Polycyclic codes as invariant subspaces.

Minjia Shi, Xiaoxiao Li, Zahra Sepasdar, Patrick Solé

Polycyclic codes as invariant subspaces

Minjia Shi*, Xiaoxiao Li†, Zahra Sepasdar‡, Patrick Solé§

Abstract

Polycyclic codes are a powerful generalization of cyclic and constacyclic codes. Their algebraic structure is studied here by the theory of invariant subspaces from linear algebra. As an application, a bound on the minimum distance of these codes is derived which outperforms, in some cases, the natural analogue of the BCH bound.

Keywords: Polycyclic codes; cyclic codes; BCH bound; invariant subspaces

MSC (2010) : Primary 94B15; Secondary 11A15.

1 Introduction

Polycyclic codes of length n over a finite field F can be described as ideals in the quotient ring of $F[x]/(f)$, where f is some polynomial of degree n. They reduce to cyclic codes when $f = x^n - 1$ and to constacyclic codes when $f = x^n - a$, for some $a \in F^*$. They have been known for a long time under the name of pseudo-cyclic codes [8]. They received a new name in [5], and a renewed interest in [1], where their algebraic structure is studied in great detail. Replacing F by a finite chain ring is considered in [6, 7]. In parallel, an algebraic approach to quasi-twisted and constacyclic codes was developed in [9, 10]. The idea is to consider the codes in the class under scrutiny as invariant subspaces under the action of an endomorphism; this allows the machinery from linear algebra to bear on the problem [3]. In the cases considered in [9, 10], the said endomorphism is the analogue of the cyclic shift of cyclic codes. For another aplication of this linear algebra method to Coding Theory see [2].

*Corresponding author: Minjia Shi, Key Laboratory of Intelligent Computing Signal Processing, Ministry of Education, School of Mathematical Sciences, Anhui University, Hefei, Anhui, 230601, China. E-mail: smjwcl.good@163.com.

†School of Mathematical Sciences, Anhui University, China. E-mail: ahulixiaoxiao@163.com

‡School of Electrical and Computer Engineering, Shiraz University, Shiraz, Iran, E-mail: zsepasdar@yahoo.com

§I2M,(CNRS, University of Aix- Marseille, Centrale Marseille), Marseilles, France, E-mail: patrick.sole@telecom-paristech.fr

In the present paper, we apply the latter approach to the study of polycyclic codes. The transform mentioned before and called here the polyshift admits for matrix the companion matrix of the polynomial $f(x)$. A notion of minimal invariant subspace is introduced, driven by the factorization of $f(x)$ into irreducible factors over the base field. This allows to describe any invariant subspace as a direct sum of its intersections with these spaces. The first benefit of this decomposition is an analogue of the generator polynomial and of the check polynomial of cyclic codes. Similarly, an analogue of the idempotent of cyclic codes is developed. Last but not least, a bound on the minimum distance is derived that outperforms, in some cases, the BCH-like bound of [4].

The material is arranged as follows. The next section develops the approach to polycyclic codes as invariant subspaces of the polyshift, and introduces the analogues of generator and check polynomials of cyclic codes. Section 3 derives a primitive idempotent decomposition of polycyclic codes. Section 4 is dedicated to a bound on the minimum distance which improves, in some cases the BCH-like bound of [4]. Section 5 concludes the paper and points out some challenging open problems.

2 Linear polycyclic codes as invariant subspaces

Let $F = \mathbb{F}_q$ be a finite field of order q and F^n be the n-dimensional vector space over F with the standard basis $e_1 = (1, 0, \ldots, 0), e_2 = (0, 1, \ldots, 0), \ldots, e_n = (0, 0, \ldots, 1)$. E is the identify matrix. Let $\mathbf{c} = (c_0, c_1, ..., c_{n-1})$ be a codeword of C with $c_0 \neq 0$ and let $T_{\mathbf{c}}$ denote the **polyshift** defined as:

$$\begin{cases} F^n \to F^n, \\ (x_1, x_2, \ldots, x_n) \to x_n\mathbf{c} + (0, x_1, \ldots, x_{n-1}). \end{cases}$$

Then $T_{\mathbf{c}} \in \mathrm{Hom}(F^n)$ and it has the following matrix:

$$A(n, \mathbf{c}) = A = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & 0 & c_0 \\ 1 & 0 & 0 & \cdots & 0 & 0 & c_1 \\ 0 & 1 & 0 & \cdots & 0 & 0 & c_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 & c_{n-2} \\ 0 & 0 & 0 & \cdots & 0 & 1 & c_{n-1} \end{bmatrix}.$$

We observe the relations

$$A^{-1}(n,\mathbf{c}) = A^{-1} = \begin{bmatrix} -\frac{c_1}{c_0} & 1 & 0 & 0 & \cdots & 0 & 0 \\ -\frac{c_2}{c_0} & 0 & 1 & 0 & \cdots & 0 & 0 \\ -\frac{c_3}{c_0} & 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ -\frac{c_{n-2}}{c_0} & 0 & 0 & 0 & \cdots & 1 & 0 \\ -\frac{c_{n-1}}{c_0} & 0 & 0 & 0 & \cdots & 0 & 1 \\ -\frac{1}{c_0} & 0 & 0 & 0 & \cdots & 0 & 0 \end{bmatrix}.$$

The characteristic polynomial of A is

$$f_A(x) = f(x) = \begin{bmatrix} -x & 0 & 0 & \cdots & 0 & 0 & c_0 \\ 1 & -x & 0 & \cdots & 0 & 0 & c_1 \\ 0 & 1 & -x & \cdots & 0 & 0 & c_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -x & c_{n-2} \\ 0 & 0 & 0 & \cdots & 0 & 1 & c_{n-1}-x \end{bmatrix} =$$
$$(-1)^{n+1}(c_0 + c_1x + c_2x^2 + \cdots + c_{n-2}x^{n-2} + c_{n-1}x^{n-1} - x^n).$$

Note that this polynomial is, up to sign, the same f as in the Introduction [1].

Let $f(x) = (-1)^{n+1}f_1^{p_1}(x)f_2^{p_2}(x)\cdots f_t^{p_t}(x)$ be the factorization of $f(x)$ into irreducible factors over F. By the theorem of Cayley-Hamilton, we have

$$f(A) = (-1)^{n+1}f_1^{p_1}(A)f_2^{p_2}(A)\cdots f_t^{p_t}(A) = \mathbf{0}.$$

Next, we consider the homogeneous set of equations $f_i^{p_i}(A)\mathbf{x} = \mathbf{0}, \mathbf{x} \in F^n$ for $i = 1, \ldots, t$. If U_i stands for the solution space of this homogeneous set of equations, then we may write $U_i = \mathrm{Ker}(f_i^{p_i}(T_\mathbf{c}))$, and consider the homogeneous set of equations $f_i(A)\mathbf{x} = \mathbf{0}, \mathbf{x} \in F^n$ for $i = 1, \ldots, t$. If V_i stands for the solution space of this homogeneous set of equations, then we may write $V_i = \mathrm{Ker}(f_i(T_\mathbf{c}))$. Now, we need the following well-known fact [3, p.200].

Proposition 2.1. *Let V be a T_c-invariant subspace of U. Then $f_{T_\mathbf{c}|U_i}(x)$ divides $f_{T_c}(x)$.*

The general properties of minimal invariant subspaces can be summarized as follows.

Theorem 2.2. *The subspaces U_i and V_i of F^n satisfy the following conditions:*

(1) $V_i \subseteq U_i$, U_i and V_i are $T_\mathbf{c}$-invariant subspace of F^n;

(2) if W is a $T_\mathbf{c}$-invariant subspace of F^n and $W_i = W \cap U_i$ for $i = 1, \ldots, t$, then W_i is $T_\mathbf{c}$-invariant and $W = W_1 \oplus W_2 \oplus \cdots \oplus W_t$;

(3) $F^n = U_1 \oplus U_2 \oplus \cdots \oplus U_t$;

(4) $\dim_F U_i = \deg f_i^{p_i}(x) = k_i p_i$, *where* $deg f_i(x) = k_i$*;*

(5) $f_{T_{\mathbf{c}}|U_i}(x) = (-1)^{k_i p_i} f_i^{p_i}(x)$*;*

(6) V_i *is a minimal* $T_{\mathbf{c}}$*-invariant subspace of* F^n*.*

Proof. (1) Let $\mathbf{u} \in U_i$, i.e. $f_i^{p_i}(A)\mathbf{u} = 0$, then $f_i^{p_i}(A)T_{\mathbf{c}}(\mathbf{u}) = f_i^{p_i}(A)A\mathbf{u} = Af_i^{p_i}(A)\mathbf{u} = 0$, so that $T_{\mathbf{c}}(\mathbf{u}) \in U_i$.

(2) Let $\hat{f}_i^{p_i}(x) = \frac{f(x)}{f_i^{p_i}(x)}$ for $i = 1, \ldots, t$. Since $(\hat{f}_1(x), \hat{f}_2(x), \ldots, \hat{f}_t(x)) = 1$, there are polynomials $a_1(x), \ldots, a_t(x) \in F[x]$ such that $a_1(x)\hat{f}_1(x) + a_2(x)\hat{f}_2(x) + \cdots + a_t(x)\hat{f}_t(x) = 1$. Then for any $\mathbf{w} \in W$, $\mathbf{w} = a_1(A)\hat{f}_1(A)\mathbf{w} + a_2(A)\hat{f}_2(A)\mathbf{w} + \cdots + a_t(A)\hat{f}_t(A)\mathbf{w}$. Let $\mathbf{w}_i = a_i(A)\hat{f}_i(A)\mathbf{w}$, then $f_i(A)^{p_i}\mathbf{w}_i = a_i(A)f(A)\mathbf{w} = \mathbf{0}$ and $\mathbf{w}_i \in U_i \bigcap W$. Hence $W = W_1 + W_2 + \cdots + W_t$. Assume that $\mathbf{w} \in W_i \bigcap \sum_{j \neq i} W_j$, then $f_i^{p_i}(A)\mathbf{w} = \mathbf{0}, \hat{f}_i^{p_i}(A)\mathbf{w} = \mathbf{0}$. Since $(f_i^{p_i}(x), \hat{f}_i^{p_i}(x)) = 1$, there are polynomials $a(x), b(x) \in F[x]$, such that $a(x)f_i^{p_i}(x) + b(x)\hat{f}_i^{p_i}(x) = 1$. Hence $a(A)f_i^{p_i}(A)\mathbf{w} + b(A)\hat{f}_i^{p_i}(A)\mathbf{w} = \mathbf{w} = \mathbf{0}$, so that $\mathbf{w} \in W_i \bigcap \sum_{j \neq i} W_j = \{\mathbf{0}\}$. Therefore $W = W_1 \bigoplus W_2 \bigoplus \ldots \bigoplus W_t$.

(3) This follows from 2) with $W = F^n$.

(4) Let $k \geq 1$ be the smallest positive integer with the property that the vectors $\mathbf{u}, T_c(\mathbf{u}), \ldots, T_c^k(\mathbf{u})$ are linearly dependent for all $\mathbf{u} \in U_i$. Then there exist elements $a_0, a_1, \ldots, a_{k-1} \in F$ such that

$$T_c^k(\mathbf{u}) = a_0\mathbf{u} + a_1 T(\mathbf{u}) + \cdots + a_{k-1}T_c^{k-1}(\mathbf{u}). \qquad (1)$$

Consider the polynomial $t(x) = x^k - a_{k-1}x^{k-1} - \cdots - a_0 x^0 \in F[x]$. Thus by Eq. (1)

$$t(T_c)(\mathbf{u}) = T_c^k(\mathbf{u}) - a_{k-1}T_c^{k-1}(\mathbf{u}) - \cdots - a_0 T_c^0(\mathbf{u}) = 0.$$

On the other hand, since $\mathbf{u} \in U_i$, we have $f_i^{p_i}(T_c)(\mathbf{u}) = \mathbf{0}$. Hence $t(T_c)(\mathbf{u}) = f_i^{p_i}(T_c)(\mathbf{u}) = \mathbf{0}$. It follows that:

$$[(t(x), f_i^{p_i}(x))(T_c)](\mathbf{u}) = \mathbf{0}. \qquad (2)$$

Since $f_i(x)$ is an irreducible polynomial, $\gcd(t(x), f_i^{p_i}(x)) = 1$ or $f_i^j(x)$ for $j \leq p_i$. By Eq. (2), $\gcd(t(x), f_i^{p_i}(x)) = f_i^j(x)$ for $j \leq p_i$. Thus $f_i^j(T_c)(\mathbf{u}) = \mathbf{0}$ for $j \leq p_i$. First, we show that $j = p_i$. Let $W = \mathrm{Ker}(f_i^j(T_c))$. It is clear that $W \subseteq U_i$. On the other hand, from $\mathbf{u} \in U_i$, we get that $f_i^j(T_c)(\mathbf{u}) = \mathbf{0}$, $\mathbf{u} \in W$. Because $\mathbf{u}$ is an arbitrary element of U_i, we conclude that $U_i \subseteq W$ and so $W = U_i$. Therefore $(t(x), f_i^{p_i}(x)) = f_i^{p_i}(x)$. So $f_i^{p_i}(x)$ divides $t(x)$ and this means that $k_i p_i = \deg(f_i^{p_i}) \leq \deg(t(x)) = k$. Now, from $f_i^{p_i}(T_c)(\mathbf{u}) = \mathbf{0}$ we get that $\mathbf{u}, T_c(\mathbf{u}), \ldots, T_c^{k_i p_i}(\mathbf{u})$ are linearly dependent. By

minimality of k, we get $k \leq k_i p_i$. Hence $k = k_i p_i$. It is clear that $\dim U_i \geq k = k_i p_i$, then we have

$$\sum_{i=1}^{t} \dim U_i = \dim_F F^n = n = \deg(f) = \sum_{i=1}^{t} \deg(f_i^{p_i}) = \sum_{i=1}^{t} k_i p_i.$$

Therefore $\dim_F U_i = k_i p_i$.

(5) Suppose that $\mathbf{g}^{(i)} = (g_1^{(i)}, g_2^{(i)}, \ldots, g_{k_i p_i}^{(i)})$ is a basis of U_i over F for $i = 1, \ldots, t$. Consider A_i as the matrix of $T_{\mathbf{c}}|_{U_i}$ with respect to that basis. Let $f_i' = f_{T_{\mathbf{c}}|_{U_i}}$. First, we show that $\gcd(f_i^{p_i}, f_i') \neq 1$. Suppose that $\gcd(f_i^{p_i}, f_i') = 1$, then there exist polynomials $a(x), b(x) \in F[x]$ such that $a(x) f_i^{p_i}(x) + b(x) f_i'(x) = 1$. Then $a(A_i) f_i^{p_i}(A_i) + b(A_i) f_i'(A_i) = E$. By the theorem of Cayley-Hamilton, $f_i'(A_i) = 0$. So $a(A_i) f_i^{p_i}(A_i) = E$. Now, we want to show that $f_i^{p_i}(A_i) = 0$, and we get the contradiction. By (3) in this Theorem, $\mathbf{g} = (g_1^{(i)}, g_2^{(i)}, \ldots, g_{k_1 p_1}^{(1)}, g_1^{(t)}, g_2^{(t)}, \ldots, g_{k_t p_t}^{(t)})$ is a basis of F^n and T_c is represented by

$$A' = \begin{bmatrix} A_1 & & & & & \\ & A_2 & & & & \\ & & A_3 & & & \\ & & & \ddots & & \\ & & & & A_t \end{bmatrix},$$

with respect to that basis. Besides $A' = T^{-1} A T$, where T is the transformation matrix from the standard basis of F^n to the basis $\mathbf{g}$. Then we have

$$f_i^{p_i}(A') = \begin{bmatrix} f_i^{p_i}(A_1) & & & & & \\ & f_i^{p_i}(A_2) & & & & \\ & & f_i^{p_i}(A_3) & & & \\ & & & \ddots & & \\ & & & & f_i^{p_i}(A_t) \end{bmatrix}.$$

Hence $f_i^{p_i}(A') = f_i^{p_i}(T^{-1} A T) = T^{-1} f_i^{p_i}(A) T$. Let $g_j^{(i)} = \lambda_{j_1}^{(i)} e_1 + \lambda_{j_2}^{(i)} e_2 + \cdots + \lambda_{j_n}^{(i)} e_n$, $j = 1, \ldots, k_i p_i$. Since $g_j^{(i)} \in U_i$, we get that

$$f_i^{p_i}(A') \begin{bmatrix} 0 \\ \vdots \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} = T^{-1} f_i^{p_i}(A) T \begin{bmatrix} 0 \\ \vdots \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} = T^{-1} f_i^{p_i}(A) \begin{bmatrix} \lambda_{j_1}^{(i)} \\ \vdots \\ \lambda_{j_n}^{(i)} \end{bmatrix} = 0,$$

where 1 is on the $(k_1+k_2+\cdots+k_{i-1}+j)$-th position. According to the last equation, $f_i^{p_i}(A_i)=0$. Therefore $\gcd(f_i^{p_i}, f_i') \neq 1$. By the proof of (3) in this theorem, it is easy to see that $\gcd(f_i^{p_i}, f_i') = f_i^{p_i}$. On the other hand, $\deg(f_i^{p_i}) = \deg(f_i')$. Therefore $f_{T_{\mathbf{c}}|U_i}(x) = (-1)^{k_i p_i} f_i^{p_i}(x)$.

(6) Suppose that V_i' is T_c-invariant subspace of F^n such that $\{\mathbf{0}\} \neq V_i' \subseteq V_i$. Then by Proposition 2.1, we know that $f_{T_{\mathbf{c}}|V_i'}$ divides f_i. Since f_i is an irreducible polynomial, $f_i = f_{T_{\mathbf{c}}|V_i'}$. So we have $\dim V_i' = \deg f_{T_{\mathbf{c}}|V_i'} = \deg f_i = \dim V_i$. Then we have $V_i' = V_i$.

This completes the proof. □

Proposition 2.3. *Let U be a $T_{\mathbf{c}}$-invariant subspace of F^n. Then U is a direct sum of some $T_{\mathbf{c}}$-invariant subspaces U_i of F^n.*

Proof. This follows immediately from (2) of Theorem 2.2. □

Definition 2.4. *A linear code of length n and dimension k is a linear subspace C of dimension k of the vector space F^n.*

Definition 2.5. *A linear code C of length n over F is called polycyclic, if whenever $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in C$, then so is $\mathbf{y} = x_n\mathbf{c} + (0, x_1, \ldots, x_{n-1})$, where $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in F^n$.*

Proposition 2.6. *A linear code C of length n over F is polycyclic if and only if C is a $T_{\mathbf{c}}$-invariant subspace of F^n.*

Proof. The proof of this proposition is immediate from Definition 2.5. □

The decomposition of a polycyclic code into minimal invariant subspaces enjoys the following properties. This is the main result of this section.

Theorem 2.7. *Let C be a linear polycyclic code of length n over F. Then the following results hold.*

(1) $C = U_{i_1} \oplus U_{i_2} \oplus \cdots \oplus U_{i_s}$ for some $T_{\mathbf{c}}$-invariant subspaces U_{i_r} of F^n and $k := \dim_F C = k_{i_1}p_{i_1} + \cdots + k_{i_s}p_{i_s}$, where $k_{i_r}p_{i_r}$ is the dimension of U_{i_r};

(2) $f_{T_{\mathbf{c}}|C}(x) = (-1)^{k_{i_1}p_{i_1}+k_{i_2}p_{i_2}+\cdots+k_{i_s}p_{i_s}} f_{i_1}^{p_{i_1}}(x) f_{i_2}^{p_{i_2}}(x) \cdots f_{i_s}^{p_{i_s}}(x) = g(x)$;

(3) $\mathbf{c}' \in C$ iff $g(A)\mathbf{c}' = \mathbf{0}$;

(4) the polynomial $g(x)$ has the smallest degree with respect to (3) in this theorem;

(5) $\mathrm{rank}(g(A)) = n-k$ and the matrix H the rows of which constitute an arbitrary set of $n-k$ linearly independent rows of $g(A)$ is a parity check matrix of C.

Proof. (1) This follows from 2) of Theorem 2.1.

(2) Let $(g_1^{(i_r)}, \ldots, g_{k_{i_r}p_{i_r}}^{(i_r)})$ be a basis of U_{i_r} over F, where $r = 1, \ldots, s$, and let A_{i_r} be the matrix of $T_{\mathbf{c}}|U_{i_r}$ with respect to that basis. Then $(g_1^{(i_1)}, \ldots, g_{k_{i_1}p_{i_1}}^{(i_1)}, \ldots, g_1^{(i_s)}, \ldots, g_{k_{i_s}p_{i_s}}^{(i_s)})$ is a basis of C over F and $T_{\mathbf{c}}|C$ is represented by the following matrix:

$$\begin{bmatrix} A_{i_1} & & & & \\ & A_{i_2} & & & \\ & & A_{i_3} & & \\ & & & \ddots & \\ & & & & A_{i_s} \end{bmatrix}$$

with respect to that basis. Hence,

$$f_{T_{\mathbf{c}}|C} = (-1)^{k_{i_1}p_{i_1}+k_{i_2}p_{i_2}+\cdots+k_{i_s}p_{i_s}} f_{i_1}^{p_{i_1}}(x) f_{i_2}^{p_{i_2}}(x) \cdots f_{i_s}^{p_{i_s}}(x).$$

(3) Let $\mathbf{c}' \in C$, then $\mathbf{c}' = \mathbf{u}_{i_1} + \cdots + \mathbf{u}_{i_s}$ for some $\mathbf{u}_{i_r} \in U_{i_r}$, where $r = 1, \ldots, s$, and

$$g(A)\mathbf{c}' = (-1)^{k_{i_1}p_{i_1}+\cdots+k_{i_s}p_{i_s}}[(f_{i_1}^{p_{i_1}} f_{i_2}^{p_{i_2}} \cdots f_{i_s}^{p_{i_s}})(A)\mathbf{u}_{i_1} + (f_{i_1}^{p_{i_1}} f_{i_2}^{p_{i_2}} \cdots f_{i_s}^{p_{i_s}})(A)\mathbf{u}_{i_s}] = \mathbf{0}.$$

Conversely, suppose that $g(A)\mathbf{c}' = 0$ for some $\mathbf{c}' \in F^n$. According to Theorem 2.2 part 3, $c' = u_1 + u_2 + \cdots + u_t$. Then

$$g(A)\mathbf{c}' = (-1)^{k_{i_1}p_{i_1}+\cdots+k_{i_s}p_{i_s}}[(f_{i_1}^{p_{i_1}} f_{i_2}^{p_{i_2}} \cdots f_{i_s}^{p_{i_s}})(A)\mathbf{u}_1 + \cdots + (f_{i_1}^{p_{i_1}} f_{i_2}^{p_{i_2}} \cdots f_{i_s}^{p_{i_s}})(A)\mathbf{u}_t] = \mathbf{0},$$

so that $g(A)(\mathbf{u}_{j_1} + \cdots + \mathbf{u}_{j_l}) = 0$, where $\{j_1, \ldots, j_l\} = \{1, \ldots, t\} \backslash \{i_1, \ldots, i_s\}$. Let $\mathbf{v} = \mathbf{u}_{j_1} + \cdots + \mathbf{u}_{j_l}$ and $h(x) = \frac{f(x)}{g(x)}$. Since $(h(x), g(x)) = 1$, there are polynomials $a(x), b(x) \in F[x]$ such that $a(x)h(x) + b(x)g(x) = 1$. Therefore, $\mathbf{v} = a(A)h(A)\mathbf{v} + b(A)g(A)\mathbf{v} = \mathbf{0}$ and so $\mathbf{c}' \in C$.

(4) Suppose that $b(x) \in F[x]$ is a nonzero polynomial of smallest degree such that $b(A)\mathbf{c}' = 0$ for all $\mathbf{c}' \in C$. By the division algorithm in $F[x]$ there are polynomials $q(x), r(x)$ such that $g(x) = b(x)q(x) + r(x)$, where $\deg(b(x)) < \deg(g(x))$. Then for each vector $\mathbf{c} \in C$, we have $g(A)\mathbf{c}' = q(A)b(A)c' + r(A)c'$ and hence, $r(A)\mathbf{c}' = \mathbf{0}$. But this contradicts the choice of $b(x)$ unless $r(x) = 0$. Thus $b(x)$ divides $g(x)$. If $\deg(b(x)) < \deg(g(x))$, then $b(x)$ is a product of some irreducible factors of $g(x)$, and without loss of generality we may assume that $b(x) = (-1)^{k_{i_1}p_{i_1}+k_{i_2}p_{i_2}+\cdots+k_{i_m}p_{i_m}} f_{i_1}^{p_{i_1}}(x) f_{i_2}^{p_{i_2}}(x) \cdots f_{i_m}^{p_{i_m}}(x)$ and $m < s$. Let us consider the code $C' = U_{i_1} \bigoplus U_{i_2} \bigoplus \cdots \bigoplus U_{i_m} \subset C$. Then $b(x) = f_{T_{\mathbf{c}}|C'}(x)$ and by the equation $g(A)\mathbf{c}' = \mathbf{0}$ for all $\mathbf{c}' \in C$, we obtain that $C \subseteq C'$. This contradiction proves the statement.

(5) $\dim_F C = k = n - \operatorname{rank}(g(A))$, so $\operatorname{rank}(g(A)) = n - k = \dim_F C^{\perp}$.

□

3 Idempotent matrices

Let $C = U_i$ be a linear polycyclic code of length n over F,

$$g(x) = (-1)^{k_i p_i} f_i^{p_i}(x)$$

and

$$h(x) = (-1)^{n-k_i p_i} \hat{f}_i^{p_i}(x),$$

where $k_i p_i = \dim_F U_i$. Since $\gcd(g(x), h(x)) = 1$, there are unique polynomials $u_i(x), v_i(x) \in F[x]$ such that $u_i(x)g(x) + v_i(x)h(x) = 1, \deg(u_i(x)) < \deg(h(x)), \deg(v_i(x)) < \deg(g(x))$. It follows that

$$v_i(x)h(x)[u_i(x)g(x) + v_i(x)h(x)] = v_i(x)h(x)$$

and hence

$$v_i(A)h(A)[u_i(A)g(A) + v_i(A)h(A)] = v_i(A)h(A).$$

If we let $e_i(A) = v_i(A)h(A)$, then we have $e_i^2(A) = e_i(A)$ because of $h(A)g(A) = f(A) = 0$. The main properties of the **idempotent matrices** $e_i(A)$ are as follows.

Theorem 3.1. *The matrices $e_i(A), i = 1, \ldots, t$, satisfy the following relations:*
(1) $e_i^2(A) = e_i(A)$;
(2) $e_i(A)e_j(A) = 0$ *for* $j \neq i$;
(3) $\mathbf{c}' \in U_i$ *iff* $e_i(A)\mathbf{c}' = \mathbf{c}'$;
(4) $e_i(A)\mathbf{c}' = 0$ *iff for all* $\mathbf{c}' \in U_j$, $j \neq i$;
(5) $\sum_{i=1}^{t} e_i(A) = E$;
(6) *the columns of* $e_i(A)$ *generate* U_i.

Proof. (1) $e_i(A) = (-1)^{n-k_i p_i} v_i(A)\hat{f}_i^{p_i}(A) = v_i(A)h(A)$, so $e_i^2(A) = e_i(A)$.

(2) $e_i(A)e_j(A) = (-1)^{2n-k_i p_i - k_j p_j} v_i(A)v_j(A)\hat{f}_i^{p_i}(A)\hat{f}_j^{p_j}(A) = u(A)f(A) = 0$ for a suitable polynomial $u(x) \in F[x]$.

(3) Let $\mathbf{c}' \in U_i$, then we have

$$(-1)^{k_i p_i} u_i(A) f_i(A)^{p_i}\mathbf{c}' + (-1)^{n-k_i p_i} v_i(A)\hat{f}_i(A)^{p_i}\mathbf{c}' = e_i(A)\mathbf{c}' = \mathbf{c}'.$$

Conversely, let $e_i(A)\mathbf{c}' = \mathbf{c}'$, then

$$f_i^{p_i}(A)\mathbf{c}' = f_i^{p_i}(A)e_i(A)\mathbf{c}' = (-1)^{n-k_i p_i} v_i(A)f(A)\mathbf{c}' = \mathbf{0},$$

so $\mathbf{c}' \in U_i$.

(4) Let $\mathbf{c}' \in U_j$, $j \neq i$. Then $e_i(A)\mathbf{c}' = (-1)^{n-k_i p_i} v_i(A)\hat{f}_i^{p_i}(A)\mathbf{c}' = u(A)f_j^{p_j}(A)\mathbf{c}' = \mathbf{0}$.

(5) For the proof of (5) we refer to Theorems 3 to 5 in [10].

(6) For the proof of (6) we refer to Theorems 3 to 6 in [10].

This completes the proof. □

Because of the preceding theorem and the form of constructing polynomial, the proofs of the following two theorems are similar to those of Theorems 4 and 5 in [10]. Thus we omit them here.

Theorem 3.2. *$e_i(A)$ is the only idempotent matrix satisfying $e_i(A)\mathbf{c}' = \mathbf{c}'$ for all $\mathbf{c}' \in U_i$ and $e_i(A)\mathbf{x} = \mathbf{0}$ for all $\mathbf{x} \in \sum_{j\neq i} U_j$.*

Now let $C = U_{i_1} \bigoplus U_{i_2} \bigoplus \cdots \bigoplus U_{i_s}$ be an arbitrary linear polycyclic code of length n over F. Then

$$f_{T_c|C}(x) = (-1)^{k_{i_1}p_{i_1}+\cdots+k_{i_s}p_{i_s}} f_{i_1}^{p_{i_1}}(x) f_{i_2}^{p_{i_2}}(x) \cdots f_{i_s}^{p_{i_s}}(x) = g(x),$$

and

$$h(x) = \frac{f(x)}{g(x)} = (-1)^{n-(k_{i_1}p_{i_1}+k_{i_2}p_{i_2}+\cdots+k_{i_s}p_{i_s})} f_{j_1}^{p_{j_1}}(x) f_{j_2}^{p_{j_2}}(x) \cdots f_{j_l}^{p_{j_l}}(x),$$

where $\{j_1, \ldots, j_l\} = \{1, \ldots, t\} \backslash \{i_1, \ldots, i_s\}$. Let $e(A) = v(A)h(A)$ for some polynomial $v(A) \in F[x]$, $e^2(A) = e(A)$.

Theorem 3.3. *Let $C = U_{i_1} \bigoplus U_{i_2} \bigoplus \cdots \bigoplus U_{i_s}$ be an arbitrary linear polycyclic code of length n over F. Then the following facts hold:*

(1) $\mathbf{c}' \in C$ iff $e(A)\mathbf{c}' = \mathbf{c}'$;

(2) the columns of $e(A)$ generate C;

(3) $e(A) = e_{i_1}(A) + e_{i_2}(A) + \cdots + e_{i_s}(A)$;

(4) the polycyclic code $C' = U_{j_1} \bigoplus U_{j_2} \bigoplus \cdots \bigoplus U_{j_l}$ has the idempotent matrix $E - e(A)$.

4 Bounds for polycyclic codes

Let $K = \mathbb{F}_{q^m}$ be the splitting field of the polynomial $f(x) = (-1)^{n+1}(\sum_{i=0}^{n-1} c_i x^i - x^n)$ over $\mathbb{F}_q$, where $0 \neq c_0 \in \mathbb{F}_q$. Let z be a root of $f(x)$. Then z is an eigenvalue of A, where

$$A = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & 0 & c_0 \\ 1 & 0 & 0 & \cdots & 0 & 0 & c_1 \\ 0 & 1 & 0 & \cdots & 0 & 0 & c_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 & c_{n-2} \\ 0 & 0 & 0 & \cdots & 0 & 1 & c_{n-1} \end{bmatrix}.$$

The corresponding eigenvector is given by

$$A^t\mathbf{v}(z)^t = z\mathbf{v}(z)^t, \mathbf{v}(z) = (1, z, \ldots, z^{n-1}),$$

where $*^t$ is transposition and $\mathbf{v}$ is an eigenvector of A^t with associated eigenvalue z.

Now we study the case that $f(x)$ has no repeated roots. Assume that $f(x)$ has n distinct roots z_j, $1 \leq j \leq n$. Each root is an eigenvalue of A and A^t.

$$A^t\mathbf{v}(z_j) = z_j\mathbf{v}(z_j), 1 \leq j \leq n.$$

These n statements can be expressed in just one matrix statement (each eigenvector being a column of the Vandermonde matrix $V = V(z_1, z_2, \ldots, z_n)$), where

$$V = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 & 1 & 1 \\ z_1 & z_2 & z_3 & \cdots & z_{n-2} & z_{n-1} & z_n \\ z_1^2 & z_2^2 & z_3^2 & \cdots & z_{n-2}^2 & z_{n-1}^2 & z_n^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ z_1^{n-2} & z_2^{n-2} & z_3^{n-2} & \cdots & z_{n-2}^{n-2} & z_{n-1}^{n-2} & z_n^{n-2} \\ z_1^{n-1} & z_2^{n-1} & z_3^{n-1} & \cdots & z_{n-2}^{n-1} & z_{n-1}^{n-1} & z_n^{n-1} \end{bmatrix}.$$

Let $D = \mathrm{diag}(z_1, z_2, \ldots, z_n)$ be the diagonal matrix with the roots $\{z_j | 1 \leq j \leq n\}$ on the main diagonal and with zeros everywhere else, we have

$$A^tV = VD \Leftrightarrow V^{-1}A^tV = D \Leftrightarrow V^tA(V^t)^{-1} = D.$$

Let $T = (V^t)^{-1}$, then $T^{-1}AT = D$, where

$$T^{-1} = \begin{bmatrix} 1 & z_1 & z_1^2 & \cdots & z_1^{n-3} & z_1^{n-2} & z_1^{n-1} \\ 1 & z_2 & z_2^2 & \cdots & z_2^{n-3} & z_2^{n-2} & z_2^{n-1} \\ 1 & z_3 & z_3^2 & \cdots & z_3^{n-3} & z_3^{n-2} & z_3^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 1 & z_{n-1} & z_{n-1}^2 & \cdots & z_{n-1}^{n-3} & z_{n-1}^{n-2} & z_{n-1}^{n-1} \\ 1 & z_n & z_n^2 & \cdots & z_n^{n-3} & z_n^{n-2} & z_n^{n-1} \end{bmatrix}.$$

Let $\mathbf{u}_i = (1, z_i, \ldots, z_i^{n-1}), 1 \leq i \leq n$, which is a row of T^{-1}. Since D is a diagonal matrix, the matrices $g(D)$ and $h(D)$ are also diagonal.

Let $\deg(h(x)) = n - k = r$, and let its r zeros be $z_{i_1}, z_{i_2}, \ldots, z_{i_r}$ and its k nonzeros be $z_{j_1}, z_{j_2}, \ldots, z_{j_k}$. It is obvious that the zeros of $g(x)$ are the nonzeros of $h(x)$ and vice versa. We denote $I = \{i_1, i_2, \ldots, i_r\}$ and $J = [n] \setminus I = \{j_1, j_2, \ldots, j_k\}$.

Assume that $\mathbf{d} = (d_1, d_2, \ldots, d_n) \in \mathbb{F}_q^n$ and let $\mathbf{d}' = T^{-1}\mathbf{d}$. We know $\mathbf{d} \in C$ iff $g(A)\mathbf{d} = \mathbf{0}$. The latter condition is equivalent to $g(D)\mathbf{d}' = T^{-1}g(A)TT^{-1}\mathbf{d} = T^{-1}g(A)\mathbf{d} = \mathbf{0}$, which, in

its turn, is equivalent to $d'_i = 0, i \in I$. Hence,

$$\mathbf{d} \in C \Leftrightarrow \mathbf{u}_i \mathbf{d} = 0, i \in I.$$

Let K be any finite field and $\mathcal{A} = [\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n]$ any matrix over K with n columns $\mathbf{a}_i, 1 \leq i \leq n$. Let $C_{\mathcal{A}}$ denote the linear code over K with $\mathcal{A}$ as parity check matrix. The minimum distance of $C_{\mathcal{A}}$ will be denoted as $d_{\mathcal{A}}$.

For any $m \times n$ matrix $X = [\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n]$ with nonzero columns $\mathbf{x}_i \in K^m$ for $1 \leq i \leq n$, we define the matrix $\mathcal{A}(X)$ as

$$\mathcal{A}(X) = \begin{pmatrix} x_{11}\mathbf{a}_1 & x_{12}\mathbf{a}_2 & \cdots & x_{1n}\mathbf{a}_n \\ x_{21}\mathbf{a}_1 & x_{22}\mathbf{a}_2 & \cdots & x_{2n}\mathbf{a}_n \\ \vdots & \vdots & \ddots & \vdots \\ x_{m1}\mathbf{a}_1 & x_{m2}\mathbf{a}_2 & \cdots & x_{mn}\mathbf{a}_n \end{pmatrix}$$

We recall the following lemma [10], which describes how the parity-check matrix $\mathcal{A}$ for a linear code can be extended with new rows in such a way that the minimum distance increases.

Lemma 4.1. *If $d_{\mathcal{A}} \geq 2$ and every $m \times (m + d_{\mathcal{A}} - 2)$ submatrix of X has full rank, then $d_{\mathcal{A}(X)} \geq d_{\mathcal{A}} + m - 1$.*

Next, we recall the following BCH type lower bound that is a direct consequence of the observation that a shortened code has at least as great a minimum distance as the original code [8, p. 241].

Theorem 4.2. *(BCH Type Lower Bound)[4] Let C be a polycyclic code over $\mathbb{F}_q$ with $g(x) = f_{T_{\mathbf{c}}|C}(x)$ and $h(x) = \frac{f(x)}{g(x)}$. If $f(x)$ has no repeated roots and $\deg(f(x)) = n_1 \geq 1$. Suppose $f(x)|(x^n - 1)$ for some positive integer n with $\gcd(n, q) = 1$. Let β be a primitive element of order n in some finite extension of $\mathbb{F}_q$. Suppose there are integers a, b, d such that $\{\beta^{a+bi} : 0 \leq i \leq d-2$ and $h(\beta^{a+bi}) = 0\}$ and $\frac{n}{\gcd(b,n)} \geq n_1 \geq d - 1$. Then the minimum distance of C is at least d.*

Definition 4.3. *Let $K = \mathbb{F}_{q^m}$. A set $M = \{\alpha_{j_1}, \alpha_{j_2}, \ldots, \alpha_{j_l}\}$ is a consecutive set of n-th roots of unity if there is some primitive n-th root of unity β in K such that M consists of consecutive powers of β.*

Definition 4.4. *Given n_1 such that $n_1 \leq n$. If $N = \{\alpha_{j_1}, \alpha_{j_2}, \ldots, \alpha_{j_t}\}$ is a set of zeros of n-th roots of unity, we denote by U_N or by $U_{(\alpha_{j_1}, \alpha_{j_2}, \ldots, \alpha_{j_t})}$ the matrix of size t by n_1 over K that has $(1, \alpha_{j_s}, \ldots, \alpha_{j_s}^{n_1 - 1})$ as its s-th row.*

From the discussion above, it is clear that U_N is a parity-check matrix for the polycyclic code C over $\mathbb{F}$ having N as a set of zeros of $h(x)$. Let C_N be the polycyclic code over K with U_N as the parity-check matrix, and let this code have minimum distance d_N. So the minimum distance of C is at least d_N, because C is a subfield subcode of C_N.

The proof of the following theorem is similar to that of Theorem 6 in [10], so we omit it here.

Theorem 4.5. *If M, N are sets of n-th roots of unity such that $|\overline{M}| \leq |M| + d_N - 2$ for some consecutive set $\overline{M}$ containing M, then $d_{MN} \geq d_N + |M| - 1$, where $MN = \{\alpha\beta | \alpha \in M, \beta \in N\}$.*

According to Theorems 4.2 and 4.5, a systematic algorithm to compute the bound for a polycyclic code C in the multiplicity free case can be sketched as follows.

(i) For a polycyclic code C over $\mathbb{F}_q$ with $f(x) = f_{T_c}(x)$, $g(x) = f_{T_c|C}(x)$ and $h(x) = \frac{f(x)}{g(x)}$. Write $n_1 = \deg(f(x))$. If $f(x)$ has no repeated roots, we can find a minimal integer n such that $f(x)|(x^n - 1)$, and $\gcd(n, q) = 1$. Let β be a primitive element of order n in the splitting field $\mathbb{F}_{q^m}$ of $x^n - 1$ over F.

(ii) Compute the cyclotomic cosets of n mod q, denoted by C_i for $i = 0, 1, \ldots, s$.

(iii) Write the zeros of $h(x)$ as β^i, with i belonging to some union of the cyclotomic cosets. If $h(x)$ has a string of $\delta - 1$ consecutive zeros, then the BCH bound of C is δ.

(iv) Find two sets M, N satisfy the conditions in Theorem 4.5 such that MN is contained in the set of zeros of $h(x)$.

(v) Find the matrix U_N that has $(1, \alpha, \ldots, \alpha^{n_1 - 1})$ as its row for all $\alpha \in N$. Let U_N be the parity-check matrix over $\mathbb{F}_{q^m}$ and compute the minimum distance d_N. Then our bound for the minimum distance C is $d \geq d_{MN} \geq d_N + |M| - 1$.

Example 4.6. *A polycyclic code C over $\mathbb{F}_2$ with $f(x) = (x^2 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)$ and $g(x) = x^4 + x^3 + 1$. We can find $f|(x^{15} - 1)$ and $(15, 2) = 1$. Let β be a primitive 15-th root of unity. We determine the cyclotomic coset of 2 mod 15. These are $C_0 = \{0\}$, $C_1 = \{1, 2, 4, 8\}$, $C_3 = \{3, 6, 9, 12\}$, $C_5 = \{5, 10\}$ and $C_7 = \{7, 11, 13, 14\}$. It is easy to check that the zeros of $h(x) = \frac{f(x)}{g(x)}$ are β^i with $i \in C_3 \cup C_5$. Since $h(x)$ has a string of two consecutive zeros, the linear polycyclic code C defined by $h(x)$ has a minimum distance $d \geq 3$ according to Theorem 4.2.*

Now take $\{\beta^i | i = 5, 9\}$ and $M = \{\beta^i | i = 0, 1\}$. Then the elements of MN are zeros of $h(x)$. Since $d_N = 3$ and $|\overline{M}| = 2 \leq |M| + d_N - 2 = 3$, Theorem 4.5 implies $d \geq d_{MN} \geq |M| + d_N - 1 = 4$.

Similar to the discussion as above, we have

(a) *Let C be a polycyclic code over $\mathbb{F}_7$ with $f(x) = (x^4+x^3+x^2+x+1)(x^4+2x^3+4x^2+2x+1)(x^4+4x^3+4x+1)(x^4+4x^3+3x^2+4x+1)(x^4+6x^3+5x^2+6x+1)$ and $g(x) = (x^4+6x^3+5x^2+6x+1)(x^4+4x^3+4x+1)$. Then the BCH bound is 5 and our bound is 6.*

(b) *Let C be a polycyclic code over $\mathbb{F}_3$ with $f(x) = (x+2)(x^5+x^4+2x^3+x^2+2)(x^5+2x^3+2x^2+2x+1)$ and $g(x) = x+2$. Then the BCH bound is 4 and our bound is 5.*

(c) *Let C be a polycyclic code over $\mathbb{F}_5$ with $f(x) = (x+1)(x+2)(x+3)(x^2+x+2)(x^2+3x+3)$ and $g(x) = (x^2+3x+3)(x+3)$. Then the BCH bound is 3 and our bound is 4.*

5 Conclusion and open problems

In the present paper, we have developed an approach to polycyclic codes based on the theory of invariant subspaces under a fixed endomorphism. When the characteristic polynomial of this endomorphism is multiplicity free in its factorization, we have derived a lower bound on the minimum distance of the polycyclic codes. This mild hypothesis is equivalent, in the cyclic codes case, to the coprimality of the length and the alphabet size. The first open problem is to derive a similar bound for the repeated root case. Another open problem would be to generalize our results from finite fields alphabets to chain rings [7]. Finally, an algebraic decoding algorithm would be a natural continuation of the minimum distance bound.

Acknowledgement: This research is supported by National Natural Science Foundation of China (61672036), the Excellent Youth Foundation of Natural Science Foundation of Anhui Province (1808085J20), the Academic Fund for Outstanding Talents in Universities (gxbjZD03)

References

[1] A. Alahmadi, S. T. Dougherty, A. Leroy, P. Solé, On the duality and the direction of polycyclic codes, Adv. Math. Commun., **10(4)**, (2016), 921–929 .

[2] C. Gueneri, F. Ozdemir, P. Solé, On the additive cyclic structure of quasi-cyclic codes. Discret. Math. **341(10)**, (2018), 2735–2741.

[3] H. K. Hoffman, R. Kunze, *Linear Algebra*, (1971), Prentice-Hall, Inc. Englewood Cliffs, New Jersey.

[4] S. Li, M. Xiong, G. Ge, Pseudo-cyclic codes and the construction of quantum MDS codes, IEEE Transactions on Information Theory, **62(4)**, (2016), 1703–1710.

[5] S. R. Lopez-Permouth, B. R. Parra-Avila, S. Szabo, Dual generalizations of the concept of cyclicity of codes, Adv. Math. Commun., **3(3)**, (2009), 227–234.

[6] S. R. Lopez-Permouth, H. Özadam, F. Özbudak, S. Szabo, Polycyclic codes over Galois rings with applications to repeated-root constacyclic codes, Finite Fields Their Appl., **19(1)**, (2013), 16-38.

[7] E. Martinez-Moro, A. Fotue, T. Blackford, On polycyclic codes over a finite chain ring. Adv. Math. Commun., **3**,(2020) 10.3934/amc.2020028

[8] W. W. Peterson and E. J. Weldon, *Error-Correcting Codes*, 2nd ed. Cambridge, MA, USA: MIT Press, (1972).

[9] D. Radkova, A. Bojilov, A. J. V. Zanten, Cyclic codes and quasi-twisted codes: an algebraic approach, Report MICC 07-08, Universiteit Maastricht, 2007.

[10] D. Radkova, A. J. V. Zanten, Constacyclic codes as invariant subspaces. Linear Algebra and its Applications, **430(2-3)**, (2009), 855–864.