

Polycyclic codes over R

Gowdhaman Karthick

Presidency University, Bangalore, Karnataka-560064, India
karthygowtham@gmail.com

Received: 28 July 2023; Accepted: 16 November 2023
Published Online: 28 November 2023

Abstract: In this paper, we discuss the structure of polycyclic codes over the ring $R = \mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q; u^2 = \alpha u, v^2 = v$ and $uv = vu = 0$, where α is an unit element in R . We introduce annihilator self-dual codes, annihilator self-orthogonal codes and annihilator LCD codes over R . Using a Gray map, we define a one to one correspondence between R and \mathbb{F}_q and construct quasi polycyclic codes over the \mathbb{F}_q .

Keywords: semi-simple ring, polycyclic codes, hamming distances, gray maps, annihilator dual codes.

AMS Subject classification: 05C50; 05C09; 05C92

1. Introduction

An interesting subtype of linear codes are polycyclic codes of length n over a finite field \mathbb{F}_q with q elements which are described by ideals of a polynomial rings $\mathbb{F}_q[x]/\langle f(x) \rangle$. In 2009, López-Permouth et al. [3] studied polycyclic codes and sequential codes, and showed that a linear code is polycyclic if and only if its Euclidean dual code is sequential which is not always polycyclic. In 2016, Alahmadi et al. [1] introduced the annihilator dual codes over \mathbb{F}_q and showed that the annihilator dual codes of polycyclic codes over \mathbb{F}_q are also polycyclic. In 2022, Wei Qi study the polycyclic codes over $\mathbb{F}_q + u\mathbb{F}_q$ with $u^2 = u$ and have constructed the annihilator self-dual codes, annihilator self-orthogonal codes and annihilator LCD codes. This motivated us to do the following works.

In this paper, we study Polycyclic codes and Sequential codes over the ring $R = \mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q; u^2 = \alpha u, v^2 = v$ and $uv = vu = 0$. We have introduced annihilator self-dual codes, annihilator self-orthogonal codes and annihilator LCD codes over R . Using a Gray map, we have defined a one to one correspondance between $\{1, R$ and $\mathbb{F}_q^3\}$ and a few codes are constructed.

2. Preliminaries

Let \mathbb{F}_q be a finite field of order q with characteristic p , then we define a ring $R = \mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q$ with $u^2 = \alpha u, v^2 = v, uv = vu = 0$ where α is an unit element in R . The ring R is a semi-local and Frobenius ring. A linear code C is a R -module. C^\perp is the Euclidean dual of C . Let $e_1 = \frac{u}{\alpha}$, $e_2 = v$ and $e_3 = (1 - \frac{u}{\alpha} - v)$. Then, we have $e_i^2 = e_i, e_i e_j = 0$ and $\sum_{i=1}^3 e_i = 1$ where $i = 1, 2, 3$ and $i \neq j$. By using decomposition theorem of rings, we have $R = \bigoplus_{i=1}^3 e_i R \cong \bigoplus_{i=1}^3 e_i \mathbb{F}_q$. Therefore, any element in R can be uniquely expressed as $r = \sum_{i=1}^3 e_i r_i$ where $r_i \in \mathbb{F}_q$.

Let C be a linear code of length n over R and $C_i = \{r_i \in \mathbb{F}_q^n \mid \sum_{i=1}^3 e_i r_i \in C\}$ for some $r_j \in \mathbb{F}_q^n$ where $j \neq i$. Then C_i is a linear code of length n over \mathbb{F}_q for $1 \leq i \leq 3$. Hence, C can be expressed as $C = \bigoplus_{i=1}^3 e_i C_i$.

Definition 1. Let C be a linear code over R and let $a = (a_0, a_1, \dots, a_{n-1}) \in R^n$ with the condition that a_0 as a unit element of R

- then C is a *a-polycyclic code* if it satisfies the right polycyclic shift operator given by

$$\sigma_a(c_0, c_1, \dots, c_{n-1}) = (0, c_1, c_2, \dots, c_{n-2}) + c_{n-1}(a_0, a_1, \dots, a_{n-1})$$

- then C is a *a-sequential code* if it satisfies the right sequential shift operator given by

$$\tau_a(c_0, c_1, \dots, c_{n-1}) = (c_1, c_2, \dots, c_{n-1}, c_0 a_0 + c_1 a_1 + \dots + c_{n-1} a_{n-1}).$$

Hereafter, we denote $R[x]/\langle x^n - a(x) \rangle$ as R^a . Then the map $\phi : R^n \longrightarrow R^a$ defined by

$$(c_0, c_1, c_2, \dots, c_{n-1}) \mapsto c(x) = c_0 + c_1 x + \dots + c_{n-1} x^{n-1},$$

is a module isomorphism and we have the following result.

Theorem 1. Let C be a polycyclic code over the ring R , then the corresponding image sets ϕ is an $R[x]$ -module over R^a .

Definition 2 ([4]). Let C be a polycyclic code of length n .

1. Let $\alpha(x), \beta(x) \in R^a$, then the annihilator product of $\alpha(x)$ and $\beta(x)$ is defined as

$$\langle \alpha(x), \beta(x) \rangle_a = r(0)$$

where $\alpha(x)\beta(x) \equiv r(x) \pmod{x^n - a(x)}$ and $\deg(r(x)) \leq n - 1$.

2. The annihilator dual code C' of an a-polycyclic code C is defined to be

$$C' = \{\beta(x) \in R^a \mid \langle \alpha(x), \beta(x) \rangle_a = r(0) = 0 \text{ for all } \alpha(x) \in C\}.$$

3. The a -polycyclic code C is said to be an *annihilator self-orthogonal code* (resp., *annihilator self-dual code*, *annihilator LCD code*) provided that $C \subseteq C'$ (resp., $C = C'$, $C \cap C' = \{0\}$).
4. The annihilator of C is

$$\text{Ann}(C) = \{\beta(x) \in R_a \mid \alpha(x)\beta(x) = 0 \in R^a \text{ for all } \alpha(x) \in C\}.$$

Theorem 2. *[[4]] Let C be an a -polycyclic code of length n over \mathbb{F}_q . Let $g(x)$ be the generator polynomial and $h(x)$ the check polynomial of C , then $C' = \langle h(x) \rangle$.*

Lemma 1 ([1]). *Let $a = (a_0, a_1, \dots, a_{n-1}) \in \mathbb{F}_q^n$ with $a_0 \neq 0$, C be an a -polycyclic code of length n over \mathbb{F}_q , then $\alpha(x)\beta(x)$ is non-degenerate, and thus $C' = \text{Ann}(C)$.*

Lemma 2 ([1]). *Let C_1 and C_2 be a -polycyclic codes over \mathbb{F}_q , g_1, g_2 their generator polynomials, respectively, then $C_1 \subseteq C_2$ if and only if $g_2|g_1$.*

Lemma 3 ([1]). *Let C be an a -polycyclic code over \mathbb{F}_q , then C is an annihilator self-orthogonal code if and only if $h(x)|g(x)$ where $g(x)$ and $h(x)$ are the generator polynomial and check polynomial of C , respectively.*

Lemma 4 ([1]). *Let C be an a -polycyclic code over \mathbb{F}_q , then C is an annihilator LCD code if and only if $\gcd(g(x), h(x)) = 1$ where $g(x)$ and $h(x)$ are the generator polynomial and check polynomial of C , respectively.*

3. Codes over the ring R

A unique representation of an element in R is defined as $r = r_1e_1 + r_2e_2 + r_3e_3$. Each coordinate a_j in $a = (a_0, a_1, \dots, a_{n-1})$ can be written as $a_j = a_j^1e_1 + a_j^2e_2 + a_j^3e_3$, $1 \leq j \leq n-1$ in a unique way and c_j in $c = (c_0, c_1, \dots, c_{n-1}) \in C$ as $c_j = c_j^1e_1 + c_j^2e_2 + c_j^3e_3$, $1 \leq j \leq n-1$. On applying the polycyclic operator,

$$\begin{aligned} \sigma_a(c) &= (0, c_1, c_2, \dots, c_{n-2}) + c_{n-1}(a_0, a_1, \dots, a_{n-1}) \\ &= (0, c_1^1e_1 + c_1^2e_2 + c_1^3e_3, c_2^1e_1 + c_2^2e_2 + c_2^3e_3, \dots, c_{n-2}^1e_1 + c_{n-2}^2e_2 + c_{n-2}^3e_3) \\ &\quad + (c_{n-1}^1e_1 + c_{n-1}^2e_2 + c_{n-1}^3e_3)(a_0^1e_1 + a_0^2e_2 + a_0^3e_3, a_1^1e_1 + a_1^2e_2 + a_1^3e_3, \dots, \\ &\quad a_{n-1}^1e_1 + a_{n-1}^2e_2 + a_{n-1}^3e_3) \\ &= (0, c_1^1e_1, e_1c_2^1, \dots, e_1c_{n-2}^1) + e_1c_{n-1}^1(a_0^1e_1, a_1^1e_1, \dots, a_{n-1}^1e_1) \\ &\quad + (0, c_1^2e_2, e_2c_2^2, \dots, e_2c_{n-2}^2) + e_2c_{n-1}^2(a_0^2e_2, a_1^2e_2, \dots, a_{n-1}^2e_2) \\ &\quad + (0, c_1^3e_3, e_3c_2^3, \dots, e_3c_{n-2}^3) + e_3c_{n-1}^3(a_0^3e_3, a_1^3e_3, \dots, a_{n-1}^3e_3) \\ &= e_1((0, c_1^1, c_2^1, \dots, c_{n-2}^1) + c_{n-1}^1(a_0^1, a_1^1, \dots, a_{n-1}^1)) \\ &\quad + e_2((0, c_1^2, c_2^2, \dots, c_{n-2}^2) + c_{n-1}^2(a_0^2, a_1^2, \dots, a_{n-1}^2)) \\ &\quad + e_3((0, c_1^3, c_2^3, \dots, c_{n-2}^3) + c_{n-1}^3(a_0^3, a_1^3, \dots, a_{n-1}^3)) \\ &= e_1(\sigma_{a_1}(c^1)) + e_2(\sigma_{a_2}(c^2)) + e_3(\sigma_{a_3}(c^3)). \end{aligned}$$

Thus, $\sigma_{a_1}(c^1) \in C_1$, $\sigma_{a_2}(c^2) \in C_2$ and $\sigma_{a_3}(c^3) \in C_3$ and vice versa. Thus, we have the following Theorem.

Theorem 3. *Let C be a linear code over R of length n , then C is an a -polycyclic code of length n if and only if every C_i is an a_i -polycyclic codes over \mathbb{F}_q ($1 \leq i \leq 3$).*

Theorem 4. *Let C be a linear code of length n over R , then C is a -sequential over R if and only if every C_i is a_i -sequential over \mathbb{F}_q .*

Proof. Proof is similar to that of Theorem 3. □

Lemma 5. *Let C be an a -polycyclic code of length n over \mathbb{F}_q , then C is a principal ideal $\langle g(x) \rangle$ of $\mathbb{F}_q[x]/\langle x^n - a(x) \rangle$ generated by some monic polynomial and a divisor of $x^n - a(x)$. In this case, $g(x)$ is said to be a generator polynomial of C .*

Theorem 5. *Let $C = \bigoplus_{i=1}^3 e_i C_i$ be a a -polycyclic code of length n over R , then $C = \langle g(x) = e_1 g_1(x) + e_2 g_2(x) + e_3 g_3(x) \rangle$ of $R[x]/\langle x^n - a(x) \rangle$ where $g_i(x) = \langle C_i \rangle, g_i(x) | x^n - a_i(x), 1 \leq i \leq 3$ over \mathbb{F}_q .*

Proof. Let $C = \bigoplus_{i=1}^3 e_i C_i$ be an a -polycyclic code over R . Let $c(x) \in C = \bigoplus_{i=1}^3 e_i C_i$, then there exists $p_i(x) \in \mathbb{F}_q[x]/\langle x^n - a_i(x) \rangle$ such that

$$\sum_{i=1}^3 e_i p_i(x) g_i(x) = c(x)$$

$$\left(\sum_{i=1}^3 e_i p_i(x) \right) \left(\sum_{i=1}^3 e_i g_i(x) \right) = c(x)$$

Then $c(x) \in \langle g(x) \rangle, \langle g(x) \rangle \subseteq \bigoplus_{i=1}^3 e_i C_i$.

Let $C = \bigoplus_{i=1}^3 e_i C_i$ be a a -polycyclic code over R , then by Theorem 3, C_i is a_i -polycyclic code of length n over \mathbb{F}_q . So by Lemma 5, we have $g_i(x) = \langle C_i \rangle$ and $g_i(x) | x^n - a_i(x)$. Then there exists $h_i(x) \in R[x]/\langle x^n - a_i(x) \rangle$ such that $g_i(x) h_i(x) = x^n - a_i(x)$. Therefore $e_i g_i(x) h_i(x) = e_i (x^n - a_i(x))$ and hence

$$\sum_{i=1}^3 e_i g_i(x) h_i(x) = x^n - a(x)$$

$$\left(\sum_{i=1}^3 e_i g_i(x) \right) \left(\sum_{i=1}^3 e_i h_i(x) \right) = x^n - a(x).$$

Thus, we have $C = \langle \sum_{i=1}^3 e_i g_i(x) h_i(x) \rangle$. □

Theorem 6 ([2]). *If $f(0) \neq 0$, then the bilinear form $\langle \cdot, \cdot \rangle$ is non degenerate.*

Theorem 7. *Let $\alpha(x), \beta(x) \in R^a$. Then $\langle \alpha(x), \beta(x) \rangle$ is a non-degenerate symmetric R -bilinear form.*

Proof. For any $\alpha, \beta, \gamma \in R^n$, $k \in R$, $\langle k(\alpha + \beta), \gamma \rangle = r(0)$,

$$\begin{aligned} \text{where } [k(\alpha + \beta)\gamma](x) &\equiv r(x) \pmod{x^n - a(x)} \\ k[\alpha(x)\gamma(x)] + k[\beta(x)\gamma(x)] &\equiv r(x) \pmod{x^n - a(x)} \end{aligned}$$

on the other hand,

$$\begin{aligned} \langle k\alpha(x), \gamma(x) \rangle &= r_1(0) \text{ where } k[\alpha(x)\gamma(x)] \equiv r_1(x) \pmod{x^n - a(x)}, \\ \langle k\beta(x), \gamma(x) \rangle &= r_1(x) \text{ where } k[\beta(x)\gamma(x)] \equiv r_2(x) \pmod{x^n - a(x)}, \end{aligned}$$

using the property compatibility with addition, we have $r(x) = r_1(x) + r_2(x)$. Thus, $\langle k(\alpha + \beta), \gamma \rangle = k\langle \alpha, \gamma \rangle + k\langle \beta, \gamma \rangle$ is bilinear. Since the ring R is commutative, we have $\langle \beta, \gamma \rangle = \langle \gamma, \beta \rangle$. To show $\langle \cdot, \cdot \rangle$ is non-degenerate, it is enough to show that the Radicals of R is $\{0\}$. Suppose not, that is, there exists $\beta \neq 0 \in R(R^n)$ such that $\langle \alpha, \beta \rangle = 0$ for all $\alpha \in R$. Since $\alpha, \beta \in R^n$, it can be uniquely represented by $\alpha = e_1\alpha_1 + e_2\alpha_2 + e_3\alpha_3$, $\beta = e_1\beta_1 + e_2\beta_2 + e_3\beta_3$. Therefore, by using the bilinear property, one can write $\langle \alpha, \beta \rangle = 0$ as

$$\langle \alpha, \beta \rangle = \sum_{i=1}^3 e_i \langle \alpha_i, \beta_i \rangle = 0,$$

which contradicts 6. Thus, $\langle \cdot, \cdot \rangle_a$ is a non-degenerate symmetric R -bilinear form. \square

Theorem 8. Let C be an a -polycyclic code over S and let $\epsilon_1 = (1, 0, \dots, 0)$, $\epsilon_2 = (0, 1, \dots, 0)$, \dots , $\epsilon_n = (0, 0, \dots, 1)$ and $A = ((\epsilon_i, \epsilon_j)_a)_{1 \leq i, j \leq n}$. Let $CA = \{cA \mid c \in C\}$. Then $C' = (CA)^\perp$. Consequently, $(C')' = C$.

Proof. Note that $\langle u, v \rangle_a = uAv^t = \langle u, Av \rangle_a$. Thus $C' = (CA)^\perp$. Using the equality, $C' = (CA)^\perp$. Since A is invertible, it follows that $(C')' = (C'A)^\perp = (C')^\perp A^{-1} = ((CA)^\perp)^\perp A^{-1} = C$. \square

Theorem 9. Let C be a polycyclic code of length n . Then $C' = e_1C'_1 \oplus e_2C'_2 \oplus e_3C'_3$.

Proof. Since every element in $d \in R$ can be represented as $d = e_1d_1 + e_2d_2 + e_3d_3$, it can be written as a matrix A uniquely as $A = e_1A_{e_1} + e_2A_{e_2} + e_3A_{e_3}$ where every A_{e_i} is a matrix over \mathbb{F}_q . Consider

$$\begin{aligned} (C') &= (e_1C_1 \oplus e_2C_2 \oplus e_3C_3)^\perp (e_1A_{e_1} + e_2A_{e_2} + e_3A_{e_3})^{-1} \\ &= (e_1C_1A_{e_1} \oplus e_2C_2A_{e_2} \oplus e_3C_3A_{e_3}) \\ &= e_1C'_1 \oplus e_2C'_2 \oplus e_3C'_3 \end{aligned}$$

Thus, $C' = e_1C'_1 \oplus e_2C'_2 \oplus e_3C'_3$. \square

Theorem 10. *Let C be a linear code over R . Then C is a -polycyclic if and only if C' is a -polycyclic.*

Proof. Since C is a polycyclic code over R , by Theorem 3, every C_i is a polycyclic codes over \mathbb{F}_q . Then, by [[2], Proposition 3], we have C'_i as polycyclic code over \mathbb{F}_q and again by Theorem 3 it is obvious that C' is a polycyclic codes. \square

Theorem 11. *Let C be a linear code of length n over R . Then C is an a -polycyclic code over R if and only if C^\perp is an a -sequential code over R .*

Proof. By Theorem 3 if C is an a -polycyclic codes then every C_i is a a_i -polycyclic code over \mathbb{F}_q . By Theorem[3.2] in [3], every C_i is a a_i -polycyclic code over \mathbb{F}_q if and only if every C_i^\perp is a a_i - sequential code over \mathbb{F}_q . Thus by from Theorem4 C^\perp is an a -sequential code. \square

Theorem 12. *Let C be an a -polycyclic code over R generated by $g(x)$. Suppose $h(x)$ is a check polynomial of C . Then C' is an a -polycyclic code generated by $h(x)$.*

Proof. It follows from the proof of Theorems 10 and 5. \square

4. Gray map

In this section, we define a Gray map from R to \mathbb{F}_q^3 . We have shown that Gray map enjoy certain properties. Let $x = x_1e_1 + x_2e_2 + x_3e_3 \in R$, then we define $\phi : R \rightarrow \mathbb{F}_q^3$ by

$$\phi(x_1e_1 + x_2e_2 + x_3e_3) = (x_1, x_2, x_3).$$

It can be easily extended to any length n . Define $\Phi : R^n \mapsto \mathbb{F}_q^{3n}$ by

$$\text{by } \Phi(c_0, c_1, \dots, c_{n-1}) = (\phi(c_0), \phi(c_1), \dots, \phi(c_{n-1})).$$

The Gray weight w_G of $c \in R^n$ is defined by $w_G(c) = \sum_{i=0}^{n-1} w_G(c_i) = \sum_{i=0}^{n-1} w_H(\phi(c_i))$, where w_H is the Hamming weight in \mathbb{F}_q , and the distance between two codewords $c, d \in C$ is $d_G(c, d) = w_G(c - d)$. The minimum Gray distance of C is

$$d_G(C) = \min\{w_G(c) \mid 0 \neq c \in C\}.$$

For any two elements $c, d \in R^n$, $d_G(c, d) = w_G(c - d) = w_H(\Phi(c - d)) = w_H(\Phi(c) - \Phi(d)) = d_H(\Phi(c), \Phi(d))$. Hence, Φ is a linear distance preserving map from (R^n, d_G) to (\mathbb{F}_q^{3n}, d_H) .

Theorem 13. Let $C = \bigoplus_{i=1}^3 e_i C_i$ be a linear code with parameter $[n, k, d_G]$, then $\Phi(C)$ is a linear code over \mathbb{F}_q^{3n} with the parameter $[3n, k, d_H]$.

Definition 3. Let C be a linear code and let $a = a^1 e_1 + a^2 e_2 + a^3 e_3 \in R$, then C is called a -quasicyclic code of index 3 over \mathbb{F}_q if it satisfies the shift operator given by

$$\begin{aligned} \tau^3(x_0, x_1, \dots, x_{n-1}, y_0, y_1, \dots, y_{n-1}, z_0, z_1, \dots, z_{n-1}) = & ((0, x_1, x_2, \dots, x_{n-2}) + x_{n-1}(a_0^1, a_1^1, \dots, a_{n-1}^1), \\ & (0, y_1, y_2, \dots, y_{n-2}) + y_{n-1}(a_0^2, a_1^2, \dots, a_{n-1}^2), \\ & (0, z_1, z_2, \dots, z_{n-2}) + z_{n-1}(a_0^3, a_1^3, \dots, a_{n-1}^3)). \end{aligned}$$

Theorem 14. Let C be a linear code over R of length $3n$. Then C is an a -polycyclic code if and only if $\Phi(C)$ is a -quasi cyclic code over \mathbb{F}_q , ($\tau^3(\Phi(c)) = \Phi(\sigma_a(c))$).

Proof. Let C be an a -polycyclic code of length n , then it satisfies the cyclic shift operator for every $c \in C$,

$$\begin{aligned} \sigma_a(c) &= (0, c_1, c_2, \dots, c_{n-2}) + c_{n-1}(a_0, a_1, \dots, a_{n-1}) \\ &= (0, c_1^1 e_1 + c_1^2 e_2 + c_1^3 e_3, c_2^1 e_1 + c_2^2 e_2 + c_2^3 e_3, \dots, c_{n-2}^1 e_1 + c_{n-2}^2 e_2 + c_{n-2}^3 e_3) \\ &\quad + (c_{n-1}^1 e_1 + c_{n-1}^2 e_2 + c_{n-1}^3 e_3)(a_0^1 e_1 + a_0^2 e_2 + a_0^3 e_3, a_1^1 e_1 + a_1^2 e_2 + a_1^3 e_3, \dots, \\ &\quad a_{n-1}^1 e_1 + a_{n-1}^2 e_2 + a_{n-1}^3 e_3) \\ &= (0, c_1^1 e_1, e_1 c_2^1, \dots, e_1 c_{n-2}^1) + e_1 c_{n-1}^1 (a_0^1 e_1, a_1^1 e_1, \dots, a_{n-1}^1 e_1) \\ &\quad + (0, c_1^2 e_2, e_2 c_2^2, \dots, e_2 c_{n-2}^2) + e_2 c_{n-1}^2 (a_0^2 e_2, a_1^2 e_2, \dots, a_{n-1}^2 e_2) \\ &\quad + (0, c_1^3 e_3, e_3 c_2^3, \dots, e_3 c_{n-2}^3) + e_3 c_{n-1}^3 (a_0^3 e_3, a_1^3 e_3, \dots, a_{n-1}^3 e_3) \\ &= e_1((0, c_1^1, c_2^1, \dots, c_{n-2}^1) + c_{n-1}^1(a_0^1, a_1^1, \dots, a_{n-1}^1)) \\ &\quad + e_2((0, c_1^2, c_2^2, \dots, c_{n-2}^2) + c_{n-1}^2(a_0^2, a_1^2, \dots, a_{n-1}^2)) \\ &\quad + e_3((0, c_1^3, c_2^3, \dots, c_{n-2}^3) + c_{n-1}^3(a_0^3, a_1^3, \dots, a_{n-1}^3)) \\ \Phi(\sigma_a(c)) &= ((0, c_1^1, c_2^1, \dots, c_{n-2}^1) + c_{n-1}^1(a_0^1, a_1^1, \dots, a_{n-1}^1), \\ &\quad (0, c_1^2, c_2^2, \dots, c_{n-2}^2) + c_{n-1}^2(a_0^2, a_1^2, \dots, a_{n-1}^2), \\ &\quad (0, c_1^3, c_2^3, \dots, c_{n-2}^3) + c_{n-1}^3(a_0^3, a_1^3, \dots, a_{n-1}^3)). \end{aligned}$$

Let $c' \in \Phi(C)$, then there exists an $c \in C$ such that $\Phi(c) = c'$. Consider

$$\begin{aligned} \Phi(c) &= (c_0^1, c_1^1, \dots, c_{n-1}^1, c_0^2, c_1^2, \dots, c_{n-1}^2, c_0^3, c_1^3, \dots, c_{n-1}^3) \\ \tau^3(\Phi(c)) &= ((0, c_1^1, c_2^1, \dots, c_{n-2}^1) + c_{n-1}^1(a_0^1, a_1^1, \dots, a_{n-1}^1), \\ &\quad (0, c_1^2, c_2^2, \dots, c_{n-2}^2) + c_{n-1}^2(a_0^2, a_1^2, \dots, a_{n-1}^2), \\ &\quad (0, c_1^3, c_2^3, \dots, c_{n-2}^3) + c_{n-1}^3(a_0^3, a_1^3, \dots, a_{n-1}^3)) \end{aligned}$$

$$\text{Hence, } \tau^3(\Phi(c)) = \Phi(\sigma_a(c)).$$

□

Definition 4. Let C be an a -quasi polycyclic code of length n over \mathbb{F}_q .

1. Let $\alpha_{a_i}(x), \beta_{a_i}(x) \in \mathbb{F}_q^{a_i}$, then the annihilator product is defined as

$$\sum_{i=1}^3 \langle \alpha_{a_i}(x), \beta_{a_i}(x) \rangle_{a_i} = \sum_{i=1}^3 r_{a_i}(0)$$

where $\alpha_{a_i}(x), \beta_{a_i}(x) \equiv r_{a_i}(x) \pmod{x^n - a_i(x)}$ and $\deg(r_{a_i}(x)) \leq n - 1$

2. The annihilator dual code C' of an a -quasi polycyclic code C is defined to be

$$C' = \{(\beta_{a_1}(x), \beta_{a_2}(x), \beta_{a_3}(x)) \in (\mathbb{F}_q^{a_1}, \mathbb{F}_q^{a_2}, \mathbb{F}_q^{a_3}) \mid \sum_{i=1}^3 \langle \alpha_{a_i}(x), \beta_{a_i}(x) \rangle_{a_i} = \sum_{i=1}^3 r_{a_i}(0) = 0 \text{ for all } \alpha_{a_i}(x) \in C_i\}$$

Theorem 15. *Let C be a polycyclic code. If C' is annihilator dual of C , then $\Phi(C')$ is annihilator dual for an a -quasi cyclic code $\Phi(C)$.*

Proof. Let $\beta(x) \in C'$, then for every $\alpha(x) \in C$, $\langle \alpha(x), \beta(x) \rangle_a = r(0) = 0$. Since $\alpha(x), \beta(x)$ is an element of R^a , $\alpha(x) = \sum_{i=1}^3 e_i \alpha_{a_i}(x)$, $\beta(x) = \sum_{i=1}^3 e_i \beta_{a_i}(x)$.

$$\langle \sum_{i=1}^3 e_i \alpha_{a_i}(x), \sum_{i=1}^3 e_i \beta_{a_i}(x) \rangle_a = \sum_{i=1}^3 e_i \langle \alpha_{a_i}(x), \beta_{a_i}(x) \rangle_a = \sum_{i=1}^3 e_i r_{a_i}(0) = 0$$

where $\alpha_{a_i}(x), \beta_{a_i}(x) \equiv r_{a_i}(x) \pmod{x^n - a_i(x)}$ which shows that $r_{a_i}(0) = 0$ for all i . To show $\Phi(\beta(x)) = (\beta_{a_1}(x), \beta_{a_2}(x), \beta_{a_3}(x)) \in \Phi(C')$, let $\alpha_{a_i}(x) \in C_i$ then

$$\sum_{i=1}^3 \langle \alpha_{a_i}(x), \beta_{a_i}(x) \rangle_{a_i} = \sum_{i=1}^3 r_{a_i}(0) = 0.$$

Thus, $\Phi(\beta(x)) = (\beta_{a_1}(x), \beta_{a_2}(x), \beta_{a_3}(x)) \in \Phi(C')$. □

Theorem 16. *Let C be an a -polycyclic code over R , then*

- C is annihilator self-orthogonal if and only if both C_{a_1}, C_{a_2} and C_{a_3} are annihilator self-orthogonal over \mathbb{F}_q .
- C is annihilator self-dual if and only if both C_{a_1}, C_{a_2} and C_{a_3} are annihilator self-dual over \mathbb{F}_q .
- C is annihilator LCD if and only if C_{a_1}, C_{a_2} and C_{a_3} are annihilator LCD over \mathbb{F}_q .

Proof. The proof of this similar to that of Theorem 15. □

Example 1. Let $a(x) = 4x^3 + 1$, then $R^a = \frac{\mathbb{F}_5[x]}{\langle x^6 - a(x) \rangle}$. Let $C = \langle g_{a_i}(x) \rangle = \langle x^2 + 4x + 4 \rangle$, then $C' = \langle h_{a_i}(x) \rangle = \langle (x^2 + 3x + 4)^2 \rangle$. Since $(g_{a_i}(x), h_{a_i}(x)) = 1$, there exists a LCD annihilator code of parameter $[18, 12, 2]_5$.

Example 2. Let $a(x) = -(x^4 + x^6 - 1)$, then $R^a = \frac{\mathbb{F}_3[x]}{\langle x^8 - a(x) \rangle}$. Let $C = \langle g_{a_i}(x) \rangle = \langle x^4 + 2x^2 + 2 \rangle$, then $C' = \langle h_{a_i}(x) \rangle = \langle (x^2 + 1)^2 \rangle$. Since $(g_{a_i}(x), h_{a_i}(x)) = 1$, there exists a LCD annihilator code of parameter $[24, 15, 3]_3$.

Example 3. Let $a(x) = -(x^4 - 1)$, then $R^a = \frac{\mathbb{F}_3[x]}{\langle x^6 - a(x) \rangle}$. Let $C = \langle g_{a_i}(x) \rangle = \langle x^3 + 2x^2 + x + 1 \rangle$, then $(g_{a_i}(x), h_{a_i}(x)) = 1$ and hence there exists a LCD annihilator code of parameter $[18, 9, 3]_3$.

Acknowledgements. The author are thankful to Prof. Gutman and the anonymous referees for their careful reading and the suggestions that improved the article.

Conflict of interest. The author declares no conflict of interest.

Data Availability. Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

References

- [1] A. Alahmadi, S.T. Dougherty, A. Leroy, and P. Solé, *On the duality and the direction of polycyclic codes*, Adv. Math. Commun. **10** (2016), no. 4, 921–929
<https://doi.org/10.3934/amc.2016049>.
- [2] A. Fotue-Tabue, E. Martínez-Moro, and J.T. Blackford, *On polycyclic codes over a finite chain ring.*, Adv. Math. Commun. **14** (2020), no. 3, 455–466
<https://doi.org/10.3934/amc.2020028>.
- [3] S.R. López-Permouth, B.R. Parra-Avila, and S. Szabo, *Dual generalizations of the concept of cyclicity of codes.*, Adv. Math. Commun. **3** (2009), no. 3, 227–234
<https://doi.org/10.3934/amc.2009.3.227>.
- [4] W. Qi, *On the polycyclic codes over $\mathbb{F}_q + u\mathbb{F}_q$* , Adv. Math. Commun., In press
<https://doi.org/10.3934/amc.2022015>.