T.C.
ONDOKUZ MAYIS ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
MATEMATİK ANA BİLİM DALI

BAZI HALKALAR ÜZERİNDE TANIMLI DEVİRLİ KODLAR HAKKINDA ARAŞTIRMALAR

Yüksek Lisans Tezi

Büşra TUSUN

Danışman

Prof. Dr. Şenol EREN

SAMSUN
2022

TEZ KABUL VE ONAYI

Büşra TUSUN tarafından, **Prof. Dr. Şenol EREN** danışmanlığında hazırlanan **"BAZI HALKALAR ÜZERİNDE TANIMLI DEVİRLİ KODLAR HAKKINDA ARAŞTIRMALAR"** başlıklı bu çalışma, jürimiz tarafından 6.7.2022 tarihinde yapılan sınav sonucunda oy birliği ile başarılı bulunarak Yüksek Lisans Tezi olarak kabul edilmiştir.

	Unvanı Adı Soyadı **Üniversitesi** **Ana Bilim/Ana Sanat Dalı**	**İmza**	**Sonuç**
Başkan **(Danışman)**	Prof. Dr. Şenol EREN Ondokuz Mayıs Üniversitesi Matematik Ana Bilim Dalı		☒ Kabul ☐ Ret
Üye	Dr. Öğr. Üyesi Abdullah DERTLİ Ondokuz Mayıs Üniversitesi Matematik Ana Bilim Dalı		☒ Kabul ☐ Ret
Üye	Dr. Öğr. Üyesi Esra ÖZTÜRK SÖZEN Sinop Üniversitesi Matematik Ana Bilim Dalı		☒ Kabul ☐ Ret

Bu tez, Enstitü Yönetim Kurulunca belirlenen ve yukarıda adları yazılı jüri üyeleri tarafından uygun görülmüştür.

ONAY
… / … / …
Prof. Dr. Ali BOLAT
Enstitü Müdürü

BİLİMSEL ETİĞE UYGUNLUK BEYANI

Hazırladığım Yüksek Lisans tezinin bütün aşamalarında bilimsel etiğe ve akademik kurallara riayet ettiğimi, çalışmada doğrudan veya dolaylı olarak kullandığım her alıntıya kaynak gösterdiğimi ve yararlandığım eserlerin Kaynaklar'da gösterilenlerden oluştuğunu, her unsurun enstitü yazım kılavuzuna uygun yazıldığını ve TÜBİTAK Araştırma ve Yayın Etiği Kurulu Yönetmeliği'nin 3. bölüm 9. maddesinde belirtilen durumlara aykırı davranılmadığını taahhüt ve beyan ederim.

Etik Kurul Gerekli mi ?

Evet ☐ (Gerekli ise ekler kısmına ekleyiniz)

Hayır ☒

İmza
06 /07/ 2022
Büşra TUSUN

TEZ ÇALIŞMASI ÖZGÜNLÜK RAPORU BEYANI

Tez Başlığı : BAZI HALKALAR ÜZERİNDE TANIMLI DEVİRLİ KODLAR HAKKINDA ARAŞTIRMALAR

Yukarıda başlığı belirtilen tez çalışması için şahsım tarafından 31.05.2022 tarihinde intihal tespit programından alınmış olan özgünlük raporu sonucunda;

Benzerlik oranı : % 9

Tek kaynak oranı : % 1 çıkmıştır.

İmza
31 /05 / 2022
Prof. Dr. Şenol EREN

ÖZET

BAZI HALKALAR ÜZERİNDE TANIMLI DEVİRLİ KODLAR HAKKINDA ARAŞTIRMALAR

Büşra TUSUN
Ondokuz Mayıs Üniversitesi
Lisansüstü Eğitim Enstitüsü
Matematik Ana Bilim Dalı
Yüksek Lisans, Temmuz/2022
Danışman: Prof. Dr. Şenol EREN

Birinci bölümde kodlama teorisi ve devirli kodlar hakkında literatür araştırmalarından bahsedilmiştir.

İkinci bölümde bazı cebirsel kavramlar, kodlama teorisi ve devirli kodlar ile ilgili temel kavramlar ve teoremler verilmiştir.

Materyal ve Yöntem bölümünün birinci kısmında, $\mathbb{Z}_4 + v\mathbb{Z}_4$ halkası tanıtılarak bu halka üzerinde tanımlı devirli kodlar gösterilmiştir. $\mathbb{Z}_4 + v\mathbb{Z}_4$ halkası üzerindeki devirli kodların bazı sonuçları anlatılmıştır.

Materyal ve Yöntem bölümünün ikinci kısmında, $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 + uv\mathbb{Z}_4$ halkası tanıtılarak bu halka üzerinde tanımlı lineer kodlar, devirli kodlar gösterilmiştir. $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 + uv\mathbb{Z}_4$ halkası üzerindeki Gray dönüşüm incelenmiştir.

Materyal ve Yöntem bölümünün son kısmında, $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 + w\mathbb{Z}_4 + uv\mathbb{Z}_4 + uw\mathbb{Z}_4 + vw\mathbb{Z}_4 + uvw\mathbb{Z}_4$ halkasının yapısı incelenerek bu halka üzerinde tanımlı devirli kodlar gösterilmiştir. Gray dönüşümü incelenmiştir ve bu halka üzerinde self-dual ve self ortogonal kodlar olduğu belirtilmiştir.

Bulgular bölümünde, $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 + w\mathbb{Z}_4 + uv\mathbb{Z}_4$ halkası elde edilerek bu halka üzerindeki devirli kodların yapısı incelenmiştir. Yeni bir uzaklık koruyan Gray dönüşüm tanımlanmıştır. $\mathbb{Z}_4$ halkası üzerindeki üreteç polinomları kullanılarak R_B halkası üzerindeki devirli kodun üreteci belirlenmiştir. Bu kodların self ortogonal ve self-dual kodlar olduğu gösterilmiştir.

Anahtar Sözcükler: Devirli kodlar, Lineer kodlar, Gray dönüşümü

ABSTRACT

RESEARCHES ON THE CYCLIC CODES OVER SOME RINGS

Büşra TUSUN
Ondokuz Mayıs University
Institute of Graduate Studies
Department of Mathematics
Master, July/2022
Supervisor: Prof. Dr. Şenol EREN

In section I, a brief survey on coding theory and cyclic codes are summarized.

In section II, basic concepts and theorems about some algebraic concepts, coding theory and cyclic codes are provided.

In the first part of the material and method section, the ring $\mathbb{Z}_4 + v\mathbb{Z}_4$ is introduced and the cyclic codes over this ring are investigated. Some consequences of cyclic codes over $\mathbb{Z}_4 + v\mathbb{Z}_4$ are described.

In the second part of the material and method section, the ring $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 + uv\mathbb{Z}_4$ presented and the linear codes and cyclic codes over this ring are illustrated. The Gray map over the ring $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 + uv\mathbb{Z}_4$ is investigated.

In the last part of the material and method section, by examining the structure of the ring $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 + w\mathbb{Z}_4 + uv\mathbb{Z}_4 + uw\mathbb{Z}_4 + vw\mathbb{Z}_4 + uvw\mathbb{Z}_4$, the cyclic codes over this ring are displayed.The investigation of the Gray map have revealed the existence of self-dual and self orthogonal codes over this ring.

In the discussion section, the ring $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 + w\mathbb{Z}_4 + uv\mathbb{Z}_4$ is obtained and the structure of the cyclic codes over this ring are examined. A new distance preserving Gray map is defined. The generator of the cyclic codes found out as self orthogonal and self-dual over ring R_B is determined by using the generator polynomials over ring $\mathbb{Z}_4$.

Keywords: Cyclic codes, Linear codes, Gray map

ÖN SÖZ VE TEŞEKKÜR

Yüksek lisans öğrenimimde bana danışmanlık yapan, beni yönlendiren yardımlarını esirgemeyen değerli hocam Sayın Prof. Dr. Şenol EREN'e sonsuz saygılarımı ve teşekkürlerimi sunarım.

Yüksek lisans eğitimim boyunca değerli bilgilerini benimle paylaşarak yardımcı olan ve desteğini esirgemeyen değerli hocam Sayın Dr. Öğr. Üyesi Abdullah DERTLİ'ye saygılarımı ve en içten teşekkürlerimi sunarım.

Hayatım boyunca her zaman yanımda olan kıymetli anneme, babama, kardeşlerime ve arkadaşlarıma teşekkür ederim.

Büşra TUSUN

İÇİNDEKİLER

SİMGELER VE KISALTMALAR

A^T	: A matrisinin transpozu
boy(V)	: V vektör uzayının boyutu
$\|C\|$	: C kodunun eleman sayısı
$C^\perp$	: C kodunun duali
$C = \langle g(x) \rangle$	: $g(x)$ tarafından üretilen C kodu
$d(C)$	: C kodunun minimum Hamming uzaklığı
$d(x, y)$	: x ile y arasındaki Hamming uzaklığı
$d_L(C)$	: C kodunun minimum Lee uzaklığı
$d_L(x, y)$	: x ile y arasındaki Lee uzaklığı
$derh(x)$	: h polinomunun derecesi
$\mathbb{F}_q$	: q elemanlı cisim
$\mathbb{F}_q^n$	: Bileşenleri $\mathbb{F}_q$ cisminin elemanı olan n uzunluğundaki vektörlerin kümesi
$\mathbb{F}_q[x]$	: Katsayıları $\mathbb{F}_q$ cisminin elemanları olan x değişkenine bağlı polinom halkaları
(n, M, d)	: n uzunluğunda M elemanlı d minimum uzaklığına sahip bir kod
$[n, k, d]$	: n uzunluğunda k boyutlu ve minimum uzaklığı d olan lineer kod
R	: $\mathbb{Z}_4 + v\mathbb{Z}_4$ halkası
R_1	: $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 + uv\mathbb{Z}_4$ halkası
R_2	: $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 + w\mathbb{Z}_4 + uv\mathbb{Z}_4 + uw\mathbb{Z}_4 + vw\mathbb{Z}_4 + uvw\mathbb{Z}_4$ halkası
R_B	: $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 + w\mathbb{Z}_4 + uv\mathbb{Z}_4$ halkası
$w_H(C)$	: C kodunun minimum Hamming ağırlığı
$w_H(x)$	: x'in Hamming ağırlığı
$w_L(C)$	: C kodunun minimum Lee ağırlığı
$w_L(x)$	: x'in Lee ağırlığı
$x.y$	: x ve y vektörlerinin iç çarpımı
$\oplus$	: Direkt toplam
$\otimes$	: Direkt çarpım

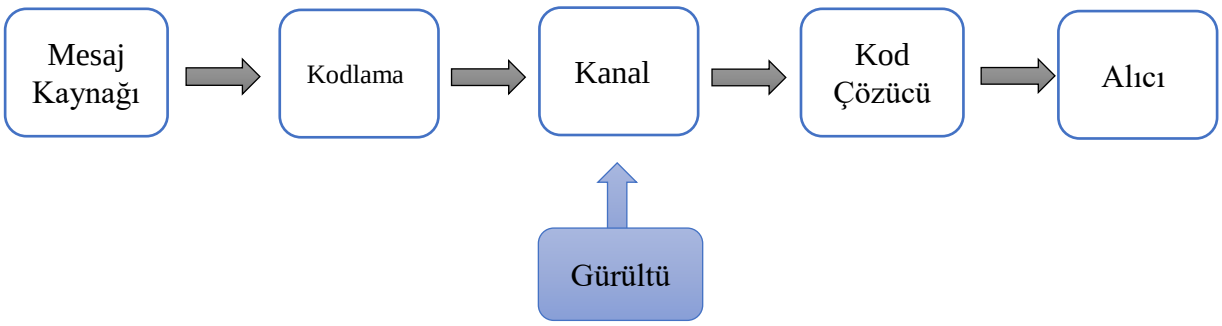
ŞEKİLLER DİZİNİ

1. GİRİŞ

Kodlama teorisinin başlangıcı Claude Shannon' un 1948 yılında yayımlanmış olan "A Mathematical Theory of Communication" adlı makalesi kabul edilmiştir. Bu makalede telefon, radyo, uydu gibi bir iletişim kanalında kodlama ve kod çözme teknikleri kullanılırsa belirlenen bir sayının altındaki değerler için güvenilir iletişimin sağlanacağı ifade edilmiştir. Başlangıç sayılan bu teoriden sonra kodlama teorisinde diğer bir adıyla hata düzeltici kodlar teorisinde, kanal boyunca kodlanmış verinin iletimi ve bozulan mesajı düzeltme gibi konularla ilgilenilmiş doğru ve iletim oranı yüksek, zaman ve enerji tasarrufu sağlayan kodlama yöntemleri geliştirme amaç edinilmiştir (Hill, 1986).

İletişimde amaç, kaynaktan gönderilen mesajı doğruluğu yüksek bir olasılıkla alıcıya ulaştırmaktır. Mesajı iletmek için alfabe olarak adlandırılan sonlu kümeler kullanılır. İletilecek mesaja oluşabilecek hatalardan korunmak üzere fazladan terim eklenir (yani kodlanır). Kodlanan mesaj kod sözcükleri olarak adlandırılır. Kod sözcüğü kanala gönderilir. Kanal bir telefon hattı, yüksek frekanslı bir radyo bağlantısı ya da bir uydu bağlantısı olabilir. Ekipman eksikliği, insan hatası ya da hava koşulları sebebiyle mesajın iletimi esnasında bazı semboller değişmiş yani hata oluşmuş olabilir. Kod çözücü hata olup olmadığını kontrol eder, hata varsa düzeltir ve orijinal mesajı elde edip alıcıya gönderir (Hill, 1986).

Aşağıda bir dijital haberleşme sistemi verilerek kodlama sistemindeki yöntemlerle kodun hatasının nasıl çözülüp, kodun nasıl elde edileceğine dair bir şema verilmiştir.



Şekil 1.1. Dijital bir haberleşme sistemi

Kodlama teorisine olan ihtiyaç gürültüden kaynaklanmaktadır. Gürültü, teknik bir terim olup kodlama sırasında oluşabilecek hataların tamamına denir. Gürültüye örnek olarak radyodaki parazitler verilebilir (Özlü, 2015).

Kod sözcüğü uzunluğu n, kod sözcüğü sayısı M ve minimum Hamming uzaklığı d olan bir kod (n, M, d) ile gösterilir. Mesajın hızlı iletilebilmesi için küçük bir n, olabildiğince çeşitli mesajlar iletilmesi için büyük bir M ve çok sayıda hatanın düzeltilmesi için büyük bir d değerine sahip olan kod iyi bir koddur.

Devirli kodlar, zengin cebirsel yapısı ile kodlama ve kod çözümleme tekniklerinin kolay uygulanabilmesi açısından lineer kodların önemli bir alt ailesidir.

Devirli kodlar, Air Force Cambrige araştırma merkezi çalışanlarından biri olan Eugene Prange tarafından keşfedilmiştir. Yapılarından dolayı devirli kodlarda kodlama ve kod çözme teknikleri kolaydır. Devirli kodlarda kullanılan kod çözücünün karmaşıklığı düzeltebilen hata sayısına bağlı olarak artmakta ve genellikle bir veya art arda gelen iki hatayı düzeltmek için kullanılmaktadır (Tuğcu, 2007). Golay kodları, BCH kodlar ve Reed-Solomon kodları gibi bazı önemli kod aileleri devirli kodlardır.

Prange tarafından bir $\mathbb{F}_q$ sonlu cismi üzerinde n uzunluğuna sahip bir devirli koda karşılık gelen $\mathbb{F}_q$ [x] $/\langle x^n - 1\rangle$ halkasının bir idealinin var olduğu gösterilmiştir. Devirli kod kavramı genelleştirilerek constacyclic (birimsel devirli), quasi-cyclic (parçalı devirli) ve negacyclic (negatif devirli) kod kavramları tanımlanmıştır. Tüm bu çalışmalar, değişmeli halkalar üzerinde tanımlı kodlara kısıtlanmıştır (Dertli, 2016).

Kodlama teorisinde çalışmalar, 1972 yılında ilk olarak Blake tarıfından sonlu halkalar üzerine taşınmıştır (Blake, 1972). Hammons ve diğerlerinin 1994 yılında yaptıkları çalışmayla beraber halkalar üzerindeki araştırmalar devam etmiştir (Hammons vd., 1994). Bu çalışmalar, lineer olmayan iyi parametrelere sahip kodlara ulaşmanın, $\mathbb{Z}_4$ sonlu halkası üzerinde tanımlanan bir Gray dönüşümü yardımıyla kolaylıkla yapılabileceğini kanıtlamıştır. Bu teknik, halkaların zengin cebirsel özelliklerinden yararlanmayı mümkün kılmakla beraber, cisimler üzerinde eleman sayısı lineer olanlara kıyasla daha fazla olan, lineer olmayan kodlar ile çalışmanın zorluklarını ortadan kaldırmıştır. Çünkü çeşitli sonlu halkalar üzerinde bazı özel lineer kodlar tanımlayarak Gray görüntü yardımıyla cisimler üzerinde lineer ya da

lineer olmayan iyi kodlar elde etme olasılığı artmıştır. Bu bağlamda, kodlama teorisinin çalışma alanı ve materyalleri sonlu cisimlerden sonlu halkalara olmak üzere önemli ölçüde değişmiştir (Güzel, 2019).

2014 yılında Rama Krishna Bandi ve Maheshanand Bhaintwal $v^2 = v$ olmak üzere $\mathbb{Z}_4 + v\mathbb{Z}_4$ halkası üzerindeki lineer kodlar ve devirli kodları incelemişlerdir (Bandi ve Bhaintwal, 2014). Bu tarihten günümüze kadar $\mathbb{Z}_4$ halkası üzerinde bir çok çalışma yapılmıştır ve yapılmaya devam etmektedir.

Bu tez çalışmasında, $\mathbb{Z}_4 + v\mathbb{Z}_4$ (Gao vd., 2014), $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 + uv\mathbb{Z}_4$ (Li vd., 2016) ve $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 + w\mathbb{Z}_4 + uv\mathbb{Z}_4 + uw\mathbb{Z}_4 + vw\mathbb{Z}_4 + uvw\mathbb{Z}_4$ (Bustomi vd., 2021) halkaları üzerindeki çalışmalardan yola çıkılarak $u^2 = u, v^2 = v, w^2 = w, uv = vu, uw = vw = 0$ olmak üzere yeni bir $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 + w\mathbb{Z}_4 + uv\mathbb{Z}_4$ halkasının cebirsel yapısı ortaya konularak bu halka üzerindeki devirli kodlar çalışıldı ve Gray görüntüsü bulundu.

2. GENEL BİLGİLER

2.1. Temel Kavramlar

Tanım 2.1.1. G boştan farklı bir küme ve "$*$", G de bir ikili işlem olsun. Aşağıdaki aksiyomları sağlayan $(G,*)$ cebirsel yapısına grup denir.

i. $\forall a,b,c \in G$ için, $a*(b*c)=(a*b)*c$ dir.

ii. $\forall a \in G$ için, $a*e=e*a=a$ olacak şekilde $\exists e \in G$ vardır.

iii. $\forall a \in G$ için, $a*a^{-1}=a^{-1}*a=e$ olacak şekilde $\exists a^{-1} \in G$ vardır (Çallıalp, 2018).

Tanım 2.1.2. $(G,*)$ bir grup ve $\forall a,b \in G$ için $a*b=b*a$ değişme özelliği de sağlanıyorsa G grubuna değişmeli grup veya Abel grubu denir (Çallıalp, 2018).

Tanım 2.1.3. G bir grup ve H,G nin boş olmayan alt kümesi olsun. Eğer H,G deki işleme göre kendi başına bir grup ise H ye, G nin alt grubu denir ve $H<G$ ile gösterilir (Çallıalp, 2018).

Tanım 2.1.4. $R \neq \emptyset$ kümesi üzerinde tanımlı iki ikili işlem "$+$" ve "$.$" olsun. Aşağıdaki aksiyomları sağlayan $(R,+,.)$ cebirsel yapısına bir halka denir.

i. $(R,+)$ bir değişmeli gruptur.

ii. $.$ işleminin R de birleşme özelliği vardır.

iii. $.$ işleminin $+$ işlemi üzerine sağdan ve soldan dağılma özellikleri vardır: $\forall a,b,c \in R$ için, $a(b+c)=ab+ac$ ve $(a+b)c=ac+bc$ dir (Çallıalp, 2018).

Tanım 2.1.5. Eğer halkanın ikinci işleme göre etkisiz elemanı varsa bu elemana, halkanın birim elemanı denir ve 1_R ile gösterilir. Böyle bir halkaya da birimli halka denir (Çallıalp, 2018).

Tanım 2.1.6. Halka ikinci işleme göre değişme özelliğine sahip ise halkaya değişmeli halka denir (Çallıalp, 2018).

Tanım 2.1.7. R halkasında, $0_R \neq a \in R$ elemanı için; $ab=0_R$ veya $ba=0_R$ olacak şekilde $\exists 0_R \neq b \in R$ bulunabilirse a ya, halkanın sıfır böleni, böyle bir b yoksa sıfır böleni değildir denir (Çallıalp, 2018).

Tanım 2.1.8. R birimli, değişmeli ve sonlu bir halka olsun. R halkasının tüm ideallerinin kümesi kapsama bağıntısına göre tam sıralı ise R halkasına sonlu zincir halkası denir (Jitman vd., 2010).

Tanım 2.1.9. Sıfır bölensiz bir halkaya tam halka denir. Birimli, değişmeli ve sıfır bölensiz halkaya da bir tamlık bölgesi denir (Çallıalp, 2018).

Tanım 2.1.10. R birimli ve değişmeli bir halka ve $R - \{0_R\} = R^*$, ikinci işlem "." ya göre bir grup ise R ye bir cisim denir (Çallıalp, 2018).

Tanım 2.1.11. p bir asal sayı $n \in \mathbb{N}$ olmak üzere $q = p^n$ elemanlı cisme Galois cismi denir. $GF(q)$ veya $\mathbb{F}_q$ ile gösterilir (Roman, 1992).

Tanım 2.1.12. R bir halka olsun. Eğer, her $a \in R$ için $na = 0$ olacak şekilde bir $n > 0$ tam sayısı varsa, böyle $n > 0$ tam sayılarının en küçüğüne R nin karakteristiği denir (Çallıalp, 2018).

Tanım 2.1.13. R bir halka ve $\emptyset \neq S \subset R$ olsun. R deki işlemlere göre S alt kümesi kendi başına bir halka ise S ye R halkasının bir alt halkası denir (Çallıalp, 2018).

Tanım 2.1.14. A, R halkasının bir alt kümesi olsun. R nin A yı kapsayan bütün alt halkalarının arakesitine A nın ürettiği alt halka denir ve $\langle A \rangle$ ile gösterilir. A nın elemanlarına da $\langle A \rangle$ nın üreteçleri denir (Çallıalp, 2018).

Tanım 2.1.15. R bir halka ve $\emptyset \neq I \subset R$ olsun.

i. $\forall a, b \in I$ için $a - b \in I$

ii. $\forall a \in I$ ve $\forall r \in R$ için, $ra \in I$ $(ar \in I)$

şartlar sağlanıyorsa I ya R nin bir sol (veya sağ) ideali denir.
I, hem sol hem de sağ idealse I ya iki taraflı ideal veya kısaca ideal denir (Çallıalp, 2018).

Tanım 2.1.16. $\{0_R\}$ ve R, her R halkasının iki idealidir. Bunlara R nin aşikar idealleri denir. Bunlardan farklı ideallerine de öz idealleri denir (Çallıalp, 2018).

Tanım 2.1.17. R değişmeli bir halka ve P de R nin kendisinden farklı bir ideali olsun. $a, b \in R; ab \in P$ ise $a \in P$ veya $b \in P$ ise P ye R nin asal ideali denir (Çallıalp, 2018).

Tanım 2.1.18. R değişmeli bir halka ve M de R nin kendisinden farklı bir ideali olsun. R nin M yi kapsayan M ve R den başka hiçbir ideali yoksa, M ye R nin maksimal ideali denir (Çallıalp, 2018).

Tanım 2.1.19. Tek bir maksimal ideali olan halkaya bir yerel (lokal) halka denir. Sonlu sayıda maksimal ideali olan halkaya ise yarı yerel (semi lokal) halka denir (Jitman vd., 2010).

Tanım 2.1.20. R halkasının, bir I idealine göre tanımlanan denklik sınıfları arasında;

$$(a+I)\oplus(b+I)=(a+b)+I, (a+I)\odot(b+I)=(ab)+I$$

ile tanımlanan $\oplus$ ve $\odot$ işlemlerine göre R/I bir halkadır. Bu halkaya R nin I idealine göre bölüm halkası denir (Çallıalp, 2018).

Tanım 2.1.21. R bir halka, x bir bilinmeyen ve $a_0, a_1, \dots, a_k$ lar R nin elemanları olmak üzere,

$$a_0 + a_1x + \cdots + a_kx^k$$

şeklindeki bir ifadeye R den katsayılı bir polinom denir. R den katsayılı tüm polinomlar $R[x]$ ile gösterilir (Çallıalp, 2018).

Tanım 2.1.22. R ve S iki halka ve $f: R \to S$ bir fonksiyon olsun $\forall\, a, b \in R$ için

i. $f(a+b)=f(a)+f(b)$

ii. $f(ab)=f(a)f(b)$

şartlar sağlanıyorsa f ye, R den S ye bir halka homomorfizması denir (Çallıalp, 2018).

Tanım 2.1.23. $f: R \to S$ homomorfizması birebir ve örten ise f ye bir izomorfizma, R ile S ye de izomorf halkalar denir (Çallıalp, 2018).

Tanım 2.1.24. R bir halka M, değişmeli bir grup olsun.

$$. : R \times M \to M$$

$$(r, m) \mapsto r.m = rm$$

ile tanımlanan "." dış işlemi aşağıdaki özellikleri sağlarsa M ye R-modül denir.

i. $\forall r \in R, \forall a, b \in M$ için $r(a+b)=ra+rb$

ii. $\forall r, s \in R, \forall a \in M$ için $(r+s)a=ra+sa$

iii. $\forall r, s \in R, \forall a \in M$ için $(rs)a=r(sa)$

Ayrıca R birimli ve $\forall a \in M$ için $1_R a = a$ ise M ye birimli R-modül denir (Hungerford, 1973).

Tanım 2.1.25. M bir R-modül olsun. N, M nin boştan farklı bir alt kümesi olmak üzere $\forall r \in R, \forall a, b \in N$ için

i. $a - b \in N$

ii. $ra \in N$

oluyorsa N ye M nin alt modülü denir (Taşçı, 2007).

Tanım 2.1.26. $A = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$ sonlu kümesine alfabe denir (Ling ve Xing, 2004).

Tanım 2.1.27. Bileşenleri A kümesinin elemanlarından oluşan sonlu dizilişlerin kümesine q-lu kod (q-ary kod) denir (Ling ve Xing, 2004).

Örnek 2.1.28. İngiliz alfabesindeki tüm kelimelerin kümesi $\{A, B, \dots, Z\}$ 26 harfli bir koddur.

Tanım 2.1.29. $\forall\, i \in \{1,2, \dots, n\}$ için $\alpha_i \in A$ olmak üzere $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)$ elemanına A üzerinde tanımlı n uzunluklu q-lu (q-ary) sözcük denir (Ling ve Xing, 2004).

Tanım 2.1.30. $\emptyset \neq C \subseteq A^n$ kümesine A üzerinde tanımlı n uzunluğunda q-lu blok kod denir. Kodun elemanlarına da kod sözcükleri denir (Ling ve Xing, 2004).

C kodunun eleman sayısı $|C| = M$ ile gösterilirse C koduna n uzunluğunda M elemanlı bir kod denir ve (n, M) parametreleri ile gösterilir.

Tanım 2.1.31. $\mathbb{F}_q = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$ olmak üzere

$$\mathbb{F}_q^n = \{(a_1, a_2, \dots, a_n) : a_i \in \mathbb{F}_q, i = 1,2, \dots, n\}$$

kümesinin elemanlarına vektör ya da sözcük denir (Ling ve Xing, 2004).

Tanım 2.1.32. Her $a, b \in \mathbb{F}_q^n$ için

$$d: \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{N} \cup \{0\}$$
$$(a, b) \mapsto d(a, b) = |\{i: a_i \neq b_i\}|$$

şeklinde tanımlanan dönüşüme Hamming uzaklığı denir (Huffman ve Pless, 2003).

Teorem 2.1.33. Hamming uzaklığı, $\forall a, b, c \in \mathbb{F}_q^n$ için

i. $d(a, b) \geq 0$

ii. $d(a, b) = 0 \Leftrightarrow a = b$

iii. $d(a,b) = d(b,a)$

iv. $d(a,c) \leq d(a,b) + d(b,c)$

özelliklerini sağlayan bir metriktir (Hill, 1986).

Tanım 2.1.34. C kodunun birbirinden farklı kod sözcüklerinin Hamming uzaklıklarının en küçüğüne C kodunun minimum uzaklığı denir ve $d(C)$ veya d ile gösterilir

$$d = d(C) = \min\{d(x,y): x \neq y, \forall x, y \in C\}$$

n uzunluklu, M elemana sahip d minimum uzaklıklı bir C kodu (n, M, d)-kod şeklinde gösterilir (Hill, 1986).

Tanım 2.1.35. $\mathbb{F}_q$ üzerinde tanımlı iki kodun biri aşağıdaki işlemlerin bir kombinasyonu ile diğerinden elde edilebiliyorsa bu kodlara denk kodlar denir.

i. Kodlardaki konumların permütasyonu

ii. Belli bir konumdaki sembollerin permütasyonu (Hill, 1986).

Tanım 2.1.36. $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n$ olmak üzere x elemanının ağırlığı x de bulunan sıfırdan farklı bileşenlerin sayısı olarak tanımlanır ve $w(x)$ ya da $w_H(x)$ ile gösterilir. $w(x) = |\{i: x_i \neq 0\}|$ dır (Hill, 1986).

Bir C kodunun sıfırdan farklı tüm kod sözcüklerinin ağırlığının en küçüğüne C kodunun minimum ağırlığı denir ve $w(C)$ ya da $w_H(C)$ ile gösterilir.

Tanım 2.1.37. $\mathbb{F}_q$ üzerindeki n boyutlu vektör uzayı $\mathbb{F}_q^n$ nin k boyutlu bir alt uzayına, uzunluğu n ve boyutu k olan C lineer kodu denir ve $[n,k]$ şeklinde gösterilir. C nin eleman sayısı $|C| = q^k$ dir (Hill, 1986).

Eğer C nin minimum uzaklığı verilirse bu durumda C lineer kodu $[n,k,d]$-kod ile gösterilir (Hill, 1986).

Teorem 2.1.38. Bir C lineer kodunun minimum uzaklığı ile minimum ağırlığı eşittir (Roman, 1992).

Tanım 2.1.39. C, $\mathbb{F}_q$ üzerinde tanımlı bir $[n,k]$-kod olsun. Her bir satırı C lineer kodunun taban elemanlarından oluşturulan $k \times n$ mertebeli matrise C kodunun üreteç matrisi denir ve G ile gösterilir. G üreteç matrisi $I_k, k \times k$ mertebeli birim matris, A, $k \times (n-k)$ mertebeli bir matris olmak üzere $(I_k|A)$ matrisine G nin standart formu adı verilir (Hill, 1986).

Tanım 2.1.40. İki $k \times n$ üreteç matristen biri aşağıdaki işlemlerle diğerinden elde ediliyorsa bu iki matris $\mathbb{F}_q$ üzerinde denk lineer $[n, k, d]$-kod üretir.

i. Satırların değişimi
ii. Bir satırın sıfırdan farklı bir skalerle çarpımı
iii. Bir satırın bir skalerle çarpımının bir diğer satıra eklenmesi
iv. Sütunların değişimi
v. Her hangi bir sütunun sıfırdan farklı bir skalerle çarpımı (Hill, 1986).

Tanım 2.1.41. Herhangi iki $x = (x_1, x_2, \dots, x_n), y = (y_1, y_2, \dots, y_n), x, y \in \mathbb{F}_q^n$ olmak üzere

$$. : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$$

$$(x, y) \longmapsto x.y = x_1y_1 + x_2y_2 + \cdots + x_ny_n$$

şeklinde tanımlanan dönüşüme iç çarpım adı verilir (Hill, 1986).

Tanım 2.1.42. $x, y \in \mathbb{F}_q^n$ olmak üzere $x.y = 0$ ise x ile y birbirine ortogonaldir denir (Hill, 1986).

Tanım 2.1.43. C, bir $[n, k]$-kod olmak üzere C deki tüm kod sözcüklerine dik olan vektörlerin kümesine C nin duali denir ve $C^\perp$ ile gösterilir.

$$C^\perp = \{x \in \mathbb{F}_q^n : \forall y \in C \; için \; x.y = 0\}$$

dir (Hill, 1986).

Teorem 2.1.44. $C, \mathbb{F}_q$ üzerinde tanımlı bir $[n, k]$-kod ve

$$G = \begin{bmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ g_{21} & g_{22} & \cdots & g_{2n} \\ \vdots & & & \vdots \\ g_{k1} & g_{k2} & \cdots & g_{kn} \end{bmatrix}_{k \times n}$$

C nin üreteç matrisi olsun. $v = (v_1, v_2, \dots, v_n) \in \mathbb{F}_q^n$ olmak üzere

$$v \in C^\perp \Leftrightarrow [v_1 v_2 \dots v_n].G^T = 0$$

olur (Hill, 1986).

Önerme 2.1.45. $C, \mathbb{F}_q$ üzerinde tanımlı bir $[n, k]$-kod olsun. Bu durumda C nin duali de $\mathbb{F}_q$ üzerinde tanımlı bir $[n, n-k]$-koddur (Hill, 1986).

Tanım 2.1.46. C bir $[n, k]$-kodu için $C^\perp$ nin üreteç matrisine C kodunun kontrol (parity-check) matrisi denir ve H ile gösterilir (Hill, 1986).

Teorem 2.1.47. $G = [I_k|A]$ bir $C, [n, k]$-kodun üreteç matrisinin standart formu ise C kodunun kontrol matrisi $H = [-A^T|I_{n-k}]$ dir (Hill, 1986).

Tanım 2.1.48. H kontrol matrisinin $H = [B|I_{n-k}]$ formuna H ın standart formu denir. Eğer lineer bir kod, $H = [B|I_{n-k}]$ standart formundaki kontrol matrisi ile tanımlanırsa bu kodun üreteç matrisi $G = [I_k|-B^T]$ dir (Hill, 1986).

2.2. Devirli Kodlar

Tanım 2.2.1. $C \subset \mathbb{F}_q^n$ alt kümesi olsun.

$\forall(a_0, a_1, \dots, a_{n-1}) \in C$ iken $(a_{n-1}, a_0, a_1, \dots, a_{n-2}) \in C$ ise C ye devirli küme denir.

C lineer kod olmak üzere C devirli bir küme ise C ye devirli kod denir (Ling ve Xing, 2004).

Örnek 2.2.2. $C = \{(0,0,0,0), (1,0,0,1), (0,1,1,0), (1,1,1,1)\} \subseteq \mathbb{F}_2^4$
kodu lineer koddur ama devirli bir küme olmadığından devirli kod değildir.

Örnek 2.2.3.

$$C_1 = \{(0,0, \dots ,0)\} \subseteq \mathbb{F}_q^n$$
$$C_2 = \{\lambda.1 : \lambda \in \mathbb{F}_q\} \subseteq \mathbb{F}_q^n$$
$$C_3 = \mathbb{F}_q^n$$

C_1, C_2 ve C_3 kodları aşikar devirli kodlardır.

Tanım 2.2.4. $n = s.l$ ve $C, \mathbb{F}_q^n$ kümesinin bir alt kümesi olmak üzere

i. $C, \mathbb{F}_q^n$ kümesinin bir alt uzayı,

ii. Her $c = \left(c_{0,0}, c_{0,1}, \dots, c_{0,l-1}, c_{1,0}, \dots, c_{1,l-1}, \dots, c_{s-1,0}, \dots, c_{s-1,l-1}\right) \in C$ için

$$T_{s,l}(c) = (c_{s-1,0}, c_{s-1,1}, \dots, c_{s-1,l-1}, c_{0,0}, \dots, c_{0,l-1}, \dots, c_{s-2,0}, \dots, c_{s-2,l-1}) \in C$$

koşulları sağlanıyorsa C ye $n = s.l$ uzunluğunda l indeksli bir quasi-cyclic (parçalı devirli) kod denir (Dertli, 2016).

Teorem 2.2.5. $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ polinom halkası bir esas ideal halkasıdır.

$$\pi: \mathbb{F}_q^n \to \mathbb{F}_q[x]/\langle x^n - 1\rangle$$
$$(a_0, a_1, \dots, a_{n-1}) \mapsto \pi(a) = \overline{a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1}}$$
$$= a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} + \langle x^n - 1\rangle$$

şeklinde tanımlanan fonksiyon bir lineer dönüşüm olmak üzere $C \subseteq \mathbb{F}_q^n$ lineer kodunun devirli kod olması için gerek ve yeter şart $\pi(C)$ nin $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ in bir ideali olmasıdır (Ling ve Xing, 2004).

Teorem 2.2.6. $I, \mathbb{F}_q[x]/\langle x^n - 1\rangle$ halkasının ideali ve $g(x), I$ idealinin sıfırdan farklı en küçük dereceli ve monik bir elemanı olsun. Bu durumda $g(x), I$ nın üretecidir ve $g(x)$ polinomu $x^n - 1$ polinomunu böler (Ling ve Xing, 2004).

Teorem 2.2.7. $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ halkasının sıfırdan farklı her idealinin en küçük dereceli monik polinomu tektir (Hill, 1986).

Tanım 2.2.8. $I \subseteq \mathbb{F}_q[x]/\langle x^n - 1\rangle$ idealinin sıfırdan farklı en küçük dereceli tek monik polinomunun denklik sınıfına I idealinin üreteci denir (Hill, 1986).

Tanım 2.2.9. C, $\mathbb{F}_q$ üzerinde tanımlı n uzunluğunda bir devirli kod ve C koduna karşılık gelen $\pi(C)$ idealindeki sıfırdan farklı en küçük dereceli monik bir polinom $g(x)$ olmak üzere, $g(x)$ polinomuna C kodunun üreteç polinomu denir ve

$$C = \langle g(x)\rangle = \{f(x).g(x) : f(x) \in \mathbb{F}_q[x]/\langle x^n - 1\rangle\}$$

şeklindedir (Ling ve Xing, 2004).

Teorem 2.2.10. $\mathbb{F}_q[x]$ halkasında $x^n - 1$ polinomunun her monik böleni $\mathbb{F}_q$ üzerinde tanımlı bir devirli kod üretir (Ling ve Xing, 2004).

Lemma 2.2.11. $g(x) = g_0 + g_1x + \cdots + g_rx^r$, devirli kodun üreteç polinomu ise $g_0 \neq 0$ dır (Hill, 1986).

Teorem 2.2.12. $g(x) = g_0 + g_1x + \cdots + g_rx^r$ polinomu n uzunluğunda C devirli kodunun üreteç polinomu olsun. C kodunun boyutu $k = boy(C) = n - der(g(x))$ ve devirli kodun üreteç matrisi

$$G = \begin{bmatrix} g(x) \\ x.g(x) \\ x^2.g(x) \\ \vdots \\ x^{k-1}.g(x) \end{bmatrix} = \begin{bmatrix} g_0 & g_1 & g_2 & \dots & g_r & 0 & 0 & \dots & 0 \\ 0 & g_0 & g_1 & \dots & & g_r & 0 & \dots & 0 \\ \vdots & & & & & & & & \vdots \\ 0 & 0 & 0 & \dots & 0 & g_0 & g_1 & \dots & g_r \end{bmatrix}$$

dir (Hill, 1986).

Tanım 2.2.13. $h(x) = a_0 + a_1x + \cdots + a_kx^k, derh(x) = k$ olmak üzere

$$h_R(x) = x^k h(x^{-1}) = a_k + a_{k-1}x + \cdots + a_0x^k$$

polinomuna $h(x)$ polinomunun ters sıralı (reciprocal) polinomu denir (Dertli, 2016).

3. MATERYAL VE YÖNTEM

Materyal ve Yöntem bölümünün birinci kısmında tanımlanan $\mathbb{Z}_4 + v\mathbb{Z}_4$ halkası üzerindeki lineer kodlar ve devirli kodlar, Jian Gao, Yun Gao ve Fang-Wei Fu tarafından hazırlanan "Some Results on Linear Codes over $\mathbb{Z}_4 + v\mathbb{Z}_4$" (Gao vd., 2014) çalışması kullanılarak incelenmiştir. Bölüm 3.2. de $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 + uv\mathbb{Z}_4$ halkası üzerindeki lineer kodlar ve devirli kodlar, Ping Li, Xuemei Guo ve Shixin Zhu in hazırlamış olduğu "Some Results of Linear Codes over the Ring $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 + uv\mathbb{Z}_4$" adlı makaledeki (Li vd., 2016) yöntemlerle elde edilmiştir. Bölüm 3.3. de tanımlanan $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 + w\mathbb{Z}_4 + uv\mathbb{Z}_4 + uw\mathbb{Z}_4 + vw\mathbb{Z}_4 + uvw\mathbb{Z}_4$ halkası üzerindeki lineer kodlar ve devirli kodlar, Bustomi, Purwa Santika ve Djoko Suprijanto tarafından hazırlanan "Linear Codes over the Ring $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 + w\mathbb{Z}_4 + uv\mathbb{Z}_4 + uw\mathbb{Z}_4 + vw\mathbb{Z}_4 + uvw\mathbb{Z}_4$" (Bustomi vd., 2021) çalışması incelenerek hazırlanmıştır.

3.1. $\mathbb{Z}_4 + v\mathbb{Z}_4$ Halkası Üzerindeki Lineer Kodlar ve Devirli Kodlar

3.1.1. $\mathbb{Z}_4 + v\mathbb{Z}_4$ Halkasının Yapısı

$R \cong \mathbb{Z}_4[v] / \langle v^2 - v \rangle$ halkası 16 elemanlı değişmeli ve karakteristiği 4 olan sonlu bir halkadır. Bu nedenle $v^2 = v$ olmak üzere bu halka $R = \mathbb{Z}_4 + v\mathbb{Z}_4$ e izomorftur. $a, b \in \mathbb{Z}_4$ olmak üzere herhangi bir $r \in R$ elemanı $r = a + vb$ olarak ifade edilir.

R halkası aşağıdaki özelliklere sahiptir.

- R nin 9 farklı ideali vardır ve bunlar (1), $(v+1)$, $(v+2)$, $(v-1)$, (2), (v), $(2v-2)$, $(2v), (0)$ dir.
- R esas ideal halkasıdır.
- R nin maksimal idealleri $(v+1)$ ve $(v+2)$ dir.
- R bir sonlu zincir halkasıdır.

Ayrıca herhangi bir $r = a + vb \in R$ nin birimsel eleman olması için gerek ve yeter koşul $a \not\equiv 0 (mod 2)$ ve $a + b \not\equiv 0 \ (mod 2)$ olmasıdır.

Tanım 3.1.1.1. R nin herhangi bir elemanı $r = a + vb$ elemanı için aşağıdaki özellikleri sağlayan

$$w_G: R \to \mathbb{N}$$

$$r \longmapsto w_G(r)$$

fonsiyonuna Gray ağırlık fonksiyonu denir.

$$a + vb \longmapsto \begin{cases} 0, & a = b = 0 \\ 1, & a = 1, b = 3 \; veya \; a = 3, b = 1 \\ 1, & a = 0, b = 1 \; veya \; a = 0, b = 3 \\ 2, & a = b = 2 \; veya \; a = 0, b = 2 \\ 2, & a = 1, b = 0 \; veya \; a = 1, \; b = 3 \\ 2, & a = 3, b = 0 \; veya \; a = 3, \; b = 2 \\ 3, & a = 1, b = 1 \; veya \; a = 3, b = 3 \\ 3, & a = 2, b = 1 \; veya \; a = 2, b = 3 \\ 4, & a = 2, b = 0 \end{cases}$$

dir.

Bir $\boldsymbol{c} = (c_0, c_1, \dots, c_{n-1}) \in R^n$ vektörünün Gray ağırlığı bileşenlerinin Gray ağırlığının toplamı yani $w_G(\boldsymbol{c}) = \sum_{i=1}^{n-1} w_G(c_i)$ olarak tanımlanır. $\forall \boldsymbol{c}_1, \boldsymbol{c}_2 \in R^n$ için Gray uzaklığı $d_G(\boldsymbol{c}_1, \boldsymbol{c}_2) = w_G(\boldsymbol{c}_1, \boldsymbol{c}_2)$ dir. Gray dönüşümü R^n e aşağıdaki şekilde genişletilebilir.

$c_i = a_i + b_i v$, $i = 0,1, \dots, n-1$ olmak üzere

$$\boldsymbol{\phi}: R^n \longmapsto \mathbb{Z}_4^{2n}$$

$$(c_0, c_1, \dots, c_{n-1}) \longmapsto (a_0, a_0 + b_0, \dots, a_{n-1}, a_{n-1} + b_{n-1})$$

dir.

$w_L(0) = 0, \; w_L(1) = w_L(3) = 1$ ve $w_L(2) = 2$ yi sağlayan $\mathbb{Z}_4 \to \mathbb{N}$ ye tanımlı fonksiyona $\mathbb{Z}_4$ deki Lee ağırlık fonksiyonu denir.

Teorem 3.1.1.2. $\boldsymbol{\phi}$ Gray dönüşümü (R^n, Gray uzaklığı) den ($\mathbb{Z}_4^{2n}$, Lee uzaklığı) e uzaklık koruyan bir dönüşümdür ve $\mathbb{Z}_4$-lineerdir.

İspat : Her $k_1, k_2 \in \mathbb{Z}_4$ $\boldsymbol{c}_1, \boldsymbol{c}_2 \in R^n$ için

$$\boldsymbol{\phi}(k_1 \boldsymbol{c}_1 + k_2 \boldsymbol{c}_2) = k_1 \boldsymbol{\phi}(\boldsymbol{c}_1) + k_2 \boldsymbol{\phi}(\boldsymbol{c}_2)$$

koşulu sağlandığı için $\boldsymbol{\phi}$ Gray dönüşümü lineer bir dönüşümdür.

$i = 0,1, \dots, n-1$ için $c_{1,i} = a_{1,i} + b_{1,i} v$ ve $c_{2,i} = a_{2,i} + b_{2,i} v$ olmak üzere R^n in herhangi iki elemanı $\boldsymbol{c}_1 = (c_{1,0}, c_{1,1}, \dots, c_{1,n-1})$ ve $\boldsymbol{c}_2 = (c_{2,0}, c_{2,1}, \dots, c_{2,n-1})$ olsun. O halde

$$\boldsymbol{c}_1 - \boldsymbol{c}_2 = (c_{1,0} - c_{2,0}, \dots, c_{1,n-1} - c_{2,n-1})$$

olup $\boldsymbol{\phi}(\boldsymbol{c}_1 - \boldsymbol{c}_2) = \boldsymbol{\phi}(\boldsymbol{c}_1) - \boldsymbol{\phi}(\boldsymbol{c}_2)$ dir. Dolayısıyla

$$d_G(\boldsymbol{c}_1, \boldsymbol{c}_2) = w_G(\boldsymbol{c}_1 - \boldsymbol{c}_2) = w_L\big(\boldsymbol{\phi}(\boldsymbol{c}_1 - \boldsymbol{c}_2)\big)$$

$$= w_L\big(\boldsymbol{\phi}(\boldsymbol{c}_1) - \boldsymbol{\phi}(\boldsymbol{c}_2)\big) = d_L\big(\boldsymbol{\phi}(\boldsymbol{c}_1), \boldsymbol{\phi}(\boldsymbol{c}_2)\big)$$

eşitliği elde edilir. O halde $\boldsymbol{\phi}$ uzaklık koruyan bir dönüşümdür.

3.1.2. $\mathbb{Z}_4 + \boldsymbol{v}\mathbb{Z}_4$ Halkası Üzerindeki Lineer Kodlar

Lemma 3.1.2.1. C, R üzerinde n uzunluğunda bir lineer kod ise $|\ C\ | = M$ ve minimum Gray uzaklığı d_G olmak üzere $\boldsymbol{\phi}(C)$, $\mathbb{Z}_4$ üzerinde $(2n, M, d_L = d_G)$ parametrelerine sahip lineer bir koddur.

İspat : Teorem 3.1.1.2. den $\boldsymbol{\phi}(C)$, $\mathbb{Z}_4$-lineerdir. Dolayısıyla $\boldsymbol{\phi}(C)$ $\mathbb{Z}_4$-lineer kod olur. $\boldsymbol{\phi}$ Gray dönüşümü tanımından $\boldsymbol{\phi}(C)$ nin uzunluğu $2n$ dir. Ayrıca, $\boldsymbol{\phi}$ nin R^n den $\mathbb{Z}_4^{2n}$ e birebir ve örten olduğu açıktır. Bu da $\boldsymbol{\phi}(C)$ nin M kod sözcüğüne sahip olduğunu gösterir. $\boldsymbol{\phi}$ nin uzaklık koruyan bir dönüşüm olması $\boldsymbol{\phi}(C)$ nin minimum Lee uzaklığının d_L olmasını sağlar.

Teorem 3.1.2.2. C bir lineer kod olsun. Bu durumda $\boldsymbol{\phi}(C)^{\perp} = \boldsymbol{\phi}(C^{\perp})$ dir. Ayrıca C self-dual ise $\boldsymbol{\phi}(C)$ de self-dualdir.

İspat: $c_{j,i} = a_{j,i} + b_{j,i}v,\ a_{j,i}, b_{j,i} \in \mathbb{Z}_4,\ j = 1,2$ ve $i = 0,1, \dots, n-1$ olmak üzere $\boldsymbol{c}_1 = (c_{1,0}, c_{1,1}, \dots, c_{1,n-1}) \in C$ ve $\boldsymbol{c}_2 = (c_{2,0}, c_{2,1}, \dots, c_{2,n-1}) \in C^{\perp}$ olsun. $\boldsymbol{c}_1.\boldsymbol{c}_2 = 0$ ise $\boldsymbol{c}_1.\boldsymbol{c}_2 = \sum_{i=0}^{n-1} c_{1,i}c_{2,i} = \sum_{i=0}^{n-1} a_{1,i}a_{2,i} + \sum_{i=0}^{n-1}\big(a_{1,i}b_{2,i} + a_{2,i}b_{1,i} + b_{1,i}b_{2,i}\big)v = 0$ olur. Bu durumda $\sum_{i=0}^{n-1} a_{1,i}a_{2,i} = 0$ ve $\sum_{i=0}^{n-1} a_{1,i}b_{2,i} + a_{2,i}b_{1,i} + b_{1,i}b_{2,i} = 0$ dir. O halde $\boldsymbol{\phi}(\boldsymbol{c}_1).\boldsymbol{\phi}(\boldsymbol{c}_2) = \sum_{i=0}^{n-1} a_{1,i}a_{2,i} + a_{1,i}a_{2,i} + a_{1,i}b_{2,i} + a_{2,i}b_{1,i} + b_{1,i}b_{2,i} = 0$ dir. Dolayısıyla $\boldsymbol{\phi}(C^{\perp}) \subseteq \boldsymbol{\phi}(C)^{\perp}$ dir. Lemma 3.1.2.1. den $|\boldsymbol{\phi}(C^{\perp})| = |\boldsymbol{\phi}(C)^{\perp}|$ elde edilir. Böylece $\boldsymbol{\phi}(C^{\perp}) = \boldsymbol{\phi}(C)^{\perp}$ dir. Bu durumda C self-dual ise $\boldsymbol{\phi}(C)$ self ortogonaldir. Lemma 3.1.2.1. den $|\boldsymbol{\phi}(C)| = |C| = 16^{n/2} = 4^{2n/2}$ dir. Böylece $\boldsymbol{\phi}(C)$ self-dualdir.

Çin Kalan Teoreminden $R = vR \oplus (1-v)R = v\mathbb{Z}_4 \oplus (1-v)\mathbb{Z}_4$ dir.
C_1 ve C_2

$$C_1 = \{\boldsymbol{x} \in \mathbb{Z}_4^n \mid \exists \boldsymbol{y} \in \mathbb{Z}_4^n, v\boldsymbol{x} + (1-v)\boldsymbol{y} \in C\}$$

$$C_2 = \{\boldsymbol{y} \in \mathbb{Z}_4^n \mid \exists \boldsymbol{x} \in \mathbb{Z}_4^n, v\boldsymbol{x} + (1-v)\boldsymbol{y} \in C\}$$

şekilde tanımlanmaktadır.

C_1 ve C_2, n uzunluğunda $\mathbb{Z}_4$-lineer kodlardır. Ayrıca R üzerinde n uzunluğunda C lineer kodu teklikle aşağıdaki gibi ifade edilir.

$$C = vC_1 \oplus (1-v)C_2$$

Teorem 3.1.2.3. C, R üzerinde n uzunluğunda bir lineer kod olsun. Bu durumda $C^{\perp} = vC_1{}^{\perp} \oplus (1-v)\, C_2{}^{\perp}$ dir. Ayrıca, C nin R üzerinde self-dual olması için gerek ve yeter koşul C_1 ve C_2 nin $\mathbb{Z}_4$ üzerinde self-dual kod olmasıdır.

İspat: $\widehat{C_1}$ ve $\widehat{C_2}$ aşağıdaki şekilde tanımlansın.

$$\widehat{C_1} = \{\boldsymbol{x} \in \mathbb{Z}_4^n \mid \exists \boldsymbol{y} \in \mathbb{Z}_4^n, v\boldsymbol{x} + (1-v)\boldsymbol{y} \in C^{\perp}\}$$

$$\widehat{C_2} = \{\boldsymbol{y} \in \mathbb{Z}_4^n \mid \exists \boldsymbol{x} \in \mathbb{Z}_4^n, v\boldsymbol{x} + (1-v)\boldsymbol{y} \in C^{\perp}\}$$

Böylece $C^{\perp} = v\widehat{C_1} + (1-v)\widehat{C_2}$ şeklinde yazılır ve bu yazılış tek türlüdür. O halde $\widehat{C_1} \subseteq C_1{}^{\perp}$ dir. Bu durumda her $\boldsymbol{x} \in C_1$ için $\boldsymbol{c}_1 \in C_1{}^{\perp}$ ve $\boldsymbol{c} = v\boldsymbol{x} + (1-v)\boldsymbol{y} \in C$ olsun. $\boldsymbol{c}_1.(v\boldsymbol{x} + (1-v)\boldsymbol{y}) = \boldsymbol{0}$ olacak şekilde en az bir $\boldsymbol{y} \in \mathbb{Z}_4^n$ vardır. $v\boldsymbol{c}_1.\boldsymbol{c} = \boldsymbol{0}$ olduğundan $v\boldsymbol{c}_1 \in C^{\perp}$ dir. $C^{\perp}$ tekliğinden $\boldsymbol{c}_1 \in \widehat{C_1}$ dir. O halde $C_1 = \widehat{C_1}$ olur. Benzer şekilde $C_2 = \widehat{C_2}$ olur. Dolayısıyla $C^{\perp} = vC_1{}^{\perp} \oplus (1-v)\, C_2{}^{\perp}$ dir.

C_1 ve C_2 kodları $\mathbb{Z}_4$ üzerinde self-dual ise C, R üzerinde self-dualdir. C self-dual ise C_1 ve C_2, $\mathbb{Z}_4$ üzerinde self ortogonaldir. Yani $C_1 \subseteq C_1{}^{\perp}$ ve $C_2 \subseteq C_2{}^{\perp}$ dir. $C_1 = C_1{}^{\perp}$ ve $C_2 = C_2{}^{\perp}$ olduğunu göstermeliyiz. Kabul edelim ki $C_1 = C_1{}^{\perp}$ ve $C_2 = C_2{}^{\perp}$ olmasın. Bu durumda $(v\boldsymbol{a} + (1-v)\boldsymbol{b})^2 \neq \boldsymbol{0}$ olacak şekilde $\boldsymbol{a} \in C_1{}^{\perp} \setminus C_1$ ve $\boldsymbol{b} \in C_2$ vardır. Bu C nin self-dual olmasıyla çelişir. Dolayısıyla $C_1 = C_1{}^{\perp}$ ve $C_2 = C_2{}^{\perp}$ dir.

Teorem 3.1.2.4. R üzerinde tanımlı keyfi n uzunluğunda self-dual kodlar vardır.

İspat: İlk olarak, R nin 2 elemanı, R üzerinde tanımlı 1 uzunluğunda self-dual bir kod üretir. İkinci olarak, C ve D n ve m uzunluklarında self-dual kod ise $C \times D$, R üzerinde $n+m$ uzunluklu self-dual koddur. $(\boldsymbol{c}_1, \boldsymbol{d}_1),\ (\boldsymbol{c}_2, \boldsymbol{d}_2) \in C \times D$ olsun. Bu durumda $(\boldsymbol{c}_1, \boldsymbol{d}_1).(\boldsymbol{c}_2, \boldsymbol{d}_2) = (\boldsymbol{c}_1.\boldsymbol{c}_2, \boldsymbol{d}_1.\boldsymbol{d}_2) = (\boldsymbol{0}, \boldsymbol{0})$ olduğundan $C \times D$ self ortogonaldir. Ayrıca C ve D, R üzerinde self-dual olduğu için $|C| = |R|^{n/2}$ ve $|D| = |R|^{m/2}$ dir. O halde $|C \times D| = |C||D| = |R|^{(n+m)/2}$ olduğundan $C \times D$ self-dualdir.

C, $\mathbb{Z}_4$-lineer kodu için, C ve $C^{\perp}$ in standart formdaki üreteç matrisleri sırasıyla G ve $G^{\perp}$ aşağıdaki şekildedir.

$$G = \begin{bmatrix} I_{k_1} & A & B \\ \mathbf{0} & 2I_{k_2} & 2C \end{bmatrix}$$

$$G^{\perp} = \begin{bmatrix} -B^t - C^t A^t & C^t & I_{n-k_1-k_2} \\ 2A^t & 2I_{k_2} & \mathbf{0} \end{bmatrix}$$

Ayrıca C ve $C^{\perp}$ sırasıyla $4^{k_1}2^{k_2}$ ve $4^{n-k_1-k_2}2^{k_2}$ tipindedir. O halde C nin $\mathbb{Z}_4$ üzerinde self-dual olması için gerek ve yeter koşul C ve $C^{\perp}$ in aynı tipte olmasıdır. Dolayısıyla C nin tipi $4^k 2^{n-2k}$ dir.

3.1.3. $\mathbb{Z}_4 + v\mathbb{Z}_4$ Halkası Üzerindeki Devirli Kodlar

Teorem 3.1.3.1. $\mathrm{C} = vC_1 \oplus (1-v)C_2$, R üzerinde tanımlı bir lineer kod olsun. C kodunun R üzerinde tanımlı bir devirli kod olması için gerek ve yeter koşul C_1 ve C_2 kodlarının $\mathbb{Z}_4$ üzerinde tanımlı devirli kodlar olmasıdır.

İspat: $(a_0, a_1, \dots, a_{n-1}) \in C_1$ ve $(b_0, b_1, \dots, b_{n-1}) \in C_2$ ve $i = 0,1, \dots, n-1$ olmak üzere $c_i = va_i + (1-v)b_i$ olsun. Bu durumda $(c_0, c_1, \dots, c_{n-1}) \in C$ dir. C kodu devirli bir kod olduğundan $(c_{n-1}, c_0, \dots, c_{n-2}) \in C$ dir. $(c_{n-1}, c_0, \dots, c_{n-2}) = v(a_{n-1}, a_0, \dots, a_{n-2}) + (1-v)\,(b_{n-1}, b_0, \dots, b_{n-2})$ olur. O halde $(a_{n-1}, a_0, \dots, a_{n-2}) \in C_1$ ve $(b_{n-1}, b_0, \dots, b_{n-2}) \in C_2$ dir. Dolayısıyla C_1 ve C_2 kodları $\mathbb{Z}_4$ üzerinde tanımlı devirli kodlardır.

Tersine, C_1, C_2 kodları $\mathbb{Z}_4$ üzerinde tanımlı devirli kodlar ve $i = 0,1, \dots, n-1$ olmak üzere $c_i = va_i + (1-v)b_i$ olacak şekilde $(c_0, c_1, \dots, c_{n-1}) \in C$ olsun. O halde $(a_0, a_1, \dots, a_{n-1}) \in C_1$ ve $(b_0, b_1, \dots, b_{n-1}) \in C_2$ dir. Dolayısıyla $(c_{n-1}, c_0, \dots, c_{n-2}) = v(a_{n-1}, a_0, \dots, a_{n-2}) + (1-v)(b_{n-1}, b_0, \dots, b_{n-2}) \in$ $vC_1 \oplus (1-v)C_2 = C$ bulunur. Bu durumda C kodu R üzerinde tanımlı bir devirli koddur.

Teorem 3.1.3.2. n tek bir pozitif tamsayı, C kodu $\mathbb{Z}_4$ üzerinde tanımlı n uzunluğunda bir devirli kod olsun. O halde $x^n - 1 = f(x)g(x)h(x)$ ve

$C = \big(f(x)g(x)\big) \oplus \big(2f(x)h(x)\big)$ olacak şekilde $f(x), g(x), h(x)$ monik polinomları vardır.

Teorem 3.1.3.3. $C = vC_1 \oplus (1-v)C_2$ kodu R üzerinde tanımlı n uzunluğunda bir devirli kod olsun. Bu durumda $f_1(x)g_1(x)h_1(x) = f_2(x)g_2(x)h_2(x) = x^n - 1$ ve $\mathbb{Z}_4$ üzerinde tanımlı $C_1 = \big(f_1(x)g_1(x)\big) \oplus \big(2f_1(x)h_1(x)\big)$, $C_2 = \big(f_2(x)g_2(x)\big) \oplus \big(2f_2(x)h_2(x)\big)$ olmak üzere $C = \big(vf_1(x)g_1(x) + (1-v)f_2(x)g_2(x)\big) \oplus \big(2vf_1(x)h_1(x) + 2(1-v)f_2(x)h_2(x)\big)$ dir.

İspat: $\tilde{C} = \big(vf_1(x)g_1(x) + (1-v)f_2(x)g_2(x)\big) \oplus \big(2vf_1(x)h_1(x) + 2(1-v)f_2(x)h_2(x)\big)$,

$$C_1 = \big(f_1(x)g_1(x)\big) \oplus \big(2f_1(x)h_1(x)\big)$$

ve

$$C_2 = \big(f_2(x)g_2(x)\big) \oplus \big(2f_2(x)h_2(x)\big)$$

olsun. Dolayısıyla $\tilde{C} \subseteq C$ olduğu açıkça görülmektedir. vC_1 için $vC_1 = vC$ dir. Benzer şekilde $(1-v)C_2 = (1-v)C$ dir. Dolayısıyla $vC_1 \oplus (1-v)C_2 \subseteq C$ dir. O halde $C = \tilde{C}$ olur.

Sonuç 3.1.3.4. $R[x]/\langle x^n - 1\rangle$ bölüm halkası esas ideal halkadır.

İspat: $x^n - 1 = f(x)g(x)h(x)$ olmak üzere $C = \big(f(x)g(x)\big) \oplus \big(2f(x)h(x)\big)$, $\mathbb{Z}_4$ üzerinde tanımlı n uzunluğunda bir devirli kod olsun. Bu durumda $C = \big(f(x)g(x) + 2f(x)\big)$ dir. Teorem 3.1.3.3. den $R[x]/\langle x^n - 1\rangle$ bir esas ideal halkasıdır.

Teorem 3.1.3.5. $f_1(x)g_1(x)h_1(x) = f_2(x)g_2(x)h_2(x) = x^n - 1$, $\mathbb{Z}_4$ üzerinde tanımlı $C_1 = \big(f_1(x)g_1(x)\big) \oplus \big(2f_1(x)h_1(x)\big)$ ve $C_2 = \big(f_2(x)g_2(x)\big) \oplus \big(2f_2(x)h_2(x)\big)$ olmak üzere $C = \big(vf_1(x)g_1(x) + (1-v)f_2(x)g_2(x)\big) \oplus \big(2vf_1(x)h_1(x) + 2(1-v)f_2(x)h_2(x)\big)$ olsun. Bu durumda C nin self-dual olması için gerek ve yeter koşul $f_1(x) = h_1^*(x)$, $g_1(x) = g_1^*(x)$ ve $f_2(x) = h_2^*(x)$, $g_2(x) = g_2^*(x)$ olmasıdır.

İspat: $C^\perp = vC_1{}^\perp \oplus (1-v)\, C_2{}^\perp$ olduğundan C bir devirli kod ise $C^\perp$ de devirli bir koddur. Ayrıca Teorem 3.1.2.3. den, C nin R üzerinde tanımlı self-dual olması için gerek ve yeter koşul C_1 ve C_2 nin $\mathbb{Z}_4$ üzerinde tanımlı self-dual olmasıdır.

Teorem 3.1.3.6. n tek, C n uzunluğunda bir devirli kod olsun. $C = \langle e(x)\rangle$ olacak şekilde bir tek $e(x) = ve_1(x) + (1-v)e_2(x) \in R_n = R[x] \,/\, \langle x^n - 1\rangle$ idempotent elemanı vardır.

İspat: n tek olsun, $C_1 = \langle e_1(x) \rangle$ ve $C_2 = \langle e_2(x) \rangle$ olacak şekilde bir tek $e_1(x),\ e_2(x) \in \mathbb{Z}_4[\mathrm{x}]$ üreteç idempotent elemanları vardır. Teorem 3.1.3.3. den $C = \langle ve_1(x) + (1-v)e_2(x) \rangle$ dir. $e(x) = ve_1(x) + (1-v)e_2(x)$ olsun. Bu durumda $e(x)^2 = ve_1(x)^2 + (1-v)e_2(x)^2 = ve_1(x) + (1-v)e_2(x) = e(x)$ dir. Dolayısıyla $e(x)$, C nin idempotent elemanıdır. $C = \langle d(x) \rangle$ ve $d(x)^2 = d(x)$ olacak şekilde $d(x) \in C$ var olsun. O halde $d(x) \in C = \langle e(x) \rangle$ olduğundan $d(x) = a(x)e(x)$ olacak şekilde $a(x) \in R_n = R[x]/\langle x^n - 1 \rangle$ vardır. Böylece $d(x)e(x) = a(x)e(x)^2 = d(x)$ olur. Benzer şekilde $d(x)e(x) = e(x)$ olur. Yani $d(x) = e(x)$ elde edilir.

Yukarıdaki teoremde $e(x)$ idempotent elemanı C nin idempotent üreteci olarak adlandırılır.

Teorem 3.1.3.7. $C = ve_1(x) \oplus (1-v)e_2(x)$, R üzerinde tanımlı, n uzunluğunda bir devirli kod ve $\mathbb{Z}_4$ üzerinde tanımlı C_1 ve C_2 nin idempotentleri sırasıyla $e_1(x)$ ve $e_2(x)$ olmak üzere $e(x) = ve_1(x) + (1-v)e_2(x)$ olsun. Dolayısıyla $C^{\perp}$ in idempotenti $1 - e(x^{-1})$ dir.

İspat: Teorem 3.1.2.3. den $C^{\perp} = v{C_1}^{\perp} \oplus (1-v)\ {C_2}^{\perp}$ dir. Ayrıca ${C_1}^{\perp}$ ve ${C_2}^{\perp}$ devirli kodlar olduğundan $C^{\perp}$ de devirli koddur. C_1 ve C_2 nin idempotentleri sırasıyla $e_1(x)$ ve $e_2(x)$ olsun. Bu durumda ${C_1}^{\perp}$ ve ${C_2}^{\perp}$ in idempotentleri sırasıyla

$1 - e_1(x^{-1}), 1 - e_2(x^{-1})$ dir. $C^{\perp}$ in idempotenti $\hat{e}(x)$ olsun. Dolayısıyla Teorem 3.1.3.6. dan $\hat{e}(x) = v\big(1 - e_1(x^{-1})\big) + (1-v)\big(1 - e_2(x^{-1})\big) = 1 - e(x^{-1})$ olur.

3.2. $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 + uv\mathbb{Z}_4$ Halkası Üzerindeki Lineer Kodlar ve Devirli Kodlar

3.2.1. $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 + uv\mathbb{Z}_4$ Halkasının Yapısı

$R_1 \cong \mathbb{Z}_4[u,v] \,/\, \langle u^2 - u, v^2 - v, uv - vu \rangle$ halkası değişmeli sonlu bir halkadır. Bu nedenle $u^2 = u, v^2 = v, uv = vu$ olmak üzere bu halka

$R_1 = \mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 + uv\mathbb{Z}_4$ e izomorftur. $a, b, c, d \in \mathbb{Z}_4$ olmak üzere herhangi $r \in R_1$ elemanı $r = a + ub + vc + uvd$ olarak ifade edilir.

$e_1 = 1 - u - v + uv,\ e_2 = u - uv,\ e_3 = v - uv,\ e_4 = uv$ olsun. O halde $e_1, e_2, e_3, e_4,\ R_1$ üzerinde tanımlı ikili olarak ortogonal sıfırdan farklı idempotent elemanlardır ve $e_1 + e_2 + e_3 + e_4 = 1$ dir. Çin Kalan teoreminden

$R_1 = e_1R_1 \oplus e_2R_1 \oplus e_3R_1 \oplus e_4R_1$ ve $r_1 = a,\ r_2 = a + b,\ r_3 = a + c,\ r_4 = a + b + c + d$ olmak üzere $r = r_1e_1 + r_2e_2 + r_3e_3 + r_4e_4$ dir. Bu durumda

$$\phi : r \longmapsto (r_1, r_2, r_3, r_4)$$

$\mathbb{Z}_4$-lineer dönüşümü tanımlanır.

$c_i = r_{1,i}, e_1 + \cdots + r_{4,i}, e_4 \in R_1$ ve ϕ, R_1 halkası üzerinde tanımlı Gray dönüşüm olmak üzere

$$\phi: R_1^n \longmapsto \mathbb{Z}_4^{4n}$$

$$r \longmapsto (r_1, r_2, r_3, r_4)$$

$$(c_0, c_1, \dots, c_{n-1}) \longmapsto (r_{1,0}, \dots, r_{1,n-1}, r_{2,0}, \dots, r_{2,n-1}, r_{3,0}, \dots, r_{3,n-1} r_{4,0}, \dots, r_{4,n-1})$$

şeklinde R_1^n e genişletilebilir.

3.2.2. $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 + uv\mathbb{Z}_4$ Halkası Üzerindeki Lineer Kodlar

$\boldsymbol{r}^{(i)} = r_{i1}e_1 + r_{i2}e_2 + r_{i3}e_3 + r_{i4}e_4$ ve $i = 0,1, \dots, n-1$ olmak üzere $\boldsymbol{r} = (r^{(0)}, r^{(1)}, \dots, r^{(n-1)}) \in R_1^n$ dir. O halde $\boldsymbol{r}_j = (r_{0j}, r_{1j}, \dots, r_{n-1j}) \in \mathbb{Z}_4^n$ ve $j = 1,2,3,4$ olmak üzere $\boldsymbol{r} = \boldsymbol{r}_1e_1 + \boldsymbol{r}_2e_2 + \boldsymbol{r}_3e_3 + \boldsymbol{r}_4e_4$ dir. $\forall \boldsymbol{r}, \boldsymbol{s} \in R_1^n$ vektörlerinin çarpımı, $\boldsymbol{s} = \boldsymbol{s}_1e_1 + \boldsymbol{s}_2e_2 + \boldsymbol{s}_3e_3 + \boldsymbol{s}_4e_4$, $\boldsymbol{s}_j = (s_{0j}, s_{1j}, \dots, s_{n-1j}) \in \mathbb{Z}_4^n$ ve $\boldsymbol{r}_j.\boldsymbol{s}_j = \sum_{k=0}^{n-1} r_{kj}s_{kj}$ olmak üzere $\boldsymbol{r}.\boldsymbol{s} = (\boldsymbol{r}_1.\boldsymbol{s}_1)e_1 + (\boldsymbol{r}_2.\boldsymbol{s}_2)e_2 + (\boldsymbol{r}_3.\boldsymbol{s}_3)e_3 + (\boldsymbol{r}_4.\boldsymbol{s}_4)e_4$ şeklinde yazılır.

C, R_1 üzerinde tanımlı bir lineer kod olsun. C_i $(1 \le i \le 4)$ olmak üzere

$$C_1 = \{\boldsymbol{a} \in \mathbb{Z}_4^n \mid \boldsymbol{a}e_1 + \boldsymbol{b}e_2 + \boldsymbol{c}e_3 + \boldsymbol{d}e_4 \in C, \exists \boldsymbol{b}, \boldsymbol{c}, \boldsymbol{d} \in \mathbb{Z}_4^n\}$$

$$C_2 = \{\boldsymbol{b} \in \mathbb{Z}_4^n \mid \boldsymbol{a}e_1 + \boldsymbol{b}e_2 + \boldsymbol{c}e_3 + \boldsymbol{d}e_4 \in C, \exists \boldsymbol{a}, \boldsymbol{c}, \boldsymbol{d} \in \mathbb{Z}_4^n\}$$

$$C_3 = \{\boldsymbol{c} \in \mathbb{Z}_4^n \mid \boldsymbol{a}e_1 + \boldsymbol{b}e_2 + \boldsymbol{c}e_3 + \boldsymbol{d}e_4 \in C, \exists \boldsymbol{a}, \boldsymbol{b}, \boldsymbol{d} \in \mathbb{Z}_4^n\}$$

$$C_4 = \{\boldsymbol{d} \in \mathbb{Z}_4^n \mid \boldsymbol{a}e_1 + \boldsymbol{b}e_2 + \boldsymbol{c}e_3 + \boldsymbol{d}e_4 \in C, \exists \boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c} \in \mathbb{Z}_4^n\}$$

$1 \le i \le 4$ için C_i kodu $\mathbb{Z}_4$ üzerinde tanımlı n uzunluğunda bir lineer koddur ve C kodu $C = e_1C_1 \oplus e_2C_2 \oplus e_3C_3 \oplus e_4C_4$ şeklinde tek türlü yazılabilir. Ayrıca

$$|C| = |C_1|.|C_2|.|C_3|.|C_4|$$

dir.

Teorem 3.2.2.1. C, R_1 üzerinde tanımlı n uzunluğunda bir lineer kod olsun.

(1) C_i $(1 \leq i \leq 4)$ $\mathbb{Z}_4$ üzerinde tanımlı n uzunluğunda bir lineer kod olmak üzere $C = e_1C_1 \oplus e_2C_2 \oplus e_3C_3 \oplus e_4C_4$ dir.

(2) ${C_i}^{\perp}$, C_i $(1 \leq i \leq 4)$ nin dual kodu olmak üzere $C^{\perp} = e_1C_1^{\perp} \oplus e_2C_2^{\perp} \oplus e_3C_3^{\perp} \oplus e_4C_4^{\perp}$ dir.

(3) C nin self ortogonal bir kod olması için gerek ve yeter koşul C_i $(1 \leq i \leq 4)$ nin $\mathbb{Z}_4$ üzerinde self ortogonal bir kod olmasıdır. Ayrıca C nin self-dual kod olması için gerek ve yeter koşul C_i $(1 \leq i \leq 4)$ nin $\mathbb{Z}_4$ üzerinde self-dual kod olmasıdır.

İspat:

(1) İspatı açıktır

(2) $D = e_1C_1^{\perp} \oplus e_2C_2^{\perp} \oplus e_3C_3^{\perp} \oplus e_4C_4^{\perp}$ olsun. $\boldsymbol{c} = \boldsymbol{c}_1e_1 + \boldsymbol{c}_2e_2 + \boldsymbol{c}_3e_3 + \boldsymbol{c}_4e_4$, $\boldsymbol{d} = \boldsymbol{d}_1e_1 + \boldsymbol{d}_2e_2 + \boldsymbol{d}_3e_3 + \boldsymbol{d}_4e_4$, $\boldsymbol{c}_i \in C_i$, $\boldsymbol{d}_i \in {C_i}^{\perp}$ olmak üzere $\forall\, \boldsymbol{c} \in C, \boldsymbol{d} \in D$ için $\boldsymbol{c}.\boldsymbol{d} = \sum_{i=1}^{4}(\boldsymbol{c}_i.\boldsymbol{d}_i)e_i$ dir. Dolayısıyla $\boldsymbol{c}.\boldsymbol{d} = 0$ dir. Bu durumda $D \subseteq C^{\perp}$ olur. Ayrıca

$$|D| = |C_1^{\perp}||C_2^{\perp}||C_3^{\perp}||C_4^{\perp}| = \frac{4^n}{|C_1|}\frac{4^n}{|C_2|}\frac{4^n}{|C_3|}\frac{4^n}{|C_4|} = \frac{|R_1|^n}{|C|} = |C^{\perp}|$$

dir. Dolayısıyla $C^{\perp} = D$ olur.

(3) C nin self ortogonal bir kod olması için gerek ve yeter koşul $C \subseteq C^{\perp}$ olmasıdır. (1) ve (2) den $C \subseteq C^{\perp}$ olması için gerek ve yeter koşul $C_i \subseteq {C_i}^{\perp}$ $(1 \leq i \leq 4)$ olmasıdır. O halde C_i $(1 \leq i \leq 4)$ $\mathbb{Z}_4$ üzerinde self ortogonal koddur. Benzer şekilde C kodunun self-dual bir kod olması için gerek ve yeter koşul C_i $(1 \leq i \leq 4)$ kodunun $\mathbb{Z}_4$ üzerinde bir self-dual kod olmasıdır.

Sonuç 3.2.2.2. R_1 üzerinde keyfi uzunluklu self-dual kodlar vardır.

İspat: Teorem 3.2.2.1. den R_1 üzerinde tanımlı self-dual kod olması için gerek ve yeter koşul $\mathbb{Z}_4$ üzerinde tanımlı self-dual kod olmasıdır. Aşağıdaki üreteç matrisi ile üretilen $\mathbb{Z}_4$ üzerinde tanımlı self-dual bir kod vardır.

$$\begin{bmatrix} 2 & & \\ & \ddots & \\ & & 2 \end{bmatrix}$$

Not 3.2.2.3.

$$G_i = \begin{bmatrix} I_{k_{i1}} & A_i & B_i \\ 0 & 2I_{k_{i2}} & 2C_i \end{bmatrix}$$

$(1 \leq i \leq 4)$

$\mathbb{Z}_4$ üzerinde tanımlı C_i kodlarının üreteç matrisi olmak üzere $C = e_1C_1 \oplus e_2C_2 \oplus e_3C_3 \oplus e_4C_4$ kodunun üreteç matrisi

$$G = \begin{bmatrix} e_1G_1 \\ e_2G_2 \\ e_3G_3 \\ e_4G_4 \end{bmatrix}$$

dir.

$$G_i' = \begin{bmatrix} -B_i^t - C_i^t A_i^t & C_i^t & I_{n-k_{i1}-k_{i2}} \\ 2A_i^t & 2I_{k_{i2}} & 0 \end{bmatrix}$$

$\mathbb{Z}_4$ üzerinde tanımlı C_i lineer kodunun duali $C_i{}^{\perp}$ in üreteç matrisi olmak üzere $C^{\perp}$ kodunun üreteç matrisi

$$H = \begin{bmatrix} e_1G_1' \\ e_2G_2' \\ e_3G_3' \\ e_4G_4' \end{bmatrix}$$

dir.

H, C kodunun kontrol matrisi olarak adlandırılır.

R_1 üzerinde tanımlı lineer kodların Gray görüntülerinin bazı özelliklerini inceleyelim. R_1 üzerindeki Lee ağırlığı ve Gray dönüşüm tanımından, ϕ, R_1^n den $\mathbb{Z}_4^{4n}$ e uzaklık koruyan bir dönüşümdür. C, R_1 üzerinde tanımlı n uzunluğunda bir lineer kod olsun. $\boldsymbol{c} = \boldsymbol{c}_1e_1 + \boldsymbol{c}_2e_2 + \boldsymbol{c}_3e_3 + \boldsymbol{c}_4e_4 \in C$ ise $\phi(\boldsymbol{c}) = (\boldsymbol{c}_1, \boldsymbol{c}_2, \boldsymbol{c}_3, \boldsymbol{c}_4) \in \mathbb{Z}_4^{4n}$ dir. A, B, C, D $\mathbb{Z}_4$ üzerinde n uzunluğunda lineer kodlar ise $A \otimes B \otimes C \otimes D = \{(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}, \boldsymbol{d}) : \boldsymbol{a} \in A, \boldsymbol{b} \in B, \boldsymbol{c} \in C, \boldsymbol{d} \in D\}$ dir.

Teorem 3.2.2.4. $C = e_1C_1 \oplus e_2C_2 \oplus e_3C_3 \oplus e_4C_4$ R_1 üzerinde tanımlı n uzunluğunda lineer kod olsun. O halde $\phi(C) = C_1 \otimes C_2 \otimes C_3 \otimes C_4$ ve $\phi(C^{\perp}) = \phi(C)^{\perp}$ dir. Ayrıca C self-dual kod ise $\phi(C)$ de self-dual koddur.

İspat:

$C_1 \otimes C_2 \otimes C_3 \otimes C_4 \subseteq \phi(C)$ ve $|C_1 \otimes C_2 \otimes C_3 \otimes C_4| = |C_1|.|C_2|.|C_3|.|C_4| = |C|$

olduğu kolaylıkla görülür. O halde $\phi(C) = C_1 \otimes C_2 \otimes C_3 \otimes C_4$ olur. Teorem 3.2.2.1. (2) den $\phi(C^{\perp}) = C_1^{\perp} \otimes C_2^{\perp} \otimes C_3^{\perp} \otimes C_4^{\perp}$ olduğu açıktır. Bu durumda $|\phi(C^{\perp})| = \frac{4^{4n}}{|C|}$ dir.

$\boldsymbol{c}_i \in C_i$, $\boldsymbol{d}_i \in C_i^{\perp}$ olmak üzere $\boldsymbol{c} = \boldsymbol{c}_1e_1 + \boldsymbol{c}_2e_2 + \boldsymbol{c}_3e_3 + \boldsymbol{c}_4e_4 \in C$, $\boldsymbol{d} = \boldsymbol{d}_1e_1 + \boldsymbol{d}_2e_2 + \boldsymbol{d}_3e_3 + \boldsymbol{d}_4e_4 \in C^{\perp}$ dir. Dolayısıyla $\phi(\boldsymbol{c}).\phi(\boldsymbol{d}) = \sum_{i=1}^{4}(\boldsymbol{c}_i.\boldsymbol{d}_i) = 0$ dir. Bu durumda $\phi(C)^{\perp} \supseteq \phi(C^{\perp})$ olur. Ayırca $|\phi(C)^{\perp}| = \frac{4^{4n}}{\boldsymbol{\phi}(C)} = |\phi(C^{\perp})|$ dir. O halde $\phi(C)^{\perp} = \phi(C^{\perp})$ eşitliği elde edilir.

C_i kodunun üreteç matrisi G_i $(1 \leq i \leq 4)$ olsun. Teorem 3.2.2.4. den $\phi(C)$ nin üreteç matrisi

$$\begin{bmatrix} G_1 & 0 & 0 & 0 \\ 0 & G_2 & 0 & 0 \\ 0 & 0 & G_3 & 0 \\ 0 & 0 & 0 & G_4 \end{bmatrix}$$

dir.

3.2.3. $\mathbb{Z}_4 + \boldsymbol{u}\mathbb{Z}_4 + \boldsymbol{v}\mathbb{Z}_4 + \boldsymbol{uv}\mathbb{Z}_4$ Halkası Üzerindeki Devirli Kodlar

Teorem 3.2.3.1. $C = e_1C_1 \oplus e_2C_2 \oplus e_3C_3 \oplus e_4C_4$ olsun. C, R_1 üzerinde devirli bir kod olması için gerek ve yeter koşul aşağıdaki üç koşuldan birinin sağlanmasıdır.

(1) $(1 \leq i \leq 4)$ için C_i, $\mathbb{Z}_4$ üzerinde tanımlı devirli koddur.

(2) $(1 \leq i \leq 4)$ için $C_i^{\perp}$, $\mathbb{Z}_4$ üzerinde tanımlı devirli koddur.

(3) $C^{\perp}$, R_1 üzerinde tanımlı devirli bir koddur.

İspat: $\forall c_i = (c_{i,0}, c_{i,1}, \dots, c_{i,n-1}) \in C_i$ $(1 \leq i \leq 4)$ için $c = c_1e_1 + c_2e_2 + c_3e_3 + c_4e_4 \in C$ dir. C bir devirli kod olduğundan $d = \left(\sum_{i=1}^{4} e_ic_{i,n-1}, \sum_{i=1}^{4} e_ic_{i,0}, \dots, \sum_{i=1}^{4} e_ic_{i,n-2}\right) \in C$ dir. Dolayısıyla $i = 1,2,3,4$ için $(c_{i,n-1}, c_{i,0}, \dots, c_{i,n-2}) \in C_i$ olur. Böylece C_i, $\mathbb{Z}_4$ üzerinde tanımlı devirli koddur.

Tersine, C_i, $\mathbb{Z}_4$ üzerinde tanımlı devirli kod olduğundan $C_i^{\perp}$, $\mathbb{Z}_4$ üzerinde tanımlı devirli koddur. (1) den $C^{\perp}$, R_1 üzerinde tanımlı devirli bir koddur. Ayrıca C, R_1 üzerinde tanımlı devirli bir koddur.

$R_n = R[x]/\langle x^n - 1\rangle$ olsun. R_1 üzerinde tanımlı n uzunluğunda devirli kodlar R_n in idealleridir. R_1 üzerinde tanımlı devirli kodların üreteç polinomlarını oluşturmak için $\mathbb{Z}_4$ üzerinde tanımlı C_i nin üreteç polinomları kullanılır.

Lemma 3.2.3.2. $f_1(x) \dots f_r(x)$ indirgenemez polinomlar, n tek tamsayı $x^n - 1 = \prod_{i=1}^{r} f_i(x)$ olmak üzere C, $\mathbb{Z}_4$ üzerinde n uzunluğunda devirli bir kod

olsun. Bu durumda $f_0(x)$ ve $f_1(x)$, x^n-1 in monik bölenleri ve $f_1(x)|f_0(x)$ olmak üzere $C=\langle f_0(x),2f_1(x)\rangle=\langle f_0(x)+2f_1(x)\rangle$ dır.

Genel olarak herhangi bir n uzunluğunda $\mathbb{Z}_4$ üzerinde lineer kod ise $f(x),g(x),p(x)\in\mathbb{Z}_4[x]$ monik polinomları vardır. $g(x)|f(x)|(x^n-1)$, $g(x)|p(x)\left(\frac{x^n-1}{f(x)}\right)$ ve $|C|=2^{2n-der(f(x))-der(g(x))}$ olmak üzere $C=\langle f(x)+2p(x),2g(x)\rangle$dir.

Teorem 3.2.3.3. $\mathrm{C}=e_1C_1\oplus e_2C_2\oplus e_3C_3\oplus e_4C_4$, R_1 üzerinde tanımlı n uzunluğunda bir devirli kod olsun. Eğer $C_i=\langle f_i(x)+2p_i(x),2g_i(x)\rangle$ olacak şekilde $f_i(x),g_i(x),p_i(x)\in\mathbb{Z}_4[x]$, $(1\le i\le 4)$ varsa bu durumda

$$C=\langle\sum_{i=1}^{4}e_if_i(x)+2\sum_{i=1}^{4}e_ip_i(x),2\sum_{i=1}^{4}e_ig_i(x)\rangle$$

dir. Ayrıca n tek ise

$$C=\langle\sum_{i=1}^{4}e_i(f_i(x)+2g_i(x))\rangle$$

dir.

İspat: $D=\langle\sum_{i=1}^{4}e_if_i(x)+2\sum_{i=1}^{4}e_ip_i(x),2\sum_{i=1}^{4}e_ig_i(x)\rangle$ olsun. $\forall c(x)\in C$ için $c(x)=\sum_{i=1}^{4}e_i(\big(f_i(x)+2p_i(x)\big)u_i(x)+2g_i(x)v_i(x))$ olacak şekilde $u_i(x),v_i(x)\in\mathbb{Z}_4[x]$ dir. O halde

$$\sum_{i=1}^{4}e_i(\big(f_i(x)+2p_i(x)\big)u_i(x)+2g_i(x)v_i(x))$$

$$=\sum_{i=1}^{4}e_iu_i(x)\sum_{i=1}^{4}e_i\big(f_i(x)+2p_i(x)\big)+\sum_{i=1}^{4}e_iv_i(x)\sum_{i=1}^{4}2e_ig_i(x)$$

olduğundan $C\subseteq D$ dir. $D\subseteq C$ olduğu açıktır. Dolayısıyla $C=D$ elde edilir.

C nin dual kodunun üreteç polinomunu inceleyelim. $\forall f(x)|(x^n-1)$, $\hat{f}(x)=\frac{x^n-1}{f(x)}$ olsun. $f(x)$ polinomunun tersini $f(x)^*=x^{der(f)}f(x^{-1})$ ve sıfırlayıcısını $Ann(C)=\{c'|c.c'=0,c\in C\}$ şeklinde tanımlayalım. C, $\mathbb{Z}_4$ üzerinde n uzunluğunda bir devirli kod olsun. Bu durumda $g(x)\mid f(x)\mid(x^n-1),der(p(x))<der(g(x))$ ve $p(x)\frac{x^n-1}{f(x)}=g(x)u(x)$ olmak

üzere $C = \langle f(x) + 2p(x), 2g(x) \rangle$ vardır. Dolayısıyla $\big(\hat{g}(x) + 2u(x)\big)\big(f(x) + 2p(x)\big) = 2\big(f(x)u(x) + \hat{g}(x)p(x)\big) = 0$ ve $der(u(x)) < der(\hat{g}(x))$ dir.

Teorem 3.2.3.4. $C = \langle f(x) + 2p(x), 2g(x) \rangle$, $\mathbb{Z}_4$ üzerinde n uzunluğunda bir devirli kod olsun. O halde $C^{\perp} = \langle \hat{g}(x)^* + 2x^{der(\hat{g}(x)) - der(u(x))} u(x)^*, 2\hat{f}(x)^* \rangle$ dir.

İspat: $D = \langle \hat{g}(x) + 2u(x), 2\hat{f}(x) \rangle$ olsun. O halde $\big(\hat{g}(x) + 2u(x)\big)\big(f(x) + 2p(x)\big) = 0$ bulunur ve $|D| = 2^{2n - der(\hat{g}(x)) - der\left(\hat{f}(x)\right)} = 2^{der(g(x)) + der(f(x))} = |Ann(C)|$ dir. Bu durumda $D = |Ann(C)|$ olur. Böylece

$$C^{\perp} = Ann(C)^* = \langle \hat{g}(x)^* + 2x^{der(\hat{g}(x)) - der(u(x))} u(x)^*, 2\hat{f}(x)^* \rangle$$

eşitliği bulunur.

Teorem 3.2.3.3. ve Teorem 3.2.3.4. ün ispatında olduğu gibi benzer bir teknik kullanılarak aşağıdaki teoremde veriden devirli kodların dualinin üreteç polinomları elde edilir.

Teorem 3.2.3.5. $C = \langle f(x) + 2p(x), 2g(x) \rangle$, $\mathbb{Z}_4$ üzerinde bir devirli kod olsun.

$$C^{\perp} = \langle \sum_{i=1}^{4} e_i \hat{g}_i(x)^* + 2\sum_{i=1}^{4} e_i x^{der\left(\hat{g}_i(x)\right) - der(u_i(x))} u_i(x)^*, 2\sum_{i=1}^{4} e_i \hat{f}_i(x)^* \rangle$$

dir.

3.3. $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 + w\mathbb{Z}_4 + uv\mathbb{Z}_4 + uw\mathbb{Z}_4 + vw\mathbb{Z}_4 + uvw\mathbb{Z}_4$ Halkası Üzerindeki Lineer Kodlar ve Devirli Kodlar

3.3.1. $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 + w\mathbb{Z}_4 + uv\mathbb{Z}_4 + uw\mathbb{Z}_4 + vw\mathbb{Z}_4 + uvw\mathbb{Z}_4$ Halkasının Yapısı

$R_2 \cong \mathbb{Z}_4[u, v, w]/\langle u^2 - u, v^2 - v, w^2 - w \rangle$ halkası değişmeli bir halkadır. Bu nedenle $u^2 = u, v^2 = v, w^2 = w, uv = vu, uw = wu, vw = wv$ olmak üzere $R_2 = \mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 + w\mathbb{Z}_4 + uv\mathbb{Z}_4 + uw\mathbb{Z}_4 + vw\mathbb{Z}_4 + uvw\mathbb{Z}_4$ e izomorftur. $a, b, c, d, e, f, g, h \in \mathbb{Z}_4$ olmak üzere herhangi bir $r \in R_2$ elemanı $r = a + bu + cv + dw + euv + fuw + gvw + huvw$ olarak ifade edilir. R_2 halkasının idempotent elemanları aşağıdaki şekildedir.

$$\lambda_1 = 1 - u - v - w + uv + uw + vw - uvw = (1 - u)(1 - v)(1 - w)$$

$$\lambda_2 = u - uv - uw + uvw = u(1 - v)(1 - w)$$

$$\lambda_3 = v - uv - vw + uvw = (1 - u)v(1 - w)$$

$$\lambda_4 = w - uw - vw + uvw = (1-u)(1-v)w$$

$$\lambda_5 = uv - uvw = uv(1-w)$$

$$\lambda_6 = uw - uvw = u(1-v)w$$

$$\lambda_7 = vw - uvw = (1-u)vw$$

$$\lambda_8 = uvw$$

$i, j = 1,2,3,4,5,6,7,8,\ i \neq j,\ \lambda_i.\lambda_j = 0$ ve $\sum_{i=1}^{8} \lambda_i = 1$ olduğundan yukarıdaki sekiz eleman ikili olarak ortogonaldir. Bu durumda Çin Kalan Teoreminden

$$R_2 = \lambda_1 R_2 \oplus \lambda_2 R_2 \oplus \lambda_3 R_2 \oplus \lambda_4 R_2 \oplus \lambda_5 R_2 \oplus \lambda_6 R_2 \oplus \lambda_7 R_2 \oplus \lambda_8 R_2$$

$$= \lambda_1 \mathbb{Z}_4 \oplus \lambda_2 \mathbb{Z}_4 \oplus \lambda_3 \mathbb{Z}_4 \oplus \lambda_4 \mathbb{Z}_4 \oplus \lambda_5 \mathbb{Z}_4 \oplus \lambda_6 \mathbb{Z}_4 \oplus \lambda_7 \mathbb{Z}_4 \oplus \lambda_8 \mathbb{Z}_4$$

dir. Ayrıca $a, b, c, d, e, f, g, h \in \mathbb{Z}_4$ olmak üzere $\forall\, r = a + bu + cv + dw + euv + fuw + gvw + huvw \in R_2$ için

$$r = r\sum_{i=1}^{8} \lambda_i = r\lambda_1 + r\lambda_2 + r\lambda_3 + r\lambda_4 + r\lambda_5 + r\lambda_6 + r\lambda_7 + r\lambda_8$$

$$= a\lambda_1 + (a+b)\lambda_2 + (a+c)\lambda_3 + (a+d)\lambda_4 + (a+b+c+e)\lambda_5 + (a+b+d+f)\lambda_6 + (a+c+d+g)\lambda_7 + (a+b+c+d+e+f+g+h)\lambda_8$$

$$= r_1\lambda_1 + r_2\lambda_2 + r_3\lambda_3 + r_4\lambda_4 + r_5\lambda_5 + r_6\lambda_6 + r_7\lambda_7 + r_8\lambda_8$$

şeklinde yazılabilir. Bu durumda $1 \leq i \leq 8$ için $r_i \in \mathbb{Z}_4$ olmak üzere

$$r_1 = a$$

$$r_2 = a + b$$

$$r_3 = a + c$$

$$r_4 = a + d$$

$$r_5 = a + b + c + e$$

$$r_6 = a + b + d + f$$

$$r_7 = a + c + d + g$$

$$r_8 = a + b + c + d + e + f + g + h$$

dir. Bu durumda aşağıdaki yazılış tek türlüdür.

$$r = r_1\lambda_1 + r_2\lambda_2 + r_3\lambda_3 + r_4\lambda_4 + r_5\lambda_5 + r_6\lambda_6 + r_7\lambda_7 + r_8\lambda_8$$

$$\phi: R_2^n \longmapsto \mathbb{Z}_4^8$$

$$r \longmapsto (r_1, r_2, r_3, r_4, r_5, r_6, r_7, r_8)$$

şeklinde tanımlanan dönüşüm lineerdir. Bu Gray dönüşümü $c_i \in R_2$ ve $r_{ji} \in \mathbb{Z}_4$ $c_i = \sum_{j=1}^{8} r_{ji}\lambda_j$ olmak üzere

$$\phi: R_2^n \longmapsto \mathbb{Z}_4^{8n}$$

$$(c_0, c_1, \dots, c_{n-1}) \longmapsto (r_{1,0}, \dots, r_{1,n-1}, r_{2,0}, \dots, r_{2,n-1}, \dots, r_{8,0}, r_{8,1}, \dots, r_{8,n-1})$$

olarak R_2^n e genişletilir.

w_L şeklinde gösterilen $\mathbb{Z}_4$ üzerindeki Lee ağırlığı

$$w_L(x) \coloneqq \begin{cases} 0, & x = 0 \\ 2, & x = 2 \\ 1, & x = 1 \; veya \; 3 \end{cases}$$

şeklinde tanımlanır.

$\phi: r \longmapsto (r_1, r_2, r_3, r_4, r_5, r_6, r_7, r_8)$ dönüşümünün R_2 üzerindeki Lee ağırlığı $w_L(r) = \sum_{i=1}^{8} w_L(r_i)$ dir.

3.3.2. $\mathbb{Z}_4 + \boldsymbol{u}\mathbb{Z}_4 + \boldsymbol{v}\mathbb{Z}_4 + \boldsymbol{w}\mathbb{Z}_4 + \boldsymbol{uv}\mathbb{Z}_4 + \boldsymbol{uw}\mathbb{Z}_4 + \boldsymbol{vw}\mathbb{Z}_4 + \boldsymbol{uvw}\mathbb{Z}_4$ Halkası Üzerindeki Lineer Kodlar

$\forall 0 \le i \le n-1$ için $\boldsymbol{r} = (r^{(0)}, r^{(1)}, \dots, r^{(n-1)}) \in R_2^n$ ve $\boldsymbol{r}^{(i)} = r_{i1}\lambda_1 + r_{i2}\lambda_2 + r_{i3}\lambda_3 + r_{i4}\lambda_4 + r_{i5}\lambda_5 + r_{i6}\lambda_6 + r_{i7}\lambda_7 + r_{i8}\lambda_8$ dir. O halde $1 \le i \le 8$ için $\boldsymbol{r}_j = (r_{0j}, r_{1j}, \dots, r_{n-1j}) \in \mathbb{Z}_4^n$ olmak üzere $\boldsymbol{r} = \boldsymbol{r}_1\lambda_1 + \boldsymbol{r}_2\lambda_2 + \boldsymbol{r}_3\lambda_3 + \boldsymbol{r}_4\lambda_4 + \boldsymbol{r}_5\lambda_5 + \boldsymbol{r}_6\lambda_6 + \boldsymbol{r}_7\lambda_7 + \boldsymbol{r}_8\lambda_8$ dir. Bu ifade kullanılarak $\forall x, y \in R_2^n$ vektörlerinin iç çarpımı $\forall\, 1 \le j \le n$ için $\boldsymbol{x} = \boldsymbol{x}_1\lambda_1 + \cdots + \boldsymbol{x}_8\lambda_8$, $\boldsymbol{x}_j = (x_{0j}, x_{1j}, \dots, x_{n-1,j}) \in \mathbb{Z}_4^n$ ve $\boldsymbol{y} = \boldsymbol{y}_1\lambda_1 + \cdots + \boldsymbol{y}_8\lambda_8$, $\boldsymbol{y}_j = (y_{0j}, y_{1j}, \dots, y_{n-1,j}) \in \mathbb{Z}_4^n$ ve $\boldsymbol{x}_j.\boldsymbol{y}_j = \sum_{k=0}^{n-1} \boldsymbol{x}_{kj}\boldsymbol{y}_{kj}$ olmak üzere

$$\boldsymbol{x}.\boldsymbol{y} = (\boldsymbol{x}_1.\boldsymbol{y}_1)\lambda_1 + (\boldsymbol{x}_2.\boldsymbol{y}_2)\lambda_2 + \cdots + (\boldsymbol{x}_8.\boldsymbol{y}_8)\lambda_8$$

şeklinde yazılır.

$1 \le i \le 8$ için C_i kodları aşağıdaki şekilde tanımlanmaktadır.

$$C_1 = \{\boldsymbol{a} \in \mathbb{Z}_4^n : \boldsymbol{a}\lambda_1 + \boldsymbol{b}\lambda_2 + \boldsymbol{c}\lambda_3 + \boldsymbol{d}\lambda_4 + \boldsymbol{e}\lambda_5 + \boldsymbol{f}\lambda_6 + \boldsymbol{g}\lambda_7 + \boldsymbol{h}\lambda_8 \in C, \; \exists\, \boldsymbol{b}, \boldsymbol{c}, \boldsymbol{d}, \boldsymbol{e}, \boldsymbol{f}, \boldsymbol{g}, \boldsymbol{h} \in \mathbb{Z}_4^n\}$$

$$C_2 = \{\boldsymbol{b} \in \mathbb{Z}_4^n : \boldsymbol{a}\lambda_1 + \boldsymbol{b}\lambda_2 + \boldsymbol{c}\lambda_3 + \boldsymbol{d}\lambda_4 + \boldsymbol{e}\lambda_5 + \boldsymbol{f}\lambda_6 + \boldsymbol{g}\lambda_7 + \boldsymbol{h}\lambda_8 \in C, \exists\, \boldsymbol{a}, \boldsymbol{c}, \boldsymbol{d}, \boldsymbol{e}, \boldsymbol{f}, \boldsymbol{g}, \boldsymbol{h} \in \mathbb{Z}_4^n\}$$

$$C_3 = \{\boldsymbol{c} \in \mathbb{Z}_4^n : \boldsymbol{a}\lambda_1 + \boldsymbol{b}\lambda_2 + \boldsymbol{c}\lambda_3 + \boldsymbol{d}\lambda_4 + \boldsymbol{e}\lambda_5 + \boldsymbol{f}\lambda_6 + \boldsymbol{g}\lambda_7 + \boldsymbol{h}\lambda_8 \in C, \exists\, \boldsymbol{a}, \boldsymbol{b}, \boldsymbol{d}, \boldsymbol{e}, \boldsymbol{f}, \boldsymbol{g}, \boldsymbol{h} \in \mathbb{Z}_4^n\}$$

$$C_4 = \{\boldsymbol{d} \in \mathbb{Z}_4^n : \boldsymbol{a}\lambda_1 + \boldsymbol{b}\lambda_2 + \boldsymbol{c}\lambda_3 + \boldsymbol{d}\lambda_4 + \boldsymbol{e}\lambda_5 + \boldsymbol{f}\lambda_6 + \boldsymbol{g}\lambda_7 + \boldsymbol{h}\lambda_8 \in C, \exists\, \boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}, \boldsymbol{e}, \boldsymbol{f}, \boldsymbol{g}, \boldsymbol{h} \in \mathbb{Z}_4^n\}$$

$$C_5 = \{\boldsymbol{e} \in \mathbb{Z}_4^n : \boldsymbol{a}\lambda_1 + \boldsymbol{b}\lambda_2 + \boldsymbol{c}\lambda_3 + \boldsymbol{d}\lambda_4 + \boldsymbol{e}\lambda_5 + \boldsymbol{f}\lambda_6 + \boldsymbol{g}\lambda_7 + \boldsymbol{h}\lambda_8 \in C, \exists\, \boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}, \boldsymbol{d}, \boldsymbol{f}, \boldsymbol{g}, \boldsymbol{h} \in \mathbb{Z}_4^n\}$$

$$C_6 = \{\boldsymbol{f} \in \mathbb{Z}_4^n : \boldsymbol{a}\lambda_1 + \boldsymbol{b}\lambda_2 + \boldsymbol{c}\lambda_3 + \boldsymbol{d}\lambda_4 + \boldsymbol{e}\lambda_5 + \boldsymbol{f}\lambda_6 + \boldsymbol{g}\lambda_7 + \boldsymbol{h}\lambda_8 \in C, \exists\, \boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}, \boldsymbol{d}, \boldsymbol{e}, \boldsymbol{g}, \boldsymbol{h} \in \mathbb{Z}_4^n\}$$

$$C_7 = \{\boldsymbol{g} \in \mathbb{Z}_4^n : \boldsymbol{a}\lambda_1 + \boldsymbol{b}\lambda_2 + \boldsymbol{c}\lambda_3 + \boldsymbol{d}\lambda_4 + \boldsymbol{e}\lambda_5 + \boldsymbol{f}\lambda_6 + \boldsymbol{g}\lambda_7 + \boldsymbol{h}\lambda_8 \in C, \exists\, \boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}, \boldsymbol{d}, \boldsymbol{e}, \boldsymbol{f}, \boldsymbol{h} \in \mathbb{Z}_4^n\}$$

$$C_8 = \{\boldsymbol{h} \in \mathbb{Z}_4^n : \boldsymbol{a}\lambda_1 + \boldsymbol{b}\lambda_2 + \boldsymbol{c}\lambda_3 + \boldsymbol{d}\lambda_4 + \boldsymbol{e}\lambda_5 + \boldsymbol{f}\lambda_6 + \boldsymbol{g}\lambda_7 + \boldsymbol{h}\lambda_8 \in C, \exists\, \boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}, \boldsymbol{d}, \boldsymbol{e}, \boldsymbol{f}, \boldsymbol{g} \in \mathbb{Z}_4^n\}$$

$1 \leq i \leq 8$ için C_i kodu $\mathbb{Z}_4$ üzerinde tanımlı n uzunluğunda bir lineer koddur ve C kodu

$$C = \lambda_1 C_1 \oplus \lambda_2 C_2 \oplus \lambda_3 C_3 \oplus \lambda_4 C_4 \oplus \lambda_5 C_5 \oplus \lambda_6 C_6 \oplus \lambda_7 C_7 \oplus \lambda_8 C_8$$

şeklinde yazılabilir. Bu durumda $|C| = \prod_{i=1}^{8} |C_i|$ dir.

Teorem 3.3.2.1. $C \subseteq R_2^n$ bir lineer kod olsun.

(1) $C = \lambda_1 C_1 \oplus \lambda_2 C_2 \oplus \lambda_3 C_3 \oplus \lambda_4 C_4 \oplus \lambda_5 C_5 \oplus \lambda_6 C_6 \oplus \lambda_7 C_7 \oplus \lambda_8 C_8$, R_2 üzerinde tanımlı n uzunluğunda bir lineer koddur.

(2) $C_i^{\perp}$, C_i $(1 \leq i \leq 8)$ nin dual kodu olmak üzere $C^{\perp} = \lambda_1 C_1^{\perp} \oplus \lambda_2 C_2^{\perp} \oplus \lambda_3 C_3^{\perp} \oplus \lambda_4 C_4^{\perp} \oplus \lambda_5 C_5^{\perp} \oplus \lambda_6 C_6^{\perp} \oplus \lambda_7 C_7^{\perp} \oplus \lambda_8 C_8^{\perp}$ dir.

İspat: Teorem 3.2.2.1. in ispatına benzer şekilde yapılır.

Not 3.3.2.2.

$$G_j = \begin{bmatrix} I_{k_{j1}} & A_j & B_j \\ 0 & 2I_{k_{j2}} & 2C_j \end{bmatrix}$$

$1 \leq j \leq 8$ için A_j ve C_j bileşenleri $\mathbb{Z}_2$ den alınan, B bileşenleri $\mathbb{Z}_4$ den alınan matrisler C_j nin üreteç matrisi olmak üzere C lineer kodunun üreteç matrisi

$$G = \begin{bmatrix} \lambda_1 G_1 \\ \lambda_2 G_2 \\ \lambda_3 G_3 \\ \lambda_4 G_4 \\ \lambda_5 G_5 \\ \lambda_6 G_6 \\ \lambda_7 G_7 \\ \lambda_8 G_8 \end{bmatrix}$$

dir.

$$G_j' = \begin{bmatrix} -B_j^T - C_j^T A_j^T & C_j^T & I_{n-k_{j1}-k_{j2}} \\ 2A_j^T & 2I_{k_{j2}} & 0 \end{bmatrix}$$

$\mathbb{Z}_4$ üzerindeki C_j lineer kodunun duali $C_j^{\perp}$ in üreteç matrisi olmak üzere $C^{\perp}$ kodunun üreteç matrisi

$$H = \begin{bmatrix} \lambda_1 G_1' \\ \lambda_2 G_2' \\ \lambda_3 G_3' \\ \lambda_4 G_4' \\ \lambda_5 G_5' \\ \lambda_6 G_6' \\ \lambda_7 G_7' \\ \lambda_8 G_8' \end{bmatrix}$$

dir.

H, C kodunun kontrol matrisi olarak adlandırılır.

3.3.3. $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 + w\mathbb{Z}_4 + uv\mathbb{Z}_4 + uw\mathbb{Z}_4 + vw\mathbb{Z}_4 + uvw\mathbb{Z}_4$ Halkası Üzerindeki Devirli Kodlar

Teorem 3.3.3.1. $C = \lambda_1 C_1 \oplus \lambda_2 C_2 \oplus \lambda_3 C_3 \oplus \lambda_4 C_4 \oplus \lambda_5 C_5 \oplus \lambda_6 C_6 \oplus \lambda_7 C_7 \oplus \lambda_8 C_8$ olsun. Bu durumda C nin R_2 üzerinde tanımlı devirli bir kod olması için gerek ve yeter koşul aşağıdaki üç koşuldan birinin sağlanmasıdır.

(1) $\forall\, t \in \{1,2,\dots,8\}$ için C_t, $\mathbb{Z}_4$ üzerinde tanımlı devirli koddur.

(2) $\forall\, t \in \{1,2,\dots,8\}$ için $C_t^{\perp}$, $\mathbb{Z}_4$ üzerinde tanımlı devirli koddur.

(3) $C^{\perp}$, R_2 üzerinde tanımlı devirli bir koddur.

İspat: $\mathbf{c} = \sum_{t=1}^{8} \lambda_t \boldsymbol{c}_t \in C$ ve $1 \le t \le 8$ için $\boldsymbol{c}_t = (c_{t,0}, c_{t,1}, \dots, c_{t,n-1}) \in C_t$ olsun. C bir devirli kod olduğundan $d = \left(\sum_{t=1}^{8} \lambda_t c_{t,n-1}, \sum_{t=1}^{8} \lambda_t c_{t,0}, \dots, \sum_{t=1}^{8} \lambda_t c_{t,n-2}\right) \in C$ dir. Bu durumda

$(c_{t,n-1}, c_{t,0}, \dots, c_{t,n-2)} \in C_t$ olur. Böylece C_t, $\mathbb{Z}_4$ üzerinde tanımlı devirli koddur. Tersi de gerçeklenir. O halde ilk koşul ispatlanmıştır.

C_t, $\mathbb{Z}_4$ üzerinde tanımlı devirli kod olduğundan $C_t^{\perp}$, $\mathbb{Z}_4$ üzerinde tanımlı devirli koddur. Koşul (1) den $C^{\perp}$, R_2 üzerinde tanımlı devirli bir koddur. Ayrıca C de R_2 üzerinde tanımlı devirli bir koddur.

Teorem 3.3.3.2. $C = \langle f(x) + 2p(x), 2g(x) \rangle$, $\mathbb{Z}_4$ üzerinde n uzunluğunda bir devirli kod olsun. $\hat{f}(x) = \left(\frac{x^n-1}{f(x)}\right)$, $\hat{g}(x) = \left(\frac{x^n-1}{g(x)}\right)$ ve $\hat{f}(x)^* = x^{der(f(x))} f(\frac{1}{x})$ olmak üzere $C^{\perp} = \langle \hat{g}(x)^* + 2x^{der(\hat{g}(x))-der(u(x))} u(x)^*, 2\hat{f}(x)^* \rangle$ dir.

İspat: Teorem 3.2.3.4. ün ispatına benzer şekilde yapılır.

Teorem 3.3.3.3. $C = \lambda_1 C_1 \oplus \lambda_2 C_2 \oplus \lambda_3 C_3 \oplus \lambda_4 C_4 \oplus \lambda_5 C_5 \oplus \lambda_6 C_6 \oplus \lambda_7 C_7 \oplus \lambda_8 C_8$, R_2 üzerinde tanımlı n uzunluğunda bir devirli kod olsun. Eğer $C_t = \langle f_t(x) + 2p_t(x), 2g_t(x) \rangle$ olacak şekilde $f_t(x), g_t(x), p_t(x) \in \mathbb{Z}_4[x]$, $(1 \le t \le 8)$ varsa bu durumda

$$C = \langle \sum_{t=1}^{8} \lambda_t f_t(x) + 2\sum_{t=1}^{8} \lambda_t p_t(x), 2\sum_{t=1}^{8} \lambda_t g_t(x) \rangle$$

dir. Ayrıca n tek ise

$$C = \langle \sum_{t=1}^{8} \lambda_t f_t(x) + 2\sum_{t=1}^{8} \lambda_t g_t(x) \rangle$$

dir.

İspat: $D = \langle \sum_{t=1}^{8} \lambda_t f_t(x) + 2\sum_{t=1}^{8} \lambda_t p_t(x), 2\sum_{t=1}^{8} \lambda_t g_t(x) \rangle$ olsun. $\forall c(x) \in C$ için $c(x) = \sum_{t=1}^{8} \lambda_t \left(\big(f_t(x) + 2p_t(x)\big) u_t(x) + 2g_t(x) v_t(x) \right)$ olacak şekilde $u_t(x), v_t(x) \in \mathbb{Z}_4[x]$ dir. O halde

$$\sum_{t=1}^{8} \lambda_t \left(\big(f_t(x) + 2p_t(x)\big) u_t(x) + 2g_t(x) v_t(x) \right)$$

$$= \sum_{t=1}^{8} \lambda_t u_t(x) \sum_{t=1}^{8} \lambda_t \big(f_t(x) + 2p_t(x)\big) + \sum_{t=1}^{8} \lambda_t v_t(x) \sum_{t=1}^{8} 2\lambda_t g_t(x)$$

olduğundan $C \subseteq D$ dir. $D \subseteq C$ olduğu açıktır. Dolayısıyla $C = D$ elde edilir.

Teorem 3.3.3.2. ve Teorem 3.3.3.3. ün ispatında olduğu gibi benzer bir teknik kullanılarak aşağıdaki teoremde verilen devirli kodların dualinin üreteç polinomları elde edilir.

Teorem 3.3.3.4. $C = \langle f(x) + 2p(x), 2g(x) \rangle$, $\mathbb{Z}_4$ üzerinde bir devirli kod olsun.

$$C^{\perp} = \langle \sum_{t=1}^{8} \lambda_t \hat{g}_t(x)^* + 2 \sum_{t=1}^{8} \lambda_t x^{der(\hat{g}_t(x)) - der(u_t(x))} u_t(x)^*, 2 \sum_{t=1}^{8} \lambda_t \hat{f}_t(x)^* \rangle$$

dir.

Teorem 3.3.3.5. $t \in \{1,2, \dots ,8\}$ olmak üzere C_t, $\mathbb{Z}_4$ üzerinde n uzunluğunda (n tek) bir devirli kod olsun. $f_{2,t}(x) | f_{1,t}(x)$ ve $\mathbb{Z}_4$ üzerindeki $x^n - 1$ in monik bölenleri $f_{1,t}(x)$ ve $f_{2,t}(x)$ olmak üzere $C_t = \langle f_{1,t}(x) + 2\, f_{2,t}(x) \rangle$ dir. Bu durumda $1 \leq t \leq 8$ için C_t nin eleman sayısı $4^{n - der\left(f_{1,t}(x)\right)} 2^{der(f_{1,t}(x)) - der(f_{2,t}(x))}$ dir.

Sonuç 3.3.3.6. $\phi(C) = \prod_{t=1}^{8} C_t$, $\mathbb{Z}_4$ üzerinde $8n$ uzunluğunda (n tek) bir lineer kod ve $\prod_{t=1}^{8} C_t$, $\mathbb{Z}_4$ üzerinde bir devirli kod olsun ($1 \leq t \leq 8$). O halde $\phi(C)$ nin eleman sayısı $4^{\sum_{t=1}^{8} (n - der\left(f_{1,t}(x)\right))} 2^{\sum_{t=1}^{8} (der(f_{1,t}(x)) - der(f_{2,t}(x))}$ dir.

4. BULGULAR VE TARTIŞMALAR

Bu bölümde $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 + w\mathbb{Z}_4 + uv\mathbb{Z}_4$ halkası bulunarak bu halka üzerindeki Gray dönüşüm, lineer kodlar ve devirli kodlar incelenmiştir.

4.1. $\mathbb{Z}_4 + \boldsymbol{u}\mathbb{Z}_4 + \boldsymbol{v}\mathbb{Z}_4 + \boldsymbol{w}\mathbb{Z}_4 + \boldsymbol{uv}\mathbb{Z}_4$ Halkası Üzerindeki Lineer Kodlar ve Devirli Kodlar

4.1.1. $\mathbb{Z}_4 + \boldsymbol{u}\mathbb{Z}_4 + \boldsymbol{v}\mathbb{Z}_4 + \boldsymbol{w}\mathbb{Z}_4 + \boldsymbol{uv}\mathbb{Z}_4$ Halkasının Yapısı

$R_B \cong \mathbb{Z}_4[u,v,w]/\langle u^2-u, v^2-v, w^2-w, uv-vu, uw, wv\rangle$ halkası değişmeli ve sonlu bir halkadır. Bu nedenle $u^2 = u, v^2 = v, w^2 = w, uv = vu, uw = vw = 0$ olmak üzere $R_B = \mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 + w\mathbb{Z}_4 + uv\mathbb{Z}_4$ e izomorftur.

$$\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 + w\mathbb{Z}_4 + uv\mathbb{Z}_4 = \{a + ub + vc + wd + uve : a,b,c,d,e \in \mathbb{Z}_4\}$$

dir.

$a_1 = u - uv$, $a_2 = 1 - u - v - w + uv$, $a_3 = v - uv$, $a_4 = uv$, $a_5 = w$ olsun. $i,j = 1,2,3,4,5$ ve $i \neq j, (a_i)^2 = a_i,\ a_i.a_j = 0,\ a_1 + a_2 + a_3 + a_4 + a_5 = 1$ olduğunu inceleyelim.

$$\begin{aligned} {a_1}^2 = (u-uv)^2 &= u^2 - 2u^2v + u^2v^2 \\ &= u - 2uv + uv \\ &= u - uv \\ &= a_1 \end{aligned}$$

olur. O halde

$${a_1}^2 = a_1$$

eşitliği bulunur.

$$\begin{aligned} {a_2}^2 &= (1-u-v-w+uv)^2 \\ &= 1 - u - v - w + uv - u + u^2 + uv + uw - u^2v - v + uv + v^2 + vw - uv^2 - w + uw + w^2 + vw - uvw + uv - u^2v - uv^2 - wuv + u^2v^2 \\ &= 1 - u - v - w + uv \\ &= a_2 \end{aligned}$$

bulunur. Böylece

$$a_2{}^2 = a_2$$

eşitliği elde edilir.

$$a_3{}^2 = (v - uv)^2 = v^2 - 2uv^2 + u^2v^2$$

$$= v - 2uv + uv$$

$$= v - uv$$

$$= a_3$$

olur. O halde

$$a_3{}^2 = a_3$$

dir.

$$a_4{}^2 = (uv)^2 = u^2v^2$$

$$= uv$$

$$= a_4$$

elde edilir. Böylece

$$a_4{}^2 = a_4$$

eşitliği bulunur.

$$a_5{}^2 = (w)^2 = w^2$$

$$= w$$

$$= a_5$$

bulunur. Bu durumda

$$a_5{}^2 = a_5$$

eşitliği elde edilir.

$$a_1 + a_2 + a_3 + a_4 + a_5 = u - uv + 1 - u - v - w + uv + v - uv + uv + w = 1$$

olur.

$$a_1.a_2 = (u - uv)(\,1 - u - v - w + uv)$$

$$= u - u^2 - uv - uw + u^2v - uv + u^2v + uv^2 + uvw - u^2v^2$$

$$= -uw + uvw$$

$$= 0$$

bulunur. O halde

$$a_1 . a_2 = 0$$

dir.

$$a_1 . a_3 = (u - uv)(v - uv)$$

$$= uv - u^2 v - uv^2 + u^2 v^2$$

$$= uv - uv - uv + uv$$

$$= 0$$

olur. Böylece

$$a_1 . a_3 = 0$$

eşitliği bulunur.

$$a_1 . a_4 = (u - uv)(uv)$$

$$= u^2 v - u^2 v^2$$

$$= uv - uv$$

$$= 0$$

elde edilir. O halde

$$a_1 . a_4 = 0$$

dir.

$$a_1 . a_5 = (u - uv)w$$

$$= uw - uvw$$

$$= 0$$

olur. Bu durumda

$$a_1 . a_5 = 0$$

eşitliği bulunur.

$$a_2 . a_3 = (1 - u - v - w + uv)(v - uv)$$

$$= v - uv - uv + u^2v - v^2 + uv^2 - wv + uvw + uv^2 - u^2v^2$$

$$= -wv + uvw$$

$$= 0$$

elde edilir. Böylece

$$a_2 . a_3 = 0$$

dir.

$$a_2 . a_4 = (1 - u - v - w + uv)(\, uv)$$

$$= uv - u^2v - uv^2 - wuv + u^2v^2$$

$$= uv - uv - uv - wuv + uv$$

$$= 0$$

bulunur. O halde

$$a_2 . a_4 = 0$$

eşitliği elde edilir.

$$a_2 . a_5 = (1 - u - v - w + uv)(\mathrm{w})$$

$$= w - uw - vw - w^2 + uvw$$

$$= 0$$

olur. Böylece

$$a_2 . a_5 = 0$$

dir.

$$a_3 . a_4 = (\, v - uv)(uv)$$

$$= uv^2 - u^2v^2$$

$$= uv - uv$$

$$= 0$$

elde edilir. O halde

$$a_3 . a_4 = 0$$

eşitliği bulunur.

$$a_3.a_5 = (v - uv)w$$

$$= vw - uvw$$

$$= 0$$

elde edilir. Böylece

$$a_3.a_5 = 0$$

eşitliği bulunur.

$$a_4.a_5 = (uv)(w)$$

$$= uvw$$

$$= 0$$

olur. O halde

$$a_4.a_5 = 0$$

eşitliği elde edilir.

Bu durumda $i, j = 1,2,3,4,5$ ve $i \neq j$ için $a_i.a_j = 0$ olduğu görülür.

Dolayısıyla

$$R_B = a_1R_B \oplus a_2R_B \oplus a_3R_B \oplus a_4R_B \oplus a_5R_B$$

eşitliği bulunur.

Gray dönüşümü aşağıdaki şekilde tanımlansın:

$$\phi_B : R_B \longmapsto \mathbb{Z}_4^5$$

$$a + ub + vc + wd + uve \rightarrow \phi_B(a + ub + vc + wd + uve)$$

$$= (x_1, x_2, x_3, x_4, x_5),\ x_i \in \mathbb{Z}_4\ ,\ 1 \leq i \leq 5$$

$$x_1 = a + b,\ x_2 = a,\ x_3 = a + c,\ x_4 = a + b + c + e,\ x_5 = a + d$$

dir.

Teorem 4.1.1.1. ϕ_B Gray dönüşümü (R_B^n, Lee uzaklığı) den ($\mathbb{Z}_4^{5n}$, Lee uzaklığı) e uzaklık koruyan bir dönüşümdür.

İspat: $\forall k_1, k_2 \in \mathbb{Z}_4$ olsun. ϕ_B Gray dönüşümü tanımına göre $\forall\ x_1, x_2 \in R_B^n$ için

$$\phi_B(k_1x_1 + k_2x_2) = k_1\phi_B(x_1) + k_2\phi_B(x_2)$$

olup Gray dönüşümü lineerdir.

$i = 1,2, \dots, n$ için $x_{1,i} = e_{1,i}a_1 + e_{2,i}a_2 + e_{3,i}a_3 + e_{4,i}a_4 + e_{5,i}a_5$ ve $x_{2,i} = f_{1,i}a_1 + f_{2,i}a_2 + f_{3,i}a_3 + f_{4,i}a_4 + f_{5,i}a_5$ olmak üzere $x_1 = (x_{1,1}, x_{1,2}, \dots, x_{1,n})$,

$x_2 = (x_{2,1}, x_{2,2}, \dots, x_{2,n}) \in R_B^n$ olsun. O halde

$$x_1 - x_2 = (x_{1,1} - x_{2,1}, x_{1,2} - x_{2,2}, \dots, x_{1,n} - x_{2,n})$$

olur. Dolayısıyla

$$\phi_B(x_1 - x_2) = \phi_B(x_1) - \phi_B(x_2)$$

dir. Böylece

$$d_L(x_1, x_2) = w_L(x_1 - x_2) = w_L\big(\phi_B(x_1 - x_2)\big)$$

$$= w_L\big(\phi_B(x_1) - \phi_B(x_2)\big)$$

$$= d_L\big(\phi_B(x_1), \phi_B(x_2)\big)$$

eşitliği bulunur. O halde ϕ_B uzaklık koruyan bir dönüşümdür.

Tanım 4.1.1.2. $\tau: R^n \to R^n$, $\forall(r_0, r_1, \dots, r_{n-1}) \in C$ olmak üzere $\tau(r_0, r_1, \dots, r_{n-1}) = (r_{n-1}, r_0, r_1, \dots r_{n-2})$ şeklinde tanımlı dönüşüme cyclic-shift (devirli öteleme) denir. Eğer $\tau(C) = C$ ise C kodu devirli koddur.

$$\psi: R^n \to R[x] \,/\, \langle x^n - 1\rangle$$

$(\alpha_0, \alpha_1, \dots, \alpha_{n-1}) \longmapsto \alpha_0 + \alpha_1 x + \cdots + \alpha_{n-1}x^{n-1} (mod\langle x^n - 1\rangle)$ dir (Aydın vd., 2017).

Tanım 4.1.1.3. $C \subseteq C^{\perp}$ ise C koduna self-ortogonal denir ve $C = C^{\perp}$ ise self-dual dir (Gao vd., 2014).

Tanım 4.1.1.4. $r = a + ub + vc + wd + uve$, R_B halkasının elemanı olsun. r elemanının Lee ağırlığı $w_L(r) = w_L(\phi_B(r))$ şeklinde tanımlanır.

Tanım 4.1.1.5. Herhangi bir $c = (c_1, c_2, \dots, c_n)$ kod sözcüğünün Lee ağırlığı $i = 1,2, \dots, n$ olmak üzere $w_L(c) = \sum_{i=1}^{n} w_L(c_i)$ şeklindedir.

Her $c, \dot{c} \in C$ için $d_L(c, \dot{c}) = w_L(c - \dot{c})$ şeklinde tanımlanan d_L fonksiyonuna Lee uzaklığı denir. C kodunun minimum Lee uzaklığı ise

$$d_L(C) = min\{d_L(c, \dot{c}): \forall c \in C, c \neq \dot{c}\}$$

şeklinde tanımlanır (Li vd., 2016).

Tanım 4.1.1.6. R^n modülünün bir R-alt modülüne R üzerinde tanımlı n uzunluğunda bir lineer kod denir (Gao vd., 2014).

Tanım 4.1.1.7. C, R^n kümesinin bir alt kümesi olsun. n uzunluğunda lineer bir C kodunun devirli olması için gerek ve yeter koşul C kodunun $R[x]/\langle x^n - 1\rangle$ bölüm halkasının bir ideali olmasıdır (Li vd., 2016).

Tanım 4.1.1.8. $R_n = R[x]/\langle x^n - 1\rangle = \{c_0 + c_1x + \ldots + c_{n-1}x^{n-1} + \langle x^n - 1\rangle | c_0, c_1, \ldots, c_{n-1} \in R\}$ olsun. R_n polinom halkasının herhangi bir elemanı $c(x) + \langle x^n - 1\rangle \in R_n$ şeklindedir (Gao vd., 2014).

Tanım 4.1.1.9. R_n üzerinde tanımlı bir $e(x)$ polinomu eğer $(e(x))^2 = e(x)$ ise bir idempotenttir (Gao vd., 2014).

4.1.2. $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 + w\mathbb{Z}_4 + uv\mathbb{Z}_4$ Halkası Üzerindeki Lineer Kodlar

Teorem 4.1.2.1. C, $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 + w\mathbb{Z}_4 + uv\mathbb{Z}_4$ üzerinde n uzunluğunda bir lineer kod ise $|C| = M$ ve minimum Lee uzaklığı d_L olmak üzere $\phi_B(C)$, $(5n, M, d_L)$ parametrelerine sahip lineer bir koddur.

İspat: Teorem 4.1.1.1. den $\phi_B(C)$ lineerdir. ϕ_B Gray dönüşüm tanımından $\phi_B(C)$ nin uzunluğu $5n$ dir. ϕ_B nin R_B^n den $\mathbb{Z}_4^{5n}$ e birebir ve örten bir dönüşüm olduğundan $\phi_B(C)$, M kod sözcüğüne sahiptir. ϕ_B uzaklık koruyan bir dönüşüm olduğundan C nin minimum Lee uzaklığı d_L dir.

Teorem 4.1.2.2. C self ortogonal ise $\phi_B(C)$ de self ortogonal koddur.

İspat: C self ortogonal ve $\alpha = a + ub + vc + wd + uve$, $\beta = x + uy + vz + ws + uvt \in C$ $a, b, c, d, e, x, y, z, s, t \in \mathbb{Z}_4$ olsun.

C self ortogonal olduğundan $\alpha.\beta = 0$ dır. Dolayısıyla

$$\begin{aligned}\alpha.\beta &= (a + ub + vc + wd + uve)(x + uy + vz + ws + uvt)\\ &= ax + uay + vaz + was + uvat + ubx + u^2by + uvbz + uwbs\\ &+ u^2vbt + vcx + uvcy + v^2cz + vwcs + uv^2ct + wdx + wudy\\ &+ vwdz + w^2ds + uvwdt + uvex + u^2vey + uv^2ez + uvwes\\ &+ u^2v^2et\end{aligned}$$

$$= ax + u(ay + bx + by) + v(az + cx + cz) + w(as + dx + ds) +$$
$$uv(at + bz + bt + cy + ct + ex + ey + ez + et) = 0$$

elde edilir.

Bu durumda

$$ax = (ay + bx + by) = (az + cx + cz) = (as + dx + ds)$$
$$= (at + bz + bt + cy + ct + ex + ey + ez + et) = 0$$

olur.

Diğer taraftan

$$\phi_B(\alpha).\phi_B(\beta) = (a + b, a, a + c, a + b + c + e, a + d)(x + y, x, x + z, x + y + z$$
$$+ t, x + s) = 0$$

eşitliği bulunur.

Dolayısıyla $\phi_B(C)$ self ortogonaldir.

Teorem 4.1.2.3. $C^{\perp}$, R_B üzerinde C kodunun duali olsun. $\phi_B(C^{\perp}) = \phi_B(C)^{\perp}$ dir. Ayrıca C self-dual kod ise $\phi_B(C)$ de self-dual koddur.

İspat: $\alpha = a + ub + vc + wd + uve$, $\beta = x + uy + vz + ws + uvt \in C$ $a, b, c, d, e, x, y, z, s, t \in \mathbb{Z}_4$ olsun. C self-dual kod olduğundan $C = C^{\perp}$ dir. $\alpha.\beta = 0$ olduğundan

$$ax = (ay + bx + by) = (az + cx + cz) = (as + dx + ds)$$
$$= (at + bz + bt + cy + ct + ex + ey + ez + et) = 0$$

dır. Bu durumda

$$\phi_B(\alpha).\phi_B(\beta) = (a + b, a, a + c, a + b + c + e, a + d)(x + y, x, x + z, x + y + z$$
$$+ t, x + s) = 0$$

dır.

Böylece $\phi_B(C^{\perp}) \subseteq \phi_B(C)^{\perp}$ dir. $|\phi_B(C^{\perp})| = |\phi_B(C)^{\perp}|$ olduğundan $\phi_B(C^{\perp}) = \phi_B(C)^{\perp}$ olur. Dolayısıyla $\phi_B(C)$ self ortogonal ise C self-dualdir. Bu durumda $|\phi_B(C)| = |C|$ olup $\phi_B(C)$ self-dualdir.

Not 4.1.2.4. B_1, B_2, B_3, B_4, B_5 lineer kodlar olsun. O halde

$$B_1 \oplus B_2 \oplus B_3 \oplus B_4 \oplus B_5 = \{b_1 + b_2 + b_3 + b_4 + b_5 : b_i \in B_i; 1 \leq i \leq 5\}$$

ve

$$B_1 \otimes B_2 \otimes B_3 \otimes B_4 \otimes B_5 = \{(b_1, b_2, b_3, b_4, b_5) : b_i \in B_i ; 1 \leq i \leq 5\}$$

dir.

C, R_B üzerinde n uzunluğunda bir lineer kod olsun.

$$C_1 = \{a \in \mathbb{Z}_4^n \mid aa_1 + ba_2 + ca_3 + da_4 + ea_5 \in C, \exists b, c, d, e \in \mathbb{Z}_4^n\}$$

$$C_2 = \{b \in \mathbb{Z}_4^n \mid aa_1 + ba_2 + ca_3 + da_4 + ea_5 \in C, \exists a, c, d, e \in \mathbb{Z}_4^n\}$$

$$C_3 = \{c \in \mathbb{Z}_4^n \mid aa_1 + ba_2 + ca_3 + da_4 + ea_5 \in C, \exists a, b, d, e \in \mathbb{Z}_4^n\}$$

$$C_4 = \{d \in \mathbb{Z}_4^n \mid aa_1 + ba_2 + ca_3 + da_4 + ea_5 \in C, \exists a, b, c, e \in \mathbb{Z}_4^n\}$$

$$C_5 = \{e \in \mathbb{Z}_4^n \mid aa_1 + ba_2 + ca_3 + da_4 + ea_5 \in C, \exists a, b, c, d \in \mathbb{Z}_4^n\}$$

Burada C_1, C_2, C_3, C_4 ve C_5, $\mathbb{Z}_4$ üzerinde n uzunluğunda lineer kodlardır.

Teorem 4.1.2.5. C, R_B üzerinde tanımlı n uzunluğunda bir lineer kod olsun.

(1) C_i $(1 \leq i \leq 5)$ $\mathbb{Z}_4$ üzerinde tanımlı n uzunluğunda bir lineer kod olmak üzere $C = a_1 C_1 \oplus a_2 C_2 \oplus a_3 C_3 \oplus a_4 C_4 \oplus a_5 C_5$ dir.

(2) $C_i^{\perp}$, C_i $(1 \leq i \leq 5)$ nin dual kodu olmak üzere $C^{\perp} = a_1 C_1^{\perp} \oplus a_2 C_2^{\perp} \oplus a_3 C_3^{\perp} \oplus a_4 C_4^{\perp} \oplus a_5 C_5^{\perp}$ dir.

(3) C nin self ortogonal bir kod olması için gerek ve yeter koşul C_i $(1 \leq i \leq 5)$ nin $\mathbb{Z}_4$ üzerinde self ortogonal bir kod olmasıdır. Ayrıca C nin self-dual kod olması için gerek ve yeter koşul C_i $(1 \leq i \leq 5)$ nin $\mathbb{Z}_4$ üzerinde self-dual kod olmasıdır.

İspat:

(1) İspatı açıktır.

(2) $D = C^{\perp} = a_1 C_1^{\perp} \oplus a_2 C_2^{\perp} \oplus a_3 C_3^{\perp} \oplus a_4 C_4^{\perp} \oplus a_5 C_5^{\perp}$ olsun. $c = c_1 a_1 + c_2 a_2 + c_3 a_3 + c_4 a_4 + c_5 a_5$, $d = d_1 a_1 + d_2 a_2 + d_3 a_3 + d_4 a_4 + d_5 a_5$, $c_i \in C_i$, $d_i \in C_i^{\perp}$ olmak üzere $\forall\, c \in C, d \in D$ için $c.d = \sum_{i=1}^{5} (c_i . d_i) a_i$ dir. Dolayısıyla $c.d = 0$ dir. Bu durumda $D \subseteq C^{\perp}$ olur. Ayrıca

$$|D| = |C_1^{\perp}||C_2^{\perp}||C_3^{\perp}||C_4^{\perp}||C_5^{\perp}| = \frac{4^n}{|C_1|}\frac{4^n}{|C_2|}\frac{4^n}{|C_3|}\frac{4^n}{|C_4|}\frac{4^n}{|C_5|} = \frac{|R_B|^n}{|C|} = |C^{\perp}|$$

dir. Dolayısıyla $C^{\perp} = D$ eşitliği elde edilir.

(3) C nin self ortogonal bir kod olması için gerek ve yeter koşul $C \subseteq C^{\perp}$ olmasıdır. (1) ve (2) den $C \subseteq C^{\perp}$ olması için gerek ve yeter koşul $C_i \subseteq C_i{}^{\perp}$ $(1 \leq i \leq 5)$ olmasıdır. Bu durumda C_i $(1 \leq i \leq 5)$ $\mathbb{Z}_4$ üzerinde self ortogonal koddur. Benzer şekilde C kodunun self-dual bir kod olması için gerek ve yeter koşul C_i $(1 \leq i \leq 5)$ kodunun $\mathbb{Z}_4$ üzerinde bir self-dual kod olmasıdır.

Sonuç 4.1.2.6. R_B üzerinde keyfi uzunlukta self-dual kodlar vardır.

İspat: Teorem 4.1.2.2. ve Teorem 4.1.2.3. den R_B üzerinde self-dual kod olması için gerek ve yeter koşul $\mathbb{Z}_4$ üzerinde self-dual kod olmasıdır. Açıkça $\mathbb{Z}_4$ self-dual kodun üreteç matrisi

$$\begin{bmatrix} 2 & & \\ & \ddots & \\ & & 2 \end{bmatrix}$$

dir.

Ayrıca , R_B üzerindeki lineer kodun üreteç matrisi olduğunu biliyoruz.

Not 4.1.2.7.

$$G_i = \begin{bmatrix} I_{k_{i1}} & A_i & B_i \\ 0 & 2I_{k_{i2}} & 2C_i \end{bmatrix}$$

$(1 \leq i \leq 5)$ $\mathbb{Z}_4$ üzerinde tanımlı C_i kodlarının üreteç matrisi olmak üzere $C = a_1C_1 \oplus a_2C_2 \oplus a_3C_3 \oplus a_4C_4 \oplus a_5C_5$ kodunun üreteç matrisi

$$G = \begin{bmatrix} a_1G_1 \\ a_2G_2 \\ a_3G_3 \\ a_4G_4 \\ a_5G_5 \end{bmatrix}$$

dir.

$$G_i' = \begin{bmatrix} -B_i^t - C_i^t A_i^t & C_i^t & I_{n-k_{i1}-k_{i2}} \\ 2A_i^t & 2I_{k_{i2}} & 0 \end{bmatrix}$$

$\mathbb{Z}_4$ üzerinde tanımlı C_i lineer kodunun duali $C_i{}^{\perp}$ in üreteç matrisi olmak üzere $C^{\perp}$ kodunun üreteç matrisi

$$H = \begin{bmatrix} a_1 G_1' \\ a_2 G_2' \\ a_3 G_3' \\ a_4 G_4' \\ a_5 G_5' \end{bmatrix}$$

dir.

H, C kodunun kontrol matrisi olarak adlandırılır.

Teorem 4.1.2.8. C, R_B üzerinde n uzunluğunda bir lineer kod olsun. O halde

$$\phi_B(C) = C_1 \otimes C_2 \otimes C_3 \otimes C_4 \otimes C_5 \text{ ve } |C| = |C_1|.|C_2|.|C_3|.|C_4|.|C_5|$$

olur.

İspat: Herhangi bir $(x_1, \dots, x_n, y_1, \dots, y_n, z_1, \dots, z_n, s_1, \dots s_n, t_1, \dots, t_n) \in \phi_B(C)$ elemanını alalım. $1 \leq i \leq n$ için $c_i = x_i + y_i + u(x_i) + v(x_i + z_i) + w(x_i + y_i + z_i + t_i) + uv(x_i + s_i)$ olsun. ϕ_B birebir ve örten olduğundan $c = (c_1, c_2, \dots, c_n) \in C$ dir. C_1, C_2, C_3, C_4, C_5 kodlarının tanımından $(x_1, \dots, x_n) \in C_1$, $(y_1, \dots, y_n) \in C_2$, $(z_1, \dots, z_n) \in C_3$, $(s_1, \dots, s_n) \in C_4$ ve $(t_1, \dots, t_n) \in C_5$ dir. Böylece $(x_1, \dots, x_n, y_1, \dots, y_n, z_1, \dots, z_n, s_1, \dots, s_n, t_1, \dots t_n) \in C_1 \otimes C_2 \otimes C_3 \otimes C_4 \otimes C_5$ olur. O halde $\phi_B(C) \subseteq C_1 \otimes C_2 \otimes C_3 \otimes C_4 \otimes C_5$ dir.

Diğer taraftan $(x_1, \dots, x_n) \in C_1$, $(y_1, \dots, y_n) \in C_2$, $(z_1, \dots, z_n) \in C_3$, $(s_1, \dots s_n) \in C_4$ ve $(t_1, \dots t_n) \in C_5$ için herhangi bir $(x_1, \dots, x_n, y_1, \dots, y_n, z_1, \dots, z_n, s_1, \dots s_n, t_1, \dots t_n) \in C_1 \otimes C_2 \otimes C_3 \otimes C_4 \otimes C_5$ elemanını alalım. Burada $p_i, q_i, r_i, n_i, m_i \in Z_4$ için $a_i = x_i + (v + w + uv)p_i$,

$b_i = y_i + (u + v + w + uv)q_i$, $c_i = z_i + (u + w + uv)r_i$, $d_i = s_i + (w)n_i$, $e_i = t_i + (u + v + uv)m_i$ olacak şekilde $a = (a_1, \dots, a_n)$, $b = (b_1, \dots, b_n)$,

$c = (c_1, \dots, c_n)$, $d = (d_1, \dots, d_n)$, $e = (e_1, \dots, e_n) \in C$ elemanları vardır. C bir lineer kod olduğundan $c = (u - uv)a + (1 - u - v - w + uv)b + (v - uv)c + (uv)d + we = x + y + (x)u + (x + z)v + (x + y + z + t)w + (x + s)uv$ dir. Bu durumda $\phi_B(C) = (x, y, z, s, t) \in \phi_B(C)$ dir. Dolayısıyla $C_1 \otimes C_2 \otimes C_3 \otimes C_4 \otimes C_5 \subseteq \phi_B(C)$ olur. O halde $\phi_B(C) = C_1 \otimes C_2 \otimes C_3 \otimes C_4 \otimes C_5$ dir.

Ayrıca $\phi_B(C)$ birebir ve örten olduğundan

$$|\phi_B(C)| = |C_1 \otimes C_2 \otimes C_3 \otimes C_4 \otimes C_5| = |C_1|.|C_2|.|C_3|.|C_4|.|C_5|$$

dir.

Sonuç 4.1.2.9. $a_1 = u - uv$, $a_2 = 1 - u - v - w + uv$, $a_3 = v - uv$, $a_4 = uv$, $a_5 = w$ olmak üzere

$\phi_B(C)$=$C_1 \otimes C_2 \otimes C_3 \otimes C_4 \otimes C_5$ ise $C = a_1C_1 \oplus a_2C_2 \oplus a_3C_3 \oplus a_4C_4 \oplus a_5C_5$

olur.

4.1.3. $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 + w\mathbb{Z}_4 + uv\mathbb{Z}_4$ Halkası Üzerindeki Devirli Kodlar

Teorem 4.1.3.1. C = $a_1C_1 \oplus a_2C_2 \oplus a_3C_3 \oplus a_4C_4 \oplus a_5C_5$, R_B üzerinde tanımlı bir lineer kod olsun. C kodunun R_B üzerinde tanımlı bir devirli kod olması için gerek ve yeter koşul C_1, C_2, C_3, C_4, C_5 kodlarının $\mathbb{Z}_4$ üzerinde tanımlı devirli kodlar olmasıdır.

İspat: $x = (x_1, \dots, x_n) \in C_1$, $y = (y_1, \dots, y_n) \in C_2$, $z = (z_1, \dots, z_n) \in C_3$, $s = (s_1, \dots s_n) \in C_4$ ve $t = (t_1, \dots t_n) \in C_5$ olsun. $j = 1, \dots, n$ için $c_j = a_1x_j + a_2y_j + a_3z_j + a_4s_j + a_5t_j$ olmak üzere $c = (c_1, \dots, c_n) \in C$ dir. C bir devirli kod olduğundan

$$\begin{aligned}\tau(c) &= (c_n, c_1, c_2, \dots, c_{n-1}) \\ &= a_1(x_n, x_1, \dots, x_{n-1}) + a_2(y_n, y_1, \dots, y_{n-1}) + a_3(z_n, z_1, \dots, z_{n-1}) \\ &+ a_4(s_n, s_1, \dots, s_{n-1}) + a_5(t_n, t_1, \dots, t_{n-1}) \in C\end{aligned}$$

dir. Böylece $\tau(x) = (x_n, x_1, \dots, x_{n-1}) \in C_1$, $\tau(y) = (y_n, y_1, \dots, y_{n-1}) \in C_2$,

$\tau(z) = (z_n, z_1, \dots, z_{n-1}) \in C_3, \tau(s) = (s_n, s_1, \dots, s_{n-1}) \in C_4$,
$\tau(t) = (t_n, t_1, \dots, t_{n-1}) \in C_5$ dir. O halde C_1, C_2, C_3, C_4 ve C_5 $\mathbb{Z}_4$ üzerinde tanımlı devirli kodlardır.

Tersine C_1, C_2, C_3, C_4 ve C_5 $\mathbb{Z}_4$ üzerinde tanımlı devirli kodlar ve $j = 1, \dots, n$ için $c_j = a_1x_j + a_2y_j + a_3z_j + a_4s_j + a_5t_j$ olmak üzere $c = (c_1, \dots, c_n) \in C$ olsun. Bu durumda $x = (x_1, \dots, x_n) \in C_1$, $y = (y_1, \dots, y_n) \in C_2$, $z = (z_1, \dots, z_n) \in C_3$, $s = (s_1, \dots, s_n) \in C_4$ ve $t = (t_1, \dots, t_n) \in C_5$ dir. C_1, C_2, C_3, C_4 ve C_5 kodları devirli kodlar olduğundan $\tau(x) = (x_n, x_1, \dots, x_{n-1}) \in C_1$, $\tau(y) = (y_n, y_1, \dots, y_{n-1}) \in C_2$, $\tau(z) = (z_n, z_1, \dots, z_{n-1}) \in C_3, \tau(s) = (s_n, s_1, \dots, s_{n-1}) \in C_4$,
$\tau(t) = (t_n, t_1, \dots, t_{n-1}) \in C_5$ dir. Bu durumda $a_1\tau(x) + a_2\tau(y) + a_3\tau(z) + a_4\tau(s) + a_5\tau(t) = (c_n, c_1, c_2, \dots, c_{n-1}) = \tau(c) \in C$ dir. O halde C, R_B üzerinde tanımlı bir devirli koddur.

Lemma 3.2.3.2. kullanılarak aşağıdaki lemma elde edilir.

Lemma 4.1.3.2. $f_1(x) \dots f_r(x)$ indirgenemez polinomlar, n tek tamsayı $x^n - 1 = \prod_{i=1}^{r} f_i(x)$ olmak üzere C, $\mathbb{Z}_4$ üzerinde n uzunluğunda devirli bir kod olsun. Bu durumda $f_0(x)$ ve $f_1(x)$, $x^n - 1$ in monik bölenleri ve $f_1(x)|f_0(x)$ olmak üzere $C = \langle f_0(x), 2f_1(x)\rangle = \langle f_0(x) + 2f_1(x)\rangle$ dır.

Genel olarak herhangi bir n uzunluğunda $\mathbb{Z}_4$ üzerinde lineer kod ise $f(x), g(x), p(x) \in \mathbb{Z}_4[x]$ monik polinomları vardır. $g(x)|f(x)|(x^n - 1)$, $g(x)|p(x)\left(\frac{x^n-1}{f(x)}\right)$ ve $|C| = 2^{2n-der(f(x))-der(g(x))}$ olmak üzere $C = \langle f(x) + 2p(x), 2g(x)\rangle$ dir.

Teorem 4.1.3.3. $\mathrm{C} = a_1C_1 \oplus a_2C_2 \oplus a_3C_3 \oplus a_4C_4 \oplus a_5C_5$, R_B üzerinde n uzunluğunda bir devirli kod olsun. Eğer $C_i = \langle f_i(x) + 2p_i(x), 2g_i(x)\rangle$ olacak şekilde $f_i(x), g_i(x), p_i(x) \in \mathbb{Z}_4[x]$, $(1 \le i \le 5)$ varsa bu durumda

$$C = \langle \sum_{i=1}^{5} a_i f_i(x) + 2\sum_{i=1}^{5} a_i p_i(x), 2\sum_{i=1}^{5} a_i g_i(x)\rangle$$

dir. Ayrıca n tek ise

$$C = \langle \sum_{i=1}^{5} a_i (f_i(x) + 2g_i(x))\rangle = \langle \sum_{i=1}^{5} a_i f_i(x) + 2\sum_{i=1}^{5} a_i g_i(x)\rangle$$

dir.

İspat: $D = \langle \sum_{i=1}^{5} a_i f_i(x) + 2\sum_{i=1}^{5} a_i p_i(x), 2\sum_{i=1}^{5} a_i g_i(x)\rangle$ olsun. $\forall c(x) \in C$ için $c(x) = \sum_{i=1}^{5} a_i((f_i(x) + 2p_i(x))u_i(x) + 2g_i(x)v_i(x))$ olacak şekilde $u_i(x), v_i(x) \in \mathbb{Z}_4[x]$ dir. Bu durumda

$$\sum_{i=1}^{5} a_i((f_i(x) + 2p_i(x))u_i(x) + 2g_i(x)v_i(x))$$

$$= \sum_{i=1}^{5} a_i u_i(x) \sum_{i=1}^{5} a_i(f_i(x) + 2p_i(x)) + \sum_{i=1}^{5} a_i v_i(x) \sum_{i=1}^{5} 2a_i g_i(x)$$

olduğundan $C \subseteq D$ dir. $D \subseteq C$ olduğu açıktır. Dolayısıyla $C = D$ elde edilir.

C nin dual kodunun üreteç polinomunu inceleyelim. $\forall f(x)|\ (x^n - 1)$,

$\hat{f}(x) = \frac{x^n-1}{f(x)}$ ve C, $\mathbb{Z}_4$ üzerinde n uzunluğunda bir devirli kod olsun. Bu durumda $g(x)|f(x)|(x^n - 1)$,

$der(p(x)) < der(g(x))$ ve $p(x)\frac{x^n-1}{f(x)} = g(x)u(x)$ olmak üzere

$C = \langle f(x) + 2p(x), 2g(x)\rangle$ vardır. Dolayısıyla $\big(\hat{g}(x) + 2u(x)\big)\big(f(x) + 2p(x)\big) = 2\big(f(x)u(x) + \hat{g}(x)p(x)\big) = 0$ ve $der(u(x)) < der(\hat{g}(x))$ dir.

Teorem 4.1.3.4. $C = \langle f(x) + 2p(x), 2g(x)\rangle$, $\mathbb{Z}_4$ üzerinde n uzunluğunda bir devirli kod olsun. Bu durumda $C^{\perp} = \langle \hat{g}(x)^* + 2x^{der(\hat{g}(x))-der(u(x))}u(x)^*, 2\hat{f}(x)^*\rangle$ dir.

İspat: $D = \langle \hat{g}(x) + 2u(x), 2\hat{f}(x)\rangle$ olsun. O halde $\big(\hat{g}(x) + 2u(x)\big)\big(f(x) + 2p(x)\big) = 0$ olur ve $|D| = 2^{2n-der(\hat{g}(x))-der\left(\hat{f}(x)\right)} = 2^{der(g(x))+der(f(x))} = |Ann(C)|$ dir. O halde $D = |Ann(C)|$ olur. Böylece

$$C^{\perp} = Ann(C)^* = \langle \hat{g}(x)^* + 2x^{der(\hat{g}(x))-der(u(x))}u(x)^*, 2\hat{f}(x)^*\rangle$$

eşitliği bulunur. Burada $Ann(C)$ ye sıfırlayıcı denir ve $Ann(C) = \{c' | c.c' = 0, c \in C\}$ şeklinde tanımlanır.

Teorem 4.1.3.3. ve Teorem 4.1.3.4 ün ispatında olduğu gibi benzer bir teknik kullanılarak aşağıdaki teoremde verilen devirli kodların dualinin üreteç polinomları elde edilir.

Teorem 4.1.3.5. $C = \langle f(x) + 2p(x), 2g(x)\rangle$, $\mathbb{Z}_4$ üzerinde bir devirli kod olsun.

$$C^{\perp} = \langle \sum_{i=1}^{5} a_i\hat{g}_i(x)^* + 2\sum_{i=1}^{5} a_i x^{der(\hat{g}_i(x))-der(u_i(x))}u_i(x)^*, 2\sum_{i=1}^{5} a_i\hat{f}_i(x)^*\rangle$$

şeklinde yazılır.

Sonuç 4.1.3.6. $\phi_B(C) = \prod_{i=1}^{5} C_i$, $\mathbb{Z}_4$ üzerinde $5n$ uzunluğunda (n tek) bir lineer kod ve $\prod_{i=1}^{5} C_i$, $\mathbb{Z}_4$ üzerinde bir devirli kod olsun ($1 \le i \le 5$). Bu durumda $\phi_B(C)$ nin eleman sayısı $4^{\Sigma_{i=1}^{5}(n-der\left(f_{1,i}(x)\right))}2^{\Sigma_{i=1}^{5}(der(f_{1,i}(x)-derf_{2,i}(x))}$ dir.

Şimdi $\mathbb{Z}_4$ üzerinde $5n$ uzunluğunda (n tek) $\phi_B(C) = \prod_{i=1}^{5} C_i$ lineer kodunu inceleyelim. $\phi_B(C)$ nin Lee uzaklığı d_L olsun. $w_L(c) = d_L(C_j)$ olacak şekilde $c \in C_j, min_{1\le i\le 5} d_L(C_i) = d_L(C_j)$ dir. O halde $d_L\left({\phi_B}^{-1}(0,\dots,0,0,\dots,0)\right) = d_L(C_j)$ ve bu durumda $d_L = min_{1\le i\le 5} d_L(C_i)$ dir.

Teorem 4.1.3.7. n tek, C n uzunluğunda bir devirli kod olsun. $C = \langle e(x) \rangle$ olacak şekilde bir tek $e(x) = a_1e_1(x) + a_2e_2(x) + a_3e_3(x) + a_4e_4(x) + a_5e_5(x) \in R_{B,n} = R[x] / \langle x^n - 1 \rangle$ idempotent elemanı vardır.

İspat: $C_1 = \langle e_1(x) \rangle$, $C_2 = \langle e_2(x) \rangle$, $C_3 = \langle e_3(x) \rangle$, $C_4 = \langle e_4(x) \rangle$, $C_5 = \langle e_5(x) \rangle$ olacak şekilde tek bir $e_1(x)$, $e_2(x)$, $e_3(x), e_4(x), e_5(x) \in \mathbb{Z}_4[x]$ üreteç idempotent elemanları vardır. Teorem 4.1.3.3. den $C = \langle a_1e_1(x) + a_2e_2(x) + a_3e_3(x) + a_4e_4(x) + a_5e_5(x) \rangle$ dir. $e(x) = a_1e_1(x) + a_2e_2(x) + a_3e_3(x) + a_4e_4(x) + a_5e_5(x)$ olsun. Bu durumda $e(x)^2 = a_1e_1(x)^2 + a_2e_2(x)^2 + a_3e_3(x)^2 + a_4e_4(x)^2 + a_5e_5(x)^2 = a_1e_1(x) + a_2e_2(x) + a_3e_3(x) + a_4e_4(x) + a_5e_5(x) = e(x)$ dir. Dolayısıyla $e(x)$ C nin idempotent elemanıdır. $C = \langle d(x) \rangle$ ve $d(x)^2 = d(x)$ olacak şekilde $d(x) \in C$ var olsun. O halde $d(x) \in C = \langle e(x) \rangle$ olduğundan $d(x) = a(x)e(x)$ olacak şekilde $a(x) \in R_{B,n}$ vardır. Bu durumda $d(x)e(x) = a(x)e(x)^2 = d(x)$ olur. Benzer şekilde $d(x)e(x) = e(x)$ olur. Yani $d(x) = e(x)$ elde edilir.

Yukarıdaki teoremden $e(x)$ idempotent elemanı C nin idempotent üreteci olarak adlandırılır.

Teorem 4.1.3.8. $C = a_1C_1 \oplus a_2C_2 \oplus a_3C_3 \oplus a_4C_4 \oplus a_5C_5$, R_B üzerinde n uzunluğunda bir devirli kod ve $\mathbb{Z}_4$ üzerindeki C_1, C_2, C_3, C_4 ve C_5 in idempotentleri sırasıyla $e_1(x)$, $e_2(x)$, $e_3(x)$, $e_4(x)$ ve $e_5(x)$ olmak üzere

$e(x) = a_1e_1(x) + a_2e_2(x) + a_3e_3(x) + a_4e_4(x) + a_5e_5(x)$ olsun. Bu durumda $C^\perp$ in idempotenti $1 - e(x^{-1})$ dir.

İspat: Teorem 4.1.2.5. den $C^\perp = a_1C_1^\perp \oplus a_2C_2^\perp \oplus a_3C_3^\perp \oplus a_4C_4^\perp \oplus a_5C_5^\perp$ dir. Ayrıca $C_i^\perp$ $(1 \leq i \leq 5)$, devirli kodlar olduğundan $C^\perp$ de devirli koddur. C_1, C_2, C_3, C_4 ve C_5 in idempotentleri sırasıyla $e_1(x)$, $e_2(x)$, $e_3(x)$, $e_4(x)$ ve $e_5(x)$ olsun. Bu durumda $C_1^\perp, C_2^\perp, C_3^\perp, C_4^\perp$ ve $C_5^\perp$ in idempotentleri sırasıyla

$1 - e_1(x^{-1}), 1 - e_2(x^{-1}), 1 - e_3(x^{-1}), 1 - e_4(x^{-1})$ ve $1 - e_5(x^{-1})$ dir. $C^\perp$ in idempotenti $\hat{e}(x)$ olsun. Dolayısıyla Teorem 4.1.3.7. den

$$\begin{aligned}\hat{e}(x) &= a_1\big(1 - e_1(x^{-1})\big) + a_2\big(1 - e_2(x^{-1})\big) + a_3\big(1 - e_3(x^{-1})\big) \\ &\quad + a_4\big(1 - e_4(x^{-1})\big) + a_5\big(1 - e_5(x^{-1})\big) \\ &= 1 - e(x^{-1})\end{aligned}$$

olur.

Tanım 4.1.3.9. $j = 0,1,\dots,n-1$, $a^{i,j} \in \mathbb{Z}_4$ olmak üzere $a^{(i)} = (a^{(i,0)},\dots,a^{(i,n-1)})$ için $\sigma(a^{(i)}) = (a^{(i,n-1)}, a^{(i,0)},\dots,a^{(i,n-2)})$ ve $a \in \mathbb{Z}_4^{5n}$, $i = 0,1,2,3,4$ için $a = (a^{(0)}|a^{(1)}|a^{(2)}|a^{(3)}|a^{(4)})$, $a^{(i)} \in \mathbb{Z}_4^{5n}$ olsun. $\varphi: \mathbb{Z}_4^{5n} \to \mathbb{Z}_4^{5n}$ olmak üzere $\varphi(a) = (\tau(a^{(0)})|\tau(a^{(1)})|\tau(a^{(2)})|\tau(a^{(3)})|\tau(a^{(4)}))$ şeklinde tanımlansın. $\varphi(C) = C$ ise $\mathbb{Z}_4$ üzerinde tanımlı $5n$ uzunluklu bir kod indeksi 5 olan quasi-cyclic kod olarak adlandırılır.

Önerme 4.1.3.10. τ, R_B^n üzerinde cyclic-shift, ϕ_B R_B^n den $\mathbb{Z}_4^{5n}$ e Gray dönüşüm ve φ Tanım 4.1.3.9. da tanımlanan dönüşüm olsun. O halde $\phi_B\tau = \varphi\phi_B$ dir.

İspat: $\forall i = 0,1,\dots,n-1$ ve $r_i = a_i + ub_i + vc_i + wd_i + uve_i$ olmak üzere $r = (r_0, r_1, \dots, r_{n-1}) \in R_B^n$ olsun.

$$\begin{aligned}\tau(r) &= (r_{n-1}, r_0, r_1, \dots, r_{n-2})\\ &= (a_{n-1} + ub_{n-1} + vc_{n-1} + wd_{n-1} + uve_{n-1}, a_0 + ub_0 + vc_0\\ &+ wd_0 + uve_0, \dots, a_{n-2} + ub_{n-2} + vc_{n-2} + wd_{n-2} + uve_{n-2})\\ &= (a_{n-1}, a_0, a_1, \dots, a_{n-2}) + u(b_{n-1}, b_0, b_1, \dots, b_{n-2})\\ &+ v(c_{n-1}, c_0, c_1, \dots, c_{n-2}) + w(d_{n-1}, d_0, d_1, \dots, d_{n-2})\\ &+ uv(e_{n-1}, e_0, e_1, \dots, e_{n-2})\end{aligned}$$

$$\begin{aligned}\phi_B(\tau(r)) = (&a_{n-1} + b_{n-1}, a_0 + b_0, \dots, a_{n-2} + b_{n-2}, a_{n-1}, a_0, \dots, a_{n-2}, a_{n-1} +\\ &c_{n-1}, a_0 + c_0, \dots, a_{n-2} + c_{n-2}, a_{n-1} + b_{n-1} + c_{n-1} + e_{n-1}, a_0 + b_0 + c_0 +\\ &e_0, \dots, a_{n-2} + b_{n-2} + c_{n-2} + e_{n-2}, a_{n-1} + d_{n-1}, a_0 + d_0, \dots, a_{n-2} + d_{n-2}) \dots\dots (1)\end{aligned}$$

$$\begin{aligned}\phi_B(r) &= (a_0 + b_0, a_1 + b_1, \dots, a_{n-1} + b_{n-1}, a_0, a_1, \dots, a_{n-1}, a_0 + c_0, a_1\\ &+ c_1, \dots, a_{n-1} + c_{n-1}, a_0 + b_0 + c_0 + e_0, a_1 + b_1 + c_1 + e_1, \dots, a_{n-1}\\ &+ b_{n-1} + c_{n-1} + e_{n-1}, a_0 + d_0, a_1 + d_1, \dots, a_{n-1} + d_{n-1})\end{aligned}$$

$$\varphi(\phi_B(r)) = (\tau(r^{(0)})|\tau(r^{(1)})|\tau(r^{(2)})|\tau(r^{(3)})|\tau(r^{(4)}))$$

olduğundan $r = (r_0, r_1, \dots, r_{n-1}) \in R_B^n$ iken $\tau(r) = (r_{n-1}, r_0, r_1, \dots, r_{n-2})$ olur.

$$\phi_B(r^{(0)}) = (a_0 + b_0, a_1 + b_1, \dots, a_{n-1} + b_{n-1})$$

$$\Rightarrow \tau\phi_B(r^{(0)}) = (a_{n-1} + b_{n-1}, a_0 + b_0, \dots, a_{n-2} + b_{n-2})$$

$$\phi_B(r^{(1)}) = (a_0, a_1, \dots, a_{n-1}) \Rightarrow \tau\phi_B(r^{(1)}) = (a_{n-1}, a_0, \dots, a_{n-2})$$

$$\phi_B(r^{(2)}) = (a_0 + c_0, a_1 + c_1, \dots, a_{n-1} + c_{n-1})$$

$$\Rightarrow \tau\phi_B\left(r^{(2)}\right) = (a_{n-1}c_{n-1}, a_0 + c_0, \dots, a_{n-2} + c_{n-2})$$

$$\phi_B\left(r^{(3)}\right) = (a_0 + b_0 + c_0 + e_0, a_1 + b_1 + c_1 + e_1, \dots, a_{n-1} + b_{n-1} + c_{n-1} + e_{n-1})$$

$$\Rightarrow \tau\phi_B\left(r^{(3)}\right) = (a_{n-1} + b_{n-1} + c_{n-1} + e_{n-1}, a_0 + b_0 + c_0 + e_0, \dots, a_{n-2} + b_{n-2} + c_{n-2} + e_{n-2})$$

$$\phi_B\left(r^{(4)}\right) = (a_0 + d_0, a_1 + d_1, \dots, a_{n-1} + d_{n-1})$$

$$\Rightarrow \tau\phi_B\left(r^{(4)}\right) = (a_{n-1} + d_{n-1}, a_0 + d_0, \dots, a_{n-2} + d_{n-2})$$

olduğundan

$$\varphi\left(\phi_B(r)\right) = (a_{n-1} + b_{n-1}, a_0 + b_0, \dots, a_{n-2} + b_{n-2}, a_{n-1}, a_0, \dots, a_{n-2}, a_{n-1} + c_{n-1}, a_0 + c_0, \dots, a_{n-2} + c_{n-2}, a_{n-1} + b_{n-1} + c_{n-1} + e_{n-1}, a_0 + b_0 + c_0 + e_0, \dots, a_{n-2} + b_{n-2} + c_{n-2} + e_{n-2}, a_{n-1} + d_{n-1}, a_0 + d_0, \dots, a_{n-2} + d_{n-2}) \quad \text{…….(2)}$$

olur.

(1) ve (2) den $\phi_B\tau = \varphi\phi_B$ elde edilir.

Teorem 4.1.3.11. R_B üzerinde tanımlı n uzunluğunda devirli kodun ϕ_B Gray görüntüsü $\mathbb{Z}_4$ üzerinde tanımlı $5n$ uzunluğunda 5 indeksli quasi-cyclic koda denktir.

İspat: C, R_B üzerinde tanımlı devirli kod olsun. Bu durumda $\tau(C) = C$ dir. ϕ_B uygulanırsa $\phi_B\left(\tau(C)\right) = \phi_B(C)$ olur. Önerme 4.1.3.10. dan

$$\phi_B\left(\tau(C)\right) = \varphi\left(\phi_B(C)\right) = \phi_B(C)$$

dir. O halde $\phi_B(C)$, $\mathbb{Z}_4$ üzerinde tanımlı $5n$ uzunluğunda indeksi 5 olan quasi-cyclic koda denktir.

5. SONUÇ VE ÖNERİLER

Bu çalışmada $v^2 = v$ olmak üzere $\mathbb{Z}_4 + v\mathbb{Z}_4$ halkası üzerindeki lineer kodlar ve devirli kodlar incelendi. $u^2 = u$, $v^2 = v$ ve $uv = vu$ olmak üzere $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 + uv\mathbb{Z}_4$ halkası üzerindeki lineer kodlar ve devirli kodlar hakkında çalışmalar gösterildi. $u^2 = u$, $v^2 = v$, $w^2 = w$, $uv = vu, uw = wu$ ve $vw = wv$ olmak üzere $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 + w\mathbb{Z}_4 + uv\mathbb{Z}_4 + uw\mathbb{Z}_4 + vw\mathbb{Z}_4 + uvw\mathbb{Z}_4$ halkası üzerindeki devirli kodlar verildi. Bu çalışmalardan yola çıkılarak $u^2 = u, v^2 = v, w^2 = w, uv = vu, uw = vw = 0$ olmak üzere yeni bir $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 + w\mathbb{Z}_4 + uv\mathbb{Z}_4$ halkasının cebirsel yapısı ortaya konularak bu halka üzerindeki devirli kodlar elde edildi. Yeni bir uzaklık koruyan Gray dönüşümü tanımlanarak bu halka üzerindeki lineer kodlar tanıtıldı. Ayrıca bu halka üzerindeki devirli kodların Gray görüntüsünün $\mathbb{Z}_4$ üzerinde tanımlı quasi-cyclic koda denk olduğu gösterildi.

Çalışmamızda kullanılan sonlu halkalar genelleştirilerek literatürde var olan çeşitli kodlar ve parametreleri araştırılabilir. Ayrıca yeni sonlu halkalar tanımlanarak benzer çalışmalar yapılabilir.

KAYNAKLAR

Aydin, N., Cengellenmis, Y., and Dertli, A. (2018). "On some constacyclic codes over $\mathbb{Z}_4[u] / \langle u^2 - 1 \rangle$, their $\mathbb{Z}_4$ images and new codes". *Designs, Codes and Cryptography*, *86*(6), 1249-1255.

Bandi, R. K., and Bhaintwal, M. (2014). "Codes over $\mathbb{Z}_4 + v\mathbb{Z}_4$". *In 2014 International Conference on Advances in Computing*, Communications and Informatics (ICACCI) (pp. 422-427). IEEE.

Blake, I. F. (1972). *"*Codes over certain rings*"*. *Information and Control*, *20*(4), 396-404.

Bustomi, Santika A. P. and Suprijanto D. (2021) "Linear codes over the ring $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 + w\mathbb{Z}_4 + uv\mathbb{Z}_4 + uw\mathbb{Z}_4 + vw\mathbb{Z}_4 + uvw\mathbb{Z}_4$". *International Journal of Computer Science*, 48(3), 686-696

Çallıalp, F. (2018). *Örneklerle soyut cebir*. İstanbul: Birsen Yayınevi.

Dertli, A. (2016). *Halkalar üzerinde tanımlı kodlar hakkında bazı araştırmalar*. Doktora Tezi. Ondokuz Mayıs Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalı, Samsun.

Gao, J., Gao, Y., and Fu, F. W. (2014). "Some result on linear codes over $\mathbb{Z}_4 + v\mathbb{Z}_4$". *arXiv preprint arXiv:1402.6771*.

Güzel, G. G. (2019). *Sonlu halkalar üzerinde tanımlı bazı özel kodların incelenmesi ve uygulanması*. Doktora Tezi. Trakya üniversitesi Fen Bilimleri Enstitüsü Hesaplamalı Bilimler Anabilim Dalı, Edirne.

Hammons, A. R., Kumar, P. V., Calderbank, A. R., Sloane, N. J., & Solé, P. (1994). "The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes". *IEEE Transactions on Information Theory*, *40*(2), 301-319.

Hill, R. (1986). *A first course in coding theory*. Oxford: The Oxford University Press.

Huffman, W. C. and Pless, V. (2003). *Fundamentals of error correcting codes.* New York: Cambridge University Press.

Hungerford, T. W. (1973). *Algebra*. New York: Springer.

Jitman, S., Ling, S. and Udamkavanich, P. (2010). "Skew constacyclic codes over finite chain rings". *Advences in Mathematics of Communications*, 6(1), 39-63.

Li P., Guo X. and Zhu S. (2016). "Some results of linear codes over the ring $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 + uv\mathbb{Z}_4$". arXiv preprint arXiv:1601.04453.

Ling, S. and Xing, C. (2004). *Coding theory a first course*. New York: Cambridge University Press.

Özlü, Ş. (2015). *Bazı sonlu cisimler üzerindeki esnek polinom kodlar*. Doktora Tezi. Nevşehir Hacı Bektaş Veli Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalı, Nevşehir.

Roman, S. (1992). *Coding and information theory*. Graduate Text in Mathematics, Springer Verlag.

Taşçı, D. (2007). *Soyut cebir*. Ankara: Alp Yayınevi.

Tuğcu, E. (2007). *Turbokodlar ve turbo denkleştiriciler.* Yüksek Lisans Tezi. Karadeniz Teknik Üniversitesi Fen Bilimleri Enstitüsü Elektrik-Elektronik Mühendisliği Anabilim Dalı, Trabzon.

ÖZ GEÇMİŞ

Büşra TUSUN, Samsun Canik İMKB Anadolu Lisesi'ni bitirdikten sonra Ondokuz Mayıs Üniversitesi Fen Edebiyat Fakültesi, Matematik bölümünden 10.06.2019 tarihinde mezun oldu. 2019 yılında OMÜ LEE Matematik Ana Bilim Dalı Yüksek Lisans programına girdi.

İletişim Bilgileri

ORCID ID : *0000-0002-5322-7685*

Yayınlar:

1. Tusun, B. ve Eren, Ş. (2021). "$\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 + w\mathbb{Z}_4 + uv\mathbb{Z}_4$ halkası üzerindeki devirli kodlar". *33. Ulusal Matematik Sempozyumu.* İstanbul Üniversitesi, İstanbul