Erzincan Üniversitesi
Fen Bilimleri Enstitüsü Dergisi
2023, 16(2), 327-344
ISSN: 1307-9085, e-ISSN: 2149-4584
Araştırma Makalesi

Erzincan University
Journal of Science and Technology
2023, 16(2), 327-344
DOI: 10.18185/erzifbed.1120896
Research Article

A Class of Skew-Cyclic Codes over $\frac{\mathbb{Z}_{2^m}[u]}{\langle u^2-r\rangle}$ with Derivation

Hayrullah ÖZİMAMOĞLU [1*]

[1] Departments of Mathematics, NEVU, Nevşehir, Turkey

Received:24/05/2022, **Revised:** 26/12/2022, **Accepted:** 02/05/2023, **Published:** 31/08/2023

Abstract

Let $R_r = \mathbb{Z}_{2^m} + u\mathbb{Z}_{2^m}$ be a finite ring, where $u^2 = r$ for $r \in \mathbb{Z}_{2^m}$, m is a positive integer, and $m \geq 2$. In this paper, we study a class of skew-cyclic codes using a skew polynomial ring over R_r with an automorphism θ_r and a derivation δ_{θ_r}. We generalize the skew-cyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4; u^2 = 1$ to the skew-cyclic codes over R_r, and call such codes as δ_{θ_r}-cyclic codes. We investigate the structures of a skew polynomial ring $R_r[x, \theta_r, \delta_{\theta_r}]$. A δ_{θ_r}-cyclic code is showed to be a left $R_r[x, \theta_r, \delta_{\theta_r}]$-submodule of $\frac{R_r[x,\theta_r,\delta_{\theta_r}]}{\langle x^n-1\rangle}$. We give the generator matrix of a δ_{θ_r}-cyclic code of length n over R_r. Also, we present the generator matrix of the dual of a free δ_{θ_r}-cyclic code of even length n over R_r.

Keywords: Cyclic codes, skew polynomial rings, skew-cyclic code.

Türetim ile $\frac{\mathbb{Z}_{2^m}[u]}{\langle u^2-r\rangle}$ Halkası Üzerindeki Aykırı Devirli Kodların Bir Sınıfı

Öz

m pozitif bir tamsayı, $m \geq 2$ ve $r \in \mathbb{Z}_{2^m}$ için $u^2 = r$ olmak üzere $R_r = \mathbb{Z}_{2^m} + u\mathbb{Z}_{2^m}$ sonlu halkası verilsin. Bu çalışmada, θ_r bir otomorfizm ve δ_{θ_r} bir türetim olmak üzere R_r üzerindeki bir aykırı polinom halkası kullanılarak aykırı devirli kodların bir sınıfı çalışılmıştır. $u^2 = 1$ olmak üzere $\mathbb{Z}_4 + u\mathbb{Z}_4$ üzerindeki aykırı devirli kodlar, R_r üzerindeki aykırı devirli kodlara genelleştirilmiştir ve bu kodlar δ_{θ_r}-devirli kodlar olarak adlandırılmştır. $R_r[x, \theta_r, \delta_{\theta_r}]$ aykırı polinom halkasının yapıları incelenmiştir. δ_{θ_r}-devirli kodun $\frac{R_r[x,\theta_r,\delta_{\theta_r}]}{\langle x^n-1\rangle}$ halkasının bir sol $R_r[x, \theta_r, \delta_{\theta_r}]$-alt modülü olduğu gösterilmiştir. R_r üzerinde n uzunluğundaki δ_{θ_r}-devirli kodun üreteç matrisi verilmiştir. Ayrıca, R_r üzerinde n çift uzunluğundaki bir serbest δ_{θ_r}-devirli kodun dualinin üreteç matrisi verilmiştir.

Anahtar Kelimeler: Devirli kodlar, aykırı polinom halkaları, aykırı devirli kod.

*Corresponding Author: h.ozimamoglu@nevsehir.edu.tr
Hayrullah Özimamoğlu, https://orcid.org/0000-0001-7844-1840

1. Introduction

Fractional analysis is a branch of mathematics that studies derivatives and integrals of real or complex order. Differential equations involving non-integer derivatives are used to model various physical phenomena. Therefore, in addition to its applications in mathematics, it is also used in the application of many branches of science such as physics, engineering, biology and finance (see [1]- [5]). Some of the most comprehensive studies for fractional derivatives and integrals (see [6]- [7]).

Cyclic codes are a significant family of linear codes because of their rich algebraic structure and high efficiency. Many crucial codes, including such binary Hamming codes, Golay codes and BCH codes, are equivalent to cyclic codes. These codes were first studied by Prange (1957), and have been studied extensively since then. (Blake 1972, 1975) and (Spiegel 1977, 1978), have initiated the work of cyclic codes over ring. After a landmark work of Hammons et al. (1994), codes over rings have become popular among researchers. They have demonstrated that some good non-linear codes over $\mathbb{Z}_2$ can be seen as the Gray images of linear codes over $\mathbb{Z}_4$. However, in most of these studies, the use of cyclic codes is constrained to commutative rings.

Boucher et al. (2007), generalized the notion of cyclic codes by defining non-commutative skew polynomial rings of automorphism type. This codes are known as skew cyclic codes. Also, (Boucher et al. 2008), (Boucher, Ulmer 2009) and (Boucher, Ulmer 2011), generalized works in skew cyclic codes. Boulagouaz and Deajim (2021), constructed novel matrix-product codes arising from (σ, δ)-codes. Boulagouaz and Deajim (2022), gave a characterization of monic principal σ-codes whose dual codes are also monic principal σ-codes. Boucher and Ulmer (2014), used skew polynomial rings with automorphism and derivation to study linear codes. Sharma and Bhaintwal (2014), have studied a family of skew-cyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$ with an automorphism θ and a derivation δ_θ, where $u^2 = 1$. By Çalışkan (2022), these codes are generalized for the $\mathbb{Z}_{2^s} + u\mathbb{Z}_{2^s}$, where $u^2 = 1$. Motivated by Sharma and Bhaintwal (2014), we consider a family of skew-cyclic codes over $R_r = \mathbb{Z}_{2^m} + u\mathbb{Z}_{2^m}$ with an automorphism θ_r of R_r and a derivation of δ_{θ_r} R_r, where $u^2 = r$ for $r \in \mathbb{Z}_{2^m}$.

The paper is structured as follows. In Section 2, we present some fundamental definitions and results that are required for this paper. Moreover, we discuss the structural properties of skew polynomial ring $R_r[x, \theta_r, \delta_{\theta_r}]$ for $r \in \mathbb{Z}_{2^m}$. In Section 3.1, we introduce the δ_{θ_r}-cyclic codes over R_r, and investigate their properties. These codes are a generalization of the δ_θ-cyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$ in Sharma and Bhaintwal (2014). In Section 3.2, we determine the structure of the dual of a free δ_{θ_r}-cyclic codes of even length n over R_r. In Section 4, the paper concludes.

2. Preliminaries

Let $m \geq 2$ be an integer. Throughout the paper, R_r denotes the ring $\mathbb{Z}_{2^m} + u\mathbb{Z}_{2^m} = \{a + ub \mid a, b \in \mathbb{Z}_{2^m}\}$ with $u^2 = r$ for $r \in \mathbb{Z}_{2^m}$. Clearly, $R_r \cong \frac{\mathbb{Z}_{2^m}[u]}{\langle u^2-r\rangle}$. R_r has characteristic 2^m and cardinality 2^{2m}. We define a map $\theta_r: R_r \to R_r$ for $r \in \mathbb{Z}_{2^m}$ such that

$$\theta_r(a + ub) = a + (u + 2^{m-1})b.$$

It can be easily shown that θ_r is an automorphism of R_r. Also, since

$$\theta_r{}^2(\alpha) = \alpha \tag{1}$$

for all $\alpha \in R_r$, the order of θ_r is 2.

Definition 2.1. Let $\boldsymbol{R}$ be a finite ring and Θ be an automorphism of $\boldsymbol{R}$. Then a map $\Delta_\Theta: \boldsymbol{R} \to \boldsymbol{R}$ is said to be a derivation on $\boldsymbol{R}$ if

$$\Delta_\Theta(a+b) = \Delta_\Theta(a) + \Delta_\Theta(b),$$

$$\Delta_\Theta(ab) = \Delta_\Theta(a)b + \Theta(a)\Delta_\Theta(b).$$

We define a map $\delta_{\theta_r}: R_r \to R_r$ for $r \in \mathbb{Z}_{2^m}$ such that

$$\delta_{\theta_r}(a+ub) = (1+u)\big(\theta_r(a+ub) - (a+ub)\big).$$

That is,

$$\delta_{\theta_r}(a+ub) = (1+u)(a + (u+2^{m-1})b - a - ub)$$

$$= 2^{m-1}b + 2^{m-1}bu$$

$$= \begin{cases} 0, & b \in 2\mathbb{Z}_{2^m} \text{ (b is a non unit of } \mathbb{Z}_{2^m}) \\ 2^{m-1} + 2^{m-1}u, & b \in 2\mathbb{Z}_{2^m} + 1 \text{ (b is a unit of } \mathbb{Z}_{2^m}). \end{cases}$$

Corollary 2.2. Let $2 \le n \in \mathbb{Z}$. We have $\delta_{\theta_r}{}^n(\alpha) = 0$ for all $\alpha \in R_r$.

Theorem 2.3. The map δ_{θ_r} is a derivation on R_r.

Proof. Let $\alpha, \beta \in R_r$. Since θ_r is an automorphism of R_r, we get

$$\delta_{\theta_r}(\alpha+\beta) = (1+u)\big(\theta_r(\alpha+\beta) - (\alpha+\beta)\big)$$

$$= (1+u)(\theta_r(\alpha) - \alpha) + (1+u)(\theta_r(\beta) - \beta)$$

$$= \delta_{\theta_r}(\alpha) + \delta_{\theta_r}(\beta),$$

and

$$\delta_{\theta_r}(\alpha\beta) = (1+u)(\theta_r(\alpha\beta) - \alpha\beta)$$

$$= (1+u)\,\theta_r(\alpha)\,\theta_r(\beta) - (1+u)\alpha\beta$$

$$= (1+u)\,\theta_r(\alpha)\,\theta_r(\beta) - (1+u)\alpha\beta - (1+u)\,\theta_r(\alpha)\beta + (1+u)\,\theta_r(\alpha)\beta$$

$$= (1+u)\,\theta_r(\alpha)(\theta_r(\beta) - \beta) + (1+u)\beta(\theta_r(\alpha) - \alpha)$$

$$= \delta_{\theta_r}(\beta)\,\theta_r(\alpha) + \delta_{\theta_r}(\alpha)\beta.$$

Thus by Definition 2.1, δ_{θ_r} is a derivation on R_r. □

The skew polynomial ring was defined by Ore (1933) as follows:

Definition 2.4. Let $\boldsymbol{R}$ be a ring with automorphism Θ and derivation Δ_Θ. Then the skew polynomial ring $\boldsymbol{R}[x, \Theta, \Delta_\Theta]$ is the set of all polynomials over $\boldsymbol{R}$ with the addition as the usual addition of polynomials and the multiplication is defined using the commutation rule

$$x\alpha = \Theta(\alpha)x + \Delta_\Theta(\alpha)$$

for any $\alpha \in \boldsymbol{R}$ and extended by distributivity and associativity.

By Definition 2.4, since R_r is a ring with automorphism θ_r and derivation δ_{θ_r}, we have

$$x\alpha = \theta_r(\alpha)x + \delta_{\theta_r}(\alpha) \quad (2)$$

for any $\alpha \in R_r$.

Lemma 2.5. For any element $\alpha \in R_r$, $\delta_{\theta_r}\big(\theta_r(\alpha)\big) + \theta_r\left(\delta_{\theta_r}(\alpha)\right) = 0$.

Proof. Let $\alpha = a + ub \in R_r$. So

$$\begin{aligned}\delta_{\theta_r}\big(\theta_r(\alpha)\big) &= \delta_{\theta_r}(a + (u + 2^{m-1})b)\\ &= 2^{m-1}b + 2^{m-1}bu,\end{aligned}$$

and

$$\begin{aligned}\theta_r\left(\delta_{\theta_r}(\alpha)\right) &= \theta_r(2^{m-1}b + 2^{m-1}bu)\\ &= 2^{m-1}b + (u + 2^{m-1})2^{m-1}b\\ &= 2^{m-1}b + 2^{m-1}bu,\end{aligned}$$

which proves. □

Lemma 2.6. For all $\alpha \in R_r$, $x^2\alpha = \alpha x^2$.

Proof. By (1), (2), Corollary 2.2 and Lemma 2.5, we get

$$\begin{aligned}x^2\alpha &= x\left(\theta_r(\alpha)x + \delta_{\theta_r}(\alpha)\right)\\ &= \big(x\,\theta_r(\alpha)\big)x + x\delta_{\theta_r}(\alpha)\\ &= \left(\theta_r^2(\alpha)x + \delta_{\theta_r}\big(\theta_r(\alpha)\big)\right)x + \left(\theta_r\left(\delta_{\theta_r}(\alpha)\right)x + \delta_{\theta_r}^2(\alpha)\right)\end{aligned}$$

$$= \alpha x^2 + \left(\delta_{\theta_r}(\theta_r(\alpha)) + \theta_r\left(\delta_{\theta_r}(\alpha)\right)\right)x$$

$$= \alpha x^2. \qquad \square$$

By (2) and Lemma 2.6, we get the following corollary.

Corollary 2.7. For any element $\alpha \in R_r$,

$$x^n\alpha = \begin{cases} \left(\theta_r(\alpha)x + \delta_{\theta_r}(\alpha)\right)x^{n-1}, & \text{if } n \text{ is odd} \\ \alpha x^n, & \text{if } n \text{ is even.} \end{cases}$$

Example 2.8. Let $f(x) = x^3 + \alpha_1 x,\ g(x) = x^2 + \beta_1 x + \beta_0 \in R_r[x, \theta_r, \delta_{\theta_r}]$ for $r \in \mathbb{Z}_{2^m}$. Then

$$f(x) + g(x) = x^3 + x^2 + (\alpha_1 + \beta_1)x + \beta_0$$

$$= g(x) + f(x).$$

By Corollary 2.7,

$$f(x)\,g(x) = (x^3 + \alpha_1 x)(x^2 + \beta_1 x + \beta_0)$$

$$= x^3(x^2 + \beta_1 x + \beta_0) + \alpha_1 x(x^2 + \beta_1 x + \beta_0)$$

$$= x^5 + \left(\theta_r(\beta_1)x + \delta_{\theta_r}(\beta_1)\right)x^2 x + \left(\theta_r(\beta_0)x + \delta_{\theta_r}(\beta_0)\right)x^3 + \alpha_1 x^3$$

$$+\alpha_1\left(\theta_r(\beta_1)x + \delta_{\theta_r}(\beta_1)\right)x + \alpha_1\left(\theta_r(\beta_0)x + \delta_{\theta_r}(\beta_0)\right)$$

$$= x^5 + \left(\theta_r(\beta_1) + \theta_r(\beta_0)\right)x^4 + \left(\delta_{\theta_r}(\beta_1) + \delta_{\theta_r}(\beta_0) + \alpha_1\right)x^3 + \alpha_1\,\theta_r(\beta_1)x^2$$

$$+\left(\alpha_1\delta_{\theta_r}(\beta_1) + \alpha_1\,\theta_r(\beta_0)\right)x + \alpha_1\delta_{\theta_r}(\beta_0),$$

and

$$g(x)f(x) = (x^2 + \beta_1 x + \beta_0)(x^3 + \alpha_1 x)$$

$$= x^2(x^3 + \alpha_1 x) + \beta_1 x(x^3 + \alpha_1 x) + \beta_0(x^3 + \alpha_1 x)$$

$$= x^5 + \alpha_1 x^2 x + \beta_1 x^4 + \beta_1\left(\theta_r(\alpha_1)x + \delta_{\theta_r}(\alpha_1)\right)x + \beta_0 x^3 + \beta_0\alpha_1 x$$

$$= x^5 + \beta_1 x^4 + (\alpha_1 + \beta_0)x^3 + \beta_1\,\theta_r(\alpha_1)x^2 + \left(\beta_1\delta_{\theta_r}(\alpha_1) + \beta_0\alpha_1\right)x.$$

Since $f(x)\,g(x) \neq g(x)f(x)$, $R_r[x,\ \theta_r, \delta_{\theta_r}]$ is a non-commutative ring.

Let $R_r^{\theta_r} = \{a + ub \mid a \in \mathbb{Z}_{2^m}, b \in 2\mathbb{Z}_{2^m}\}$ for $r \in \mathbb{Z}_{2^m}$. $R_r^{\theta_r}$ is subring of R_r. Also α is fixed by θ_r, that is $\theta_r(\alpha) = \alpha$, and $\delta_{\theta_r}(\alpha) = 0$ for all $\alpha \in R_r$. Hence we have $x\alpha = \alpha x$ for all $\alpha \in R_r$.

Definition 2.9. An element $f(x) \in R_r[x, \theta_r, \delta_{\theta_r}]$ is said to be a central element of $R_r[x, \theta_r, \delta_{\theta_r}]$ if $f(x)c(x) = c(x)f(x)$ for all $c(x) \in R_r[x, \theta_r, \delta_{\theta_r}]$.

Lemma 2.10. Let $\alpha \in R_r$ for $r \in \mathbb{Z}_{2^m}$. Then $\theta_r(\alpha) - \alpha \neq \delta_{\theta_r}(\beta)$ for any $\beta \in R_r$ unless α, β both are fixed by θ_r.

Proof. Let $\theta_r(\alpha) - \alpha = \delta_{\theta_r}(\beta)$ for some arbitrary fixed values of α and β. The only possible values of $\delta_{\theta_r}(\beta)$ are 0 and $2^{m-1} + 2^{m-1}u$. Suppose $\delta_{\theta_r}(\beta) = 0$. Clearly, $\theta_r(\alpha) = \alpha$. Then α and β both are fixed by θ_r. Suppose $\delta_{\theta_r}(\beta) = 2^{m-1} + 2^{m-1}u$. Let $\beta = \beta_0 + \beta_1 u$ such that $\beta_0, \beta_1 \in \mathbb{Z}_{2^m}$. Since $\beta_1 \in 2\mathbb{Z}_{2^m}$, $\theta_r(\beta) = \beta$. Let $\alpha = \alpha_0 + \alpha_1 u$ such that $\alpha_0, \alpha_1 \in \mathbb{Z}_{2^m}$. Then $\theta_r(\alpha) - \alpha = 2^{m-1}\alpha_1$, which contradicts $\theta_r(\alpha) - \alpha$ contains u. Therefore, the proof is completed. □

We define

$$S_r = \{a + ub \mid a, b \in 2\mathbb{Z}_{2^m}\}$$

for $r \in \mathbb{Z}_{2^m}$.

Lemma 2.11. For all $\alpha \in S_r$ and $\beta \in R_r$, $\alpha\theta_r(\beta) = \alpha\beta$ and $\alpha\delta_{\theta_r}(\beta) = 0$.

Proof. Let $\alpha = 2\alpha_0 + 2\alpha_1 u$ and $\beta = \beta_0 + \beta_1 u$ such that $\alpha_0, \alpha_1, \beta_0, \beta_1 \in \mathbb{Z}_{2^m}$. Then we have

$$\begin{aligned}\alpha\theta_r(\beta) &= (2\alpha_0 + 2\alpha_1 u)\theta_r(\beta_0 + \beta_1 u) \\ &= (2\alpha_0 + 2\alpha_1 u)(\beta_0 + u\beta_1 + 2^{m-1}\beta_1) \\ &= (2\alpha_0 + 2\alpha_1 u)(\beta_0 + u\beta_1) + (2^m\alpha_0\beta_1 + 2^m\alpha_1\beta_1 u) \\ &= \alpha\beta,\end{aligned}$$

and if $\beta_1 \in 2\mathbb{Z}_{2^m}$, it is clear that $\alpha\delta_{\theta_r}(\beta) = 0$, if $\beta_1 \in 2\mathbb{Z}_{2^m} + 1$, then

$$\begin{aligned}\alpha\delta_{\theta_r}(\beta) &= (2\alpha_0 + 2\alpha_1 u)(2^{m-1} + 2^{m-1}u) \\ &= 2(\alpha_0 + \alpha_1 u)2^{m-1}(1 + u) \\ &= 2^m(\alpha_0 + \alpha_1 u)(1 + u) \\ &= 0.\end{aligned}$$

□

Theorem 2.12. A polynomial $f(x) \in R_r[x, \theta_r, \delta_{\theta_r}]$ is a central element if and only if $f(x) \in R_r^{\theta_r}[x]$ such that the coefficients of all odd powers of x belong to the set $S_r = \{a + ub \mid a, b \in 2\mathbb{Z}_{2^m}\}$.

Proof. (⇒): Let $f(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_k x^k \in R_r[x, \theta_r, \delta_{\theta_r}]$ be a polynomial of odd degree. Suppose $f(x)$ is a central element. Then

$$\begin{aligned}0 &= xf(x) - f(x)x \\ &= x\alpha_0 + x\alpha_1 x + x\alpha_2 x^2 + \cdots + x\alpha_k x^k - (\alpha_0 x + \alpha_1 x^2 + \alpha_2 x^3 + \cdots + \alpha_k x^{k+1})\end{aligned}$$

$$= \left(\theta_r(\alpha_0)x + \delta_{\theta_r}(\alpha_0)\right) + \left(\theta_r(\alpha_1)x + \delta_{\theta_r}(\alpha_1)\right)x + \left(\theta_r(\alpha_2)x + \delta_{\theta_r}(\alpha_2)\right)x^2 + \cdots$$

$$+ \left(\theta_r(\alpha_k)x + \delta_{\theta_r}(\alpha_k)\right)x^k - \sum_{i=0}^{k} \alpha_i x^{i+1}$$

$$= \delta_{\theta_r}(\alpha_0) + \sum_{i=0}^{k-1} \left(\theta_r(\alpha_i) + \delta_{\theta_r}(\alpha_{i+1})\right)x^{i+1} + \theta_r(\alpha_k)x^{k+1} - \sum_{i=0}^{k} \alpha_i x^{i+1}.$$

If we equate coefficients of all terms to zero then we get

$$\delta_{\theta_r}(\alpha_0) = 0 \tag{3}$$

$$\theta_r(\alpha_i) - \alpha_i + \delta_{\theta_r}(\alpha_{i+1}) = 0;\ i = 0,1,\dots,k-1 \tag{4}$$

$$\theta_r(\alpha_k) - \alpha_k = 0. \tag{5}$$

We have $\theta_r(\alpha_i) = \alpha_i$ for $i = 0,1,\dots,k$ by equations (3), (4), (5), and Lemma 2.10. Let $\alpha_i = \alpha_0^{(i)} + \alpha_1^{(i)}u$ for $i = 0,1,\dots,k$. As $\theta_r(\alpha_i) = \alpha_i$, we get $\alpha_1^{(i)} \in 2\mathbb{Z}_{2^m}$. Then $f(x) \in R_r^{\theta_r}[x]$.

As $f(x)$ is a central element, we have $f(x)\beta = \beta f(x)$ for all $\beta \in R_r$. We choose $\beta = \beta_0 + \beta_1 u \in R_r$ such that $\theta_r(\beta) \neq \beta$. Then $\beta_1 \in 2\mathbb{Z}_{2^m} + 1$. By Corollary 2.7, we have

$$0 = \beta f(x) - f(x)\beta$$

$$= \sum_{i=0}^{k} \beta\alpha_i x^i - \sum_{i=0}^{\frac{k-1}{2}} \alpha_{2i}x^{2i}\beta - \sum_{i=0}^{\frac{k-1}{2}} \alpha_{2i+1}x^{2i+1}\beta$$

$$= \sum_{i=0}^{\frac{k-1}{2}} \beta\alpha_{2i}x^{2i} + \sum_{i=0}^{\frac{k-1}{2}} \beta\alpha_{2i+1}x^{2i+1} - \sum_{i=0}^{\frac{k-1}{2}} \alpha_{2i}\beta x^{2i} - \sum_{i=0}^{\frac{k-1}{2}} \alpha_{2i+1}\left(\theta_r(\beta)x + \delta_{\theta_r}(\beta)\right)x^{2i}$$

$$= \sum_{i=0}^{\frac{k-1}{2}} \left(\beta\alpha_{2i} - \alpha_{2i}\beta - \alpha_{2i+1}\delta_{\theta_r}(\beta)\right)x^{2i} + \sum_{i=0}^{\frac{k-1}{2}} \left(\beta\alpha_{2i+1} - \alpha_{2i+1}\theta_r(\beta)\right)x^{2i+1}$$

$$= -\sum_{i=0}^{\frac{k-1}{2}} \alpha_{2i+1}\delta_{\theta_r}(\beta)x^{2i} + \sum_{i=0}^{\frac{k-1}{2}} \alpha_{2i+1}\left(\beta - \theta_r(\beta)\right)x^{2i+1}.$$

This implies that $\alpha_{2i+1}\delta_{\theta_r}(\beta) = 0$ and $\alpha_{2i+1}\left(\beta - \theta_r(\beta)\right) = 0$ for all $i = 0,1,2,\dots,\frac{k-1}{2}$.

We denote $\alpha_{2i+1} = \alpha_0^{(2i+1)} + 2\gamma^{(2i+1)}u$ for $i = 0,1,2,\dots,\frac{k-1}{2}$. As $\beta_1 \in 2\mathbb{Z}_{2^m} + 1$, $\delta_{\theta_r}(\beta) = 2^{m-1} + 2^{m-1}u$. Since

$$0 = \left(\alpha_0^{(2i+1)} + 2\gamma^{(2i+1)}u\right)(2^{m-1} + 2^{m-1}u)$$

$$= 2^{m-1}\alpha_0^{(2i+1)} + 2^m r\gamma^{(2i+1)} + \left(2^{m-1}\alpha_0^{(2i+1)} + 2^m\gamma^{(2i+1)}\right)u$$

$$= 2^{m-1}\alpha_0^{(2i+1)} + 2^{m-1}\alpha_0^{(2i+1)}u,$$

so $\alpha_0^{(2i+1)} \in 2\mathbb{Z}_{2^m}$. Moreover since

$$0 = \alpha_{2i+1}\left(\beta_0 + \beta_1 u - \theta_r(\beta_0 + \beta_1 u)\right)$$

$$= \left(\alpha_0^{(2i+1)} + 2\gamma^{(2i+1)}u\right)(-2^{m-1}\beta_1)$$

$$= -2^{m-1}\beta_1\alpha_0^{(2i+1)},$$

and $\beta_1 \in 2\mathbb{Z}_{2^m} + 1$, then $\alpha_0^{(2i+1)} \in 2\mathbb{Z}_{2^m}$. Hence we have $\alpha_{2i+1} \in S_r$ for all $i = 0,1,2,\dots,\frac{k-1}{2}$. It can be proved similarly for polynomials of even degree.

($\Leftarrow$): Suppose $f(x)$ satisfies the given conditions. Then to show $f(x)c(x) = c(x)f(x)$ for all $c(x) \in R_r[x, \theta_r, \delta_{\theta_r}]$, it is sufficient to show that $(c_i x^i)(\alpha_j x^j) = (\alpha_j x^j)(c_i x^i)$ for $0 \le i \le \deg(c)$ and $0 \le j \le \deg(f)$. Since $f(x) \in R_r^{\theta_r}[x]$, we have $\theta_r(\alpha_i) = \alpha_i$ and $\delta_{\theta_r}(\alpha_i) = 0$ for $i = 0,1,\dots,k$. We obtain the following by Corollary 2.7. If i is even, we have

$$(c_i x^i)(\alpha_j x^j) = c_i(\alpha_j x^i)x^j = c_i\alpha_j\, x^{i+j}. \tag{6}$$

If i is odd, we have

$$(c_i x^i)(\alpha_j x^j) = c_i(x^i\alpha_j)x^j$$

$$= c_i\left(\theta_r(\alpha_j)x + \delta_{\theta_r}(\alpha_j)\right)x^{i-1}x^j$$

$$= c_i\alpha_j\, x^{i+j}. \tag{7}$$

Also, if j is even, we have

$$(\alpha_j x^j)(c_i x^i) = \alpha_j(c_i x^j)x^i = c_i\alpha_j\, x^{i+j}. \tag{8}$$

If j is odd, $\alpha_j \in S_r$ and then we have

$$(\alpha_j x^j)(c_i x^i) = \alpha_j(x^j c_i)x^i$$

$$= \alpha_j \left(\theta_r(c_i)x + \delta_{\theta_r}(c_i)\right) x^{j-1}x^i$$

$$= \left(\alpha_j\theta_r(c_i)x + \alpha_j\delta_{\theta_r}(c_i)\right) x^{i+j-1}$$

$$= c_i\alpha_j\, x^{i+j} \tag{9}$$

by Lemma 2.11. Therefore, we obtain the required result by (6), (7), (8) and (9). □

The ring $R_r[x, \theta_r, \delta_{\theta_r}]$ is not a left or right Euclidean ring, so the division algorithm does not hold in it. But we can still apply division algorithm on some particular elements of $R_r[x, \theta_r, \delta_{\theta_r}]$. We give this case in the following theorem.

Theorem 2.13. (Right division algorithm) Let $f(x), g(x) \in R_r[x, \theta_r, \delta_{\theta_r}]$ such that $g(x)$ has leading coefficient a unit of R_r. Then

$$f(x) = q(x)g(x) + r(x)$$

for some $q(x), r(x) \in R_r[x, \theta_r, \delta_{\theta_r}]$, where $r(x) = 0$ or $\deg(r) < \deg(g)$.

Proof. Let

$$f(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_s x^s$$

$$g(x) = \beta_0 + \beta_1 x + \beta_2 x^2 + \cdots + \beta_t x^t,$$

where β_t is a unit of R_r. If $s < t$, then $f(x) = 0 \cdot g(x) + f(x)$ gives the required result. Suppose $s \geq t$. We define

$$h(x) = f(x) - A_r(x)g(x),$$

where

$$A_r(x) = \begin{cases} \alpha_s\theta_r(\beta_t^{-1})x^{s-t}, & \text{if } s-t \text{ is odd} \\ \alpha_s\beta_t^{-1}x^{s-t}, & \text{if } s-t \text{ is even} \end{cases}. \tag{10}$$

By Corollary 2.7, if $s - t$ is odd, the most degree term of $h(x)$ is

$$\alpha_s x^s - \alpha_s\theta_r(\beta_t^{-1})\theta_r(\beta_t)x x^{s-t-1}x^t = \alpha_s x^s - \alpha_s\theta_r(\beta_t^{-1})\theta_r(\beta_t)x^s$$

$$= 0 \cdot x^s,$$

and if $s - t$ is even, the most degree term of $h(x)$ is

$$\alpha_s x^s - \alpha_s\beta_t^{-1}x^{s-t}\beta_t x^t = \alpha_s x^s - \alpha_s\beta_t^{-1}\beta_t x^{s-t}x^t$$

$$= 0 \cdot x^s.$$

Then, $h(x)$ is a polynomial of degree $\deg(f)-1$. We prove the result by induction on $\deg(f)$. Assume that the result is true for every polynomial having degree less than $\deg(f)$. Clearly, the result is true for $\deg(f)=0$. Let $\deg(f)>0$. As $\deg(h)<\deg(f)$, there exist $q'(x), r(x)$ such that $h(x)=q'(x)g(x)+r(x)$, where $r(x)=0$ or $\deg(r)<\deg(g)$. So by (10), we obtain

$$f(x) = q'(x)g(x)+r(x)+A_r(x)g(x)$$

$$= \big(q'(x)+A_r(x)\big)g(x)+r(x)\text{a}$$

$$= q(x)g(x)+r(x),$$

where $q(x)=q'(x)+A_r(x)$. Therefore, the proof is completed. □

Similarly, the left division algorithm can be proved. Throughout the paper, division means the right division.

Example 2.14. Let $m=5, r=12\in\mathbb{Z}_{2^5}$ and $f(x), g(x)\in R_r\left[x,\theta_r,\delta_{\theta_r}\right]$ such that

$$f(x)=(3+20u)x^3+(14+2u)x^2+4u$$

$$g(x)=(7+18u)x^2+11u.$$

Here $s=3, t=2, \alpha_3=3+20u, u^2=12,\ \beta_2=7+18u, \beta_2^{-1}=7+14u$. By (10), $A_{12}(x)=\alpha_3\theta_{12}\left(\beta_2^{-1}\right)x^{3-2}$

$$=(3+20u)\theta_{12}(7+14u)x$$

$$=(3+20u)(7+14u)x$$

$$=(21+22u)x.$$

Then

$$A_{12}(x)g(x)=(21+22u)x\big((7+18u)x^2+11u\big)$$

$$=(21+22u)\left(\theta_{12}(7+18u)x+\delta_{\theta_{12}}(7+18u)\right)x^2$$

$$+(21+22u)\left(\theta_{12}(11u)x+\delta_{\theta_{12}}(11u)\right)$$

$$=(21+22u)(7+18u)x^3+(21+22u)(16+11u)x$$

$$+(21+22u)(16+16u)$$

$$=(3+20u)x^3+(8+7u)x+(16+16u).$$

We define

$$h(x) = f(x) - A_{12}(x)g(x) \tag{11}$$

$$= (14 + 2u)x^2 + (24 + 25u)x + (16 + 20u).$$

Now repeating the above argument on $h(x)$, we have

$$r(x) = h(x) - q'(x)g(x) \tag{12}$$

$$= (24 + 25u)x + (8 + 14u)$$

such that $q'(x) = 18 + 18u$ by (10). Hence by (11) and (12) we obtain $f(x) = q(x)\, g(x) + r(x)$, where $q(x) = (21 + 22u)x + (18 + 18u)$.

3. Main Theorem and Proof

3.1. δ_{θ_r} −Cyclic Codes over R_r

In this section, we define a class of skew-cyclic codes over R_r for $r \in \mathbb{Z}_{2^m}$ and call them δ_{θ_r}-cyclic codes over R_r.

A code of length n over R_r is a non-empty subset of R_r^n, and a code of length n is a linear code over R_r if it is an R_r-submodule of R_r^n. By identifying R_r^n with $\frac{R_r[x,\theta_r,\delta_{\theta_r}]}{\langle f(x)\rangle}$, where $f(x)$ is a polynomial of degree n over R_r, we can associate a word $\alpha = (\alpha_0, \alpha_1, \alpha_2, \dots, \alpha_{n-1}) \in R_r^n$ with the polynomial $\alpha(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_{n-1}x^{n-1} \in \frac{R_r[x,\theta_r,\delta_{\theta_r}]}{\langle f(x)\rangle}$. In addition, $\frac{R_r[x,\theta_r,\delta_{\theta_r}]}{\langle f(x)\rangle}$ is a left $R_r[x, \theta_r, \delta_{\theta_r}]$-module with scalar multiplication defined by $r(x)(\alpha(x) + \langle f(x)\rangle) = r(x)\alpha(x) + \langle f(x)\rangle$.

Definition 3.1.1. A code C is called a δ_{θ_r}-linear code of length n over R_r if C is a left $R_r[x, \theta_r, \delta_{\theta_r}]$-submodule of $\frac{R_r[x,\theta_r,\delta_{\theta_r}]}{\langle f(x)\rangle}$, where $f(x)$ is a polynomial of degree n over R_r. Moreover, if $f(x)$ is a central polynomial in $R_r[x, \theta_r, \delta_{\theta_r}]$, then C is called a central δ_{θ_r}-linear code.

Definition 3.1.2. (δ_{θ_r}- cyclic code) A code C is called a δ_{θ_r}-cyclic code of length n over R_r if C is a δ_{θ_r}-linear code of length n over R_r, and for all $c = (c_0, c_1, \dots, c_{n-1}) \in C$, we have $T_{\delta_{\theta_r}}(c) = \left(\theta_r(c_{n-1}) + \delta_{\theta_r}(c_0),\ \theta_r(c_0) + \delta_{\theta_r}(c_1), \dots,\ \theta_r(c_{n-2}) + \delta_{\theta_r}(c_{n-1})\right) \in C$. Here, $T_{\delta_{\theta_r}}$ is called the δ_{θ_r}-cyclic shift operator.

We denote $R_r^{(n,\delta_{\theta_r})}$ by $R_r^{(n,\delta_{\theta_r})} := \frac{R_r[x,\theta_r,\delta_{\theta_r}]}{\langle x^n-1\rangle}$.

Lemma 3.1.3. If $\alpha(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_{n-1}x^{n-1} \in R_r^{(n,\delta_{\theta_r})}$ represents the word $\alpha = (\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_{n-1}) \in R_r^n$, then $x\alpha(x)$ represents the word $\left(\theta_r(\alpha_{n-1}) + \delta_{\theta_r}(\alpha_0),\ \theta_r(\alpha_0) + \delta_{\theta_r}(\alpha_1), \ldots,\ \theta_r(\alpha_{n-2}) + \delta_{\theta_r}(\alpha_{n-1})\right) \in R_r^n$.

Proof. Since $x^n = 1$, we have

$$x\alpha(x) = x\left(\sum_{i=0}^{n-1} \alpha_i x^i\right) = \sum_{i=0}^{n-1} (x\alpha_i)x^i$$

$$= \sum_{i=0}^{n-1} \left(\theta_r(\alpha_i)x + \delta_{\theta_r}(\alpha_i)\right)x^i$$

$$= \sum_{i=0}^{n-1} \theta_r(\alpha_i)x^{i+1} + \sum_{i=0}^{n-1} \delta_{\theta_r}(\alpha_i)x^i$$

$$= \sum_{i=1}^{n-1} \theta_r(\alpha_{i-1})x^i + \theta_r(\alpha_{n-1})x^n + \sum_{i=1}^{n-1} \delta_{\theta_r}(\alpha_i)x^i + \delta_{\theta_r}(\alpha_0)x^0$$

$$= \sum_{i=0}^{n-1} \left(\theta_r(\alpha_{i-1})x + \delta_{\theta_r}(\alpha_i)\right)x^i,$$

where indices are in modulo n. Then the proof is completed. □

Theorem 3.1.4. A code C is a δ_{θ_r}-cyclic code of length n over R_r if and only if C is an $R_r[x, \theta_r, \delta_{\theta_r}]$-submodule of $R_r^{(n,\delta_{\theta_r})}$.

Proof. Suppose C is a δ_{θ_r}-cyclic code of length n over R_r. Then for any $c(x) \in C$, $xc(x) \in C$ and for all $i \in \mathbb{Z}^+$, $x^i c(x) \in C$ by Lemma 3.1.3. It follows that $a(x)c(x) \in C$ for all $a(x) \in R_r[x, \theta_r, \delta_{\theta_r}]$. Therefore C is an $R_r[x, \theta_r, \delta_{\theta_r}]$- submodule of $R_r^{(n,\delta_{\theta_r})}$. Converse is clear. □

Corollary 3.1.5. If C is a δ_{θ_r}-cyclic code of even length n over R_r, then C is an ideal of $R_r^{(n,\delta_{\theta_r})}$, and so, C is a central δ_{θ_r}-linear code.

Proof. By Theorem 2.12, since n is even, $x^n - 1$ is a central element. Then $\langle x^n - 1\rangle$ is a two-sided ideal of $R_r[x, \theta_r, \delta_{\theta_r}]$, and so $R_r^{(n,\delta_{\theta_r})}$ is a ring. In addition, as C is a submodule of $R_r^{(n,\delta_{\theta_r})}$ by Theorem 3.1.4, C is an ideal of $R_r^{(n,\delta_{\theta_r})}$. By Definition 3.1.1, since $x^n - 1$ is a central polynomial, C is a central δ_{θ_r}-linear code. □

Theorem 3.1.6. Let C be a δ_{θ_r}-cyclic code of length n over R_r. Then the following statements hold.

i) If n is odd, C is a cyclic code of length n over R_r.

ii) If n is even, C is a quasi-cyclic code of length n and index 2 over R_r.

Proof. Let $c(x) = c_0 + c_1x + \cdots + c_{n-2}x^{n-2} + c_{n-1}x^{n-1} \in C$.

i) Let n be odd. Then there exist an integer s such that $2s = n + 1$. Since $x^n = 1$, we have

$$x^{2s}c(x) = x^{n+1}c(x)$$

$$= c_0x^{n+1} + c_1x^{n+2} + \cdots + c_{n-2}x^{n+n-1} + c_{n-1}x^{n+n}$$

$$= c_{n-1} + c_0x + c_1x^2 + \cdots + c_{n-2}x^{n-1},$$

which is a cyclic shift of $c(x)$ by Lemma 2.6. As $x^{2s}c(x) \in C$, C is a cyclic code.

ii) Let n is even. In general, C is not cyclic. Since $x^n = 1$, we have

$$x^2c(x) = c_0x^2 + c_1x^3 + \cdots + c_{n-2}x^n + c_{n-1}x^{n+1}$$

$$= c_{n-2} + c_{n-1}x + c_0x^2 + c_1x^3 + \cdots + c_{n-4}x^{n-2} + c_{n-3}x^{n-1},$$

which is a cyclic shift of $c(x)$ by two positions by Lemma 2.6. As $x^2c(x) \in C$, C is quasi-cyclic code of index 2. □

Let C be a δ_{θ_r}-cyclic code of length n over R_r such that C contains a minimum degree polynomial $g(x)$ with its leading coefficient is a unit. Hence $C = \langle g(x)\rangle$. Also it is easy to see that $g(x)|(x^n - 1)$ and $\{g(x), xg(x), \ldots, x^{n-k-1}g(x)\}$ is a basis of C, where $k = \deg(g)$. Clearly, if C is free, we have the following corollary.

Corollary 3.1.7. Let C be a free δ_{θ_r}-cyclic code of length n over R_r. Then there exists a minimum degree polynomial $g(x)$ such that $C = \langle g(x)\rangle$ and $g(x)|(x^n - 1)$.

Let $C = \langle g(x)\rangle$ be a δ_{θ_r}-cyclic code of length n over R_r generated by a right divisor $g(x)$ with its leading coefficient is a unit of $x^n - 1$. Then the $(n-k) \times n$ generator matrix of C is

$$G = \begin{bmatrix} g(x) \\ xg(x) \\ x^2g(x) \\ \vdots \\ x^{n-k-1}g(x) \end{bmatrix},$$

where $g(x) = g_0 + g_1x + g_2x^2 + \cdots + g_kx^k$. Then we have the following corollary.

Corollary 3.1.8. Let $C = \langle g(x)\rangle$ be a δ_{θ_r}-cyclic code of length n over R_r such that $g(x) = g_0 + g_1x + g_2x^2 + \cdots + g_kx^k$. Then the $(n-k)\times n$ generator matrix G of C is

$$\begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_k & 0 & \cdots & 0 \\ \delta_{\theta_r}(g_0) & \theta_r(g_0)+\delta_{\theta_r}(g_1) & \theta_r(g_1)+\delta_{\theta_r}(g_2) & \cdots & \theta_r(g_{k-1})+\delta_{\theta_r}(g_k) & \theta_r(g_k) & \cdots & 0 \\ 0 & 0 & g_0 & \cdots & g_{k-3} & g_{k-2} & \cdots & 0 \\ \cdots & \cdots & \cdots & \ddots & \cdots & \ddots & \ddots & \cdots \\ 0 & 0 & \cdots & 0 & g_0\cdots & g_{k-2} & g_{k-1} & g_k \end{bmatrix}$$

for an odd $n-k$, and

$$\begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_k & 0 & \cdots & 0 \\ \delta_{\theta_r}(g_0) & \theta_r(g_0)+\delta_{\theta_r}(g_1) & \theta_r(g_1)+\delta_{\theta_r}(g_2) & \cdots & \theta_r(g_{k-1})+\delta_{\theta_r}(g_k) & \theta_r(g_k) & \cdots & 0 \\ 0 & 0 & g_0 & \cdots & g_{k-3} & g_{k-2} & \cdots & 0 \\ \cdots & \cdots & \cdots & \ddots & \cdots & \ddots & \ddots & \cdots \\ 0 & 0 & \cdots & \delta_\theta(g_0) & \theta_r(g_0)+\delta_{\theta_r}(g_1) & \cdots & \theta_r(g_{k-1})+\delta_{\theta_r}(g_k) & \theta_r(g_k) \end{bmatrix}$$

for an even $n-k$.

Example 3.1.9. Let $r \in 2\mathbb{Z}_{2^m}+1$. Let C be a δ_{θ_r}-cyclic code of length 6 over R_r generated by the right divisor $g(x) = (2^{m-1}+u)x^3 + 2^{m-1}x^2 - u$ of x^6-1. Then the set $\{g(x), xg(x), x^2g(x)\} = \{(2^{m-1}+u)x^3 + 2^{m-1}x^2 - u, ux^4 + 2^{m-1}ux^3 + (2^{m-1}-u)x + 2^{m-1} + 2^{m-1}u, (2^{m-1}+u)x^5 + 2^{m-1}x^4 - ux^2\}$ forms a basis for C. Thus C has cardinality 2^{6m}. The generator matrix of C is

$$\begin{bmatrix} -u & 0 & 2^{m-1} & 2^{m-1}+u & 0 & 0 \\ 2^{m-1}+2^{m-1}u & 2^{m-1}-u & 0 & 2^{m-1}u & u & 0 \\ 0 & 0 & -u & 0 & 2^{m-1} & 2^{m-1}+u \end{bmatrix}.$$

3.2. Dual of δ_{θ_r} −Cyclic Codes over R_r

In this section, we find the generator matrix of the dual of δ_{θ_r}-cyclic code C of even length n over R_r. Hence we need to find the parity check matrix of C.

Definition 3.2.1. Let C be a free δ_{θ_r}-cyclic code of length n over R_r. Then its dual is defined as

$$C^{\perp} = \{x \in R_r^n | x \cdot y = 0, \forall y \in C\},$$

where $x \cdot y$ denotes the usual inner product of x and y.

Lemma 3.2.2. Let n be an even. $x^n - 1$ is a central element of $R_r[x, \theta_r, \delta_{\theta_r}]$. Also we have

$$x^n - 1 = h(x)g(x) = g(x)h(x)$$

for some $h(x), g(x) \in R_r[x, \theta_r, \delta_{\theta_r}]$.

Proof. By Theorem 2.12, it is clear that $x^n - 1 = h(x)g(x)$ is a central element. Since $h(x)g(x)$ is a central element, we get

$$h(x)\big(h(x)g(x)\big) = \big(h(x)g(x)\big)h(x) = h(x)\big(g(x)h(x)\big) \quad .$$

As $R_r\big[x,\ \theta_r, \delta_{\theta_r}\big]$ has non-trivial zero divisors, $h(x)$ is not a zero divisor. Hence the proof is completed. □

We obtain the following lemma from Lemma 3.2.2.

Lemma 3.2.3. Let $C = \langle g(x)\rangle$ be a δ_{θ_r}-cyclic code of even length n over R_r, where $g(x)$ is a monic right divisor of $x^n - 1$. Let $x^n - 1 = h(x)g(x)$. Then $c(x) \in R_r^{(n,\delta_{\theta_r})}$ is in C if and only if $c(x)h(x) = 0$ in $R_r^{(n,\delta_{\theta_r})}$.

Proof. If $c(x) \in C$, then there exists $a(x) \in R_r^{(n,\delta_{\theta_r})}$ such that $c(x) = a(x)g(x)$. By Lemma 3.2.2,

$$c(x)h(x) = a(x)g(x)h(x) = a(x)h(x)g(x) = a(x)(x^n - 1) = 0$$

in $R_r^{(n,\delta_{\theta_r})}$. Conversely, if $c(x)h(x) = 0$ in $R_r^{(n,\delta_{\theta_r})}$, then by Lemma 3.2.2 there exists $b(x) \in R_r\big[x, \theta_r, \delta_{\theta_r}\big]$ such that

$$c(x)h(x) = b(x)(x^n - 1) = b(x)\ h(x)g(x) = b(x)g(x)h(x).$$

Since $h(x)$ is not a zero divisor, we get $c(x) = b(x)\ g(x)$. So the proof is completed. □

Lemma 3.2.4. If $\alpha \in R_r$ is a unit in R_r, then $\theta_r(\alpha) + \delta_{\theta_r}(\beta)$ is a unit for all $\beta \in R_r$.

Proof. Let $\gamma = \theta_r(\alpha) + \delta_{\theta_r}(\beta)$, where $\alpha, \beta \in R_r$ such that α is a unit. Let $\theta_r(\alpha) = a + ub$. Then $a + ub$ is a unit, and hence either a or b is unit but not both. We know $\delta_{\theta_r}(\beta)$ is either 0 or $2^{m-1} + 2^{m-1}u$ for all $\beta \in R_r$. If $\delta_{\theta_r}(\beta) = 0$, then we are done. Otherwise, we have

$$\gamma = a + ub + 2^{m-1} + 2^{m-1}u$$

$$= (a + 2^{m-1}) + (b + 2^{m-1})u.$$

Moreover, any $v \in \mathbb{Z}_{2^m}$ is a unit if and only if $v + 2^{m-1}$ is a unit. Hence γ is a unit. □

Let $C = \langle g(x)\rangle$ be a δ_{θ_r}-cyclic code of even length n over R_r. Then there exists $h(x) = h_0 + h_1x + h_2x^2 + \cdots + h_{k-1}x^{k-1} + h_kx^k \in R_r\big[x, \theta_r, \delta_{\theta_r}\big]$ such that $x^n - 1 = h(x)g(x)$. Let $c(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{n-2}x^{n-2} + c_{n-1}x^{n-1}$. By Lemma 3.2.3, we have $c(x)h(x) = 0$ in $R_r^{(n,\delta_{\theta_r})}$. Hence the coefficients of $x^k, x^{k+1}, \ldots, x^{n-1}$ in $c(x)h(x)$ are all zero. If k is odd, we have

$$c_ih_k + c_{i+1}\Big(\theta_r(h_{k-1}) + \delta_{\theta_r}(h_k)\Big) + c_{i+2}h_{k-2} + \cdots + c_{i+k}\Big(\theta_r(h_0) + \delta_{\theta_r}(h_1)\Big) = 0 \qquad (13)$$

for an even i, and

$$c_i\,\theta_r(h_k) + c_{i+1}h_{k-1} + c_{i+2}\left(\theta_r(h_{k-2}) + \delta_{\theta_r}(h_{k-1})\right) + \cdots + c_{i+k}h_0 + c_{i+k+1}\delta_{\theta_r}(h_0) = 0 \quad (14)$$

for an odd i. If k is even, we have

$$c_i h_k + c_{i+1}\left(\theta_r(h_{k-1}) + \delta_{\theta_r}(h_k)\right) + c_{i+2}h_{k-2} + \cdots + c_{i+k}h_0 + c_{i+k+1}\delta_{\theta_r}(h_0) = 0 \quad (15)$$

for an even i, and

$$c_i\,\theta_r(h_k) + c_{i+1}h_{k-1} + c_{i+2}\left(\theta_r(h_{k-2}) + \delta_{\theta_r}(h_{k-1})\right) + \cdots + c_{i+k}\left(\theta_r(h_0) + \delta_{\theta_r}(h_1)\right) = 0 \quad (16)$$

for an odd i. By equations (13) and (14) (or (15) and (16)), $Hc^T = 0$, where H is dimension $(n-k)\times n$ matrix. Then we get $GH^T = 0$, where G is a generator matrix of C. By Lemma 3.2.4, $\theta_r(h_k)$ is unit, as h_k is a unit. Since the diagonal elements of H are h_k or $\theta_r(h_k)$, H contains a square submatrix of dimension $(n-k)\times(n-k)$ with non-zero determinant. Then all rows of H are linearly independent. Hence $|Span(H)| = |R_r|^{n-k} = |C^{\perp}|$. Therefore $Span(H) = C^{\perp}$, and so the following corollary is obtained.

Corollary 3.2.5. Let $C = \langle g(x)\rangle$ be a δ_{θ_r}-cyclic code of even length n over R_r such that $x^n - 1 = h(x)g(x)$ for some $h(x) = h_0 + h_1x + h_2x^2 + \cdots + h_{k-1}x^{k-1} + h_kx^k \in R_r[x,\theta_r,\delta_{\theta_r}]$. Then the $(n-k)\times n$ parity check matrix H of C is

$$\begin{bmatrix} h_k & \theta_r(h_{k-1}) + \delta_{\theta_r}(h_k) & h_{k-2} & \cdots & \theta_r(h_0) + \delta_{\theta_r}(h_1) & \cdots & 0 & 0 \\ 0 & \theta_r(h_k) & h_{k-1} & \cdots & h_0 & \delta_{\theta_r}(h_0) & \cdots & 0 \\ 0 & 0 & h_k & h_{k-2} & \theta_r(h_{k-3}) + \delta_{\theta_r}(h_{k-2}) & \cdots & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & h_k & \theta_r(h_{k-1}) + \delta_{\theta_r}(h_k) & \cdots & h_1 & \theta_r(h_0)+\delta_{\theta}(h_1) \end{bmatrix}$$

for an odd k, and

$$\begin{bmatrix} h_k & \theta_r(h_{k-1}) + \delta_{\theta_r}(h_k) & h_{k-2} & \cdots & h_0 & \delta_{\theta_r}(h_0) & \cdots & 0 \\ 0 & \theta_r(h_k) & h_{k-1} & \cdots & h_1 & \theta_r(h_0) + \delta_{\theta_r}(h_1) & \cdots & 0 \\ 0 & 0 & h_k & \cdots & h_2 & \theta_r(h_1) + \delta_{\theta_r}(h_2) & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \theta_r(h_k) & h_{k-1} & \cdots & h_1 & \theta_r(h_0) + \delta_{\theta_r}(h_1) \end{bmatrix}$$

for an even k.

Now, we give the parity check matrix of δ_{θ_r}-cyclic code C in Example 3.1.9.

Example 3.2.6. Let $r \in 2\mathbb{Z}_{2^m} + 1$. Let C be a δ_{θ_r}-cyclic code of length 6 over R_r generated by the right divisor $g(x) = (2^{m-1}+u)x^3 + 2^{m-1}x^2 - u$ of $x^6 - 1 = (r^{-1}ux^3 + 2^{m-1}r^{-1}ux^2 + r^{-1}u)\left((2^{m-1}+u)x^3 + 2^{m-1}x^2 - u\right)$. Let $h(x) = r^{-1}ux^3 + 2^{m-1}r^{-1}ux^2 + r^{-1}u$. By Corollary 3.2.5, the parity check matrix H of C is

$$\begin{bmatrix} r^{-1}u & 2^{m-1} & 0 & 2^{m-1}r^{-1} + r^{-1}u & 0 & 0 \\ 0 & 2^{m-1}r^{-1} + r^{-1}u & 2^{m-1}r^{-1}u & 0 & 2^{m-1}r^{-1} & 2^{m-1} + 2^{m-1}u \\ 0 & 0 & r^{-1}u & 2^{m-1} & 0 & 2^{m-1}r^{-1} + r^{-1}u \end{bmatrix},$$

and so $Span(H) = C^{\perp}$.

4. Conclusion

Sharma and Bhaintwal (2018) have studied a class of δ_θ-cyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4;\ u^2 = 1$ with derivation. We define a generalization of these codes as δ_{θ_r}-cyclic codes over $\mathbb{Z}_{2^m} + u\mathbb{Z}_{2^m};\ u^2 = r$ for $r \in \mathbb{Z}_{2^m}$ with derivation. We establish existence of the right division algorithm in $R_r[x, \theta_r, \delta_{\theta_r}]$. A δ_{θ_r}-cyclic code is proved to be a left $R_r[x, \theta_r, \delta_{\theta_r}]$-submodule of $\frac{R_r[x,\theta_r,\delta_{\theta_r}]}{\langle x^n-1\rangle}$. The form of a generator matrix of δ_{θ_r}-cyclic code of length n over R_r is obtained. The properties of δ_{θ_r}-cyclic codes as well as dual of δ_{θ_r}-cyclic codes are investigated. The form of a parity-check matrix of a free δ_{θ_r}-cyclic code of even length n over R_r is given. Then we find the generator matrix of its dual.

Ethics in Publishing

There are no ethical issues regarding the publication of this study.

References

[1] Blake, I. F., (1972). "Codes over certain rings", Information and Control, 20(4), 396-404.

[2] Blake, I. F., (1975). "Codes over integer residue rings", Information and Control, 29(4), 295-300.

[3] Boucher, D., Geiselmann, W., Ulmer, F., (2007). "Skew cyclic codes", Appl. Algebra Engrg. Comm. Comput., 18, 379-389.

[4] Boucher, D., Solé, P., Ulmer, F., (2008). "Skew constacylic codes over Galois rings", Adv. Math. Commun., 2(3), 273-292.

[5] Boucher, D., Ulmer, F., (2011). "A note on the dual codes of module skew codes", In Proc. of the 13^{th} IMA International Conference on Cryptography and Coding, Oxford, UK, LNCS, 7089, 230–243.

[6] Boucher, D., Ulmer, F., (2009). "Codes as modules over skew polynomial rings", In Proc. of the 12^{th} IMA International Conference on Cryptography and Coding, Cirencester, UK, LNCS, 5921, 38–55.

[7] Boucher, D., Ulmer, F., (2009). "Coding with skew polynomial rings", J. of Symbolic Comput., 44(12), 1644–1656.

[8] Boucher, D., Ulmer, F., (2014). "Linear codes using skew polynomials with automorphisms and derivations", Des. Codes Cryptogr., 70, 405–431.

[9] Boulagouaz, M., Deajim, A., (2022). "Characterizations and properties of monic principal skew codes over rings", Security and Communication Networks.

[10] Boulagouaz, M., Deajim, A., (2021). "Matrix-product codes over commutative rings and

constructions arising from (σ, δ)-codes ", Journal of Mathematics.

[11] Çalışkan, B., (2022). "Türetim ile $Z_{2^s} + uZ_{2^s}$ halkası üzerinde aykırı devirli kodlar", Journal of Advanced Research in Natural and Applied Sciences, 8(1), 114-123.

[12] Hammons, A. R., Kumar, P. V., Calderbank, A. R., Sloane, N. J. A., Solé, P., (1994). "The Z_4-linearity of Kerdock, Preparata, Goethals, and related codes", IEEE Trans. Inf. Theory, 40(2), 301-319.

[13] Ore, O., (1933). "Theory of non-commutative polynomials", Ann. Math., 2nd Ser, 34(3), 480–508.

[14] Prange, E., (1957). "Cyclic error-correcting codes in two symbols", Air Force Cambridge Research Center, Cambridge, MA, Tech. Rep. AFCRC-TN, 57-103.

[15] Sharma, A., Bhaintwal, M., (2018). "A class of skew cyclic codes over $Z_4 + uZ_4$ with derivation", Adv. Math. Commun., 12(4), 723-739.

[16] Spiegel, E., (1977). "Codes over Z_m", Information and Control, 35(1), 48-51.

[17] Spiegel, E., (1978). "Codes over Z_m (revisited)", Information and Control, 37(1), 100-104.