AIMS Mathematics, 9(11): 29707–29717.
DOI: 10.3934/math.20241439
Received: 30 August 2024
Revised: 04 October 2024
Accepted: 14 October 2024
Published: 21 October 2024

https://www.aimspress.com/journal/Math

Research article

The polycyclic codes over the finite field $\mathbb{F}_q$

Wei Qi*

School of Mathematics and Statistics, Shandong University of Technology, Zibo, Shandong 255049, China

* **Correspondence:** Email: qwrghj@126.com.

Abstract: This article extended the properties of the idempotent generator of cyclic codes to polycyclic codes over the finite field $\mathbb{F}_q$. In addition, the check matrix of polycyclic codes was provided over $\mathbb{F}_q$. Specifically, it has been proven that the constacyclic code is an MDS code over $\mathbb{F}_q$ if and only if its annihilator dual code is also an MDS code. Finally, we have provided some examples of good codes.

Keywords: polycyclic codes; idempotent generator; check matrix; MDS codes
Mathematics Subject Classification: 94B15, 94B05

1. Introduction

In 1972, Peterson first introduced the concept of pseudocyclic codes over fields through the quotient ring angle of polynomial rings in [13, p.241]. The important engineering application value of pseudocyclic codes is elaborated, and it is pointed out that pseudocyclic codes can be used to correct any sudden errors in information transmission. Compared with cyclic codes and constacyclic codes, the algebraic structure of pseudocyclic codes is more complex. So in the following period, there was relatively little research on pseudocyclic codes (see [4,7,10,12]). Until 2009, López-Permouth et al. [8] redefined pseudocyclic codes from the perspective of linear algebra and called them polycyclic codes, and discussed the basic properties of polycyclic codes and sequential codes over $\mathbb{F}_q$. It was proved that the Euclidean dual codes of polycyclic codes are sequential codes. In 2011, López-Permouth et al. [9] discussed the structure and generating sets of polycyclic codes on the Galois ring $GR(p^a, m)$. The Hamming distance of the cyclic code with a length of p^s over $GR(p^2, m)$ was calculated in detail. However, one of the main reasons why polycyclic codes have not been as widely studied as cyclic codes is that the Euclidean dual codes of polycyclic codes are no longer polycyclic codes. In 2016, to solve this issue, Alahmadi et al. [1] studied the algebraic properties of polycyclic codes over fields, introduced the annihilator product and annihilator dual codes, gave the MacWilliams identities of

polycyclic codes and their annihilator dual codes, and finally obtained the equivalent characterization of constacyclic codes. In 2020, Shi et al. [15] studied polycyclic codes over finite fields through the perspective of invariant subspace theory in linear algebra, and gave the bounds of the minimum distance of these polycyclic codes. Subsequently, scholars shifted the research scope of polycyclic codes from finite fields to finite rings. In 2020, Martinez-Moro et al. [11] studied the properties of free polycyclic codes on finite chain rings, and gave the basic properties of Euclidean dual codes and annihilator dual codes of polycyclic codes. It is shown that the dual annihilator code of polycyclic codes over finite chain rings is still a polycyclic code. In 2024, the author [14] gave the concepts of annihilator self-orthogonal code, annihilator self-dual code, and annihilator LCD code by using the annihilator product over finite rings, and studied their discrimination conditions and counting problems over the ring $\mathbb{F}_q + u\mathbb{F}_q$, using their generator polynomials and check polynomials over $\mathbb{F}_q$.

So far, there is relatively little research on polycyclic codes over finite rings. This article conducts research on polycyclic codes over the finite field $\mathbb{F}_q$. This lays the foundation for future research on polycyclic codes over finite rings. The main research content of this article is as follows. This article will extend the properties of the idempotent generator of cyclic codes to polycyclic codes over the finite field $\mathbb{F}_q$. In addition, the check matrix of polycyclic codes is provided over $\mathbb{F}_q$. Specifically, it has been proven that the constacyclic code is an MDS code over $\mathbb{F}_q$ if and only if its annihilator dual code is also an MDS code. Finally, we provide some examples of good codes.

2. Idempotent generator of polycyclic codes over $\mathbb{F}_q$

In 2009, López-Permouth [8] proposed the concept of polycyclic codes and sequential codes over the finite field $\mathbb{F}_q$.

Definition 2.1. *[8] Let C be a linear code of length n over $\mathbb{F}_q$, if there exists $\mathbf{a} = (a_0, a_1, ..., a_{n-1}) \in \mathbb{F}_q^n$, where $a_0 \neq 0$, such that for every $c = (c_0, c_1, ..., c_{n-1}) \in C$,*

(1) $(0, c_0, c_1, ..., c_{n-2}) + c_{n-1}(a_0, a_1, ..., a_{n-1}) \in C$. Then C is said to be an $\mathbf{a}$-polycyclic code over $\mathbb{F}_q$;

(2) $(c_1, c_2, ..., c_{n-1}, c_0a_0 + c_1a_1 + ... + c_{n-1}a_{n-1}) \in C$. Then C is said to be an $\mathbf{a}$-sequential code over $\mathbb{F}_q$.

Some properties of the idempotent generator of cyclic codes over $\mathbb{F}_q$ are provided in [6, Section 4.3]. In 2020, Shi et al. [15] extended the idempotent generator from cyclic codes to polycyclic codes, and studied the idempotent matrix of polycyclic codes over finite fields and its basic properties. As an application, the lower bounds of the minimum distance of some polycyclic codes are given. This section assumes $x^n - \mathbf{a}(x) \in \mathbb{F}_q[x]$ in $\mathbb{F}_q$ which is not a double root in the algebraic closure of $\mathbb{F}_q$. This section mainly discusses some properties of the idempotent generator of polycyclic codes over $\mathbb{F}_q$.

Definition 2.2. *Let C be an $\mathbf{a}$-polycyclic code over $\mathbb{F}_q$, $e(x) \in C$. If $e^2(x) = e(x)$, then $e(x)$ is an idempotent of C. Further, if $C = \langle e(x) \rangle$, then $e(x)$ is called the idempotent generator of C.*

The existence of the idempotent generator of cyclic codes over fields in [6, Theorem 4.3.2], and the existence of the idempotent generative matrix of polycyclic codes over fields was studied in [15, Theorem 3.1 (6)]. Next, we study the unique existence of the idempotent generator of $\mathbf{a}$-polycyclic codes over fields.

Theorem 2.3. *Let C be a polycyclic code of length n over $\mathbb{F}_q$, if there are no double roots in $x^n - \mathbf{a}(x) \in \mathbb{F}_q[x]$. Then*

(1) There exists a unique idempotent element $e(x) \in C$, such that $C = \langle e(x) \rangle$;

(2) If $e(x)$ is a non-zero idempotent element of C, then $C = \langle e(x) \rangle$ if and only if $e(x)$ is the unity of C.

Proof. First, we construct idempotent elements of C. Let $g(x)$ be the generator polynomial of $\mathbf{a}$-polycyclic code C, and then $g(x)|(x^n - \mathbf{a}(x))$. Let $h(x) = (x^n - \mathbf{a}(x))/g(x)$. Since $x^n - \mathbf{a}(x)$ has no double roots, $\gcd(g(x), h(x)) = 1$. So there exist $s(x), t(x) \in \mathbb{F}_q[x]$, such that $s(x)g(x) + t(x)h(x) = 1$. Set $e(x) = s(x)g(x)$, and we have

$$\begin{aligned} e^2(x) &= s(x)g(x)s(x)g(x) = s(x)g(x)(1 - t(x)h(x)) \\ &\equiv s(x)g(x) \bmod (x^n - \mathbf{a}(x)). \end{aligned}$$

Hence, $e^2(x) = e(x)$.

The necessity of proving (2). Let $c(x) \in C$. As $C = \langle e(x) \rangle$, there exists $m(x) \in \mathbb{F}_q[x]$ such that $c(x) = e(x)m(x)$. From the fact that $e(x)$ is a non-zero idempotent element in C, we have

$$c(x)e(x) = e^2(x)m(x) = e(x)m(x) = c(x).$$

$e(x)$ is the unity of C.

The sufficiency of proving (2). Let $e(x)$ be the unity of C, and then $e(x) \in C$. In light of [14, Proposition 1], the $\mathbf{a}$-polycyclic code C over $\mathbb{F}_q$ is the ideal of the quotient rings of $\mathbb{F}_q[x]/\langle x^n - \mathbf{a}(x) \rangle$. It implies that $\langle e(x) \rangle \subseteq C$.

On the other hand, if for any $c(x) \in C$, $c(x) = e(x)c(x) \in \langle e(x) \rangle$ is known from the fact that $e(x)$ is the unity of C. Therefore, $C \subseteq \langle e(x) \rangle$. So $C = \langle e(x) \rangle$.

Next, we use the equivalent characterization of the idempotent generator in (2) to continue to prove (1): The existence and uniqueness of the idempotent generator.

Assuming any $c(x) \in C$, there exists $f(x) \in \mathbb{F}_q[x]$ such that $c(x) = g(x)f(x)$, and therefore,

$$\begin{aligned} c(x)e(x) &= g(x)f(x)s(x)g(x) = g(x)f(x)(1 - t(x)h(x)) \\ &\equiv g(x)f(x) \equiv c(x) \bmod (x^n - \mathbf{a}(x)). \end{aligned}$$

Thus, $e(x)$ is the unity of C. From (2), we have $C = \langle e(x) \rangle$.

Uniqueness. Set $e_1(x), e_2(x)$ are idempotent generators of C, and $e_1(x), e_2(x)$ are the unities of C. Therefore

$$e_1(x) = e_1(x)e_2(x) = e_2(x).$$

□

It can be seen from the above that polycyclic codes can be generated not only by generator polynomials, but also by idempotent generators. Therefore, we will build a relationship between idempotent generators and generator polynomials.

Theorem 2.4. *Let C be an $\mathbf{a}$-polycyclic code of length n over $\mathbb{F}_q$, $g(x)$ be the generator polynomial of C, and $e(x)$ be the idempotent generator of C. Then* $\gcd(e(x), x^n - \mathbf{a}(x)) = g(x)$.

Proof. Let $g(x)$ be the generator polynomial of the **a**-polycyclic code C over $\mathbb{F}_q$, and then $g(x)|(x^n - \mathbf{a}(x))$. Let $h(x) = (x^n - \mathbf{a}(x))/g(x)$. Since $x^n - \mathbf{a}(x)$ has no double roots, $\gcd(g(x), h(x)) = 1$. Thus, there exist $s(x), t(x) \in \mathbb{F}_q[x]$, such that $s(x)g(x) + t(x)h(x) = 1$. According to Theorem 2.3, we obtain $e(x) = s(x)g(x)$. Therefore

$$\begin{aligned}\gcd(e(x), x^n - \mathbf{a}(x)) &= \gcd(s(x)g(x), g(x)h(x)) \\ &= g(x)\gcd(s(x), h(x)) \\ &= g(x).\end{aligned}$$

□

Proposition 1. *Let C be an* **a***-polycyclic code of length n and dimension k over $\mathbb{F}_q$, and let $e(x)$ be the idempotent generator of C. Then $\{e(x), xe(x), .., x^{k-1}e(x)\}$ is a basis of C.*

Proof. Let $b_0e(x) + b_1xe(x) + ...b_{k-1}x^{k-1}e(x) = 0$, where $b_i \in \mathbb{F}_q$ $(0 \leqslant i \leqslant k-1)$. Then

$$b(x)e(x) = 0,$$

where $b(x) = b_0 + b_1x + ...b_{k-1}x^{k-1}$, $\deg(b(x)) \leqslant k-1$. Let $g(x)$ be the generator polynomial of the **a**-polycyclic code C. Then

$$g(x)b(x)e(x) = 0.$$

According to the idempotent generator $e(x)$ of C and Theorem 2.3, we know that $e(x)$ is the unity of C. So $g(x)b(x) = 0$ because

$$\deg(g(x)) = n - k,\ \deg(b(x)) \leqslant k - 1.$$

So we can obtain $\deg(g(x)b(x)) \leqslant n-1$. Therefore, $b(x) = 0$. Thus $b_i = 0$ $(0 \leqslant i \leqslant k-1)$. Note that the dimension of C is k, and therefore, $\{e(x), xe(x), .., x^{k-1}e(x)\}$ is a basis of C. □

If C_1 and C_2 are **a**-polycyclic codes of length n over $\mathbb{F}_q$, then $C_1 + C_2 = \{c_1 + c_2 | c_1 \in C_1, c_2 \in C_2\}$, and $C_1 \cap C_2$ are still **a**-polycyclic codes of length n over $\mathbb{F}_q$. Next, we discuss their generator polynomials and idempotent generators.

Theorem 2.5. *Let C_1 and C_2 be* **a***-polycyclic codes of length n over $\mathbb{F}_q$, $g_1(x)$ and $g_2(x)$ are, respectively, generator polynomials of C_1 and C_2, and $e_1(x)$ and $e_2(x)$ are, respectively, idempotent generators of C_1 and C_2. Then*

(1) The generator polynomial of $C_1 \cap C_2$ is $\mathrm{lcm}(g_1(x), g_2(x))$, and the idempotent generator is $e_1(x)e_2(x)$;

(2) The generator polynomial of $C_1 + C_2$ is $\gcd(g_1(x), g_2(x))$, and the idempotent generator is $e_1(x) + e_2(x) - e_1(x)e_2(x)$.

Proof. (1) Let $g(x) = \mathrm{lcm}(g_1(x), g_2(x))$, and the following proves that $C_1 \cap C_2 = \langle g(x) \rangle$.

Obviously, $g_1(x)|g(x)$, $g_2(x)|g(x)$. Thus, there exist $b_1(x), b_2(x) \in \mathbb{F}_q[x]$, such that $g(x) = g_1(x)b_1(x)$, $g(x) = g_2(x)b_2(x)$. So

$$g(x) \in \langle g_1(x) \rangle,\ g(x) \in \langle g_2(x) \rangle.$$

Since $C_1 = \langle g_1(x) \rangle$ and $C_2 = \langle g_2(x) \rangle$ are **a**-polycyclic codes over $\mathbb{F}_q$, thus

$$\langle g(x) \rangle \subseteq \langle g_1(x) \rangle,\ \langle g(x) \rangle \subseteq \langle g_2(x) \rangle,$$

and therefore, $\langle g(x)\rangle \subseteq C_1 \cap C_2$.

For any $c(x) \in C_1 \cap C_2$, then $c(x) \in C_1 = \langle g_1(x)\rangle$, $c(x) \in C_2 = \langle g_2(x)\rangle$. Therefore, there exist $b_1(x), b_2(x) \in \mathbb{F}_q[x]$, such that $c(x) = g_1(x)b_1(x)$, $c(x) = g_2(x)b_2(x)$. So $c(x)$ is a common multiple of $g_1(x)$ and $g_2(x)$. Also, we have obtained that $g(x) = \text{lcm}(g_1(x), g_2(x))$,

$$g(x)|c(x).$$

So there exists $f(x) \in \mathbb{F}_q[x]$, such that $c(x) = g(x)f(x)$. Therefore, $c(x) \in \langle g(x)\rangle$. We have $C_1 \cap C_2 \subseteq \langle g(x)\rangle$. Hence $C_1 \cap C_2 = \langle g(x)\rangle$.

Set any $c(x) \in C_1 \cap C_2$, and then $c(x) \in C_1$, $c(x) \in C_2$. Since $e_1(x)$ and $e_2(x)$ are, respectively, idempotent generators of C_1 and C_2,

$$c(x)e_1(x)e_2(x) = c(x)e_2(x) = c(x).$$

This implies $e_1(x)e_2(x)$ is the unity of $C_1 \cap C_2$. So by Theorem 2.3, $e_1(x)e_2(x)$ is the idempotent generator of $C_1 \cap C_2$.

(2) Let $g(x) = \gcd(g_1(x), g_2(x))$. Let us prove that $C_1 + C_2 = \langle g(x)\rangle$.

Obviously $g(x)|g_1(x), g(x)|g_2(x)$. So

$$\langle g_1(x)\rangle \subseteq \langle g(x)\rangle,\ \langle g_2(x)\rangle \subseteq \langle g(x)\rangle.$$

This implies $C_1 + C_2 \subseteq \langle g(x)\rangle$.

Since $g(x) = \gcd(g_1(x), g_2(x))$ can be obtained, there exist $b_1(x), b_2(x) \in \mathbb{F}_q[x]$, such that $g(x) = b_1(x)g_1(x) + b_2(x)g_2(x)$. We get $g(x) \in \langle g_1(x)\rangle + \langle g_2(x)\rangle$. Note that $C_1 + C_2$ is an **a**-polycyclic code of length n over $\mathbb{F}_q$. Thus $\langle g(x)\rangle \subseteq C_1 + C_2$. Therefore, $C_1 + C_2 = \langle g(x)\rangle$.

Set for any $c(x) \in C_1 + C_2$, $c(x) = c_1(x) + c_2(x)$, where $c_1(x) \in C_1$, $c_2(x) \in C_2$. Since $e_1(x)$ and $e_2(x)$ are, respectively, idempotent generators of C_1 and C_2, and Theorem 2.3 implies that $e_1(x)$ and $e_2(x)$ are, respectively, the unities of C_1 and C_2, we observe that

$$\begin{aligned} c(x)(e_1(x) + e_2(x) - e_1(x)e_2(x)) &= (c_1(x) + c_2(x))(e_1(x) + e_2(x) - e_1(x)e_2(x)) \\ &= c_1(x)e_1(x) + c_1(x)e_2(x) - c_1(x)e_1(x)e_2(x) \\ &\quad + c_2(x)e_1(x) + c_2(x)e_2(x) - c_2(x)e_1(x)e_2(x) \\ &= c_1(x) + c_2(x) = c(x). \end{aligned}$$

It follows that $e_1(x) + e_2(x) - e_1(x)e_2(x)$ is the unity of $C_1 + C_2$, and is also the idempotent generator of $C_1 + C_2$. □

Proposition 2. *Let C_1 and C_2 be* **a***-polycyclic codes over $\mathbb{F}_q$, and $g_1(x)$ and $g_2(x)$ are generator polynomials of C_1 and C_2, respectively. Then $C_1 \subseteq C_2$ if and only if $g_2(x)|g_1(x)$.*

Proof. Necessity. Set $C_1 \subseteq C_2$, namely, $\langle g_1(x)\rangle \subseteq \langle g_2(x)\rangle$. Then $g_1(x) \in \langle g_1(x)\rangle \subseteq \langle g_2(x)\rangle$, so there exists $f(x) \in \mathbb{F}_q[x]$, such that $g_1(x) = g_2(x)f(x)$, implying $g_2|g_1$.

Sufficiency. Set $g_2|g_1$, so there exists $f(x) \in \mathbb{F}_q[x]$, such that $g_1(x) = g_2(x)f(x)$. It shows $g_1(x) \in \langle g_2(x)\rangle$. As $\langle g_2(x)\rangle$ is an ideal of R_n, thus $\langle g_1(x)\rangle \subseteq \langle g_2(x)\rangle$, then $C_1 \subseteq C_2$. □

3. MDS codes and the check matrix of polycyclic codes over $\mathbb{F}_q$

In 2009, López-Permouth [8] discussed the basic properties of polycyclic codes and sequential codes over $\mathbb{F}_q$. In reference [8, Theorem 3.2], it was found that the Euclidean dual codes of polycyclic codes are sequential codes over $\mathbb{F}_q$.

Proposition 3. *[8] Let C be an $\mathbf{a}$-polycyclic code over $\mathbb{F}_q$. Then $C^{\perp}$ is an $\mathbf{a}$-sequential code over $\mathbb{F}_q$.*

From this, it can be concluded that the Euclidean dual codes of polycyclic codes are not necessarily polycyclic codes. Therefore, Alahmadi defined the inner products of annihilator and annihilator dual codes in [1]. This section continues on this basis, studying annihilator dual codes of the $\mathbf{a}$-polycyclic code over $\mathbb{F}_q$. Let $\rho(x) \in \mathbb{F}_q[x]$, and denote by $\{\rho(x)\}_{\mathbf{a}} = \{r(x)|\rho(x) \equiv r(x) \bmod (x^n - \mathbf{a}(x)), \deg(r(x)) \leqslant n-1\}$.

Definition 3.1. *[1] Let $\alpha, \beta \in \mathbb{F}_q^n$, and let C be an $\mathbf{a}$-polycyclic code of length n over $\mathbb{F}_q$.*

(1) The annihilator product of $\alpha(x)$ and $\beta(x)$ is defined to be

$$\langle \alpha, \beta \rangle_{\mathbf{a}} = (\{\alpha(x)\beta(x)\}_{\mathbf{a}})(0).$$

(2) The annihilator dual code C° of an $\mathbf{a}$-polycyclic code C is defined to be

$$C^{\circ} = \{\beta \in \mathbb{F}_q^n | \langle \alpha, \beta \rangle_{\mathbf{a}} = 0, \forall \alpha \in C\}.$$

By [14, Lemma 2.4], the following conclusion holds.

Lemma 3.2. *[14] Let C be an $\mathbf{a}$-polycyclic code over $\mathbb{F}_q$. Then $C^{\circ} = \langle h(x) \rangle$, where $h(x)$ is the check polynomial of C.*

Definition 3.3. *[3] Let C be a code with parameter $[n, k, d]$ over $\mathbb{F}_q$. If $n = k + d - 1$ is satisfied, then C is called a maximum distance separable code, also known as an* MDS *code.*

As is well-known, MDS codes are good codes. This has prompted many scholars to study them. It is well-known that a linear code C is an MDS code if and only if $C^{\perp}$ is an MDS code (see [3, Theorem 2.3.1]). Naturally, let us consider whether we can get the annihilator dual code C° of C and still maintain the property of MDS when the $\mathbf{a}$-polycyclic code C is MDS.

The following Theorem 3.7 indicates that for $\mathbf{a} = (\lambda, 0, ..., 0)$-polycyclic codes, where $\lambda \in \mathbb{F}_q^*$, the annihilator dual codes C° of λ-constacyclic codes over $\mathbb{F}_q$ also maintain the MDS property. It is easy to obtain another type of good code from one type of good code, which is of great significance in theoretical research and practical applications.

Lemma 3.4. *[3] Let C be an $\mathbf{a}$-polycyclic code of length n and dimension k over $\mathbb{F}_q$, $G_{k\times n}$ and $H_{(n-k)\times n}$ are the generator matrix and check matrix of code C, respectively. Then, the following statements are equivalent:*

(1) C is an MDS code;

(2) Any k column of the generator matrix of C is $\mathbb{F}_q$-linearly independent;

(3) Any $n-k$ column of the check matrix of $H_{(n-k)\times n}$ is $\mathbb{F}_q$-linearly independent;

(4) $C^{\perp}$ is an MDS code.

The following two lemmas give the generator matrix of **a**-polycyclic codes and the check matrix of λ-constacyclic codes, respectively.

Lemma 3.5. *[8] Let C be an* **a***-polycyclic code of length n and dimension k over $\mathbb{F}_q$. $C = \langle g(x)\rangle$, where $g(x) = g_0 + g_1x + \cdots + g_{n-k}x^{n-k}$, $g_{n-k} \neq 0$. Then the generator matrix of C is*

$$G = \begin{pmatrix} g_0 & g_1 & \cdots & g_{n-k} & & & \\ & g_0 & g_1 & \cdots & g_{n-k} & & \\ & & \ddots & \ddots & \ddots & \ddots & \\ & & & g_0 & g_1 & \cdots & g_{n-k} \end{pmatrix}_{k\times n}.$$

Lemma 3.6. *[2] Let θ be an automorphism over $\mathbb{F}_q$. Let C be a θ-λ-constacyclic code of length n and dimension k over $\mathbb{F}_q$, $n|\mathrm{Ord}(\theta)$, $\lambda \in \mathbb{F}_q^*$, $\theta(\lambda) = \lambda$, $C = \langle g(x)\rangle$, the first coefficient of $g(x)$ is 1, and $g(x)$ is the right factor of $x^n - \lambda$. Set $h(x) = \frac{x^n-\lambda}{g(x)}$, $h(x) = h_0 + h_1x + ... + h_kx^k$, and $h_k = 1$. Then the check matrix of C is*

$$H' = \begin{pmatrix} h_k & \theta(h_{k-1}) & \cdots & \theta^k(h_0) & & & \\ & h_k & \theta^2(h_{k-1}) & \cdots & \theta^{k+1}(h_0) & & \\ & & \ddots & \ddots & \ddots & \ddots & \\ & & & h_k & \theta^{n-k}(h_{k-1}) & \cdots & \theta^{n-1}(h_0) \end{pmatrix}_{(n-k)\times n}.$$

Specifically, when $\theta = 1$, then C is a λ-constacyclic code of length n and dimension k over $\mathbb{F}_q$, and the check matrix of C is

$$H = \begin{pmatrix} h_k & h_{k-1} & \cdots & h_0 & & & \\ & h_k & h_{k-1} & \cdots & h_0 & & \\ & & \ddots & \ddots & \ddots & \ddots & \\ & & & h_k & h_{k-1} & \cdots & h_0 \end{pmatrix}_{(n-k)\times n}. \tag{3.1}$$

From this, we can obtain the following theorem.

Theorem 3.7. *Let C be a λ-constacyclic code over $\mathbb{F}_q$. Then C is an MDS code if and only if C° is an MDS code.*

Proof. Let C be a λ-constacyclic code of length n with dimension k over $\mathbb{F}_q$, and then by Lemma 3.6, the check matrix $H_{(n-k)\times n}$ is (3.1). Obviously C is a linear code over $\mathbb{F}_q$, by Lemma 3.4: C is an MDS code if and only if any $n-k$ column of the check matrix $H_{(n-k)\times n}$ of C is $\mathbb{F}_q$-linearly independent. By Lemma 3.2: $C^\circ = \langle h(x)\rangle$, where $h(x) = h_0 + h_1x + \cdots + h_kx^k$, and lemma 3.5 knows that the generator matrix of C° is

$$G^\circ = \begin{pmatrix} h_0 & h_1 & ... & h_k & & & \\ & h_0 & h_1 & ... & h_k & & \\ & & \ddots & \ddots & \ddots & \ddots & \\ & & & h_0 & h_1 & ... & h_k \end{pmatrix}_{(n-k)\times n}. \tag{3.2}$$

Compare (3.1) with (3.2), and it is easy to see $\lambda_1H_{i_1} + \cdots + \lambda_{n-k}H_{i_{n-k}} = 0$ if and only if $\lambda_1G^\circ_{n-i_1+1} + \cdots + \lambda_{n-k}G^\circ_{n-i_{n-k}+1} = 0$, where each $\lambda_j \in \mathbb{F}_q$, and H_j and G°_j are the j-th column vector of H and G°,

respectively. So any $n-k$ column of the check matrix (3.1) of C is $\mathbb{F}_q$-linearly independent, if and only if any $n-k$ column of the generator matrix (3.2) of C° is $\mathbb{F}_q$-linearly independent. Again by Lemma 3.4: Any $n-k$ column of the generator matrix (3.2) of C° is $\mathbb{F}_q$-linearly independent if and only if C° is an MDS code. Then, C is an MDS code if and only if C° is an MDS code.

□

In reference [8], the generator matrix of **a**-polycyclic codes of length n with demension k is given. But the check matrix is not given. The following Theorem 3.8 gives the check matrix of **a**-polycyclic codes.

Theorem 3.8. *Let C be an* **a***-polycyclic code of length n with dimension k over $\mathbb{F}_q$, $\deg(a(x)) \leqslant n-k-1$, $C = \langle g(x)\rangle$, and $g(x)$ and $h(x)$ are the generator polynomial and check polynomial of C, respectively, where $g(x) = g_0 + g_1x + \cdots + g_{n-k}x^{n-k}(g_{n-k} = 1, g_0 \neq 0)$, and $h(x) = h_0 + h_1x + \cdots + h_kx^k(h_k = 1, h_0 \neq 0)$. Then the check matrix $H = (h_{i,j})_{(n-k)\times n}$ of C satisfies*

$$h_{i,j} = \begin{cases} 0, & 1 \leqslant j < i; \\ h_{k+i-j}, & i \leqslant j \leqslant i+k; \\ \sum_{s=2k+i-j+1}^{k} a_{n+k+i-j-s}h_s, & i+k < j \leqslant n. \end{cases}$$

That is to say, the form of the check matrix H is as follows:

$$H = \begin{pmatrix} h_k & h_{k-1} & \ldots & h_0 & h_{n-k-1,n} & h_{n-k-2,n} & \cdots & h_{2,n} & h_{1,n} \\ & h_k & h_{k-1} & \cdots & h_0 & h_{n-k-1,n} & h_{n-k-2,n} & \cdots & h_{2,n} \\ & & & & & & \ddots & \ddots & \vdots \\ & & \ddots & \ddots & & \ddots & \ddots & \ddots & h_{n-k-2,n} \\ & & & \ddots & \ddots & & \ddots & \ddots & h_{n-k-1,n} \\ & & & & h_k & h_{k-1} & \cdots & \cdots & h_0 \end{pmatrix}_{(n-k)\times n}, \tag{3.3}$$

where $h_{i,j} = \sum_{s=2k+i-j+1}^{k} a_{n+k+i-j-s}h_s,\ i+k < j \leqslant n$.

Proof. Due to $\deg(\mathbf{a}(x)) \leqslant n-k-1$, we set $\mathbf{a}(x) = a_{n-k-1}x^{n-k-1} + a_{n-k-2}x^{n-k-2} + \cdots + a_1x + a_0$. For any $c(x) \in C = \langle g(x)\rangle$, there exists $s(x) \in \mathbb{F}_q[x]$, such that $c(x) = s(x)g(x)$. Since $h(x) = h_0 + h_1x + \cdots + h_kx^k(h_k = 1, h_0 \neq 0)$, we can obtain

$$c(x)h(x) = s(x)g(x)h(x) = s(x)(x^n - \mathbf{a}(x)) = 0 \bmod (x^n - \mathbf{a}(x)).$$

Let $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$, and then

$$\begin{aligned} 0 &= c(x)h(x) \\ &= (c_0 + c_1x + \cdots + c_{n-1}x^{n-1})(h_0 + h_1x + \cdots + h_kx^k) \\ &= t_0 + t_1x + \cdots + t_{n-1}x^{n-1} \bmod (x^n - \mathbf{a}(x)), \end{aligned}$$

where $t_0, t_1, \ldots, t_{n-1}$ are as follows:

$$
\begin{aligned}
t_0 &: c_0h_0 + c_{n-1}h_1 + c_{n-2}h_2 + \cdots + c_{n-k+2}h_{k-2} + c_{n-k+1}h_{k-1} + c_{n-k}h_k = 0,\\
t_1 &: c_1h_0 + c_0h_1 + c_{n-1}h_2 + \cdots + c_{n-k+3}h_{k-2} + c_{n-k+2}h_{k-1} + c_{n-k+1}h_k = 0,\\
&\vdots\\
t_{k-3} &: c_{k-3}h_0 + c_{k-4}h_1 + c_{k-5}h_2 + \cdots + c_{n-1}h_{k-2} + c_{n-2}h_{k-1} + c_{n-3}h_k = 0,\\
t_{k-2} &: c_{k-2}h_0 + c_{k-3}h_1 + c_{k-4}h_2 + \cdots + c_0h_{k-2} + c_{n-1}h_{k-1} + c_{n-2}h_k = 0,\\
t_{k-1} &: c_{k-1}h_0 + c_{k-2}h_1 + c_{k-3}h_2 + \cdots + c_1h_{k-2} + c_0h_{k-1} + c_{n-1}h_k = 0,\\
t_k &: c_kh_0 + c_{k-1}h_1 + c_{k-2}h_2 + \cdots + c_2h_{k-2} + c_1h_{k-1} + c_0h_k = 0,\\
t_{k+1} &: c_{k+1}h_0 + c_kh_1 + c_{k-1}h_2 + \cdots + c_3h_{k-2} + c_2h_{k-1} + c_1h_k = 0,\\
&\vdots\\
t_{n-1} &: c_{n-1}h_0 + c_{n-2}h_1 + c_{k-3}h_2 + \cdots + c_{n-k+1}h_{k-2} + c_{n-k}h_{k-1} + c_{n-k-1}h_k = 0.
\end{aligned}
$$

From this, it can be seen that the number of corresponding terms in $t_k, t_{k+1}, ..., t_n$ does not exceed n times, and the number of corresponding terms in $t_0, t_1, ..., t_{k-1}$ exceeds n times.

For items in t_{k-1}, where the number of times the corresponding item exceeds n is $c_{n-1}h_k$, and due to $R_n = \frac{\mathbb{F}_q[x]}{x^n - \mathbf{a}(x)}$ and $\mathbf{a}(x) = a_{n-k-1}x^{n-k-1} + a_{n-k-2}x^{n-k-2} + \cdots + a_1x + a_0$, therefore

$$
\begin{aligned}
c_{n-1}x^{n-1}h_kx^k &= c_{n-1}h_kx^nx^{k-1}\\
&= c_{n-1}h_k\mathbf{a}(x)x^{k-1}\\
&= c_{n-1}h_k(a_{n-k-1}x^{n-k-1} + a_{n-k-2}x^{n-k-2} + \cdots + a_1x + a_0)x^{k-1}\\
&= c_{n-1}h_ka_{n-k-1}x^{n-2} + c_{n-1}h_ka_{n-k-2}x^{n-3} + \cdots + c_{n-1}h_ka_1x^k + c_{n-1}h_ka_0x^{k-1}.
\end{aligned}
$$

It can be seen that after calculation, the term $c_{n-1}h_ka_{n-k-1}x^{n-2}$ obtained from $c_{n-1}x^{n-1}h_kx^k$ should correspond to t_{n-2}, the obtained term $c_{n-1}h_ka_{n-k-2}x^{n-3}$ should correspond to t_{n-3},..., and the obtained term $c_{n-1}h_ka_1x^k$ should correspond to t_k.

Next, calculate the corresponding terms in t_{k-2} that exceed n times: $c_{n-1}h_{k-1}$ and $c_{n-2}h_k$.

$$
\begin{aligned}
c_{n-1}x^{n-1}h_{k-1}x^{k-1} &= c_{n-1}h_{k-1}x^nx^{k-2}\\
&= c_{n-1}h_{k-1}a(x)x^{k-2}\\
&= c_{n-1}h_{k-1}(a_{n-k-1}x^{n-k-1} + a_{n-k-2}x^{n-k-2} + \cdots + a_1x + a_0)x^{k-2}\\
&= c_{n-1}h_{k-1}a_{n-k-1}x^{n-3} + c_{n-1}h_{k-1}a_{n-k-2}x^{n-4} + \cdots + c_{n-1}h_{k-1}a_1x^{k-1} + c_{n-1}h_{k-1}a_0x^{k-2}.
\end{aligned}
$$

It can be seen that after calculation, the term $c_{n-1}h_{k-1}a_{n-k-1}x^{n-3}$ obtained from $c_{n-1}x^{n-1}h_{k-1}x^{k-1}$ should correspond to t_{n-3}, the obtained term $c_{n-1}h_{k-1}a_{n-k-2}x^{n-4}$ should correspond to t_{n-4},..., and the obtained term $c_{n-1}h_ka_2x^k$ should correspond to t_k. Similarly, $c_{n-2}x^{n-2}h_kx^k$ can be calculated.

Calculate the corresponding terms in t_{k-3} that exceed n times: $c_{n-1}h_{k-2}$, $c_{n-2}h_{k-1}$ and $c_{n-3}h_k$. By following this method of calculation, we can obtain

$$\begin{pmatrix} h_k & h_{k-1} & \dots & h_0 & h_{n-k-1,n} & h_{n-k-2,n} & \cdots & h_{2,n} & h_{1,n} \\ & h_k & h_{k-1} & \cdots & h_0 & h_{n-k-1,n} & h_{n-k-2,n} & \cdots & h_{2,n} \\ & & & & & & \ddots & \ddots & \vdots \\ & & \ddots & \ddots & & \ddots & \ddots & \ddots & h_{n-k-2,n} \\ & & & \ddots & \ddots & & \ddots & \ddots & h_{n-k-1,n} \\ & & & & h_k & h_{k-1} & \cdots & & h_0 \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{pmatrix} = 0.$$

Therefore, we obtain the check matrix of code C in (3.3), where $h_{i,j} = \sum_{s=2k+i-j+1}^{k} a_{n+k+i-j-s} h_s,\ i + k < j \leqslant n$. □

4. Examples

In this section, some examples of polycyclic codes over $\mathbb{F}_2$ are given to illustrate the main results obtained in this paper.

Example 4.1. *Let $\mathbb{F}_2$ be a finite field with 2 elements. Consider* **a***-polycyclic codes of length $n = 12$ over $\mathbb{F}_2$, where* $\mathbf{a} = (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$. *Note that $x^n - \mathbf{a}(x) = x^{12} + x^8 + x^2 + 1$. The irreducible decomposition of $x^n - \mathbf{a}(x)$ on $\mathbb{F}_2$ is as follows*:

$$x^7 + x^6 + x^5 + x^4 + x^2 + 1 = (x + 1)^2(x^2 + x + 1)^2(x^3 + x + 1)^2.$$

For convenience, write $g_1 = x + 1,\ \ g_2 = x^2 + x + 1$, and $g_3 = x^3 + x + 1$. So there are a total of 27 **a***-polycyclic codes with a length of* 12 *over $\mathbb{F}_2$. Then the parameters of codes $C_1 = \langle g_1 g_2 g_3 \rangle$, $C_2 = \langle g_1 g_3^2 \rangle$, $C_3 = \langle g_1 g_2^2 g_3 \rangle$, and $C_4 = \langle g_1 g_2 g_3^2 \rangle$ are, respectively,* $[12, 6, 4]$, $[12, 5, 4]$, $[12, 4, 6]$, *and* $[12, 3, 6]$. *They are all optimal codes* (*see reference [5]*).

Example 4.2. *Calculated through Magma software, the following Table 1 provides all generator polynomials $g(x)$ of* $(1, 1, 0, 0, 0)$*-polycyclic codes of length* 5 *over $\mathbb{F}_2$.*

Table 1. Polycyclic codes of length 5.

Codes	*Parameters*	$g(x)$	C°
C_1	$[5, 0, 0]$	0	C_4
C_2	$[5, 3, 2]$	$x^2 + x + 1$	C_3
C_3	$[5, 2, 3]$	$x^3 + x^2 + 1$	C_2
C_4	$[5, 5, 1]$	1	C_1

It is clear that C_3 is an MDS code, reaching the Griesmer boundary.

5. Conclusions

In this article, we extend the properties of the idempotent generator of cyclic codes to polycyclic codes over the finite field $\mathbb{F}_q$. The check matrix of polycyclic codes is provided over $\mathbb{F}_q$. Specifically, it has been proven that the constacyclic code is an MDS code over $\mathbb{F}_q$ if and only if its annihilator dual code is also an MDS code. Finally, some examples of good codes are provided.

Acknowledgments

The author was supported by the National Natural Science Foundation of China (No.12201361) and the Doctoral Research Initiation Fund of Shandong University of Technology (No. 423002).

Conflict of interest

The author declares that he has no conflict of interest.

References

1. A. Alahmadi, A. Dougherty, A. Leroy, P. SolÉ, On the duality and the direction of polycyclic codes, *Adv. Math. Commun.,* **12** (2016), 723–739.
2. D. Boucher, F. Ulmer, Coding with skew polynomial rings, *J. Symb. Comput.,* **44** (2009), 1644–1656. https://doi.org/10.1016/j.jsc.2007.11.008
3. K. Q. Feng, *Algebraic theory of error-correcting codes*, Beijing: Tsinghua University Press, 2005.
4. E. M. Gabidulin, Rank q-cyclic and pseudo-q-cyclic codes, *IEEE Int. Sym. Inform. Theory (ISIT2009)*, 2009, 2799–2802. https://doi.org/10.1109/ISIT.2009.5205787
5. M. Grassl, Bounds on the minimum distance of linear codes and quantum codes. Available form: `http://www.codetables.de`.
6. W. C. Huffman, V. Pless, *Fundamentals of error-correcting codes*, New York: Cambridge University Press, 2003. https://doi.org/10.1017/CBO9780511807077
7. S. Li, M. Xiong, G. Ge, Pseudo-cyclic codes and the construction of quantum MDS Codes, *IEEE T. Inform. Theory*, **62** (2016), 1703–1710. https://doi.org/10.1109/TIT.2016.2535180
8. S. R. L. Permouth, B. R. P. Avila, S. Szabo, Dual generalizations of the concept of cyclicity of codes, *Adv. Math. Commun.,* **3** (2009) 227–234. https://doi.org/10.3934/amc.2009.3.227
9. S. R. L. Permouth, H. Özadam, F. Özbudak, S. Szabo, Polycyclic codes over Galois rings with applications to repeated-root constacyclic codes, *Finite Fields Th. Appl.,* **19** (2013), 16–38. https://doi.org/10.1016/j.ffa.2012.10.002
10. T. Maruta, Optimal pseudo-cyclic codes and caps in $PG(3, q)$, *Geometriae Dedicata,* **54** (1995), 263–266. https://doi.org/10.1007/BF01265342
11. E. M. Moro, A. Fotue, T. Blackford, On polycyclic codes over a finite chain ring, *Adv. Math. Commun.,* **14** (2020), 445–466. https://doi.org/10.3934/amc.2020028
12. J. P. Pedersen, C. Dahl, Classification of pseudo-cyclic MDS codes, *IEEE T. Inform. Theory,* **37** (1991), 365–370. https://doi.org/10.1109/18.75254
13. W. W. Peterson, E. J. Weldon, *Error correcting codes*, Cambridge: MIT Press, 1972.
14. W. Qi, On the polycyclic codes over $\mathbb{F}_q + u\mathbb{F}_q$, *Adv. Math. Commun.,* **18** (2024), 661–673. https://doi.org/10.3934/amc.2022015
15. M. J. Shi, X. X. Li, Z. Sepasdar, P. Solé, Polycyclic codes as invariant subspaces, *Finite Fields Th. App.,* **68** (2020), 101760. https://doi.org/10.1016/j.ffa.2020.101760