ldots, a_{n-1}) & \longmapsto & \sum_{i=0}^{n-1} a_i x^i \end{array} \tag{1}$$

It is shown in [1] that the right polycyclic codes with associate vector $R = (r_0, r_1, \ldots, r_{n-1})$ are the ideals of the polynomials ring $\mathbb{F}_q[x]/\langle x^n - R(x)\rangle$, via φ_R. Also, all the left polycyclic codes with associate vector $L = (l_0, l_1, \ldots, l_{n-1})$ are the ideals of the polynomials ring $\mathbb{F}_q[x]/\langle x^n - L(x)\rangle$, via a chosen realization φ_L, where $L(x) = l_{n-1} + l_{n-2}x + \cdots + l_0 x^{n-1}$. Then, as in the case of the cyclic codes, the irreducible factorization of $x^n - R(x)$ (resp. $x^n - L(x)$) permits to construct all the right polycyclic codes of length n with associate vector R (resp. all the right polycyclic codes of length n with associate vector L). In the following proposition, we regroup some basic results on the right polycyclic codes that are presented in [1].

Proposition 1
Let $C \subseteq \mathbb{F}_q^n$ be a right polycyclic code of length n over $\mathbb{F}_q$ with associate vector $R = (r_0, r_1, \ldots, r_{n-1})$.

1. There is a monic polynomial of least degree $g(x) \in \mathbb{F}_q[x]$ such that $g(x)$ divides $x^n - R(x)$ and $\varphi_R(C) = \langle g(x) \rangle$.
2. The family $\{g(x), xg(x), \ldots, x^{n-\deg(g)-1}g(x)\}$ forms a basis of $\varphi_R(C)$ and the dimension of C is $n - \deg(g)$.
3. A generator matrix G of C is given by :

$$G = \begin{pmatrix} \varphi_R^{-1}(g(x)) \\ \varphi_R^{-1}(xg(x)) \\ \vdots \\ \vdots \\ \varphi_R^{-1}\left(x^{k-1}g(x)\right) \end{pmatrix} = \begin{pmatrix} g_0 & g_1 & \cdots & g_{n-k} & 0 & \cdots & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & \ddots & & \ddots & \vdots \\ 0 & \ldots & & 0 & g_0 & g_1 & \cdots & g_{n-k} \end{pmatrix}$$

where $k = n - \deg(g)$ and $g(x) = \sum_{i=0}^{n-k} g_i x^i$.

Definition 2
A right polycyclic code C with associate vector $R = (r_0, r_1, \ldots, r_{n-1}) \in \mathbb{F}_q^n$ is said to be generated by $g(x)$ if $\varphi_R(C) = \langle g(x) \rangle$, and $g(x)$ is called its generator polynomial.

Let $P(x) \in \mathbb{F}_q[x]$ be a polynomial of degree n with $P(0) \neq 0$. It is shown in [4] that there exists a positive integer $e \leq q^n - 1$ such that $P(x)$ divides $x^e - 1$. The smallest positive integer e with this property is called the polynomial order of $P(x)$ and we write $\mathrm{ord}(P) = e$. If $P(0) = 0$, there is a polynomial $Q(x) \in \mathbb{F}_q[x]$ with $Q(0) \neq 0$ and an integer $h \in \mathbb{N} \setminus \{0\}$ such that $P(x) = x^h Q(x)$. In this case, the order of $P(x)$ is defined to be the order of $Q(x)$.

Remark 1
Note that if $P(x) \in \mathbb{F}_q[x]$, such that $P(0) \neq 0$, is a polynomial with order e such that $\gcd(e, q) = 1$. Then all the roots of $P(x)$ are simple.

Let C be a right polycyclic code with associate vector $R = (r_0, r_1, \ldots, r_{n-1}) \in \mathbb{F}_q^n$ and $f(x) = x^n - R(x)$ of order e. Then the irreducible factorization of $f(x)$ permits to determine all the simple right polycyclic codes when $\gcd(e, q) = 1$.

Example 2
In this example, we propose to construct right polycyclic codes with associate vector $R = (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$ of length 11 over $\mathbb{F}_2$. Let $R(x) = x^8 + x^7 + x^5 + x^3 + x^2 + x + 1$, then $f(x) = x^{11} - R(x)$ is a polynomial of order $e = 15$ over $\mathbb{F}_2$. The irreducible factorization of $f(x)$ is

$$f(x) = (x+1)\left(x^2 + x + 1\right)\left(x^4 + x^3 + 1\right)\left(x^4 + x^3 + x^2 + x + 1\right)$$

As $\gcd(2, 15) = 1$, the linear code C generated by

$$g(x) = \left(x^2 + x + 1\right)\left(x^4 + x^3 + x^2 + x + 1\right) = x^6 + x^4 + x^3 + x^2 + 1$$

is a simple right poycyclic code of length 11 with a generator matrix

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}$$

and the minimum Hamming distance $d_H = 4$.

More generally, in the following table, we list all the non trivial binary right polycyclic codes with associate vector R and all the binary cyclic codes of length 11.

Type of code	Generator polynomial of the code	Dimension	d_H
Right polycyclic codes	$x^7 + x^6 + x^4 + 1$	4	4
	$x^9 + x^8 + x^5 + x^4 + x^3 + 1$	2	6
	$x^{10} + x^9 + x^8 + x^6 + x^5 + x^2 + 1$	1	7
	$x^8 + x^4 + x^2 + x + 1$	3	5
	$x^5 + x^3 + x + 1$	6	4
	$x^6 + x^4 + x^3 + x^2 + 1$	5	4
	$x^5 + 1$	6	2
	$x^3 + 1$	8	2
	$x + 1$	10	2
	$x^6 + x^3 + x^2 + x + 1$	5	3
	$x^4 + x^3 + x^2 + x + 1$	7	2
	$x^7 + x^6 + x^5 + x^2 + x + 1$	4	4
	$x^4 + x^3 + 1$	7	3
	$x^2 + x + 1$	9	2
Cyclic codes	$x + 1$	10	2
	$x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$	1	11

3. Right polycyclic codes as invariant subspaces

Let $\mathbb{F}_q$ be a finite field and $\mathbb{F}_q^n$ be the $n-$dimensional vector space over $\mathbb{F}_q$ with the standard basis $B = \{e_1, e_2, \ldots, e_{n-1}\}$ where, $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$. Recall that a subspace $F \subseteq \mathbb{F}_q^n$ is invariant under an operator T or $T-$invariant if $T(F) \subseteq F$. Recall also that an operator T is called cylic if there is a vector $v_0 \in \mathbb{F}_q^n$ such that the set $B_{v_0} := \left\{v_0; T(v_0); \ldots; T^{n-1}(v_0)\right\}$ is a basis of $\mathbb{F}_q^n$, $T^n(v_0) = \sum_{i=0}^{n-1} m_i T^i(v_0)$ and $\pi_T(x) = x^n - \sum_{i=0}^{n-1} m_i x^i$.

The following theorem gives a characterization of the $T-$invariant subspaces of $\mathbb{F}_q^n$ by the ideals of the polynomials ring $\mathbb{F}_q[x]/\langle \pi_T(x)\rangle$, where T is a cyclic operator with minimal polynomial $\pi_T(x)$.

Theorem 1
Let $T : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$ be a cyclic operator with minimal polynomial $\pi_T(x)$. Then, there is a realization $\varphi : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q[x]/\langle \pi_T(x)\rangle$ between $\mathbb{F}_q^n$ and $\mathbb{F}_q[x]/\langle \pi_T(x)\rangle$, such that

$$T(F) \subseteq F \text{ if, and only if } \varphi(F) \text{ is an ideal of } \mathbb{F}_q[x]/\langle \pi_T(x)\rangle.$$

Proof. As T is a cyclic operator, then there is a vector $v_0 \in \mathbb{F}_q^n$ such that the set $B_{v_0} := \left\{v_0; T(v_0); \ldots; T^{n-1}(v_0)\right\}$ is a basis of $\mathbb{F}_q^n$. Consider the realization φ_{v_0} between $\mathbb{F}_q^n$ and $\mathbb{F}_q[x]/\langle \pi_T(x)\rangle$ defined by :

$$\varphi_{v_0} : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q[x]/\langle \pi_T(x)\rangle : \sum_{i=0}^{n-1} v_i T^i(v_0) \longmapsto \sum_{i=0}^{n-1} v_i x^i. \tag{2}$$

Let F be an invariant subspace of $\mathbb{F}_q^n$, then $(\varphi(F), +)$ is a group. Now, let $a(x) := a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \in \varphi(F)$.

Then, for $a = \sum_{i=0}^{n-1} a_i T^i(v_0) \in F$,

$$\begin{aligned} xa(x) &= x\sum_{i=0}^{n-1} a_i x^i \\ &= \sum_{i=0}^{n-1} a_i x^{i+1} \\ &= \sum_{i=1}^{n-1} a_{i-1} x^i + a_{n-1} x^n \\ &= \sum_{i=1}^{n-1} a_{i-1} x^i + a_{n-1}\left(x^n - \sum_{i=0}^{n-1} m_i x^i\right) + a_{n-1}\sum_{i=0}^{n-1} m_i x^i \\ &= a_{n-1}m_0 + \sum_{i=1}^{n-1} \left(a_{i-1} + a_{n-1}m_i\right) x^i + a_{n-1}\pi_T(x) \\ &= a_{n-1}m_0 + \sum_{i=1}^{n-1} \left(a_{i-1} + a_{n-1}m_i\right) x^i \ \ (mod\ \ \pi_T(x)). \end{aligned} \tag{3}$$

since $\pi_T(x) = x^n - \sum_{i=0}^{n-1} m_i x^i$.
On the other hand,

$$\begin{aligned} T(a) &= T\left(\sum_{i=0}^{n-1} a_i T^i(v_0)\right) = \sum_{i=0}^{n-1} a_i T^{i+1}(v_0) = \sum_{i=1}^{n-1} a_{i-1} T^i(v_0) + a_{n-1} T^n(v_0) \\ &= \sum_{i=1}^{n-1} a_{i-1} T^i(v_0) + a_{n-1}\left(\sum_{i=0}^{n-1} m_i T^i(v_0)\right) \\ &= a_{n-1}m_0 T^0(v_0) + \sum_{i=1}^{n-1} \left(a_{i-1} + a_{n-1}m_i\right) T^i(v_0). \end{aligned} \tag{4}$$

Since $T(F) \subseteq F$, we deduce by (3) and (4), that : $xa(x) = \varphi_{v_0}(T(a)) \in \varphi_{v_0}(F)$. By the inductive argument, for any positive integer k, $x^k a(x) = \varphi_{v_0}(T^k(a)) \in \varphi(F)$. Hence, $\varphi_{v_0}(F)$ is an ideal of $\mathbb{F}_q[x]/\langle \pi_T(x)\rangle$.

Conversely, assume that $\varphi_{v_0}(F)$ is an ideal of $\mathbb{F}_q[x]/\langle \pi_T(x)\rangle$. Let $a = \sum_{i=0}^{n-1} a_i T^i(u_0) \in F$, then the polynomial

$$\varphi_{v_0}(a) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in \varphi_{v_0}(F).$$

Finally, by (3) and (4), we have $\varphi_{v_0}(T(a)) = x\varphi_{v_0}(a) \in \varphi_{v_0}(F)$, Hence $T(F) \subseteq F$.

□

Now, let $R = (r_0, r_1, \ldots, r_{n-1}) \in \mathbb{F}_q^n$ and consider the operator T_R defined by :

$$\begin{array}{rccc} T_R & : & \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q^n \\ & & (a_0, a_1, \ldots, a_{n-1}) & \longmapsto & (a_{n-1}r_0, a_0 + a_{n-1}r_1, \ldots, a_{n-2} + a_{n-1}r_{n-1}) \end{array} \tag{5}$$

The matrix of T_R with respect to the standard basis is

$$A = \begin{pmatrix} 0 & 0 & \dots & 0 & r_0 \\ 1 & 0 & \dots & 0 & r_1 \\ \vdots & 1 & \ddots & \vdots & \vdots \\ \vdots & \dots & \ddots & 0 & \vdots \\ 0 & 0 & \dots & 1 & r_{n-1} \end{pmatrix}$$

As the minimal polynomial $f(x) = x^n - R(x)$ of T_R has degree n and each right polycyclic code is an invariant subspaces by T_R. Then, in the proof of the theorem above, by putting $v_0 = e_1 \in \mathbb{F}_q^n$, the set $B_{e_1} := \left\{e_1; T_R(e_1); \dots; T_R^{n-1}(e_1)\right\} = \{e_1; e_2; \dots; e_n\}$ is the standard basis of $\mathbb{F}_q^n$. It follows that the image of each right polycyclic code by the realization φ_R, defined in (1), is an ideal of $\mathbb{F}_q[x]/\langle f(x)\rangle$. Hence, we have the following result, where the first and the second assertion are given in [13, Proposition 2.5].

Theorem 2
Let $C \subseteq \mathbb{F}_q^n$ be a linear code of length n over $\mathbb{F}_q$. The following assertions are equivalent :

1. C is a right polycyclic code.
2. C is an invariant subspace of $\mathbb{F}_q^n$ by T_R.
3. $\varphi_R(C)$ is an ideal of $\mathbb{F}_q[x]/\langle f(x)\rangle$.

Example 3
Each $\lambda-$constacyclic code is a right polycyclic code with associate vector $R_\lambda = (\lambda, 0, \dots, 0) \in \mathbb{F}_q^n$. Then it is invariant by the operator T_λ, defined by :

$$T_\lambda(v_0, v_1, \dots, v_{n-1}) = (0, v_0, v_1, \dots, v_{n-2}) + v_{n-1}(\lambda, 0, \dots, 0) = (\lambda v_{n-1}, v_0, \dots, v_{n-2}),$$

for each $v = (v_0, v_1, \dots, v_{n-1}) \in \mathbb{F}_q^n$. Hence the cyclic codes ($\lambda = 1$) and the negacyclic codes ($\lambda = -1$) are right polycyclic codes.

Inspired by the work presented by Radkova, D. and Van Zanten A.J. in [2], we consider the irreducible factorization of $f(x)$ given as

$$f(x) = \prod_{i=1}^{r} f_i^{\alpha_i}(x) \tag{6}$$

By the Cayley-Hamilton theorem [7, Theorem 4 p. 194], the matrix A satisfies

$$f(A) = f(T_R) = 0$$

Furthermore, we consider the following homogeneous set of equations

$$f_i^{\alpha_i}(A)v = 0, \quad v \in \mathbb{F}_q^n \tag{7}$$

for $i = 1, \dots, r$. If U_i stands for the solution space of (7), then we may write

$$U_i := \ker\left(f_i^{\alpha_i}(A)\right) \tag{8}$$

The most of the assertions in the following Theorem are already proved for constacyclic code in [2, Theorem 1] for constacyclic codes and in [13, Theorem 2.2] for polycyclic codes, here we reproving them for polycyclic codes where we give possibly simpler proofs and discuss the repeated polycyclic code case.

Theorem 3
The subspaces U_i of $\mathbb{F}_q^n$ satisfy the following conditions :

1. $\mathbb{F}_q^n = U_1 \oplus U_2 \oplus \cdots \oplus U_r$.
2. U_i is an invariant subspace of $\mathbb{F}_q^n$ by T_R.
3. If W is an invariant subspace of $\mathbb{F}_q^n$ by T_R and $W_i = W \cap U_i$, for $i = 1, \ldots, r$. Then W_i is also invariant by T_R and $W = W_1 \oplus W_2 \oplus \cdots \oplus W_r$.
4. $\varphi_R(U_i)$ is the ideal of $\mathbb{F}_q[x]/\langle f(x)\rangle$ generated by $\widehat{f_i^{\alpha_i}}(x)$, where $\widehat{f_i^{\alpha_i}}(x) = \dfrac{f(x)}{f_i^{\alpha_i}(x)}$.
5. The dimension of U_i is given by $\dim_{\mathbb{F}_q}(U_i) = \deg\left(f_i^{\alpha_i}\right) = \alpha_i \deg(f_i)$.
6. If $P(x)$ is a divisor of $f(x)$ in $\mathbb{F}_q[x]$, then $\ker(P(A))$ is a direct sum of invariant subspaces of $\mathbb{F}_q^n$.
7. If $\gcd(e, p) = 1$, then U_i is a minimal invariant subspace of $\mathbb{F}_q^n$ by T_R.
8. If $\gcd(e, p) = 1$ and $P(x)$ is a divisor of $f(x)$ in $\mathbb{F}_q[x]$, then $\ker(P(A))$ is a direct sum of minimal invariant subspaces of $\mathbb{F}_q^n$.

Proof. 1. Since $f_1, f_2, \ldots, f_r$ are distinct monic irreducible polynomials, then according to the primary decomposition theorem [7, Theorem 12 P. 220] we have that

$$\mathbb{F}_q^n = U_1 \oplus U_2 \oplus \cdots \oplus U_r.$$

2. Let $a \in U_i$. Then
$$f_i^{\alpha_i}(T_R(a)) = f_i^{\alpha_i}(A)Aa = Af_i^{\alpha_i}(A)a = 0.$$
So $T_R(a) \in U_i$.
3. Since U_i is an invariant subspace, then $W_i = W \cap U_i$ is also an invariant subspace, for all $i = 1, \ldots, r$. From the statement 1, we have
$$W_1 \oplus W_2 \oplus \cdots \oplus W_r \subseteq \mathbb{F}_q^n \cap W = W \tag{9}$$
On the other hand $\gcd\left(\widehat{f_1^{\alpha_1}}(x), \widehat{f_2^{\alpha_2}}(x), \ldots, \widehat{f_r^{\alpha}}(x)\right) = 1$. By the Euclidean algorithm there are polynomials $(a_1(x), a_2(x), \ldots, a_r(x))$ such that
$$a_1(x)\widehat{f_1^{\alpha_1}}(x) + a_2(x)\widehat{f_2^{\alpha_2}}(x) + \ldots + a_r(x)\widehat{f_r^{\alpha_r}}(x) = 1$$
Then for every vector $w \in W$,
$$a_1(A)\widehat{f_1^{\alpha_1}}(A)w + a_2(A)\widehat{f_2^{\alpha_2}}(A)w + \ldots + a_r(A)\widehat{f_r^{\alpha_r}}(A)w = w$$
Let $w_i = \widehat{f_i^{\alpha_i}}(A)w$. Then $f_i^{\alpha_i}(A)w_i = f_i^{\alpha_i}(A)\widehat{f_i^{\alpha_i}}(A)w = f(A)w = 0$. Hence $w_i \in U_i \cap W = W_i$. Finally we show that
$$W_1 \oplus W_2 \oplus \ldots . \oplus W_r = W$$
4. Since U_i is an invariant subspace, the result follows by the Theorem1.
5. As $\varphi_R(U_i) = \langle \widehat{f_i^{\alpha_i}}(x)\rangle$, then by the similar argument as in Proposition1
$$\dim_{\mathbb{F}_q}(U_i) = n - \deg(\widehat{f_i^{\alpha_i}}(x)) = \alpha_i \deg(f_i).$$
6. In statement 3, take $W = ker(P(A))$.
7. If $\gcd(e, n) = 1$, then $\alpha_i = 1$ in (6) for each $i = 1, \ldots, r$. Let $U \subseteq U_i$. The polynomial $f_i^{\alpha_i}(x) = f_i(x)$ is irreducible, therefore $\dim_{\mathbb{F}_q}(U) = \dim_{\mathbb{F}_q}(U_i)$ and $U = U_i$.

8. It is immediate from the above statement.
□

According to the above theorem, we have the following characterization of the right polycyclic codes.

Theorem 4
Let C be a right polycyclic code of length n over $\mathbb{F}_q$ generated by $g(x) = \prod_{i=1}^{r} f_i^{k_i}(x)$, $0 \leq k_i \leq \alpha_i$ and $h(x) \in \mathbb{F}_q[x]$ such that $f(x) = h(x)g(x)$. Then

1. $\varphi_R(C) = \varphi_R(\ker(h(T_R)))$
2. $C = \ker(h(T_R))$ and $\dim_{\mathbb{F}_q}(C) = n - \operatorname{rank}(h(T_R)) = n - \deg(g)$.
3. $C = C_1 \oplus C_2 \oplus \cdots \oplus C_r$ where C_i is the right polycyclic code generated by $g_i(x) = \operatorname{lcm}\left(g(x), \widehat{f_i^{\alpha_i}}(x)\right) = f_i^{k_i}(x)\widehat{f_i^{\alpha_i}}(x)$, for all $i = 1, \ldots, r$.
4. If $\gcd(\operatorname{ord}(f), p) = 1$, then $C = C_1 \oplus C_2 \oplus \cdots \oplus C_R$, where C_i is a right minimal polycyclic codes.

Proof. 1. Let $c(x) = \sum_{i=0}^{n-1} c_i x^i \in \varphi_R(C)$. Since $\varphi_R(C) = \langle g(x) \rangle$, then there is $a(x) \in \mathbb{F}_q[x]$ such that $c(x) = a(x)g(x)$.
It follows that

$$h(x)c(x) = h(x)a(x)g(x) = 0 \ mod\ f(x).$$

So

$$h(x)c(x) = \sum_{i=0}^{\deg(h)} h_i x^i c(x) = \sum_{i=0}^{\deg(h)} h_i \varphi_R\left(T_R^i(c)\right) = \varphi_R\left(\sum_{i=0}^{\deg(h)} h_i T_R^i(c)\right) = \varphi_R\left(h(T_R)\right)(c)$$

Hence, $h(T_R)(c) = 0$, which means that $c \in \ker(h(T_R))$ and $\varphi_R(C) \subseteq \varphi_R(\ker(h(T_R)))$.
Conversely, let $a(x) \in \varphi_R(\ker(h(T_R)))$. There exist $q(x), r(x) \in \mathbb{F}_q[x]$, such that

$$a(x) = q(x)g(x) + r(x), \text{ where } \deg(r(x)) < \deg(g(x)).$$

Then $h(x)r(x) = 0 \ \ mod\ f(x)$.
Assume that $r(x) \neq 0$. Let $K(x) \in \mathbb{F}_q[x]$ such that $h(x)r(x) = K(x)f(x)$. Since $f(x)$ is monic, then

$$\deg(h(x)r(x)) = \deg\left(K(x)f(x)\right) = \deg(K(x)) + \deg(f(x)) \geq n.$$

Otherwise, as $h(x)$ is monic then

$$\deg(h(x)r(x)) = \deg(h) + \deg(r(x)) < n$$

Contradiction. Hence $r(x)) = 0$ and $a(x) \in \varphi_R(C)$.
2. The result follows from the statement above.
3. Let $C_i = C \cap U_i$, for all $i = 1, \ldots, r$. The right polycyclic C_i is generated by

$$g_i(x) = \operatorname{lcm}\left(g(x), \widehat{f_i^{\alpha_i}}(x)\right) = f_i^{k_i}(x)\widehat{f_i^{\alpha_i}}(x)$$

By the statement 3 of Theorem3, we have that $C = C_1 \oplus C_2 \oplus \cdots \oplus C_r$.
4. It is immediate from the statement above.
□

4. Dual of the right polycyclic codes

In this section, we aim to characterize the dual of the right polycyclic codes. Let us recall the Euclidean inner product in $\mathbb{F}_q^n$ of two vectors $x = (x_0, x_1, \ldots, x_{n-1})$ and $y = (y_0, y_1, \ldots, y_{n-1})$ defined by

$$\langle x, y\rangle = \sum_{i=0}^{n} x_i y_i \,.$$

The Euclidean dual code of each linear code C is defined by

$$C^{\perp} := \left\{ x \in \mathbb{F}_q^n : \langle x, y\rangle = 0, \ \ \forall y \in C \right\}.$$

Note that if $b : \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{F}_q$ is a non degenerate bilinear form on $\mathbb{F}_q^n$ and T is an operator, then there is an unique operator $\widehat{T}$, called the adjoint operator of T, such that $b(x, \widehat{T}(y)) = b(T(x), y)$ and the matrix of $\widehat{T}$ in a $b-$normal basis $B_N = \{e_0, e_2, \ldots, e_{n-1}\}$, (i.e) $b(e_i, e_j) = \delta_{i,j}$ for $i, j = 0, \ldots, n-1$, is the transpose matrix of the representation matrix of T in B_N. In the following result, we show that the Euclidean dual of a right polycyclic code is invariant by the adjoint operator $\widehat{T_R}$.

Theorem 5
Let C be a right polycyclic code with associate vector $R = (r_0, r_1, \ldots, r_{n-1}) \in \mathbb{F}_q^n$. Then $C^{\perp}$ is an invariant subspace of $\mathbb{F}_q^n$ by $\widehat{T_R}$.

Proof. Note that the Euclidean dual $b = \langle \, . \, , \, . \, \rangle$ is a non degenerate bilinear form. Let $c \in C$ and $v \in C^{\perp}$, then

$$\langle c, \widehat{T_R}(v)\rangle = \langle T_R(c), v\rangle = 0$$

It follows that $\widehat{T_R}(v) \in C^{\perp}$ and $\widehat{T_R}(C^{\perp}) \subseteq C^{\perp}$.
□

As the standard basis B of $\mathbb{F}_q^n$ is normal with respect to the Euclidean inner product on $\mathbb{F}_q^n$, the matrix of $\widehat{T_R}$ in B is ${}^tA$. Hence the operator $\widehat{T_R}$ is defined by

$$\begin{array}{rccc} \widehat{T_R} \ : & \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q^n \\ & (a_0, a_1, \ldots, a_{n-1}) & \longmapsto & \left(a_1, a_2, \ldots, a_{n-1}, \sum_{i=0}^{n-1} a_i r_i \right) \end{array} \tag{10}$$

Note that if S and T are two operators such that $S \circ T = T \circ S$, then each invariant subspace of $\mathbb{F}_q^n$ by S is also invariant by T and it follows that

Theorem 6
If the operator T_R is normal, then the dual code $C^{\perp}$ of a right polycyclic code C is also a right polycyclic code.

Proof. Let C be right polycyclic code. By the above theorem, $C^{\perp}$ is invariant by $\widehat{T_R}$. As T_R is a normal operator (i.e) $T_R \circ \widehat{T_R} = \widehat{T_R} \circ T_R$, $C^{\perp}$ is invariant by T_R. Hence $C^{\perp}$ is a right polycyclic code. □

In general, like $f(x) = x^n - R(x)$ is the minimal polynomial of $\widehat{T_R}$ then as in the proof of Theorem1 there is a vector $w_0 \in \mathbb{F}_q^n$ such that the set $B_{w_0} := \left\{ w_0; \widehat{T_R}(w_0); \ldots; \widehat{T_R}^{n-1}(w_0) \right\}$ is a basis of $\mathbb{F}_q^n$. Let ψ_R be the realization from $\mathbb{F}_q^n$ to $\mathbb{F}_q[x]/\langle f(x)\rangle$ defined by

$$\begin{array}{rccc} \psi_R \ : & \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q[x]/\langle f(x)\rangle \\ & \sum_{i=0}^{n-1} v_i \, \widehat{T_R}^{\,i}(w_0) & \longmapsto & \sum_{i=0}^{n-1} v_i x^i \end{array} \tag{11}$$

and $\phi : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$ be the transition map from $\mathbb{F}_q^n$ endowed with the standard basis B to $\mathbb{F}_q^n$ endowed with the basis B_{w_0} as follows

$$\begin{array}{rccc} \phi & : & \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q^n \\ & & (a_0, a_1, \ldots, a_{n-1}) & \longmapsto & \sum_{i=0}^{n-1} v_i \, \widehat{T}_R^{\,i}(w_0) \end{array} \tag{12}$$

Then $\psi_R \circ \phi(C^\perp)$ is an ideal of $\mathbb{F}_q[x]/\langle f(x)\rangle$. Let $P = \left(w_0; \widehat{T}_R(w_0); \ldots; \widehat{T}_R^{\,n-1}(w_0)\right)$ be the transition matrix from B to B_{w_0}, then $A = P^{-1}\,{}^tA\,P$.

The following result gives a characterization of the Euclidean dual of a right polycyclic code, when T_R isn't normal.

Theorem 7
Let C be a right polycyclic code with associate vector $R = (r_0, r_1, \ldots, r_{n-1}) \in \mathbb{F}_q^n$, then $\psi_R(P^{-1} * C^\perp)$ is an ideal of $\mathbb{F}_q[x]/\langle f(x)\rangle$, where $P^{-1} * C^\perp := \left\{P^{-1}\,{}^tc \in \mathbb{F}_q^n : c \in C^\perp\right\}$.

The following lemma gives an elementary method to compute the product of two polynomials in $\mathbb{F}_q[x]/\langle f(x)\rangle$ using the matrix A.

Lemma 1
Let $h(x), a(x)$ two polynomials in $\mathbb{F}_q[x]/\langle f(x)\rangle$, then

$$h(x)a(x) \ \ mod \ \ f(x) \ \ = \ \ \sum_{j=0}^{n-1} \langle a, H_j\rangle x^j$$

where H_j is the $j^{th}-$row of the matrix $H = \left[h; Ah; \cdots; A^{n-1}h\right]$, $h = \varphi_R^{-1}(h(x))$ and $a = \varphi_R^{-1}(a(x))$.

Proof. Let us use the following notation, for each $i = 0, \ldots, n-1$, $A^i h = \begin{pmatrix} h_0^{(i)} \\ \vdots \\ h_{n-1}^{(i)} \end{pmatrix}$, then

$$\begin{aligned} h(x)a(x) \ mod \ f(x) &= \sum_{i=0}^{n-1} a_i x^i h(x) \\ &= \sum_{i=0}^{n-1} a_i \varphi_R\left(A^i h\right) \\ &= \sum_{i=0}^{n-1} a_i \sum_{j=0}^{n-1} h_j^{(i)} x^j \\ &= \sum_{j=0}^{n-1}\sum_{i=0}^{n-1} a_i h_j^{(i)} x^j \\ &= \sum_{j=0}^{n-1} \langle a, H_j\rangle x^j, \end{aligned}$$

where $H_j = \left(h_j^{(0)}, h_j^{(1)}, \ldots, h_j^{(n-1)}\right)$ the j^{th} row of the matrix $H = \left[h; A(h); \cdots; A^{n-1}(h)\right]$.

□

Corollary 1
Let C be a right polycyclic code of length n over $\mathbb{F}_q$ generated by $g(x)$, (i.e) $\varphi_R(C) = \langle g(x)\rangle$ and $h(x) \in \mathbb{F}_q[x]$ such that $f(x) = g(x)h(x)$. Then there are $\deg(g)$ independent rows H_i of the matrix H (as in lemma1) which form a basis of the dual code $C^\perp$.

Proof. Let $c(x) \in \varphi_R(C)$ then $c(x)h(x) = v(x)f(x) = 0$, for some $v(x) \in \mathbb{F}_q[x]$. By the first statement we have

$$c(x)h(x) = \sum_{i=0}^{n-1} \langle c, H_i\rangle x^i$$

Hence, $\langle c, H_i\rangle = 0$, for each $i = 0, \ldots, n-1$, and c is orthogonal to each row H_i of H.
Since $\dim_{\mathbb{F}_q}(C^\perp) = n - \deg(h(x))$ and the rank of H is $\deg(g)$, then there is $\deg(g)$ independents rows H_i of the matrix H which form a basis of $C^\perp$. □

5. BCH-like and Hartmann-Tzeng-like bounds for right polycyclic codes

In this section, we prove the BCH-like and the Hartmann–Tzeng-like bounds for the right polycyclic codes using the order e of the polynomial $f(x)$. Let e be the order of $f(x) = x^n - R(x)$ with $f(0) \neq 0$, and suppose that $\gcd(e, q) = 1$. Therefore all the roots of $f(x)$ are simple. Let α be a e^{th} −primitive root of unity and $\lambda_1, \lambda_2, \ldots, \lambda_n$ be the eigenvalues of T_R. As $f(0) \neq 0$; λ_i, $i = 1, \ldots, n$ are non zero and distinct, and if $v_{\lambda_1}, v_{\lambda_2}, \ldots, v_{\lambda_n}$ are the eigenvectors associated with $\lambda_1, \ldots, \lambda_n$, respectively. So, there is an invertible matrix $P = (v_{\lambda_1}, v_{\lambda_2}, \ldots, v_{\lambda_n})$ such that $P^{-1}AP = D$, where $D = \operatorname{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n)$ is a diagonal matrix.

Let C be a $[n, k]-$ right polycyclic code generated by $g(x)$. From Theorem 4, $C = \ker(h(T_R))$, where $h(x) = \dfrac{f(x)}{g(x)}$. Hence

$$c \in C \iff h(T_R)(c) = 0.$$

It follows, that the set containing the eigenvalues of $h(T_R)$ is the set of the roots of $g(x)$ (i.e)

$$V(C) = \left\{\lambda_i \in \mathbb{F}_{q^m} \ : \ \exists v_i \in \mathbb{F}_q^n \backslash \{0\},\ h(T_R)(v_i) = \lambda v_i\right\} = \left\{\lambda_i \in \mathbb{F}_{q^m} \ : \ g(\lambda_i) = 0\right\}$$

where m is the multiplicative order of q modulo e. Since for each $i = 1, \ldots, n$ one can write $\lambda_i = \alpha^{k_i}$ for some $k_i \in [1, \ldots, e]$, then

$$V(C) = \left\{\alpha^{k_i} \in \mathbb{F}_{q^m} \ : \ g\left(\alpha^{k_i}\right) = 0\right\}.$$

Let us recall that the Hamming weight of $x \in \mathbb{F}_q^n$ is $w_H(x) := \operatorname{card}(\{i \ : \ x_i \neq 0\})$ and the minimum distance of each linear code is defined as follows :

Definition 3
Let C be a linear code of length n over $\mathbb{F}_q$ then the *minimum Hamming distance* of C is

$$d_H := \min\{w_H(c) \ : \ c \in C,\ c \neq 0\}$$

In line with the proof of [5, Theorem 4.5.3], we show the following theorem.

Theorem 8 (BCH-like bound for right polycyclic codes)
Let C be a right polycyclic code of length n over $\mathbb{F}_q$ generated by $g(x)$ with minimum distance d_H such that $V(C)$ contains the set

$$T_g = \left\{\alpha^{a+ib} \text{ for } i = 0, \ldots, \delta - 2\right\}$$

If $\gcd(e, b) = 1$, then $d_H \geq \delta$.

Proof. Let c be a codeword of weight $w < \delta$, then

$$c(x) := \varphi_R(c) = \sum_{i=0}^{w-1} c_i x^{k_i} \quad \text{for some } \{k_0, \dots, k_{w-1}\} \subseteq \{1, \dots, n-1\}.$$

Then for $j = 0, \dots, \delta - 2$,

$$c(\alpha^{a+jb}) = \sum_{i=0}^{w-1} c_i \alpha^{k_i(a+jb)} = 0,$$

It follows that c is in the left kernel of the matrix M where

$$M = \begin{pmatrix} \alpha^{k_0 a} & \alpha^{k_0(a+b)} & \cdots & \alpha^{k_0(a+(\delta-2)b)} \\ \alpha^{k_1 a} & \alpha^{k_1(a+b)} & \cdots & \alpha^{k_1(a+(\delta-2)b)} \\ & & \cdots & \\ \vdots & \vdots & \vdots & \vdots \\ \alpha^{k_{w-1} a} & \alpha^{k_{w-1}(a+b)} & \cdots & \alpha^{k_{w-1}(a+(\delta-2)b)} \end{pmatrix}$$

Since $c \neq 0$, M is a singular matrix and hence $\det M = 0$. However

$$\det(M) = \alpha^{(k_0+k_1+\cdots+k_{w-1})a} \begin{vmatrix} 1 & \alpha^{k_0 b} & \cdots & \left(\alpha^{k_0 b}\right)^{\delta-2} \\ 1 & \alpha^{k_1 b} & \cdots & \left(\alpha^{k_1 b}\right)^{\delta-2} \\ & & \cdots & \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{k_{w-1} b} & \cdots & \left(\alpha^{k_{w-1} b}\right)^{\delta-2} \end{vmatrix}$$

Since $\gcd(e, b) = 1$, $\alpha^{k_i b}$, $i = 0, \dots, \delta - 2$ are distinct. In fact, for $i, j \in [0, \dots, \delta - 2]$ with $i < j$,

$$\alpha^{k_i b} = \alpha^{k_j b} \iff \alpha^{(k_j - k_i)b} = 1 \iff e \text{ divides } (k_j - k_i)b.$$

As $k_j - k_i < e$ and $\gcd(e, b) = 1$, $k_i - k_j = 0$ and $k_i = k_j$.

Hence $\det M \neq 0$, contradiction!!! Then C doesn't contain any codeword of weight less than δ and $d_H \geq \delta$.

□

Remark 2

Not that the result of the above theorem is given in [13, Theorem 4.2.] by another approach based on the so-called Roos bound for cyclic codes in [15].

Now, by similar argument as in the proof of the above theorem and from [9, Lemma 3.2, Theorem 3.3], we show the Hartmann–Tzeng-like bound for the right polycyclic codes.

Theorem 9 (Hartmann-Tzeng-like bound for the right polycyclic codes)

Let C be a right polycyclic code of length n over $\mathbb{F}_q$ generated by $g(x)$ such that $V(C)$ contains the set

$$T_g = \left\{\alpha^{a+ib_1+jc_1} \ : \ i = 0, \dots, \delta - 2, j = 0, \dots, r\right\}.$$

If $\gcd(e, b_1) = 1$ and $\gcd(e, c_1) = 1$, then $d_H \geq \delta + r$.

Proof. Let c be a codeword of weight $w = \delta + r - 1$, then $w < \delta + r$ and one can write

$$c(x) := \varphi_R(c) = \sum_{l=0}^{w-1} c_l x^{k_l} \quad \text{for some } \{k_0, \dots, k_{w-1}\} \subseteq \{1, \dots, n-1\}.$$

Then for $i = 0, \ldots, \delta - 2,\ j = 0, \ldots, r$

$$c(\alpha^{a+ib_1+jc_1}) = \sum_{l=0}^{w-1} c_l \alpha^{k_l(a+ib_1+jc_1)} = 0,$$

It follows that c is in the left kernel of the matrix L $L = \left(M \mid \alpha^{c_1}M \mid \alpha^{2c_1}M \mid \alpha^{3c_1}M \mid \ldots. \mid \alpha^{rc_1}M\right)$ where

$$M = \begin{pmatrix} \alpha^{k_0 a} & \alpha^{k_0(a+b_1)} & \cdots & \alpha^{k_0(a+(\delta-2)b_1)} \\ \alpha^{k_1 a} & \alpha^{k_1(a+b_1)} & \cdots & \alpha^{k_1(a+(\delta-2)b_1)} \\ & & \cdots & \\ \vdots & \vdots & \vdots & \vdots \\ \alpha^{k_{w-1}a} & \alpha^{k_{w-1}(a+b_1)} & \cdots & \alpha^{k_{w-1}(a+(\delta-2)b_1)} \end{pmatrix}$$

As in the proof of the above theorem, $\det(M) \neq 0$. Since $\gcd(e, c_1) = 1$, then $\alpha^{jc_1} \neq 1$ are distinct for $j = 1, \ldots, r$. Hence the matrix L has full rank equal

$$\min(w, (\delta - 1)(r + 1)) = w.$$

On the other hand, $c \neq 0$ means that M is a singular matrix. Contradiction! Then C doesn't contain any codeword of weight less than $\delta + r$. Hence, $d_H \geq \delta + r$.

□

By the inductive argument on the above result, we deduce the following corollary

Corollary 2
Let C be a right polycyclic code of length n over $\mathbb{F}_q$ such that $V(C)$ contains the set

$$T_g = \left\{\alpha^{a+ib+\sum_{k=1}^{r} j_k c_k} \text{ for } i = 0, \ldots, \delta - 2,\ j_k = 1, \ldots, s_k\right\}$$

where $\gcd(e, b) = 1$ and $\gcd(e, c_k) = 1$ for each $j_k = 1, \ldots, s_k$. Then, $d \geq \delta + \sum_{k=1}^{r} s_k$.

Now, we define the BCH-right polycyclic codes with designed distance δ.

Definition 4
Let C be a right polycyclic code of length n over $\mathbb{F}_q$ generated by $g(x)$ and δ be a positive integer. The code C is said to be a BCH-right polycyclic code with designed distance δ, if $V(C)$ contains the set $\left\{\alpha^{a+ib} : i = 0, \ldots, \delta - 2\right\}$ where $\gcd(e, b) = 1$. In this case, C satisfies the BCH-like bound.

Example 4 (BCH-like bound of right polycyclic codes)
Let $R = (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \in \mathbb{F}_8^{11}$, then $R(x) = x^8 + x^7 + x^5 + x^3 + x^2 + x + 1$. The order of $f(x) = x^{11} - R(x)$ over $\mathbb{F}_8$ is $e = 15$, the multiplicative order of 15 modulo 8 is $m = 4$ and the field extension $\mathbb{F}_{8^4} = \mathbb{F}_8(\alpha)$ contains the e^{th} primitive root of unity $\beta = \alpha^{\frac{8^4-1}{15}} = \alpha^{273}$.
It follows that the 8−cyclotomic cosets modulo 15 are:

$$C_0 = \{0\}; C_1 = \{1, 2, 4, 8\}; C_3 = \{3, 6, 9, 12\}; C_5 = \{5, 10\}; C_7 = \{7, 11, 13, 14\}.$$

In the following table, we list all the BCH-like right polycyclic codes with associate vector $R \in \mathbb{F}_8^{11}$ of length 11 and all the BCH codes of length 11 over $\mathbb{F}_8$.

	δ	a	b	Defining consecutive set T_g	Generator polynomial	k	d_H
Right polycyclic codes	2	0	|	{0}	$x+1$	10	2
		11	|	{11}	x^4+x^3+1	7	3
		9	|	{9}	$x^4+x^3+x^2+x+1$	7	2
		10	|	{10}	x^2+x+1	9	2
	3	0	7	{0,7}	x^5+x^3+x+1	6	4
		3	4	{3,7}	$x^8+x^4+x^2+x+1$	3	5
		3	7	{3,10}	$x^6+x^4+x^3+x^2+1$	5	4
		5	2	{5,7}	$x^6+x^3+x^2+x+1$	5	3
		13	1	{13,14}	x^4+x^3+1	7	3
	4	0	7	{0,7,14}	x^5+x^3+x+1	6	4
		3	2	{3,5,7}	$x^{10}+x^9+x^8+x^6+x^5+x^2+1$	1	7
		7	2	{7,9,11}	$x^8+x^4+x^2+x+1$	3	5
	5	9	1	{9,10,11,12}	$x^{10}+x^9+x^8+x^6+x^5+x^2+1$	1	7
		11	1	{11,12,13,14}	$x^8+x^4+x^2+x+1$	3	5
	6	5	2	{5,7,9,11,13}	$x^{10}+x^9+x^8+x^6+x^5+x^2+1$	1	7
	7	3	2	{3,5,7,9,11,13}	$x^{10}+x^9+x^8+x^6+x^5+x^2+1$	1	7
Cyclic codes	2	0	|	{0}	$x+1$	10	2
	11	1	1	{1,2,3,4,5,6,7,8,9,10}	$x^{10}+x^9+x^8+x^7+x^6+x^5+$ $x^4+x^3+x^2+x+1$	1	11

Remark 3
The similar idea can be developed to left polycyclic codes with associate vector $L=(l_0,l_1,...,l_{n-1})$ by considering the operator T_L defined by

$$T_L(v_0,v_1,\ldots,v_{n-1})=(v_1+v_0l_0,\ldots,v_{n-2}+v_0l_{n-2},v_0l_{n-1}). \tag{13}$$

where its matrix in the standard basis of $\mathbb{F}_q^n$ is

$$M=\begin{pmatrix} l_0 & 1 & 0 & \ldots & 0 \\ l_1 & 0 & 1 & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ l_{n-2} & \vdots & 0 & 0 & 1 \\ l_{n-1} & 0 & \ldots & 0 & 0 \end{pmatrix}$$

but we need here to compute a T_L-cyclic basis of $\mathbb{F}_q^n$, the fact that yields an in-depth study in this case.

Conclusion

In this paper, we have developed an approach to right polycyclic codes using the theory of the invariant subspaces by a fixed operator T_R. A characterization of the Euclidean dual code with the adjoint operator of T_R is given. The problem to develop more this idea in the case of Hermitian dual codes and the Galois dual codes is good. Also, to determine explicitly the generator polynomial of a right polycyclic code such as in cyclic and constacyclic cases. It is a very important problem to develop studies on the duality of these codes. When the order of the minimal polynomial of T_R is coprime with the alphabet size, a lower bound on the minimum distance of the right polycyclic codes such as BCH-like and Hartmann–Tzeng-like are proved. However, the contrary case still not solved. Also, the problem on similar bounds for the polycyclic codes over the finite rings is also proposed. Finally, the study of the linear codes that are invariant by a cyclic operator or by an arbitrary operator (not necessary cyclic) is an important field to develop the main idea of this paper.

References

[1] S. R. Lopez-Permouth, B. R. Parra-Avila and S. Szabo, Dual generalizations of the concept of cyclicity of codes, Adv. Math. Commun., 3 (2009), 227-234.
[2] D. Radkova, A.J.Van Zanten, Constacyclic codes as invariant subspaces, Linear Algebra Appl., 430 (2009), 855-864.
[3] C.R. Hartmann ,K.K. Tzeng , Generalizations of the BCH bound, Inf. Control, 20 (1972), 489-498.
[4] R.L. Lidl and H. Niederreiter, Introduction to Finite Fields and their Applications (rev. ed.), Cambridge University Press, Cambridge (1987).
[5] W.C. Huffman, V. Pless, Fundermentals of Error Correcting Codes, Cambridge University Press (2003).
[6] A. Alahmadi, S. Dougherty, A. Leroy and P. Solé, On the duality and the direction of polycyclic codes, Adv. Math. Commun., 10 (2016), 921-929.
[7] H. K. Hoffman, R. Kunze, Linear Algebra, Prentice-Hall, Inc. Englewood Cliffs, New Jersey, (1971).
[8] SageMath, the Sage Mathematics Software System (Version 8.7), The Sage Developers, 2019, https://www.sagemath.org.
[9] J. Gómez-Torrecillas, F. J. Lobillo, G. Navarro, and A. Neri. Hartmann-Tzeng bound and skew cyclic codes of designed Hamming distance. Finite Fields and Their Applications, 50 (2018), 84–112.
[10] W. W. Peterson and E. J. Weldon, Error Correcting Codes, MIT Press, 1972.
[11] S. R. Lopez-Permouth, H. Ozadam, F. Ozbudak, S. Szabo, Polycyclic codes over Galois rings with applications to repeated-root constacyclic codes, Finite Fields Their Appl., 19 (2013), 16-38.
[12] E. Martinez-Moro, A. Fotue, T. Blackford, On polycyclic codes over a finite chain ring, Adv. Math. Commun., 3,(2020).
[13] M. Shi, X. Li, Z. Sepasdar, P. Solé:Polycyclic codes as invariant subspaces. Finite Fields Their Appl. 68: 101760 (2020).
[14] S. Li, M. Xiong, G. Ge, Pseudo-cyclic codes and the construction of quantum MDS codes, IEEE Transactions on Information Theory, 62 (2016), 1703–1710.
[15] C. Roos, A generalization of the BCH bound for cyclic codes, including the Hartmann-Tzeng bound, J. Comb. Theory Ser. A 33 (1982), 229-232.