e-ISSN 2757-5195

Çanakkale Onsekiz Mart University
Journal of Advanced Research in Natural and Applied Sciences
Open Access

doi.org/10.28979/jarnas.941782 2022, Cilt 8, Sayı 1, Sayfa: 114-123 dergipark.org.tr/tr/pub/jarnas

Türetim ile $\mathbb{Z}_2s+u\mathbb{Z}_2s$ Halkası Üzerinde Aykırı Devirli Kodlar

Basri Çalışkan[1*]

[1]Matematik Bölümü, Fen Edebiyat Fakültesi, Osmaniye Korkut Ata Üniversitesi, Osmaniye, Türkiye

Makale Tarihçesi
Gönderim: 24.05.2021
Kabul: 08.09.2021
Yayım: 10.03.2022
Araştırma Makalesi

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 $u^2=1$ olmak üzere $\mathbb{Z}_4+u\mathbb{Z}_4$ halkası üzerinde tanımlı aykırı devirli kodlar için elde edilmiş bazı sonuçların $s\geq 2$ için $S=\mathbb{Z}_2s+u\mathbb{Z}_2s$ halkası için genellemesi yapılmıştır. θ, S üzerinde bir otomorfizm ve δ_θ, S üzerinde bir türetim olmak üzere $S[x,\theta,\delta_\theta]$ aykırı polinom halkaları kullanılarak, δ_θ-devirli kodlar tanımlanmıştır. $S[x,\theta,\delta_\theta]$ daki herhangi bir elemanın merkez eleman olabilmesi için gerek ve yeter koşul verilmiştir. δ_θ dönüşümü ile S halkasının tüm elemanlarının görüntüleri elde edilmiş ve tanımlanan Gray dönüşümü ile S halkasının elemanları için Gray ağırlığı ile S nin θ tarafından sabit bırakılan alt halkası S^θ tanımlanmıştır. Ayrıca bu kodların üreteç ve kontrol matrislerinin formu belirlenmiş ve özellikle $s=4$ için bazı örnekler verilmiştir.

Anahtar Kelimeler – *Aykırı devirli kod, aykırı polinom halkası, devirli kod, Gray dönüşümü, türetim*

Skew Cyclic Codes over the Ring $\mathbb{Z}_2s+u\mathbb{Z}_2s$ with Derivation

[1]Department of Mathematics, Faculty of Arts and Science, Osmaniye Korkut Ata University, Osmaniye, Turkey

Article History
Received: 24.05.2021
Accepted: 08.09.2021
Published: 10.03.2022
Research Article

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 may 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, some results which are obtained for the skew cyclic codes defined over the ring $\mathbb{Z}_4+u\mathbb{Z}_4$ with $u^2=1$ are generalized for the ring $S=\mathbb{Z}_2s+u\mathbb{Z}_2s$, where $u^2=1$, $s\geq 2$. Using the skew polynomial rings $S[x,\theta,\delta_\theta]$ where θ is an automorphism on S and δ_θ is a derivation on S, δ_θ-cyclic codes are defined. Necessary and sufficient conditions are given for any element in $S[x,\theta,\delta_\theta]$ to be the central element. The image of all elements of the ring S are obtained with the mapping δ_θ and the Gray weight is defined for the elements of the ring S with the defined Gray map. The subring S^θ of S fixed by θ is defined. Also, generator and parity-check matrisces of these codes are determined and given some examples especially for the case $s=4$.

Keywords – *Cyclic code, derivation, Gray map, skew cyclic code, skew polynomial ring*

[1] bcaliskan@osmaniye.edu.tr
*Sorumlu Yazar / Corresponding Author

1. Giriş

Sonlu cisimler üzerindeki devirli kodlar üzerine birçok araştırma yapılmasına rağmen, Hammons, Kumar, Calderbank, Sloane ve Solé, (1994) 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 ailelerinin tanımlanması önem kazanmıştır (Cengellenmis, 2010; Çalışkan, 2020a; Çalışkan, 2020b; Dertli ve Cengellenmis, 2019).

Boucher, Geiselmann ve Ulmer (2007) 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, $\mathbb{F}_q$ cisimi üzerinde bir otomorfizm olmak üzere $\mathbb{F}_q[x,\theta]$ aykırı (skew) polinom halkaları kullanılmıştır. 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 avantajlıdır. Boucher ve Ulmer (2009) 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 (2018) de, olmak üzere 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 (double) kodlara genellemişlerdir.

Yukarıda bahsedilen çalışmalardan motive olunarak, bu makalede özellikle Sharma ve Bhaintwal (2018) de, elde edilen bazı sonuçların için olmak üzere halkası üzerindeki aykırı devirli kodlara bir genellemesi yapılmıştır.

2. Materyal ve Yöntem

2.1. S[x,θ,Δθ] Aykırı Polinom Halkası

s≥2 ve $u^2=1$ olmak üzere $S=\mathbb{Z}_2s+u\mathbb{Z}_2s$ değişmeli ve karakteristiği 2^S olan bir halkadır. S halkası $\frac{\mathbb{Z}_2s[u]}{\langle u^2-1\rangle}$ bölüm halkasına izomorftur. S halkasının elemanları, 2.1'de

$$S=\{a+ub|a,b\in\mathbb{Z}_{2^s}\} \tag{2.1}$$

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

$\theta: S\to S, a,b\in\mathbb{Z}_{2^s}$ olmak üzere, dönüşümü 2.2'de

$$\theta(a+ub)=a+(u+2^{s-1})b \tag{2.2}$$

şeklinde tanımlansın. Açıkça görülebilir ki θ, S halkasının aşikar olmayan bir otomorfizmidir. Ayrıca, her $d=a+ub\in S$ için, 2.3'ten $\theta^2(d)$ dir.

$$\begin{aligned}\theta^2(a+ub)&=\theta\big(\theta(a+ub)\big)\\&=\theta(a+(u+2^{s-1})b)\\&=\theta(a+2^{s-1}b+ub)\\&=a+2^{s-1}b+(u+2^{s-1})b\\&=a+2^{s-1}b+2^{s-1}b+ub\\&=a+2^sb+ub\\&=a+ub\end{aligned} \tag{2.3}$$

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 2.4 ve 2.5'te verilen özellikleri sağlayan dönüşümüne üzerinde bir türetim denir.

$$\Delta_\theta(x+y) = \Delta_\theta(x) + \Delta_\theta(y) \tag{2.4}$$

ve

$$\Delta_\theta(xy) = \Delta_\theta(x)y + \theta(x)\Delta_\theta(y). \tag{2.5}$$

Teorem 2.1.2 $\delta_\theta: S \to$ S, dönüşümü $\delta_\theta(a+ub) = (1+u)[\theta(a+ub) - (a+ub)]$ olarak tanımlansın. Yani, 2.6'daki gibi

$$\begin{aligned}\delta_\theta(a+ub) &= (1+u)[\theta(a+ub) - (a+ub)] \\ &= (1+u)[a + 2^{s-1}b + ub - a - ub] \\ &= (1+u)2^{s-1}b \\ &= 2^{s-1}b + 2^{s-1}ub\end{aligned} \tag{2.6}$$

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

KANIT: Sharma ve Bhaintwal (2018), Theorem 2.2 nin ispatının benzeridir.

2.7'de δ_θ dönüşümü altındaki S halkasının elemanlarının görüntüleri verilmiştir.

$$\delta_\theta(a+ub) = \begin{cases} 0, & b \text{ birim değilse} \\ 2^{s-1} + 2^{s-1}u, & b \text{ birim ise}. \end{cases} \tag{2.7}$$

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

KANIT: $n \geq 2$ bir tamsayı ve $d = a + ub \in S$ için 2.8'de

$$\begin{aligned}\delta_\theta^2(a+ub) &= \delta_\theta\big(\delta_\theta(a+ub)\big) \\ &= \delta_\theta(2^{s-1}b + 2^{s-1}ub) \\ &= 2^{s-1}(2^{s-1}b) + 2^{s-1}(2^{s-1}b)u \\ &= 2^s(2^{s-2}b) + 2^s(2^{s-2}b)u \\ &= 0\end{aligned} \tag{2.8}$$

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 (Hammons vd., 1994).

Carlet, bu Gray dönüşümünü $\mathbb{Z}_{2^s}$ üzerinde 2.9'daki gibi genelleştirmiştir (Carlet, 1998). $\phi: \mathbb{Z}_{2^s} \to \mathbb{Z}_2^{2^{s-1}}$

$$\phi(i) = \begin{cases} 0_{2^{s-1}-i}1_i, & 0 \leq i \leq 2^{s-1} \\ 1_{2^{s-1}} + \phi(i - 2^{s-1}), & i > 2^{s-1} \end{cases} \tag{2.9}$$

Burada 0_t, bütün bileşenleri 0 olan t uzunluklu vektörü ve 1_t de bütün bileşenleri 1 olan t 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. Örneğin s = 4 için $\mathbb{Z}_{16}$ nın elemanlarının görüntüleri 2.10'daki gibidir.

$$
\begin{aligned}
&\phi: \mathbb{Z}_{2^4} \to \mathbb{Z}_2^8 \\
&\phi(0) = (00000000), \quad \phi(1) = (00000001), \quad \phi(2) = (00000011), \\
&\qquad \phi(3) = (00000111), \\
&\phi(4) = (00001111), \quad \phi(5) = (00011111), \quad \phi(6) = (00111111), \\
&\qquad \phi(6) = (01111111), \\
&\phi(8) = (11111111), \quad \phi(9) = (11111110), \quad \phi(10) = (11111100), \\
&\qquad \phi(11) = (11111000), \\
&\phi(12) = (11110000), \quad \phi(13) = (11100000), \quad \phi(14) = (11000000), \quad \phi(15) = (1000000).
\end{aligned}
\tag{2.10}
$$

$\mathbb{Z}_{2^s}$ üzerindeki Lee ağırlığı, $w_L: \mathbb{Z}_{2^s} \to \mathbb{Z}_{2^s}$, $w_L(x) = min(x, 2^s - x)$ biçiminde tanımlanır (Dougherty ve Fernández-Córdoba, 2011).

Tanım 2.2.4 Bir $d \in \mathbb{Z}_{2^s}^2$ vektörü için Lee ağırlığı $w_L(d)$, d nin koordinatlarının Lee ağırlıklarının toplamı olarak tanımlanır. $\varphi: S \to \mathbb{Z}_{2^s}^2$ dönüşümü $\varphi(a + ub) = (b, a + b)$ olmak üzere, herhangi bir $v \in S$ için v nin Gray ağırlığı, $w_G(v) = w_L(\varphi(v))$ olarak tanımlanır.

3. Bulgular ve Tartışma

Tanım 3.5 S, θ otomorfizmi ve Δ_θ türetimi ile bir halka olsun. S üzerindeki tüm polinomların kümesi polinomların bilinen toplaması ve herhangi olmak üzere $d \in S$ 3.1'de

$$xd = \theta(d)x + \Delta_\theta(d) \tag{3.1}$$

şeklinde tanımlanan çarpma işlemi ile aykırı polinom halkası olarak adlandırılır. Tanımlanan bu çarpma işlemi S[x,θ,Δθ] nın tüm elemanları için genişletilebilir.

Örnek 3.6 $p_1 = x + d_0$ ve $p_2 = e_0$, $S[x, \theta, \delta_\theta]$ halkasında herhangi iki polinom olsun. Bu durumda 3.2'de

$$p_1 + p_2 = x + d_0 + e_0 = p_1 + p_2 \tag{3.2}$$

ve

$$
\begin{aligned}
p_1 p_2 &= (x + d_0)e_0 \\
&= xe_0 + d_0 e_0 \\
&= \theta(e_0)x + \delta_\theta(e_0) + d_0 e_0
\end{aligned}
\tag{3.3}
$$

$$
\begin{aligned}
p_2 p_1 &= e_0(x + d_0) \\
&= e_0 x + e_0 d_0
\end{aligned}
\tag{3.4}
$$

3.3 ve 3.4'teki çarpımlardan, x li terimlerin katsayıları sırasıyla θ (e_0) ve e_0 olup, S de her zaman θ (e_0)= e_0 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 3.7 $S^{\theta} = \{a' + ub' | a' \in \{0,1,\dots,2^s - 1\}, b' \equiv 2k \ (mod\ 2^s), k = 0,1,\dots,2^{s-1} - 1\}$ olmak üzere, her $e \in S^{\theta}$ için $\theta(e) = e$ olacak şekildeki elemanların kümesi S^{θ} ya S nin θ nin tarafından sabit bırakılan bir alt halkası denir. Ayrıca, her için olup, $e \in S^{\theta}$ için $\delta_{\theta}(e) = 0$ olup, $xe = ex$ dir.

Tanım 3.8 $p(x) \in S[x, \theta, \delta_{\theta}]$ 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 3.9 $d \in S$ 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.

KANIT: Sharma ve Bhaintwal (2018) 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 $2^{s-1} + 2^{s-1}u$ olduğu bilinmektedir. $\delta_{\theta}(e) = 0$ ise d ve e nin her ikisi de θ tarafından sabit bırakıldığı görülür ve istenen elde edilmiş olur. $\delta_{\theta}(e) = 2^{s-1} + 2^{s-1}u$ olduğunu kabul edelim. Bu durumda, ifadesinde $\theta(d) - d = a + (u + 2^{s-1})b - a - ub = 2^{s-1}b$ ifadesinde u bulunmaz, o zaman bir çelişki elde ederiz. Dolayısıyla ispat tamamlanmış olur.

Teorem 3.10 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 tüm tek dereceli terimlerinin katsayılarının 3.5'teki

$$\{\alpha + u\beta | \alpha, \beta \equiv 2k \ (mod\ 2^s), k = 0,1,2,\dots,2^{s-1} - 1\} \tag{3.5}$$

kümesine ait olmasıdır.

KANIT: Sharma ve Bhaintwal (2018), Theorem 2.6 da s=2 için yapılan ispatın benzeridir.

Lemma 3.11 Herhangi bir $d \in S$ için $\delta_{\theta}\big(\theta(d)\big) + \theta\big(\delta_{\theta}(d)\big) = 0$ dır. Ayrıca her $d \in S$ için $x^2 d = dx^2$ dir.

KANIT: Sharma ve Bhaintwal (2018) Lemma 2.7.'nin ispatının benzeridir. $d = a + ub \in S$ olsun. O zaman $\theta(a + ub) = a + (u + 2^{s-1})b$ ve $\delta_{\theta}(a + ub) = 2^{s-1}b + 2^{s-1}bu$ olduğundan, 3.6 ve 3.7'den

$$\begin{aligned} \delta_{\theta}\big(\theta(d)\big) &= \delta_{\theta}\big(\theta(a + ub)\big) \\ &= \delta_{\theta}(a + (u + 2^{s-1})b) \\ &= \delta_{\theta}(a + 2^{s-1}b + ub) \\ &= 2^{s-1}b + 2^{s-1}bu \end{aligned} \tag{3.6}$$

ve

$$\begin{aligned} \theta\big(\delta_{\theta}(d)\big) &= \theta\big(\delta_{\theta}(a + ub)\big) \\ &= \theta(2^{s-1}b + 2^{s-1}bu) \\ &= 2^{s-1}b + (u + 2^{s-1})2^{s-1}b \\ &= 2^{s-1}b + 2^{s-1}2^{s-1}b + 2^{s-1}bu \\ &= 2^{s-1}b + 2^{s}(2^{s-2}b) + 2^{s-1}bu \\ &= 2^{s-1}b + 2^{s-1}bu \\ &= -(2^{s-1}b + 2^{s-1}bu) \\ &= -\delta_{\theta}\big(\theta(d)\big) \end{aligned} \tag{3.7}$$

olduğundan, $\delta_{\theta}\big(\theta(d)\big) + \theta\big(\delta_{\theta}(d)\big) = 0$ eşitliği gösterilmiş olur. Şimdi, $xd = \theta(d)x + \delta_{\theta}(d)$ eşitliğini soldan x ile çarpalım, 3.8'den

$$\begin{aligned} x^2d &= x\theta(d)x + x\delta_\theta(d) \\ &= \left[\theta^2(d)x + \delta_\theta\big(\theta(d)\big)\right]x + \theta\big(\delta_\theta(d)\big)x + {\delta_\theta}^2(d) \\ &= dx^2 + \left[\delta_\theta\big(\theta(d)\big) + \theta\big(\delta_\theta(d)\big)\right]x + {\delta_\theta}^2(d) \\ &= dx^2 \end{aligned} \tag{3.8}$$

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

Sonuç 3.12 Herhangi bir için, 3.9'dan

$$x^n d = \begin{cases} \big(\theta(d)x + \delta_\theta(d)\big)x^{n-1}, & n \text{ tek ise} \\ dx^n, & n \text{ çift ise} \end{cases} \tag{3.9}$$

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 $S[x, \theta, \delta_\theta]$ bazı elemanları için uygulanabileceğini göstermektedir.

Teorem 3.13 (Sağ Bölme Algoritması) $f(x)$ ve $g(x)$ polinomları $g(x)$ in baş katsayısı birim olacak şekilde $S[x, \theta, \delta_\theta]$ halkasında herhangi iki polinom olsun. Bu durumda, 3.10'dan

$$f(x) = q(x)g(x) + r(x) \tag{3.10}$$

$der\big(r(x)\big) < der\big(g(x)\big)$ veya $r(x) = 0$ olacak şekilde $q(x), r(x) \in S[x, \theta, \delta_\theta]$ vardır (Sharma ve Bhaintwal (2018)).

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. Ayrıca, $f(x) = f_0 + f_1x + f_2x^2 + \cdots + f_rx^r$ ve $g(x) = g_0 + g_1x + g_2x^2 + \cdots + g_sx^s$, g_s birim olsun. 3.11'de

$$A(x) = \begin{cases} f_r\theta(g_s^{-1})x^{r-s}, & r-s \text{ tek ise} \\ f_r g_s^{-1}x^{r-s}, & r-s \text{ çift ise} \end{cases} \tag{3.11}$$

şeklinde tanımlanan $A(x)$ polinomu yardımıyla, $f(x)$ polinomunun sağ böleni bulunabilir. Daha detaylı bilgi için Sharma ve Bhaintwal (2018) Theorem 2.8 e bakılabilir.

Örnek 3.14 $s = 4$, için $S = \mathbb{Z}_{16} + u\mathbb{Z}_{16}$ olsun. $S[x, \theta, \delta_\theta]$ de $f(x) = ux^2 + 7x + 12u$ ve $g(x) = (15 + 8u)x + 13 + 9u$ polinomlarını alalım. Sharma ve Bhaintwal (2018), Theorem 2.8 de verilen sağ bölme algoritmasını kullanarak $g(x)$ nin $f(x)$ için bir sağ bölen olduğunu gösterelim. Bunun için önce $A(x) = f_2\theta(g_1^{-1})x^{2-1} = u\theta(15 + 8u)x = (8 + 15u)x$ bulunur. Sonra ise, 3.12'de

$$\begin{aligned} A(x)g(x) &= (8 + 15u)x[(15 + 8u)x + 13 + 9u\,] \\ &= (8 + 15u)[\theta(15 + 8u)x + \delta_\theta(15 + 8u)]x + (8 + 15u)[\theta(13 + 9u\ )x + \delta_\theta(13 + 9u\ )] \\ &= (8 + 15u)[(15 + 8u)x + 0]x + (8 + 15u)[(5 + 9u\ )x + 8 + 8u] \\ &= ux^2 + (15 + 3u)x + 8 + 8u \end{aligned} \tag{3.12}$$

hesaplanır. Şimdi ise, 3.13'ten

$$h(x) = f(x) - A(x)g(x) \\ = (8 + 13u)x + 8 + 4u \tag{3.13}$$

elde edilir. $h(x)$ derecesi 1 olduğundan, aynı algoritma için uygulanırsa, $h(x)$ in $g(x)$ cinsinden değeri $h(x) = 3ug(x) + 13 + 13u$ bulunur. O zaman son olarak, 3.14'ten

$$f(x) = h(x) + A(x)g(x) \\ = 3ug(x) + 13 + 13u + (8 + 15u)xg(x) \\ = [(8 + 15u)x + 3u]g(x) + 13 + 13u \tag{3.14}$$

elde edilir. Dolayısıyla, $q(x) = (8 + 15u)x + 3u$ ve $r(x) = 13 + 13u$ olmak üzere, $f(x) = q(x)g(x) + r(x)$ şeklinde yazılabildiği görülür.

3.1. S Halkası Üzerinde δ_θ-Devirli Kodlar

Bu bölümde üzerinde δ_θ -devirli kodlar olarak isimlendirilen 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.

$p(x)$, S üzerinde derecesi n herhangi bir polinom olmak üzere $S_n = \frac{S[x,\theta,\delta_\theta]}{\langle p(x)\rangle}$ olsun.
Bir $c = (c_0, c_1, \dots, c_{n-1}) \in C$ kodu polinom gösterimi olarak $c = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$ 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 herhangi bir polinom olmak üzere $S_n = \frac{S[x,\theta,\delta_\theta]}{\langle p(x)\rangle}$ 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-öteleme operatörü (cyclic shift) olmak üzere, her c $= (c_0, c_1, \dots, c_{n-1}) \in C$ için $T_{\delta_\theta}(c) = \big(\theta(c_{n-1}) + \delta_\theta(c_0), \theta(c_0) + \delta_\theta(c_1), \dots, \theta(c_{n-2}) + \delta_\theta(c_{n-1})\big) \in C$ için 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 $S[x,\theta,\delta_\theta]$ -modülü olmasıdır.

KANIT: Sharma ve Bhaintwal (2018), 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,δ_θ} nin bir idealidir.

Teorem 3.1.4 C, S üzerinde n uzunluklu bir δ_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.

KANIT: Sharma ve Bhaintwal (2018), Theorem 3.6 nın ispatının benzeridir.

$C = \langle g(x)\rangle$, $x^n - 1$ in bir sağ böleni $g(x) = g_0 + g_1x + g_2x^2 + \cdots + g_kx^k$ tarafından üretilen ve uzunluğu n olan S üzerinde bir δ_θ-devirli kod ise, C nin $(n-k) \times n$ tipindeki üreteç matrisi 3.15'teki gibi

$$G = \begin{bmatrix} g(x) \\ xg(x) \\ x^2g(x) \\ \vdots \\ x^{n-k-1}g(x) \end{bmatrix}_{(n-k)\times n} \tag{3.15}$$

formundadır. Daha açık bir şekilde eğer n - k çift ise 3.16'da verilen

$$G = \begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_k & 0 & \cdots & 0 \\ \delta_\theta(g_0) & \theta(g_0)+\delta_\theta(g_1) & \theta(g_1)+\delta_\theta(g_2) & \cdots & \theta(g_{k-1})+\delta_\theta(g_k) & \theta(g_k) & \cdots & 0 \\ 0 & 0 & g_0 & \cdots & g_{k-3} & g_{k-2} & \cdots & 0 \\ \cdots & \cdots & \cdots & \ddots & \cdots & \ddots & \ddots & \cdots \\ 0 & 0 & \cdots & \delta_\theta(g_0) & \theta(g_0)+\delta_\theta(g_1) & \cdots & \theta(g_{k-1})+\delta_\theta(g_k) & \theta(g_k) \end{bmatrix} \quad (3.16)$$

ve n - k tek ise 3.17'de verilen

$$G = \begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_k & 0 & \cdots & 0 \\ \delta_\theta(g_0) & \theta(g_0)+\delta_\theta(g_1) & \theta(g_1)+\delta_\theta(g_2) & \cdots & \theta(g_{k-1})+\delta_\theta(g_k) & \theta(g_k) & \cdots & 0 \\ 0 & 0 & g_0 & \cdots & g_{k-3} & g_{k-2} & \cdots & 0 \\ \cdots & \cdots & \cdots & \ddots & \cdots & \ddots & \ddots & \cdots \\ 0 & 0 & \cdots & 0 & g_0 \cdots & g_{k-1} & g_{k-2} & \theta(g_k) \end{bmatrix} \quad (3.17)$$

şeklindedir.

Örnek 3.1.5 $s = 4$ için $S = \mathbb{Z}_{16} + u\mathbb{Z}_{16}$ olsun. C, $x^4 - 1$ ün sağ böleni $g(x) = (1+8u)x^2 + 9u$ polinomu tarafından üretilen 4 uzunluklu bir δ_θ-devirli kod olsun. Bu durumda $\{g(x), xg(x)\} = \{(1+8u)x^2 + 9u\ , (1+8u)x^3 + (8+9u)x + 8 + 8u\ \}$ kümesi C kodu için bir bazdır. C nin kardinalitesi $|C| = 256^2$ olup, C nin üreteç matrisi 3.18'deki gibidir,

$$\begin{aligned} G &= \begin{bmatrix} g(x) \\ xg(x) \end{bmatrix} \\ &= \begin{bmatrix} g_0 & g_1 & g_2 & 0 \\ \delta_\theta(g_0) & \theta(g_0)+\delta_\theta(g_1) & \theta(g_1)+\delta_\theta(g_2) & \theta(g_2) \end{bmatrix} \\ &= \begin{bmatrix} 9u & 0 & 1+8u & 0 \\ 8+8u & 8+9u & 0 & 1+8u \end{bmatrix}. \end{aligned} \quad (3.18)$$

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, 3.19'daki gibi

$$C^\perp = \{w | \text{ her } v \in C \text{ için } w.v = 0\} \quad (3.19)$$

olarak tanımlanır.

Teorem 3.1.7 k bir tek tamsayı ve en az bir $h(x) = h_0 + h_1x + h_2x^2 + \cdots + h_kx^k \in S[x, \theta, \delta_\theta]$ için $x^n - 1 = h(x)g(x)$ olsun. Eğer $C = \langle g(x) \rangle$ uzunluğu çift tamsayı n olan S üzerinde bir δ_θ-devirli kod ise C nin kontrol matrisi 3.20'de verilen

$$H = \begin{bmatrix} h_k & \theta(h_{k-1})+\delta_\theta(h_k) & h_{k-2} & \cdots & \theta(h_0)+\delta_\theta(h_1) & \cdots & 0 & 0 \\ 0 & \theta(h_k) & h_{k-1} & \cdots & h_0 & \delta_\theta(h_0) & \cdots & 0 \\ 0 & 0 & h_k & h_{k-2} & \theta(h_{k-3})+\delta_\theta(h_{k-2}) & \cdots & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & h_k & \theta(h_{k-1})+\delta_\theta(h_k) & \cdots & h_1 & \theta(h_0)+\delta_\theta(h_1) \end{bmatrix} \quad (3.20)$$

formundadır. k bir çift tamsayı olduğunda H matrisi 3.21'deki gibi verilir

$$\begin{bmatrix} h_k & \theta(h_{k-1})+\delta_\theta(h_k) & h_{k-2} & \cdots & h_0 & \delta_\theta(h_0) & \cdots & 0 \\ 0 & \theta(h_k) & h_{k-1} & \cdots & h_1 & \theta(h_0)+\delta_\theta(h_1) & \cdots & 0 \\ 0 & 0 & h_k & \cdots & h_2 & \theta(h_1)+\delta_\theta(h_2) & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \theta(h_k) & h_{k-1} & \cdots & h_1 & \theta(h_0)+\delta_\theta(h_1) \end{bmatrix}. \quad (3.21)$$

KANIT: Sharma ve Bhaintwal (2018), Theorem 4.5 in ispatının benzeridir.

Örnek 3.1.8 $x^6-1=(ux^3+8ux^2+u)\big((8+u)x^3+8x^2+15u\big)$ olmak üzere, C, $g(x)=(8+u)x^3+8x^2+15u$ polinomu tarafından üretilen 6 uzunluklu bir δ_θ-devirli kod olsun. $h(x)=ux^3+8ux^2+u$ olmak üzere Teorem 3.1.7 den C nin kontrol matrisi 3.22'deki gibi

$$H=\begin{bmatrix} h_3 & \theta(h_2)+\delta_\theta(h_3) & h_1 & \theta(h_0)+\delta_\theta(h_1) & 0 & 0 \\ 0 & \theta(h_3) & h_2 & \theta(h_1) & h_0 & \delta_\theta(h_0) \\ 0 & 0 & h_3 & \theta(h_2)+\delta_\theta(h_3) & h_1 & \theta(h_0)+\delta_\theta(h_1) \end{bmatrix}$$
$$=\begin{bmatrix} u & 8 & 0 & 8+u & 0 & 0 \\ 0 & 8+u & 8u & 0 & u & 8+8u \\ 0 & 0 & u & 8 & 0 & 8+u \end{bmatrix} \quad (3.22)$$

olarak elde edilir. Ayrıca $GH^T=0$ ve H nin satırları lineer bağımsız olduğundan, H, C nin kontrol matrisidir.

4. Sonuçlar

Bu çalışmada, $u^2=1$ olmak üzere $s\geq 2$ için $S=\mathbb{Z}_{2^s}+u\mathbb{Z}_{2^s}$ halkası üzerindeki aykırı devirli kodlar tanıtılmıştır. θ, S üzerinde bir otomorfizm ve δ_θ bir türetim olmak üzere $S[x,\theta,\delta_\theta]$ aykırı polinomlar halkası kullanılarak δ_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.

Yazar Katkıları

Basri Çalışkan: Araştırma yaparak problemi belirlemiş, temel sonuçları kanıtlamış ve makaleyi yazmıştır.

Çıkar Çatışması

Yazarlar çıkar çatışması bildirmemişlerdir.

Kaynaklar

Boucher, D., Geiselmann, W. ve Ulmer, F. (2007). Skew Cyclic Codes. *Applicable Algebra in Engineering Communication Computing*, *18*(4), 379–389. https://doi.org/10.1007/s00200-007-0043-z

Boucher, D. ve Ulmer, F. (2009). Coding with Skew Polynomial Rings. *Journal of Symbolic Computation, 44*, 1644–1656. https://doi.org/10.1016/j.jsc.2007.11.008

Carlet, C. (1998). $\mathbb{Z}_{2^k}$ linear codes. *IEEE Transactions on Information Theory*, *44*, 1543–1547. https://doi.org/10.1109/18.681328

Cengellenmis, Y. (2010). On the Cyclic Codes over $\mathbb{F}_3+v\mathbb{F}_3$. *International Journal of Algebra*, *4*(6), 253–259. Erişim adresi: http://www.m-hikari.com/ija/ija-2010/ija-5-8-2010/cengellenmisIJA5-8-2010-1.pdf

Çalışkan, B. (2020a). Cylic Codes over the Ring $\mathbb{Z}_8+u\mathbb{Z}_8+v\mathbb{Z}_8$. *ICMASE 2020, Proceedings Book, Ankara Hacı Bayram Veli University,* (pp. 7–12). Ankara, Turkey. https://doi.org/10.14201/0AQ0302

Çalışkan, B. (2020b). Linear Codes over the Ring $\mathbb{Z}_8+u\mathbb{Z}_8+v\mathbb{Z}_8$. *ICOMAA-2020, CPOST*, *3*(1), 19–23. Erişim adresi: https://dergipark.org.tr/en/pub/cpost/issue/57935/763109

Dertli, A. ve 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. Erişim adresi: https://prespacetime.com/index.php/pst/article/view/1543/1468

Dougherty, S.T. ve Fernández-Córdoba, C. (2011). Codes over $\mathbb{Z}_{2^k}$, gray map and self-dual codes. *Advances in Mathematics of Communications, 5*, 571–588. https://doi.org/10.3934/amc.2011.5.571

Hammons, A.R., Kumar, P.V., Calderbank, A.R., Sloane, N.J.A. ve Solé, P. (1994). The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and Related Codes. *IEEE Transactions on Information Theory*, *40*, 301–319. https://doi.org/10.1109/18.312154

Sharma, A. ve Bhaintwal, M. (2018). A class of skew-cyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$ with derivation. *Advances in Mathematics of Communications*, *12*(4), 723–739. https://doi.org/10.3934/amc.2018043