BEÜ Fen Bilimleri Dergisi
10 (4),1272-1281, 2021
DOI: 10.17798/bitlisfen.904152

BEU Journal of Science
10 (4), 1272-1281, 2021

Araştırma Makalesi / Research Article

$\mathbb{Z}_8 + u\mathbb{Z}_8$ Halkası Üzerinde Çift Aykırı Devirli Kodlar

Basri ÇALIŞKAN*

Osmaniye Korkut Ata Üniversitesi, Fen Edebiyat Fakültesi, Matematik Bölümü
(ORCID: 0000-0003-0512-4208)

Öz
Bu çalışmada $u^2 = 1$ olmak üzere $S = \mathbb{Z}_8 + u\mathbb{Z}_8$ halkası üzerindeki aykırı devirli ve çift aykırı devirli kodlar çalışılmıştır. θ, S üzerinde bir otomorfizm ve δ_θ, S üzerinde bir türetim olmak üzere $S[x, \theta, \delta_\theta]$ aykırı polinom halkaları tanımlanmıştır. S üzerinde δ_θ-devirli kodlar tanımlanarak bu kod ailesinin bazı cebirsel özellikleri incelenmiştir. Ayrıca, aykırı devirli kodların bir genellemesi olan çift aykırı devirli kodlar çalışılmıştır.

Anahtar kelimeler: Devirli kod, Aykırı polinom halkası, Aykırı devirli kod, Gray dönüşümü.

Double Skew Cyclic Codes over the Ring $\mathbb{Z}_8 + u\mathbb{Z}_8$

Abstract
In this work, skew cyclic and double skew cyclic codes over the ring $S = \mathbb{Z}_8 + u\mathbb{Z}_8$ where $u^2 = 1$ are studied. The skew polynomial rings $S[x, \theta, \delta_\theta]$ are introduced, where θ is an automorphism on S and δ_θ is a derivation on S. Defining δ_θ-cyclic codes on S, some algebraic properties of these families of codes are investigated. Also, double skew cyclic codes regarding as a generalization of skew cyclic codes are studied.

Keywords: Cyclic code, Skew polynomial ring, Skew cyclic code, Gray map.

1. Giriş

Sonlu halkalar üzerindeki kodlama teorisi, sonlu halkaların zengin cebirsel özelliklerinden dolayı 1970 li yıllardan bu yana birçok araştırmacının ilgisini çekmektedir.

Özellikle kodlama ve kod çözmedeki avantajlarından dolayı devirli kodlar, lineer kodların en önemli alt sınıfları olarak ele alınırlar. Sonlu cisimler üzerindeki devirli kodlar üzerine birçok araştırma yapılmasına rağmen, Hammons ve ark. [1] $\mathbb{Z}_4$ halkası üzerinde tanımlı lineer kod ailelerinin özel bir dönüşüm altındaki görüntülerinden, lineer olmayan ikili (binary) kodlar elde etmişlerdir. Bu çalışma ile birlikte çeşitli halkalar üzerinde birçok yeni kod aileleri tanımlanmıştır [2-5]. Çift (double) devirli kodlar, devirli kodların bir genellemesidir. Literatürde bu kodlarla ilgili önemli çalışmalar bulunmaktadır. Örneğin, Borges ve ark. [6] $\mathbb{Z}_2$-çift devirli kodların cebirsel özelliklerini araştırmışlardır. Kısa bir zaman sonra Gao, Shi ve Wu [7] $\mathbb{Z}_4$-çift devirli kodlar ile ilgili bazı sonuçlar elde etmişlerdir.

Devirli kodların bir başka genellemesi ise, değişmeli olmayan halkalar üzerinde tanımlı aykırı devirli (skew cyclic) kodlardır. Boucher ve ark. [8] de, $\mathbb{F}_q$, q elemanlı bir cisim ve θ, $\mathbb{F}_q$ üzerinde bir otomorfizm olmak üzere $\mathbb{F}_q[x, \theta]$ aykırı (skew) polinom halkalarını kullanmışlardır. $\mathbb{F}_q[x, \theta]$ halkasının en önemli özelliği çarpanlara ayrılışın tek türlü olmamasıdır. Bu özellik sayesinde devirli kodlara kıyasla daha fazla sayıda üreteç polinomu ve böylece aynı uzunluğa ve boyuta sahip daha fazla sayıda kod elde etmek mümkündür. Dolayısıyla aykırı devirli kodlar optimal kod elde etmesi açısından daha

*Sorumlu yazar: bcaliskan@osmaniye.edu.tr
Geliş Tarihi: 26.03.2021, Kabul Tarihi: 12.10.2021

avantajlıdır. Boucher ve Ulmer [9] da, aykırı devirli kodların dualleri üzerinde durmuşlar ve bir aykırı devirli kodun dualinin de aykırı devirli kod olduğunu göstermişlerdir.

Aykırı devirli kodlar farklı halkalar üzerinde de tanımlanmıştır. Özellikle Sharma ve Bhaintwal [10] da, $u^2 = 1$ olmak üzere, $\mathbb{Z}_4 + u\mathbb{Z}_4$ halkası üzerinde türetim ile aykırı devirli kodların bir sınıfını incelemişler ve çift tamsayı uzunluklu bir serbest aykırı devirli kodun üreteç ve kontrol matrislerini tanımlamışlardır. Ayrıca bu kod sınıfını çift kodlara genellemişlerdir.

Yukarıda bahsedilen çalışmalardan motive olunarak, bu makalede $u^2 = 1$ olmak üzere $S = \mathbb{Z}_8 + u\mathbb{Z}_8$ halkası dikkate alınmıştır. θ, S üzerinde bir otomorfizm ve δ_θ bir türetim olmak üzere $S[x, \theta, \delta_\theta]$ aykırı polinom halkaları üzerindeki θ-devirli kodlar tanımlanmış, bu kodların bazı cebirsel özellikleri araştırılmış ve çift aykırı devirli kodlar çalışılmıştır.

2. Materyal ve Metot

2.1. $S[x, \theta, \Delta_\theta]$ Aykırı Polinom Halkası

$u^2 = 1$ olmak üzere $S = \mathbb{Z}_8 + u\mathbb{Z}_8$ değişmeli ve karakteristiği 8 olan bir halkadır. S halkası $\frac{\mathbb{Z}_8[u]}{\langle u^2-1\rangle}$ bölüm halkasına izomorftur. S halkasının elemanları

$$S = \{a + ub | a, b \in \mathbb{Z}_8\}$$

$d = a + ub \in S$ şeklinde tek türlü yazılır.

$\theta: S \to S$, $a, b \in \mathbb{Z}_8$ olmak üzere,

$$\theta(a + ub) = a + (u + 4)b$$

şeklinde tanımlansın. Açıkça görülebilir ki θ, S halkasının aşikar olmayan bir otomorfizmidir. Ayrıca, her $d = a + ub \in S$ için

$$\theta^2(a + ub) = \theta\big(\theta(a + ub)\big) = \theta(a + (u + 4)b) = \theta(a + 4b + ub) = a + 4b + (u + 4)b$$
$$= a + 4b + 4b + ub = a + ub$$

olduğundan, $\theta^2(d) = d$ dir. Dolayısıyla, θ nın mertebesi 2 dir.

Tanım 2.1.1. S sonlu bir halka ve θ, S nin bir otomorfizmi olsun. Bu durumda, $\Delta_\theta: S \to S$ ye tanımlanan ve aşağıda verilen özellikleri sağlayan Δ_θ dönüşümüne S üzerinde bir türetim denir.

$$\Delta_\theta(x + y) = \Delta_\theta(x) + \Delta_\theta(y)$$

ve

$$\Delta_\theta(xy) = \Delta_\theta(x)y + \theta(x)\Delta_\theta(y).$$

Teorem 2.1.2. $\delta_\theta: S \to S$ ye dönüşümü, $\delta_\theta(a + ub) = (1 + u)[\theta(a + ub) - (a + ub)]$ olarak tanımlansın. Yani,

$$\delta_\theta(a + ub) = (1 + u)[\theta(a + ub) - (a + ub)] = (1 + u)[a + 4b + ub - a - ub] = (1 + u)4b$$
$$= 4b + 4ub$$

olsun. Bu durumda, δ_θ dönüşümü S üzerinde bir türetimdir.

İspat. [10] Theorem 2.2 nin ispatının benzeridir.

Aşağıda, S halkasının elemanlarının δ_θ dönüşümü altındaki görüntüleri verilmiştir.

$$\delta_\theta(a+ub)=\begin{cases}0, & b \text{ birim değil ise}\\ 4+4u, & b \text{ birim ise}.\end{cases}$$

Sonuç 2.1.3. $2\le n\in\mathbb{Z}^+$ olmak üzere, her $d\in S$ için $\delta_\theta^n(d)=0$ dır.

İspat. $2\le n\in\mathbb{Z}^+$ ve $d=a+ub\in S$ olsun. Bu durumda

$$\delta_\theta^2(a+ub)=\delta_\theta\big(\delta_\theta(a+ub)\big)=\delta_\theta(4b+4ub)=4(4b)+4(4b)u=0$$

olduğundan ispat tamamlanır.

2.2. Gray Dönüşümü

$\mathbb{Z}_4$ halkası üzerinde tanımlı Gray dönüşümü, $\phi:\mathbb{Z}_4\to\mathbb{Z}_2^2$ olmak üzere, $\phi(0)=(00)$, $\phi(1)=(01)$, $\phi(2)=(11)$ ve $\phi(3)=(10)$ biçiminde tanımlıdır [1].

Carlet [11] de, bu Gray dönüşümünü $\mathbb{Z}_{2^s}$ üzerinde aşağıdaki gibi genelleştirmiştir.

$$\phi:\mathbb{Z}_{2^s}\to\mathbb{Z}_2^{2^{s-1}}$$
$$\phi(i)=\begin{cases}0_{2^{s-1}-i}1_i, & 0\le i\le 2^{s-1}\\ 1_{2^{s-1}}+\phi(i-2^{s-1}), & i>2^{s-1}\end{cases}$$

Burada, 0_i bütün bileşenleri 0 olan i uzunluklu vektörü ve 1_i de bütün bileşenleri 1 olan i uzunluklu vektörü göstermektedir. Bu Gray dönüşüm bir izometridir ve $\mathbb{Z}_{2^s}$ üzerindeki Lee uzaklığını $n=2^{s-1}$ olmak üzere $\mathbb{Z}_2^n$ üzerindeki Hamming uzaklıklarına dönüştürür. $s=3$ için $\mathbb{Z}_8$ in elemanlarının görüntüleri aşağıdaki gibidir.

$$\phi:\mathbb{Z}_{2^3}\to\mathbb{Z}_2^4$$
$$\phi(0)=(0000),\ \phi(1)=(0001),\ \phi(2)=(0011),\ \phi(3)=(0111),$$
$$\phi(4)=(1111),\ \phi(5)=(1110),\ \phi(6)=(1100),\ \phi(7)=(1000).$$

$\mathbb{Z}_8$ üzerindeki Lee ağırlığı, $w_L:\mathbb{Z}_8\to\mathbb{Z}_8$, $w_L(x)=min(x,8-x)$ biçiminde tanımlanır [12].

Tanım 2.2.1. Bir $d\in S$ vektörü için Lee ağırlığı $w_L(d)$, d nin koordinatlarının Lee ağırlıklarının toplamı olarak tanımlanır. $\varphi:S\to\mathbb{Z}_8^2$ dönüşümü $\varphi(a+ub)=(b,a+b)$ olmak üzere, herhangi bir $v\in S$ için v nin Gray ağırlığı, $w_G(v)=w_L\big(\varphi(v)\big)$ olarak tanımlanır.

Tanım 2.2.2. S, θ otomorfizmi ve Δ_θ türetimiyle bir halka olsun. S üzerindeki tüm polinomların kümesi polinomların bilinen toplaması ve herhangi $d\in S$ olmak üzere

$$xd=\theta(d)x+\Delta_\theta(d)$$

şeklinde tanımlanan çarpma işlemi ile $S[x,\theta,\Delta_\theta]$ aykırı polinom halkası olarak adlandırılır. Tanımlanan bu çarpma işlemi $S[x,\theta,\Delta_\theta]$ nın tüm elemanları için genişletilebilir.

Örnek 2.2.3. $p_1=x+d$ ve $p_2=d'$, $S[x,\theta,\delta_\theta]$ halkasında herhangi iki polinom olsun. Bu durumda

$$p_1+p_2=x+d+d'=d'+x+d=p_2+p_1$$

ve

$p_1p_2 = (x+d)d' = xd' + dd' = \theta(d')x + \delta_\theta(d') + dd'$
$p_2p_1 = d'(x+d) = d'x + d'd$

çarpımlarından, x li terimlerin katsayıları sırasıyla $\theta(d')$ ve d' olup, S de her zaman $\theta(d') = d'$ olmak zorunda olmadığı için x li terimlerin katsayıları birbirinden farklıdır. Benzer durum sabit terimler içinde geçerlidir. Dolayısıyla $S[x,\theta,\delta_\theta]$ değişmeli olmayan bir halkadır.

Tanım 2.2.4. $S^\theta = \{a' + ub' | a' \in \mathbb{Z}_8, b' \in \{0,2,4,6\}\}$ olmak üzere, her $e \in S^\theta$ için $\theta(e) = e$ olacak şekildeki elemanların kümesi S^θ ya S nin θ tarafından sabit bırakılan bir alt halkası denir. Ayrıca, her $e \in S^\theta$ için $\delta_\theta(e) = 0$ olup, $xe = ex$ dir.

Tanım 2.2.5. $p(x) \in S[x,\theta,\delta_\theta]$ olsun. Her $d(x) \in S[x,\theta,\delta_\theta]$ için $p(x)d(x) = d(x)p(x)$ oluyorsa, $p(x)$ polinomuna $S[x,\theta,\delta_\theta]$ nin bir merkez elemanı denir.

Lemma 2.2.6. $d \in S$ olmak üzere, herhangi bir $e \in S$ için d ve e nin her ikisi de θ tarafından sabit bırakılmadıkça $\theta(d) - d \neq \delta_\theta(e)$ dir.

İspat. [10] Lemma 2.5.'in ispatının benzeridir. $d = a + ub \in S$ ve e nin sabit bırakılan bir değerleri için $\theta(d) - d = \delta_\theta(e)$ olsun. $\delta_\theta(e)$ nin mümkün olan değerleri sadece 0 ve $4 + 4u$ olduğu bilinmektedir. $\delta_\theta(e) = 0$ ise d ve e nin her ikisi de θ tarafından sabit bırakıldığı görülür ve istenen elde edilmiş olur. $\delta_\theta(e) = 4 + 4u$ olduğunu kabul edelim. Bu durumda, $\theta(d) - d = a + (u+4)b - a - ub = 4b$ ifadesinde u bulunmaz, o zaman bir çelişki elde ederiz. Dolayısıyla ispat tamamlanmış olur.

Teorem 2.2.7. Bir $f(x) \in S[x,\theta,\delta_\theta]$ polinomunun bir merkez elemanı olabilmesi için gerek ve yeter koşul $f(x) \in S^\theta[x]$ olması ve x in tüm tek dereceli terimlerinin katsayılarının

$$\{\alpha + u\beta | \alpha, \beta \in \{0,2,4,6\}\}$$

kümesine ait olmasıdır.

İspat. [10] Lemma 2.7.'nin ispatının benzeridir..

Lemma 2.2.8. Herhangi bir $d \in S$ için $\delta_\theta(\theta(d)) + \theta(\delta_\theta(d)) = 0$ dır. Ayrıca her $d \in S$ için $x^2d = dx^2$ dir.

İspat. $d = a + ub \in S$ olsun. O zaman $\theta(a+ub) = a + (u+4)b$ ve $\delta_\theta(a+ub) = 4b + 4bu$ olduğundan,

$$\delta_\theta(\theta(d)) = \delta_\theta(\theta(a+ub)) = \delta_\theta(a + (u+4)b) = \delta_\theta(a + 4b + ub) = 4b + 4bu$$

ve

$$\theta(\delta_\theta(d)) = \theta(\delta_\theta(a+ub)) = \theta(4b + 4bu) = 4b + (u+4)4b = 4b + 16b + 4bu = 4b + 4bu$$
$$= -(4b + 4bu) = -\delta_\theta(\theta(d))$$

olduğundan, $\delta_\theta(\theta(d)) + \theta(\delta_\theta(d)) = 0$ eşitliği gösterilmiş olur. Şimdi, $xd = \theta(d)x + \delta_\theta(d)$ eşitliğini soldan x ile çarpalım,

$$x^2d = x\theta(d)x + x\delta_\theta(d) = [\theta^2(d)x + \delta_\theta(\theta(d))]x + \theta(\delta_\theta(d))x + {\delta_\theta}^2(d)$$
$$= dx^2 + [\delta_\theta(\theta(d)) + \theta(\delta_\theta(d))]x + {\delta_\theta}^2(d) = dx^2$$

elde edilir. Bu lemmanın birinci kısmı ile her $d \in S$ için ${\delta_\theta}^2(d) = 0$ olduğu kullanılırsa ispat tamamlanmış olur.

Sonuç 2.2.9. Herhangi bir $d \in S$ için,

$$x^n d = \begin{cases} \big(\theta(d)x + \delta_\theta(d)\big)x^{n-1}, & n \text{ tek ise} \\ dx^n, & n \text{ çift ise} \end{cases}$$

dır.

$S[x, \theta, \delta_\theta]$ bir Euclidean halka olmadığından, hem sağ hem de sol bölme algoritması bu halkada sağlanmaz. Aşağıdaki teorem hem sağ hem de sol bölme algoritmasının $S[x, \theta, \delta_\theta]$ nın bazı elemanları için uygulanabileceğini göstermektedir.

Teorem 2.2.10. (Sağ Bölme Algoritması) $f(x)$ ve $g(x)$, $g(x)$ in baş katsayısı birim olacak şekilde $S[x, \theta, \delta_\theta]$ halkasında herhangi iki polinom olsun. Bu durumda,

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

$der\big(r(x)\big) < der\big(g(x)\big)$ veya $r(x) = 0$ olacak şekilde $q(x), r(x) \in S[x, \theta, \delta_\theta]$ vardır [10].

Yukarıdaki teoremde $f(x)$ polinomu $g(x)$ polinomu ile sağdan bölünmüştür. Aynı teorem soldan bölme için de geçerlidir. Dolayısıyla $S[x, \theta, \delta_\theta]$ halkası için bölme algoritması sağdan ve soldan sağlanır.

$f(x) = f_0 + f_1 x + f_2 x^2 + \cdots + f_r x^r$ ve $g(x) = g_0 + g_1 x + g_2 x^2 + \cdots + g_s x^s$ polinomları, g_s birim ve $r \geq s$ olacak şekilde $S[x, \theta, \delta_\theta]$ de iki polinom olsun.

$$A(x) = \begin{cases} f_r \theta(g_s^{-1}) x^{r-s}, & r-s \text{ tek ise} \\ f_r g_s^{-1} x^{r-s}, & r-s \text{ çift ise} \end{cases}$$

şeklinde tanımlanan $A(x)$ polinomu yardımıyla, $f(x)$ polinomunun sağ böleni bulunabilir. Daha detaylı bilgi için [10] Theorem 2.8 e bakılabilir.

Örnek 2.2.11. $S[x, \theta, \delta_\theta]$ de $f(x) = ux^2 + (4 + 4u)x + 6u$ ve $g(x) = (5 + 4u)x + 7 + 3u$ polinomlarını alalım. [10] Theorem 2.8 de verilen sağ bölme algoritmasını kullanarak $g(x)$ nin $f(x)$ için bir sağ bölen olduğunu gösterelim. Bunun için önce $A(x) = f_2 \theta(g_1^{-1}) x^{2-1} = u\theta(5 + 4u)x = (4 + 5u)x$ bulunur. Sonra ise,

$$A(x)g(x) = (4 + 5u)x[(5 + 4u)x + 7 + 3u\ ]$$
$$= (4 + 5u)[\theta(5 + 4u)x + \delta_\theta(5 + 4u)]x + (4 + 5u)[\theta(7 + 3u\ )x + \delta_\theta(7 + 3u\ )]$$
$$= (4 + 5u)[(5 + 4u)x + 0]x + (4 + 5u)[(3 + 3u\ )x + 4 + 4u] = ux^2 + (3 + 3u)x + 4 + 4u$$

hesaplanır. Şimdi ise,

$$h(x) = f(x) - A(x)g(x) = (1 + u)x + 4 + 2u$$

elde edilir. $h(x)$ derecesi 1 olduğundan, aynı algoritma $h(x)$ için uygulanırsa, $h(x)$ in $g(x)$ cinsinden değeri $h(x) = (1 + u)g(x) + 2$ bulunur. O zaman son olarak,
$f(x) = h(x) + A(x)g(x) = (1 + u)g(x) + 2 + (4 + 5u)xg(x) = [(4 + 5u)x + 1 + u]g(x) + 2$
elde edilir. Dolayısıyla, $q(x) = (4 + 5u)x + 1 + u$ ve $r(x) = 2$ olmak üzere, $f(x) = q(x)g(x) + r(x)$ şeklinde yazılabildiği görülür.

3. Bulgular ve Tartışma

3.1. S Halkası Üzerinde δ_θ-Devirli Kodlar

Bu bölümde, S üzerinde δ_θ-devirli kodlar tanımlanarak, üreteç ve kontrol matrislerinin formları belirlenmiştir.

Bilindiği üzere S^n nin boş olmayan bir alt kümesine S üzerinde bir kod denir. C, S üzerinde bir kod olmak üzere eğer C, S^n nin bir S-alt modülü oluyorsa C ye S üzerinde bir lineer kod denir. Eğer S^n üzerindeki bir C kodu sonlu sayıda lineer bağımsız vektörler tarafından üretiliyorsa, C ye bir serbest kod denir.

$p(x)$, S üzerinde derecesi n olan herhangi bir polinom olmak üzere $S_n = \frac{S[x,\theta,\delta_\theta]}{\langle p(x)\rangle}$ olsun. Bir $c = (c_0, c_1, \dots, c_{n-1}) \in C$ kodunun polinom gösterimi $c = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$ şeklindedir. Ayrıca, $S_n = \frac{S[x,\theta,\delta_\theta]}{\langle p(x)\rangle}$, $r(x)(q(x) + \langle p(x)\rangle) = r(x)q(x) + \langle p(x)\rangle$ çarpma işlemi ile bir sol $S[x,\theta,\delta_\theta]$-modüldür.

Tanım 3.1.1. $p(x)$, S üzerinde derecesi n olan herhangi bir polinom olsun. $S_n = \frac{S[x,\theta,\delta_\theta]}{\langle p(x)\rangle}$ nin bir sol $S[x,\theta,\delta_\theta]$-modülü C ye S üzerinde n uzunluklu bir δ_θ-lineer kod denir. Eğer $p(x)$ merkez polinomu ise C ye bir merkez δ_θ-lineer kod denir. Ayrıca, T_{δ_θ}, δ_θ-devirsel ötelemesi olmak üzere, her $c = (c_0, c_1, \dots, c_{n-1}) \in C$ için $T_{\delta_\theta}(c) = \big(\theta(c_{n-1}) + \delta_\theta(c_0), \theta(c_0) + \delta_\theta(c_1), \dots, \theta(c_{n-2}) + \delta_\theta(c_{n-1})\big) \in C$ oluyorsa, C ye S üzerinde δ_θ-devirli kod denir.

Teorem 3.1.2. S üzerinde n uzunluklu bir C kodunun δ_θ-devirli kod olabilmesi için gerek ve yeter koşul C nin, $S_{n,\delta_\theta} = \frac{S[x,\theta,\delta_\theta]}{\langle x^n-1\rangle}$ nın bir $S[x,\theta,\delta_\theta]$-alt modülü olmasıdır.

İspat: [10] Theorem 3.4 ün ispatının benzeridir.

Sonuç 3.1.3. Eğer C, n çift tamsayı uzunluklu bir δ_θ-devirli kod ise, C, $S_{n,\delta_\theta} = \frac{S[x,\theta,\delta_\theta]}{\langle x^n-1\rangle}$ nın bir idealidir.

İspat: [10] Corollary 2 nin ispatının benzeridir.

Teorem 3.1.4. C, S üzerinde n uzunluklu bir δ_θ-devirli kod olsun. Eğer C kodu, minimum dereceli ve baş katsayısı birim olan bir $g(x)$ polinomunu içeriyorsa, $C = \langle g(x)\rangle$ dir. Ayrıca $g(x)|(x^n - 1)$ ve $\{g(x), xg(x), \dots, x^{n-der(g(x))-1}g(x)\}$ kümesi C nin bir bazını oluşturur.

İspat. [10] Theorem 3.6 nın ispatının benzeridir.

$C = \langle g(x)\rangle$, $x^n - 1$ in bir sağ böleni $g(x) = g_0 + g_1 x + g_2 x^2 + \cdots + g_k x^k$ tarafından üretilen ve uzunluğu n olan S üzerinde bir δ_θ-devirli kod ise, C nin $(n-k)\times n$ tipindeki üreteç matrisi

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

formundadır. Daha açık bir şekilde eğer $n-k$ çift ise üreteç matrisi

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

şeklindedir. $n-k$ tek ise üreteç matrisi

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

şeklindedir.

Örnek 3.1.5. C, x^4-1 ün sağ böleni $g(x)=(3+4u)x^2+5u$ polinomu tarafından üretilen, 4 uzunluklu bir δ_θ-devirli kod olsun. Bu durumda $\{g(x), xg(x)\}=\{(3+4u)x^2+5u\ , (3+4u)x^3+(4+5u)x+4+4u\ \}$ kümesi C kodu için bir baz oluşturur. C nin kardinalitesi $|C|=64^2$ olup, C nin üreteç matrisi aşağıdaki gibidir,

$$G=\begin{bmatrix} g(x) \\ xg(x) \end{bmatrix}=\begin{bmatrix} g_0 & g_1 & g_2 & 0 \\ \delta_\theta(g_0) & \theta(g_0)+\delta_\theta(g_1) & \theta(g_1)+\delta_\theta(g_2) & \theta(g_2) \end{bmatrix}$$

$$=\begin{bmatrix} 5u & 0 & 3+4u & 0 \\ 4+4u & 4+5u & 0 & 3+4u \end{bmatrix}.$$

Tanım 3.1.6. C, S üzerinde n uzunluklu bir δ_θ-devirli kod olsun. $w=(w_0,w_1,\dots,w_{n-1}), v=(v_0,v,\dots,v_{n-1})\in S^n$ ve $w.v$ bilinen iç çarpım olmak üzere C nin duali,

$$C^\perp=\{w|\ \text{her } v\in C \text{ için } w.v=0\}$$

olarak tanımlanır.

Teorem 3.1.7. k bir tek tamsayı olmak üzere, $x^n-1=h(x)g(x)$ olacak şekilde en az bir $h(x)=h_0+h_1x+h_2x^2+\cdots+h_kx^k\in S[x,\theta,\delta_\theta]$ olsun. C de $g(x)$ tarafından üretilen, S üzerinde uzunluğu n çift tamsayı olan bir δ_θ-devirli kod olsun. Bu durumda C nin kontrol matrisi

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

formundadır. k bir çift tamsayı olduğunda H matrisi

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

şeklindedir.

İspat. [10] Theorem 4.5 in ispatının benzeridir.

Örnek 4: $x^4-1=\big((3+4u)x^2+3u\big)\big((3+4u)x^2+5u\big)$ olmak üzere, C, $g(x)=(3+4u)x^2+5u$ polinomu tarafından üretilen 4 uzunluklu bir δ_θ-devirli kod olsun. $h(x)=(3+4u)x^2+3u$ olmak üzere Teorem 3.1.7 den C nin kontrol matrisi

$$H = \begin{bmatrix} h_2 & \theta(h_1)+\delta_\theta(h_2) & h_0 & \delta_\theta(h_0) \\ 0 & \theta(h_2) & h_1 & \theta(h_0)+\delta_\theta(h_1) \end{bmatrix}$$
$$H = \begin{bmatrix} 3+4u & 0 & 3u & 4+4u \\ 0 & 3+4u & 0 & 4+3u \end{bmatrix}$$

olarak elde edilir. Ayrıca, Örnek 3.1.5.'de bulunan G üreteç matrisi dikkate alınırsa, $GH^T = 0$ olduğu elde edilir. H nin satırları lineer bağımsız olduğundan, H, C nin kontrol matrisidir.

3.2. Çift Aykırı Devirli Kodlar

Bir C kodunun koordinatları iki alt kümeye ayrılabiliyorsa, C ye bir çift θ-lineer kod denir. s ve t, $n = s+t$ olacak şekilde negatif olamayan iki tamsayı olsun. n uzunluklu koordinatın sırasıyla s ve t parçalanışını dikkate alalım. Herhangi bir $d \in S$ ve $w = (e_0, e_1, \dots, e_{s-1}, f_0, f_1, \dots, f_{t-1}) \in S^{s+t}$ için

$$dw = (de_0, de_1, \dots, de_{s-1}, df_0, df_1, \dots, df_{t-1}) \in S^{s+t}$$

şeklinde tanımlanan işlem ile birlikte S^{s+t} bir S-modüldür.

Tanım 3.2.1. Herhangi bir $w = (e_0, e_1, \dots, e_{s-1}, f_0, f_1, \dots, f_{t-1}) \in S^{s+t}$ için, w nun $\delta_\theta(s,t)(w)$ devirli ötelemesi ${}^{st}_{\delta_\theta}T(w)$ şeklinde gösterilir ve

$${}^{st}_{\delta_\theta}T(w) = (\theta(e_{s-1})+\delta_\theta(e_0), \theta(e_0)+\delta_\theta(e_1), \theta(e_1)+\delta_\theta(e_2), \dots, \theta(e_{s-2})+\delta_\theta(e_{s-1}),$$
$$\theta(f_{t-1})+\delta_\theta(f_0), \theta(f_0)+\delta_\theta(f_1), \theta(f_1)+\delta_\theta(f_2) \dots, \theta(f_{t-2})+\delta_\theta(f_{t-1})\Big)$$

olarak tanımlanır.

S^{s+t} nin bir S- alt modülüne bir çift δ_θ-lineer kod denir.

Tanım 3.2.2. C, bir çift δ_θ-lineer kod olsun. Eğer C, $\delta_\theta(s,t)$ devirli ötelemesi ${}^{st}_{\delta_\theta}T$ altında invaryant kalıyorsa C ye bir δ_θ-devirli kod denir.

$w = (e_0, e_1, \dots, e_{s-1}, f_0, f_1, \dots, f_{t-1}) \in C$ olsun. Bu durumda $e(x) = e_0 + e_1x + \cdots + e_{s-1}x^{s-1} \in \frac{S[x,\theta,\delta_\theta]}{\langle x^s-1\rangle}$ ve $f(x) = f_0 + f_1x + \cdots + f_{t-1}x^{t-1} \in \frac{S[x,\theta,\delta_\theta]}{\langle x^t-1\rangle}$ olmak üzere

$$w(x) = \big(e(x)\big|f(x)\big)$$

şeklinde yazılabilir. Bu S^{s+t} ile $S_{s+t} = \frac{S[x,\theta,\delta_\theta]}{\langle x^s-1\rangle} \times \frac{S[x,\theta,\delta_\theta]}{\langle x^t-1\rangle}$ arasında birebir bir eşleme verir. $d(x)e(x)$ ve $d(x)f(x)$ işlemleri sırasıyla $\frac{S[x,\theta,\delta_\theta]}{\langle x^s-1\rangle}$ ve $\frac{S[x,\theta,\delta_\theta]}{\langle x^t-1\rangle}$ üzerinde tanımlı polinom çarpmaları olmak üzere, $d(x) \in S[x,\theta,\delta_\theta]$ ile $\big(e(x)\big|f(x)\big) \in \frac{S[x,\theta,\delta_\theta]}{\langle x^s-1\rangle} \times \frac{S[x,\theta,\delta_\theta]}{\langle x^t-1\rangle}$ arasındaki çarpma işlemi

$$d(x)\big(e(x)\big|f(x)\big) = \big(d(x)e(x)\big|d(x)f(x)\big)$$

olarak tanımlanır. Bu işlem ile S_{s+t} bir sol $S[x,\theta,\delta_\theta]$-modüldür. Açıkça görülebilir ki $xw(x)$, w nun $\delta_\theta(s,t)$ devirli ötelemesidir.

Teorem 3.2.3. C, S üzerinde $n = s+t$ uzunluklu bir δ_θ-lineer kod olsun. C nin bir çift δ_θ-devirli kod olabilmesi için gerek ve yeter koşul, C nin $\frac{S[x,\theta,\delta_\theta]}{\langle x^s-1\rangle} \times \frac{S[x,\theta,\delta_\theta]}{\langle x^t-1\rangle}$ sol modülünün bir sol $S[x,\theta,\delta_\theta]$-alt modülü olmasıdır.

İspat. C nin bir çift δ_θ-devirli kod olduğunu kabul edelim. $w(x)$, $w \in C$ nin polinom gösterimi olsun. $xw(x)$, w nun $\delta_\theta(s,t)$ devirli ötelemesi olduğundan $xw(x) \in C$ dir. C bir lineer kod olduğundan herhangi bir $d(x) \in S[x,\theta,\delta_\theta]$ için $d(x)w(x) \in C$ dir. Dolayısıyla C, S_{s+t} nin bir $S[x,\theta,\delta_\theta]$-alt modülüdür. İspatın diğer yönü açıktır.

Teorem 3.2.4. $g_1(x)$ ve $g_2(x)$ polinomları sırasıyla $g_1(x)|x^m-1$ ve $g_2(x)|x^n-1$ olacak şekilde monik polinomlar olsunlar. M ve N, S üzerinde $g_1(x)$ ve $g_2(x)$ polinomları tarafından üretilen m ve n uzunluklu iki serbest devirli kod olsunlar. Bu durumda $h(x)$, $h_1(x)$ ve $h_2(x)$ polinomlarının en küçük sol ortak katı ve $k = der\big(h(x)\big)$ olmak üzere $g(x) = \big(g_1(x)\big|g_2(x)\big)$ tarafından üretilen C kodu bir çift δ_θ-devirli koddur ve $B = \{g(x), xg(x), \dots, x^{n-k-1}g(x)\}$ kümesi C nin bir geren kümesidir.

İspat. $h_1(x)$ ve $h_2(x) \in S[x,\theta,\delta_\theta]$ polinomlarının $x^m-1 = h_1(x)\,g_1(x)$ ve $x^n-1 = h_2(x)g_2(x)$ olacak şekildeki monik polinomlar olduğunu kabul edelim. Bu durumda $h(x)g_1(x) = h_3(x)h_1(x)g_1(x) = 0$ ve $h(x)g_2(x) = h_4(x)h_2(x)g_2(x) = 0$ olduğundan $h(x)\big(g_1(x)\big|g_2(x)\big) = \big(h(x)g_1(x)\big|h(x)g_2(x)\big) = 0$ dır. $z(x) \in C$ sıfırdan farklı herhangi bir kodsöz olsun. Bu durumda en az bir $k(x) \in S[x,\theta,\delta_\theta]$ için $z(x) = k(x)g(x)$ dir. Bölme algoritmasından, $der\big(r(x)\big) = 0$ veya $der\big(r(x)\big) < der\big(h(x)\big)$ olacak şekilde $k(x) = q(x)h(x) + r(x)$ eşitliğine sahip oluruz. O zaman $z(x) = k(x)g(x) = r(x)g(x) = 0$ dır. $der\big(r(x)\big) = 0$ veya $der\big(r(x)\big) < der\big(h(x)\big)$ olduğundan, bu bize C kodunun $g(x)$ tarafından üretilen bir çift δ_θ-devirli kod olduğunu ispatlar.

Örnek 3.2.5. $g_1(x) = (3+4u)x^2 + 3u$ ve $g_2(x) = x + 5 + 4u$ polinomları sırasıyla $g_1(x)|x^4-1$ ve $g_2(x)|x^2-1$ olacak şekilde polinomlar ve C, S üzerinde $\big(g_1(x)\big|g_2(x)\big)$ tarafından üretilen $n = 6(= 4+2)$ uzunluklu bir çift δ_θ-devirli kod olsun. $h(x)$, $h_1(x) = (3+4u)x^2 + 5u$ ve $h_2(x) = x + 3 + 4u$ polinomlarının en küçük sol ortak katı olsun. Teorem 2.2.10'da verilen sağ bölme algoritması yardımıyla, $h_1(x) = (3+4u)xh_2(x) + 7 + 5u$ olduğu elde edilir. Bu durumda, h_1 ile h_2 nin aralarında asal oldukları görülür. Dolayısıyla $der\big(h(x)\big) = 3$ olup, $\{g(x), xg(x), x^2g(x)\}$ kümesi C nin bir geren kümesidir. C nin üreteç matrisi aşağıdaki gibi elde edilir.

$$G = \begin{bmatrix} g(x) \\ xg(x) \\ x^2g(x) \end{bmatrix}$$

$$= \left[\begin{array}{ccc|c} g_{1_0} & g_{1_1} & g_{1_2} & 0 \\ \delta_\theta(g_{1_0}) & \theta(g_{1_0}) + \delta_\theta(g_{1_1}) & \theta(g_{1_1}) + \delta_\theta(g_{1_2}) & \theta(g_{1_2}) \\ g_{1_2} & 0 & g_{1_0} & g_{1_1} \end{array}\right| \left.\begin{array}{cc} g_{2_0} & g_{2_1} \\ \theta(g_{2_1}) + \delta_\theta(g_{2_0}) & \theta(g_{2_0}) + \delta_\theta(g_{2_1}) \\ g_{2_0} & g_{2_1} \end{array}\right]$$

$$= \left[\begin{array}{cccc|cc} 3u & 0 & 3+4u & 0 & 5+4u & 1 \\ 4+4u & 4+3u & 0 & 3+4u & 1 & 5+4u \\ 3+4u & 0 & 3u & 0 & 5+4u & 1 \end{array}\right].$$

4. Sonuç ve Öneriler

Bu çalışmada, $u^2 = 1$ olmak üzere $S = \mathbb{Z}_8 + u\mathbb{Z}_8$ halkası dikkate alınmıştır. θ, S üzerinde bir otomorfizm ve δ_θ bir türetim olmak üzere $S[x,\theta,\delta_\theta]$ aykırı polinom halkaları üzerindeki devirli kodların bazı cebirsel özellikleri araştırılmıştır. Ayrıca bu kodlar çift devirli kodlara genellenmiştir. Elde edilen sonuçlar yardımıyla, gelecekte kodlama teorisinde önemli bir araştırma problemi olan optimal kod bulma ile ilgili yeni araştırmalar yapılabilir.

Araştırma ve Yayın Etiği Beyanı

Yapılan çalışmada araştırma ve yayın etiğine uyulmuştur.

Kaynaklar

[1] Hammons A.R., Kumar P.V., Calderbank A.R., Sloane N.J.A., Solé P. 1994. The linearity of Kerdock, Preparata, Goethals, and Related Codes. IEEE Transactions on Information Theory, 40: 301-319.

[2] Cengellenmis Y. 2010. On the cyclic codes over $\mathbb{F}_3 + v\mathbb{F}_3$. International Journal of Algebra, 4 (6): 253-259.

[3] Dertli A., Cengellenmis Y. 2019. On the codes over the ring $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$ cyclic, constacyclic, quasi-cyclic codes, their skew codes, cyclic DNA and skew cyclic DNA codes. Prespacetime Journal, 10 (2): 196-213.

[4] Çalışkan B. 2020. Cylic codes over the ring $\mathbb{Z}_8 + u\mathbb{Z}_8 + v\mathbb{Z}_8$. International Conference on Mathematics and its Applications in Science and Engineering (ICMASE 2020), 9-10 July, Ankara, 7-12.

[5] Çalışkan B. 2020. Linear Codes over the Ring $\mathbb{Z}_8 + u\mathbb{Z}_8 + v\mathbb{Z}_8$. Conference Proceeding of 3rd International E-Conference on Mathematical Advances and Applications (ICOMAA 2020), 24-27 June, İstanbul, 19-23.

[6] Borges J., Fernández-Córdoba C., Ten-Valls R. 2018. $\mathbb{Z}_2$-double cyclic codes. Desings, Codes and Cryptography, 86: 463-479.

[7] Gao J., Shi M.J., Wu T.T. On double cyclic codes over $\mathbb{Z}_4$. Finite Fields and Their Applications, 39: 233-250.

[8] Boucher D., Geiselmann W., Ulmer F. 2007. Skew cyclic codes. Applicable Algebra in Engineering, Communication and Computing, 18(4): 379-389.

[9] Boucher D., Ulmer F. 2009. Coding with skew polynomial rings. Journal of Symbolic Computation, 44: 1644-1656.

[10] Sharma A., Bhaintwal M. 2017. A class of skew-constacyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$ with derivation. International Journal of Information and Coding Theory, 4 (4): 289-303.

[11] Carlet C. 1998. $\mathbb{Z}_{2^k}$ linear codes. IEEE Transactions on Information Theory, 44: 1543-1547.

[12] Dougherty S.T., Fernández-Córdoba C. 2011. Codes over $\mathbb{Z}_{2^k}$, gray map and self-dual codes. Advances in Mathematics Communications, 5: 571-588.