Avrupa Bilim ve Teknoloji Dergisi
Özel Sayı 28, S. 660-664, Kasım 2021

Araştırma Makalesi

www.ejosat.com ISSN:2148-2683

European Journal of Science and Technology
Special Issue 28, pp. 660-664, November 2021

Research Article

$\mathbb{Z}_8 + u\mathbb{Z}_8 + v\mathbb{Z}_8$ Üzerinde Aykırı Devirli Kodlar İçin Bazı Sonuçlar

Basri Çalışkan [1*]

[1*] Osmaniye Korkut Ata Üniversitesi, Fen Edebiyat Fakültesi, Matematik Bölümü, Osmaniye, Türkiye, (ORCID: 0000-0003-0512-4208), bcaliskan@osmaniye.edu.tr

(1st International Conference on Applied Engineering and Natural Sciences ICAENS 2021, November 1-3, 2021)

(**DOI:** 10.31590/ejosat.1010014)

ATIF/REFERENCE: Çalışkan, B. (2021). $\mathbb{Z}_8 + u\mathbb{Z}_8 + v\mathbb{Z}_8$ Üzerinde Aykırı Devirli Kodlar İçin Bazı Sonuçlar. *Avrupa Bilim ve Teknoloji Dergisi*, (28), 660-664.

Öz

Kodlama teorisinde, lineer kodların özel bir sınıfı olan devirli kodlar ile ilgili araştırmalar büyük ilgi görmektedir. Bu ilginin en önemli nedenlerinden bazıları devirli kodların zengin cebirsel özelliklere sahip olmaları, birçok uygulama alanlarının bulunması, kodlama ve kod çözmede kolaylık sağlamaları olarak sayılabilir. Devirli kodların sabit-devirli, parçalı devirli ve yarı burmalı devirli kodlar gibi genellemeleri bulunmaktadır. Bu genellemelerin çoğunda değişmeli yapılar üzerinde çalışılmıştır. Son zamanlarda devirli kodların değişmeli olmayan halkalardaki üreteç polinomları kullanılarak bir başka genellemesi (aykırı devirli kodlar) tanımlanmıştır. Aykırı polinom halkalarının cebirsel özellikleri nedeniyle, aykırı devirli kodlar optimal kod bulma açısından devirli kodlara göre daha avantajlıdır. Bu çalışmada, $u^2 = v^2 = uv = vu = 0$ olmak üzere $R = \mathbb{Z}_8 + u\mathbb{Z}_8 + v\mathbb{Z}_8$ halkası üzerinde tanımlı aykırı devirli kodlar dikkate alınmış ve bazı sonuçlar elde edilmiştir. θ, R üzerinde bir otomorfizm olmak üzere $R[x,\theta]$ aykırı polinom halkaları kullanılarak, θ-devirli kodlar tanımlanmıştır. $R[x,\theta]$ daki herhangi bir elemanın merkez eleman olabilmesi için gerek ve yeter koşul verilmiştir. R halkasının elemanları için Gray ağırlığı ve R nin θ tarafından sabit bırakılan alt halkası R^θ tanımlanmıştır. Ayrıca bu kodların üreteç ve kontrol matrislerinin formu belirlenmiş ve bazı örnekler verilmiştir.

Anahtar Kelimeler: Lineer kod, Aykırı devirli kod, Gray dönüşümü.

Some Results For Skew Cyclic Codes Over $\mathbb{Z}_8 + u\mathbb{Z}_8 + v\mathbb{Z}_8$

Abstract

In coding theory, researches on cyclic codes, which are special class of linear codes, have attracted great attention. Some of the most important reasons for this interest are that cyclic codes have rich algebraic properties, have many application areas, and provide convenience in coding and decoding. There are many generalizations of cyclic codes such as consta-cyclic codes, quasi-cyclic codes and quasi-twisted codes. In most of these generalizations, cyclic codes have been studied in commutative settings. Recently, another generalization of cyclic codes, skew cyclic codes, has been defined by using generator polynomials in non commutative polynomial rings. Since skew polynomial rings have algebraic properties, skew cyclic codes have more advantages than the cyclic codes for finding optimal codes. In this study, the ring $R = \mathbb{Z}_8 + u\mathbb{Z}_8 + v\mathbb{Z}_8$, where $u^2 = v^2 = uv = vu = 0$ is considered and some results which are obtained for the skew cyclic codes defined over the ring R. Using the skew polynomial rings $R[x,\theta]$ where θ is an automorphism on R, θ-cyclic codes are defined. Necessary and sufficient conditions are given for any element in $R[x,\theta]$ to be the central element. The Gray weight for the elements of the ring R and the subring R^θ of R fixed by θ are defined. Also, generator and parity-check matrisces of these codes are determined and given some examples.

Keywords: Linear cod, Skew cyclic code, Gray map.

[*] Sorumlu Yazar: bcaliskan@osmaniye.edu.tr

1. Giriş

Devirli kodlar, kodlama teorisindeki en önemli kod sınıfı olan lineer kodların bir alt sınıfıdır. Sonlu cisimler üzerindeki devirli kodlar üzerine birçok araştırma yapılmasına rağmen, Hammons ve ark. [1] de $\mathbb{Z}_4$ halkası üzerinde tanımlı lineer kod ailelerinin özel bir dönüşüm altındaki görüntülerinden Kerdock, Preparata gibi iyi hata düzeltme kabiliyetine sahip, lineer olmayan ikili (binary) kodlar elde etmişlerdir. Bu çalışma ile birlikte çeşitli halkalar üzerinde kod aileleri tanımlanması önem kazanmıştır [2],[3],[4].

Boucher ve ark. [5] de değişmeli olmayan halkalar kullanarak devirli kodların genellemesini yapmışlar, bu yeni kod ailesini aykırı devirli (skew cyclic) kodlar olarak adlandırmışlardır. Böylece devirli kodlar alanına yeni bir boyut kazandırmışlardır. Bu çalışmada, $\mathbb{F}_q$, q elemanlı bir cisim ve θ, $\mathbb{F}_q$ üzerinde bir otomorfizm olmak üzere $\mathbb{F}_q[x,\theta]$ aykırı (skew) polinom halkaları kullanılmıştır. $\mathbb{F}_q[x,\theta]$ 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 avantajlıdır. Boucher ve Ulmer [6] 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 [7] de $u^2=1$ 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. [8] nolu çalışmada, yazarlar $u^2=v^2=uv=vu=0$ olmak üzere, $\mathbb{Z}_4+u\mathbb{Z}_4+v\mathbb{Z}_4$ değişmeli halkası üzerindeki devirli ve sabit devirli kodları incelemişlerdir. Bu çalışmada, bu kod sınıflarının üreteç kümeleri araştırılmış ve devirli kodlar için minimum üreteç kümeleri belirlenmiştir. $\mathbb{Z}_4$ halkası ve onun genişlemeleri üzerine literatürde çok fazla çalışma bulunmasının yanında, $\mathbb{Z}_8$ halkası üzerindeki kodlar ile ilgili de bir çok çalışma bulunmaktadır [9],[10].

Yukarıda bahsedilen çalışmalardan motive olunarak, bu makalede $u^2=v^2=uv=vu=0$, $R=\mathbb{Z}_8+u\mathbb{Z}_8+v\mathbb{Z}_8$, ve θ, R üzerinde bir otomorfizm olmak üzere $R[x,\theta]$ aykırı polinom halkaları üzerindeki θ-devirli kodlar tanımlanmış, bu kodların bazı cebirsel özellikleri araştırılmıştır.

2. Materyal ve Metot

2.1. $\mathbb{Z}_8+u\mathbb{Z}_8+v\mathbb{Z}_8$ Halkası ve Gray Dönüşümü

$u^2=v^2=uv=vu=0$ olmak üzere $R=\mathbb{Z}_8+u\mathbb{Z}_8+v\mathbb{Z}_8$ değişmeli, karakteristiği 8 olan ve 512 elemanlı bir halkadır. R halkası $\frac{\mathbb{Z}_8[u]}{\langle u^2v^2,uv,vu,\rangle}$ bölüm halkasına izomorftur. R halkasının elemanları

$$R=\{a+ub+vc|a,b,c\in\mathbb{Z}_8\}$$

$d=a+ub+vc\in R$ şeklinde tek türlü yazılır. $a+ub+vc$ elemanı R de birim eleman olsun. Bu durumda

$$(a+ub+vc)(\alpha+u\beta+v\gamma)=1$$

olacak şekilde, en az bir $\alpha+u\beta+v\gamma\in R$ elemanı vardır. Buradan, $a\alpha=1$ olduğu elde edilir. Bu ise, $a\in\mathbb{Z}_8$ nin birim olmasını gerektirir.

Tersine, $a\in\mathbb{Z}_8$ birim olsun. Bu durumda

$$(a+ub+vc)(a^{-1}-a^{-1}uba^{-1}-a^{-1}vca^{-1})=1$$

olup, $a+ub+vc\in R$ elemanının birim olduğu elde edilir. Böylece, R nin birimleri aşağıda verilen lemma ile karakterize edilebilir.

Lemma 2.1. R nin birimlerinin kümesi

$$\{a'+ub+vc|a',\mathbb{Z}_8 \text{ de birim}, b,c\in\mathbb{Z}_8\}$$

dir.

R nin 256 tane birimi ve 256 tane de birim olmayan elemanı vardır. $\langle 2,u\rangle$ ve $\langle 2,v\rangle$ idealleri dikkate alınırsa, R nin $\mathbb{Z}_8$ in zincir olmayan bir genişlemesi olduğu görülür. Ayrıca, $\langle 2,u\rangle$ ideali tek bir eleman tarafından üretilmediği için R bir esas ideal halkası değildir. Son olarak, $\langle 2,u,v\rangle$ maksimal ideali ile R bir lokal Frobenius halkasıdır.

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

$$\theta(a+ub+vc)=a+vb+uc$$

şeklinde tanımlansın. $d=a+ub+vc$ ve $d'=a'+ub'+vc'\in R$ olsun.

$$\begin{aligned}\theta(d+d')&=\theta\big((a+ub+vc)+(a'+ub'+vc')\big)\\&=\theta\big(a+a'+u(b+b')+v(c+c')\big)\\&=a+a'+u(c+c')+v(b+b')\\&=a+uc+vb+a'+uc'+vb'\\&=\theta(d)+\theta(d')\end{aligned}$$

$$\begin{aligned}\theta(dd')&=\theta\big((a+ub+vc)(a'+ub'+vc')\big)\\&=\theta\big(aa'+u(ab'+ba')+v(ac'+ca')\big)\\&=aa'+u(ac'+ca')+v(ab'+ba')\end{aligned}$$

$$\begin{aligned}\theta(d)\theta(d')&=\theta(a+ub+vc)\theta(a'+ub'+vc')\\&=(a+uc+vb)(a'+uc'+vb')\\&=aa'+u(ac'+ca')+v(ab'+ba')\end{aligned}$$

elde edilir. Açıkça görülebilir ki θ, R halkasının aşikar olmayan bir otomorfizmidir. Ayrıca, her $d=a+ub+vc\in R$ için

$$\begin{aligned}\theta^2(a+ub+vc)&=\theta\big(\theta(a+ub+vc)\big)\\&=\theta(a+uc+vb)\\&=a+ub+vc\end{aligned}$$

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

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

$$\phi: \mathbb{Z}_{2^s} \to \mathbb{Z}_2^{2^{s-1}}$$

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

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. Ayrıca, Bir $e \in \mathbb{Z}_8^n$ vektörü için Lee ağırlığı $w_L(e)$, e nin koordinatlarının Lee ağırlıklarının toplamı olarak tanımlanır. [12].

Tanım 2.1. $\varphi: R \to \mathbb{Z}_8^3$ dönüşümü $\varphi(a + ub + vc) = (a, a+b, a+c)$ olmak üzere, herhangi bir $d \in R$ için d nin Gray ağırlığı, $w_G(d) = w_L(\varphi(d))$ olarak tanımlanır.

3. Araştırma Sonuçları ve Tartışma

3.1. $R[x, \theta]$ Aykırı Polinom Halkası

Tanım 3.1. R, θ otomorfizmi ile bir halka olsun. R üzerindeki tüm polinomların kümesi

$$R[x, \theta] = \{a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}\},$$

polinomların bilinen toplaması ve herhangi $d \in R$ olmak üzere

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

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

Örnek 3.1. $p = x^2 + (1+u+v)x + u + v$ ve $q = x + 7 + 3u + 5v$ olsun.

$$pq = [x^2 + (1+u+v)x + u + v][x + 7 + 3u + 5v\,]$$
$$= x^3 + (4u+6v)x^2 + (1+5u+3v)x + 7u + 7v$$

$$qp = [x + 7 + 3u + 5v\,][x^2 + (1+u+v)x + u + v]$$
$$= x^3 + (4u+6v)x^2 + (7+2u+4v)x + 7u + 7v$$

açıkça görülmektedir ki, pq polinomundaki x li terimin katsayısı ile ve qp polinomundaki x li terimin katsayısı farklıdır. Dolayısıyla $pq \neq qp$ olduğundan $R[x, \theta]$, değişmeli olmayan bir halkadır.

Lemma 3.1. $R^\theta = \{\alpha + u\beta + v\gamma | \alpha, \beta, \gamma \in \mathbb{Z}_8, \beta = \gamma\}$ olmak üzere, her $e \in R^\theta$ için $\theta(e) = e$ olacak şekildeki elemanların kümesi R^θ, R nin θ tarafından sabit bırakılan bir alt halkasıdır.

Tanım 3.2. $p(x) \in R[x, \theta]$ olsun. Her $d(x) \in R[x, \theta]$ için $p(x)d(x) = d(x)p(x)$ oluyorsa, $p(x)$ polinomuna $R[x, \theta]$ nin bir merkez elemanı denir [7].

Teorem 3.2. $center(R) = \left\{\sum_{i=0}^{l} d_i x^{2i} \,\middle|\, d_i \in R^\theta\right\}$ dır.

İspat: $D = \left\{\sum_{i=0}^{l} d_i x^{2i} \,\middle|\, d_i \in R^\theta\right\}$ ve $p = \sum_{i=0}^{l} d_i x^{2i} \in D$ olsun. Negatif olmayan herhangi bir i ve her $d_i \in R$ için, θ nın mertebesi 2 olduğundan

$$x^{2i}d_i = (\theta^2)^i(d_i)x^{2i} = d_i x^{2i}$$

olduğu elde edilir. Bu $x^{2i} \in center(R)$ olmasını gerektirir. Dolayısıyla

$$p = d_0 + d_1 x^2 + \cdots + d_l x^{2l}$$

formundaki tüm polinomların $center(R)$ olduğunu gösterir.

Tersine, $p = p_0 + p_1 x + \cdots + p_k x^k \in center(R)$ olsun. Bu durumda $xp = px$ dir. Dolayısıyla, tüm p_i ler θ tarafından sabit bırakılır ve $p_i \in R^\theta$ dır. Ayrıca, $\theta(d_i) \neq d_i$ olacak şekilde bir $d_i \in R$ olarak seçilirse, $d_i p = p d_i$ bağıntısından 2 ile bölünemeyen tüm i indisleri için $p_i = 0$ olur. Dolayısıyla,

$$p = p_0 + p_2 x^2 + p_4 x^4 + \cdots + p_l x^{2l} \in D$$

elde edilir. Buradan $center(R) \subseteq D$ olduğundan, ispat tamamlanır.

Sonuç 3.1. $p(x) = x^m - 1$ olsun. $p(x) \in center(R)$ olabilmesi için gerek ve yeter koşul $2|m$ olmasıdır.

Sonuç 3.1, eğer m çift ise $R[x, \theta] \,/\, \langle x^m - 1 \rangle$ nin bir halka olduğunu ve $x^m - 1$ polinomunun $R[x, \theta]$ halkasının merkezi $center(R)$ de olduğunu göstermektedir. Dolayısıyla, $x^m - 1$ nin iki taraflı bir ideal üretebilmesi için $2|m$ olması gereklidir. Aksi durumda $R[x, \theta] \,/\, \langle x^m - 1 \rangle$ sadece bir R-modül olacaktır.

Örnek 3.2. $p(x) = (u+v)x^2 + 3$ ve $q(x) = (u+v)x$ olsun. Bu durumda

$$p(x) = xq(x) + 3$$

$$p(x) = (1 + 5u + 6v)xq(x) + 3$$

olarak yazılabilir. Açıkça görülmektedir ki, $x \neq (1+5u+6v)x$ ve $der(3) < der\big((1+5u+6v)x\big)$ dir. Dolayısıyla, $R[x, \theta]$ bir Euclidean halka değildir, bu nedenle hem sağ hem de sol bölme algoritması bu halkada sağlanmaz. Aşağıdaki teorem hem sağ hem de sol bölme algoritmasının $R[x, \theta]$ bazı elemanları için uygulanabileceğini göstermektedir.

Teorem 3.3. (Sağ Bölme Algoritması) $f(x)$ ve $g(x)$ polinomları $g(x)$ in baş katsayısı birim olacak şekilde $R[x, \theta]$ 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 $q(x), r(x) \in R[x, \theta]$ vardır [7].

3.2. $\mathbb{Z}_8 + u\mathbb{Z}_8 + v\mathbb{Z}_8$ Üzerinde Aykırı Devirli Kodlar

Bu bölümde, θ-devirli kodlar olarak adlandıracağımız, R üzerinde aykırı devirli kodlar çalışılmıştır.

Bilindiği üzere, R^n nin boş olmayan bir alt kümesine R üzerinde bir kod denir. C, R üzerinde bir kod olmak üzere eğer

C, R^n nin bir R-alt modülü oluyorsa C ye R üzerinde bir lineer kod denir.

Tanım 3.3. θ, R üzerinde bir otomorfizm ve $(d_0, d_1, \dots, d_{n-1}) \in R^n$ olmak üzere, $\sigma_\theta: R^n \to R^n$ ye

$$\sigma_\theta(d_0, d_1, \dots, d_{n-1}) = \big(\theta(d_{n-1}), \theta(d_0), \dots, \theta(d_{n-2})\big)$$

şeklinde tanımlı devirsel öteleme operatörü olsun. Eğer bir C kodu, σ_θ devirsel öteleme altında kapalı ise, C ye bir θ-devirli kod denir.

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

Teorem 3.4. $R_{n,\theta} = \frac{R[x,\theta]}{\langle x^n - 1\rangle}$ üzerinde n uzunluklu bir C kodunun θ-devirli kod olabilmesi için gerek ve yeter koşul C nin $R_{n,\theta}$ nın bir $R[x,\theta]$-alt modülü olmasıdır.

İspat. C nin $R_{n,\theta}$ üzerinde n uzunluklu bir θ-devirli kod olduğunu kabul edelim. $u(x) = u_0 + u_1 x + \cdots + u_{n-1}x^{n-1}$ ve $v(x) = v_0 + v_1 x + \cdots + v_{n-1}x^{n-1} \in C$ olsun. C bir linear kod olduğundan, $u + v \in C$ dir. Ayrıca, her $i \in \mathbb{N}$ için, C devirli olduğundan $x^i u(x) \in C$ dir. Bu ise, tüm $p(x) \in R_{n,\theta}$ polinomları için $p(x)u(x) \in C$ olması demektir. Dolayısıyla, C, $R_{n,\theta}$ nın bir $R[x,\theta]$-alt modülüdür. Şimdi ise, C nin $R_{n,\theta}$ nın bir $R[x,\theta]$-alt modülü olduğunu kabul edelim. $u, v \in C$ olsun. Alt modül tanımından $u + v \in C$ ve $x^i u(x) \in C$ elde edilir. Dolayısıyla, C bir θ-devirli koddur.

Sonuç 3.2. Eğer C, n çift tamsayı uzunluklu bir θ-devirli kod ise, C, $R_{n,\theta}$ nin bir idealidir.

İspat. n bir çift tamsayı olsun. Bu durumda, $\langle x^n - 1\rangle$ iki taraflı bir ideal olur, dolayısıyla $\frac{R[x,\theta]}{\langle x^n-1\rangle}$ bir halkadır.

Teorem 3.5. C, R üzerinde n uzunluklu bir θ--devirli kod ve C de, baş katsayısı birim olan minimum dereceli bir $g(x)$ polinomu bulunsun. Bu durumda $C = \langle g(x)\rangle$ 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 bazıdır.

İspat. [7] Theorem 14 ün 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 R üzerinde bir 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

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

ve $n-k$ tek ise

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

şeklindedir.

Örnek 3.3. $x^6 - 1 = [(1 + 7u + 7v)\,x^3 + (4u + 4v)\,x^2 + 4x + 7 + u + v][(1 + u + v)x^3 + (4u + 4v)x^2 + 4x + 1 + u + v]$ olmak üzere, C, $x^6 - 1$ in sağ böleni $g(x) = (1 + u + v)x^3 + (4u + 4v)x^2 + 4x + 1 + u + v$ polinomu tarafından üretilen 6 uzunluklu bir θ-devirli kod olsun. Bu durumda $\{g(x), xg(x), x^2 g(x)\}$ kümesi C kodu için bir bazdır. C nin kardinalitesi $|C| = 2^{27}$ olup, C nin üreteç matrisi

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

$$= \begin{bmatrix} g_0 & g_1 & g_2 & g_3 & 0 & 0 \\ 0 & \theta(g_0) & \theta(g_1) & \theta(g_2) & \theta(g_3) & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & g_3 \end{bmatrix}$$

$$= \begin{bmatrix} 1+u+v & 4 & 4u+4v & 1+u+v & 0 & 0 \\ 0 & 1+u+v & 4 & 4u+4v & 1+u+v & 0 \\ 0 & 0 & 1+u+v & 4 & 4u+4v & 1+u+v \end{bmatrix}$$

. Ayrıca, G üreteç matrisinin Gray görüntüsü

$$\begin{bmatrix} 122 & 444 & 044 & 122 & 000 & 000 \\ 000 & 122 & 444 & 044 & 122 & 000 \\ 000 & 000 & 122 & 444 & 044 & 122 \end{bmatrix}$$

olup, $\varphi(C)$, $(18, 8^9, 2)$ parametrelerine sahip bir koddur.

Tanım 3.4. C, R üzerinde n uzunluklu bir θ-devirli kod olsun.

$$w = (w_0, w_1, \dots, w_{n-1}), v = (v_0, v, \dots, v_{n-1}) \in R^n$$

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 3.6. k bir tek tamsayı ve en az bir $h(x) = h_0 + h_1 x + h_2 x^2 + \cdots + h_k x^k \in R[x,\theta]$ için $x^n - 1 = h(x)g(x)$ olsun. Eğer $C = \langle g(x)\rangle$ uzunluğu çift tamsayı n olan R üzerinde bir θ-devirli kod ise C nin kontrol matrisi

$$H = \begin{bmatrix} h_k & \theta(h_{k-1}) & h_{k-2} & \cdots & h_1 & \theta(h_0) & 0 & \cdots & 0 \\ 0 & \theta(h_k) & h_{k-1} & \cdots & h_2 & \theta(h_1) & h_0 & \cdots & 0 \\ 0 & 0 & h_k & \cdots & h_3 & \theta(h_2) & h_1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & h_k & \theta(h_{k-1}) & h_{k-2} & \cdots & \theta(h_0) \end{bmatrix}$$

formundadır. k bir çift tamsayı olduğunda H matrisi

$$H = \begin{bmatrix} h_k & \theta(h_{k-1}) & h_{k-2} & \cdots & h_1 & \theta(h_0) & 0 & \cdots & 0 \\ 0 & \theta(h_k) & h_{k-1} & \cdots & h_2 & \theta(h_1) & h_0 & \cdots & 0 \\ 0 & 0 & h_k & \cdots & h_3 & \theta(h_2) & h_1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \theta(h_k) & h_{k-1} & \theta(h_{k-2}) & \cdots & h_0 \end{bmatrix}$$

şeklindedir.

İspat. [7] Theorem 4.5 in ispatının benzeridir.

Örnek 3.4. Örnek 3.3'te verilen C kodu için kontrol polinoumu $h(x) = (1 + 7u + 7v)\,x^3 + (4u + 4v)\,x^2 + 4x + 7 + u + v$ dir. Bu durumda Teorem 3.6'dan dolayı, C nin kontrol matrisi

$$\begin{bmatrix} 7+u+v & 4 & 4u+4v & 1+7u+7v & 0 & 0 \\ 0 & 7+u+v & 4 & 4u+4v & 1+7u+7v & 0 \\ 0 & 0 & 7+u+v & 4 & 4u+4v & 1+7u+7v \end{bmatrix}$$

şeklindedir.

4. Sonuç

Bu çalışmada, $u^2 = v^2 = uv = vu = 0$ olmak üzere $R = \mathbb{Z}_8 + u\mathbb{Z}_8 + v\mathbb{Z}_8$ halkası üzerindeki aykırı devirli kodlar tanıtılmıştır. θ, R üzerinde bir otomorfizm olmak üzere $R[x, \theta]$ aykırı polinomlar halkası kullanılarak θ-devirli kodların bazı cebirsel özellikleri araştırılmıştır. Elde edilen sonuçlar yardımıyla, kodlama teorisinde önemli bir araştırma problemi olan optimal kod bulmak ile ilgili yeni araştırmalar yapılabilir.

Kaynakça

[1] Hammons, A. R., Kumar, P. V, Calderbank, A. R., Sloane, N. J. A. and Solé, P., (1994), The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and Related Codes, IEEE Transactions on Information Theory, vol. 40, pp. 301-319.

[2] Çalışkan, B. and Balıkçı, K., (2019), Counting $\mathbb{Z}_2\mathbb{Z}_4\mathbb{Z}_8$ - additive codes, European Journal of Pure and Applied Mathematics, vol. 12, no. 2, pp. 668-679.

[3] Çalışkan, B. ve Özkan, Ö., (2020), Serbest $\mathbb{Z}_2\mathbb{Z}_4\mathbb{Z}_8$-Toplamsal Kodları Sayma, Erzincan Üniversitesi Fen Bilimleri Enstitüsü Dergisi, vol. 13, pp. 70 -75.

[4] Çalışkan, B., (2021), On one-weight and acd codes in $\mathbb{Z}_2^r \times \mathbb{Z}_4^s \times \mathbb{Z}_8^t$, Filomat, vol. 35(3).

[5] Boucher, D. Geiselmann, W. and Ulmer, F., (2007), Skew Cyclic Codes, Applicable Algebra in Engineering, Communication and Computing, vol. 18, no. 4, pp. 379-389.

[6] Boucher, D. and Ulmer, F., (2009), Coding with Skew Polynomial Rings, Journal of Symbolic Computation, vol. 44, pp. 1644-1656.

[7] Sharma, A. and Bhaintwal, M., (2017), A class of skew-constacyclic codes over $\mathbb{Z}_4 + \mathrm{u}\mathbb{Z}_4$ with derivation, International Journal of Information and Coding Theory, vol. 4, no. 4, pp. 289-303.

[8] Islam, H. and Parakash, O., (2018), A study of cyclic and constacyclic codes over $\mathbb{Z}_4 + \mathrm{u}\mathbb{Z}_4 + \mathrm{v}\mathbb{Z}_4$, Int. J. of Information and Coding Theory, vol. 5, pp. 155-168.

[9] Dougherty, S.T., Gulliver, T.A. and Wong, J., (2006), Self-dual codes over $\mathbb{Z}_8$ and $\mathbb{Z}_9$, Des. Codes Crypt., vol. 41, pp. 235-249.

[10] Çalışkan, B., (2020), Linear Codes over the Ring $\mathbb{Z}_8 + \mathrm{u}\mathbb{Z}_8 + \mathrm{v}\mathbb{Z}_8$, Conference Proceeding Science and Technology, vol. 3, no. 1, pp. 19-23.

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

[12] Dougherty, S.T. and Fernández-Córdoba, C., (2011), Codes over $\mathbb{Z}_{2^k}$, gray map and self-dual codes, Adv. Math. Commun., vol. 5, pp. 571-588.