T.C.
ONDOKUZ MAYIS ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

HALKALAR ÜZERİNDE TANIMLI MACDONALD KODLAR

RABİA DERTLİ

MATEMATİK ANABİLİM DALI

SAMSUN
2020

TEZ ONAYI

Rabia DERTLİ tarafından hazırlanan "Halkalar Üzerinde Tanımlı MacDonald Kodlar'' adlı tez çalışması 08/01/2020 tarihinde aşağıdaki jüri tarafından Ondokuz Mayıs Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalı'nda **Yüksek Lisans Tezi** olarak kabul edilmiştir.

Danışman Prof. Dr. Şenol EREN
Matematik Anabilim Dalı

Jüri Üyeleri

Başkan Prof. Dr. Şenol EREN
Ondokuz Mayıs Üniversitesi
Matematik Anabilim Dalı

Üye Doç. Dr. Hamza ÇALIŞICI
Ondokuz Mayıs Üniversitesi
Matematik ve Fen Bilimleri Eğitimi Anabilim Dalı

Üye Dr. Öğr. Üyesi Esra ÖZTÜRK SÖZEN
Sinop Üniversitesi
Matematik Anabilim Dalı

Yukarıdaki sonucu onaylarım. / /2020

Prof. Dr. Bahtiyar ÖZTÜRK
Enstitü Müdürü

ETİK BEYAN

Ondokuz Mayıs Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına uygun olarak hazırladığım bu tez içindeki bütün bilgilerin doğru ve tam olduğunu, bilgilerin üretilmesi aşamasında bilimsel etiğe uygun davrandığımı, yararlandığım bütün kaynakları atıf yaparak belirttiğimi beyan ederim.

08.01.2020

Rabia Dertli

ÖZET

Yüksek Lisans Tezi

HALKALAR ÜZERİNDE TANIMLI
MACDONALD KODLAR

Rabia Dertli

Ondokuz Mayıs Üniversitesi
Fen Bilimleri Enstitüsü
Matematik Anabilim Dalı

Danışman: Prof. Dr. Şenol Eren

Beş bölümden oluşan bu tezin, birinci bölümünde; kodlama teorisi, Simplex kodlar ve MacDonald kodlar hakkında yapılan çalışmalardan bahsedilmiştir. İkinci bölümde; cebirsel ifadeler, kodlama teorisi ile ilgili kavramlar ve teoremler verilmiştir. Materyal bölümünde; $u^2 = 0$ olmak üzere $\mathbb{F}_2 + u\mathbb{F}_2$, $u^3 = 0$ olmak üzere $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$, $v^2 = 1$ olmak üzere $\mathbb{F}_3 + v\mathbb{F}_3$ sonlu değişmeli halkalarının cebirsel yapıları incelenmiş ve bu halkalar üzerinde Gray dönüşümü tanımlanarak ağırlık kavramları elde edilmiştir. Böylelikle bu halkalarda tanımlanan Simplex kodların üreteç matrisleri yardımıyla MacDonald kodlar oluşturulmuş ve özellikleri incelenmiştir. Bulgular bölümünün birinci kısmında, $u^2 = u, v^2 = v, uv = vu = 0$ olmak üzere $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2$ sonlu ve değişmeli halkası üzerinde bir Gray dönüşümü tanımlanarak Hamming, Lee ve Bachoc ağırlıkları elde edilmiştir. Bu halka üzerinde MacDonald kodlar inşa edilerek ağırlık dağılımları ve parametreler belirlenmiştir. Bulgular bölümünün ikinci kısmında, $u^2 = 0, v^2 = 0, uv = vu = 0$ olmak üzere $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2$ sonlu ve değişmeli halkası tanıtılarak bu halka üzerinde Gray dönüşümü tanımlanmıştır. Bu halka üzerindeki Simplex kodların üreteç matrisleri yardımıyla MacDonald kodlar inşa edilmiş ve Lee ağırlık dağılımları belirlenmiştir.

Ocak 2020, 50 sayfa

Anahtar Kelimeler: Sonlu halkalar, MacDonald kodlar, Ağırlık dağılımları

ABSTRACT

Master's Thesis

MACDONALD CODES OVER RINGS

Rabia Dertli

Ondokuz Mayıs University
Graduate School of Sciences
Department of Mathematics

Supervisor: Prof. Dr. Şenol Eren

In the first part of this thesis, which contains of five section; coding theory, Simplex codes and MacDonald codes are introduced. In the second part; algebraic definitions, basic concepts and theorems about the coding theory are given. In the material section; algebraic structures are examined over the finite commutative rings $\mathbb{F}_2 + u\mathbb{F}_2$, where $u^2 = 0$, $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$, where $u^3 = 0$, $\mathbb{F}_3 + v\mathbb{F}_3$, where $v^2 = 1$ and Gray map is defined over these rings and weight distributions were obtained. In this way, MacDonald codes are constructed by using generator matrices of Simplex codes over these rings and their properties are examined. In the first part of the last section, Hamming, Lee and Bachoc weights were obtained by defining a Gray map over the finite and commutative rings $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2$ with $u^2 = u, v^2 = v, uv = vu = 0$. MacDonald codes were constructed over this ring and weight distributions and parameters were determined. In the second part of the last section, the finite and commutative ring $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2$, with $u^2 = 0, v^2 = 0, uv = vu = 0$ is introduced and Gray map is defined over this ring. MacDonald codes were constructed by using generator matrices of Simplex codes over this ring and Lee weight distributions were determined.

January 2020, 50 pages

Kew Words: Finite rings, MacDonald codes, Weight distributions

ÖNSÖZ VE TEŞEKKÜR

Akademik çalışmalarım boyunca destek ve yardımlarını esirgemeyen değerli hocam Sayın Prof. Dr. Şenol Eren'e teşekkürlerimi sunarım.

Her yönüyle örnek edindiğim ve tecrübeleriyle beni yönlendiren değerli hocam Sayın Doç. Dr. Yasemin Çengellenmiş'e içten teşekkürlerimi sunarım.

Hayatım boyunca her türlü maddi ve manevi desteklerini esirgemeyen sevgili aileme ve bu süreçte en büyük manevi desteğim olan sevgili eşime sonsuz teşekkürlerimi sunarım.

Ocak 2020, Samsun

Rabia Dertli

İÇİNDEKİLER DİZİNİ

KISALTMALAR

$A \cong B$	A ve B izomorftur
$\mathbb{F}_q$	q elemanlı cisim
$\mathbb{F}_q^n$	Bileşenleri $\mathbb{F}_q$ cisminin elemanı olan n uzunluğundaki vektörlerin kümesi
boy(T)	T vektör uzayının boyutu
$\langle p, r \rangle$	p ile r vektörlerinin iç çarpımı
$\lvert \mathcal{C} \rvert$	$\mathcal{C}$ kodunun eleman sayısı
$\mathcal{C}^{\perp}$	$\mathcal{C}$ kodunun duali
N^T	N matrisinin transpozu
$w_H(r)$	r'nin Hamming ağırlığı
$w_L(r)$	r'nin Lee ağırlığı
$w_H(\mathcal{C})$	$\mathcal{C}$ kodunun minimum Hamming ağırlığı
$w_L(\mathcal{C})$	$\mathcal{C}$ kodunun minimum Lee ağırlığı
$d(r, s)$	r ile s arasındaki Hamming uzaklığı
$d(\mathcal{C})$	$\mathcal{C}$ kodunun minimum Hamming uzaklığı
$d_L(r, s)$	r ile s arasındaki Lee uzaklığı
$d_L(\mathcal{C})$	$\mathcal{C}$ kodunun minimum Lee uzaklığı
(n, M)	n uzunluğunda M elemanlı bir kod
(n, M, d)	d minimum uzaklığına sahip M elemanlı n uzunluğunda bir kod
$[n, k]$	k boyutlu n uzunluğunda lineer kod
$[n, k, d]$	Minimum uzaklığı d olan k boyutlu n uzunluğunda bir lineer kod
$d_q(n, k)$	Kodun en büyük minimum uzaklığı
$B_q(n, d)$	F_q üzerinde tanımlı lineer bir kodun eleman sayısının alabileceği en büyük değer
$A_q(n, d)$	A alfabesi üzerinde tanımlı bir kodun eleman sayısının alabileceği en büyük değer
$\mathcal{C} = \langle h(x) \rangle$	$h(x)$ tarafından üretilen $\mathcal{C}$ kodu
$\mathbb{F}_q[x]$	Katsayıları $\mathbb{F}_q$ cisminde olan polinom halkası

ŞEKİLLER DİZİNİ

ÇİZELGELER DİZİNİ

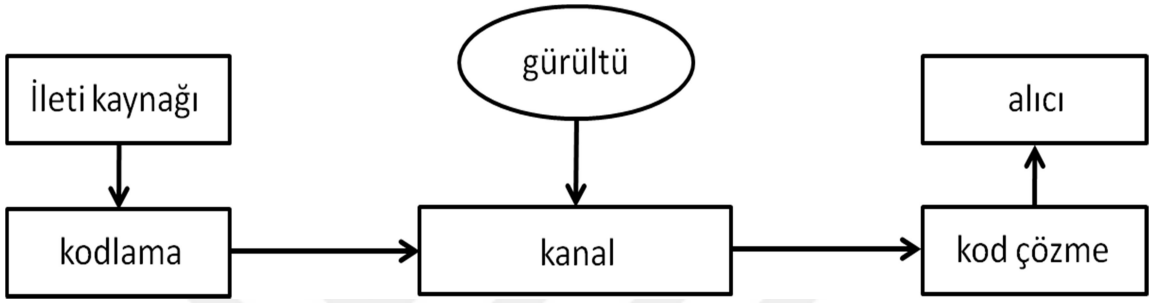
1. GİRİŞ

1996 yılında Pathfinger adında NASA'ya ait olan ve Mars'ı araştırmak için gönderilen bir robottan dünyaya çok sayıda bilimsel veri ve fotoğraf aktarılmıştır. Loş bir ampulü yakacak kadar güç ile aktif olan radyo vericisine sahip bir araçtan, milyonlarca kilometre uzaklıktan güvenli ve orijinal bilgiler almak nasıl mümkün olmuştur? Elektronik mühendisliği, bilgisayar mühendisliği ve matematiğin disiplinler arası birleşimi olan kodlama kuramı ile olmuştur.

Claude Shannon tarafından yazılan ve 1948 yılında yayımlanan "İletişimin Matematiksel Modellemesi" adlı çalışma, daha önce bazı temel fikirleri anlaşılmış olan bilişim kuramının sağlam temeller üzerine kurulmasını ve popüler hale gelmesini sağlamıştır (Shannon, 1948). C. Shannon'un çalışmasında gürültülü bir kanalda, özel kod çözme teknikleri kullanılırsa, kanal kapasitesi altındaki herhangi bir oranda güvenli iletişimin sağlanabileceği açıklanmıştır. Ama Shannon ve diğerlerinin verdiği kanıtlar yeterli olmamış, Shannon'un bahsettiği bir kodlama oluşturma yöntemi bulunamamıştır. Başlangıç kabul edilen bu teoriden sonra kodlama teorisinde yani hata düzeltici kodlar teorisinde, gürültü kanalları boyunca kodlanmış verilerin iletimi ve bozulan mesajı düzeltme gibi konularla ilgilenilmiş; doğru, iletim seviyesi yüksek, zaman ve enerji tasarrufu sağlayan kodlama yöntemlerini geliştirme amaç edinilmiştir (Hill, 1986). İlk olarak 1958 yılında tek hata düzeltici kodlar Hamming tarafından bulunmuştur. Alınan mesajın gönderilen mesaja yakın hatta aynı olacak şekilde belirleyebilmek için mesaja fazladan veri eklenerek ve bu eklemelerin zaman ve maliyet açısından düşük tutmaya çalışılarak mesajdaki güvenirliliği arttırmak hedeflenmiştir.

Kodlama teorisi, gürültülü bir kanalda veri gönderilmesi ve bu esnada bozulan verilerin düzeltilmesi ile ilgilenmektedir. Bilginin daha basit okunabilir olmasıyla ilgilenen bu alan, daha zor okunmasını sağlamayı amaçlayan, şifreleme (cryptography) ile karıştırılmamalıdır. Burada verilen ileti ve kanal kelimeleri ile içerebilecekleri en geniş anlamlar kastedilmektedir. İletiler konuşma dili yahut yazı dili olabileceği gibi resim, müzik gibi yapılar da olabilir. Verilerin aktarılması ile istenen başka bir yere gönderilmesi (yani haberleşme) olabilecegi gibi şimdiden sonraya gönderilmesi de (yani saklama da) olabilir. Buna göre söz konusu kanal uzay, telefon hattı vb. bir ortam olabilecegi gibi veri depolamada zaman kavramı veya verilerin depolanmasında kullanılan ortamlar da (örneğin kompakt disk yüzeyi) kanal olarak düşünülebilir. Düşünülürse

yukarıda örnekleri verilen kanalların hiçbiri veri aktarımı konusunda mükemmel değildir. Uzayda ve atmosferde oluşabilecek manyetik alanlar radyo dalgalarına, olumsuz hava koşulları telefon telleri üzerinden aktarılan sinyalleri, bir kompakt disk üzerinde bulunan çizikler ve lekeler disk üzerindeki bilgileri bozabilmektedir. Örnekleri çoğaltılabilecek bunun gibi olumsuzluklara sahip kanallara gürültülü kanal denir. Gürültülere rağmen verilerin gönderiminde oluşabilecek hataların sezilmesi ve hatta düzeltilmesi, kodlama kuramının temel problemlerini oluşturmaktadır.



Şekil 1.1. Dijital haberleşme sistemi

İletişimde hedef, kaynaktan iletilen mesajı doğruluğu yüksek bir olasılıkla alıcıya ulaştırmaktır. Mesajı göndermek için alfabe olarak sonlu kümeler kullanılır. İletilecek mesaj, hatalardan korunmak için kodlanır. Kodlanan mesaj, kod sözcükleridir. Kod sözcüğü kanala gönderilir. Kanal bir telefon hattı ya da yüksek frekanslı radyo bağlantısı olabilir. Donanım eksikliği, insan hatası veya yıldırım nedeniyle mesajın iletimi sırasında bazı hatalar olmuş olabilir. Kod çözücü, hatanın var olup olmadığını inceler, hata varsa düzeltir ve orijinal halini alıcıya gönderir.

Bu alanda yapılan ilk çalışmalar sonlu cisimler üzerinde tanımlı lineer kodlardır. Daha sonra Hamming kodlar, BCH kodlar, Golay kodlar gibi bazı önemli kodlar elde edilmiştir. 1970 yılının başından itibaren halkalar üzerinde tanımlı kodlar çalışılmaya başlanmıştır. 1994 yılında Hammons vd. tarafından lineer olmayan fakat iyi bir takım kod ailelerinin $\mathbb{Z}_4$ üzerinde tanımlı lineer kodların Gray dönüşümü altındaki görüntüsü olarak elde edilmesinden sonra kodlama teorisindeki araştırmaların büyük bir çoğunluğu halkalar üzerinde tanımlanmaya başlanmıştır (Hammons vd,1994). Lineer bir kod, sonlu halkalar üzerinde tanımlı ise alt modüle, sonlu cisimler üzerinde tanımlı ise alt vektör uzayına karşılık gelmektedir. Ayrıca bir kod, minimum uzaklık (d), eleman sayısı (M) ve uzunluk (n) olmak üzere üç parametre ile ifade edilir.

İdeal bir kodun sahip olması gereken özellikler; hızlı transfer edilmesi, fazla sayıda mesaj gönderebilmesi yani fazla sayıda kod kelimesi içermesi ve aynı anda fazla sayıda hata düzeltmesi yani kod kelimelerinin birbirinden oldukça farklı olması gerekmektedir. Minimum uzaklığı büyük kodlar daha fazla hata düzelteceğinden minimum uzaklıkları büyük kodlar elde edilmesi önemlidir. Bununla ilgili pek çok yöntem vardır. Bu yöntemlerden bir tanesi sonlu halkalar ve sonlu cisimler üzerinde tanımlı MacDonald kodlardır.

$\mathbb{F}_2$ üzerindeki MacDonald kodlar, ilk olarak J. MacDonald tarafından 1960 yılında ortaya atılmıştır (MacDonald, 1960). $q \geq 2$ olmak üzere $\mathbb{F}_q$ üzerindeki MacDonald kodlar A. Patel tarafından 1975 yılında çalışılmıştır (Patel, 1975). C. J. Colbourn ve M. Gupta, $\mathbb{Z}_4$ üzerindeki α tipi ve β tipi Simplex kodlar yardımıyla $\mathbb{Z}_4$ üzerinde MacDonald kodları tanmlamıştır (Colbourn ve Gupta, 2003). Mohammed Al Ashker $u^2 = 0$ olmak üzere $\mathbb{F}_2[u]/\langle u^2 \rangle$ üzerindeki MacDonald kodları elde etmiştir. Çalışmasında, bu kodların Gray dönüşümü altındaki görüntüsü, Torsion kodu ve ağırlık dağılımlarına değinmiştir. Benzer şekilde $u^3 = 0$ olmak üzere $\mathbb{F}_2[u]/ < u^3 >$ halkası üzerinde MacDonald kodlar çalışılmıştır (Al Ashker, 2010). $u^2 = 0$ olmak üzere $\mathbb{F}_2 + u\mathbb{F}_2$ halkası üzerinde Simplex kodlar Mohammed Al Ashker tarafından oluşturulmuş ve bu kodların bazı özellikleri incelenmiştir (Al Ashker, 2005). $v^2 = v$ olmak üzere $\mathbb{F}_2 + v\mathbb{F}_2$ halkası üzerinde A. Dertli ve Y. Çengellenmiş tarafından MacDonald kodlar çalışılmıştır (Dertli ve Çengellenmiş, 2011). $v^2 = 1$ olmak üzere $\mathbb{F}_3 + v\mathbb{F}_3$ halkası üzerinde Simplex kodlar Y. Çengellenmiş tarafından oluşturulmuş daha sonra bu çalışma yardımıyla $\mathbb{F}_3 + v\mathbb{F}_3$ halkası üzerinde, $v^2 = 1$ olmak şartıyla MacDonald kodlar Y. Çengellenmiş ve M. Al-Ashker tarafından yapılmıştır (Çengellenmiş ve Al-Ashker, 2012).

Bu tezde, birinci bölümünde; kodlama teorisi, Simplex kodlar ve MacDonald kodlar hakkında yapılan çalışmalardan bahsedilmiştir. İkinci bölümde; cebirsel ifadeler, kodlama teorisi ile ilgili kavramlar ve teoremler verilmiştir. Materyal bölümünde; $u^2 = 0$ olmak üzere $\mathbb{F}_2 + u\mathbb{F}_2$, $u^3 = 0$ olmak üzere $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$, $v^2 = 1$ olmak üzere $\mathbb{F}_3 + v\mathbb{F}_3$ sonlu değişmeli halkalarının cebirsel yapıları incelenmiş ve bu halkalar üzerinde Gray dönüşümü tanımlanarak ağırlık kavramları elde edilmiştir. Böylelikle bu halkalarda tanımlanan Simplex kodların üreteç matrisleri yardımıyla MacDonald kodlar oluşturulmuş ve özellikleri incelenmiştir. Bulgular bölümünün birinci kısmında, $u^2 = u, v^2 = v, uv = vu = 0$ olmak üzere $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2$ sonlu ve değişmeli halkası üzerinde bir Gray dönüşümü tanımlanarak Hamming, Lee ve Bachoc ağırlıkları elde edilmiştir. Bu halka üzerinde MacDonald kodlar

inşa edilerek ağırlık dağılımları ve parametreler belirlenmiştir. Bulgular bölümünün ikinci kısmında, $u^2 = 0, v^2 = 0, uv = vu = 0$ olmak üzere $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2$ sonlu ve değişmeli halkası tanıtılarak bu halka üzerinde Gray dönüşümü tanımlanmıştır. Bu halka üzerindeki Simplex kodların üreteç matrisleri yardımıyla MacDonald kodlar inşa edilmiş ve Lee ağırlık dağılımları belirlenmiştir.

2. GENEL BİLGİLER

Tanım 2.1. $H \neq \emptyset$ bir küme ve " $\diamond$ ", H üzerinde bir ikili işlem olmak üzere

i) Her $f, g, h \in H$ için $f \diamond (g \diamond h) = (f \diamond g) \diamond h$,

ii) En az bir $e \in H$ vardır öyle ki her $f \in H$ için $f \diamond e = e \diamond f = f$ dir,

iii) Her $f \in H$ için $f \diamond b^{-1} = b^{-1} \diamond f = e$ olacak şekilde $\exists\, b^{-1} \in H$ vardır.

koşulları sağlanıyorsa $(H,\diamond)$ cebirsel yapısına grup denir (Çallıalp, 2013).

Tanım 2.2. $(H,\diamond)$ bir grup olsun. Her $f_1, f_2 \in H$ için $f_1 \diamond f_2 = f_2 \diamond f_1$ oluyorsa H grubuna değişmeli grup veya Abel grubu denir (Çallıalp, 2013).

Tanım 2.3. $K \neq \emptyset$ bir küme, " $+$ " ve " $\cdot$ ", K üzerinde ikili işlemler olmak üzere

i) $(K, +)$ bir değişmeli grup,

ii) Her $p_1, p_2, p_3 \in K$ için $p_1 \cdot (p_2 \cdot p_3) = (p_1 \cdot p_2) \cdot p_3$,

iii) Her $p_1, p_2, p_3 \in K$ için $p_1 \cdot (p_2 + p_3) = p_1 \cdot p_2 + p_1 \cdot p_3$ ve $(p_1 + p_2) \cdot p_3 = p_1 \cdot p_3 + p_2 \cdot p_3$,

koşulları sağlanıyorsa $(K, +, \cdot)$ cebirsel yapısına bir halka denir (Hungerford, 1973).

Tanım 2.4. $(K, +, \cdot)$ bir halka olsun. K halkasının " $+$ " işlemine göre birimine halkanın sıfırı denir ve 0 ile gösterilir. K halkası " $\cdot$ " işlemine göre birim elemana sahipse $(K, +, \cdot)$ halkasına birimli halka denir ve halkanın birimi 1 ile gösterilir (Hungerford, 1973).

Eleman sayısı sonlu olan halkaya sonlu halka denir ve K sonlu bir halka olmak üzere K halkasının eleman sayısı $|K|$ ile gösterilir.

Tanım 2.5. K birimli bir halka olsun. K halkasında tersi mevcut elemanlara birimsel eleman denir (Hungerford, 1973).

Tanım 2.6. $(K, +, \cdot)$ bir halka olsun. Her $p_1, p_2 \in K$ için $p_1 \cdot p_2 = p_2 \cdot p_1$ oluyorsa $(K, +, \cdot)$ halkasına değişmeli halka denir (Hungerford, 1973).

Tanım 2.7. K bir halka, $L \subseteq K$ olsun. L, K daki işlemlere göre bir halka ise L ye K nın bir alt halkası denir (Çallıalp, 1995).

Tanım 2.8. K nın sıfırdan farklı m ve n elemanları için $mn = 0$ oluyorsa, m ve n ye K nın sıfır bölenleri denir. Eğer her $m, n \in K$ için ve $mn = 0$ iken $m = 0$ veya $n = 0$ ise K ya sıfır bölensiz halka denir (Çallıalp, 1995).

Teorem 2.9. $\mathbb{Z}_n$ halkasının sıfır bölenleri n ile aralarında asal olmayan elemanlardır (Çallıalp, 1995).

Tanım 2.10. K bir halka ve $\emptyset \neq I \subset K$ olsun.

i) Her $p_1, p_2 \in I$ için $p_1 - p_2 \in I$ ve

ii) Her $p_1 \in I$ ve her $t \in K$ için $tp_1 \in I$ ($p_1 t \in I$)

koşulları sağlanıyorsa I ya K nın bir sol (sağ) ideali denir (Hungerford, 1973).

Hem sol, hem de sağ ideale iki taraflı ideal veya kısaca ideal denir. $\{0\}$ ve K ideallerine K halkasının aşikar idealleri denir. K halkasının bu ideallerden farklı ideallerine de öz idealleri denir.

Tanım 2.11. D, K halkasının bir alt kümesi olsun. K nın D kümesini kapsayan bütün ideallerinin arakesitine D kümesinin ürettiği ideal denir ve $< D >$ ile gösterilir. $D = \{d\}$ tek elemanlı bir küme ise D nin ürettiği ideale temel ideal denir ve $< d >$ ile gösterilir (Hungerford, 1973).

Tanım 2.12. K bir halka olmak üzere her $t \in K$ için $nt = 0$ eşitliğini sağlayan en küçük pozitif n tam sayısına K halkasının karakteristiği denir. Böyle bir n tam sayısı yoksa halkanın karakteristiği sıfırdır denir (Hungerford, 1973).

Tanım 2.13. K değişmeli, birimli bir halka ve M de K nın $< 1 >$ den farklı bir ideali olmak üzere K halkasınınn M idealini kapsayan M ve K dan başka hiçbir ideali yoksa, M idealine K halkasının bir maksimal ideali denir (Hungerford, 1973).

Tanım 2.14. Tek bir maksimal ideali olan halkaya lokal (yerel) halka denir. Birden fazla maksimal ideali olan halkaya ise yarı lokal (semi local) halka denir (Jitman vd, 2012).

Tanım 2.15. K birimli, değişmeli ve sonlu bir halka olsun. $j \in I = \{0,1,2, \dots, e-1\}$ ve B_j, K halkasının idealleri olmak üzere

$$< 0 >= B_0 \subsetneq B_1 \subsetneq B_2 \subsetneq \cdots \subsetneq B_{e-1} \subsetneq < 1 >= K$$

oluyorsa K halkasına sonlu zincir halkası denir (Jitman vd, 2012).

Tanım 2.16. T bir halka, x bir bilinmeyen ve $b_0, b_1, \ldots, b_n$ ler T nin elemanları olmak üzere $\{b_0 + b_1x + \cdots + b_nx^n\}$ şeklindeki bir ifadeye T den katsayılı tüm polinomların kümesi denir ve $T[x]$ ile gösterilir (Hungerford, 1973).

Önerme 2.17. T bir halka ise $T[x]$ de bir halkadır (Hungerford, 1973).

Önerme 2.18. S bir cisim ve $s(x) \in S[x]$, $der\big(s(x)\big) \geq 1$ olsun. $< s(x) >= s(x)S[x]$ temel ideali için $S[x]/< s(x) >$ bölüm halkasının tam temsilciler sistemi $der\big(t(x)\big) < der\big(s(x)\big)$ olan $t(x) \in S[x]$ polinomları şeklinde alınabilir (Çallıalp, 1995).

Tanım 2.19. T bir halka ve $(M, +)$ değişmeli grup olmak üzere her $t_1 \in T$ ve her $m_1 \in M$ için

$$h: T \times M \to M$$

$$h(t_1, m_1) = t_1m_1$$

şeklinde gösterilen ve aşağıdaki özellikleri sağlayan bir h fonksiyonu varsa M değişmeli grubuna bir sol T-modül denir. Her $t_1, t_2 \in T$ ve her $m_1, m_2 \in M$ için

i) $t_1(m_1 + m_2) = t_1m_1 + t_1m_2$,

ii) $(t_1 + t_2)m_1 = t_1m_1 + t_2m_1$,

iii) $(t_1t_2)m_1 = t_1(t_2m_1)$.

Aynı şekilde sağ T-modül tanımı da tanımlanabilir. T değişmeli bir halka ise M ye T-modül denir (Taşcı, 2007).

Tanım 2.20. M bir T- modül ve $B \subseteq M$ olmak üzere B, M ve T deki işlemlere göre bir T-modül ise B ye M nin bir sol alt modülü denir (Taşcı, 2007).

Teorem 2.21. M bir T-modül ve $B \subseteq M$ olmak üzere B nin alt modül olması için gerek ve yeter şart her $b_1, b_2 \in B$ için $b_1 - b_2 \in B$ ve her $t_1 \in T$, her $b_1 \in B$ için $t_1b_1 \in B$ olmasıdır (Taşcı, 2007).

Tanım 2.22. M bir sol T-modül ve $i = 1,2,\dots,n$ olmak üzere $x_i \in M$ olsun. $D = \{x_1, x_2, \dots, x_n\}$ kümesi,

i) D kümesi M yi gerer. Yani her $x \in M$ için $x = b_2x_2 + \cdots + b_nx_n$ olacak şekilde $b_1, b_2, \dots, b_n \in T$ vardır.

ii) D kümesi lineer bağımsızdır. Yani her $b_1, b_2, \dots, b_n \in T$ için $bx_1 + b_2x_2 + \cdots + b_nx_n = 0$ olması için gerek ve yeter koşul $b_1 = b_2 = \cdots = b_n = 0$ olmasıdır.

koşullarını sağlıyorsa D kümesine sol T- modül M için bir baz denir (Taşcı, 2007).

Tanım 2.23. $(T, +, \cdot)$ birimli ve değişmeli bir halka olsun. $T - \{0\} = T^*$ olmak üzere $(T^*, \cdot)$ bir grup ise T halkasına cisim denir (Çallıalp, 2013).

Tanım 2.24. Bir cismin elemanları sonlu ise bu cisme sonlu cisim denir (Roman, 1992).

Teorem 2.25. $1 < q \in \mathbb{Z}$ olmak üzere q elemanlı bir cismin var olması için gerek ve yeter şart q sayısının bir asalın kuvvveti şeklinde yazılmasıdır (Roman, 1992).

Tanım 2.26. p bir asal sayı, $n \in \mathbb{N}$ olmak üzere $q = p^n$ elemanlı cisme Galois cismi denir ve $GF(q)$ (veya $\mathbb{F}_q$) şeklinde gösterilir (Roman, 1992).

Tanım 2.27: $(V, \oplus)$ değişmeli bir grup, $(S, +, .)$ bir cisim olmak üzere

$$\odot : SxV \to V$$

$$(a_1, v_1) \to a_1 \odot v_1$$

dış işlemi aşağıdaki özellikleri sağlıyorsa, V ye $(S, +, .)$ cismi üzerinde vektör uzayı denir (Çallıalp ve Kuruoğlu, 1996).

i) Her $a_1 \in S$ ve her $v_1, v_2 \in V$ için $a_1 \odot (v_1 \oplus v_2) = (a_1 \odot v_1) \oplus (a_1 \odot v_2)$ dir.

ii) Her $a_1, a_2 \in S$ ve her $v_1 \in V$ için $(a_1 + a_2) \odot v_1 = (a_1 \odot v_1) \oplus (a_2 \odot v_1)$ dir.

iii) Her $a_1, a_2 \in S$ ve her $v_1 \in V$ için $(a_1.a_2) \odot v_1 = a_1 \odot (a_2 \odot v_1)$ dir.

iv) $1 \in S$ ve her $v_1 \in V$ için $1 \odot v_1 = v_1$ dir.

Tanım 2.28. V bir vektör uzayı ve $\emptyset \neq V_1 \subseteq V$ alt kümesi olsun. V_1, V deki işlemlere göre bir vektör uzayı ise V_1 e V vektör uzayının bir alt uzayı denir (Çallıalp ve Kuruoğlu, 1996).

Teorem 2.29. V, S cismi üzerinde bir vektör uzayı olsun. $\emptyset \neq V_1 \subseteq V$ kümesinin V nin bir alt uzayı olması için gerek ve yeter şart her $v_1, v_2 \in V_1$ ve her $l_1, l_2 \in S$ için $(l_1 \odot v_1) \oplus (l_2 \odot v_2) \in V_1$ olmasıdır (Çallıalp ve Kuruoğlu, 1996).

Tanım 2.30. V, S cismi üzerinde bir vektör uzayı ve $v_1, v_2, \dots, v_n$, V nin farklı vektörleri olsun. Eğer $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = 0$ iken $\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$ ise $v_1, v_2, \dots, v_n$ vektörleri lineer bağımsızdır, aksi halde bu vektörler lineer bağımlıdır denir (Ling ve Xing, 2004).

Tanım 2.31. V, S cisminde bir vektör uzayı ve $v_1, v_2, \dots, v_n \in V$ olsun. Her $v \in V$ için $v = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$ olacak şekilde $\alpha_1, \alpha_2, \dots, \alpha_n \in S$ varsa $v_1, v_2, \dots, v_n$ vektörleri V yi üretiyor (geriyor) denir (Ling ve Xing, 2004).

Tanım 2.32. V, S cismi üzerinde bir vektör uzayı ve $v_1, v_2, \dots, v_n \in V$ olmak üzere $v_1, v_2, \dots, v_n$ vektörleri lineer bağımsız ve V vektör uzayını geriyorsa $\{v_1, v_2, \dots, v_n\}$ kümesine V nin bir tabanı (bazı) denir. V nin tabanındaki eleman sayısına V nin boyutu denir ve $boy(V)$ ile gösterilir (Ling ve Xing, 2004).

Tanım 2.33. $F = \{f_1, f_2, \dots, f_q\}$, q elemanlı küme olsun.

i) Her $j \in \{1,2, \dots, n\}$ için $v_j \in F$ olmak üzere $v = v_1 v_2 v_3 \dots v_n$ elemanına F üzerinde tanımlı n uzunluğunda bir q-ary (q-lu) sözcük denir. Aynı zamanda v, $v = (v_1, v_2, v_3, \dots, v_n)$ şeklinde bir vektör olarak düşünülebilir.

ii) $\emptyset \neq \mathcal{C} \subseteq F^n$ kümesine, F üzerinde tanımlı n uzunluğunda bir q-lu blok kod denir.

iii) $\mathcal{C}$ kodundaki her bir elemana kod sözcüğü denir.

iv) $\mathcal{C}$ kodunun eleman sayısı $|\mathcal{C}|$ ile gösterilir.

v) $\emptyset \neq \mathcal{C} \subseteq F^n$ kümesinin M tane elemanı varsa $\mathcal{C}$ koduna n uzunluğunda M elemanlı bir kod denir ve (n, M) parametreleri ile gösterilir.

vi) F kümesine kod alfabesi ve F nin elemanlarına da kod sembolleri denir (Ling ve Xing, 2004).

Tanım 2.34. T sonlu bir halka ve $n \in \mathbb{Z}^+$ olmak üzere

$$T^n = \{(v_1, v_2, \dots, v_n) : v_j \in T, j = 1,2, \dots, n\}$$

T-modülünün M elemanlı bir $\mathcal{C}$ T-alt modülüne, n uzunluğunda ve M elemanlı bir lineer kod denir. Kodun elemanlarına kod sözcüğü, T^n nin elemanlarına da sözcük denir (Huffman ve Pless, 2003).

Tanım 2.35. $\mathbb{F}_q^n = \{a = (\mathfrak{f}_1, \mathfrak{f}_2, \dots, \mathfrak{f}_n) : \mathfrak{f}_i \in \mathbb{F}_q, i = 1,2, \dots, n\}$ kümesi $\mathbb{F}_q$ üzerinde n boyutlu bir vektör uzayı olmak üzere, $\mathbb{F}_q^n$ nin her $\mathcal{C}$ alt uzayına lineer kod denir. $\mathcal{C}$ nin boyutu k ise $\mathcal{C}$ ye $\mathbb{F}_q$ da bir lineer $[n, k]$-kod ya da kısaca $[n, k]$-kod denir (Hill, 1986).

Tanım 2.36. Her $\mathfrak{a} = (\mathfrak{a}_1, \mathfrak{a}_2, \dots, \mathfrak{a}_n), \mathfrak{b} = (\mathfrak{b}_1, \mathfrak{b}_2, \dots, \mathfrak{b}_n) \in \mathbb{F}_q^n$ için

$$d : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{N} \cup \{0\}$$

$$(\mathfrak{a}, \mathfrak{b}) \mapsto d(\mathfrak{a}, \mathfrak{b}) = |\{i : \mathfrak{a}_i \neq \mathfrak{b}_i\}|$$

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

Önerme 2.37. Hamming uzaklığı

i) $\forall \mathfrak{s}, \mathfrak{t} \in \mathbb{F}_q^n$ için $d(\mathfrak{s}, \mathfrak{t}) \geq 0$, $d(\mathfrak{s}, \mathfrak{t}) = 0 \Leftrightarrow \mathfrak{s} = \mathfrak{t}$

ii) $\forall \mathfrak{s}, \mathfrak{t} \in \mathbb{F}_q^n$ için $d(\mathfrak{s}, \mathfrak{t}) = d(\mathfrak{t}, \mathfrak{s})$

iii) $\forall \mathfrak{s}, \mathfrak{t}, \mathfrak{u} \in \mathbb{F}_q^n$ için $d(\mathfrak{s}, \mathfrak{t}) \leq d(\mathfrak{s}, \mathfrak{u}) + d(\mathfrak{u}, \mathfrak{t})$

özelliklerini sağlayan bir metriktir (Hill, 1986).

Tanım 2.38. Bir $\mathcal{C}$ kodunun minimum uzaklığı

$$d = d(\mathcal{C}) = min\{d(\mathfrak{s}, \mathfrak{t}) : \mathfrak{s} \neq \mathfrak{t}, \ \mathfrak{s}, \mathfrak{t} \in \mathcal{C}\}$$

biçiminde tanımlanır. n uzunluğunda, M elemanlı ve minimum uzaklığı d olan bir $\mathcal{C}$ koduna (n, M, d)-kod denir (Hill, 1986).

$\mathcal{C}$ $[n, k]$-kodunun d minimum uzaklığı da kullanılırsa $[n, k, d]$-kod şeklinde gösterilir.

Bir $\mathcal{C}$ $[n, k, d]$-kodunun eleman sayısı q^k dır.

Not 2.39. $\mathcal{C}$, bir $[n, k, d]$-kod ise $\mathcal{C}$, bir q-ary (n, q^k, d)-koddur.

$\mathcal{C}$, bir q-ary (n, q^k, d)-kod ise $\mathcal{C}$, bir $[n, k, d]$-kod olmayabilir.

Tanım 2.40. r, $\mathbb{F}_q^n$ vektör uzayının herhangi bir elemanı olsun. r nin sıfırdan farklı bileşenlerinin sayısına r elemanının Hamming ağırlığı denir. $w(r)$ ya da $w_H(r)$ ile gösterilir (Hill, 1986).

Bir $\mathcal{C}$ kodunun sıfırdan farklı tüm kod sözcüklerinin ağırlıklarının en küçüğüne $\mathcal{C}$ kodunun minimum Hamming ağırlığı denir ve $w(\mathcal{C})$ ya da $w_H(\mathcal{C})$ ile gösterilir.

Lemma 2.41. $\mathfrak{s}, \mathfrak{t} \in F_q^n$ vektör uzayının herhangi iki elemanı olmak üzere

$$d(\mathfrak{s}, \mathfrak{t}) = w(\mathfrak{s} - \mathfrak{t})$$

dir (Hill, 1990).

İspat: $\mathfrak{a} = (\mathfrak{a}_1, \mathfrak{a}_2, \dots, \mathfrak{a}_n), \mathfrak{b} = (\mathfrak{b}_1, \mathfrak{b}_2, \dots, \mathfrak{b}_n)$ ve $d(\mathfrak{a}, \mathfrak{b}) = n - j$ olsun. Bu durumda $\mathfrak{a}$ ve $\mathfrak{b}$ vektörlerinin j adet koordinatı ortaktır. Dolayısıyla $\mathfrak{a} - \mathfrak{b}$ vektöründe ortak olan koordinatlar sıfır ve diğer bütün koordinatlar sıfırdan farklı olacaktır. Bu da $w(\mathfrak{a} - \mathfrak{b}) = n - j$ olduğunu gösterir. Sonuç olarak $d(\mathfrak{a}, \mathfrak{b}) = w(\mathfrak{a} - \mathfrak{b})$ eşitliği elde edilir.

Teorem 2.42. Bir $\mathcal{C}$ lineer kodunun minimum ağırlığı ile minimum uzaklığı eşittir (Hill, 1990).

İspat: Bir $\mathcal{C}$ lineer kodunun minimum ağırlığı $w(\mathcal{C})$ ve minimum uzaklığı $d(\mathcal{C})$ ile gösterilsin. Buna göre $\exists\, \mathfrak{a}, \mathfrak{b} \in \mathcal{C}$ için $d(\mathcal{C}) = d(\mathfrak{a}, \mathfrak{b})$ dir. Lemma 2.41 den $d(\mathcal{C}) = w(\mathfrak{a} - \mathfrak{b})$ ve aynı zamanda $\mathfrak{a} - \mathfrak{b} \in \mathcal{C}$ olduğundan $w(\mathfrak{a} - \mathfrak{b}) \geq w(\mathcal{C})$ elde edilir. Yani $d(\mathcal{C}) \geq w(\mathcal{C})$ olur. Diğer yandan $\exists\, \mathfrak{a} \in \mathcal{C}$ için $w(\mathcal{C}) = w(\mathfrak{a}) = d(\mathfrak{a}, 0) \geq d(\mathcal{C})$ elde edilir. Dolayısıyla $d(\mathcal{C}) \geq w(\mathcal{C})$ ve $w(\mathcal{C}) \geq d(\mathcal{C})$ olduğundan $d(\mathcal{C}) = w(\mathcal{C})$ dir.

Örnek 2.43. $\mathcal{C} = \{(0,1,2,1), (1,0,2,2), (1,2,0,1)\}$, $\mathbb{F}_3$ üzerinde lineer olmayan bir kod olmak üzere

$$d\big((0,1,2,1), (1,0,2,2)\big) = 3$$

$$d\big((0,1,2,1), (1,2,0,1)\big) = 3$$

$$d\big((1,0,2,2), (1,2,0,1)\big) = 3$$

dir. $d(\mathcal{C}) = min\{d(\mathfrak{s}, \mathfrak{t}) : \mathfrak{s} \neq \mathfrak{t},\ \mathfrak{s}, \mathfrak{t} \in \mathcal{C}\}$ olduğundan $d = 3$ dir. O halde $\mathcal{C}$ kodu (4,3,3)-koddur.

Tanım 2.44. $\mathcal{C}$, $\mathbb{F}_q$ üzerinde bir $[n, k]$-kod olsun. Satırları $\mathcal{C}$ lineer kodununun taban elemanlarından oluşan $k \times n$ mertebeli matrise $\mathcal{C}$ kodunun üreteç matrisi denir ve G ile

gösterilir. G, I_k, $k \times k$ mertebeli birim matris, A, $k \times (n-k)$ mertebeli bir matris olmak üzere $(I_k \mid A)$ şeklinde düzenlenirse $(I_k \mid A)$ matrisine G matrisinin standart formu denir (Hill, 1986).

Örnek 2.45. $\mathbb{F}_2$ üzerinde

$$\mathcal{C} = \{(0,0,0,0,0), (0,0,1,1,1), (1,1,0,0,1), (1,1,1,1,0)\}$$

lineer kodunun bir tabanı

$$S = \{(0,0,1,1,1), (1,1,1,1,0)\}$$

olduğu için $G = \begin{bmatrix} 11110 \\ 00111 \end{bmatrix}_{2\times 5}$ matrisi, $\mathcal{C}$ kodunun üreteç matrisidir. $\mathcal{C}$ kodu $\mathbb{F}_2$ üzerinde bir $[5,2,3]$-koddur.

Teorem 2.46. $\mathcal{C}$, minimum uzaklığı d olan bir kod olmak üzere

i) $d \geq k+1$ ise $\mathcal{C}$ kodu k tane hatayı belirler.
ii) $d \geq 2t+1$ ise $\mathcal{C}$ kodu t tane hatayı düzeltir (Hill, 1986).

Sonuç 2.47. Minimum uzaklığı d olan bir $\mathcal{C}$ kodu herhangi bir kod sözcüğünde $d-1$ tane hatayı belirler ya da $\left\lfloor \frac{d-1}{2} \right\rfloor$ tane hatayı düzeltir (Ling ve Xing, 2004).

Teorem 2.48. C ve D, $k \times n$ lik matrisler olmak üzere C matrisine

i) Satırların yer değişimi
ii) Satırın bir sıfırdan farklı bir skaler ile çarpımı
iii) Satırın bir skalerle çarpımının bir diğer satır üzerine toplamı
iv) Sütunların yer değişimi
v) Sütunun sıfırdan farklı bir skaler ile çarpımı

ifadelerinden en az biri uygulanarak D matrisi elde ediliyorsa, C ve $D, \mathbb{F}_q$ da denk $[n,k]$-kodları üretir (Hill, 1986).

Tanım 2.49. Her $\mathfrak{y} = (\mathfrak{y}_1, \mathfrak{y}_2, \dots, \mathfrak{y}_n)$, $\mathfrak{z} = (\mathfrak{z}_1, \mathfrak{z}_2, \dots, \mathfrak{z}_n) \in \mathbb{F}_q^n$ elemanları için

$$\cdot : \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{F}_q$$

$$(\mathfrak{y}, \mathfrak{z}) \mapsto \mathfrak{y}.\mathfrak{z} = \mathfrak{y}_1\mathfrak{z}_1 + \cdots + \mathfrak{y}_n\mathfrak{z}_n$$

şekildeki dönüşüme bir iç çarpım denir. Eğer $\mathfrak{y}.\mathfrak{z} = 0$ ise $\mathfrak{y}$ ve $\mathfrak{z}$ birbirine diktir denir (Hill, 1986).

Tanım 2.50. $\mathcal{C}$, $\mathbb{F}_q$ üzerinde bir $[n,k]$-kod olmak üzere

$$\mathcal{C}^{\perp} = \{\mathfrak{y} \in \mathbb{F}_q^n : \mathfrak{y}.\mathfrak{z} = 0, \ \forall \mathfrak{z} \in \mathcal{C}\}$$

kümesine $\mathcal{C}$ kodunun duali denir. $\mathcal{C}^{\perp} = \mathcal{C}$ ise $\mathcal{C}$ koduna self-dual kod, $\mathcal{C} \subseteq \mathcal{C}^{\perp}$ ise $\mathcal{C}$ koduna self-ortogonal kod denir (Ling ve Xing, 2004).

Teorem 2.51. $\mathcal{C}$, $\mathbb{F}_q$ üzerinde bir $[n,k]$-kod olmak üzere

i) $|\mathcal{C}| = q^k$,

ii) $\mathcal{C}^{\perp}$ de bir lineer koddur ve boy($\mathcal{C}$)+boy($\mathcal{C}^{\perp}$)$= n$,

iii) $(\mathcal{C}^{\perp})^{\perp} = \mathcal{C}$

dir (Ling ve Xing, 2004).

Teorem 2.52. $\mathcal{C}$, $\mathbb{F}_q$ üzerinde bir $[n,k]$-kod,

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

$\mathcal{C}$ kodunun üreteç matrisi ve $\mathfrak{y} = (\mathfrak{y}_1, \mathfrak{y}_2, \ldots, \mathfrak{y}_n) \in \mathbb{F}_q^n$ olsun. $\mathfrak{y} \in \mathcal{C}^{\perp}$ olması için gerek ve yeter şart $[\mathfrak{y}_1 \ \mathfrak{y}_2 \ \ldots \mathfrak{y}_n]_{1\times n} G_{n\times k}^{\mathrm{T}} = 0$ olmasıdır (Hill, 1986).

Önerme 2.53. $\mathcal{C}$, $\mathbb{F}_q$ üzerinde bir $[n,k]$-kod ise $\mathcal{C}^{\perp}$ de $\mathbb{F}_q$ üzerinde bir $[n, n-k]$-koddur (Hill, 1986).

Tanım 2.54. $\mathcal{C}$ bir $[n,k]$-kod olsun. $\mathcal{C}^{\perp}$ nin üreteç matrisine $\mathcal{C}$ kodunun kontrol (parity-check) matrisi denir ve H ile gösterilir (Hill, 1986).

Teorem 2.55. $\mathcal{C}$, $\mathbb{F}_q$ üzerinde bir $[n,k]$-kod olmak üzere G ve H, $\mathcal{C}$ kodunun sırasıyla üreteç ve kontrol matrisleri ise $GH^T = 0$ dır (Hill, 1986).

Not 2.56. H, $\mathcal{C}$ kodunun kontrol matrisi olmak üzere

$$\mathcal{C} = \{(\mathfrak{y}_1, \mathfrak{y}_2, \dots, \mathfrak{y}_n) \in \mathbb{F}_q^n : [\mathfrak{y}_1\ \mathfrak{y}_2 \dots \mathfrak{y}_n]H^T = 0\}$$

şeklinde de ifade edilir (Hill, 1986).

Teorem 2.57. $\mathcal{C}$ bir lineer kod ve H, $\mathcal{C}$ kodunun kontrol matrisi olmak üzere

i) $d(\mathcal{C}) \geq d$ olması için gerek ve yeter şart H matrisinin herhangi $d-1$ sütunu lineer bağımsız olmasıdır.

ii) $d(\mathcal{C}) \leq d$ olması için gerek ve yeter şart H matrisinin herhangi d sütunu lineer bağımlı olmasıdır.

iii) $d(\mathcal{C}) = d$ olması için gerek ve yeter şart H matrisinin herhangi $d-1$ sütunu lineer bağımsız ve en az d tane sütunu lineer bağımlı olmasıdır (Ling ve Xing, 2004).

Teorem 2.58. $\mathcal{C}$ bir $[n,k]$-kod olmak üzere $\mathcal{C}$ nin üreteç matrisinin standart formu $G = (I_k \mid A)$ ise $\mathcal{C}$ kodunun kontrol matrisi $H = (-A^T \mid I_{n-k})$ dir (Hill, 1986).

Örnek 2.59. $\mathbb{F}_2$ üzerinde bir $\mathcal{C}$ [7,4,3]-kodunun üreteç matrisi

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

olmak üzere $\mathcal{C}$ kodunun üreteç matrisinin standart formu

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

dir. Bu durumda $\mathcal{C}$ kodunun kontrol matrisi

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

şeklindedir.

Tanım 2.60. $\mathcal{C}$ bir $[n,k]$-kod ve G, $\mathcal{C}$ kodunun üreteç matrisi olsun. Bir $u \in \mathbb{F}_q^k$ mesajı $uG = v$ olmak üzere $v \in \mathcal{C}$ olarak kodlanır. Bu kodlamaya u mesaj vektörünün v kod sözcüğü olarak

kodlanması denir. Buradaki $\boldsymbol{u}$, u vektörünün bileşenlerinden oluşan satır matrisidir (Hill, 1986).

Örnek 2.61. $\mathcal{C}$, $\mathbb{F}_2$ üzerinde bir [7,4]-kod ve $\mathcal{C}$ kodunun üreteç matrisi

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

olsun. Bir $u = (1,1,1,0) \in \mathbb{F}_2^4$ mesajı $\boldsymbol{u}G = [1110100]$ olduğundan $(1,1,1,0,1,0,0)$ olarak kodlanır.

3. MATERYAL VE YÖNTEM

Bu bölümde bazı sonlu ve değişmeli halkalar üzerinde MacDonald kodlarla ilgili yapılan çalışmalar verilmiştir. Torsion kod kavramı tanıtılarak ağırlık dağılımları incelenmiştir.

3.1. $\mathbb{F}_2 + u\mathbb{F}_2$ Halkası Üzerindeki MacDonald Kodlar

$\mathbb{F}_2[u]/\langle u^2\rangle = \{ a_0 + ua_1 + \langle u^2\rangle \mid a_0, a_1 \in \mathbb{F}_2\}$ halkası için $u^2 = 0$ olması durumunda $a_0 + ua_1 + \langle 0 \rangle = \{ a_0 + ua_1 + 0.b \mid a_0, a_1 \in \mathbb{F}_2, b \in \mathbb{F}_2[u] \} = \{a_0 + ua_1\}$ olacağından

$$\mathbb{F}_2[u]/\langle u^2\rangle = \{\{a_0 + ua_1\} \mid a_0, a_1 \in \mathbb{F}_2\}$$

bulunur. $R = \mathbb{F}_2 + u\mathbb{F}_2 = \{ a_0 + ua_1 \mid a_0, a_1 \in \mathbb{F}_2\}$ de bir halkadır (Al-Ashker, 2005).

Teorem 3.1.1. $u^2 = 0$, $R = \mathbb{F}_2 + u\mathbb{F}_2 = \{0,1,u,1+u\}$ olmak üzere aşağıdaki toplama ve çarpma işlemlerine göre 4 elemanlı değişmeli bir halkadır (Al-Ashker, 2005).

Çizelge 3.1. $\mathbb{F}_2 + u\mathbb{F}_2$ halkasının toplam ve çarpım tablosu

$+$	0	1	u	$1+u$
0	0	1	u	$1+u$
1	1	0	$1+u$	u
u	u	$1+u$	0	1
$1+u$	$1+u$	u	1	0

$.$	0	1	u	$1+u$
0	0	0	0	0
1	0	1	u	$1+u$
u	0	u	0	u
$1+u$	0	$1+u$	u	1

Teorem 3.1.2.

$$h: \mathbb{F}_2 + u\mathbb{F}_2 \longrightarrow \mathbb{F}_2[u]/\langle u^2\rangle$$
$$\mathfrak{h}_0 + u\mathfrak{h}_1 \mapsto h(\mathfrak{h}_0 + u\mathfrak{h}_1) = \{\mathfrak{h}_0 + u\mathfrak{h}_1\}$$

dönüşümü bir izomorfizmadır (Al-Ashker, 2005).

İspat: Tanımlanan h dönüşümü kapalı ve iyi tanımlıdır.

(1)

$\forall\, \mathfrak{z}_1 = \mathfrak{h}_1 + u\mathfrak{r}_1, \mathfrak{z}_2 = \mathfrak{h}_2 + u\mathfrak{r}_2 \in R$ için

$h(\mathfrak{z}_1) = h(\mathfrak{z}_2)$

$\Rightarrow \{\mathfrak{h}_1 + u\mathfrak{r}_1\} = \{\mathfrak{h}_2 + u\mathfrak{r}_2\}$

$\Rightarrow \{\mathfrak{h}_1 - \mathfrak{h}_2 + u(\mathfrak{r}_1 - \mathfrak{r}_2)\} = 0$

$\Rightarrow\ \mathfrak{h}_1 - \mathfrak{h}_2 = \mathfrak{r}_1 - \mathfrak{r}_2 = 0$

$\Rightarrow\ \mathfrak{h}_1 = \mathfrak{h}_2, \mathfrak{r}_1 = \mathfrak{r}_2$

$\Rightarrow \mathfrak{z}_1 = \mathfrak{z}_2$

elde edilir. O halde h bire birdir.

(2)

h bire bir ve $|R| = |\mathbb{F}_2[u]/\langle u^2\rangle| = 2^2 = 4$ olduğundan h örtendir.

(3)

$$h(\mathfrak{z}_1 + \mathfrak{z}_2) = h\big(\mathfrak{h}_1 + \mathfrak{h}_2 + u(\mathfrak{r}_1 + \mathfrak{r}_2)\big)$$
$$= \{\mathfrak{h}_1 + \mathfrak{h}_2 + u(\mathfrak{r}_1 + \mathfrak{r}_2)\}$$
$$= \{\mathfrak{h}_1 + u\mathfrak{r}_1\} + \{\mathfrak{h}_2 + u\mathfrak{r}_2\}$$
$$= h(\mathfrak{z}_1) + h(\mathfrak{z}_2)$$

$$h(\mathfrak{z}_1\mathfrak{z}_2) = h\big(\mathfrak{h}_1\mathfrak{h}_2 + u(\mathfrak{h}_1\mathfrak{r}_2 + \mathfrak{r}_1\mathfrak{h}_2)\big)$$
$$= \{\mathfrak{h}_1\mathfrak{h}_2 + u(\mathfrak{h}_1\mathfrak{r}_2 + \mathfrak{r}_1\mathfrak{h}_2)\}$$

$$h(\mathfrak{z}_1)h(\mathfrak{z}_2) = \{\mathfrak{h}_1 + u\mathfrak{r}_1\}\{\mathfrak{h}_2 + u\mathfrak{r}_2\}$$
$$= \{\mathfrak{h}_1\mathfrak{h}_2 + u(\mathfrak{h}_1\mathfrak{r}_2 + \mathfrak{r}_1\mathfrak{h}_2)\}$$
$$= h(\mathfrak{z}_1\mathfrak{z}_2)$$

bu durumda h homomorfizmadır.

h, 1-1, örten ve homomorfizma olduğundan bir izomorfizmadır. Bu durumda

$\mathbb{F}_2 + u\mathbb{F}_2 \coloneqq \mathbb{F}_2[u]/\langle u^2\rangle$

yazılır.

Tanım 3.1.3. ξ kod sözcüğünün Lee ağırlığı,

$$w_L(\xi_i) = \begin{cases} 0 & \xi_i = 0 \\ 1 & \xi_i = 1 \ \ ya \quad da \ \ \xi_i = 1+u \\ 2 & \xi_i = u \end{cases}$$

olmak üzere

$$w_L(\xi) = \sum_{i=1}^{n} w_L(\xi_i)$$

şeklinde tanımlanır (Al-Ashker, 2005).

Tanım 3.1.4. ξ kod sözcüğünün Euclidean ağırlığı,

$$w_E(\xi_i) = \begin{cases} 0 & \xi_i = 0 \\ 1 & \xi_i = 1 \ \ ya \quad da \ \ \xi_i = 1+u \\ 4 & \xi_i = u \end{cases}$$

olmak üzere

$$w_E(\xi) = \sum_{i=1}^{n} w_E(\xi_i)$$

şeklinde tanımlanır (Al-Ashker, 2005).

Teorem 3.1.5. $\xi \ \ ve \ \varsigma \in R^n$ olmak üzere ξ ve ς arasındaki Lee uzaklığı

$$d_L(\xi, \varsigma) = w_L(\xi - \varsigma) = \sum_{i=1}^{n} w_L(\xi_i - \varsigma_i)$$

dir (Betsumiya ve Harada, 2004).

Tanım 3.1.6. C kodunun minimum Lee uzaklığı ve minimum Euclidean uzaklığı sırasıyla

$$d_L = d_L(C) = \min\{d_L(u,v) : u \neq vu, v \in C\}$$

$$d_E = d_E(C) = \min\{d_E(u,v) : u \neq vu, v \in C\}$$

şeklinde tanımlanır (Al-Ashker, 2005).

Teorem 3.1.7. Bir lineer kodun minimum uzaklığı ve minimum ağırlığı eşittir (Roman, 1992).

Tanım 3.1.8. x ve y $\mathbb{F}_2$ nin herhangi iki elemanı olmak üzere

$$\phi: \mathbb{F}_2 + u\mathbb{F}_2 \longrightarrow \mathbb{F}_2^2$$
$$x + uy \mapsto \phi(x + uy) = (y, x + y)$$

şeklinde tanımlanan ϕ dönüşümüne Gray dönüşümü denir. Bu dönüşüm $(\mathbb{F}_2 + u\mathbb{F}_2)^n$ den $\mathbb{F}_2^{2n}$ e genelleştirilebilir (Al-Ashker, 2005).

Teorem 3.1.9. $\phi: ((\mathbb{F}_2 + u\mathbb{F}_2)^n, d_L) \longrightarrow (\mathbb{F}_2^{2n}, d_H)$ şeklinde tanımlanan Gray dönüşümü uzaklık koruyan bir dönüşümdür (Al-Ashker, 2005).

İspat: $\forall\, \mathfrak{u}_1, \mathfrak{u}_2 \in (\mathbb{F}_2 + u\mathbb{F}_2)^n$ olsun. Bu durumda

$$\phi(\mathfrak{u}_1 - \mathfrak{u}_2) = \phi(\mathfrak{u}_1) - \phi(\mathfrak{u}_2)$$

dir.

$$\begin{aligned} d_L(\mathfrak{u}_1, \mathfrak{u}_2) &= w_L(\mathfrak{u}_1 - \mathfrak{u}_2) \\ &= w_H\big(\phi(\mathfrak{u}_1 - \mathfrak{u}_2)\big) \\ &= w_H\big(\phi(\mathfrak{u}_1) - \phi(\mathfrak{u}_2)\big) \\ &= d_H\big(\phi(\mathfrak{u}_1), \phi(\mathfrak{u}_2)\big) \end{aligned}$$

eşitliği elde edilir. O halde ϕ uzaklık koruyan bir dönüşümdür.

Böylece, $\mathcal{C} = (n, 4^{k_1}2^{k_2}, d_L)$, $\mathbb{F}_2 + u\mathbb{F}_2$ üzerinde bir lineer kod olmak üzere $\phi(\mathcal{C})$, $\mathbb{F}_2$ üzerinde bir $[2n, 2k_1 + k_2, d_H]$-koddur.

Teorem 3.1.10. $\mathcal{C}$, $\mathbb{F}_2 + u\mathbb{F}_2$ üzerindeki bir kod olsun. A ve B, $\mathbb{F}_2 + u\mathbb{F}_2$ üzerinde, D $\mathbb{F}_2$ üzerinde alınan matrisler olmak üzere, $\mathcal{C}$ kodu

$$G = \begin{bmatrix} I_{k_1} & A & B \\ 0 & uI_{k_2} & uD \end{bmatrix}$$

matrisi ile üretilen bir koda denktir (Dougherty vd, 1999).

3.1.1. $\mathbb{F}_2 + u\mathbb{F}_2$ halkasındaki MacDonald kodun özellikleri

α tipi Simplex S_k^α kodu, $v = 1 + u$ alındığında $G_1^\alpha = [0 \quad 1 \quad u \quad v]$ ve $k \geq 2$ için

$$G_k^\alpha = \begin{bmatrix} 0..0 & 1..1 & u..u & v..v \\ G_{k-1}^\alpha & G_{k-1}^\alpha & G_{k-1}^\alpha & G_{k-1}^\alpha \end{bmatrix}_{k \times 2^{2k}}$$

olmak üzere G_k^α üreteç matrisiyle üretilen bir lineer koddur.

Tanım 3.1.1.1. $[L \backslash M]$ matrisi, L matrisinden M matrisinin sütunlarının silinmesiyle elde edilen matristir (Al-Ashker, 2005).

Tanım 3.1.1.2. $1 \leq t \leq k-1$ olmak üzere G_k^α matrisinden G_t^α matrisinin sütunlarının ve $(k-t) \times 2^{2t}$ mertebeli **0** matrisinin silinmesiyle oluşturulan matrise $G_{k,t}^\alpha$ üreteç matrisi denir. Bu matris $G_{k,t}^\alpha = \left[G_k^\alpha \setminus \frac{0}{G_t^\alpha} \right]$ şeklindedir (Al-Ashker, 2005).

Tanım 3.1.1.3. α tipi S_k^α Simplex kodun G_k^α üreteç matrisiyle oluşturulan $G_{k,t}^\alpha$ üreteç matrisine sahip koda α tipi MacDonald kod denir. Bu kod $M_{k,t}^\alpha$ ile gösterilir. $M_{k,t}^\alpha$, $n = 2^{2k} - 2^{2t}$ uzunluğuna sahip bir koddur (Al-Ashker, 2005).

Tanım 3.1.1.4. $1 \leq j \leq n$ olmak üzere $\mathcal{C}$ kodunda Hamming ve Lee ağırlığı j olan kod sözcüklerinin sayısı sırasıyla $A_H(j)$, $A_L(j)$ ile gösterilsin.

$\{A_H(0), A_H(1), \ldots, A_H(n)\}$,

$\{A_L(0), A_L(1), \ldots, A_L(n)\}$

ifadelerine sırasıyla $\mathcal{C}$ kodunun Hamming ve Lee ağırlık dağılımı denir (Al-Ashker, 2005).

Tanım 3.1.1.5. $\mathcal{C}$, R üzerinde bir kod olmak üzere,

$$\mathcal{C}_1 = \{x \in \mathbb{F}_2^n : ux \in \mathcal{C}\}$$

kümesine $\mathcal{C}$ kodunun Torsion kodu,

$$\mathcal{C}_2 = \{x \in \mathbb{F}_2^n : \exists\, y \in \mathbb{F}_2^n : x + uy \in \mathcal{C}\}$$

kümesine C kodunun Rezidü kodu denir (Al-Ashker, 2005).

Lemma 3.1.1.6. $M_{k,t}^\alpha$ kodunun Torsion kodu $\mathbb{F}_2 + u\mathbb{F}_2$ üzerinde tanımlı bir lineer

$[2^{2k}\text{-}2^{2t}, k, 2^{2k-1}\text{-}2^{2t-1}]$-koddur (Al-Ashker, 2005). Bu kodun ağırlık dağılımları aşağıdaki gibidir:

$$A_H(0) = 1$$
$$A_H\left(2^{2k-1} - 2^{2t-1}\right) = 2^{k-t}(2^t - 1)$$
$$A_H\left(2^{2k-1}\right) = 2^{k-t} - 1$$

İspat: $M_{k,t}^{\alpha}$ nin Torsion kodu $u.G_{k,t}^{\alpha}$ matrisinde u elemanlarının yerine 1 yazılarak elde edilir. k ve t ye bağlı tümevarım ile ispatlanır.

$M_{k,t}^{\alpha}$ nin ilk k-t satırındaki birimsellerin adedi 2^{2k-1} ve birimsel olmayanları adedi 2^{2k-2} dir. Son t satırdaki birimsellerin adedi $2^{2k-1}\text{-}2^{2t-1}$ ve birimsel olmayanların adedi $2^{2k-2}\text{-}2^{2t-2}$ dir.

Lemma 3.1.1.7. $c \in M_{k,t}^{\alpha}, c \neq 0$ olsun. c nin en az bir bileşeni birimsel ise bu durumda 3 tip kod sözcüğü vardır (Al-Ashker, 2005).

$I. w_1(c) + w_v(c) = 2^{2k-1} - 2^{2t-1}$ ve $w_0(c) = w_u(c) = 2^{2k-2} - 2^{2t-2}$

$II. w_1(c) + w_v(c) = 2^{2k-1}$ ve $w_0(c) = 2^{2k-2} - 2^{2t}, w_u(c) = 2^{2k-}$

$III. w_1(c) + w_v(c) = 2^{2k-1}$ ve $w_0(c) = w_u(c) = 2^{2k-2} - 2^{2t-1}$

aksi taktirde

$I. w_0(c) = w_u(c) = 2^{2k-1} - 2^{2t-1}$

$II. w_0(c) = 2^{2k-1} - 2^{2t}$ ve $w_u(c) = 2^{2k-1}$

dir.

Teorem 3.1.1.8. $M_{k,t}^{\alpha}$ kodunun Hamming ve Lee ağırlık dağılımları aşağıdaki gibidir (Al-Ashker, 2005):

$$A_H(0) = 1$$

$$A_H\left(2^{2k-1} - 2^{2t-1}\right) = 2^{k-t}(2^t - 1)$$

$$A_H\left(2^{2k-1}\right) = \left(2^{k-t} - 1\right)$$

$$A_H\left(3.2^{2k-2}\right) = 2^{k-t}\left(2^{k-t} - 1\right)$$

$$A_H\left(3.\left(2^{2k-2}-2^{2t-2}\right)\right)=2^{2k-t}(2^t-1)$$

$$A_H\left(3.2^{2k-2}-2^{2t-1}\right)=2^{k-t}(2^t-1)\left(2^{k-t}-1\right)$$

$$A_L(0)=1$$

$$A_L\left(2^{2k}-2^{2t}\right)=2^{2k-2t}(2^{2t}-1)$$

$$A_L\left(2^{2k}\right)=\left(2^{2(k-t)}-1\right)$$

İspat: $M_{k,t}^{\alpha}$ kodunun sıfırdan farklı kod sözcüklerinin Hamming ağırlığı ya $2^{2k-1}-2^{2t-1}$, 2^{2k-1}, $3.\left(2^{2k-2}-2^{2t-2}\right)$, 3.2^{2k-2} ya da $3.2^{2k-2}-2^{2t-1}$ ve Lee ağırlığı ya $2^{2k}-2^{2t}$ ya da 2^{2k} dır.

Sonuç 3.1.1.9. $M_{k,t}^{\alpha}$ nin Gray dönüşümü altındaki görüntüsü $2^{2k}-2^{2t}$ ve 2^{2k} ağırlıklarına sahip $\mathbb{F}_2$ üzerinde $\left[2^{2k+1}-2^{2t+1},2^{2k},2^{2k}-2^{2t}\right]$-koddur (Al-Ashker, 2005).

3.2. $\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2$ Halkası Üzerinde Tanımlı MacDonald Kodlar

$$\mathbb{F}_2[u]/\langle u^3\rangle=\{a_0+ua_1+u^2a_2+\langle u^3\rangle : a_0,a_1,a_2\in\mathbb{F}_2\}$$

halkası için $u^3=0$ olması durumunda

$$a_0+ua_1+u^2a_2+\langle 0\rangle=\{a_0+ua_1+u^2a_2+0b :\ a_0,a_1,a_2\in\mathbb{F}_2, b\in\mathbb{F}_2[u]\}$$
$$=\{a_0+ua_1+u^2a_2\}$$

olacağından

$$\mathbb{F}_2[u]/\langle u^3\rangle=\left\{\{a_0+ua_1+u^2a_2\} : a_0,a_1,a_2\in\mathbb{F}_2\right\}$$

bulunur.

$$R_2=\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2=\left\{\{a_0+ua_1+u^2a_2\} : a_0,a_1,a_2\in\mathbb{F}_2\right\}$$

kümesi de bir halkadır (Al-Ashker, 2010).

Teorem 3.2.1. f: $\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2\longrightarrow\mathbb{F}_2[u]/\langle u^3\rangle$

$$a_0+ua_1+u^2a_2\ \longmapsto f(a_0+ua_1+u^2a_2)=\{a_0+ua_1+u^2a_2\}$$

dönüşümü bir izomorfizmadır (Al-Ashker, 2010).

İspat: Tanımlanan f dönüşümü kapalı ve iyi tanımlıdır.

(1)

$\forall\, y_1 = {a_0}^1 + u{a_1}^1 + u^2{a_2}^1, y_2 = {a_0}^2 + u{a_1}^2 + u^2{a_2}^2 \in R_2$ için

$f(y_1) = f(y_2)$

$\Rightarrow \{{a_0}^1 + u{a_1}^1 + u^2{a_2}^1\} = \left\{{a_0}^2 + u{a_1}^2 + u^2{a_2}^2\right\}$

$\Rightarrow \{a_0^1 - {a_0}^2 + u(a_1^1 - {a_1}^2) + u^2(a_2^1 - {a_2}^2)\} = 0$

$\Rightarrow a_0^1 - {a_0}^2 = a_1^1 - {a_1}^2 = a_2^1 - {a_2}^2 = 0$

$\Rightarrow a_0^1 = {a_0}^2, a_1^1 = {a_1}^2, a_2^1 = {a_2}^2,$

$\Rightarrow y_1 = y_2$

elde edilir. O halde f bire birdir.

(2)

f bire bir ve $|R_2| = |\mathbb{F}_2[u]/\langle u^3\rangle| = 2^3 = 8$ olduğundan f örtendir.

(3)

$$f(y_1 + y_2) = f(a_0^1 + {a_0}^2 + u(a_1^1 + {a_1}^2) + u^2(a_2^1 + {a_2}^2))$$

$$= \{a_0^1 + {a_0}^2 + u(a_1^1 + {a_1}^2) + u^2(a_2^1 + {a_2}^2)\}$$

$$= \{{a_0}^1 + u{a_1}^1 + u^2{a_2}^1\} + \left\{{a_0}^2 + u{a_1}^2 + u^2{a_2}^2\right\}$$

$$= f(y_1) + f(y_2)$$

$$f(y_1y_2) = f\begin{pmatrix}{a_0}^1{a_0}^2 + {a_1}^1{a_2}^2 + {a_2}^1{a_1}^2 + u({a_0}^1{a_1}^2 + {a_1}^1{a_0}^2 + {a_2}^1{a_2}^2) + \\ u^2({a_0}^1{a_2}^2 + {a_1}^1{a_1}^2 + {a_2}^1{a_0}^2)\end{pmatrix}$$

$$= \begin{Bmatrix}{a_0}^1{a_0}^2 + {a_1}^1{a_2}^2 + {a_2}^1{a_1}^2 + u({a_0}^1{a_1}^2 + {a_1}^1{a_0}^2 + {a_2}^1{a_2}^2) + \\ u^2({a_0}^1{a_2}^2 + {a_1}^1{a_1}^2 + {a_2}^1{a_0}^2)\end{Bmatrix}$$

$$f(y_1)f(y_2) = \{{a_0}^1 + u{a_1}^1 + u^2{a_2}^1\}\left\{{a_0}^2 + u{a_1}^2 + u^2{a_2}^2\right\}$$

$$= \begin{Bmatrix}{a_0}^1{a_0}^2 + {a_1}^1{a_2}^2 + {a_2}^1{a_1}^2 + u({a_0}^1{a_1}^2 + {a_1}^1{a_0}^2 + {a_2}^1{a_2}^2) + \\ u^2({a_0}^1{a_2}^2 + {a_1}^1{a_1}^2 + {a_2}^1{a_0}^2)\end{Bmatrix}$$

$$= f(y_1y_2)$$

bu durumda f homomorfizmadır.

f, 1-1, örten ve homomorfizma olduğundan bir izomorfizmadır. Bu durumda

$$\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 \coloneqq \mathbb{F}_2[u]/\langle u^3 \rangle$$

yazılır (Al-Ashker, 2010).

$R_2 = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$ halkası karakteristiği 2 olan, sekiz elemanlı sonlu değişmeli bir halkadır. R_2 halkasının maksimal ideali $uR_2 = \{0, u, u^2, uv\}$ dir (Al-Ashker, 2010).

Tanım 3.2.2. $\varsigma \in R_2$ nin Lee ağırlığı,

$$w_L(\varsigma) = \begin{cases} 0, & \varsigma = 0 \\ 1, & \varsigma = 1 \ ya \ da \ \varsigma = v^2 \\ 2, & \varsigma = u \ ya \ da \ \varsigma = uv \\ 3, & \varsigma = v \ ya \ da \ \varsigma = v^3 \\ 4, & \varsigma = u^2 \end{cases}$$

şeklindedir (Sadek vd, 2002).

Tanım 3.2.3. Her $m + un + u^2p \in R_2$ için

$$\theta_{GL}: R_2 \longrightarrow F_2^4$$
$$m + un + u^2p \longmapsto \theta(m + un + u^2p) = (p, m + p, n + p, m + n + p)$$

şeklinde tanımlanan θ dönüşümüne genelleştirilmiş Gray dönüşümü denir (Al-Ashker, 2010).

Teorem 3.2.4. $\theta_{GL}: ((R_2{}^n), d_{GL}) \longrightarrow (F_2^{4n}, d_H)$ şeklinde tanımlanan Gray dönüşümü uzaklık koruyan bir dönüşümdür. Böylece $\mathcal{C} = (n, 8^{k_0}4^{k_1}2^{k_2}, d_H)$ R_2 üzerinde bir lineer kod olmak üzere $\theta_{GL}(C)$, $\mathbb{F}_2$ üzerinde $[4n, 3k_0 + 2k_1 + k_2, d_L]$-koddur (Al-Ashker, 2010).

Tanım 3.2.5. $t \in R_2$ kod sözcüğünün Genelleştirilmiş Lee ağırlığı,

$$w_{GL}(t) = \begin{cases} 0, & t = 0 \\ 2, & t \neq u^2 \\ 4, & t = u^2 \end{cases}$$

şeklindedir (Al-Ashker, 2010).

Lemma 3.2.6. $\mathcal{C}$, R_2 üzerindeki bir kod olsun. B_{ij} binary matris $i > 0$ olmak üzere, $\mathcal{C}$ kodu

$$G = \begin{bmatrix} I_{k_0} & B_{01} & B_{02} & B_{03} \\ 0 & uI_{k_1} & uB_{12} & uB_{13} \\ 0 & 0 & u^2 I_{k_2} & u^2 B_{23} \end{bmatrix}$$

matrisi ile üretilen bir koda denktir (Al-Ashker, 2010).

3.2.1. $F_2 + uF_2 + u^2F_2$ halkasındaki MacDonald kodun özellikleri

α tipi simpleks S_k^α kodu, $v = 1 + u$ alındığında

$$G_1^\alpha = [0 \quad 1 \; u \quad v = 1 + u \;\; u^2 \quad v^2 = 1 + u^2 \quad v^3 = 1 + u + u^2 \quad uv = u + u^2]$$

ve $k \geq 2$ için

$$G_k^\alpha = \begin{bmatrix} 0..0 & 1..1 & u..u & \dots & v^3..v^3 \\ G_{k-1}^\alpha & G_{k-1}^\alpha & G_{k-1}^\alpha & \dots & G_{k-1}^\alpha \end{bmatrix}_{k \times 2^{3k}}$$

olmak üzere G_k^α matrisiyle üretilen bir lineer koddur. (Al-Ashker, 2010)

Tanım 3.2.1.1. (M\N) matrisi, M matrisinden N matrisinin sütunlarının silinmesiyle elde edilen matristir (Al-Ashker, 2010).

Tanım 3.2.1.2. $1 \leq t \leq k-1$ olmak üzere G_k^α matrisinden G_t^α matrisinin sütunlarının ve

$(k-t) \times 2^{3t}$ mertebeli **0** matrisinin silinmesiyle oluşturulan matrise $G_{k,t}^\alpha$ matrisi denir. Bu matris

$$G_{k,t}^\alpha = \left(G_k^\alpha \setminus \frac{0}{G_t^\alpha} \right)$$

şeklindedir (Al-Ashker, 2010).

Tanım 3.2.1.3. α tipi S_k^α Simplex kodun G_k^α üreteç matrisinden oluşturulan $G_{k,t}^\alpha$ üreteç matrisine sahip koda α tipi MacDonald kod denir. Bu kod $M_{k,t}^\alpha$ ile gösterilir. $M_{k,t}^\alpha$, $n = 2^{3k} - 2^{3t}$ uzunluğuna sahip bir koddur (Al-Ashker, 2010).

Tanım 3.2.1.4. $1 \leq t \leq n$ olmak üzere $\mathcal{C}$ kodunda Hamming ve Lee ağırlığı t olan kod sözcüklerinin sayısı sırasıyla $A_H(t)$, $A_L(t)$ ile gösterilsin.

$\{A_H(0), A_H(1), \ldots, A_H(n)\}$,

$\{A_L(0), A_L(1), \ldots, A_L(n)\}$

ifadelerine sırasıyla $\mathcal{C}$ kodunun Hamming ve Lee ağırlık dağılımı denir (Al-Ashker, 2010).

Tanım 3.2.1.5. $\mathcal{C}$, R_2 üzerinde bir kod olmak üzere,

$$\mathcal{C}_i = \{v \mid u^i v \in \mathcal{C}\}$$

kümesine $\mathcal{C}$ nin Torsion kodu denir (Dougherty ve Park, 2007).

Lemma 3.2.1.6. $M_{k,t}^{\alpha}$ kodunun Torsion kodu R_2 üzerinde bir lineer $[2^{3k}\text{-}2^{3t}, k, 2^{3k-1}\text{-}2^{3t-1}]$-koddur ve ağırlık dağılımları aşağıdaki gibidir:

$$A_H(0) = 1$$
$$A_H\left(2^{3k-1} - 2^{3t-1}\right) = 2^{k-t}(2^t - 1)$$
$$A_H\left(2^{3k-}\ \right) = 2^{k-t} - 1$$

$M_{k,t}^{\alpha}$ kodunun ilk k-t satırındaki birimsellerin adedi 2^{3k-1} ve birimsel olmayanların adedi 3.2^{3k-3} dir. Son t satırdaki birimsellerin adedi $2^{3k-1}\text{-}2^{3t-1}$ ve birimsel olmayanların adedi $3.(2^{3k-3}\text{-}2^{3t-3})$ dir (Al-Ashker, 2010).

Teorem 3.2.1.7. $M_{k,t}^{\alpha}$ kodunun Hamming ve Lee ağırlık dağılımları aşağıdaki gibidir (Al-Ashker, 2010):

$$A_H(0) = 1$$

$$A_H\left(2^{3k-1} - 2^{3t-1}\right) = 2^{k-1}(2^t - 1)$$

$$A_H\left(2^{3k-1}\right) = \left(2^{k-t} - 1\right)$$

$$A_H\left(3.2^{3k-2}\right) = 2^{k-t}\left(2^{k-t} - 1\right)$$

$$A_H\left(3.\left(2^{3k-2} - 2^{3t-2}\right)\right) = 2^{2k-t}(2^t - 1)$$

$$A_H\left(3.2^{2k-2} - 2^{2t-1}\right) = 2^{k-t}(2^t - 1)\left(2^{k-t} - 1\right)$$

$$A_H\left(7.2^{3k-3}\right) = 2^{2k-t}\left(2^{k-t} - 1\right)$$

$$A_H\left(7.\left(2^{3k-3}-2^{3t-3}\right)\right)=2^{3k-t}(2^t-1)$$

$$A_H\left(7.2^{3k-3}-2^{2t-1}\right)=2^{2k-t}-(2^t-1)\left(2^{k-t}-1\right)$$

$$A_L(0)=1$$

$$A_L\left(2^{3k+1}\right)=2^{3(k-t)}-1$$

$$A_L\left(2^{3k+1}-2^{3t+1}\right)=2^{3k-3t}(2^{3t}-1)$$

$$A_{GL}(0)=1$$

$$A_{GL}\left(2^{3k+1}\right)=2^{3(k-t)}-1$$

$$A_{GL}\left(2^{3k+1}-2^{3t+1}\right)=2^{3(k-t)}\left(2^{3k}-1\right)$$

3.3 $\mathbb{F}_3+v\mathbb{F}_3$ Halkası Üzerinde Tanımlı MacDonald Kodlar

$\mathbb{F}_3[v]/\langle v^2-1\rangle=\{a+vb+\langle v^2-1\rangle : a,b\in\mathbb{F}_3\}$

halkası için $v^2=1$ olması durumunda

$$a+vb+\langle v^2-1\rangle=\{a+vb+0c:\ a,b\in\mathbb{F}_3, c\in\mathbb{F}_3[v]\}$$

$$=\{a+vb\}$$

olacağından

$$\mathbb{F}_3[v]/\langle v^2-1\rangle=\left\{\{a+vb\}:a,b\in\mathbb{F}_3\right\}$$

bulunur.

$$R_3=\mathbb{F}_3+v\mathbb{F}_3=\left\{\{a+vb\}:a,b\in\mathbb{F}_3\right\}$$

kümesi de bir halkadır (Çengellenmiş ve Al-Ashker, 2012).

Teorem 3.3.1. f: $\mathbb{F}_3+v\mathbb{F}_3\longrightarrow\mathbb{F}_3[v]/\langle v^2-1\rangle$

$$a+vb\ \longmapsto f(a+vb)=\{a+vb\}$$

dönüşümü bir izomorfizmadır (Çengellenmiş ve Al-Ashker, 2012).

$v^2 = 1$ ve $\mathbb{F}_3 = \{0,1,2\}$ olmak üzere $R_3 = \mathbb{F}_3 + v\mathbb{F}_3 = \{0,1,2, v, 2v, a = 1 + v, b = 2 + v, c = 1 + 2v, d = 2 + 2v\}$ halkası 9 elemanlı sonlu, değişmeli bir halkadır. Bu halkanın $\{1,2, v, 2v\}$ elemanları birimseldir. R_3 halkasının 2 tane maksimal ideali vardır. Bu idealler

$m_1 =< b >=< v - 1 >=< v + 2 > = \{0, v + 2, 1 + 2v\}$,

$m_2 =< 1 + v >= \{0,1 + v, 2 + 2v\}$

dir (Chapman vd, 2002).

Tanım 3.3.2. $\xi_i \in R_3$ ün Lee ağırlığı,

$$w_L(\xi_i) = \begin{cases} 0, & \xi_i = 0 \\ 1, & \xi_i = 1,2,v,2v \\ 2, & \xi_i = 1+v, 2+v, 1+2v, 2+2v \end{cases}$$

şeklindedir (Çengellenmiş ve Al-Ashker, 2012).

Tanım 3.3.3. $\varsigma_i \in R_3$ ün Bachoc ağırlığı,

$$w_B(\varsigma_i) = \begin{cases} 0, & \varsigma_i = 0 \\ 1, & \varsigma_i = 1+v, 2+v, 1+2v, 2+2v \\ 3, & \varsigma_i = 1,2,v,2v \end{cases}$$

şeklindedir (Chapman vd, 2002).

Tanım 3.3.4. $\forall\, x + vy \in R_3$ için

$\sigma: R_3 \longrightarrow \mathbb{F}_3^2$

$x + vy \mapsto \theta(x + vy) = (x, y)$

şeklinde tanımlanan σ dönüşümüne Gray dönüşümü denir (Çengellenmiş ve Al-Ashker, 2012).

Lemma 3.3.5. C, R_3 üzerindeki bir kod olsun. A_i, B_i $\mathbb{F}_3$ üzerinde matrisler olmak üzere, $\mathcal{C}$ kodu

$$G = \begin{bmatrix} I_{k_1} & (1-v)A_1 & (1+v)B_1 & (1+v)B_2 + (1-v)A_2 & (1+v)B_3 + (1-v)A_3 \\ 0 & (1+v)I_{k_2} & 0 & (1+v)B_4 & 0 \\ 0 & 0 & (1-v)I_{k_3} & 0 & (1-v)A_4 \end{bmatrix}$$

matrisi ile üretilen bir koda denktir (Chapman vd, 2002).

3.3.1. $R_3 = \mathbb{F}_3 + v\mathbb{F}_3$ halkasındaki MacDonald kodun özellikleri

α tipi Simplex S_k^α kodu, $[3^{2k}, 2k, 6.3^{2k-2}, 4.3^{2k-1}, 2.3^{2k-1}]$-kod

$G_1^\alpha = [0 \quad 1 \; 2 \quad v \;\; 2v \quad a \quad b \;\; c \quad d]$

olmak üzere ve $k \geq 2$ için

$$G_k^\alpha = \begin{bmatrix} 0..0 & 1..1 & 2..2 & \dots & d..d \\ G_{k-1}^\alpha & G_{k-1}^\alpha & G_{k-1}^\alpha & \dots & G_{k-1}^\alpha \end{bmatrix}_{k \times 2^{3k}}$$

olmak üzere G_k^α matrisiyle üretilen bir lineer koddur (Çengellenmiş ve Al-Ashker, 2012).

MacDonald kod, Simplex kodun üreteç matrisi ile elde edilir.

$$G_{k,u}^\alpha = \left(G_k^\alpha \setminus \frac{0}{G_u^\alpha}\right)$$

olmak üzere $G_{k,u}^\alpha$ üreteç matrisi ile oluşturulan koda α tipi MacDonald kod denir. Bu kod $M_{k,u}^\alpha$ ile gösterilir. $M_{k,u}^\alpha$, $n = 3^{2k} - 3^{2u}$ uzunluklu, boyutu $2k_1 + k_2$ olan bir koddur (Çengellenmiş ve Al-Ashker, 2012).

Tanım 3.3.1.1. $\mathcal{C}$, R_2 üzerinde bir kod,

$H = (1+v)H^+ \oplus (1-v)H^-$

olmak üzere

$H^+ = \{s: \exists\, t \in {F_3}^n \,|(1+v)s + (1-v)t \in H\}$

$H^- = \{t: \exists\, s \in {F_3}^n \,|(1+v)s + (1-v)t \in H\}$

kümelerine $\mathcal{C}$ nin Torsion kodu denir (Çengellenmiş ve Al-Ashker, 2012).

Lemma 3.3.1.2. $M_{k,u}^\alpha$ kodunun Torsion kodu R_3 üzerinde tanımlı bir lineer $[3^{2k} - 3^{2u}, 2k_1 + k_2, \sum_{n=1}^{k-u} 6.8.3^{2u-2+(2n-2)}]$-koddur ve ağırlık dağılımları

$\mathrm{A_H}\,(0) = 1$

$\mathrm{A_H}\left(6.3^{2\mathrm{k}-2}\right) = 3^{\mathrm{k}-\mathrm{u}} - 1$

$\mathrm{A_H}\left(\sum_{n=1}^{k-u} 6.8.\,3^{2u-2+(2n-2)}\right) = 3^{\mathrm{k}-\mathrm{u}}(3^{\mathrm{u}} - 1)$

şeklindedir (Çengellenmiş ve Al-Ashker, 2012).

Lemma 3.3.1.3. $c \in \mathrm{M}_{\mathrm{k,t}}^{\alpha}, c \neq 0$ olmak üzere c nin en az bir bileşeni birimsel ise bu durumda 4 tip kod sözcüğü vardır (Çengellenmiş ve Al-Ashker, 2012).

$I. w_1(t) = w_2(t) = w_v(t) = w_{2v}(t) = w_a(t) = w_b(t) = w_c(t) = w_d(t) = 3^{2\mathrm{k}-2}$,
$w_0(t) = 3^{2\mathrm{k}-2} - 3^{2\mathrm{u}}$

$II. w_1(t) = w_2(t) = w_v(t) = w_{2v}(t) = w_b(t) = w_c(t) = 3^{2\mathrm{k}-2}$,

$w_a(t) = w_d(t) = w_0(t) = 3^{2\mathrm{k}-2} - 3^{2\mathrm{u}-1}$

$III. w_1(t) = w_2(t) = w_v(t) = w_{2v}(t) = w_a(t) = w_d(t) = 3^{2\mathrm{k}-2}$,

$w_c(t) = w_b(t) = w_0(t) = 3^{2\mathrm{k}-2} - 3^{2\mathrm{u}-1}$

$IV. w_0(t) = w_1(t) = w_2(t) = w_v(t) = w_{2v}(t) = w_a(t) = w_b(t) = w_c(t) = w_d(t) =$
$3^{2\mathrm{k}-} - 3^{2\mathrm{u}-2}$,

aksi taktirde

$I. w_a(t) = w_d(t) = 3^{2\mathrm{k}-1},\ w_0(t) = 3^{2\mathrm{k}-1} - 3^{2\mathrm{u}}$

$II. w_c(t) = w_b(t) = 3^{2\mathrm{k}-}\ , w_0(t) = 3^{2\mathrm{k}-} - 3^{2\mathrm{u}}$

$III. w_a(t) = w_d(t) = w_0(t) = 3^{2\mathrm{k}-1} - 3^{2\mathrm{u}-1}$

$IV. w_c(t) = w_b(t) = w_0(t) = 3^{2\mathrm{k}-1} - 3^{2\mathrm{u}-1}$

dir.

Teorem 3.3.1.4. $\mathrm{M}_{\mathrm{k,t}}^{\alpha}$ kodunun Hamming ve Lee ağırlık dağılımları aşağıdaki gibidir (Çengellenmiş ve Al-Ashker, 2012):

$\mathrm{A_H}\,(0) = 1$

$\mathrm{A_H}\left(8.\,3^{2\mathrm{k}-2}\right) = 4$

$\mathrm{A_H}\left(6.3^{2\mathrm{k}-2} + 2\left(3^{2\mathrm{k}-2} - 3^{2\mathrm{k}-1}\right)\right) = 4\left(3^{2\mathrm{k}-2} - 3\right)$

$$A_H\left(8.\left(3^{2k-2}-3^{2u-2}\right)\right)=3\left(3^{2k-2}+3\right)$$

$$A_H\left(2.3^{2k-1}\right)=4$$

$$A_H\left(2.\left(3^{2k-1}-3^{2u-}\ \right)\right)=2\left(3^{2k-2}-3\right)$$

$$A_L\left(0\right)=1$$

$$A_L\left(4.3^{2k-2}+4.2.3^{2k-2}\right)=3^{2(k-u)}-1$$

$$A_L\left(4.\left(3^{2k-2}-3^{2u-2}\right)+4.2.\left(3^{2k-2}-3^{2u-2}\right)\right)=3^{2k-2}\ \ (3^{2u}-1)$$

4. BULGULAR VE TARTIŞMA

Bu bölümde, $u^2 = u, v^2 = v, uv = vu = 0$ olmak üzere $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2$ sonlu ve değişmeli halkası üzerinde bir Gray dönüşümü tanımlanarak Hamming, Lee ve Bachoc ağırlık dağılımları elde edilmiştir. Son olarak, $u^2 = 0, v^2 = 0, uv = vu = 0$ olmak üzere $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2$ sonlu ve değişmeli halkası tanıtılarak bu halka üzerinde Gray dönüşümü tanımlanmıştır. Bu halka üzerindeki Simplex kodların üreteç matrisi yardımıyla MacDonald kodlar inşa edilmiş ve Lee ağırlık dağılımları parametrelere bağlı olarak elde edilmiştir.

4.1 $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2$ Halkası Üzerinde Tanımlı MacDonald Kodlar

$u^2 = u, v^2 = v, uv = vu = 0$ olmak üzere

$$R_a = \mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2$$

$$\coloneqq \mathbb{F}_2[u,v]/\langle u^2 - u, v^2 - v, uv\rangle = \{a + ub + cv : a, b, c \in \mathbb{F}_2\}$$

halkası karakteristiği 2 olan 8 elemanlı sonlu bir halkadır (Dertli vd, 2015).

Teorem 4.1.1: f: $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 \longrightarrow \mathbb{F}_2[u,v]/\langle u^2 - u, v^2 - v, uv\rangle$

$$a_0 + ua_1 + va_2 \longmapsto f(a_0 + ua_1 + va_2) = \{a_0 + ua_1 + va_2\}$$

dönüşümü bir izomorfizmadır.

İspat: Tanımlanan f dönüşümü kapalı ve iyi tanımlıdır.

(1) $\forall\, y_1 = {a_0}^1 + u{a_1}^1 + v{a_2}^1$, $y_2 = {a_0}^2 + u{a_1}^2 + v{a_2}^2 \in R_a$ için

$$f(y_1) = f(y_2)$$

$$\Rightarrow \{{a_0}^1 + u{a_1}^1 + v{a_2}^1\} = \{{a_0}^2 + u{a_1}^2 + v{a_2}^2\}$$

$$\Rightarrow \{a_0^1 - {a_0}^2 + u(a_1^1 - {a_1}^2) + v(a_2^1 - {a_2}^2)\} = 0$$

$$\Rightarrow a_0^1 - {a_0}^2 = a_1^1 - {a_1}^2 = a_2^1 - {a_2}^2 = 0$$

$$\Rightarrow a_0^1 = {a_0}^2, a_1^1 = {a_1}^2, a_2^1 = {a_2}^2,$$

$$\Rightarrow y_1 = y_2$$

elde edilir. O halde f bire birdir.

(2) f bire bir ve $|R_a| = |\mathbb{F}_2[u,v]/\langle u^2 - u, v^2 - v, uv\rangle| = 2^3 = 8$ olduğundan f örtendir.

(3) $f(y_1+y_2)=f(a_0^1+{a_0}^2+u(a_1^1+{a_1}^2)+v(a_2^1+{a_2}^2))$

$$=\{a_0^1+{a_0}^2+u(a_1^1+{a_1}^2)+v(a_2^1+{a_2}^2)\}$$

$$=\{{a_0}^1+u{a_1}^1+v{a_2}^1\}+\{{a_0}^2+u{a_1}^2+v{a_2}^2\}$$

$$=f(y_1)+f(y_2)$$

$$f(y_1y_2)=f\begin{pmatrix}{a_0}^1{a_0}^2+u({a_0}^1{a_1}^2+{a_1}^1{a_0}^2+{a_1}^1{a_1}^2)+\\ v({a_0}^1{a_2}^2+{a_2}^1{a_0}^2+{a_2}^1{a_2}^2)\end{pmatrix}$$

$$=\begin{Bmatrix}{a_0}^1{a_0}^2+u({a_0}^1{a_1}^2+{a_1}^1{a_0}^2+{a_1}^1{a_1}^2)+\\ v({a_0}^1{a_2}^2+{a_2}^1{a_0}^2+{a_2}^1{a_2}^2)\end{Bmatrix}$$

$$f(y_1)f(y_2)=\{{a_0}^1+u{a_1}^1+v{a_2}^1\}\{{a_0}^2+u{a_1}^2+v{a_2}^2\}$$

$$=\begin{Bmatrix}{a_0}^1{a_0}^2+u({a_0}^1{a_1}^2+{a_1}^1{a_0}^2+{a_1}^1{a_1}^2)+\\ v({a_0}^1{a_2}^2+{a_2}^1{a_0}^2+{a_2}^1{a_2}^2)\end{Bmatrix}=f(y_1y_2)$$

bu durumda f homomorfizmadır. f, 1-1, örten ve homomorfizma olduğundan bir izomorfizmadır. Bu durumda $\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2 \coloneqq \mathbb{F}_2[u,v]/\langle u^2-u, v^2-v, uv\rangle$ yazılır.

Halkanın elemanları $\{0, 1, u, v, a=1+u, b=1+v, a+b=u+v, ab=1+u+v\}$ olmak üzere R_a halkasının işlem tabloları aşağıdaki gibidir.

Çizelge 4.1. R_a halkasının toplam ve çarpım tablosu

$+$	0	1	u	v	$1+u$	$1+v$	$u+v$	w
0	0	1	u	v	$1+u$	$1+v$	$u+v$	w
1	1	0	$1+u$	$1+v$	u	v	w	$u+v$
u	u	$1+u$	0	$u+v$	1	w	v	$1+v$
v	v	$1+v$	$u+v$	0	w	1	u	$1+u$
$1+u$	$1+u$	u	1	w	0	$u+v$	$1+v$	v
$1+v$	$1+v$	v	w	1	$u+v$	0	$1+u$	u
$u+v$	$u+v$	w	v	u	$1+v$	$1+u$	0	1
w	w	$u+v$	$1+v$	$1+u$	v	u	1	0

.	0	1	u	v	$1+u$	$1+v$	$u+v$	w
0	0	0	0	0	0	0	0	0
1	0	1	u	v	$1+u$	$1+v$	$u+v$	w
u	0	u	u	0	0	u	u	0
v	0	v	0	v	v	0	v	0
$1+u$	0	$1+u$	0	v	$1+u$	w	v	w
$1+v$	0	$1+v$	u	0	w	$1+v$	u	w
$u+v$	0	$u+v$	u	v	v	u	$u+v$	0
w	0	w	0	0	w	w	0	w

R_a halkasının 8 tane ideali vardır ve bu ideallerden 3 tanesi maximaldir (Dertli vd, 2015). R_a esas ideal halkasıdır ve yarı-lokal olduğundan sonlu zincir halkası değildir. R_a halkasının maksimal idealleri aşağıdaki gibidir.

$m_1 =< a >= \{0, a, v, ab\}$,

$m_2 =< b >= \{0, b, u, ab\}$,

$m_3 =< u+v >= \{0, u+v, u, v\}$

dir.

Tanım 4.1.2. $\varsigma_i \in R_a$ nın Lee ağırlığı,

$$w_L(\varsigma_i) = \begin{cases} 0, & \varsigma_i = 0 \\ 1, & \varsigma_i = u, v, (ab) \\ 2, & \varsigma_i = b, a, a+b \\ 3, & \varsigma_i = 1 \end{cases}$$

şeklindedir.

Tanım 4.1.3. $\xi_i \in R_a$ nın Bachoc ağırlığı,

$$w_B(\xi_i) = \begin{cases} 0, & \xi_i = 0 \\ 1, & \xi_i = 1 \\ 2, & \xi_i = u, v, a, b, a+b, (ab) \end{cases}$$

şeklindedir.

Tanım 4.1.4. Her $m + un + vp \in R_a$ için

$\sigma : R_a \longrightarrow \mathbb{F}_2^3$

$$m + un + vp \longmapsto \sigma(m + un + vp) = (m, m+n, m+p)$$

şeklinde tanımlanan σ dönüşümüne Gray dönüşümü denir.

Teorem 4.1.5. $\sigma : (R_a^n, d_L) \longrightarrow (\mathbb{F}_2^{3n}, d_H)$ şeklinde tanımlanan Gray dönüşümü uzaklık koruyan bir dönüşümdür. Böylece $\mathcal{C} = (n, 8^{k_1}4^{k_2}2^{k_3}, d_L)$, R_a üzerinde bir lineer kod olmak üzere $\sigma(C)$, $\mathbb{F}_2$ üzerinde $[3n, 3k_1 + 2k_2 + k_3, d_H = d_L]$-koddur.

Teorem 4.1.6. $\sigma : ((R_a)^n, d_L) \longrightarrow (\mathbb{F}_2^{3n}, d_H)$ şeklinde tanımlanan Gray dönüşümü uzaklık koruyan bir dönüşümdür.

İspat: $\forall\, p_1, p_2 \in (R_a)^n$ olsun. Bu durumda $\sigma(p_1 - p_2) = \sigma(p_1) - \sigma(p_2)$ dir.

$$\begin{aligned} d_L(p_1, p_2) &= w_L(p_1 - p_2) \\ &= w_H\big(\sigma(p_1 - p_2)\big) \\ &= w_H\big(\sigma(p_1) - \sigma(p_2)\big) \\ &= d_H\big(\sigma(p_1), \sigma(p_2)\big) \end{aligned}$$

eşitliği elde edilir. O halde σ uzaklık koruyan bir dönüşümdür.

4.1.1. $R_a = \mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2$ halkasındaki MacDonald kodun özellikleri

α tipi Simplex S_k^{α} kodu,

$G_1^{\alpha} = [0 \quad 1 \quad u \quad v \quad a \quad b \quad a+b \quad (ab)\,]$

olmak üzere ve $k \geq 2$ için

$$G_k^{\alpha} = \begin{bmatrix} 0..0 & 1..1 & u..u & \dots & (ab)..(ab) \\ G_{k-1}^{\alpha} & G_{k-1}^{\alpha} & G_{k-1}^{\alpha} & \dots & G_{k-1}^{\alpha} \end{bmatrix}_{k\times 2^{3k}}$$

olmak üzere G_k^{α} üreteç matrisiyle oluşturulan bir lineer koddur.

MacDonald kod, Simplex kodun üreteç matrisi ile elde edilir.

$$G_{k,t}^{\alpha} = \left(G_k^{\alpha} \setminus \frac{0}{G_t^{\alpha}}\right)$$

$G_{k,t}^{\alpha}$ üreteç matrisiyle oluşturulan koda α tipi MacDonald kod denir ve $M_{k,t}^{\alpha}$ ile gösterilir. $M_{k,u}^{\alpha}$, $n = 2^{3k} - 2^{3t}$ uzunluklu, boyutu $3k$ olan bir koddur.

Tanım 4.1.1.1. $\mathcal{C}$, R_a üzerinde bir kod

$$H = (ab)H_1 \oplus uH_2 \oplus vH_3$$

olmak üzere

$$H_1 = \{x: \exists y, z \in {F_2}^n \,|(ab)x + uy + vz \in H\}$$

$$H_2 = \{y: \exists x, z \in {F_2}^n \,|(ab)x + uy + vz \in H\}$$

$$H_3 = \{z: \exists x, y \in {F_2}^n \,|(ab)x + uy + vz \in H\}$$

kümelerine $\mathcal{C}$ nin Torsion kodu denir.

Lemma 4.1.1.2. $M_{k,t}^{\alpha}$ kodunun Torsion kodu, R_a üzerinde bir lineer $[2^{3k} - 2^{3t}, k, 2^{3k-1} - 2^{3t-1}]$-koddur ve ağırlık dağılımları

$$A_H(0) = 1,$$

$$A_H(2^{3k-1} - 2^{3t-1}) = [2^{k-2} + 2^{k+t-3}]$$

$$A_H(2^{3k-1}) = [2^{k-t} - 1]$$

şeklindedir.

$M_{k,t}^{\alpha}$ kodunun ilk $k - t$ satırındaki birimsellerinin adedi 2^{4k-t-4} ve birimsel olmayanların adedi 3.2^{4k-t-3} dir. Son t satırdaki birimsellerin adedi $2^{3k+t-4} - 2^{4t-4}$ ve birimsel olmayanların adedi $3.(2^{3k+t-3} - 2^{4t-3})$ dir.

Lemma 4.1.1.3. $c \in \mathrm{M}_{\mathrm{k,t}}^{\alpha}, c \neq 0$ olmak üzere c elemanının en az bir bileşeni birimsel ise bu durumda 8 tip kod sözcüğü vardır.

I. $w_0(t) = w_1(t) = w_u(t) = w_v(t) = w_a(t) = w_b(t) = w_{a+b}(t) = w_{ab}(t) = 2^{3k-3} - 2^{3t-3}$

II. $w_1(t) = w_u(t) = w_v(t) = w_a(t) = w_b(t) = w_{a+b}(t) = w_{ab}(t) = 2^{3k-3}$, $w_0(t) = 2^{3k-3} - 2^{3t}$

III. $w_1(t) = w_v(t) = w_a(t) = w_b(t) = w_{a+b}(t) = w_{ab}(t) = 2^{3k-3}$, $w_0(t) = w_u(t) = 2^{3k-3} - 2^{3t-1}$

IV. $w_1(t) = w_u(t) = w_a(t) = w_b(t) = w_{a+b}(t) = w_{ab}(t) = 2^{3k-3}$, $w_0(t) = w_v(t) = 2^{3k-3} - 2^{3t-1}$

V. $w_1(t) = w_u(t) = w_v(t) = w_a(t) = w_b(t) = w_{a+b}(t) = 2^{3k-3}$, $w_0(t) = w_{ab}(t) = 2^{3k-3} - 2^{3t-1}$

VI. $w_1(t) = w_u(t) = w_b(t) = w_{a+b}(t) = 2^{3k-3}$, $w_0(t) = w_a(t) = w_v(t) = w_{ab}(t) = 2^{3k-3} - 2^{3t-2}$

VII. $w_1(t) = w_v(t) = w_a(t) = w_{a+b}(t) = 2^{3k-3}$, $w_0(t) = w_u(t) = w_b(t) = w_{ab}(t) = 2^{3k-3} - 2^{3t-2}$

VIII. $w_1(t) = w_a(t) = w_b(t) = w_{ab}(t) = 2^{3k-3}$, $w_0(t) = w_u(t) = w_v(t) = w_{a+b}(t) = 2^{3k-3} - 2^{3t-2}$

aksi takdirde;

I. $w_0(t) = w_u(t) = w_v(t) = w_{ab}(t) = 2^{3k-1} - 2^{3t-1}$

II. $w_0(t) = w_u(t) = w_v(t) = w_a(t) = w_b(t) = w_{a+b}(t) = w_{ab}(t) = 2^{3k-2} - 2^{3t-2}$

III. $w_u(t) = w_v(t) = w_{ab}(t) = 2^{3k-1}$, $w_0(t) = 2^{3k-1} - 2^{3t}$

IV. $w_u(t) = w_a(t) = w_{a+b}(t) = w_{ab}(t) = 2^{3k-2}$, $w_0(t) = w_v(t) = 2^{3k-2} - 2^{3t-1}$

V. $w_v(t) = w_{a+b}(t) = 2^{3k-2}$, $w_0(t) = w_u(t) = 2^{3k-2} - 2^{3t-1}$

VI. $w_u(t) = w_v(t) = w_a(t) = w_b(t) = 2^{3k-2}$, $w_0(t) = w_{ab}(t) = 2^{3k-2} - 2^{3t-1}$

VII. $w_u(t) = w_v(t) = w_a(t) = w_b(t) = w_{a+b}(t) = w_{ab}(t) = 2^{3k-2}$, $w_0(t) = 2^{3k-2} - 2^{2t+1}$

VIII. $w_a(t) = w_b(t) = w_{ab}(t) = 2^{3k-2}$, $w_0(t) = w_u(t) = w_v(t) = 2^{3k-2} - 2^{3t-1}$

Örnek 4.1.1.4. $k = 2, t = 1, p = a + b, q = (ab)$ olmak üzere $\mathrm{M}_{2,1}^{\alpha}$ kodu aşağıdaki gibidir:

$$\begin{cases} bubbuubuubuubbub0q00qq0qq0qq00q0bubbuubuubuubbubq0qq00q0 \\ pppppppppuuuuuuuvvvvvvvvvvvvvvvvuuuuuuuupppppppp00000000 \\ pqvuba01ua0p1qvbvbp0q1uavbp0q1uaua0p1qvbpqvuba0101uvabpq \\ pvvppvvpu00uu00uvppvvppvvppvvppvu00uu00upvvppvvp0uu00uu0 \\ pupuupupupuppupuv0v00v0vv0v00v0vupuppupupupuupup0v0vv0v0 \\ pbpub1u1u1up1bpbvqv0qa0avqv0qa0au1up1bpbpbpub1u10a0vaqvq \\ pavp1av1uq0ubq0bv1pva1pav1pva1pauq0ubq0bpavp1av10bu0qbuq \\ p0vuuv0puv0pp0vuvup00puvvup00puvuv0pp0vup0vuuv0p0puvvup0 \\ p1pp11p1ubuubbubvavvaavavavvaavaubuubbubp1pp11p10q00qq0q \\ qqqqqqqq0000000000000000qqqqqqqqqqqqqqqq00000000qqqqqqqq \\ qpbavu1001uvabpq01uvabpqqpbavu10qpbavu1001uvabpqqpbavu10 \\ qbbqqbbq0uu00uu00uu00uu0qbbqqbbqqbbqqbbq0uu00uu0qbbqqbbq \\ qaqaaqaq0v0vv0v00v0vv0v0qaqaaqaqqaqaaqaq0v0vv0v0qaqaaqaq \\ qvqav0a00a0vaqvq0a0vaqvqqvqav0a0qvqav0a00a0vaqvqqvqav0a0 \\ qubq0ub00bu0qbuq0bu0qbuqqubq0ub0qubq0ub00bu0qbuqqubq0ub0 \\ q1baab1q0puvvup00puvvup0q1baab1qq1baab1qopuvvup0q1baab1q \\ q0qq00q00q00qq0q0q00qq0qq0qq00q0q0qq00q00q00qq0qq0qq00q0 \end{cases}$$

Teorem 4.1.1.5. $M_{k,t}^{\alpha}$ kodunun Hamming, Bachoc ve Lee ağırlık dağılımları aşağıdaki gibidir:

(1) $A_H(0)=1$

$A_H(7.2^{3k-3})=(2^{k-t}-1).(2^{k-t}-1).(2^{k-t}-1)$

$A_H(2^{3k-1}-2^{3t-1})=3.(2^{k+t-3}+1)$

$A_H(2^{3k-1})=3.(2^{k-t}-1)$

$A_H(3.2^{3k-2})=3.(2^{k-t}-1).(2^{k-t}-1)$

$A_H(3.(2^{3k-2}-2^{3t-2}))=3.(2^{k+t-1}-2^{k-2}+1)$

$A_H(7.(2^{3k-3}-2^{3t-3}))=2^{3.(k-t)}.(2^t-1).(2^t-1).(2^t-1)$

$A_H(7.2^{3k-3}-2^{3t-1})=3.[2^{3k-2t}.(2^t-1)-2^k(2^{2k-2}-3.2^{k-1}+4)-5.2^{k+t-3}-1]$

$A_H(3.2^{3k-2}-2^{3t-1})=3.2^k$

$A_H(7.2^{3k-3}-3.2^{3t-2})=3.[(2^{k-1}-1).(2^{k-1}-1).(2^{k-1}-1).2+2^{k-2}+1]$

(2) $A_L(0)=1$

$A_L(3.2^{3k-1})=(2^{k-t}-1).(2^{k-t}-1).(2^{k-t}-1)$

$A_L(2^{3k-1}-2^{3t-1})=3.(2^{k+t-3}+1)$

$A_L(2^{3k-1}) = 3.(2^{k-t} - 1)$

$A_L(2^{3k} - 2^{3t}) = 3.(2^{k+t-1} - 2^{k-2} + 1)$

$A_L(2^{3k} - 2^{3t-1})) = 3.2^k$

$A_L(2^{3k}) = 3.(2^{k-t} - 1).(2^{k-t} - 1)$

$A_L(3.(2^{3k-1} - 2^{3t-1})) = 2^{3.(k-t)}.(2^t - 1).(2^t - 1).(2^t - 1)$

$A_L(3.2^{3k-1} - 2^{3t}) = 3.[(2^{k-1} - 1).(2^{k-1} - 1).(2^{k-1} - 1).2 + 2^{k-2} + 1]$

$A_L(3.2^{3k-1} - 2^{3t-1}) = 3.[2^{3k-2t}.(2^t - 1) - 2^k(2^{2k-2} - 3.2^{k-1} + 4) - 5.2^{k+t-3} - 1]$

(3) $A_B(0) = 1$

$A_B(13.2^{3k-3}) = (2^{k-t} - 1).(2^{k-t} - 1).(2^{k-t} - 1)$

$A_B(2^{3k} - 2^{3t}) = 3.(2^{k+t-3} + 1)$

$A_B(2^{3k}) = 3.(2^{k-t} - 1)$

$A_B(3.2^{3k-1}) = 3.(2^{k-t} - 1).(2^{k-t} - 1)$

$A_B(3.(2^{3k-1} - 2^{3t-1})) = 3.(2^{k+t-1} - 2^{k-2} + 1)$

$A_B(13.(2^{3k-3} - 2^{3t-3})) = 2^{3.(k-t)}.(2^t - 1).(2^t - 1).(2^t - 1)$

$A_B(13.2^{3k-3} - 2^{3t}) = 3.[2^{3k-2t}.(2^t - 1) - 2^k(2^{2k-2} - 3.2^{k-1} + 4) - 5.2^{k+t-3} - 1]$

$A_B(3.2^{3k-1} - 2^{3t}) = 3.2^k$

$A_B(13.2^{3k-3} - 3.2^{3t-1}) = 3.[(2^{k-1} - 1).(2^{k-1} - 1).(2^{k-1} - 1).2 + 2^{k-2} + 1]$

4.2. $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2$ Halkası Üzerinde Tanımlı MacDonald Kodlar

$u^2 = 0, v^2 = 0, uv = vu = 0$ olmak üzere

$R_s = \mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2$

$\coloneqq \mathbb{F}_2[u, v]/\langle u^2, v^2, uv\rangle = \{a + ub + cv : a, b, c \in \mathbb{F}_2\}$

halkası karakteristiği 2 olan 8 elemanlı sonlu bir halkadır.

Teorem 4.2.1. f: $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 \longrightarrow \mathbb{F}_2[u,v]/\langle u^2, v^2, uv\rangle$

$$a_0 + ua_1 + va_2 \longmapsto f(a_0 + ua_1 + va_2) = \{a_0 + ua_1 + va_2\}$$

dönüşümü bir izomorfizmadır.

İspat: Tanımlanan f dönüşümü kapalı ve iyi tanımlıdır.

(1)

$\forall\, y_1 = {a_0}^1 + u{a_1}^1 + v{a_2}^1$, $y_2 = {a_0}^2 + u{a_1}^2 + v{a_2}^2 \in R_a$ için

$f(y_1) = f(y_2)$

$\Rightarrow \{{a_0}^1 + u{a_1}^1 + v{a_2}^1\} = \{{a_0}^2 + u{a_1}^2 + v{a_2}^2\}$

$\Rightarrow \{a_0^1 - {a_0}^2 + u(a_1^1 - {a_1}^2) + v(a_2^1 - {a_2}^2)\} = 0$

$\Rightarrow a_0^1 - {a_0}^2 = a_1^1 - {a_1}^2 = a_2^1 - {a_2}^2 = 0$

$\Rightarrow a_0^1 = {a_0}^2, a_1^1 = {a_1}^2, a_2^1 = {a_2}^2,$

$\Rightarrow y_1 = y_2$

elde edilir. O halde f bire birdir.

(2)

f bire bir ve $|R_s| = |\mathbb{F}_2[u,v]/\langle u^2, v^2, uv\rangle| = 2^3 = 8$ olduğundan f örtendir.

(3)

$$f(y_1 + y_2) = f(a_0^1 + {a_0}^2 + u(a_1^1 + {a_1}^2) + v(a_2^1 + {a_2}^2))$$
$$= \{a_0^1 + {a_0}^2 + u(a_1^1 + {a_1}^2) + v(a_2^1 + {a_2}^2)\}$$
$$= \{{a_0}^1 + u{a_1}^1 + v{a_2}^1\} + \{{a_0}^2 + u{a_1}^2 + v{a_2}^2\}$$
$$= f(y_1) + f(y_2)$$

$$f(y_1y_2) = f\begin{pmatrix} {a_0}^1{a_0}^2 + u({a_0}^1{a_1}^2 + {a_1}^1{a_0}^2) + \\ v({a_0}^1{a_2}^2 + {a_2}^1{a_0}^2) \end{pmatrix}$$

$$= \begin{Bmatrix} {a_0}^1{a_0}^2 + u({a_0}^1{a_1}^2 + {a_1}^1{a_0}^2) + \\ v({a_0}^1{a_2}^2 + {a_2}^1{a_0}^2) \end{Bmatrix}$$

$$f(y_1)f(y_2) = \{{a_0}^1 + u{a_1}^1 + v{a_2}^1\}\{{a_0}^2 + u{a_1}^2 + v{a_2}^2\}$$

$$= \begin{Bmatrix} {a_0}^1{a_0}^2 + u({a_0}^1{a_1}^2 + {a_1}^1{a_0}^2) + \\ v({a_0}^1{a_2}^2 + {a_2}^1{a_0}^2) \end{Bmatrix}$$

$$= f(y_1 y_2)$$

bu durumda f homomorfizmadır.

f, 1-1, örten ve homomorfizma olduğundan bir izomorfizmadır. Bu durumda

$$\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 \coloneqq \mathbb{F}_2[u, v]/\langle u^2, v^2, uv\rangle$$

yazılır.

Halkanın elemanları $\{0, 1,\ u,\ v,\ a = 1 + u,\ b = 1 + v,\ a + b = u + v,\ ab = 1 + u + v\}$ olmak üzere R_s halkasının işlem tabloları aşağıdaki gibidir.

Çizelge 4.2. R_s halkasının toplam ve çarpım tablosu

$+$	0	1	u	v	a	b	$a+b$	ab
0	0	1	u	v	a	b	$a+b$	ab
1	1	0	a	b	u	v	ab	$a+b$
u	u	a	0	$a+b$	1	ab	v	b
v	v	b	$a+b$	0	ab	1	u	a
a	a	u	1	ab	0	$a+b$	b	v
b	b	v	ab	1	$a+b$	0	a	u
$a+b$	$a+b$	ab	v	u	b	a	0	1
ab	ab	$a+b$	b	a	v	u	1	0

.	0	1	u	v	a	b	$a+b$	ab
0	0	0	0	0	0	0	0	0
1	0	1	u	v	a	b	$a+b$	ab
u	0	u	0	0	u	u	0	u
v	0	v	0	0	v	v	0	v
a	0	a	u	v	1	ab	$a+b$	b
b	0	b	u	v	ab	1	$a+b$	a
$a+b$	0	$a+b$	0	0	$a+b$	$a+b$	0	$a+b$
ab	0	ab	u	v	b	a	$a+b$	1

R_s halkasının 6 tane ideali vardır ve

$s =< u, v >= \{0, u, v, a+b\}$

maksimal idealidir. R_s halkasının birimselleri

$R_s{}^* = \{1, a, b, ab\}$

şeklindedir.

Tanım 4.2.2. $\varsigma_i \in R_s$ nin Lee ağırlığı,

$$w_L(\varsigma_i) = \begin{cases} 0, & \varsigma_i = 0 \\ 1, & \varsigma_i = 1, u, (ab) \\ 2, & \varsigma_i = a, b, a+b \\ 3, & \varsigma_i = v \end{cases}$$

şeklindedir.

Tanım 4.2.3. Her $\mathfrak{c} + u\mathfrak{d} + v\mathfrak{f} \in R_s$ için

$\sigma : R_s \longrightarrow \mathbb{F}_2^3$

$\mathfrak{c} + u\mathfrak{d} + v\mathfrak{f} \mapsto \sigma(\mathfrak{c} + u\mathfrak{d} + v\mathfrak{f}) = (\mathfrak{f}, \mathfrak{c} + \mathfrak{f}, \mathfrak{d} + \mathfrak{f})$

şeklinde tanımlanan σ dönüşümüne Gray dönüşümü denir.

Teorem 4.2.4. $\sigma: ({R_s}^n,\ d_L) \longrightarrow (\mathbb{F}_2^{3n}, d_H)$ şeklinde tanımlanan Gray dönüşümü uzaklık koruyan bir dönüşümdür. Böylece $\mathcal{C} = (n, 2^k, d_L)$, R_s üzerinde bir lineer kod olmak üzere $\sigma(C)$, $\mathbb{F}_2$ üzerinde $[3n, k, d_H = d_L]$-koddur.

Teorem 4.2.5. $\sigma:\ ({R_s}^n,\ d_L) \longrightarrow (\mathbb{F}_2^{3n}, d_H)$ şeklinde tanımlanan Gray dönüşümü uzaklık koruyan bir dönüşümdür.

İspat. $\forall\ p_1, p_2 \in {R_s}^n$ olsun. Bu durumda $\sigma(p_1 - p_2) = \sigma(p_1) - \sigma(p_2)$ dir.

$$d_L(p_1, p_2) = w_L(p_1 - p_2)$$
$$= w_H\big(\sigma(p_1 - p_2)\big)$$
$$= w_H\big(\sigma(p_1) - \sigma(p_2)\big)$$
$$= d_H\big(\sigma(p_1), \sigma(p_2)\big)$$

eşitliği elde edilir. O halde σ uzaklık koruyan bir dönüşümdür.

4.2.1. $R_s = \mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2$ halkasındaki MacDonald kodun özellikleri

α tipi Simplex $\mathrm{S}_\mathrm{k}^\alpha$ kodu,

$\mathrm{G}_1^\alpha = [0 \quad 1\ u \quad v \quad a \quad b \quad a+b\ \ (ab)]$

olmak üzere ve $\mathrm{k} \geq 2$ için

$$\mathrm{G}_\mathrm{k}^\alpha = \begin{bmatrix} 0..0 & 1..1 & u..u & \dots & (ab)..(ab) \\ \mathrm{G}_{\mathrm{k}-1}^\alpha & \mathrm{G}_{\mathrm{k}-1}^\alpha & \mathrm{G}_{\mathrm{k}-1}^\alpha & \dots & \mathrm{G}_{\mathrm{k}-1}^\alpha \end{bmatrix}_{k \times 2^{3k}}$$

olmak üzere $\mathrm{G}_\mathrm{k}^\alpha$ üreteç matrisiyle oluşturulan bir lineer koddur.

MacDonald kod, Simplex kodun üreteç matrisiyle elde edilir.

$$\mathrm{G}_{\mathrm{k,t}}^\alpha = \left(\mathrm{G}_\mathrm{k}^\alpha \setminus \frac{0}{\mathrm{G}_\mathrm{t}^\alpha}\right)$$

$\mathrm{G}_{\mathrm{k,t}}^\alpha$ üreteç matrisiyle oluşturulan koda α tipi MacDonald kod denir. Bu kod $\mathrm{M}_{\mathrm{k,t}}^\alpha$ ile gösterilir. $\mathrm{M}_{\mathrm{k,u}}^\alpha$, $n = 2^{3k} - 2^{3t}$ uzunluklu, boyutu $3k$ olan bir koddur.

Örnek 4.2.1.1. $k = 2,\ t = 1,\ p = a + b, q = (ab)$ olmak üzere $\mathrm{M}_{2,1}^\alpha$ kodu aşağıdaki gibidir:

$$\begin{cases} b0q1uvapuq0pbav1v1p0abuqquba0p1v1vabp0qupavu1q0bap1qvub0 \\ babbaabauvuuvvuvvuvvuuvuq1qq11q11q11qq1qp0pp00p0abaabbab \\ buq10pavub0pq1vavap01qubq0bauv1p1pabvuq0p1vuab0qav1qp0bu \\ pppppppp00000000000000000ppppppppppppppppp00000000ppppppppp \\ pqvuba0101uvabpq01uvabpqpqvuba01pqvuba0101uvabpqpqvuba01 \\ pvppvvpv0u00uu0u0u00uu0upvppvvpvpvppvvpv0u00uu0upvppvvpv \\ puppuupu0v00vv0v0v00vv0vpuppuupupuppuupu0v00vv0vpuppuupu \\ pbvuq10a0auv1qpb0auv1qpbpbvuq10apbvuq10a0auv1qpbpbvuq10a \\ pavu1q0b0buvq1pa0buvq1papavu1q0bpavu1q0b0buvq1papqvu1q0b \\ p0pp00p00p00pp0p0p00pp0pp0pp00p0p0pp00p00p00pp0pp0pp00p0 \\ p1vuab0q0quvbap10quvbap1p1vuab0qp1vuab0q0quvbap1p1vuab0q \\ qqqqqqqquuuuuuuuvvvvvvvvbbbbbbbbaaaaaaaappppppppp11111111 \\ qpbavu10ua0p1qvbvbp0q1uabvq1p0auau1q0pbvpqvuba0110abuvqp \\ qbqqbbqbu0uu00u0vpvvppvpbqbbqqbqa1aa11a1pvppvvpv1a11aa1a \\ qaqqaaqaupuuppupv0vv00v0b1bb11b1aqaaqqaqpuppuupu1b11bb1b \\ qvbap01uu10pabvqvqp0bau1bpq1vua0a01quvbapbvuq10a1uab0pqv \\ quba0p1vuq0pbav1v1p0abuqb0q1uvapap1qvub0pavu1q0b1vabp0qu \\ q1qq11q1uvuuvvuvvuvvuuvubabbaabaabaabbabp0pp00p01q11qq1q \\ q0bauv1pub0pq1vavap01qubbuq10pavav1qp0bup1vuab0q1pabvuq0 \end{cases}$$

Teorem 4.2.1.2. $M_{k,t}^{\alpha}$ kodunun Lee ağırlık dağılımı aşağıdaki gibidir:

(2) $A_L(0) = 1$

$A_L(2^{3k-1} - 2^{3t-1}) = 2.(2^{k-1} - 2^{k-t-1}) - 2^{k-2} + 1$

$A_L(2^{3k-1}) = (2^{k-t} - 1)$

$A_L(2^{3k} - 2^{3t}) = 2.(2^{k-1} - 2^{k-t-1}) - 2^{k-2} + 1$

$A_L(2^{3k}) = 2^{k-t} - 1$

$A_L(3.(2^{3k-1} - 2^{3t-1})) = (2^{3k} - 2^{3k-2t+1} + 2^{3(k-t)})$

$A_L(3.2^{3k-1} - 2^{3t}) = (2^{3k-2t} - 2^{3k-3t-1} - 3.2^{k-2} - 3.2^{2k-2t} + 5.2^{k-t} - 1)$

$A_L(3.2^{3k-1} - 2^{3t-1}) = (2^{3k-2t} - 2^{3k-3t-1} - 3.2^{k-2} - 3.2^{2k-2t} + 5.2^{k-t} - 1)$

$A_L(3.2^{3k-1}) = 6.[(2^{k-t} - 1).(2^{k-t} - 1) + (2^{k-t-1} - 1)] - (2^{k-t} - 1)$

Sonuç 4.2.3.1. Benzer şekilde bu halka üzerinde Hamming ve Bachoc ağırlık dağılımları bulunabilir.

5. SONUÇ VE ÖNERİLER

$u^2 = u, v^2 = v, uv = vu = 0$ olmak üzere $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2$, $u^2 = 0, v^2 = 0, uv = vu = 0$ olmak üzere $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2$ sonlu ve değişmeli halkaları üzerinde Gray dönüşümleri tanımlanarak Hamming, Lee ve Bachoc ağırlıkları elde edilmiştir. Bu halkalar üzerinde Simplex kodların üreteç matrisleri yardımıyla MacDonald kodlar inşa edilerek ağırlık dağılımları ve parametreler belirlenmiştir.

Çalışmamızda kullanılan halkalar genişletilerek MacDonald kodlar ve Simplex kodlar incelenebilir. Ayrıca son tanımlanan, $u^2 = 0, v^2 = 0, uv = vu = 0$ olmak üzere $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2$ sonlu ve değişmeli halkası üzerinde Hamming ve Bachoc ağırlık dağılımları belirlenebilir. Bu halkalar üzerinde yapılan MacDonald kodlar yardımıyla gizlilik paylaşım şemaları oluşturulabilir.

KAYNAKLAR

Al-Ashker, M. M. and El-Naowq, F. R. 2005. MacDonald codes over the ring $F_2 + uF_2$. *Journal of the Islamic University of Gaza (Series of Natural Studies and Engineering)*, 2, 47-57.

Al-Ashker, M. M. 2005. Simplex Codes over the Ring $F_2 + uF_2$. *Arabian Journal for Science and Engineering*, 30:2, 277-286.

Al-Ashker, M. 2005. Simplex codes over the ring $\sum_{n=0}^{s} u^n F_2$. *Turkish Journal of Mathematics,* 29, 221-234.

Al-Ashker, M. M. 2010. MacDonald codes over the ring $F_2 + uF_2 + u^2F_2$. *Journal of the Islamic University, Series of Natural Studies and Egineering*, 18:2, 1-9.

Betsumiya, K. and Harada, M. 2004. Optimal Self-Dual Codes Over $F_2 + vF_2$. *IEEE Transactions on Information Theory*, 50, 356-358.

Chapman, R., Dougherty, S. T., Gaborit, P. and Sole, P. 2002. 2-modular lattices from ternary codes. *Journal de Theorie des Nombres de Bordeaux tome*, 14:1, 73-85.

Colbourn, C. J. and Gupta, M. K. 2003. On quaternary MacDonald codes. *In Information Technology: Coding and Computing [Computers and Communications], Proceedings. ITCC 2003. International Conference on* (pp. 212-215), IEEE.

Çallıalp, F. 2013. *Örneklerle Soyut Cebir*. Birsen yayınevi, İstanbul.

Çallıalp, F. 1995. *Cebir*. Sakarya Üniversitesi yayınları, Sakarya.

Çallıalp, F. ve Kuruoğlu, N. 1996. *Lineer cebir*. Ondokuz Mayıs Üniversitesi Yayınları, Samsun.

Çengellenmiş, Y. and Al-Ashker, M. M. 2012. MacDonald codes over the ring $F_3 + vF_3$. *Islamic University of Gaza,* 20:1.

Çengellenmiş, Y. 2010. Simplex codes of type α over $F_3 + vF_3$. *Journal Informatics and Mathematical Sciences*, 5:40.

Dougherty, S. T., Gaborit, P., Harada, M., Solé, P. 1999. Type II Codes Over $F_2 + uF_2$. *IEEE Transactions on Information Theory*, 45, 32-45.

Dougherty, S. T. and Park, Y. H. 2007. On modular cyclic codes. *Finite Fields and Their Applications*, 13, 31-57.

Dertli, A. and Çengellenmiş, Y. 2011. MacDonald codes over the ring $F_2 + vF_2$. *International Journal of Algebra*, 5, 985-991.

Dertli, A., Çengellenmiş, Y. and Eren, Ş. 2015. Quantum Codes Over $F_2 + uF_2 + vF_2$. *Palestine Journal of Mathematics*, 4, 547-552.

Hammons, A. R., Kumar, V., Calderbank, A. R., Sloane, N. J. A. and Solé P. 1994. The Z_4 linearity of Kerdock, Preparata, Goethals and related codes. *IEEE Transactions on Information Theory*, 40, 301-319.

Hill, R. 1986. *A First Course in Coding Theory*. Clarendon Press, The Oxford University Press, Oxford, UK.

Hill, R. 1990. *A First Course in Coding Theory*. Oxford Applied Mathematics and Computing Science Series, UK.

Huffman, W. C. and Pless, V. 2003. *Fundamentals of Error Correcting Codes*. Cambridge University Preess, New York.

Hungerford, T. W. 1973. *Algebra*. Springer-Verlag, New York.

Jitman, S., Udomkavanich, P. and Ling, S. 2012. Skew Constacyclic Codes over Finite Chain Rings. *Advances in Mathematics of Communications*, 6, 29-63.

Ling, S. and Xing, C. 2004. *Coding Theory A First Course*. Cambridge University Press, New York.

MacDonald, J. E. 1960. Design methods for maximum minimum-distance error-correcting codes. *IBM J*, 43-57.

Patel, A. 1975. Maximal q-ary linear codes with large minimum distance. *IEEE Transactions on Information Theory*, 21:1, 106-110.

Roman, S. 1992. *Coding and Information Theory*. Graduate Texts in Mathematics, Springer Verlag.

Sadek, S., El-Atrash, M. and Naji, A. 2002. The second conference of the Islamic University on Mathematical Science-Gaza.27-28 Aug.

Shannon, C. 1948. A Mathematical Theory of Communication. *The Bell System Technical Journal*, 27, 379-423.

Taşcı, D. 2007. *Soyut Cebir*. Alp yayınevi, Ankara.

ÖZ GEÇMİŞ

Adı Soyadı : Rabia DERTLİ

Doğum Yeri : Ankara/Çankaya

Doğum Tarihi : 27.11.1993

Yabancı Dili : İngilizce

Eğitim Durumu

Lise : Şehit Vural Arıcı Anadolu Lisesi/Ankara

Lisans : Ondokuz Mayıs Üniversitesi, Fen Edebiyat Fakültesi, Matematik Bölümü

Yüksek Lisans : Ondokuz Mayıs Üniversitesi, Fen Bilimleri Enstitüsü

Yayınlar

- Dertli, R. ve Eren, Ş., MacDonald codes over the ring $F_2+uF_2+vF_2$, 2019.

Sunumlar

- Dertli, R. ve Eren, Ş., $F_2+uF_2+vF_2$ Halkası Üzerindeki MacDonald Kodlar, 14. Ankara Matematik Günleri, 2019, Gazi Üniversitesi, Ankara.