OKU Fen Bilimleri Enstitüsü Dergisi
5(1):103-117, 2022

OKU Journal of The Institute of Science and Technology 5(1):103-117, 2022

Osmaniye Korkut Ata Üniversitesi Fen Bilimleri Enstitüsü Dergisi

Osmaniye Korkut Ata University Journal of The Institute of Science and Technology

$\mathbb{Z}_2^r \times \mathbb{Z}_2^s \times R^t$ Halkası Üzerindeki Devirli Kodlar İçin Bazı Sonuçlar

Kemal BALIKÇI[1*]

[1]Osmaniye Korkut Ata Üniversitesi, Mühendislik Fakültesi, Elektrik-Elektronik Mühendisliği Bölümü, Osmaniye

[1]https://orcid.org/0000-0001-6234-5627
*Sorumlu yazar: kbalikci@osmaniye.edu.tr

Araştırma Makalesi

Makale Tarihçesi:
Geliş tarihi:07.10.2021
Kabul tarihi:08.12.2021
Online Yayınlanma:08.03.2022

Anahtar Kelimeler:
Lineer kod
Devirli kod
$\mathbb{Z}_2\mathbb{Z}_2[u]$-lineer kod
Dual kod

ÖZ

$\mathbb{Z}_4$ halkası kodlama teorisinde çok önemli bir yere sahiptir. $\mathbb{Z}_4$ gibi dört elemanlı önemli diğer bir halka da $\mathbb{Z}_2[u]$ halkasıdır. $\mathbb{Z}_2[u]$ halkası üzerindeki lineer ve devirli kodların $\mathbb{Z}_4$ halkası üzerindeki lineer ve devirli kodlara göre bazı avantajları olduğu iyi bilinmektedir. Bu çalışmada, ilk olarak $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-lineer kodlar ve devirli kodlar tanımlandı. Daha sonra, $\mathbb{Z}_2^r \times \mathbb{Z}_2^s \times R^t$'deki Lee uzaklığını $\mathbb{Z}_2^n$'deki Hamming uzaklığına dönüştüren Φ Gray dönüşümü kullanılarak $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-lineer kodların Gray görüntüleri elde edildi. Ayrıca, $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-lineer kodların standart üreteç ve kontrol matrislerinin formu belirlendi. Böylece bir $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-lineer kodun tipi ve sahip olduğu kodsöz sayısı verildi. Dahası, $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-devirli kodların cebirsel yapıları incelendi ve bu kodların üreteç polinomları ile minimum üreteç kümeleri belirlendi. Son olarak, ayrılabilir $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-devirli kodların duallerinin formu araştırıldı ve etkili bazı örnekler verildi.

Some Results For Cyclic Codes Over The Ring $\mathbb{Z}_2^r \times \mathbb{Z}_2^s \times R^t$

Research Article

Article History:
Received: 07.10.2021
Accepted: 08.12.2021
Published online:08.03.2022

Keywords:
Linear code
Cyclic code
$\mathbb{Z}_2\mathbb{Z}_2[u]$-linear code
Dual code

ABSTRACT

The ring $\mathbb{Z}_4$ has a critical role in coding theory. Another important ring with four elements like ring $\mathbb{Z}_4$ is the ring $\mathbb{Z}_2[u]$. It is well known that linear and cyclic codes over the ring $\mathbb{Z}_2[u]$ has some advantages compared to $\mathbb{Z}_4$. In this paper, firstly, $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-linear and cyclic codes are defined. Then, using the Gray map Φ that transforms the Lee distance in $\mathbb{Z}_2^r \times \mathbb{Z}_2^s \times R^t$ to Hamming distance in $\mathbb{Z}_2^n$, the Gray images of $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-linear codes are obtained. Also, the standart forms of generating and parity-check matrices of $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-linear codes are determined. So, the types and sizes of $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-linear codes are given. Further, algebraic structures of $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-cyclic codes are investigated and the generator polynomials and spanning sets of these codes are determined. Finally, the forms of the dual of separable $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$- cyclic codes are presented and are given some illustrative examples.

To Cite: Balıkçı K. $\mathbb{Z}_2^r \times \mathbb{Z}_2^s \times R^t$ Halkası Üzerindeki Devirli Kodlar İçin Bazı Sonuçlar. Osmaniye Korkut Ata Üniversitesi Fen Bilimleri Enstitüsü Dergisi 2022; 5(1):103-117.

1.Giriş

q bir asal sayı veya bir asal sayının kuvveti ve $\mathrm{F_q}$ da bir sonlu cisim olmak üzere, F_q^n nin bir C alt uzayına $\mathrm{F_q}$ üzerinde n uzunluklu bir lineer kod denir. Kodlama teorisinde yaygın olarak cisimler

kullanılmasına rağmen, farklı halkalar üzerindeki kodlarda araştırmacılar tarafından oldukça ilgi görmektedir (Hammons ve ark., 1994; Çalışkan, 2021a, Çalışkan ve Balıkçı, 2019; Çalışkan ve Özkan, 2020; Çalışkan, 2021b). $\mathbb{Z}_2$ ve $\mathbb{Z}_4$ sırasıyla, tamsayıların 2 ve 4 kalan sınıflar halkaları olsun. $\mathbb{Z}_2^n$'nin boş olmayan bir alt kümesine bir ikili kod ve bir alt grubuna ise bir ikili lineer kod denir. Benzer şekilde $\mathbb{Z}_4^n$'nin boş olmayan bir alt kümesine bir dörtlü kod ve bir alt grubuna ise bir dörtlü lineer kod denir.

Karışık alfabeler üzerindeki kodlar ile ilgili ilk çalışma (Brouwer ve ark., 1998)'de tanıtılmış ve bu kodların bazı sınırları belirlenmiştir. (Borges ve ark., 2009)'da, ikili ve dörtlü lineer kodların bir genellemesi olan $\mathbb{Z}_2 \times \mathbb{Z}_4$-toplamsal kod adı verilen iki alfabe üzerinde $\mathbb{Z}$ -altmodül olan hata düzelten kodların yeni bir sınıfı çalışılmıştır. $\alpha + 2\beta = n$ olmak üzere $\mathbb{Z}_2^{\alpha} \times \mathbb{Z}_4^{\beta}$ nın bir altgrubu C'ye bir $\mathbb{Z}_2\mathbb{Z}_4$-toplamsal kod denir. Eğer $\beta = 0$ ise $\mathbb{Z}_2\mathbb{Z}_4$-toplamsal kodlar, ikili lineer koddurlar ve eğer $\alpha = 0$ ise $\mathbb{Z}_2\mathbb{Z}_4$-toplamsal kodlar, $\mathbb{Z}_4$ üzerinde dörtlü lineer koddurlar. Bugüne kadar $\mathbb{Z}_2\mathbb{Z}_4$-toplamsal kodlar ve onlarla ilgili çok yoğun çalışmalar yapılmıştır (Abualrub ve ark., 2014; Siap ve Aydogdu, 2013).

Son yıllarda yapılan çalışmalarda $\mathbb{Z}_4$ halkası sıklıkla kullanılmasına rağmen, $u^2 = 0$ olmak üzere $R = \mathbb{Z}_2 + u\mathbb{Z}_2 = \{0,1,u,1+u\}$ halkası da araştırmacıların ilgisini çekmiştir (Aydogdu ve ark., 2015; Aydogdu ve ark., 2017). Çünkü, $\mathbb{Z}_4$ ile karşılaştırıldığında bu halka üzerinde tanımlanan lineer ve devirli kodların bazı avantajları vardır. Örneğin, R halkası üzerinde tanımlanan lineer kodların Gray görüntüleri her zaman ikili lineer koddurlar, fakat bu durum $\mathbb{Z}_4$ üzerinde tanımlı kodlar için her zaman geçerli değildir. Ayrıca, R üzerindeki devirli kodların kod çözme algoritmaları $\mathbb{Z}_4$ üzerindeki kodlara göre daha kolaydır.

Yakın bir zamanda (Mostafanasab, 2017)'de $\mathbb{Z}_2$ üzerinde üçlü devirli kodları, (Aydogdu ve Gursoy, 2019)'da $\mathbb{Z}_2\mathbb{Z}_4\mathbb{Z}_8$-toplamsal kodları ve (Wu ve ark., 2018)'de ise $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_4$-toplamsal kodları çalışmışlardır. Bu makalelerde, genellikle ilgili kodların ve duallerinin üreteç matrisleri ve polinomları belirlenmiştir.

Yukarıda bahsedilen çalışmalardan motive olunarak, bu çalışmada, $\mathbb{Z}_2\mathbb{Z}_2[u]$-devirli kodların bir özel hali olarak $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-lineer kodların cebirsel yapıları dikkate alınmıştır. Öncelikle, $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-lineer kodların ve duallerinin standart üreteç matrislerinin formları belirlenmiştir. Daha sonra ise, $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-devirli kodların üreteç polinomları ve minimum geren kümeleri tanımlanmıştır. Ayrıca, bu kodların ayrılabilir olanlarının dualleri çalışılmıştır. Son olarak, bu kodlarla ilgili çeşitli örnekler verilmiştir.

2. Materyal ve Metot

$\mathbb{Z}_2 = \{0,1\}$ sonlu cismi ve $u^2 = 0$ olmak üzere $R = \mathbb{Z}_2 + u\mathbb{Z}_2 = \{0,1,u,1+u\}$ sonlu halkasını dikkate alalım. Halka olarak $\mathbb{Z}_2$'nin R halkasının bir althalkası olduğu açıktır. Bu halka kısaca $R = \mathbb{Z}_2[u]$ ile gösterilir. $\mathbb{Z}_2\mathbb{Z}_2[u]$'nun (Aydogdu ve ark., 2015)'de verilen tanımına benzer bir şekilde aşağıdaki kümeyi tanımlayabiliriz.

$$\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u] = \{(a|b|c): a, b \in \mathbb{Z}_2, c \in R\}.$$

$\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$ kümesi, $u \in R$ elemanı için standart çarpma işlemine göre kapalı değildir. Bu durum, $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$ kümesinin standart çarpma işlemi altında bir R -modül olmadığını gösterir. Bu kümeyi bir R -modül yapmak için aşağıda verilen çarpma işlemi metoduna ihtiyacımız vardır.

$\eta: R \to \mathbb{Z}_2$ dönüşümünü $\eta(e_1 + ue_2) = e_1$ olacak şekilde tanımlayalım. O zaman, $\eta(0) = 0$, $\eta(1) = 1$, $\eta(u) = 0$ ve $\eta(1 + u) = 1$ olduğu görülür. Açıkça görülmektedir ki, η dönüşümü bir halka homomorfizmasıdır. Şimdi herhangi bir $d \in R$ için, $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$ üzerinde $u \in R$-skaler çarpması aşağıdaki gibi tanımlansın.

$$d * v = (\eta(d)a|\eta(d)b|dc).$$

Bu işlem iyi tanımlıdır. Ayrıca, bu çarpma aşağıda verilen yöntem ile $\mathbb{Z}_2^r \times \mathbb{Z}_2^s \times R^t$ halkasına genellenebilir. Herhangi bir $d \in R$ ve $v = (a_0, a_1, \dots, a_{r-1}|b_0, b_1, \dots, b_{s-1}|c_0, c_1, \dots, c_{t-1}) \in \mathbb{Z}_2^r \times \mathbb{Z}_2^s \times R^t$ için,

$$d * v = (\eta(d)a_0, \eta(d)a_1, \dots, \eta(d)a_{r-1}|\eta(d)b_0, \eta(d)b_1, \dots, \eta(d)b_{s-1}|dc_0, dc_1, \dots, dc_{t-1}).$$

dır.

Bu tanım bize aşağıdaki sonucu verir.

Lemma 2.1. $\mathbb{Z}_2^r \times \mathbb{Z}_2^s \times R^t$ halkası yukarıda tanımlanan çarpma işlemi altında bir R-modüldür.

Tanım 2.2. r, s ve t pozitif tamsayılar ve $r + s + 2t = n$ olmak üzere, eğer bir C kodu bir R-modül $\mathbb{Z}_2^r \times \mathbb{Z}_2^s \times R^t$ oluyorsa, C'ye bir $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-lineer kod denir.

$d \in R$ için, $d = e_1 + ue_2$ olacak şekilde en az bir $e_1, e_2 \in \mathbb{Z}_2$ elemanları vardır. R halkasının $\mathbb{Z}_2^2$'ye toplamsal grup olarak izomorfik olduğunu hatırlayalım. Dolayısıyla, C bir $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-lineer kod ise, bu durumda bazı k_0, k_1, k_2 ve k_3 pozitif tamsayıları için C, bir grup olarak $\mathbb{Z}_2^{k_0+k_1+k_3} \times \mathbb{Z}_2^{2k_2}$ ye izomorfik olur.

$C_t^F = \langle\{(a|b|c) \in \mathbb{Z}_2^r \times \mathbb{Z}_2^s \times R^t: c,\ R^t \text{ üzerinde serbest}\}\rangle$ bir altmodül ve $dim(C_t^F) = k_2$ olsun.

$$C_0 = \langle\{(a|b|uc) \in C \setminus C_t^F: a \neq 0, b = 0\}\rangle$$

$$C_1 = \langle\{(a|b|uc) \in C \setminus C_t^F: a = 0, b \neq 0\}\rangle$$

$$C_2 = \langle\{(a|b|uc) \in C \setminus C_t^F: a = 0, b = 0\}\rangle$$

olmak üzere, $D = C_0 \oplus C_1 \oplus C_2$ ve C_0, C_1 ve C_2 kümelerinin boyutları sırasıyla k_0, k_1 ve k_3 olsun.

Tanım 2.3. $C \subseteq \mathbb{Z}_2^r \times \mathbb{Z}_2^s \times R^t$ bir $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-lineer kod olsun. Eğer C, $\mathbb{Z}_2^{k_0+k_1+k_3} \times \mathbb{Z}_2^{2k_2}$ ye grup izomorfik ise, bu durumda k_0, k_1, k_2 ve k_3 yukarıda tanımlandığı gibi olmak üzere, C, $(r, s, t; k_0, k_1, k_2, k_3)$ tipinde bir $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-lineer koddur.

$e_i + uq_i \in R$ için, $e_i, q_i \in \mathbb{Z}_2$ $0 \leq i \leq t-1$ olsun. $e_i \oplus q_i = e_i + q_i \pmod 2$ ve $r + s + 2t = n$ olmak üzere

$$\Phi: \mathbb{Z}_2^{r+s} \times R^t \to \mathbb{Z}_2^n$$

$$\Phi(a_0, a_1, \dots, a_{r-1} | b_0, b_1, \dots, b_{s-1} | e_0 + q_0, e_1 + q_1, \dots, e_{t-1} + q_{-1})$$

$$= (a_0, a_1, \dots, a_{r-1} | b_0, b, \dots, b_{s-1} | q_0, q_1, \dots, q_{t-1}, e_0 \oplus q_0, e_1 \oplus q_1, \dots, e_{t-1} \oplus q_{-1})$$

şeklinde bir Gray dönüşümü tanımlayalım.

Φ dönüşümü $\mathbb{Z}_2^r \times \mathbb{Z}_2^s \times R^t$'deki Lee uzaklığını $\mathbb{Z}_2^n$'deki Hamming uzaklığına dönüştüren bir izometridir. Dahası, bir $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-lineer kod C için, $\Phi(C)$ bir ikili lineer koddur. Bu özellik genel olarak $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_4$-toplamsal kodlar için geçerli değildir.

$w_H(a)$ ve $w_H(b)$ sırasıyla, a ve b kodsözlerinin Hamming ağırlıkları, $w_L(c)$'de c kodsözünün Lee ağırlığı olmak üzere, $\mathbb{Z}_2^r \times \mathbb{Z}_2^s \times R^t$'deki bir kodsözün Lee ağırlığı

$$w_L(a|b|c) = w_H(a) + w_H(b) + w_L(c)$$

şeklinde tanımlanır. $e \in R$ koordinatının Lee ağırlığı, eğer $e = u$ ise $w_L(e) = 2$, eğer $e \in \{1, 1+u\}$ ve sıfır ise $w_L(e) = 1$ olarak tanımlanır.

Bir $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-lineer kod C'nin $\Phi(C)$ ikili görüntüsü, uzunluğu $r + s + 2t = n$ ve 2^n tane kodsözden oluşan bir ikili lineer koddur.

$|X| = r$, $|Y| = s$ ve $|Z| = t$ olmak üzere, X ve Y, $\mathbb{Z}_2$ koordinatlara, Z'de R koordinatlara sahip olsun. C_r, C_s ve C_t, sırasıyla X, Y ve Z dışındaki koordinatların silinmesiyle elde edilen kodları göstersinler.

Herhangi iki eleman $v = (a_0, a_1, \dots, a_{r-1} | b_0, b_1, \dots, b_{s-1} | c_0, c_1, \dots, c_{t-1})$, $v' = (a'_0, a'_1, \dots, a'_{r-1} | b'_0, b'_1, \dots, b'_{s-1} | c'_0, c'_1, \dots, c'_{t-1}) \in \mathbb{Z}_2^r \times \mathbb{Z}_2^s \times R^t$ olsun. v ile v' nün iç çarpımı

$$\langle v, v' \rangle = u\left(\sum_{i=0}^{r-1} a_i a'_i\right) + u\left(\sum_{j=0}^{s-1} b_j b'_j\right) + \sum_{k=0}^{t-1} c_k c'_k \in (\mathbb{Z}_2 + u\mathbb{Z}_2)$$

şeklinde tanımlanır. Burada çarpma işlemleri R üzerinde yapılmaktadır.

3. Bulgular ve Tartışma

3.1. $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-Lineer Kodların Üreteç ve Kontrol Matrisleri

Teorem 3.1.1. C, $(r,s,t;k_0,k_1,k_2,k_3)$ tipinde bir $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-lineer kod olsun. C kodunun üreteç matrisinin standart hali, aşağıdaki gibi verilen bir $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-lineer koda permütasyon denktir.

$$G=\left(\begin{array}{cc|cc|ccc} I_{k_0} & A_1 & 0 & T_1 & 0 & 0 & uT_2 \\ 0 & 0 & I_{k_1} & A_2 & 0 & 0 & uT_3 \\ 0 & S_1 & 0 & S_2 & I_{k_2} & A_3 & B_1+uB_2 \\ 0 & 0 & 0 & 0 & 0 & uI_{k_3} & uD \end{array}\right). \tag{3.1}$$

Burada $A_1, A_2, A_3, B_1, B_2, D, S_1, S_2, T_1, T_2$ ve T_3, $\mathbb{Z}_2$ üzerinde matrislerdir. I_{k_0}, I_{k_1}, I_{k_2}ve I_{k_3} birim matrislerdir ve C'de $2^{k_0+k_1}4^{k_2}2^{k_3}$ kodsöz vardır.

İspat: R üzerinde t uzunluklu herhangi bir lineer kodun üreteç matrisinin

$$\begin{pmatrix} I_{k_1} & A' & B'_1+uB'_2 \\ 0 & uI'_{k_3} & uD' \end{pmatrix}$$

şeklinde olduğu bilinmektedir (Aydogdu ve ark., 2015).

Ayrıca, r ve s uzunluklu herhangi iki lineer kod sırasıyla $(I'_{k_0} \quad A'_1)$ ve $(I'_{k_1} \quad A'_2)$ matrisleri tarafından üretildiği kabul edilebilir. C, $r+s+2t$ uzunluklu bir $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-lineer kod olduğundan, C kodu tüm bileşenleri $\mathbb{Z}_2$'den olan

$$\left(\begin{array}{cc|cc|ccc} I'_{k_0} & A'_1 & T_{01} & T_{02} & T_{03} & T_{04} & T_{05} \\ S_{01} & S_{02} & I'_{k_1} & A'_2 & T_{11} & T_{12} & T_{13} \\ S_{11} & S_{12} & S_{13} & S_{14} & I_{k_1} & A' & B'_1+uB'_2 \\ S_{21} & S_{22} & S_{23} & S_{24} & 0 & uI'_{k_3} & uD' \end{array}\right)$$

şeklindeki bir matris tarafından üretilir. Şimdi bu matrise gerekli satır ve sütun işlemlerinin uygulanmasıyla istenen standart form matrisi elde edilebilir.

Örnek 3.1.2. C, aşağıdaki üreteç matrisine sahip bir $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-lineer kod olsun.

$$G=\left(\begin{array}{ccc|cc|ccc} 0 & 1 & 1 & 0 & 1 & 1+u & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & u \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1+u & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & u & 1 & u \end{array}\right) \tag{3.2}$$

Eğer G matrisine elemanter satır sütun işlemleri uygulanırsa, aşağıda verilen standart formdaki matris elde edilir.

$$G_S = \left(\begin{array}{ccc|cc|ccc} 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & u \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & u \\ 0 & 0 & 1 & 0 & 1 & 1+u & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & u & u \end{array}\right).$$

Dolayısıyla C, $(3,2,3;2,1,1,1)$ tipindedir ve $2^{2+1+1}4^1 = 64$ kodsöze sahiptir.

Teorem 3.1.3. C, standart üreteç matrisi 3.1'deki formda olan ve $(r,s,t;k_0,k_1,k_2,k_3)$ tipinde bir $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-lineer kod olsun. O zaman, C'nin kontrol matrisi

$$H = \left(\begin{array}{cc|cc|ccc} -A_1^t & I_{r-k_0} & 0 & T_1 & -uS_1^t & 0 & 0 \\ -T_1^t & 0 & -A_2^t & I_{s-k_1} & -uS_2^t & 0 & 0 \\ -T_2^t & 0 & -T_3^t & 0 & -(B_1+uB_2)^t + D^tA_3^t & D^t & I_{t-k_2-k_3} \\ 0 & 0 & 0 & 0 & -uA_3^t & uI_{k_3} & 0 \end{array}\right)$$

şeklinde verilir. Bu durumda, $C^\perp$ dual kodu, $(r,s,t;r-k_0,s-k_1,t-k_2-k_3,k_3)$ tipindedir.

İspat. $GH^\perp = 0$ olduğu açıktır. Dolayısıyla, H'nin her satırı, G'nin satırlarına ortogonaldir. Dahası, lineer kodların standart formdaki üreteç matrisleri minimum sayıda satır içerdiğinden, $C^\perp$, $2^{r-k_0}2^{s-k_1}2^{2(t-k_2-k_3)}2^{k_3}$ tane kodsöze sahiptir. Böylece

$$|C||C^\perp| = 2^{k_0+k_1}2^{2k_2}2^{k_3}2^{r-k_0}2^{s-k_1}2^{2(t-k_2-k_3)}2^{k_3} = 2^{r+s+2t}$$

elde edilir. Bu yüzden, H matrisinin satırları sadece C'ye ortogonal değil, ayrıca dual uzayını da üretir.

Örnek 3.1.4. C, standart formdaki üreteç matrisi 3.2'de verilen $(3,2,3;2,1,1,1)$ tipinde bir $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-lineer kod olsun. C'nin kontrol matrisi

$$H = \left(\begin{array}{ccc|cc|ccc} 1 & 0 & 1 & 0 & 0 & u & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & u & 0 & 0 \\ 0 & 1 & 0 & u & 0 & u & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & u & u \end{array}\right)$$

şeklindedir. Bu durumda $C^\perp$, $(3,2,3;1,1,1,1)$ tipindedir ve $2^{1+1+1}4^1 = 32$ kodsöze sahiptir. Açıkça görülmektedir ki, $|C||C^\perp| = 2^6 2^5$ dir.

3.2. $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-Lineer Devirli Kodlar

Devirli kodların belirli halkaların idealleri olarak tanımlandığı iyi bilinen bir gerçektir. Bu yüzden, $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-lineer devirli kodların $\mathcal{R}_{r,s,t} = \mathbb{Z}_2[x]/\langle x^r-1\rangle \times \mathbb{Z}_2[x]/\langle x^s-1\rangle \times R[x]/\langle x^t-1\rangle$ 'nin sol $R[x]$ altmodüleri oldukları gösterilecektir.

Tanım 3.2.1. C, $\mathbb{Z}_2^r \times \mathbb{Z}_2^s \times R^t$'nin bir alt kümesi olmak üzere, eğer C aşağıdaki koşulları sağlıyorsa, C'ye bir $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-lineer devirli kod denir.

i) C, $\mathbb{Z}_2^r \times \mathbb{Z}_2^s \times R^t$'nin bir R -altmodülüdür,

ii) herhangi bir $v = (a_0, a_1, \dots, a_{r-1}|b_0, b_1, \dots, b_{s-1}|c_0, c_1, \dots, c_{t-1}) \in C$ için, $T(v) = (a_{r-1}, a_0, \dots, a_{r-2}|b_{s-1}, b_0, \dots, b_{s-2}|c_{t-1}, c_0, \dots, c_{t-2})$ devirsel ötelemesi de C'nin bir elemanıdır.

Tanım 3.2.2. C, bir $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-lineer devirli kod olsun. C'nin duali

$$C^{\perp} = \{w \in \mathbb{Z}_2^r \times \mathbb{Z}_2^s \times R^t : \text{her } v \in C \text{ için } \langle w, v\rangle = 0\}$$

olarak tanımlanır. Dualin bu tanımını kullanarak aşağıdaki sonuca sahip oluruz.

Sonuç 3.2.3. Eğer C, bir $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-lineer devirli kod ise, $C^{\perp}$ de bir $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-lineer devirli koddur.

Bir $v = (a_0, a_1, \dots, a_{r-1}|b_0, b_1, \dots, b_{s-1}|c_0, c_1, \dots, c_{t-1}) \in \mathbb{Z}_2^r \times \mathbb{Z}_2^s \times R^t$ elemanı, $\mathcal{R}_{r,s,t}$ modülünde üç polinomdan oluşan bir eleman olarak aşağıdaki gibi belirlenebilir.

$$v = (a_0 + a_1x + \cdots + a_{r-1}x^{r-1}|b_0 + b_1x + \cdots + b_{s-1}x^{s-1}|c_0 + c_1x + \cdots + c_{t-1}x^{t-1})$$

$$= \big(a(x)|b(x)|c(x)\big).$$

Bu belirleniş, $\mathbb{Z}_2^r \times \mathbb{Z}_2^s \times R^t$'nin elemanları ile $\mathcal{R}_{r,s,t}$ 'nin elemanları arasında bir bire bir eşleme verir.

$f(x) = f_0 + f_1x + \cdots + f_kx^k \in R[x]$, $\big(a(x)|b(x)|c(x)\big) \in \mathcal{R}_{r,s,t}$ olsun ve $\eta\big(f(x)\big) = \eta(f_0) + \eta(f_1)x + \cdots + \eta(f_k)x^k$ olmak üzere,

$$f(x) * \big(a(x)|b(x)|c(x)\big) = \Big(\eta\big(f(x)\big)a(x)|\eta\big(f(x)\big)b(x)\big|f(x)c(x)\Big)$$

verilen çarpma işlemi dikkate alınsın.

Şimdi $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-lineer devirli kodların polinom tanımını yapabiliriz.

Tanım 3.2.4. C, $\mathcal{R}_{r,s,t}$'nin bir alt kümesi olsun. Eğer C, $\mathcal{R}_{r,s,t}$ nin bir altgrubu oluyor ve her

$$v = (a_0 + a_1x + \cdots + a_{r-1}x^{r-1}|b_0 + b_1x + \cdots + b_{s-1}x^{s-1}|c_0 + c_1x + \cdots + c_{t-1}x^{t-1}) \in C$$

için

$$x * v = (a_{r-1} + a_0x + \cdots + a_{r-2}x^{r-1}|b_{s-1} + b_0x + \cdots + b_{s-2}x^{s-1}|c_{t-1} + c_0x + \cdots + c_{t-2}x^{t-1})$$

elemanı da C'nin bir elemanı oluyorsa, C'ye bir $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-devirli kod denir.

Yukarıdaki tanımdan, aşağıdaki sonuca sahip oluruz.

Lemma 3.2.5. Bir C kodunun bir $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-devirli kod olabilmesi için gerek ve yeter koşul C'nin $\mathcal{R}_{r,s,t}$ 'nin bir $R[x]$-altmodülü olmasıdır.

Gösterim 3.2.6. Bundan sonra bir $f(x) \in \mathbb{Z}_2[x]$ (ya da $R[x]$) polinomu kısaca f ile, $f(x)$ tarafından üretilen bir ideal ise $\langle f \rangle$ ile gösterilecektir. Ayrıca, t'yi daima tek tamsayı olarak kabul edeceğiz.

3.3. $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-Devirli Kodların Cebirsel Yapısı

Bu bölümde, $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-devirli kodların $\mathcal{R}_{r,s,t}$ nin bir $R[x]$-altmodülü olarak üreteç kümeleri çalışılacaktır.

Teorem 3.3.1. C, bir $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-devirli kod olsun. Bu durumda $f_1, f_2, l_1, l_2 \in \mathbb{Z}_2[x]$; $f_3, a \in R[x]$, $f_1 | \langle x^r - 1 \rangle \ (mod\ 2)$, $f_2 | \langle x^s - 1 \rangle \ (mod\ 2)$, $f_3 | \langle x^t - 1 \rangle \ (mod\ 2)$ olmak üzere C kodu

$$C = \langle (f_1|0|0), (0|f_2|0), (l_1|l_2|f_3 + ua) \rangle$$

şeklinde tek türlü olarak belirlenir.

İspat. C ve $R[x] \ / \ \langle x^t - 1 \rangle$, $\mathcal{R}_{r,s,t}$ nin $R[x]$-altmodülleri olduğundan,

$$\Psi: C \to R[x] \ / \ \langle x^t - 1 \rangle$$

$$\Psi(c_1|c_2|c_3) = c_3$$

şeklinde bir dönüşüm tanımlayabiliriz. Açıkça görülmektedir ki, tanımlanan bu dönüşüm bir $R[x]$-modül homomorfizmasıdır. Ayrıca $\Psi(C)$, $R[x] \ / \ \langle x^t - 1 \rangle$ nin bir $R[x]$-modülüdür, aslında bir idealidir ve $Ker(\Psi)$ de C'nin bir altmodülüdür.

t bir tek tamsayı olduğundan, yukarıdaki tartışmalardan ve (Aydogdu ve ark., 2017)'deki Teorem 3 den $\Psi(C) = \langle f_3 + ua \rangle$ olacak şekilde $f_3, a \in R[x]$, $a | f_3 | \langle x^t - 1 \rangle \ (mod\ 2)$ polinomları vardır.

Dikkat edilirse

$$Ker(\Psi) = \{(c_1|c_2|0) \in \mathcal{R}_{r,s,t} : (c_1|c_2|0) \in C\}$$

dır. Bu durumda $\mathcal{R}_{r,s} = \mathbb{Z}_2[x] \ / \ \langle x^r - 1 \rangle \times \mathbb{Z}_2[x] \ / \ \langle x^s - 1 \rangle$ olmak üzere

$$I = \{(c_1|c_2) \in \mathcal{R}_{r,s} : (c_1|c_2|0) \in Ker(\Psi)\},$$

kümesini tanımlayabiliriz. I nın $\mathcal{R}_{r,s}$ nin bir ideali olduğu açıktır. $I = I_1 \times I_2$ olacak şekilde $\mathbb{Z}_2[x] \ / \ \langle x^r - 1 \rangle$ nin bir I_1 ideali ve $\mathbb{Z}_2[x] \ / \ \langle x^s - 1 \rangle$ nin bir I_2 ideali vardır. Dolayısıyla, $I_1 = \langle f_1 \rangle$, $I_2 = \langle f_2 \rangle$ olacak şekilde $f_1, f_2 \in \mathbb{Z}_2[x]$, $f_1 | \langle x^r - 1 \rangle \ (mod\ 2)$, $f_2 | \langle x^s - 1 \rangle \ (mod\ 2)$ polinomları vardır. Bu

yüzden $I = \langle (f_1|0), (0|f_2) \rangle$ olduğunu elde ederiz. Şimdi herhangi bir $(c_1|c_2|0) \in Ker(\Psi)$ elemanı için $(c_1|c_2) \in I$ dır ve

$$(c_1|c_2) = m * \big((f_1|0), (0|f_2)\big)$$

olacak şekilde en az bir $m \in \mathbb{Z}_2[x]$ polinomu vardır. Buradan

$$(c_1|c_2|0) = m * \big((f_1|0|0), (0|f_2|0)\big)$$

olduğunu elde ederiz. Bu ise

$$Ker(\Psi) = \langle (f_1|0|0), (0|f_2|0) \rangle$$

olmasını gerektirir. Birinci izomorfizm teoreminden $C \,/\, Ker(\Psi) \cong \langle f_3 + ua \rangle$ olduğu bulunur.

$\Psi(C) = (l_1|l_2|f_3 + ua)$ olacak şekilde bir $(l_1|l_2|f_3 + ua) \in C$ olsun. Bu tartışmalar, herhangi bir $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-devirli kodun $\mathcal{R}_{r,s,t}$ nin bir $R[x]$-altmodülü olarak $(f_1|0|0)$, $(0|f_2|0)$, $(l_1|l_2|f_3 + ua)$, $f_1, f_2, l_1, l_2 \in \mathbb{Z}_2[x]$; $f_3, a \in R[x]$, $f_1|\langle x^r - 1 \rangle \ (mod\ 2)$, $f_2|\langle x^s - 1 \rangle \ (mod\ 2)$, $f_3|\langle x^t - 1 \rangle \ (mod\ 2)$ şeklindeki elamanlar tarafından üretildiğini gösterir. Ayrıca, $d_1, d_2, d_3 \in R[x]$ olmak üzere, C nin herhangi bir elemanı

$$d_1 * (f_1|0|0) + d_2 * (0|f_2|0) + d_3 * (l_1|l_2|f_3 + ua)$$

formundadır.

Lemma 3.3.2. Eğer $C = \langle (f_1|0|0), (0|f_2|0), (l_1|l_2|f_3 + ua) \rangle$ bir $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-devirli kod ise, bu durumda $deg(l_1) < deg(f_1)$ ve $deg(l_2) < deg(f_2)$ olduğunu kabul edebiliriz.

İspat. $deg(l_1) - deg(f_1) = i$ olacak şekilde $deg(l_1) > deg(f_1)$ olduğunu kabul edelim.

$$C' = \langle (f_1|0|0), (0|f_2|0), \big(l_1 + x^i f_1 \big| l_2 | f_3 + ua\big) \rangle$$

kodunu alalım. Dikkat edilirse

$$\big(l_1 + x^i f_1 | l_2 | f_3 + ua\big) = \big(x^i f_1 | 0 | 0\big) + (l_1|l_2|f_3 + ua)$$

dır. Buradan $C' \subseteq C$ elde edilir. Ayrıca,

$$(l_1|l_2|f_3 + ua) = \big(l_1 + x^i f_1 | l_2 | f_3 + ua\big) - x^i * (f_1|0|0)$$

olduğundan, $C \subseteq C'$ olduğunu elde ederiz. Dolayısıyla, $C' = C$ bulunur. Benzer metot $deg(l_2) < deg(f_2)$ olduğunu ispatlamak için de kullanılabilir.

Lemma 3.3.3. Eğer $C = \langle (f_1|0|0), (0|f_2|0), (l_1|l_2|f_3 + ua) \rangle$ bir $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-devirli kod ise, bu durumda

$f_1|\frac{x^t-1}{a}l_1 \ (mod\ u)$, $f_2|\frac{x^t-1}{a}l_2 \ (mod\ u)$ ve $f_1f_2|\frac{x^t-1}{a}obeb(f_1f_2, f_1l_2, f_2l_1) \ (mod\ u)$ olduğunu kabul edebiliriz.

İspat. $\Psi\left(\frac{x^t-1}{a} * (l_1|l_2|f_3 + ua)\right) = \Psi\left(\left(\eta\left(\frac{x^t-1}{a}\right)l_1|\eta\left(\frac{x^t-1}{a}\right)l_2|0\right)\right)$ olduğundan,

$$\left(\left(\eta\left(\frac{x^t-1}{a}\right)l_1|\eta\left(\frac{x^t-1}{a}\right)l_2|0\right)\right) \in Ker(\Psi) \subseteq C$$

dır. Buradan $f_i|\frac{x^t-1}{a}l_i$, $i = 1,2$ elde edilir. Dolayısıyla, $f_1f_2|\frac{x^t-1}{a}obeb(f_1f_2, f_1l_2, f_2l_1) \ (mod\ u)$ ya sahip oluruz.

Lemma 3.3.2, eğer C sadece $(l_1|l_2|f_3 + ua)$ tarafından üretilen bir $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-devirli kod ise, $x^r - 1|\frac{x^t-1}{a}l_1$, $x^s - 1|\frac{x^t-1}{a}l_2$ ve $a|f_3|\langle x^t - 1\rangle \ (mod\ 2)$ olduğunu gösterir.

Lemma 3.3.2. ve Lemma 3.3.3.'ten aşağıdaki sonuca sahip oluruz.

Sonuç 3.3.5. Eğer $obeb\left(f_i, \frac{x^t-1}{a}\right) = 1$ ise, $l_i = 0$, $i = 1,2$ dır.

3.4. Minimum Üreteç Kümeleri

Bu bölümde $\mathcal{R}_{r,s,t}$ de bir $R[x]$-modül olarak C nin minimum üreteç kümesi belirlenmiştir. Bu sayede C nin eleman sayısı hakkında bilgi sahibi olabileceğiz.

Teorem 3.4.1. $C = \langle (f_1|0|0), (0|f_2|0), (l_1|l_2|f_3 + ua) \rangle$, $deg(f_1) = r_1$, $deg(f_2) = s_1$, $deg(f_3) = t_1$, $deg(a) = t_2$ ve $h = \frac{x^t-1}{f_3}$ ile bir $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-devirli kod olsun.

$$S_1 = \bigcup_{i=0}^{r-r_1-1} \{x^i * (f_1|0|0)\}$$

$$S_2 = \bigcup_{i=0}^{s-s_1-1} \{x^i * (0|f_2|0)\}$$

$$S_3 = \bigcup_{i=0}^{t-t_1-1} \{x^i * (l_1|l_2|f_3 + ua)\}$$

$$S_4 = \bigcup_{i=0}^{t_1-t_2-1} \{x^i * (\eta(h)l_1|\eta(h)l_2|uha)\}$$

olarak tanımlanırsa, $S_1 \cup S_2 \cup S_3 \cup S_4$, $\mathcal{R}_{r,s,t}$ de bir $R[x]$-modül olarak C nin minimum üreteç kümesini oluşturur ve C nin $2^{r-r_1}2^{s-s_1}4^{t-t_1}2^{t_1-t_2}$ tane kodsözü vardır.

İspat. c, C nin bir kodsözü olsun. Teorem 3.3.1.'e göre

$$d_1 * (f_1|0|0) + d_2 * (0|f_2|0) + d_3 * (l_1|l_2|f_3 + ua)$$

olacak şekilde $d_1, d_2, d_3 \in R[x]$ polinomları vardır.

Eğer $deg(\eta(d_1)) = r - r_1 - 1$ ise, $(\eta(d_1)f_1|0|0) \in Span(S_1)$ dir. Aksi takdirde, bölme algoritmasından dolayı

$$\eta(d_1) = \frac{x^r - 1}{f_1}\eta(q_1) + \eta(e_1)$$

olacak şekilde $\eta(e_1) = 0$ ya da $deg(\eta(e_1)) \leq r - r_1 - 1$, $q_1, e_1 \in R[x]$ polinomları vardır. Dolayısıyla, $d_1 * (f_1|0|0) = e_1 * (f_1|0|0)$ olduğu elde edilir. Buradan $d_1 * (f_1|0|0) \in Span(S_1)$ dir. Benzer şekilde $d_2 * (0|f_2|0) \in Span(S_2)$ olduğu da gösterilebilir.

Eğer $deg(d_3) = t - t_1 - 1$ ise, $d_3 * (l_1|l_2|f_3 + ua) \in Span(S_1 \cup S_2 \cup S_3 \cup S_4)$ tür. Aksi takdirde, yine bölme algoritmasından,

$$d_3 = hq_3 + e_3$$

olacak şekilde $e_3 = 0$ ya da $deg(e_3) \leq t - t_1 - 1$, $q_3, e_3 \in R[x]$ polinomları vardır. Dolayısıyla,

$$d_3 * (l_1|l_2|f_3 + ua) = q_3 * (\eta(h)l_1|\eta(h)l_2|uha) + e_3 * (l_1|l_2|f_3 + ua)$$

dır. $e_3 * (l_1|l_2|f_3 + ua) \in Span(S_3)$ olduğu açıktır. Bu durumda $q_3 * (\eta(h)l_1|\eta(h)l_2|uha) \in Span(S_1 \cup S_2 \cup S_4)$ olduğunu göstermek kalıyor.

Lemma 3.3.3.'ten $f_1|\frac{x^t-1}{a}l_1$, $f_2|\frac{x^t-1}{a}l_2$ dir. Dolayısıyla, $\frac{x^t-1}{a}l_1 = f_1k_1$ ve $\frac{x^t-1}{a}l_2 = f_2k_2$ olacak şekilde $k_1, k_2 \in R[x]$ polinomları vardır. Eğer $deg(q_3) \leq t_1 - t_2 - 1$ ise, istenen elde edilmiş olur. Aksi takdirde,

$$q_3 = \frac{x^t - 1}{ha}q_4 + e_4$$

olacak şekilde $e_4 = 0$ ya da $deg(e_4) \leq t_1 - t_2 - 1$, $q_4, e_4 \in R[x]$ polinomları vardır. Bu durumda

$$q_3 * (\eta(h)l_1|\eta(h)l_2|uha) = q_3 * \left(\frac{x^t-1}{ha} q_4\eta(h)l_1|\frac{x^t-1}{ha} q_4\eta(h)l_2|0\right) + e_4 * (\eta(h)l_1|\eta(h)l_2|uha)$$

olduğunu elde ederiz. O zaman $e_4 * (\eta(h)l_1|\eta(h)l_2|uha) \in Span(S_4)$ tür. $f_1|\frac{x^t-1}{a} l_1 \ (mod\ u)$, $f_2|\frac{x^t-1}{a} l_2 \ (mod\ u)$ olduğundan

$$\left(\frac{x^t-1}{ha} q_4\eta(h)l_1|\frac{x^t-1}{ha} q_4\eta(h)l_2|0\right) \in Span(S_1 \cup S_2)$$

elde ederiz.

Sonuç olarak, $S_1 \cup S_2 \cup S_3 \cup S_4$ kümesi, C nin bir üreteç kümesi olarak elde edilir. Dikkat edilirse, S_1, 2^{r-r_1} kodsöz katkıda bulunur, S_2, 2^{s-s_1} kodsöz ve S_3 ve S_4 ise sırasıyla 4^{t-t_1} ve $2^{t_1-t_2}$ sayıda kodsöz katkısında bulunur. Bu durumda C, $2^{r-r_1}2^{s-s_1}4^{t-t_1}2^{t_1-t_2}$ tane kodsöze sahip olur.

Örnek 3.4.2. $f_1 = 1+x+x^2+x^4$, $f_2 = 1+x+x^3+x^4+x^6+x^7$, $f_3 = 1+x+x^2+x^3+x^5+x^7+x^8+x^{11}$, $a = 1+x+x^2+x^3+x^6$, $l_1 = 1+x^2+x^3$ ve $l_2 = 1+x^3+x^6$ olmak üzere, C, $\langle (f_1|0|0), (0|f_2|0), (l_1|l_2|f_3+ua)\rangle$ tarafından üretilen $\mathbb{Z}_2[x] / \langle x^7-1\rangle \times \mathbb{Z}_2[x] / \langle x^9-1\rangle \times R[x] / \langle x^{15}-1\rangle$ de bir $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-devirli kod olsun.

Yukarıda verilen polinomların $R[x]$ de x^7-1 ve x^9-1 polinomların çarpanlarından elde edildiğini hatırlayalım. Bu çarpanlara ayrılış R de sağlandığından, bu çarpanlara ayrılışı $\mathbb{Z}_2[x]$'de de kullanabiliriz. Dahası,

$$f_3 h_{f_3} = x^{15}-1 \Rightarrow h_{f_3} = 1+x+x^4$$

polinomunu elde ederiz. Dolayısıyla, Teorem 3.4.1.'deki üreteç kümeleri kullanılırsa, $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-devirli kodun üreteç matrisi G aşağıdaki gibi elde edilir.

$$\left(\begin{array}{ccccccc|ccccccccc|ccccccccccccccc}
1&1&1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&1&1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&1&1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&1&0&1&1&0&1&1&0&1&1&0&1&1&1&1&1&1&1&1&1&1&1&1\\
0&0&0&0&0&0&0&0&1&1&0&1&1&0&1&1&0&1&1&0&1&1&1&1&1&1&1&1&1&1&1\\
1&0&1&1&0&0&0&1&0&1&1&0&1&1&0&1&1+u&1+u&1+u&1+u&0&1&u&1&1&0&0&0&0&0&0\\
0&1&0&1&1&0&0&1&1&0&1&1&0&1&1&0&0&1+u&1+u&1+u&1+u&0&1&u&1&1&0&0&0&0&0\\
0&0&1&0&1&1&0&0&1&1&0&1&1&0&1&1&0&0&1+u&1+u&1+u&1+u&0&1&u&1&1&0&0&0&0\\
0&0&0&1&0&1&1&1&0&1&1&0&1&1&0&1&0&0&0&1+u&1+u&1+u&1+u&0&1&u&1&1&0&0&0\\
0&1&1&0&0&0&1&1&1&0&1&1&0&1&1&0&u&0&0&0&0&u&0&0&0&0&u&0&0&0&0\\
1&0&1&1&0&0&0&1&0&0&1&0&0&1&0&0&0&u&0&0&0&0&u&0&0&0&0&u&0&0&0\\
0&1&0&1&1&0&0&0&1&0&0&1&0&0&1&0&0&0&u&0&0&0&0&u&0&0&0&0&u&0&0\\
0&0&1&0&1&1&0&0&0&1&0&0&1&0&0&1&0&0&0&u&0&0&0&0&u&0&0&0&0&u&0\\
0&0&0&1&0&1&1&1&0&0&1&0&0&1&0&0&0&0&0&0&u&0&0&0&0&u&0&0&0&0&0
\end{array}\right)$$

$$S_1 = \bigcup_{i=0}^{7-4-1} \{x^i * (f_1|0|0)\} = \bigcup_{i=0}^{2} \{x^i * (1+x+x^2+x^4|0|0)\}$$

$$S_2 = \bigcup_{i=0}^{9-7-1} \{x^i * (0|f_2|0)\} = \bigcup_{i=0}^{1} \{x^i * (0|1+x+x^3+x^4+x^6+x^7|0)\}$$

$$S_3 = \bigcup_{i=0}^{15-11-1} \{x^i * (l_1|l_2|f_3+ua)\}$$

$$= \bigcup_{i=0}^{3} \left\{x^i * \left(1+x^2+x^3|1+x^3+x^6 \left| \begin{matrix} 1+u+(1+u)x+(1+u)x^2 \\ +(1+u)x^3+x^5+ux^6+x^7+x^8+x^{11} \end{matrix} \right.\right)\right\}$$

$$S_4 = \bigcup_{i=0}^{11-6-1} \{x^i * (\eta(h)l_1|\eta(h)l_2|uha)\} = \bigcup_{i=0}^{4} \{x^i * (x+x^2+x^3|1+x^3+x^6|u+ux^5+ux^{10})\}$$

ve C, $2^3 2^2 2^4 2^5$ kodsöze sahiptir. Dahası, $\Phi(C)$, $(46, 2^{18}, 4)$ parametrelerine sahip ikili bir lineer koddur. $\Phi(C)$ nin Hamming ağırlık sayacı MAGMA ile hesaplanırsa (http://magma.maths.usyd.\linebreak edu.au/calc/)

$$\begin{aligned} x^{46} + 7x^{42}y^4 + 3x^{40}y^6 + 51x^{38}y^8 + 189x^{36}y^{10} + 1318x^{34}y^{12} + 2673x^{32}y^{14} + 14398x^{30}y^{16} \\ + 20714x^{28}y^{18} + 44844x^{26}y^{20} + 46874x^{24}y^{22} + 46874x^{22}y^{24} + 44844x^{20}y^{26} \\ + 20714x^{18}y^{28} + 14398x^{16}y^{30} + 2673x^{14}y^{32} + 1318x^{12}y^{34} + 189x^{10}y^{36} \\ + 51x^8y^{38} + 3x^6y^{40} + 7x^4y^{46} \end{aligned}$$

şeklinde elde edilir.

4. Ayrılabilir $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-Devirli Kodların Dualleri

Sonuç 3.2.3.'e göre, bir $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-lineer kodun dualininde bir $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-lineer kod olduğunu biliyoruz. C'nin dual kodunu

$$C^{\perp} = \langle (\hat{f}_1|0|0), (0|\hat{f}_2|0), (\hat{l}_1|\hat{l}_2|\hat{f}_3 + u\hat{a}) \rangle$$

olarak ele alalım.

Tanım 4.1. Eğer bir $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-lineer kod C, $C = C_r \times C_s \times C_t$ şeklinde yazılabiliyorsa, C'ye ayrılabilir kod denir.

(Wu ve ark., 2018) de ifade edildiği gibi, eğer C ayrılabilir ise, C kodu

$$C = \langle (f_1|0|0), (0|f_2|0), (0|0|f_3 + ua) \rangle$$

formundadır.

Teorem 4.2. $f_1|x^r-1$, $f_2|x^s-1$, $f_3=ab$ ve en az bir $h_{f_3}\in R[x]$ için $abh_{f_3}=x^t-1$ ile $C=\langle(f_1|0|0),(0|f_2|0),(0|0|f_3+ua)\rangle$ ayrılabilir bir $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-devirli kod olsun. Bu durumda

$$C^{\perp}=\langle\left(\frac{x^r-1}{f_1^*}\middle|0|0\right),\left(0|\frac{x^s-1}{f_2^*}\middle|0\right),(0|0|h_{f_3}^*b^*+uh_{f_3}^*)\rangle$$

dır.

İspat. C ayrılabilir olduğundan,

$$(C^{\perp})_r=(C_r)^{\perp}=\langle\frac{x^r-1}{f_1^*}\rangle$$

$$(C^{\perp})_s=(C_s)^{\perp}=\langle\frac{x^s-1}{f_2^*}\rangle$$

$$(C^{\perp})_t=(C_t)^{\perp}=\langle h_{f_3}^*b^*+uh_{f_3}^*\rangle$$

olduğunu biliyoruz. (Wu ve ark., 2018) den $C^{\perp}=(C^{\perp})_r\times(C^{\perp})_s\times(C^{\perp})_t$ olduğunu elde ederiz. Bu da ispatı tamamlar.

Örnek 4.3. $r=3$, $s=5$ ve $t=7$ için $f_1=1+x$, $f_2=1+x+x^2+x^3+x^4$, $f_3=1+x+x^2+x^3+x^4+x^5+x^6$, $a=1+x^2+x^3$, $b=1+x+x^3$ ve $h_{f_3}=1+x^2+x^3$ olmak üzere, $C=\langle(f_1|0|0),(0|f_2|0),(0|0|f_3+ua)\rangle$ ayrılabilir bir $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-devirli kod olsun.

Bu durumda, Teorem 4.2'den C nin dual kodu, $\hat{f}_1=1+x+x^2$, $\hat{f}_2=1+x$, $\hat{f}_3=1+x+x^2+x^4$, $\hat{a}=1+x$, $\hat{b}=1+x^2+x^3$ ve $\hat{h}_{f_3}=1+x+x^3$ olmak üzere, $C^{\perp}=\langle(\hat{f}_1|0|0),(0|\hat{f}_2|0),(\hat{l}_1|\hat{l}_2|\hat{f}_3+u\hat{a})\rangle$ şeklinde elde edilir. Dahası, $\Phi(C^{\perp})$, $(22,2^{14},2)$ parametreli bir ikili lineer koddur.

6. Sonuç

$\mathbb{Z}_2[u]$ halkası üzerindeki lineer ve devirli kodların $\mathbb{Z}_4$ halkası üzerindeki lineer ve devirli kodlara göre bazı avantajları olduğu iyi bilinmektedir. Özellikle, $\mathbb{Z}_2[u]$ üzerindeki lineer kodların Gray görüntüleri daima lineer iken $\mathbb{Z}_4$ için bu durum her zaman doğru değildir. Literatürde, karışık alfabeler üzerindeki kodlarla ilgili çok sayıda araştırma yapılmıştır. Bu amaçla bu makalede $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-lineer ve devirli kodlar çalışıldı. $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-lineer kodların standart üreteç ve kontrol matrislerinin formları araştırıldı. Ayrıca, $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-devirli kodların üreteç polinomları ve minimum üreteç kümeleri belirlendi. Son olarak, ayrılabilir $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-devirli kodların dualleri incelendi. Gelecek çalışmalar için ayrılabilir olmayan $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_2[u]$-devirli kodların dualleri ve bunların cebirsel yapıları araştırılabilir.

Çıkar Çatışması Beyanı

Makalenin yazarı olarak herhangi bir çıkar çatışması bulunmadığını beyan ederim.

Araştırmacıların Katkı Oranı Beyan Özeti

Makalenin yazarı olarak bu çalışmaya %100 oranında katkı sağladığımı beyan ederim.

Kaynakça

Abualrub T., Siap I., Aydin N. $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes. IEEE Trans. Inf. Theory 2014; 60(3): 1508-1514.

Aydogdu I., Abualrub T., Siap, I. On $\mathbb{Z}_2\mathbb{Z}_2[u]$-additive codes. Int. J. Comput. Math.. 2015; 92: 1806-1814.

Aydogdu I., Abualrub T., Siap I. $\mathbb{Z}_2\mathbb{Z}_2[u]$-cyclic and constacyclic codes. IEEE Trans. Inf. Theory 2017; 63(8): 4883-4893.

Aydogdu I., Gursoy F. $\mathbb{Z}_2\mathbb{Z}_4\mathbb{Z}_8$-Cyclic Codes. J. Appl. Math. Comput. 2019; 60(1-2): 327-341.

Borges J., Fernández-Córdoba C., Pujol J., Rifa J. Villanueva M. $\mathbb{Z}_2\mathbb{Z}_4$-linear codes: Generator matrices and duality, Des. Codes Cryptogrph. 2009; 54(2): 167-179.

Borges J. Fernández-Córdoba C. A characterization of $\mathbb{Z}_2\mathbb{Z}_2[u]$-linear codes. Des. Codes Cryptogrph., Des. Codes Cryptogr. 2018; 86(7): 1377-1389.

Brouwer AE., Hamalainen HO., Ostergard PRJ., Sloane NJA. Bounds on mixed binary/ternary codes. IEEE Trans. Inf. Theory 1998; 44(1): 140-161.

Çalışkan B. On one-weight and acd codes in $\mathbb{Z}_2^{\mathrm{r}} \times \mathbb{Z}_4^{\mathrm{s}} \times \mathbb{Z}_8^{\mathrm{t}}$. Filomat 2021; 35(3): 871-882.

Çalışkan B., Balıkçı K. Counting $\mathbb{Z}_2\mathbb{Z}_4\mathbb{Z}_8$ -additive codes. European Journal of Pure and Applied Mathematics 2019; 12(2): 668-679.

Çalışkan B., Özkan Ö. Serbest $\mathbb{Z}_2\mathbb{Z}_4\mathbb{Z}_8$-toplamsal kodları sayma. Erzincan Üniversitesi Fen Bilimleri Enstitüsü Dergisi 2020; 13: 70-75.

Çalışkan B. $\mathbb{Z}_8 + u\mathbb{Z}_8 + v\mathbb{Z}_8$ üzerinde aykırı devirli kodlar için bazı sonuçlar. Avrupa Bilim ve Teknoloji Dergisi 2021; 28: 660-664.

Hammons AR., Kumar PV., Calderbank AR., Sloane NJA., Solé P. The $\mathbb{Z}_4$-linearity of kerdock, preparata, goethals and related codes. IEEE Trans. Inform. Theory 1994; 40: 301-319.

Mostafanasab H. Triple cyclic codes over $\mathbb{Z}_2$. Palest. J. Math. 2017; 6(Special Issue: II): 123-134.

Siap I., Aydogdu I. The structure of $\mathbb{Z}_2\mathbb{Z}_{2^s}$-additive codes: Bounds on the minimum distance. Appl. Math. Inf. Sci. 2013; 7(6): 2271-2278.

Wu T., Gao J., Gao Y., Fu FW. $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes. Adv. Math. Commun. 2018; 12: 641-657.