SAU Fen Bilimleri Enstitüsü Dergisi
7.Cilt, 1.Sayı (Mart 2003)

$F_q[u]/(u^s)$ HALKASI ÜZERİNDEKİ LİNEER KODLARIN YAPISI VE DEKODLAMA

Nurcan Külhan, İrfan Şiap, Mehmet Özen

Özet – $F_q[u]/(u^s)$ **halkası üzerindeki lineer kodların üreteç matrislerinin yapısı ve bir dekodlama tekniği verilmektedir.** $F_2[u]/(u^2)$ **halkası üzerindeki devirli kodların yapısı incelendi. Devirli kodlar için BCH tipinde bir sınır ispatlandı. Dekodlama tekniği devirli kodlar için uygulandı.**

Anahtar kelimeler – Lineer kodlar, $F_q[u]/(u^s)$ **halkası üzerindeki kodlar, devirli kodlar, dekodlama.**

Abstract – **The structure of generator matrices and a decoding technique is given for linear codes over the ring** $F_q[u]/(u^s)$**. The structure of cyclic codes over the ring** $F_2[u]/(u^2)$ **is investigated. A BCH-type bound for cyclic codes is proven. The decoding method is applied to cyclic codes.**

Key words – Linear codes, codes over the ring $F_q[u]/(u^s)$**, cyclic codes, decoding.**

Nurcan Külhan, Şehit Üsteğmen Selçuk Esedoğlu Lisesi, ADAPAZARI
İrfan Şiap, Gaziantep Üniversitesi, Adıyaman Eğitim Fakültesi, email: siap@gantep.edu.tr, ADIYAMAN
Mehmet Özen, Sakarya Üniversitesi, Fen-Edebiyat Fakültesi, Matematik Bölümü, email:ozen@sakarya.edu.tr, SAKARYA

I.GİRİŞ

$q = p^e$ pozitif tamsayısı p asal sayısının bir tamsayı pozitif kuvveti olsun. F_q, q elemanlı sonlu bir cisim olsun. s birden büyük pozitif bir tamsayı olmak üzere

$$R_s = F_q[u]/(u^s)$$

halkası üzerindeki lineer ve R_2 üzerindeki devirli kodların cebirsel yapıları incelenecektir.

Bu halkanın özel bazı durumları literatürde aşağıdaki bazı makaleler ile işlenmiştir: $s=1$ halinde R_s halkası q elemanlı sonlu bir cisme izomorfik olduğundan bu konuda köklü çalışmalar yapılmış ve devam etmektedir MacWilliams ve Sloane [8] ve Roman [10]. Lineer kodların halkalar üzerindeki incelenmesi ise Hammons ve diğerleri [7] çalışması ile ön plana çıkmıştır. Bu çalışmada bazı önemli lineer olmayan kodların Z_4 (dört elemanlı modülo 4 tamsayıların kalan sınıfları) halkasındaki bazı lineer kodların görüntüsü olduğu gösterilmiştir. Bu yaklaşım ile lineer olmayan kodların yapıları hakkında daha iyi bilgi edinilme ve onları kolay temsil etme olanağı elde edilmiştir. Bu çalışma lineer kodların halkalar üzerinde incelenmesini hızlandırmıştır. Galois halkasının özel durumu olan Z_4 halkası üzerindeki kodlar üzerinde yapılan çalışmalar Wan [12] kitabında toplanmıştır. Sırasıyla Z_{p^k} Galois halkaları üzerindeki lineer kodları için dekodlama teknikleri Greferath ve Vellbinger [6] ile Babu ve Zimmermann [1] tarafından verilmiştir. İlk olarak, Bachoc [2] $F_p[u]/(u^2)$ halkası üzerindeki lineer kodların latisler ile olan bağlantısını göstermiş ve yeni latisler bulmuştur. Sonra, $q=2$ ve $s=2$ (dört elemanlı bir halka) olmak

üzere $F_2[u]/(u^2)$ halkası ile Z_4 arasındaki benzerlikten (bu iki halka arasında izomorfizma olmamasına karşılık u ile 2 arasında benzerlik vardır) faydalanarak $F_2[u]/(u^2)$ üzerindeki lineer kodların yapıları ile duallerinin ilişkisini ve devirli kodların yapıları ve dualleri ile olan ilişkilerini sırasıyla Dougherty ve diğerleri [4] ile Bonnecaze ve Udaya [3] makalelerinde incelenmiştir. Ayrıca, Udaya ve Bonnecaze [11] $F_2[u]/(u^2)$ halkası üzerindeki devirli kodların dekodlaması incelenmiştir.

Bu makaledeki amacımız yapılan bu çalışmaları genelleştirmek bir çatı altında toplamaktadır. Önce, iyi bilinen sonuçlardan olan R_s halkasının yapısı ve bu halka üzerindeki lineer kodların üreteç matrisleri verilecektir. II. bölümde lineer kodların bu halka üzerinde standart dekodlamada daha iyi bir dekodlama yöntemi verilecektir. III. bölümde R_2 halkası üzerindeki devirli kodların yapıları, BCH tipinde bir alt sınır verilecek ve dekodlama incelenecektir.

II. R_s ÜZERİNDEKİ KODLAR VE DEKODLAMASI

R_s halkası lokal ve temel ideal halkasıdır McDonnald [9]. R_s halkasının idealleri

$$\{0\}=(0)\subset(u^{s-1})\subset\cdots\subset(u^2)\subset(u)\subset(1)=R_s$$

şeklinde olup (u) ideali R_s halkasının tek maksimal idealidir. Ayrıca, (u) maksimal idealinin dışındaki bütün elemanlar tersinirdir (çarpmaya göre tersleri vardır). $r\in R_s$ ise

$$r=r_0+r_1u+\cdots+r_{s-1}u^{s-1}$$

olacak şekilde tek türlü belirli $0\le i\le s-1$ için $r_i\in F_q$ vardır. Dolayısıyla, $r_0\neq 0$ olan elemanlar tersinirdir.

Tanım II.1: R_s^n in R_s- alt modülü olan bir C modülüne n uzunluğunda ***lineer kod*** veya kısaca bir ***R_s-kod*** denir. C kodunun eleman sayılarına ***kod sözler*** denir.

R_s halkası sonlu olduğundan C kodunu üreten ve satırları lineer bağımsız olan sonlu bir küme vardır. Elemanları en az sayıda ve C yi üreten bu kümenin elemanlarından oluşan bir matrise C lineer kodun ***üreteç matrisi*** denir.

Teorem II.1: R_s üzerindeki sıfırdan farklı bir C kodun üreteç matrisi

$$G=\begin{bmatrix} I_{k_1} & A_{12} & A_{13} & \cdots & A_{1,s-1} & A_{1s} \\ 0 & uI_{k_2} & uA_{23} & \cdots & uA_{2,s-1} & uA_{2s} \\ 0 & 0 & u^2I_{k_3} & \cdots & u^2A_{3,s-1} & u^2A_{3s} \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & u^{s-1}I_{k_s} & u^{s-1}A_{ss} \end{bmatrix} \quad ...(I.1)$$

şeklindedir. Burada, I_{k_i} matrisleri tipleri $k_i\times k_i$ olan birim matrisler ve 0 ise ilgili tipteki sıfır matrisidir. $A_{1,j+1}, A_{2,j+1},\ldots, A_{j,j+1}$ matrislerin bileşenleri R_j (R_j, R_s içindeki kopyası) halkasındadır. Ayrıca, C kodun eleman sayısı $q^{k_1+k_2+\cdots+k_s}$.

İspat: G, C lineer kodun herhangi bir üreteç matrisi olsun. G nin bileşenleri içinde tersinir olan bir eleman varsa satır ve sütun permütasyonları uygulanarak (1,1) pozisyonuna getirilebilir. Eğer tersinir elemanı yoksa bu durumda u^j yı bölen olarak kabul eden ($g_{11}=u^jb$ ve $u\nmid b$) ve j si en küçük olan bir bileşeni vardır ve bu bileşen (1,1) pozisyonuna getirilir. Birinci durumda (1,1) bileşenindeki eleman tersinir olduğundan onun altındaki bütün bileşenler satır işlemleri ile sıfırlanabilir. İkinci durumda ise $g_{11}=u^jb$ olduğundan b tersinirdir ve birinci satır b elemanın tersi ile çarpılarak (1,1) pozisyonuna u^j elemanı getirilir. u^j elamanın j kuvveti en küçük olduğundan ve matrisinin tersinir elemanı bulunmadığından birinci sütunda bulunan u^j nin altındaki bütün bileşenler u^kd $(k\ge j)$ d tersinir tipinde olduğundan önce satırlar d nin tersi ile çarpılır ve sonra sıfırlanabilir. Yukarıda uyguladığımız metot yardımıyla verilen matrisin 1. sütunu istenen forma getirilmiş olur. Geriye kalan kısma tumevarım uyguladığımızda matris üst üçgensel forma getirilmiş olur. Birim matrisler yardımıyla gerekli elemanter işlemler uygulandığında $A_{1,j+1}, A_{2,j+1},\ldots, A_{j,j+1}$ matrislerin bileşenleri R_j halkasının birer elemanı yapılabilir. Üreteç matris üst üçgensel olduğundan satırlar lineer bağımsız olduklarından $q^{k_1+k_2+\cdots+k_s}$ tane farklı kod söz elde edilir.□

Sonuç II.1 [3,4]: R_2 üzerinde tanımlı sıfırdan farklı bir C kodunun üreteç matrisi,

$$G = \begin{bmatrix} I_{k_1} & A & B \\ 0 & uI_{k_2} & uD \end{bmatrix} \qquad (I.2)$$

formundaki bir üreteç matrise sahip bir lineer R_2 koduna (sütun) permütasyon denktir ve buradaki I_{k_1} ve I_{k_2} sırasıyla tipleri $k_1 \times k_1$ ve $k_2 \times k_2$ olan birim matrislerdir. A ve D, bileşenleri R den alınan matrislerdir. B ise bileşenleri F_2 den alınan bir matristir. C, $4^{k_1}2^{k_2}$ tipinde (kısaca (k_1, k_2) tipinde) ve $4^{k_1}2^{k_2}$ tane kodsöze sahiptir.

Tanım II.2: $R_2 = F_2 + uF_2 = \{0,1,u,1+u\}$ ve $u^2 = 0$ halkasındaki elemanlara aşağıdaki gibi Lee ağırlığı olarak adlandırılan negatif olmayan tamsayı değerleri alan bir w_L fonksiyonu tanımlanır: $w_L(0) = 0, w_L(1) = 1, w_L(1+u) = 1$ ve $w_L(u) = 2$.

Yukarıdaki ağırlık fonksiyonu yardımıyla, R_2^n modülünün elemanları arasındaki uzaklığı ölçen ve ***Lee uzaklığı*** olarak adlandırılan d_L fonksiyonu

$$d_L(c,v) = w_L(c-v)$$

şeklinde tanımlanır. (R_2^n, d_L) ikilisi bir metrik uzaydır. Ayrıca, bir C lineer ***kodun minimum Lee uzaklığı*** $d_L(C) = \min_{c \in C \setminus \{0\}} \{w_L(c)\}$ olarak tanımlanır.

Bir bilgi transferi esnasında R_2 halkası üzerinde tanımlanan bir C lineer kodun kod sözleri alıcıya ulaştığında herhangi bir sebepten dolayı (manyetik alanlar, CD deki çizikler, vs) bileşenlerinde değişiklik meydana gelebilir. Alıcı kendisine ulaşan kod sözü inceler; kod söz C kodun bir elemanı ise hata yok diye yorumlar ancak C kodun bir elemanı olmadığını görünce hatanın meydana geldiğini tespit eder (ulaşan elemanın R_2^n kümesinin bir elemanı olduğu açıktır). Bu elemana Lee uzaklığına göre en yakın olan C kodunun içindeki bir kod söz olarak yorumlar ve alıcının gönderdiği kod söz olarak alır. Bu dekodlama metoduna ***minimum uzaklığa göre dekodlama*** denir.

Önerme II.1: R_2 üzerinde tanımlı bir kodun Lee uzaklığı $2t+1$ veya $2t+2$ ise minimum uzaklık dekodlamasına göre ağırlığı en çok t olan hataları düzeltebilir.

F_q üzerinde tanımlı kodlar için ***Hamming ağırlığı*** $c = (c_0, c_1, \ldots, c_n) \in F_q^n$ olmak üzere $w_H(c) = |\{i \mid c_i \neq 0\}|$ (sıfırdan farklı bileşenlerin sayısı) olarak tanımlanır. Lee uzaklığa benzer olarak

$$d_H(c,v) = w_H(c-v)$$

Hamming uzaklığı tanımlanır. C ***kodun Hamming ağırlığı*** ise sıfırdan farklı en küçük ağırlıklı kod söze eşittir. F_q üzerinde tanımlı uzaklığı n, boyutu k ve minimum Hamming uzaklığı $d = d_H(C)$ olan C kodu $[n,k,d]_2$ ile gösterilir.

Önerme II.2:[8] F_q üzerinde tanımlı bir kodun Hamming uzaklığı $2t+1$ veya $2t+2$ ise minimum uzaklık dekodlamasına göre (Lee uzaklığına benzer) ağırlığı en çok t olan hataları düzeltebilir.

Tanım II.3: C, R_s halkası üzerinde tanımlı n uzunluğunda bir lineer kod olsun.

$$W_L(x,y) = \sum_{c \in C} y^{w_L(c)}$$

şeklinde tanımlanan $2n$. dereceden homojen polinomuna C lineer kodun ***Lee ağırlık sayacı*** denir.

Lee ağırlık sayacındaki y nin en küçük pozitif kuvveti C kodun Lee uzaklığını vermektedir.

Dekodlama kısmına geçmeden önce burada sunacağımız teknik Greferath ve Vellbinger [6] tarafından Z_{p^k} halkası üzerindeki kodlar için sunulan metoda denk fakat daha basit ve farklı bir yaklaşım ile verilecektir. Ayrıca Greferath ve Vellbinger [6] makalesinde sunulan metodun benzer şekilde R_s halkası üzerindeki kodlara uygulanabileceğini vurgulamışlardır. R_s halkası üzerinde dekodlama yapabilmek için aşağıdaki yardımcı fonksiyonları tanımlayalım: Her $0 \le i \le s-1$ için

$$\phi_i : R_s \to F_q$$

$$\phi_i\left(r_0 + r_1 u + \cdots + r_{s-1}u^{s-1}\right) = r_i .$$

Bu fonksiyonu $(c_1, c_2, \ldots, c_n) \in R_s^{\,n}$ için genişletelim:

$$\Phi_i : C \to F_q^{\,n}$$

$$(c_1, c_2, \ldots, c_n) = \left(\phi_i(c_1), \phi_i(c_2), \ldots, \phi_i(c_n)\right).$$

Yukarıdaki tanımlardan aşağıdaki önerme kolayca elde edilir.

Önerme II.3: $\Phi_i(C)$ kümesi $F_q^{\,n}$ üzerinde bir F_q-vektör uzayıdır. Yani, $\Phi_i(C)$ n uzunluğunda F_q cismi üzerinde tanımlı bir lineer kodtur.

Önerme II.4: C kodun üreteç matrisinin bir üreteç matrisi

$$G = \begin{bmatrix} B_1 \\ uB_2 \\ \vdots \\ u^{s-1}B_s \end{bmatrix}$$

şeklinde ise her $0 \le i \le s-1$ için $\Phi_i(C)$ F_q-lineer kodun bir üreteç matrisi

$$\begin{bmatrix} B_1 \\ B_2 \\ \vdots \\ B_{i+1} \end{bmatrix}$$

şeklindedir.

İspat: $c = (c_1, c_2, \ldots, c_n) \in C$ için $c = \nu G$ olacak şekilde $\nu \in R_s^{\,l}$ ve $l = k_1 + k_2 + \cdots + k_s$ vardır.

$$\nu = \left[\nu_0 + \nu_1 u + \cdots + \nu_{s-1}u^{s-1}\right] G$$

$$\nu = \nu_0 B_1 + \left(\nu_0 B_2 + \nu_1 B_1\right)u + \cdots + \left(\nu_0 B_s + \nu_1 B_{s-1} + \cdots + \nu_{s-1} B_1\right)u^{s-1}$$

ve $\nu_i \in F_q^{\,l}$ olduğundan, son toplam

$$B_1, uB_1, u^2B_1, \ldots, u^{s-1}B_1,$$
$$uB_2, u^2B_2, \ldots, u^{s-1}B_2,$$
$$\vdots$$
$$u^{s-1}B_s$$

matrislerinin satırlarının bir F_q-lineer toplamıdır.

$$c = \left(c_{10} + c_{11}u + \cdots + c_{1,s-1}u^{s-1}, \ldots, c_{n0} + c_{n1}u + \cdots + c_{n,s-1}u^{s-1}\right)$$
$$= (c_{10}, c_{20}, \ldots, c_{n0}) + \cdots + (c_{1,s-1}, \ldots, c_{n,s-1})u^{s-1}$$

olsun. $\Phi_i(c) = (c_{1i}, c_{2i}, \ldots, c_{ni}) \in F_q^{\,n}$ olduğundan $\Phi_0(c) = (c_{10}, \ldots, c_{n0})$ B_1 matrisinin satırlarının bir F_q-lineer toplamıdır. $\Phi_1(c) = (c_{11}, \ldots, c_{n1})$ ise B_1 ve B_2 matrislerin satırlarının bir F_q-lineer

toplamıdır. Dolayısıyla herhangi bir $\Phi_i(c) = (c_{1i}, c_{2i}, \ldots, c_{ni}) \in F_q^{\,n}$ ise $B_1, B_2, \ldots, B_i$ matrislerin , satırlarının bir F_q-lineer toplamıdır. □

Yukarıdaki önermenin yardımıyla R_s halkası üzerinde tanımlanan kodlar için hata düzeltme kabiliyetleri hakkında bilgi edinilebilir. □

Teorem II.2: C kodun üreteç matrisinin bir üreteç matrisi

$$G = \begin{bmatrix} B_1 \\ uB_2 \\ \vdots \\ u^{s-1}B_s \end{bmatrix}$$

şeklinde olsun. $\begin{bmatrix} B_1 \\ B_2 \\ \vdots \\ B_{i+1} \end{bmatrix}$ tarafından F_q üzerinde üretilen kod t_i hata düzeltsin. Bu durumda, C kodu $e = \Phi_0(e) + \Phi_1(e)u + \cdots + \Phi_s(e)u^{s-1} \in R_s^{\,n}$ ve $w_H(\Phi_i(e)) \le t_i$ şeklindeki tüm hataları düzeltir.

İspat: $c \in C$ kod sözünde bir $e \in R_s^{\,n}$ hatanın meydana gelmesiyle $v = c + e$ hatalı olarak alıcıya ulaştığını kabul edelim. $w_H(\Phi_i(e)) \le t_i$ olsun. $\phi_0(v)$ B_1 matrisinin ürettiği kodun elemanı olmak zorundadır. $w_H(\Phi_0(e)) \le t_0$ olduğundan ve B_1 matrisin ürettiği kod t_0 hata düzeltebildiğinden $\Phi_0(v) = \Phi_0(c)$ olarak düzeltilir. Benzer şekilde $\phi_1(v)$ B_1 ve B_2 matrislerinin ürettiği kodun elemanıdır. $w_H(\Phi_1(e)) \le t_1$ olduğundan ve B_1 ve B_2 matrislerinin ürettiği kod t_1 hata düzelttiğinden $\Phi_1(v) = \Phi_1(c)$ olarak düzeltilir. Benzer şekilde $i = 2,3,..,s-1$ için $\Phi_i(v) = \Phi_i(c)$ olarak düzeltilir. $v = \Phi_0(v) + \cdots + \Phi_{s-1}(v)u^{s-1}$ tek türlü belirli olduğundan v, c kod sözü olarak dekodlanır. □

Yukarıdaki Teorem II.2 deki yöntemin standart dekodlamanın düzeltemediği hataları nasıl düzeltebildiğini bir örnek üzerinde görelim:

Örnek II.1:

$$G = \begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & u & 0 & 0 & 0 & u & u & u & 0 & 0 & u \\ 0 & 0 & 0 & u & 0 & 0 & u & u & 0 & u & u & 0 \\ 0 & 0 & 0 & 0 & u & 0 & u & 0 & u & u & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & u & 0 & u & u & u & u & u \end{bmatrix}$$

matrisinin R_2 halkası üzerinde ürettiği C kodunu inceleyelim: C kodun Lee minimum uzaklığı 6 olduğundan C kodu standart dekodlamaya (minimum dekodlama) göre Lee ağırlığı 2 veya daha küçük olan hataları düzeltir. Önerme II.1 e göre

$$G = \begin{bmatrix} B_1 \\ uB_2 \end{bmatrix}$$

olur.

$$B_1 = \begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

olduğundan B_1 in ürettiği F_2 üzerindeki C_0 kodun minimum Hamming ağırlığı $d_H(C_0) = 6$ ve boyutu 2 olduğundan C_0 ikili kodu $[12,2,6]_2$ şeklindedir. Diğer yandan,

$$\begin{bmatrix} B_1 \\ B_2 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

olduğundan B_1 ve B_2 matrislerinin ürettiği C_1 kodun minimum Hamming ağırlığı 3 ve boyutu 4 olduğundan C_1 ikili kodu $[12,4,3]_2$ tipindedir. Önerme II.2 ye göre C_0 kodun ağırlığı 2 veya daha küçük ve C_1 ise ağırlığı 1 veya daha küçük olan hataları düzeltir. G matrisinin 1. satır ile 3. satırın toplamlarından oluşan

$c = (0,1,1+u,0,1,0,1+u,u,1+u,0,1,u)$ kod sözü alıcıya gönderilsin. Alıcıya ulaşan söz ise $v = (1,0,1,u,1,0,1+u,u,1+u,0,1,u) \notin C$ olsun.

Hata sözü $c - v = e = (1,1,u,0,0,0,0,0,0,0)$ olur.

$w_L(e) = 4$ olduğundan standart Lee minimum uzaklığına göre hata düzeltilemez! Ancak, Teorem II.2 deki yaklaşım ile

$$e = \Phi_0(e) + \Phi_1(e)u = (1,1,0,0,0,0,0,0,0,0,0,0) + (0,0,1,0,0,0,0,0,0,0,0,0)u$$

bulunur. $w_H(\Phi_0(e)) = 2$ ve $w_H(\Phi_1(e)) = 1$ olduğundan v sözü düzeltilebilirdir! Gerçekten,

$$v = \Phi_0(v) + \Phi_1(v) = (1,1,1,0,1,0,1,0,1,0,1,0) + (0,0,1,0,0,0,1,1,1,0,0,1)u$$

olduğundan C_0 ın elemanı olması gereken $\Phi_0(v)$ için $d_H(\Phi_0(u), \Phi_0(v)) = 2$ olduğundan

$\Phi_0(v) = (0,1,1,0,1,0,1,0,1,0,1,0)$ ve

C_1 kodun elemanı olması gereken $\Phi_1(v)$ için $d_H(\Phi_1(u), \Phi_1(v)) = 1$ olduğundan

$\Phi_1(v) = (0,0,1,0,0,0,1,1,1,0,1,1)$ olarak dekodlanır ve gönderilen c kodsözü bulunmuş olur.

III. R_2 ÜZERİNDEKİ DEVİRLİ KODLAR

Tanım III.1: C, R_2 üzerinde tanımlı bir lineer kod olsun. Her $(c_0, c_1, \ldots, c_n) \in C$ için $(c_n, c_0, c_1, \ldots, c_{n-1}) \in C$ oluyorsa C koduna ***devirli*** bir kod denir.

$(c_0, c_1, c_2, \ldots\ldots, c_{n-1})$ ile $c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$ polinomunu eşleştirdiğimizde, yukarıdaki tanımdan n uzunluğundaki devirli bir C kodun $R_2[x]/(x^n - 1)$ halkasının bir ideali olduğu görülür. $R_2[x]/(x^n - 1)$ üzerindeki ideallerin yapısını veren aşağıdaki önemli teoremi verelim:

Teorem III.1: [11] C uzunluğu tek olan ve R_2 üzerinde tanımlı devirli bir kod olsun. $fgh = x^n - 1$ ve f, g ve h tek türlü monik polinomlar olmak üzere $C = (fh, ufg)$ (iki üreteçli ideal). Ayrıca, C nin eleman sayısı $4^{\deg(g)} 2^{\deg(h)}$ olur.

Teorem III.2: C uzunluğu tek olan ve R_2 üzerinde tanımlı $C = (fh, ufg)$ şeklinde bir devirli kod olsun. $\Phi_0(C) = (fh)$ ve $\Phi_1(C) = (f)$ olan F_2 üzerinde tanımlı devirli kodlardır.

İspat: $\Phi_0(C)=(fh)$ olduğu kolayca görülür.

$ufh \in C$ ve $ufg \in C$ olduğundan ve $F_q[x]$ üzerinde $(h,g)=1$ olduğundan $th+sg=1$ olacak şekilde $s,t \in F_q[x]$ vardır. Dolayısıyla,

$ufth+ufsg=uf \in C$ olur ve $f \in \Phi_1(C)$ olur.

Buradan $(f) \subseteq \Phi_1(C)$ elde edilir. $\Phi_1(C) \subseteq (f)$ açık olduğundan $\Phi_1(C)=(f)$ olur. □

R_2 halkası üzerinde yukarıdaki gibi tanımlı devirli bir kodun dekodlamasında ise alıcıya ulaşan bir kod söz $v=\Phi_0(v)+\Phi_1(v)u$ olsun. $\Phi_0(v)$ kısmını (fh) devirli bir kodun elemanı olarak algılar ve dekodlarız. Diğer yandan ise $\Phi_1(v)$ kısmını ise (f) devirli kodun elemanı olarak algılar ve dekodlarız. Dolayısıyla, (fh) ve (f) devirli kodlar t_0 ve t_1 ağırlığındaki hataları düzeltebiliyorsa C kodundan gönderilen herhangi bir kod sözde $e=\Phi_0(e)+\Phi_1(e)u$ ve $w_H(\Phi_0(e)) \le t_0$, $w_H(\Phi_1(e)) \le t_1$ şeklinde bir hata oluştuğunda C kodu bu hataları düzeltebilir.

Teorem III.3 (BCH sınırı):[8,10] $C=(f(x))$ n uzunluğunda devirli bir kod olsun. α, x^n-1 polinomunun parçalanış cisminin bir ilkel elemanı olsun. f nin kökleri arasında olan α^i elemanlarının en yüksek ardışık kuvvetlerin sayısı a_f ise

$$d_H(C) \ge a_f+1$$

olur.

Yukarıdaki teorem, devirli kodlarda kodun minimum Hamming uzaklığı (ağırlığı) hakkında sadece üreteç polinomunu inceleyerek fikir sahibi olunabilir.

Aşağıdaki teoreme denk bir teorem Udaya ve Bonnecaze [11] tarafından ispatlanmıştır ancak burada geliştirdiğimiz yeni yaklaşım ile tekrar aşağıdaki gibi elde edilir.

Teorem III.4: C uzunluğu tek olan ve R_2 üzerinde tanımlı $C=(fh,ufg)$ şeklinde bir devirli kod olsun.

$$w_H(e_0) \le \left\lfloor \frac{a_{fh}+1}{2} \right\rfloor \quad w_H(e_1) \le \left\lfloor \frac{a_f+1}{2} \right\rfloor$$

olmak üzere $e=e_0+e_1u$ şeklindeki tüm hataları C devirli kodu düzeltebilir. Burada, $r \in R$ için $\lfloor r \rfloor$ r sayısından küçük en büyük tamsayıyı göstermektedir.

İspat: Teorem III.2 ye göre $\Phi_0(C)=(fh)$ ve $\Phi_1(C)=(f)$ olduğundan sırasıyla olmak üzere F_2 üzerinde tanımlı $\Phi_0(C)$ ve $\Phi_1(C)$ devirli kodların sırasıyla minimum uzaklıkları $a_{fh}+1$ ve a_f+1 sayılarından büyük eşittir. Dolayısıyla, Önerme II.2 ye göre e_0, e_1 hataları $w_H(e_0) \le \left\lfloor \frac{a_{fh}+1}{2} \right\rfloor$ $w_H(e_1) \le \left\lfloor \frac{a_f+1}{2} \right\rfloor$ şartları altında düzeltir. □

Örnek: F_2 üzerinde $x^{15}-1=fgh$ ve $f=x^9+x^6+x^5+x^4+x+1$, $h=x^2+x+1$ ve $g=x^4+x^3+1$. C, $n=15$ uzunluğunda R_2 üzerinde devirli bir kod ve $F_2 \subset R_2$ olduğundan, $C=(fh,ufg)$ devirli kodunu inceleyelim.

$$W_L(y)=1+30y^8+300y^{12}+585y^{16}+108y^{20}$$

olduğundan $d_L(C)=8$, minimum uzaklığa göre ağırlığı 3 veya daha düşük olan hataları kadar düzeltir.

Teorem III.3 e göre, $\Phi_0(C)=(fh)$ ve $a_{fh}=6$ olduğundan devirli kodun Hamming minimum uzaklığı $d_H(\Phi_0(C)) \ge 7=2\times3+1$ ve $\Phi_1(C)=(f)$ ve $a_f=5$ olduğundan devirli kodun Hamming minimum uzaklığı $d_H(\Phi_1(C)) \ge 6=2\times2+2$ şeklindedir.

Dolayısıyla, bu devirli kodlar sırasıyla $w_H(e_0) \le 3$ ve $w_H(e_1) \le 2$ hatalarını düzeltir. Yani, yukarıdaki dekodlama tekniği ile Lee ağırlığı 7 olan hatalar bile düzeltilebilir!

Gerçekte $d_H\left(\Phi_0(C)\right)=15=2\times 7+1$ ve $d_H\left(\Phi_1(C)\right)=6=2\times 2+2$ olduğundan yeni dekodlama metodu ile Lee ağırlığı 11 e kadar olan hatalar düzeltilebilir.

IV.SONUÇ

R_s halkası üzerindeki kodların üreteç matrislerinin yapısı verildi. Lee maksimum uzaklık dekodlamasından daha iyi bir dekodlama tekniği verildi. Ayrıca, Teoremin ispat kısmından R_s halkası üzerindeki kodların dekodlaması için aşağıdaki algoritmayı kullanabiliriz:

G üreteç matrisi verilsin. v sözü alıcıya ulaşsın:

1. G üreteç matrisi $G=\begin{bmatrix} B_1 \\ uB_2 \\ \vdots \\ u^{s-1}B_s \end{bmatrix}$ formuna getirilir.
2. Alıcıya ulaşan v sözü
   $v=\Phi_0(v)+\Phi_1(v)u+\cdots+\Phi_{s-1}(v)u^{s-1}$
   şeklinde yazılır.
3. F_q cismi üzerinde C_i lineer kodlarını üreten

$$\begin{bmatrix} B_1 \\ B_2 \\ \vdots \\ B_{i+1} \end{bmatrix}$$

matrislerinin hata düzeltme kabiliyetleri hesaplanır. C_i kodların t_i veya daha küçük hataları düzeltebildiğini kabul edelim.

4. Her $0\le i\le s-1$ için $\Phi_i(v)$ kod sözlerinin C_i kodlardaki hataları t_i veya daha az ise $\Phi_i(v)$ sözleri düzeltilir aksi halde hataların meydana gelmediği sonucuna varılır.

R_2 üzerinde tanımlı devirli kodlar için de yukarıdaki dekodlama algoritması uygulanabilir. Bunu yanında BCH sınırı tipinde bir teorem verildi. R_2 üzerindeki devirli kodlar üzerindeki bu dekodlama metodunun çok etkili olduğu gösterildi.

KAYNAKLAR

[1] BABU N.S., ZIMMERMANN K.H., "*Decoding of Linear Codes over Galois Rings*", IEEE Transactions on Information Theory, Vol. 47, No. 4, May 2001.

[2] BACHOC C., "*Applications of Coding Theory to the Constructions of Modular Lattices*", J. Comb. Theory Ser. A, Vol. 78, pp. 92-119, 1997.

[3] BONNECAZE, A., UDAYA, P., "*Cyclic codes and self-dual codes over* F_2+uF_2" IEEE IT, Vol 45, N. 4, pages 1250-1254, May 1999.

[4] DOUGHERTY, GABORİT, P., HARADA, M., SOLE, P., "*Type II codes over* F_2+uF_2" IEEE Trans. Inform. Theory 45, pp. 32-45, 1999.

[5] GULLIVER T. A., HARADA M., "*Construction of Optymal Type IV Self-Dual Codes over* F_2+uF_2",

[6] GREFERATH MARCUS, VELLBİNGER UTE, "*Efficient Decoding of* Z_{p^k}*-Linear Codes*", IEEE Trans. Inform. Theory, Vol. 44, No. 3, pp. 1288-1293, May 1998.

[7] HAMMONS A.R., KUMAR Jr. P. V., CALDERBANK A.R., SLOANE N.J., SOLE P, "*The* Z_4*-Linearity of Kerdock, Preparata Goethals and Related Codes*", IEEE Trans. Inform. Theory, Vol. 40, pp. 301-319, March 1994.

[8] MACWILLIAMS F.J, SLOANE N.J.A, "*The Theory of Error-Correcting Codes*", North Holland, 1977.

[9] McDONNALD B.R., "*Finite Rings with Identity*", Pure and Applied Mathematics Series, Marcel Dekker, New York, 1974.

[10] ROMAN S., "*Coding and Information Theory*", Graduate Text in Mathematics, Springer Verlag, 1992.

[11] UDAYA P., BONNECAZE A., "*Decoding of Cyclic Codes over* F_2+uF_2",

[12] WAN Z.X., "*Quaternary Codes*", Series on Applied Math., Vol. 8, World Scientific pub., Singapore, 1997.