T.C.

TRAKYA ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

Abdullah DERTLİ

YÜKSEK LİSANS TEZİ

CEBİR VE SAYILAR TEORİSİ ANABİLİM DALI

Tez Yönetici: Yrd. Doç. Dr. Yasemin ÇENGELLENMİŞ

2012-EDİRNE

TRAKYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BELİRLİ TİPTEKİ HALKALAR ÜZERİNDE TANIMLANMIŞ KODLAR HAKKINDA

Abdullah DERTLİ

YÜKSEK LİSANS TEZİ

CEBİR VE SAYILAR TEORİSİ
ANABİLİM DALI

Tez Yönetici: Yrd. Doç. Dr. Yasemin ÇENGELLENMİŞ

2012-EDİRNE

BELİRLİ TİPTEKİ HALKALAR ÜZERİNDE TANIMLANMIŞ
KODLAR HAKKINDA

Abdullah DERTLİ
YÜKSEK LİSANS TEZİ

CEBİR VE SAYILAR TEORİSİ ANABİLİM DALI

Bu Tez 3../03/2012 Tarihinde Aşağıdaki Jüri Tarafından Kabul Edilmiştir.

Prof.Dr. Hülya İŞCAN
Üye

Yrd.Doç.Dr.Yasemin ÇENGELLENMİŞ
Danışman

Doç.Dr. Şaban AKTAŞ
Üye

ÖZET

Bu çalışma dört bölümden oluşmaktadır.

I.Bölümde kodlarla ilgili gerekli ön bilgiler verilmiştir.

II.Bölümde skew cyclic kodlar, skew quasi-cyclic kodlar ve skew constacyclic kodlarla ilgili çalışmalar incelenmiştir.

III.Bölümde, $u_1^2 = 1$, $u_2^2 = 1$, $u_1u_2 = u_2u_1$ olmak üzere

$$M_2 = IF_2[u_1, u_2]/< u_1^2 - 1, u_2^2 - 1, u_1u_2 - u_2u_1 >$$

halkası üzerinde tanımlı self dual kodlarla ilgili bazı sonuçlar elde edilmiş ve bu halka üzerinde Gray dönüşümleri ve Lee ağırlık dönüşümü tanımlanmıştır. Ayrıca M_2 halkası üzerinde aşikar olmayan bir θ otomorfizması tanımlanarak, $M_2[x, \theta]$ skew polinom halkası oluşturulmuştur.

IV.Bölümde $v^2 = v$ olmak üzere $R = F_2 + v F_2 \cong F_2[v]/\langle v^2 - v \rangle$ halkası üzerinde Macdonald kodlar tanımlanmış ve bu kodların Hamming, Lee ve Bachoc ağırlık dağılımları belirlenmiştir.

ABSTRACT

The study consists of four chapters.

In Chapter I, the pertinent backround material about the codes are given.

In Chapter II, the works about the skew cyclic codes, the skew quasi-cyclic codes and the skew constacyclic codes are investigated.

In Chapter III, some results about the self dual codes over the ring

$$M_2 = IF_2[u_1, u_2]/< u_1^2 - 1, u_2^2 - 1, u_1u_2 - u_2u_1 >$$

where $u_1^2 = 1$, $u_2^2 = 1$, $u_1u_2 = u_2u_1$are obtained. The Gray maps and Lee weight over the ring are defined. By defining an non trivial automorphism θ over the ring M_2, the skew polynomial ring $M_2[x, \theta]$ is constructed.

In Chapter IV, it is constructed Macdonald codes over $R = F_2 + v\,F_2 \cong F_2[v]/\langle v^2 - v\rangle$ where $v^2 = v$ and investigated some of their properties.

ÖNSÖZ

Çalışmalarım boyunca matematiksel bakış açısını, tecrübesini, bilgisini benimle paylaşan, maddi ve manevi yönden her türlü yardımcı olan sevgili hocam Yrd.Doç.Dr Yasemin Çengellenmiş'e, yorumlarıyla benden desteğini esirgemeyen Prof. Dr. Hülya İşcan'a teşekkürlerimi sunarım.

Tüm bu süreç içerisinde bana her türlü destek veren aileme, Nuh Hatipoğlu'na, isimlerini sayamadığım hocalarım ve arkadaşlarıma teşekkür ederim.

İÇİNDEKİLER

GÖSTERİMLER

$GR(q) = IF_q$: q bir asalın kuvveti olmak üzere q elemanlı sonlu cisim, Galois cismi

θ : IF_q sonlu cismi üzerinde tanımlı aşikar olmayan otomorfizma

$|< \theta >|$: Aşikar olmayan θ otomorfizmasının mertebesi

$IF_q[x, \theta]$: Skew polinom halkası

$d(a, b)$: a ve b arasındaki Hamming uzaklığı

$d = d(C)$: C kodunun minimum uzaklığı

$(n, M, d)\_kod$: Uzunluğu n, eleman sayısı M, minimum uzaklığı d olan linear kod

$[n, k, d]$_kod:IF_q cismi üzerinde uzunlugu n, boyutu k ve minimum uzaklığı d olan bir lineer kod

$\lfloor x \rfloor$: x in tam değeri

$w(x)$: x elemanının ağırlığı

$w(C)$: C kodunun minimum ağırlığı

$d_q(n, k)$: Kodun en büyük minimum uzaklığı

$C^{\perp}$: C kodunun duali

$[K: F]$: Cisim genişlemesinin derecesi

$Z(R[x, \theta])$: $R[x, \theta]$ skew polinom halkasının merkezi

IF_q^{θ} : θ tarafından sabit bırakılan IF_q sonlu cisminin elemanlarının kümesi

$d = (a, b)$: a ve b nin en büyük ortak böleni

$GR(q, m)$: q asalın bir kuvveti olmak üzere $\mathbb{Z}_q$ üzerinde $m.inci$ dereceden Galois halkası

$\mathcal{A}$: $GR(q, m)$ Galois halkası üzerinde tanımlı otomorfizma grubu

$K = R/< \gamma >$: Rezidü cismi (R sonlu zincir halkası, γ maksimal idealin üreteci)

$Aut\ (R)$: R sonlu zincir halkası üzerinde tanımlı otomorfizmaların kümesi

GİRİŞ

Dört bölümden oluşan tezin I. Bölümünde gerekli önbilgiler , II. Bölümde skew cyclic, skew quasi-cyclic, skew constacyclic kodlarla ilgili yapılmış çalışmalara yer verilmiştir. III. Bölümde $u_1^2 = 1$, $u_2^2 = 1$, $u_1u_2 = u_2u_1$ olmak üzere $M_2 = IF_2[u_1, u_2]/<u_1^2 - 1, u_2^2 - 1, u_1u_2 - u_2u_1>$ halkası üzerinde self dual kodlarla ilgili bazı sonuçlar elde edilmiştir. IV.Bölümde $v^2 = v$ olmak üzere $R = F_2 + v F_2 \cong F_2[v]/\langle v^2 - v\rangle$ halkası üzerinde Macdonald kodlar tanımlanmış ve bu kodların Hamming, Lee ve Bachoc ağırlık dağılımları elde edilmiştir.

Kodlama teorisinin başlangıcı olarak Claude Shannon' un 1948 yılında yayınlanmış olan "A Mathematical Theory of Communication" adlı makalesi kabul edilir. Bu makalede C. Shannon tarafından, gürültülü bir iletişim kanalında, eğer özel şifreleme ve çözme teknikleri kullanılırsa, "kanal kapasitesi" adı verilen sayının altındaki herhangi bir oranda güvenilir iletişimin sağlanabileceği ifade edilmiştir. Fakat ne Shannon'un verdiği kanıt ne de daha sonra verilen kanıtlar yeterli olmamış, Shannon'un teoreminde bahsedilen bir şifreleme oluşturma yöntemi bulunamamıştır. Başlangıç sayılan bu teoriden sonra kodlama teorisinde, gürültü kanalları boyunca veri iletimi ve bozulan mesajı düzeltme gibi konularla ilgilenilmiş, doğru, iletim oranı yüksek, zaman ve enerji tasarrufu sağlayan şifreleme yöntemlerini geliştirme amaç edinilmiştir.

İletişimde amaç, kaynaktan gönderilen mesajı doğruluğu yüksek bir olasılıkla alıcıya ulaştırmaktır. Mesajı iletmek için alfabe olarak adlandırılan sonlu kümeler kullanılır. Bu küme genellikle sonlu bir halka veya cisim olarak alınır. İletilecek mesaj, oluşabilecek hatalardan korunmak üzere şifrelenir. Şifrelenen mesaj, kod sözcükleridir. Kod sözcüğü kanala gönderilir. Bazı sembolleri değişmiş yani hata olmuş olabilir. Şifre çözücü hata olup olmadığını kontrol eder, hata varsa düzeltir ve orijinal mesajı elde edip alıcıya gönderir.

Bir kodun minimum uzaklığı ne kadar büyük olursa o kod o kadar fazla hata düzelteceğinden, minimum uzaklıkları büyük kodlar elde edilmesi önemlidir. Araştırmacıların kodlar üzerine yapmış oldukları bir kısım çalışma, sonlu cisimler üzerinde tanımlı kodlar ile sonlu halkalar üzerinde tanımlı kodlar arasında bir ilişki kurulması ile ilgilidir. Pek çok bilim adamı tarafından yapılan çalışmada, çeşitli sonlu halkalar üzerinde tanımlı cyclic, quasi-cyclic ve constacyclic kodlarla, sonlu cisimler üzerinde tanımlı kodlar arasındaki ilişkiler belirlenerek minimum uzaklıkları büyük yeni kodlar elde edilmiştir.

Cyclic kodlar, son 50 yıldır pek çok bilim adamı tarafından çalışılmıştır. Kodların bu sınıfı ilk olarak $Prange$ tarafından 1957 de tanımlanmıştır. Cyclic kodlar, kodlama teorisindeki önemli bir sınıfı olan hata düzeltici kodlar sınıfını oluşturur. $Prange$ tarafından bir F sonlu cismi üzerinde n uzunluğuna sahip bir cyclic koda karşılık gelen $F[x]/< x^n - 1 >$ halkasının bir idealinin var olduğu gösterilmiştir. İdeallerle cyclic kodlar arasındaki bu ilişki BCH ve $Reed\ Solomon$ kodlarının oluşturulmasına yol açmıştır.

1970 yılından sonra çoğu matematikçi ve mühendis tarafından sonlu cisimler üzerinde tanımlı cyclic kodlarla ilgili çalışmalar sonlu halkalar üzerine taşınmıştır. $Hammons$ tarafından, $\mathbb{Z}_4$ üzerinde tanımlı lineer kodların $Gray\ dönüşümü$ altındaki görüntüsü sayesinde iyi hata düzeltme kapasitesine sahip non lineer kodlar elde edilmiştir. Tüm bu çalışmalar, değişmeli halkalar üzerinde tanımlı kodlara kısıtlanmıştır.

Çalışmanın ikinci bölümünde, cyclic, quasi-cyclic, constacyclic kodlar sınıfından daha geniş bir sınıf olan skew cyclic, skew quasi-cyclic ve skew constacyclic kodlarla ilgili yapılmış çalışmalara ağırlık verilmiştir.

Değişmeli olmayan halkalar kullanılarak, cyclic ve lineer kodların daha genel bir sınıfı olan $Skew\ Cyclic$ kodlar $D.Boucher,\ F.Ulmer$ ve $W.Geiselmann$ tarafından tanımlanmıştır. $D.Boucher,\ F.Ulmer,\ W.Geiselmann$ tarafından IF_q sonlu bir cisim, θ aşikar olmayan bir homomorfizma olmak üzere $IF_q\ [x, \theta]$ skew polinom halkası kullanılarak, skew cyclic kodun skew polinom temsili oluşturulmuştur. Bu sayede $m = |< \theta >|$, θ nın mertebesi olmak üzere $m|n$

olduğu durumda bir skew cyclic koda karşılık gelen $IF_q\,[x,\theta]/< x^n-1 >$ halkasının bir sol idealinin var olduğu gösterilmiştir. Aynı çalışmada $D.Boucher$, $F.Ulmer$ ve $W.Geiselmann$ tarafından skew cyclic kodlar yardımıyla, aynı uzunluğa ve boyuta sahip iyi bilinen lineer kodlardan daha büyük $Hamming$ uzaklıklara sahip yeni kodlar elde edilmiştir.

2007 yılında $D.Boucher$ ve $F.Ulmer$ tarafından, daha önce $D.Boucher$, $F.Ulmer$ ve $W.Geiselmann$ tarafından oluşturulan skew cyclic kodlar genelleştirilmiş ve $\theta-Cyclic$ (skew cyclic) kodların duallerinin yine $\theta-Cyclic$ olduğunu gösterilmiştir.

$D.Boucher$, $W.Geiselmann$, $F.Ulmer$ tarafından yapılan çalışmada sonlu cisimler üzerinde tanımlı skew cyclic kodların uzunluğu, θ otomorfizmasının mertebesine bağlı olarak belirlenmişti. $\dot{I}.Şiap,\ T.Abualrub, N.Aydın, P.Seneviratne$ tarafından 2010 yılında yapılan çalışmada bu kısıtlama kaldırılarak skew cyclic kodların en genel durumu çalışılmıştır. Ayrıca n kodun uzunluğu, m otomorfizmanın mertebesi olmak üzere (n,m)=1 olması durumunda skew cyclic kodun cyclic koda eşit, (n,m)=d olması durumunda quasi-cyclic koda denk olduğu gösterilmiştir.

2010 yılında $T.Abualrub$ ve $P.Seneviratre$ tarafından $v^2=v$ olmak üzere $R=IF_2[v]/< v^2-v >$ sonlu halkası üzerinde tanımlı skew cyclic kodlar tanımlanmıştır. Bu çalışmada θ, R üzerinde tanımlı aşikar olmayan bir otomorfizma olmak üzere R üzerinde tanımlı n uzunluğundaki skew cyclic koda karşılık gelen $R[x,\theta]/< x^n-1 >\ nin\ bir$ sol $R[x,\theta]$ -alt modülün var olduğu gösterilmiştir.

$T.Abualrub,\ N.Aydın,\ \dot{I}.Şiap,\ P.Seneviratne$ tarafından, 2011 yılında Skew $Quasi-Cyclic$ kodlar tanımlanmıştır. Bu çalışmada, $|<\theta>|=m$ θ otomorfizmasının mertebesi olmak üzere $m|s$ olduğu durumda IF_q üzerinde tanımlı $n=s.l$ uzunluğunda l indeksli skew $quasi-cyclic$ koda karşılık gelen $R_s^l=(IF_q[x,\theta]/< x^s-1 >)^{\ l}$ modülünün bir sol R_s-alt modülün var olduğu gösterilmiştir. Bu kodların üreteç ve kısmi kontrol matrisleri verilmiştir. Bu sayede bilinen lineer kodlardan daha iyi yeni kodlar elde edilmiştir.

2011 yılında M. Bhaintwal tarafından Galois halkaları üzerinde skew quasi-cyclic kodlar tanımlanmıştır.

2008 yılında $D.Boucher, P.Sole\ ve\ F.Ulmer$ tarafından sonlu cisimler yerine Galois halkaları üzerinde tanımlı skew polinom halkaları kullanılarak skew constacyclic kod tanımlanmış ve $GR(4,2)$ üzerinde skew constacyclic self dual kodlar oluşturulmuştur. 2009 yılında S. Jitman, S. Ling, P. Udomkavanich tarafından sonlu zincir halkaları üzerinde tanımlı constacyclic kodlar çalışılmıştır.

Skew polinom halkası tek türlü asal çarpanlara ayrılabilen bir bölge olmadığı için skew cyclic, skew constacyclic ve skew quasi-cyclic kodlar tanımlanarak, cyclic, constacyclic, quasi-cyclic kodların bulunduğu sınıftan daha büyük bir sınıf ortaya çıkarılmış ve minimum uzaklığı yüksek kodlar elde etme ihtimalini arttırmıştır.

2009 yılında B.Yıldız ve S. Karadeniz tarafından "Linear codes over $IF_2 + u_1IF_2 + u_2IF_2 + u_1u_2IF_2$" adlı çalışmada $u_1^2 = 0,\ u_2^2 = 0,\ u_1u_2 = u_2u_1$ olmak üzere $M_2 = IF_2[u_1, u_2]\Big/< u_1^2,\ u_2^2, u_1u_2 - u_2u_1 >$ halkasının yapısı analiz edilmiş ve bu halkalar üzerindeki lineer kodlar incelenmiştir. Ayrıca bu kodlar üzerinde Lee ağırlık dönüşümü ve Gray dönüşümleri tanımlanmıştır. 2010 yılında B.Yıldız ve S. Karadeniz tarafından "Cylic codes over $IF_2 + u_1IF_2 + u_2IF_2 + u_1u_2IF_2$" adlı çalışmada bu halka üzerindeki cyclic kodların yapısı "Self dual codes over $IF_2 + u_1IF_2 + u_2IF_2 + u_1u_2IF_2$" adlı çalışmada self dual kodlar incelenmiştir. 2010 yılında S Dougherty, B.Yıldız ve S. Karadeniz tarafından "Codes over R_k, Gray maps and their binary images" adlı çalışmada yapılanların bir kısmı $i = 1, \dots k,\ j = 1, \dots, k\ \ için\ \ u_i^2 = 0,\ u_iu_j = u_ju_i$ olmak üzere $R_k = IF_2[u_1, \dots, u_k]\Big/< u_i^2,\ u_iu_j - u_ju_i >$ sonsuz halkalar ailesine genelleştirilmiştir.

Çalışmanın son bölümünde, $u_1^2 = 1,\ u_2^2 = 1,\ u_1u_2 = u_2u_1$ olmak üzere $M_2 = IF_2[u_1, u_2]\Big/< u_1^2 - 1,\ u_2^2 - 1,\ u_1u_2 - u_2u_1 >$ halkası ve üzerinde tanımlı self dual kodlar incelenmiş, bu halka üzerinde Gray dönüşümleri ve Lee ağırlık dönüşümü tanımlanmıştır. Bu halkalar üzerinde tanımlı self dual kodlarla ilgili bazı sonuçlar elde edilmiştir. Ayrıca M_2 halkası üzerinde aşikar olmayan θ otomorfizması tanımlanarak, $M_2[x, \theta]$ skew polinom halkası oluşturulmuştur. Bu

sayede bu halka üzerinde skew cyclic, skew quasi-cyclic, skew constacyclic kodlar tanımlama ihtimali oluşturulmuştur.

Tezin son bölümünde $v^2 = v$ olmak üzere $R = F_2 + v F_2 \cong F_2[v]/\langle v^2 - v\rangle$ halkası üzerinde tanımlı Macdonald kodlarla ilgili elde edilen sonuçlar yer almıştır.

F_2 üzerindeki MacDonald kodlar, ilk olarak 1960 yılında J. MacDonald tarafından tanımlanmıştır. $q \geq 2$ olmak üzere F_q üzerindeki MacDonald kodlar 1975 yılında A. Patel tarafından çalışılmıştır. C.J. Coulbourn ve M. Harada, Z_4 üzerindeki α ve β tipi simpleks kodları kullanarak Z_4 üzerindeki MacDonald kodları elde etmiştir. Mohammed Al Ashker $u^2 = 0$ olmak üzere $F_2[u]/<u^2>$ halkası üzerindeki MacDonald kodları 2003 yılında tanımlamıştır. Bu çalışmasında, bu kodların Gray dönüşümü altındaki görüntüsü, Torsion kodu ve ağırlık sayaçları konularına değinilmiştir. Ardından benzer bir çalışma $u^3 = 0$ olmak üzere $F_2[u]/<u^3>$ halkası için yapılmıştır.

"Simplex linear codes over the ring $F_2 + vF_2$" adlı çalışmada $v^2 = v$ olmak üzere $R = F_2 + v F_2 \cong F_2[v]/\langle v^2 - v\rangle$ halkası üzerinde lineer simpleks kodlar Mohammed Al Ashker ve Ibtisam Isleem tarafından oluşturulmuş ve bu kodların bazı özellikleri belirlenmiştir.

Tezin son kısmında $v^2 = v$ olmak üzere $R = F_2 + v F_2 \cong F_2[v]/\langle v^2 - v\rangle$ halkası üzerinde tanımlı simpleks kodlar yardımıyla bu halka üzerindeki MacDonald kodların oluşumu ve bu kodların Hamming, Lee ve Bachoc ağırlık dağılımları belirlenmiştir.

I.BÖLÜM

ÖN BİLGİLER

1.1.Kod Tanımı ve Özellikleri

1.1.1 Tanım: R sonlu bir halka olsun.

$$R^n = \{(u_1, u_2, \dots, u_n) | u_i \in R, i = 1,2, \dots, n\}$$

kümesinin s elemanlı bir C R-alt modülüne, n uzunluklu, s elemanlı bir lineer kod denir. Kodun herhangi bir elemanına kod sözcüğü, R^n kümesinin herhangibir elemanına sözcük adı verilir.

1.1.2 Tanım: p bir asal sayı, $n \in \mathbb{N}$ olmak üzere $q = p^n$ elemanlı cisme Galois cismi denir. $GF(q)$ veya IF_q ile gösterilir.

1.1.3 Tanım: $V(n,q) = IF_q^n = \{x = (x_1, x_2, \dots, x_n) | x_i \in IF_q, i = 1,2, \dots, n\}$ kümesi IF_q üzerinde n boyutlu bir vektör uzayı olmak üzere, IF_q^n vektör uzayının bir C alt uzayına lineer kod adı verilir.

C, IF_q^n vektör uzayının k boyutlu bir alt uzayı ise C bir $[n,k]$-lineer kod denir.

1.1.4 Tanım: Her $a = (a_1, a_2, \dots, a_n), b = (b_1, b_2, \dots, b_n) \in IF_q^n$ için

$$\begin{aligned} d \ &: IF_q^n \times IF_q^n \to \mathbb{N} \cup \{0\} \\ &(a,b) \mapsto d(a,b) = \sharp\{i | a_i \neq b_i\} \end{aligned}$$

şeklinde tanımlanan dönüşüme Hamming uzaklığı denir ve

$$\begin{aligned} &i) \ \ \forall a,b \in IF_q^n \text{ için } d(a,b) \geq 0, \ \ d(a,b) = 0 \Leftrightarrow a = b \\ &ii) \ \ \forall a,b \in IF_q^n \text{ için } d(a,b) = d(b,a) \\ &iii) \ \ \forall a,b,c \in IF_q^n \ için \ d(a,b) \leq d(a,c) + d(c,b) \end{aligned}$$

özelliklerini sağlar ve bir metriktir.

1.1.5 Tanım: Bir C kodunun minimum uzaklığı

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

biçiminde tanımlanır. Uzunluğu n, eleman sayısı M ve minimum uzaklığı d olan bir C kodu verildiğinde C koduna (n, M, d)-kod denir.

C bir [n,k]-kodun, d minimum uzaklığı da belirtilmek isteniyorsa C bir $[n, k, d]_q$-lineer kod şeklinde gösterilir.

C, bir $[n, k, d]_q$- lineer kod ise kodun eleman sayısı q^k, kodun oranı k/n dir.

1.1.6 Tanım: x, IF_q^n vektör uzayının herhangi bir elemanı olmak üzere x elemanının sıfırdan farklı bileşenlerinin sayısına x elemanının ağırlığı denir ve $w(x)$ ile gösterilir.

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

1.1.7 Lemma: x, y, IF_q^n vektör uzayının herhangi iki elemanı olmak üzere $d(x, y) = w(x - y)$ tir. (Roman,1992)

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

1.1.9 Tanım: C, IF_q üzerinde tanımlı bir $[n, k]-$lineer kod olsun. Satırları C lineer kodununun taban elemanlarınından oluşturulan, $k \times n$ mertebeli matrise C kodunun üretici matrisi denir ve G ile gösterilir. G üretici matrisi, I_k, $k \times k$ mertebeli birim matris, A, $k \times (n - k)$ mertebeli bir matris olmak üzere $(I_k \mid A)$ şeklinde düzenlenirse bu biçimdeki haline, G matrisinin standart formu adı verilir.

1.1.10 Örnek: IF_2 üzerinde tanımlı $C = \{(0,0,0), (0,1,1), (1,0,1), (1,1,0)\}$ kodunun bir tabanı $S = \{(0,1,1), (1,0,1)\}$ olduğu için $G = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}_{2\times 3}$ matrisi C kodunun üreteci matrisidir. C kodu IF_2 üzerinde tanımlı bir $[3,2,2]\_$ koddur. ■

Kodun parametreleri hakkındaki bazı bilgiler aşağıdaki gibidir.

C bir (n, M, d) −lineer kod olsun. Kodun eleman sayısı büyük ise kodun fazla sayıda mesajı şifrelemesi, minimum uzaklığı büyük ise kodun fazla hatayı düzeltmesinin yanı sıra kodun eleman sayısı büyüdükçe minimum uzaklığı küçülmekte, minimum uzaklığı küçüldükçe kodun elemen sayısı büyümektedir.

IF_q üzerindeki var olan bir lineer kodun belli uzunluk ve boyuta karşılık mümkün en büyük minimum uzaklığı $d_q(n,k)$, var olan bir d minimum uzaklıklı lineer kodun eleman sayısının en büyük değeri $A_q(n,d)$ ile gösterilirse $d_q(n,k)$ ve $A_q(n,d)$ belirlemek kodlama teorisinin en önemli problemlerindendir. Çalışmaların çoğu q, n, d nin küçük değerleri için $A_q(n,d)$ yi belirlemek ve $A_q(n,d)$ için sınırlar tespit etmekle ilgilidir. Ayrıca belirli bir uzunluk ve boyutlu mümkün en büyük minimum uzaklığa sahip IF_q üzerindeki kodları belirlemek ve cebirsel olarak karşılık gelen kodu oluşturmakla ilgili çalışmalar da bulunmaktadır.

$q = 2,3,5,7,8,9$ değerleri için $d_q(n,k)$ nin değerleri, $A.E.Brauwer$ tarafından düzenlenmiş **www.win.tue.nl/~aeb** web sayfasında bulunmaktadır.

1.1.11 Teorem: C, d minimum uzaklığa sahip bir kod olsun.

(i) $d \geq k+1$ ise C kodu herhangi bir kod sözcüğündeki k tane hatayı tespit eder.

(ii) $d \geq 2t+1$ ise C kodu herhangi bir kod sözcüğündeki t tane hatayı düzeltir. (Hill, 1986)

1.1.12 Sonuç: d minimum uzaklığa sahip olan bir C kodu herhangi bir kod sözcüğünde $d-1$ tane hatayı tespit etmekte ya da $\left\lfloor \frac{d-1}{2} \right\rfloor$ tane hatayı düzeltmekte kullanılır. (Ling, 2004)

1.1.13 Teorem: C ve D, $k \times n$ mertebeli iki matris olsun. 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

işlemlerinden en az biri uygulanarak D matrisi elde ediliyorsa C ve D , $GF(q)$ üzerinde tanımlı denk [n,k]- lineer kodlarını üretir.

1.1.14 Tanım: C, IF_q^n vektör uzayının bir alt kümesi olsun. Eğer her $c = (c_0, c_1, \dots, c_{n-1}) \in C$ iken $(c_{n-1}, c_0, \dots, c_{n-2}) \in C$ oluyorsa C kümesine cyclic küme denir.

C lineer bir kod cyclic bir küme ise bu koda cyclic kod denir.

1.1.15 Örnek: $C_1 = \{(0,0,0), (1,0,1), (0,1,1), (1,1,0)\} \subseteq IF_2^3$,

$$C_2 = \{(0,1,1,2), (2,0,1,1), (1,2,0,1), (1,1,2,0)\} \subseteq IF_3^4,$$

$$C_3 = \{(1,1,1,1,1)\} \subseteq IF_2^5,$$

kodları veriliyor.

C_1 cyclic bir koddur. C_2 ve C_3 kümeleri cyclic küme olmalarına rağmen lineer kod olmadıkları için cyclic kod değildir.

1.1.16 Teorem: $\pi : IF_q^n \longrightarrow IF_q[x]/< x^n - 1 >$ şeklinde tanımlanan dönüşüm bir izomorfizma olmak üzere $C \subseteq IF_q^n$ alt kümesinin cyclic kod olması için gerekli ve yeterli koşul $\pi(C)$ $nin,$ $IF_q[x]/< x^n - 1 >$ halkasının bir ideali olmasıdır. (Prange, 1958)

1.1.17 Teorem: IF_q, q elemanlı bir cisim, f(x) $\in IF_q[x]$ olsun.

i) $IF_q[x]$ bir esas ideal bölgesidir.

ii) $IF_q[x]/(f(x))$ esas ideal bölgesidir. (Mac Williams, Sloane, 1978)

1.1.18 Teorem: I, $IF_q[x]/< x^n - 1 >$ halkasının bir ideali olsun.

$\overline{g(x)}$ $=g(x)+< x^n-1 >$, I idealinin sıfırdan farklı en küçük dereceli ve monik bir elemanı olsun. Bu durumda I= $< \overline{g(x)} >$ ve g$(x) \mid x^n-1$ tir

1.1.19 Örnek: $C=\{(0,0,0),(1,0,1),(0,1,1),(1,1,0)\} \subseteq IF_2^3$

IF_2 üzerinde tanımlı cyclic kodunu ele alalım. Bu durumda

$$\pi: IF_2^3 \longrightarrow IF_2[x]/< x^3-1 >$$

olduğu için

$$\pi(C)=\left\{\bar{0}, \overline{1+x}, \overline{1+x^2}, \overline{x+x^2}\right\} \subseteq IF_2[x]/< x^3-1 >$$

idealdir. $\pi(C)$ aynı zamanda bir esas idealdir. $\pi(C) =< \overline{1+x} >$ dir. Gerçekten de

$$\bar{0}.\overline{(1+x)}=\bar{0}=\overline{(1+x)}.\overline{(1+x+x^2)}$$

$$\bar{1}.\overline{(1+x)}=\overline{1+x}=\overline{(1+x)}.\overline{(x+x^2)}$$

$$\bar{x}.\overline{(1+x)}=\overline{x+x^2}=\overline{(1+x^2)}.\overline{(1+x)}$$

$$\overline{x^2}.\overline{(1+x)}=\overline{1+x^2}=\overline{(1+x)}.\overline{(1+x)}$$

$$IF_2[x]/< x^3-1 >=\left\{\overline{a_0+a_1x+a_2x^2} \mid a_i \in IF_2, i=0,1,2\right\}$$
$$=\left\{\bar{0}, \bar{1}, \overline{1+x}, \overline{1+x^2}, \bar{x}, \overline{x^2}, \overline{1+x+x^2}, \overline{x+x^2}\right\}$$

$$< \overline{1+x} >=\left\{\overline{(1+x)}.\overline{f(x)} \mid \overline{f(x)} \in IF_2[x]/< x^3-1 >\right\}$$

1.1.20Örnek: $I=\left\{\bar{0}, \overline{1+x^2}, \overline{x+x^2}, \overline{1+x+x^2+x^3}\right\} \subset IF_2[x]/< x^4-1 >$

idealine karşılık gelen cyclic kod $\pi(C)=I$ sağlayan C kodu $C=\{(0,0,0,0),(1,0,1,0),(0,1,1,0),(1,1,1,1)\}$ dir.

1.1.21 Tanım: $n=s.l$ ve C, IF_q^n kümesinin bir alt kümesi olsun. Eğer

i) C, IF_q^n nin bir alt uzayı ve

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

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

koşulları sağlanıyorsa C ye $n = s.l$ uzunluğunda l indeksli bir quasi-cyclic koddur denir.

1.1.22 Tanım: R sonlu bir halka, $\lambda \in R$ birim, C, R üzerinde tanımlı bir lineer kod olsun.

$$\begin{aligned} \sigma: \quad & R^n \longrightarrow R^n \\ & (c_0, c_1, \dots, c_{n-1}) \mapsto \sigma(c_0, c_1, \dots, c_{n-1}) = (\lambda . c_{n-1}, c_0, \dots, c_{n-2}) \end{aligned}$$

olmak üzere $\sigma(C) = C$ oluyorsa C koduna R üzerinde tanımlı bir λ-constacyclic kod dur denir.

1.1.23 Tanım: Her $u = (u_1, u_2, \dots, u_n),\ v = (v_1, v_2, \dots, v_n) \in IF_q^n$ elemanları için

$$\begin{aligned} \cdot \ : IF_q^n \times IF_q^n &\longrightarrow IF_q \\ (u, v) &\mapsto u.v = u_1 v_1 + \dots + u_n v_n \end{aligned}$$

biçiminde tanımlanan dönüşüme bir iç çarpım denir. $u.v = 0$ ise u ile v birbirine diktir denir.

1.1.24 Tanım: $C,\ IF_q$ üzerinde tanımlı bir $[n, k]$_ kod olsun.

$$C^{\perp} = \left\{ v \in IF_q^n \mid u.v = 0,\ \forall u \in C \right\}$$

kümesine C nin duali denir. $C^{\perp} = C$ ise C ye self dual kod, $C \subseteq C^{\perp}$ise C koduna self ortagonal kod denir.

1.1.25 Teorem: C, IF_q üzerinde tanımlı bir $[n, k]$_kod ve $G = \begin{bmatrix} g_{11} & g_{12} & \dots & g_{1n} \\ g_{21} & g_{22} & \dots & g_{2n} \\ & \vdots & & \\ & . & & \\ g_{k1} & g_{k2} & \dots & g_{kn} \end{bmatrix}_{k \times n}$, C kodunun üreteci matrisi olsun.

$v = (v_1, v_2, \dots, v_n) \in IF_q^n$ olmak üzere $v \in C^{\perp}$ olması için gerekli ve yeterli koşul

$$[v_1\ v_2 \dots v_n]_{1 \times n} . G_{n \times k}^{\mathrm{T}} = [0\ 0 \dots\ 0]_{1 \times k}$$

olmasıdır.

1.1.26 Önerme: C, IF_q üzerinde tanımlı bir lineer $[n,k]$_kod ise $C^{\perp}$ de IF_q üzerinde tanımlı bir lineer $[n,n-k]$_ koddur. (Hill, 1986)

1.1.27 Tanım: C bir $[n,k]$_kod ise $C^{\perp}$ nin üretici matrisine parity-check matrisi denir ve H ile gösterilir.

1.1.28 Not: H, $(n-k) \times n$ tipinde $G.H^T = 0$ koşulunu sağlayan bir matristir.

H , bir C lineer $[n,k]$_ kodunun parity-check matrisi ise

$$C = \{x = (x_1, x_2, \dots, x_n) \in IF_q^n \mid [x_1 \quad x_2 \quad x_3 \dots\dots \quad x_n]_{1\times n}.H^{\mathrm{T}}_{n\times(n-k)} = [0]_{n\times(n-k)}\}$$

biçiminde ifade edilir.

1.1.29 Lemma: F sonlu bir cisim olmak üzere $[K:F] = d$ ise $|K| = |F|^d$ dir. (Roman, 1992)

1.1.30 Teorem: F sonlu bir cisim olmak üzere, F cisminin karakteristiği asal bir sayıdır. Ayrıca $charF = p$ ise $n \in \mathbb{Z}^+$ olmak üzere F cismi $q = p^n$ tane elemana sahiptir. (Roman, 1992)

1.1.31 Teorem: K sonlu bir cisim, $|K| = p^n$ ve F, K cisminin bir alt cismi olsun. Bu durumda F cisminin eleman sayısı $d \mid n$ olmak üzere p^d dir. (Roman, 1992)

1.1.32 Sonuç: F sonlu bir cisim olsun. F^*, F cisminin sıfırdan farklı elemanlarının oluşturduğu grup ise F^* cyclic bir gruptur. (Roman, 1992)

1.1.33 Tanım: IF_q^* devirli grubunu üreten IF_q cisminin herhangi bir elemanına ilkel eleman denir.

1.1.34 Tanım: α, IF_{q^n} cisminin ilkel bir elemanı olmak üzere α, elemanının IF_q cismi üzerindeki minimal polinomuna ilkel polinom adı verilir.

Ayrıca IF_{q^n} üzerindeki ilkel polinom, IF_q üzerinde asal ve monik bir polinomdur ve bu polinomun tüm kökleri IF_{q^n} cisminin ilkel elemanlarıdır.

1.1.35 Teorem: $f(x) \in IF_q[x]$, d. dereceden asal bir polinom ve α, $f(x)$ polinomunun bir kökü olsun. bu durumda f(x) polinomunun parçalanma cismi

$$IF_q(\alpha) \cong IF_{q^d}$$

dir. Ayrıca f(x) polinomunun parçalanma cisminin IF_q cismi üzerindeki derecesi d ye eşittir. (Roman,1992)

1.1.36 Teorem: $f(x) \in IF_q[x]$ d.dereceden asal bir polinom olsun. a, $f(x)$ polinomunun IF_{q^d} cismi içindeki bir kökü ise f(x) polinomunun tüm kökleri d,

$$\alpha^{q^d} = \alpha$$

eşitliğin sağlayan en küçük pozitif tamsayı olmak üzere

$$\alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{d-1}}$$

şeklindedir. (Roman, 1992)

Sonlu bir cismin elemanlarını belirlemek için çeşitli yöntemler vardır. Bunlardan bir tanesi $p(x)$, IF_q üzerinde asal bir polinom olmak üzere $IF_q[x]/\langle p(x)\rangle$ bölüm halkasının elemanlarını yazmaktır.

Diğer bir yöntem de ilkel elemanın tüm kuvvetleri IF_q^* devirli grubunun elemanları olduğu için bu devirli grup yardımıyla sonlu cismin elemanlarını yazmaktır.

$p(x)$, IF_q üzerinde $\deg p(\mathrm{x}) = d$ olan asal bir polinom ise $IF_q[x]/\langle p(x)\rangle$ bölüm halkası bir cisimdir ve

$$IF_{q^d} \cong F_q[x]/\langle p(x)\rangle = \{r(x) + < p(x) > \mid \deg r(x) < d, r(x) \in IF_q[x]\}$$

şeklindedir.

α, $p(x)$ polinomunun bir kökü ise IF_{q^d} cisminin elemanları derecesi d den küçük α elemanına bağlı polinomlar şeklinde de belirlenebilir. Ayrıca $IF_q[x]/\langle p(x)\rangle$ cismi $IF_q(\alpha)$ cismine izomorftur.

1.1.37 Örnek: $p(x) = x^4 + x + 1$, IF_2[x] üzerinde asal bir polinom olsun. $\alpha, p(x)$ polinomunun bir kökü olmak üzere

$$IF_2[x]/< x^4 + x + 1 > = \{\overline{a(x)} = a_0 + a_1x + a_2x^2 + a_3x^3 + \langle x^4 + x + 1\rangle \mid a_i \in IF_2, i = 0,1,2,3\}$$
$$\cong \{a(\alpha) \mid \overline{a(x)} \in IF_2[x]/\langle x^4 + x + 1\rangle\}$$
$$= \{0,1,\alpha,\alpha^2,\dots,\alpha^3 + \alpha^2 + 1\}$$

şeklindedir. α, $p(x)$ polinomunun bir kökü olduğu için $\alpha^4 + \alpha + 1 = 0$ ve α^{15}=1 olduğu için α elemanının mertebesi 15 i bölmelidir. $\alpha^3 \neq 1$ ve $\alpha^5 \neq 1$ nedeniyle α elemanının mertebesi 15 tir. O halde α bir ilkel elemandır. Bu nedenle IF_{16} cisminin sıfırdan farklı her elemanı $k = 0,1,2,3,\dots,14$ olmak üzere α^k şeklinde yazılır. k, α nın kuvveti ve $a_3a_2a_1a_0$ sırasıyla $a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0$ polinomunun katsayılarınca belirlenen ifade olmak üzere

k	$a_3a_2a_1a_($
0	0001
1	0010
2	0100
3	1000
4	0011
5	0110
6	1100
7	1011
8	0101
9	1010
10	0111
11	1110
12	1111
13	1101
14	1001

şeklindedir

II.BÖLÜM

SKEW CYCLIC, SKEW QUASICYCLIC VE SKEW CONSTACYCLIC KODLAR

SKEW CYCLIC KODLAR

Sonlu cisimler üzerinde tanımlı skew cyclic kodlar ilk olarak 2007 yılında $D.Boucher, W.Geiselmann, F.Ulmer$ tarafından tanımlanmıştır. Bu çeşit kodlar cyclic kodların bir genellemesidir. $D.Boucher, W.Geiselmann, F.Ulmer$tarafından sadece belirli uzunluğa sahip skew cyclic kodların (değişmeli olmayan halkaları kullanarak) diğer bir oluşumu belirlenmiştir. 2010 yılında $\dot{I}.Şiap$, $T.Abualrub, N.Aydın, P.Seneviratne$ tarafından uzunluk üzerindeki kısıtlamalar ortadan kaldırılarak skew cyclic kodların değişmeli olmayan halkalara bağlı olan tanımı elde edilmiştir. Ayrıca bu kodların belirli şartlar altında ya cyclic kodlara eşit ya da Quasi cyclic kodlara denk olduğunu belirlenmiştir.

2009 yılında $D.Boucher, F.Ulmer$ tarafından sonlu cisimler üzerindeki skew cyclic kodlar genelleştirilmiştir.

$IF_2 + vIF_2$halkası üzerindeki skew cyclic kodların yapısı ise 2010 yılında $T.Abualrub, P.Seneviratne$ tarafından belirlenmiştir.

2.1.Sonlu cisimler üzerinde tanımlı skew cyclic kodlar

2.1.1 Önerme:F, karakteristiği p olan sonlu bir cisim, θ, mertebesi m olan F cisminin bir otomorfizması ve $K = \{a \in F \mid \theta(a) = a\}$, F cisminin alt cismi olsun. Bu durumda $[F: K] = m$ ve $t \epsilon \mathbb{Z}_+$, $F = IF_{p^{tm}}$ olmak üzere $K = IF_{p^t}$ dir.

Ayrıca $her\ a \in F$ için $\theta(a) = a^{p^t}$dir.

(Şiap, $Abualrub,\ Aydın,\ Seneviratne$,2010)

2.1.2 Örnek: α, $p(x) = x^2 + x + 1 \in IF_2[x]$ polinomunun bir kökü olmak üzere

$$IF_4 \cong IF_2[x]/< x^2 + x + 1 > \cong \{0,1,\alpha,\alpha^2\} \quad \text{ve} \quad \begin{matrix} \theta: IF_4 \longrightarrow IF_4 \\ a \longmapsto a^2 \end{matrix}$$

olsun. Bu durumda $\theta(0) = 0$, $\theta(1) = 1$, $\theta(\alpha) = \alpha^2$, $\theta(\alpha^2) = \alpha$ dır. Ayrıca

$IF_2 = \{s \in IF_4 \mid \theta(s) = s\}$ dır.

2.1.3Tanım: θ, IF_qüzerinde tanımlı aşikar olmayan bir otomorfizma olsun. C_θ, IF_q üzerinde tanımlı bir kod olsun. Eğer her $(a_0, a_1, \dots, a_{n-1}) \in C_\theta$ iken $\big(\theta(a_{n-1}), \theta(a_0), \dots, \theta(a_{n-2})\big) \in C_\theta$ oluyorsa C_θ lineer koduna IF_q üzerinde tanımlı n uzunluğundaki (θ-cyclic) skew cyclic kod denir.

2.1.4Tanım:IF_q sonlu bir cisim ve θ, IF_qüzerinde tanımlı aşikar olmayan bir otomorfizma olsun. $IF_q[x]$ polinomlar kümesi üzerinde tanımlı toplama, m<n ve her $p(x) = p_0 + p_1x + \cdots + p_mx^m$ ve her $r(x) = r_0 + r_1x + \cdots + r_nx^n$ için $h_0 = p_0r_0$, $h_1 = p_0r_1 + p_1\theta(r_0)$, $h_2 = p_0r_2 + p_1\theta(r_1) + p_2\theta^2(r_0)$,…., $h_{m+n} = p_m\theta^m(r_n)$ olmak üzere

$$. : IF_q[x] \times IF_q[x] \to IF_q[x]$$

$$\big(p(x), r(x)\big) \mapsto p(x).r(x) = h(x) = \sum_{i=0}^{m+n} h_i x^i$$

şeklinde tanımlı çarpma işlemine göre $IF_q[x]$ değişmeli olmayan halkadır. Bu halkaya skew polinom halkası denir ve $IF_q[x, \theta]$ ile gösterilir.

2.1.5 Önerme:$IF_q[x, \theta]$ skew polinom halkası olsun.

i)$IF_q[x, \theta]$ sıfır bölensizdir.

ii) $IF_q[x, \theta]$ nın birimleri F nin birimleridir.

iii)$Her\ \ f, g\ \in IF_q[x, \theta]$ için $\deg(f + g) \leq \max\{\deg f, \deg g\}$ dir.

iv)$Her\ \ f, g\ \in IF_q[x, \theta]$ için $\deg(f.g) = \deg f + \deg g$ dir.

koşulları sağlanır.(Şiap, $Abualrub,\ Aydın,\ Seneviratne$,2010)

İspat:i)$\forall\ a(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \neq 0$ ve
$b(x) = b_0 + b_1x + \cdots + b_{m-1}x^{m-1} \in IF_q[x, \theta]$ için $a(x).b(x) = 0$ olsun.

$$a(x).b(x) = 0 \Longrightarrow (a_0 + a_1x + \cdots + a_{n-1}x^{n-1}).(b_0 + b_1x + \cdots + b_{m-1}x^{m-1}) = 0$$
$$\Longrightarrow a_0b_0 + a_1x.b_1x + \cdots + a_{n-1}x^{n-1}b_{m-1}x^{n-1} = 0$$
$$\Longrightarrow a_0b_0 + a_1\theta(b_1)x + \cdots + a_{n-1}\theta^{n-1}(b_{m-1})x^{n-1+m-1} = 0$$
$$\Longrightarrow a_0b_0 = 0, \quad a_1\theta(b_1) = 0, \quad , \dots , \quad \theta^{n-1}(b_{m-1}) = 0$$
$$\Longrightarrow b_0 = \theta(b_1) = \cdots = \theta^{n-1}(b_{m-1}) = 0$$
$$\Longrightarrow b_0 = b_1 = \cdots = b_{m-1} = 0$$

$a(x) \neq 0\ olduğu\ için\ b(x) = 0$ dır. O halde $IF_q[x,\theta]$ sıfır bölensizdir.

ii) IF_q nun birimi 1_{IF_q} ise $IF_q[x,\theta]$ nın birimi 1_{IF_q} sabit polinomudur. $\forall f \in IF_q[x,\theta]$ için

$$f.1_{IF_q} = 1_{IF_q}.f = f$$

şeklinde elde edilir.

iii) Kolaylıkla görülür.

iv) $f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$, $g(x) = b_0 + \cdots + b_{m-1}x^{m-1} \in IF_q[x,\theta]$ için

$$f(x).g(x) = (a_0 + a_1x + \cdots + a_{n-1}x^{n-1}).(b_0 + b_1x + \cdots + b_{m-1}x^{m-1})$$
$$= a_0b_0 + \cdots + a_{n-1}\theta^{n-1}(b_{m-1})x^{n-1+m-1}$$

$\deg\big(f(x).g(x)\big) = m + n - 2$ $\boxed{\text{I}}$

$\deg\big(f(x)\big) + \deg\big(g(x)\big) = n - 1 + m - 1 = n + m - 2$ $\boxed{\text{II}}$

$\boxed{\text{I}}$ ve $\boxed{\text{II}}$ den $\deg\big(f(x).g(x)\big) = \deg\big(f(x)\big) + \deg\big(g(x)\big)$

2.1.6 Teorem: (Sağdan bölme algoritması) Her $f(x) \neq 0$, $g(x) \in IF_q[x,\theta]$ için

$$g(x) = q(x).f(x) + r(x) \quad \text{ve} \quad \deg r(x) < \deg f(x)$$

olacak şekilde tek şekilde tanımlı $q(x)$, $r(x)$polinomları vardır.

$r(x) = 0$ ise $f(x)$ polinomuna sağ bölen adı verilir.(Şiap, $Abualrub,\ Aydın,\ Seneviratne$,2010)

Benzer şekilde soldan bölme algoritması da tanımlanabilir.

2.1.7 Örnek: α, $p(x) = x^2 + x + 1 \in IF_2[x]$ polinomunun bir kökü olmak üzere $IF_4 \cong IF_2[x]/< x^2 + x + 1 > \cong \{0,1,\alpha,\alpha^2\}$ ve $her\ \ s \in IF_4$ olmak üzere $\theta(s) = s^2$ olsun.

$x + \alpha$ nın $IF_4[x,\theta]$ daki sağ ve sol böleni $\alpha x + 1$ dir. Gerçekten,

$$x + \alpha = \alpha^2(\alpha x + 1) + 1 = (\alpha x + 1).\alpha + 0$$

dır.

2.1.8 Teorem: $IF_q[x,\theta]$ skew polinom halkası esas ideal bölgesidir. (McDonald,1974)

İspat : $I = \{0\}$ ise $I = (0)$ dir. I, $IF_q[x,\theta]$ halkasının herhangi bir sol ideali, p , I idealinin sıfırdan farklı en küçük dereceli polinomu olsun. $Her\ g \in I$ için $g = qp + r$, $r = 0$ veya $\deg r < \deg p$ olacak şekilde uygun q ve r elemanları vardır. r≠ 0 $ise\ g = qp + r \Longrightarrow r = g - qp \in I$ dir. p en küçük dereceli polinom olduğundan çelişki olur. r = 0 dır. Yani I esas idealdir. $IF_q[x,\theta]$ halkasının her sağ idealinin de esas ideal olduğu benzer şekilde gösterilir.

2.1.9. Teorem: θ, IF_q üzerinde tanımlı aşikar olmayan bir otomorfizma olsun. θ otomorfizmasının mertebesi m, $a_1, \ldots . a_n \epsilon IF_q$ ve $t \in \mathbb{Z}_+$ olmak üzere $IF_q[x,\theta]$ halkasının ideali

$$f(x) = (a_0 + a_1 x^m + a_2 x^{2m} + \cdots + a_n x^{nm}).x^t$$

biçimindeki eleman ile üretilir. (McDonald,1974)

İspat: I ideal olsun. Bu durumda $\exists g, f \in IF_q[x,\theta] \ni\ I = IF_q[x,\theta].g$ ve $I = f.IF_q[x,\theta]$ şeklinde yazılabilir. Teorem 2.1.9 dan $f.s = g$ ve $t.g = f$ olacak şekilde s ve t polinomları vardır.

$t.f \in I \Longrightarrow t.f = f.t'$olacak biçimde $\exists t'$ polinomu vardır.

$$f = t.g = t.f.s = f.t'.s$$

olur. Bu durumda $1 = t'.s$ olur. Yani s, IF_q da birimdir. Kısaca sol üreteç sağ üreteç ve sağ üreteç sol üreteç olur.

$$f(x) = a_0 x^t + a_1 x^{t+1} + a_2 x^{t+2} + \cdots + a_n x^{t+n}$$

I idealinin bir üreteci olsun. x^t nin ideali ürettiği açıktır. $a_0 \neq 0$ olmak üzere

$$a_0 + a_1 x + \cdots + a_n x^n = f$$

elemanının ideali ürettiğini görmek için;

$$f = a_0 + a_1 x + \cdots + a_n x^n$$

olsun. $\beta \in IF_q$ ise $\beta.f = f.\delta,\ \exists \delta \in IF_q[x,\theta]$ vardır. $\deg \delta = 0$ ve $\delta \in IF_q[x,\theta]$ olsun. O zaman

$$f.\delta = (a_0 + a_1x + \cdots + a_nx^n).\delta$$
$$= a_0\delta + a_1x\delta + \cdots + a_nx^n\delta$$
$$= a_0\delta + a_1\theta(\delta) + \cdots + a_n\theta^n(\delta).x^n$$
$$= \beta.f$$

Öyleyse

$$\beta = \delta, \qquad \beta = \theta(\delta) \ \ldots \ \beta = \theta^n(\delta)$$

olur. β, IF_q da keyfi olduğundan m, θ nın mertebesi f de x in her bir kuvvetini bölmelidir. Yani;

$$f(x) = (a_0 + a_1x^m + a_2x^{2m} + \cdots + a_nx^{nm}).x^t$$

olur.■

$IF_q[x,\theta]/< x^n - 1 >$ Kümesinin Cebirsel Yapısı

θ, IF_q sonlu cismi üzerinde tanımlı aşikar olmayan bir otomorfizma ve m, θ otomorfizmasının mertebesi olmak üzere $m \mid n$ ise $R_n = IF_q[x,\theta]/< x^n - 1 >$ kümesi toplama ve $her \ \ f_1(x) + \langle x^n - 1\rangle$ ve her $f_2(x) + \langle x^n - 1\rangle \in R_n$ için

$$(f_1(x) + \langle x^n - 1\rangle).(f_2(x) + \langle x^n - 1\rangle) = f_1(x).f_2(x) + \langle x^n - 1\rangle$$

şeklinde tanımlanan çarpma işlemine göre bir halkadır.

$m \nmid n$ ise $R_n = IF_q[x,\theta]/< x^n - 1 >$, toplama ve $her \ r(x) \in IF_q[x,\theta]$ için

$$r(x).(f(x) + \langle x^n - 1\rangle) = r(x).f(x) + \langle x^n - 1\rangle$$

işlemine göre bir sol $IF_q[x,\theta]$ −modüldür. Dolayısıyla her iki durum için sonlu cisimler üzerinde tanımlanan skew cyclic kodun eşdeğer tanımı verilecektir.

I. Durum: $m \mid n$ olsun.

2.1.9.Tanım: $Z\big(IF_q[x,\theta]\big) = \big\{f \in IF_q[x,\theta] \mid \forall p \in IF_q[x,\theta] \text{ için } p.f = f.p\big\}$

kümesine $IF_q[x,\theta]$ skew polinom halkasının merkezi , f skew polinomuna merkezi eleman adı verilir.

2.1.10 Teorem: IF_q sonlu bir cisim,

$$IF_q{}^{\theta} = \big\{a \in IF_q \mid \theta(a) = a\big\}$$

alt cismi olsun.$p \in IF_q[x,\theta]$ elemanının merkezi eleman olması için gerek ve yeter koşul m, θ otomorfizmasının mertebesi olmak üzere

$$p = \sum_{i=0}^{s} c_i x^{im} \in IF_q{}^{\theta}[x]$$

olmasıdır.

Ayrıca $IF_q[x,\theta]$ halkasının merkezi elemanları, $IF_q[x,\theta]$ halkasının ideallerinin üreteçleridir. (Boucher,Geiselmann, Ulmer,2007)

2.1.11 Lemma: $x^n - 1 \in Z\big(IF_q[x,\theta]\big)$ olması için gerek ve yeter koşul $m \mid n$ olmasıdır.(Şiap, *Abualrub, Aydın, Seneviratne*,2010)

İspat: $m \mid n$ ve $f(x) = a_0 + a_1 x + \cdots + a_r x^r \in IF_q[x,\theta]$ olsun. $\forall a \in IF_q$ için $\theta^m(a) = a$. Böylece

$$\begin{aligned}(x^n-1).f(x) &= (x^n-1).(a_0 + a_1x + \cdots + a_rx^r)\\ &= x^n a_0 + x^n a_1 x + \cdots + x^n a_r x^r - (a_0 + a_1x + \cdots + a_rx^r)\\ &= \theta^n(a_0)x^n + \theta^n(a_1)x^n x + \cdots + \theta^n(a_r)x^n x^r - (a_0 + a_1x + \cdots + a_rx^r)\\ &= a_0 + a_1x^n x + \cdots + a_r x^n x^r - (a_0 + a_1x + \cdots + a_rx^r)\\ &= (a_0 + a_1x + \cdots + a_rx^r)x^n - (a_0 + a_1x + \cdots + a_rx^r)\\ &= f(x).x^n - f(x)\\ &= f(x).(x^n-1)\end{aligned}$$

$O\ halde\ x^n - 1 \in Z\big(IF_q[x,\theta]\big)$

Tersine $x^n - 1 \in Z\big(IF_q[x,\theta]\big)$ olsun. Böylece $\forall a \in IF_q$ için

$$(x^n-1).a.x^m = a.x^m.(x^n-1)$$

olur.

$$(x^n-1).a.x^m = \theta^n(a).x^{n+m} - a.x^m \quad \boxed{\text{I}}$$

$$a.x^m.(x^n-1) = a.x^{n+m} - a.x^m \boxed{\text{II}}$$

$\boxed{\text{I}}$ ve $\boxed{\text{II}}$ den $\theta^n(a) = a$ olur. θ nın mertebesi m idi. Böylece $m \mid n$ olur.

2.1.12 Önerme: R_r polinomu, P polinomunun $x^n - 1$ polinomu ile sağdan bölümü sonucu elde edilen kalan olmak üzere

$$\begin{aligned}\Psi : IF_q[x,\theta] &\longrightarrow IF_q[x,\theta]/< x^n - 1 >\\ P &\longmapsto \Psi(P) = R_r\end{aligned}$$

şeklinde tanımlanan dönüşüm bir morfizmadır.(Boucher,Geiselmann, Ulmer,2007)

2.1.13 Lemma: IF_q sonlu bir cisim, θ, IF_q üzerinde tanımlı mertebesi m olan aşikar olmayan otomorfizma bir olsun. $m \mid n$ olmak üzere

$$IF_q[x,\theta]/< x^n - 1 >$$

halkası esas sol ideal halkasıdır ve $IF_q[x,\theta]/< x^n - 1 >$halkasının sol idealleri, G, $x^n - 1 \in IF_q[x,\theta]$ polinomun sağ böleni olmak üzere $\Psi(G)$ tarafından üretilir.(Boucher,Geiselmann, Ulmer,2007)

İspat: I, $IF_q[x,\theta]/< x^n - 1 >$ halkasının bir sol ideali olsun. $I = \{0\}$ ise ispat aşikardır. $I \neq \{0\}$ olsun.

$\tilde{G} \in I$, I da sıfırdan farklı en küçük dereceli monik polinom olsun, Ψ nin tanımından $\tilde{G} \in IF_q[x,\theta]$ için $\Psi(\tilde{G}) = \tilde{G}$ dir.

Gerçekten;

$$\tilde{G} = Q_r(x^n - 1) + R_r \Longrightarrow \tilde{G} = 0 + R_r \Longrightarrow \tilde{G} = R_r$$

ve $\deg(\tilde{G}) < n$ dir.

$$\begin{gathered} \forall \tilde{p} \in I \Longrightarrow \tilde{p} = Q_r.\tilde{G} + R_r \quad \deg Q_r < \deg \tilde{G} < n \\ \Longrightarrow \Psi(\tilde{p}) = \Psi(Q_r).\Psi(\tilde{G}) + \Psi(R_r) \\ \Longrightarrow \tilde{p} = \Psi(Q_r).\tilde{G} + R_r \\ \Longrightarrow R_r = \tilde{p} - \Psi(Q_r).\tilde{G} \in I \end{gathered}$$

$\tilde{G}$ nin en küçük olması ile çelişir. Bu nedenle $R_r = \Psi(R_r) = 0$ olmalıdır.

$$\begin{gathered} \Longrightarrow \tilde{p} = \Psi(Q_r).\tilde{G} \\ \Longrightarrow I =< \tilde{G} > \end{gathered}$$

olur. $\tilde{G}$, $x^n - 1$ in sağ böleni mi?

$$x^n - 1 = Q_r.\tilde{G} + R_r\,, \qquad \ni \deg R_r < \deg \tilde{G}$$

olacak şekilde $\exists Q_r, R_r$ $elemanları\, vardır. x^n - 1$ ve $\tilde{G} \in I$ olduğundan $R_r \in I$ olur. $\tilde{G}$ polinomu en küçük dereceli idi. Bu durumda $R_r = 0$ olur.

$$x^n - 1 = Q_r.\tilde{G}$$

O halde $\tilde{G}$, $x^n - 1$ in sağ böleni olur.

(Sağ ideal için de benzer şekilde ispat yapılır.)

2.1.14Önerme:

$$\pi \quad : \quad IF_q^n \longrightarrow IF_q[x,\theta]/< x^n - 1 >$$
$$a = (a_0, a_1, \dots, a_{n-1}) \longmapsto \pi(a) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + \langle x^n - 1\rangle$$

şeklinde tanımlanan dönüşüm bir izomorfizmadır.

Bu dönüşüm yardımıyla $a = (a_0, a_1, \dots, a_{n-1})$ vektörünü kısaca

$$\pi(a) = \overline{a(x)} = \overline{a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}} \in IF_q[x,\theta]/< x^n - 1 >$$

ile göstereceğiz.

2.1.15 Teorem: θ, IF_q sonlu cismi üzerinde tanımlı mertebesi m olan aşikar olmayan bir otomorfizma ve C, IF_q üzerinde tanımlı n uzunluklu bir lineer kod olsun. Eğer $m \mid n$ ise C, θ-cyclic (skew cyclic) olması için gerek ve yeter koşul $\pi(C)$ nin $IF_q[x,\theta]/< x^n - 1 >$ halkasının bir sol ideali olmasıdır. (Boucher,Geiselmann, Ulmer,2007)

$$C \subseteq IF_q^n \quad \leftrightarrow \quad \pi(C) \subseteq IF_q[x,\theta]/< x^n - 1 >$$

skew cylic kod sol ideal

İspat: C, θ-cyclic kod olsun. Bu durumda $her\ c = (c_0, c_1, \dots, c_{n-1}) \in C$ iken $\big(\theta(c_{n-1}), \theta(c_0), \dots, \theta(c_{n-2})\big) \in C$ dir.

C lineer kod olduğundan $\forall \overline{f(x)} \in \pi(C)$ ve $\forall \overline{r(x)} \in IF_q[x,\theta]/< x^n - 1 >$ için $\overline{r(x).f(x)} \in \pi(C)$ olduğunu göstermemiz gerekir.$\overline{f(x)} = \overline{a_0 + \cdots + a_{n-1}x^{n-1}}$olsun.

$$\begin{aligned} \bar{x}.\overline{f(x)} &= \bar{x}.\left(\overline{a_0 + \cdots + a_{n-1}x^{n-1}}\right) \\ &= \overline{x.a_0 + x.a_1.x \dots + x.a_{n-1}.x^{n-1}} \\ &= \theta(a_0)x + \theta(a_1)x^2 + \cdots + \theta(a_{n-1})x^n \end{aligned}$$

C, θ-cyclic kod olduğundan $\bar{x}.\overline{f(x)} \in \pi(C)$ dir. Bu şekilde devam edilirse

$$\begin{aligned} \bar{x^\iota}.\overline{f(x)} &= \bar{x^\iota}.\left(\overline{a_0 + \cdots + a_{n-1}x^{n-1}}\right) \\ &= \overline{x^\iota.a_0 + x^\iota.a_1.x \dots + x^\iota.a_{n-1}.x^{n-1}} \\ &= \theta^i(a_{n-i}) + \theta^i(a_{n-i+1})x + \cdots + \theta(a_{n-i-1})x^{n-1} \in \pi(C) \end{aligned}$$

$\forall \overline{r(x)} \in IF_q[x,\theta]/< x^n - 1 >$,$\forall \overline{f(x)} \in \pi(C)$ için $\overline{r(x).f(x)} \in \pi(C)$ olduğundan $\pi(C) \subset IF_q[x,\theta]/< x^n - 1 >$ sol ideal olur.

Tersine $\pi(C)$ sol ideal olsun.$\forall c = (a_0, a_1, \dots, a_{n-1}) \in C$için

$$\overline{a(x)} = \overline{a_0 + \cdots + a_{n-1}x^{n-1}} \in \pi(C)$$

olur. Yani;

$$\begin{aligned} \bar{x}.\overline{a(x)} &= \bar{x}.\left(\overline{a_0 + a_1x + \cdots + a_{n-1}x^{n-1}}\right) \\ &= \overline{xa_0 + xa_1x + \cdots + xa_{n-1}x^{n-1}} \\ &= \overline{\theta(a_0)x + \theta(a_1)x^2 + \cdots + \theta(a_{n-1})x^n} \in \pi(C) \\ \leftrightarrow &\left(\theta(a_{n-1}), \theta(a_0), \theta(a_1), \dots, \theta(a_{n-2})\right) \in C \text{ olur.} \end{aligned}$$

Bu durumda C, $(skew\ cyclic)$ θ $-$cyclic koddur.

2.1.16 Not: i)$f, x^n - 1$ polinomunun derecesi n-k olan bir sağ böleni olmak üzere (f) sol ideali , $[n, k]$ parametreli bir lineer koda karşılık gelir.

ii) $IF_q[x, \theta]$ halkası tek türlü asal çarpanlarına ayrılabilen bölge değildir. Dolayısıyla $x^n - 1$ polinomunun çok fazla sağ çarpanı ve sağ çarpanlar tarafından üretilen sol idealler vardır. IF_q üzerinde tanımlı bir cyclic koda karşılık gelen $x^n - 1$ polinomunun bir böleni tarafından üretilen $IF_q[x]/< x^n - 1 >$ halkasının bir ideali var olduğundan dolayı, skew cyclic kodların oluşturduğu sınıf, cyclic kodların oluşturduğu sınıftan daha büyüktür.

2.1.17 Örnek:α, $p(x) = x^2 + x + 1$ polinomunun bir kökü olmak üzere $IF_4 \cong IF_2[x]/< x^2 + x + 1 > \cong \{0,1, \alpha, \alpha^2\}$ sonlu bir cisim ve θ

$$\begin{aligned} \theta: IF_4 &\longrightarrow IF_4 \\ s &\longmapsto s^2 \end{aligned}$$

şeklinde tanımlı bir otomorfizma olmak üzere $x^4 + 1 \in IF_4[x, \theta]$ polinomunun 2.dereceden tüm çarpanları aşağıdaki gibidir.

$$\begin{aligned} x^4 + 1 &= (x^2 + 1).(x^2 + 1) \\ &= (x^2 + \alpha x + \alpha).(x^2 + \alpha^2 x + \alpha) \\ &= (x^2 + \alpha^2 x + \alpha^2).(x^2 + \alpha^2 x + \alpha) \\ &= (x^2 + \alpha^2 x + \alpha).(x^2 + \alpha^2 x + \alpha^2) \\ &= (x^2 + \alpha x + \alpha^2).(x^2 + x + \alpha) \end{aligned}$$

■

2.2 Sonlu Cisimler Üzerinde Tanımlı θ −kodlar

$D.Boucher$ ve $F.Ulmer$ tarafından "Coding with skew polynomial rings" adlı makalede, daha önce $W.Gieselman$ ile skew cyclic kodu tanımladıkları

çalışmada yer alan $x^n - 1$ polinomu yerine derecesi n olan bir $f \in IF_q[x,\theta]$ polinomu alınarak merkezi θ −kod kavramı tanımlanmıştır.

$$C \subseteq IF_q^n \quad \leftrightarrow \quad \pi(C) \quad \subseteq \quad IF_q[x,\theta]/(f)$$

merkezi θ −kodu sol ideal

2.2.1 Teorem: θ, IF_q üzerinde tanımlı aşikar olmayan bir otomorfizma $f \in IF_q[x,\theta]$, $\deg f = n$ olan bir polinom olmak üzere $I = (f)$, $IF_q[x,\theta]$ halkasının bir ideali olsun. $\overline{a(x)} = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1}$, $IF_q[x,\theta]/(f)$ halkasının bir J sol idealinin elemanları olmak üzere elemanları $a = (a_0, a_1, \dots, a_{n-1})$ şeklinde olan IF_q üzerinde tanımlı n uzunluğunda bir $\theta - kod$ vardır.

2.2.2.Tanım: C , $IF_q[x,\theta]/(f)$ halkasının bir J sol idealine karşılık gelen $\theta - kod$ ve g , f polinomunun bir sağ böleni olsun

i) $f \in Z(IF_q[x,\theta])$ olmak üzere $J = \{gt + (f) |\ t \epsilon IF_q[x,\theta]\}$ sol idealine karşılık gelen θ −koda merkezi θ −kod adı verilir.

ii) θ otomorfizmasının mertebesi m , $f = x^n - 1$ ve $m \mid n$ olmak üzere $J = \{gt + (f) |\ t \epsilon IF_q[x,\theta]\}$ sol idealine karşılık gelen θ −koda θ-cyclic kod (skew cyclic kod) adı verilir.

2.2.3 Önerme: (f) ideal olmak üzere $g = g_r x^r + \cdots + g_0$ polinomu, derecesi n olan bir $f \in IF_q[x,\theta]$ polinomunun bir böleni olsun. g ile üretilen sol ideale karşılık gelen [n,n-r] parametreli θ −kod'un üreteç matrisi

$$G = \begin{bmatrix} g_0 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & g_r & 0 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 0 \\ 0 & \theta(g_0) & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \theta & (g_r) & \dots & \dots & \dots & \dots & 0 \\ \vdots & & \vdots & & \vdots & & \vdots & & \vdots & & \vdots \\ 0 & 0 & \dots & \dots & \dots & 0 & \dots & \dots & \theta^{n-r-1}(g_0) & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \theta^{n-r-1}(g_r) \end{bmatrix}$$

şeklindedir.$(Boucher, Ulmer, 2008)$

2.2.4Örnek: α, $p(x) = x^2 + x + 1$ polinomunun bir kökü olmak üzere $IF_4 \cong IF_2[x]/< x^2 + x + 1 > \cong \{0,1,\alpha,\alpha^2\}$ sonlu bir cisim, θ , IF_4 sonlu cismi üzerinde tanımlı bir otomorfizması olmak üzere $IF_4[x,\theta]$ skew polinom halkası verilsin. $x^2 + \alpha x + 1 \epsilon IF_4[x,\theta]$ polinomu tarafından üretilen $IF_4[x,\theta]/< x^4 + x^2 + 1 >$ halkasının bir sol idealine karşılık gelen $d_H(C) = 2$ olan cyclic olmayan C lineer kodunu ele alalım.

$\overline{a(x)} = a_0 + a_1x + a_2x^2 + a_3x^3 \in \pi(C)$ iken $\overline{x}.\overline{a(x)} \in \pi(C)$ dir.

$$\bar{x}.\overline{a(x)} = \overline{x.a_0 + x.a_1x + x.a_2x^2 + x.a_3x^3}$$
$$= \overline{\theta(a_0)x + \theta(a_1)x^2 + \theta(a_2)x^3 + \theta(a_3)x^4}$$
$$= \overline{\theta(a_3) + \theta(a_0)x + \big(\theta(a_1) + \theta(a_3)\big)x^2 + \theta(a_2)x^3}$$

Yani;

$$(a_0, a_1, a_2, a_3) \in C \Longrightarrow \big(\theta(a_3), \theta(a_0), \theta(a_1) + \theta(a_3), \theta(a_2)\big) \in C$$

dir. O halde C, merkezi θ −kod ama θ −cyclic kod değildir.

2.2.5Lemma: $f = x^n - 1 \in IF_q[x, \theta]$ idealin üreteci olsun. $\deg g < n - 1$ olmak üzere f polinomunun monik bir g sağ böleni tarafından üretilen θ −cyclic kodun cyclic olabilmesi için gerek ve yeter koşul $IF_q^{\theta} = \{a \in IF_q \mid \theta(a) = a\}$ olmak üzere $g \epsilon IF_q^{\theta}[x]$ olmasıdır. $(Boucher, Ulmer, 2008)$

2.2.6 Örnek: α, $p(x) = x^2 + x + 1$ polinomunun bir kökü olmak üzere $IF_4 \cong IF_2[x]/< x^2 + x + 1 > \cong \{0,1,\alpha,\alpha^2\}$ sonlu bir cisim, $IF_4[x, \theta]$ skew polinom halkası ve θ Frobenius otomorfizması olsun. $x^4 + x^2 + 1 \in IF_4[x, \theta]$ nın beş farklı çarpanlara ayrılışı vardır ve aşağıdaki gibidir.

$$x^4 + x^2 + 1 = (x^2 + x + 1).(x^2 + x + 1)$$
$$= (x^2 + \alpha^2).(x^2 + \alpha)$$
$$= (x^2 + \alpha).(x^2 + \alpha^2)$$
$$= (x^2 + \alpha^2x + 1).(x^2 + \alpha^2x + 1)$$
$$= (x^2 + \alpha x + 1).(x^2 + \alpha x + 1)$$

2.2.7Lemma: $h.g \in Z\big(IF_q[x, \theta]\big)$ ise $h.g = g.h \in IF_q[x, \theta]$ dır.

$(Boucher, Ulmer, 2008)$

İspat: $h.g \in Z\big(IF_q[x, \theta]\big) \Longrightarrow \forall p \in IF_q[x, \theta]$ için $(h.g).p = p.(h.g)$ dir.

$p = h$ seçersek

$$(h.g).p = p.(h.g) \underbrace{\Longrightarrow}_{p=h} (h.g).h = h.(h.g) = h.(g.h)$$

olur. $\therefore hg = gh$

2.2.8Lemma: $h.g \in Z\big(IF_q[x, \theta]\big)$ olmak üzere C, $IF_q[x, \theta]/< h.g >$ halkasının g ile üretilmiş sol idealine karşılık gelen merkezi θ −kod olsun.

$$a = (a_0, \dots, a_{n-1}) \in C \Leftrightarrow a(x).h = 0$$

dir. $(Boucher, Ulmer, 2008)$

İspat:C, $< g >$ sol idealine karşılık gelen kod olduğundan $a \in C$ ise $a(x) = s.g$ olacak şekilde bir s $\epsilon\, IF_q[x,\theta]/< h.g >$ vardır.

$$a(x) = s.g \Longrightarrow a(x).h = (s.g).h = s.(g.h) = s.(h.g) = 0 \in IF_q[x,\theta]/< hg >$$

Tersine;

$$\begin{aligned} a(x).h = 0 \in IF_q[x,\theta]/< hg > \Longrightarrow a(x).h &= f.(h.g) \quad ,\exists f \\ &= f.(g.h) \\ &= (f.g).h \in IF_q[x,\theta]/< hg > \\ \Longrightarrow a(x) &= f.g \end{aligned}$$

Bu durumda $a \in C$ elde edilir.

2.2.9 Lemma: $m,\ \theta$ otomorfizmasının mertebesi olmak üzere $m \mid n$ olsun. $x^n - 1 = h.g \in Z\big(IF_q[x,\theta]\big)$ ve C, g ile üretilen $IF_q[x,\theta]/< x^n - 1 >$ halkasının sol idealine karşılık gelen $\theta -$ cyclic kod olsun. Eğer $g = g_0 + g_1 x + \cdots + g_r x^r$ ve $h = h_0 + h_1 x + \cdots + h_{n-r} x^{n-r}$ ise C nin parity kontrol matrisi

$$H = \begin{bmatrix} h_{n-r} & \dots & \dots \theta^{n-r-1}(h_1)\theta^{n-r}(h_0) & 0 \dots \dots \dots \dots \dots \dots \dots \dots \dots 0 \\ 0 & \theta(h_{n-r}) \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots . \theta^{n-r+1}(h_0) \dots \dots & \dots \dots 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 \dots \dots \dots 0. \dots \dots \theta^{r-1}(h_{n-r}) \dots \dots \dots \dots \dots \dots . \dots \dots \theta^{n-1}(h_0) \end{bmatrix}$$

dir. $(Boucher, Ulmer, 2008)$

İspat:2.2.8 Lemma kullanılırsa

$$a \in C \Longrightarrow a(x).h = 0 \in IF_q[x,\theta]/< x^n - 1 >$$

dir. $k = n - r,\ C$ nin boyutu olmak üzere $\deg a(x).h < n + k$ olduğu için $x^k, x^{k+1}, \dots, x^{n-1}$ in katsayıları sıfırdır.

$l \in \{0,1, \dots, r-1\}$ olmak üzere $x^{l+k}\ in$ katsayıları

$$\sum_{i=l}^{l+k} a_i \theta^i(h_{l+k-i})$$

şeklindedir.

$a = (a_0, \dots., a_{n-1}) \in C$ olduğundan $H.[a_0 \dots. a_{n-1}]^t = 0$ dolayısıyla C nin duali $C^{\perp}$, H tarafından üretilir. $C^{\perp}$ nin boyutu $n - \dim(C) = r$ yani H ın satırlarının sayısıdır. H, C nin dualinin üreteç matrisidir.

2.2.10 Sonuç: m|n olsun. $h.g = x^n - 1 \in Z(IF_q[x,\theta])$ olmak üzere $IF_q[x,\theta]$ $halkasının$ $g = \sum_{i=0}^{r} g_i x^i$ ve $h = \sum_{i=0}^{n-r} h_i x^i$ iki elemanı olsun. g ile üretilen sol ideale karşılık gelen θ −cyclic kodunun duali

$$g^{\perp} = h_{n-r} + \theta(h_{n-r-1})x + \cdots . + \theta^{n-r}(h_0)x^{n-r}$$

ile üretilen, bir θ −cyclic koda karşılık gelir. $(Boucher, Ulmer, 2008)$

2.2.11 Örnek:$IF_4[x,\theta]$ skew polinom halkası, θ Frobenius otomorfizması ve $IF_4^* =< \alpha >$ olsun. $g = x^2 + \alpha x + \alpha^2 \in IF_4[x,\theta]$, $h = x^2 + \alpha x$ ve $g.h = x^4 - 1$ olmak üzere

$$g^{\perp} = \theta^2(\alpha)x^2 + \theta(\alpha)x + 1 = \alpha x^2 + \alpha^2 x + 1$$

dir. $\alpha^2.g^{\perp} = g$olduğundan g ile üretilen $IF_4[x,\theta]/< x^4 - 1 >$nin sol ideali Euclidean self-dual koddur.

II.Durum: $m \nmid n$ olsun.

$m \nmid n$ ise $R_n = IF_q[x,\theta]/< x^n - 1 >$ kümesi, toplama ve her $r(x) \in IF_q[x,\theta]$ ve her $f\ (x) + \langle x^n - 1\rangle \in R_n$ için

$$r(x).(f(x) + \langle x^n - 1\rangle) = r(x).f(x) + \langle x^n - 1\rangle$$

işlemine göre bir sol $IF_q[x,\theta]$ −modüldür.

2.2.12 Önerme:

$$\pi: IF_q^n \longrightarrow R_n = IF_q[x,\theta]/< x^n - 1 >$$
$$a = (a_0, \ldots, a_{n-1}) \longmapsto \pi(a) = \overline{a(x)} = a_0 + \cdots + a_{n-1}x^{n-1} + < x^n - 1 >$$

şeklinde tanımlanan dönüşüm bir izomorfizmadır.

2.2.13 Teorem:C, IF_q üzerinde n uzunluğuna sahip bir skew cyclic kod olması için gerek ve yeter koşul $\pi(C)$ nin $R_n = IF_q[x,\theta]/< x^n - 1 >$in bir sol $IF_q[x,\theta]\_$ alt modül olmasıdır. (Şiap,Abualrub,Aydın,Seneviratne,2010)

$$C \subseteq IF_q^n \quad \leftrightarrow \quad \pi(C) \subseteq \quad IF_q[x,\theta]/< x^n - 1 >$$

skew cylic kod sol $IF_q[x,\theta]\_$ alt modül

İspat:C, IF_q üzerinde n uzunluğunda bir skew cyclic kod olsun. Her $(a_0, a_1, \ldots, a_{n-1}) \in C$ için

$$\overline{f(x)} = \overline{a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}} \in \pi(C)$$

dir. C, skew cyclic kod olduğu için $(a_0, a_1, \dots, a_{n-1}) \in C$ iken

$$\big(\theta(a_{n-1}), \theta(a_0), \theta(a_1), \dots, \theta(a_{n-2})\big) \in C$$

dir. Yani;

$$\begin{aligned} x.\overline{f(x)} &= x.\big(\overline{a_0 + a_1x + \cdots + a_{n-1}x^{n-1}}\big) \\ &= \overline{xa_0 + xa_1x + \cdots + xa_{n-1}x^{n-1}} \\ &= \overline{\theta(a_{n-1}) + \theta(a_0)x + \cdots + \theta(a_{n-2})x^{n-1}} \\ &\leftrightarrow (\theta(a_{n-1}), \theta(a_0), \dots, \theta(a_{n-2})) \end{aligned}$$

...

$$x^i.\overline{f(x)} = \theta^i(a_{n-i}) + \cdots + \theta^i(a_{n-i-1})x^{n-1}$$

$$\leftrightarrow (\theta^i(a_{n-i}), \dots, \theta^i(a_{n-i-1}))$$

C, lineer olduğu için $\forall r(x) \in IF[x, \theta]$ için $r(x).\overline{f(x)} \in \pi(C)$. Bu durumda $\pi(C)$ bir sol $IF_q[x, \theta]$ −alt modüldür.

Tersine $\pi(C)$ bir sol $IF_q[x, \theta]$ −alt modül olsun.

$\forall(c_0, c_1, \dots, c_{n-1}) \in C$ için $\overline{f(x)} = \overline{c_0 + c_1x + \cdots + c_{n-1}x^{n-1}} \in \pi(C)$ dir. Varsayımdan $x \in IF_q[x, \theta]$ için

$$\begin{aligned} x.\overline{f(x)} &= x.\big(\overline{c_0 + c_1x + \cdots + c_{n-1}x^{n-1}}\big) \\ &= \overline{\theta(c_{n-1}) + \theta(c_0)x + \cdots + \theta(c_{n-2})x^{n-1}} \in \pi(C) \end{aligned}$$

Yani $\big(\theta(c_{n-1}), \theta(c_0), \dots, \theta(c_{n-2})\big) \in C$ dir. Yani C, skew cyclic koddur.

2.2.14 Lemma: $\pi(C)$, bir sol $IF_q[x, \theta]$ −alt modül olsun. Bu durumda $\pi(C)$, $f(x) \in IF_q[x, \theta]$ en küçük dereceli monik bir polinom olmak üzere $\overline{f(x)}$ tarafından üretilmiştir. (Şiap, Abualrub, Aydın, Seneviratne, 2010)

İspat: $\overline{f(x)} \in \pi(C)$ olmak üzere $f(x)$ en küçük dereceli dereceli bir polinom olsun.

$Her\ c(x) \in \pi(C)$ için sağ bölme algoritmasıyla

$c(x) = q(x).\overline{f(x)} + r(x), r(x) = 0$ veya $\deg r(x) < \deg f(x)$

olacak şekilde tek şekilde tanımlı $q(x)$ ve $r(x)$ polinomları vardır. O halde

$$c(x) = q(x).f(x) + r(x) \underbrace{\Rightarrow}_{\text{varsayımdan}} r(x) = c(x) - \overline{q(x).f(x)} \in \pi(C)$$

olur. $f(x)$ en küçük dereceli olacağı için $r(x) = 0$ olmalıdır. O halde $c(x) = q(x).\overline{f(x)}$ olur ve $\pi(C) =< \overline{f(x)} >$ dir.

2.2.15 Teorem: $\pi(C) =< \overline{f(x)} >$ olsun. Bu durumda $f(x)$, $x^n - 1$ in bir sağ bölenidir.(Şiap,Abualrub,Aydın,Seneviratne,2010)

İspat: $f(x)$ en küçük dereceli bir monik polinom olsun. $x^n - 1$ polinomunu $f(x)$ ile sağdan bölersek

$$x^n - 1 = q(x).f(x) + r(x), \qquad \deg r < \deg f \ \ veya \ \ r(x) = 0$$

olacak şekilde q ve r polinomları vardır.

$f(x)$ en küçük dereceli monik bir polinom olduğu için $r(x) = 0$ olmalıdır. O halde

$$x^n - 1 = q(x).f(x)$$

olur ve $f(x)$, $x^n - 1$ in bir sağ bölenidir.

Skew Cyclic Kodların Cyclic ve Quasi Cyclic Kodlarla İlişkisi

2.2.16 Lemma: $a, b \epsilon Z$ olmak üzere $a \ ve \ b$ elemanlarının en büyük ortak böleni vardır ve $d = (a, b)$ ise

$$d = ax + by$$

olacak şekilde en az bir $x, y \in \mathbb{Z}$ bulunabilir.

2.2.17 Not: Fakat bu yazılış tek türlü değildir. $En \ az \ bir \ k \in \mathbb{Z}$ için

$$x_0 = x - k.\frac{b}{(a,b)} \quad \text{ve} \quad y_0 = y - k.\frac{a}{(a,b)}$$

alınırsa

$$\begin{aligned} ax_0 + by_0 &= ax - k.\frac{ab}{(a,b)} + by - k.\frac{ab}{(a,b)} \\ &= ax + by \\ &= d \end{aligned}$$

sağlanır.

2.2.18Teorem: C, n uzunluğunda IF_q üzerinde tanımlı bir skew cyclic kod ve θ, IF_q cismi üzerinde tanımlı mertebesi $|< \theta >| = m$ olan aşikar olmayan bir

otomorfizma olsun. Eğer $(m,n)=1$ ise bu durumda C, n uzunluğunda bir cyclic koddur.(Şiap,Abualrub,Aydın,Seneviratne,2010)

İspat: C, n uzunluğunda, IF_q üzerinde bir skew cyclic kod ve $(m,n)=1$ olsun. $\forall(c_0,c_1,\dots,c_{n-1})\in C$ için $\overline{c_0+c_1x+\cdots+c_{n-1}x^{n-1}}\in\pi(C)$ olsun.

$$\begin{aligned}(m,n)=1 &\Longrightarrow \exists a_1,a_2 \ni 1=a_1m+a_2n\\ &\Longrightarrow a_1m=1-a_2n\\ &\Longrightarrow a_1m=1+Dn, \qquad \exists D\in IN\end{aligned}$$

yazabiliriz. Şimdi $\overline{c(x)}$ i, x^{a_1m} ile çarpalım.

$$\begin{aligned}x^{a_1m}.\overline{c(x)} &= x^{1+Dn}.\overline{(c_0+c_1x+\cdots+c_{n-1}x^{n-1})}\\ &= \theta^{a_1m}(c_0)x^{1+Dn}+\cdots+\theta^{a_1m}(c_{n-1})x^{Dn+n}\end{aligned}$$

$\forall a\in F$için$\theta^m(a)=a$ olduğu kullanılarak

$$x^{a_1m}.\overline{c(x)}=\overline{c_0x+c_1x^2+\cdots+c_{n-1}}\in\pi(C)$$

elde edilir. O halde $(c_{n-1},c_0,c_1,\dots,c_{n-2})\in C$ dir. Yani C, n uzunluğunda bir cyclic koddur.

2.2.19Sonuç: $(m,n)=1$ ve $f(x),\ x^n-1\in IF_q[x,\theta]$ polinomunun bir çarpanı ise $f(x),\ x^n-1\in IF_q[x]$ polinomunun da bir çarpanıdır.

2.2.20Teorem: C, IF_q üzerinde n uzunluğunda bir skew cyclic kod ve θ, IF_q cismi üzerinde mertebesi $|<\theta>|=m$ olan aşikar olmayan bir otomorfizma olsun. Eğer $(m,n)=d$ ise C uzunluğu n indeksi d olan quasi-cyclic koda denktir. (Şiap,Abualrub,Aydın,Seneviratne,2010)

İspat: C, $n=d.s$ uzunluğunda bir skewcyclic kod olsun.

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

için$\exists t$ için $\theta^t(c)\in C$ olduğunu göstermeliyiz.

$\forall c=\left(c_{0,0},c_{0,1},\dots,c_{0,d-1},c_{1,0},\dots,c_{s-1,0},\dots,c_{s-1,d-1}\right)\in C$ olsun. $(m,n)=d$ olduğundan $\exists a_1,a_2\in\mathbb{Z}\ni a_1m+a_2n=d.$

$$\begin{aligned}a_1m+a_2n=d &\Longrightarrow a_1m=d-a_2n\\ &\Longrightarrow a_1m=d+jn, \qquad \exists j\in\mathbb{Z}_+\end{aligned}$$

$c=\left(c_{0,0},c_{0,1},\dots,c_{0,d-1},c_{1,0},\dots,c_{s-1,0},\dots,c_{s-1,d-1}\right)\in C$ ye θ^{d+jn} uygulanırsa

$$\theta^{d+jn}\left(c_{0,0},c_{0,1},\dots,c_{s-1,d-1}\right)=\left(\theta^{d+jn}\left(c_{0,0}\right),\dots\theta^{d+jn}\left(c_{s-1,d-1}\right)\right)$$

$\forall a\in F$ için $\theta^{d+jn}(a)=\theta^{a_1m}(a)=a$ olduğundan

$$\theta^{d+jn}(c_{0,0}, c_{0,1}, \dots, c_{s-1,d-1}) = (c_{s-1,0}, c_{s-1,1}, \dots, c_{s-2,d-1}) \in C$$

dir. O halde C, n uzunluğunda indexi d olan bir quasi-cyclic koda denktir.

2.3 Sonlu $IF_2 + vIF_2$ Halkası Üzerinde Tanımlı Skew Cyclic Kodlar

2.3.1 Tanım: $v^2 = v$ olmak üzere $R = IF_2[v]/< v^2 - v >$,

kümesi aşağıda tanımlı $+$ ve $\cdot$ işlemlerine göre 4 elemanlı değişmeli bir halkadır.

+	0	1	v	$1+v$
0	0	1	v	$1+v$
1	1	0	$1+v$	v
v	v	$v+1$	0	1
$1+v$	$v+1$	v	1	0

$\cdot$	0	1	v	$1+v$
0	0	0	0	0
1	0	1	v	$1+v$
v	0	v	v	0
$1+v$	0	$1+v$	0	$1+v$

Bu halka *Bachoc* tarafından 1997 yılında tanımlanmıştır.

2.3.2 Teorem: R sonlu halkası üzerinde tanımlı θ otomorfizması $\theta(0) = 0$, $\theta(1) = 1$, $\theta(v) = v + 1$, $\theta(v + 1) = v$ olmak üzere

$$R[x, \theta] = \{f(x) = a_0 + a_1 x + \cdots + a_n x^n \mid \forall a_i \in R, i = 0, \dots, n, \quad n \in \mathbb{N}\}$$

skew polinom halkası verilsin. $R[x, \theta]/< x^n - 1 >$ polinomlar kümesi üzerinde tanımlı toplama ve $her\ \ r(x) \in R[x, \theta]$, her $f(x) + \langle x^n - 1\rangle \in R[x, \theta]/< x^n - 1 >$ için

$$r(x).(f(x) + \langle x^n - 1\rangle) = r(x).f(x) + \langle x^n - 1\rangle$$

şeklinde tanımlı çarpma işlemine göre bir sol $R[x, \theta]$ −modüldür.(Abualrub, Seneviratne,2010)

2.3.4 Önerme:

$$\pi : R^n \longrightarrow R[x, \theta]/< x^n - 1 >$$
$$(c_0, c_1, \dots, c_{n-1}) \mapsto \overline{c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}}$$

şeklinde tanımlanan dönüşüm bir izomorfizmadır.

2.3.5 Teorem: C, R üzerinde n uzunluğuna sahip bir skew cyclic kod olması için gerek ve yeter koşul $\pi(C)$ nin bir sol $R[x, \theta]$-alt modül olmasıdır.(Abualrub, Seneviratne,2010)

$$C \subseteq R^n \quad \leftrightarrow \quad \pi(C) \subseteq R\ [x,\theta]/< x^n - 1 >$$

skew cylic kod sol R$[x,\theta]$_ alt modül

2.3.6Teorem: C, n uzunluğunda R üzerinde bir skew cyclic kod ve $\overline{f(x)} \in \pi(C)$ olacak şekilde $f(x)$ en küçük dereceli bir polinom olsun. $f(x)$ monik ise $f(x)$, $x^n - 1$ in bir sağ böleni olmak üzere $\pi(C) =< \overline{f(x)} >$ dir.(Abualrub, Seneviratne,2010)

SKEW QUASI-CYCLIC KODLAR

Skew quasi cyclic kodlar ilk olarak 2010 yılında $T.Abualrub, A.Ghrayeb, N.Aydın$ ve $\text{İ.}Şiap$ tarafından sonlu cisimler üzerinde tanımlanmıştır.

2011 yılında $M.Bhaintwal$ tarafından Galois halkaları üzerinde skew quasi cyclic kodlar çalışılmıştır.

2.4 Sonlu Cisimler Üzerinde Tanımlı Skew Quasi Cyclic Kodlar

2.4.1 Tanım:p asal bir sayı, $t\epsilon\mathbb{Z}_+$, $q = p^{mt}$ olmak üzere IF_q, q elemanlı, karakteristiği p olan sonlu bir cisim ve θ, mertebesi m olan IF_q üzerinde tanımlı aşikar olmayan bir otomorfizma olsun. $n = s.l$ ve $m \mid s$ olmak üzere aşağıdaki koşullar sağlanıyorsa C ye n uzunluğunda l indeksli skew quasi cyclic kod (Skew l −Quasi Cyclic kod)adı verilir.

i) $C \subset IF_q^n$ alt uzayı

ii) $Her\ \ e = (e_{0,0}, e_{0,1}, \dots, e_{0,l-1}, e_{1,0}, \dots, e_{1,l-1}, \dots, e_{s-1,0}, \dots, e_{s-1,l-1}) \in C$ için

$$T_{\theta,s,l}(e) = \begin{pmatrix} \theta(e_{s-1,0}), \dots, \theta(e_{s-1,l-1}), \theta(e_{0,0}), \dots, \theta(e_{0,l-1}) \\ , \dots, \theta(e_{s-2,0}), \dots, \theta(e_{s-2,l-1}) \end{pmatrix} \in C$$

(θ aşikar otomorfizma ise skew quasi cyclic kod tanımı quasi cyclic kod tanımı ile çakışır.)

2.4.2 Teorem:$m \mid s$ ve $R_s = IF_q[x,\theta]/< x^s - 1 >$ olmak üzere R_s^l , toplama ve aşağıda tanımlanan çarpma işlemine göre bir sol R_s-modüldür.

$$\overline{f(x)}.(\overline{g_1(x)}, \overline{g_2(x)}, \dots, \overline{g_l(x)}) = (\overline{f(x).g_1(x)}, \overline{f(x).g_2(x)}, \dots \overline{f(x).g_l(x)})$$

(Abualrub, Ghrayeb, Aydın, Siap, 2010)

2.4.3 Teorem: $\overline{c_j(x)} = \sum_{i=0}^{s-1} c_{i,j}x^i \in IF_q[x,\theta]/< x^s - 1 >,\ j = 0,1,\dots,l-1$ olmak üzere

$$\emptyset \quad : \quad IF_q^{sl} \longrightarrow R_s^l$$
$$c = \left(c_{0,0},\dots,c_{0,l-1},\dots,c_{s-1,l-1}\right) \longmapsto \emptyset(c) = \left(c_0(x), c_1(x),\dots,c_{l-1}(x)\right)$$

şeklinde tanımlanan $\emptyset$ dönüşümü bir izomorfizmadır.(Abualrub, Ghrayeb, Aydın, Siap, 2010)

2.4.4Teorem: C, IF_q üzerinde $n = s.l$ uzunluğunda l indeksli skew quasi cyclic kod olması için gerek ve yeter şart $\emptyset(C)$ nin R_s^l halkasının bir sol R_s-alt modülü olmasıdır.(Abualrub, Ghrayeb, Aydın, Siap, 2010)

$$C \subseteq IF_q^n \qquad \leftrightarrow \qquad \emptyset(C) \ \subseteq R_s^l$$

l indeksli skew quasi-cylic kod sol R_s-alt modülü

İspat: C, skew quasi cyclic kod olsun. $\forall c = \left(c_{0,0},\dots,c_{0,l-1},\dots,c_{s-1,l-1}\right) \in C$ için $\emptyset(c) = \left(c_0(x), c_1(x),\dots,c_{l-1}(x)\right) \in \emptyset(C)$ dir.

$$\bar{x}.\emptyset(c) = \left(x.\overline{c_0(x)}, x.\overline{c_1(x)},\dots,x.\overline{c_{l-1}(x)}\right)$$
$$= \begin{pmatrix} \theta\left(c_{s-1,0}\right) + \theta\left(c_{0,0}\right)x + \dots + \theta\left(c_{s-2,0}\right)x^{s-1}, \theta\left(c_{s-1,1}\right) + \dots \\ +\theta\left(c_{s-2,1}\right)x^{s-1},\dots,\theta\left(c_{s-1,l-1}\right) + \dots + \theta\left(c_{s-2,l-1}\right)x^{s-1} \end{pmatrix}$$
$$\leftrightarrow \emptyset\begin{pmatrix} \theta\left(c_{s-1,0}\right),\theta\left(c_{0,0}\right),\dots,\theta\left(c_{s-2,0}\right),\theta\left(c_{s-1,1}\right),\dots \\ \theta\left(c_{s-2,1}\right),\dots,\theta\left(c_{s-1,l-1}\right)\dots,\theta\left(c_{s-2,l-1}\right) \end{pmatrix} \in \emptyset(C)$$

Bu şekilde devam edersek $\forall\overline{p(x)} \in R_s$ için $\overline{p(x)}.\emptyset(c) \in \emptyset(C)$. O halde, $\emptyset(C)$, R_s^l nin sol R_s alt modülüdür.

Tersine D, R_s^l nin sol $R_s - \ alt$ modülü ve $C = \emptyset^{-1}(D)$ olduğunu varsayalım.

$$C = \emptyset^{-1}(D) = \left\{c \in IF_q^n \mid \emptyset(c) \in D\right\}$$

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

O zaman $g_j(x) = \sum_{i=j}^{s-1} c_{i,j}x^i,\ j = 0,1,\dots,l-1$ olmak üzere

$\emptyset(c) = (\overline{g_0(x)},\dots,\overline{g_{l-1}(x)}) \in D$dir.

$$\emptyset\left(T_{\theta,s,l}(c)\right) = x.(\overline{g_0(x)},\dots,\overline{g_{l-1}(x)})$$
$$= \left(x\overline{g_0(x)},\dots,x\overline{g_{l-1}(x)}\right) \in D$$

olur. O halde $T_{\theta,s,l}(c) \in C$ elde edilir. Dolayısıyla C, skew quasi- cyclic koddur.

2.4.5 Not: Burada özellikle 1 üreteçli skew quasi cyclic kodlar incelenecektir. Bu üreteçli skew quasi koda karşılık gelen sol R_s-alt modülü

$$\emptyset(C) = \{\overline{f(x)}.G(x) \mid \overline{f(x)} \in R_s \; ve \; G(x) = (\overline{g_1(x)}, \dots, \overline{g_l(x)})\}$$

şeklinde ifade edilir.

2.4.6 Teorem: C, $n = s.l$ uzunluğunda l indeksli bir üreteçli skew quasi cyclic kod olsun. $g_i(x)$ polinomları $x^s - 1$ in bölenleri olmak üzere $\emptyset(C)$

$$(\overline{p_1(x)}.\overline{g_1(x)}, \overline{p_2(x)}.\overline{g_2(x)}, \dots, \overline{p_l(x)}.\overline{g_l(x)})$$

şeklindeki bir eleman tarafından üretilmiştir.(Abualrub, Ghrayeb, Aydın, Siap, 2010)

İspat:, $\emptyset(C)$, $(\overline{f_1}, \overline{f_2}, \dots, \overline{f_l})$ tarafından üretilsin . $1 \leq i \leq l$olmak üzere

$$\pi_i : \emptyset(C) \longrightarrow R_s$$
$$(k\overline{f_1}, k\overline{f_2}, \dots, k\overline{f_l}) \longmapsto \pi_i\left((k\overline{f_1}, k\overline{f_2}, \dots, k\overline{f_l})\right) = kf_i$$

şeklinde tanımlanan π_i fonksiyonu bir modül homomorfizmasıdır. $\pi_i(\emptyset(C))$, sol idealdir ve dolayısıyla R_s de bir skew cyclic koddur. Bu nedenle her $i = 1,2, \dots, l$ için $k.f_i \in \pi_i(\emptyset(C)) = (\overline{g_i})$ dir.

Böylece $g_i(x)$ ler $x^s - 1$ in bir böleni olmak üzere

$$\emptyset(C) = (\overline{p_1(x)}.\overline{g_1(x)}, \overline{p_2(x)}.\overline{g_2(x)}, \dots, \overline{p_l(x)}.\overline{g_l(x)})$$

şeklindedir.

2.4.7 Tanım :C, $n = s.l$ uzunluğunda indeksi l olan skew quasi cyclic kod,

$\emptyset(C) = (\overline{p_1(x)}.\overline{g_1(x)}, \overline{p_2(x)}.\overline{g_2(x)}, \dots, \overline{p_l(x)}.\overline{g_l(x)})$ olsun.

$$g(x) = \text{ebosolb}(p_1(x).g_1(x), p_2(x).g_2(x), \dots, p_l(x).g_l(x), x^s - 1)$$

şeklindeki tek monik polinomuna C skew quasi kodunun üreteci polinomu adı verilir.

2.4.8Tanım:$\overline{h(x)} = (\overline{p_1(x)}.\overline{g_1(x)}, \overline{p_2(x)}.\overline{g_2(x)}, \dots, \overline{p_l(x)}.\overline{g_l(x)}) =$ $(0,0, \dots ,0)$ olacak şekildeki en küçük dereceli monik $h(x)$ polinomuna C skew quasi kodunun kısmi kontrol polinomu denir.

2.4.9 Teorem: $d(x)$ polinomu,$f(x)$ ve $g(x)$ polinomlarının en büyük sağ ortak böleni olsun. Bu durumda

$$a(x).f(x) + b(x).g(x) = d(x)$$

olacak şekilde $a(x)$ ve $b(x)$ polinomları vardır. (Abualrub, Ghrayeb, Aydın, Siap, 2010)

İspat: $d(x)$, $f(x)$ ve $g(x)$ polinomlarının en büyük sağ ortak böleni olsun.

$$\big(f(x), g(x)\big)$$

tarafından üretilen sol ideali ele alalım. $IF_q\,[x,\theta]$ esas sol ideal halkası olduğundan

$$\big(h(x)\big) = \big(f(x), g(x)\big)$$

olacak şekilde $h(x)$ polinomu vardır. Böylece

$$f(x) = r_1(x).h(x) \qquad g(x) = r_2(x).h(x)$$

olur.

$d(x), f(x)$ ve $g(x)$ polinomlarının en büyük sağ ortak böleni olduğundan $d(x) = k(x).h(x)$ ve $\big(d(x)\big) \subset \big(h(x)\big)$ dir.

Aynı zamanda $\big(d(x)\big)$ sol ideal olmak üzere $f(x), g(x) \in \big(d(x)\big)$ yani $\big(h(x)\big) \subseteq \big(d(x)\big)$ dir. Bu durumda

$$\big(d(x)\big) = \big(f(x), g(x)\big) = \big(h(x)\big)$$

elde edilir.

Dolayısıyla

$$a(x).f(x) + b(x).g(x) = d(x)$$

olacak şekilde $a(x)$ ve $b(x)$ polinomları vardır.

Benzer şeyler en büyük ortak sol bölen içinde yapılır.

2.4.10 Sonuç: $d(x)$, polinomu $f(x)$ ve $g(x)$ polinomlarının en büyük sol ortak böleni olsun. Bu durumda

$$a(x).f(x) + b(x).g(x) = d(x)$$

olacak şekilde $a(x)$ ve $b(x)$ polinomları vardır.

2.4.11 Lemma: $g(x)$ ve $h(x)$, C skew quasi cyclic kodunun sırasıyla üreteç ve kısmi kontrol polinomları olsun. Bu durumda

$$x^s - 1 = h(x).g(x) = g(x).h(x)$$

dir.(Abualrub, Ghrayeb, Aydın, Siap, 2010)

İspat: $g(x)$ polinomu $p_1(x).g_1(x),\dots,p_l(x).g_l(x)$ ve x^s-1 polinomlarının en büyük sol ortak böleni olduğundan

$$x^s-1=g(x).k(x)$$

olacak şekilde bir $k(x)$ polinomu vardır. $x^s-1\in Z\left(IF_q[x,\theta]\right)$ olduğundan

$$x^s-1=g(x).k(x)=k(x).g(x)$$

dir. Bu durumda tüm $i=1,2,\dots l$ için

$$p_i(x).g_i(x)=g(x).a_i(x)$$

olacak şekilde $\overline{a_i(x)}\in R_s$ vardır. mod x^s-1e göre

$$k(x).\left(p_1(x).g_1(x),\dots,p_l(x).g_l(x)\right)=k(x).\left(g(x).a_1(x),\dots,g(x).a_l(x)\right)$$
$$=(0,0,\dots,0)$$

elde edilir. Böylece $k(x)=q(x).h(x)$ ve $\deg k(x)\geq \deg h(x)$ dir.

Sonuç 2.4.10 dan

$$p_1(x).g_1(x).a_1(x)+\cdots+(x^s-1).a_{l+1}(x)=g(x)$$

olacak şekilde $a_i(x)$ polinomları bulunabilir. Bu nedenle

$h(x).\left(p_1(x).g_1(x).a_1(x)+\cdots+(x^s-1).a_{l+1}(x)\right)=h(x).g(x)=0$ *ve dolayısıyla*

$$\deg h(x)\geq \deg\frac{x^s-1}{g(x)}$$

tir. O halde $k(x)=h(x)$tir.

2.5 Galois Halkaları Üzerinde Skew Quasi Cyclic Kodlar

2.5.1Tanım: $r\in\mathbb{Z}_+$, p asal sayı, $q=p^r$ ve $f(x)$, $\mathbb{Z}_q[x]$ halkasında ilkel bir polinom, $\deg f(x)=m$ ve $f(x)|x^{p^m-1}-1$ olmak üzere $\mathbb{Z}_q[x]/(f(x))$ halkasına $\mathbb{Z}_q$ üzerinde $m.inci$ dereceden Galois halkası denir ve GR(q,m) ile gösterilir. **2.5.2 Önerme:** $GR(q,m)$ Galois halkası yerel bir halkadır. $<p>$ maksimal idealidir ve IF_{p^m} rezidü cismidir.(Bhaintwal, 2011)

2.5.3 Önerme: $< p >$, $GR(q,m)$ Galois halkasının maksimal ideali olmak üzere

$$-: GR(q,m) \longrightarrow IF_{p^m} \cong GR(q,m)/< p >$$

izdüşüm dönüşümü $GR(q,m)[x]$ kümesine

$$-: GR(q,m)[x] \longrightarrow IF_{p^m}[x]$$

şeklinde genişletilir.(Bhaintwal, 2011)

2.5.4Tanım: $GR(q,m) = \mathbb{Z}_q[x]/(f(x))$ Galois halkası verilsin. ζ, $f(x)$ polinomunun kökü olmak üzere ζ elemanına $GR(q,m)$ halkasının ilkel elemanı denir.ζ, $(p^m - 1) - inci$ mertebeden bir elemandır. $T_m = \{0,1,\zeta, \dots \zeta^{p^m-2}\}$ kümesineTeichmüller kümesi denir.

2.5.5.Önerme:$GR(q,m)$ halkasının her bir elemanı, $c_i \in \mathbb{Z}_q$ olmak üzere

$$c = c_0 + c_1\zeta + c_2\zeta^2 + \cdots + c_{m-1}\zeta^{m-1}$$

şeklinde yazılır. θ, Frobenius otomorfizması olmak üzere

$$\theta(c) = c_0 + c_1\zeta^p + c_2\zeta^{2p} + \cdots + c_{m-1}\zeta^{(m-1)p}$$

dir.

$$\mathcal{A} = \{\tau \mid \tau: GR(q,m) \longrightarrow GR(q,m)\text{otomorfizma}\}$$

kümesi θ ile üretilmiş $m - inci$ dereceden bir gruptur.(Bhaintwal, 2011)

2.5.6Tanım: $\tau, GR(q,m)$ üzerinde tanımlı aşikar olmayan bir otomorfizma olsun.Polinomlar kümesi üzerinde tanımlı toplama ve $a, b \in GR(q,m)$ olmak üzere

$$\left(ax^i\right)\left(bx^j\right) = a\,\tau^i(b)x^{i+j}$$

şeklinde tanımlanan çarpma işlemine göre

$$\{a_0 + a_1x + \cdots + a_nx^n \mid a_i \in GR(q,m), i = 0,1,\dots,n,\ \ n \in \mathbb{N}\}$$

halkasına skew polinom halkası denir. $GR(q,m)[x,\tau]$ şeklinde gösterilir. Skew polinomlar halkası değişmeli olmayan bir halkadır.

2.5.7Önerme:$\bar{\tau}$,$\bar{\tau}(\bar{x}) = \overline{\tau(x)}$ olmak üzere IF_{p^m} üzerinde tanımlı bir otomorfizma olmak üzere

$$-: GR(q,m)[x,\tau] \longrightarrow IF_{p^m}[x,\bar{\tau}]$$

şeklinde tanımlanan dönüşüm bir halka morfizmasıdır.(Bhaintwal, 2011)

2.5.8 Önerme: r nin mertebesi t olsun. Bu durumda $r = \theta^d$ ve $m = t.d$ olacak şekilde t pozitif tamsayısı vardır.

$$GR(q,d) = \{a \in GR(q,m) \mid r(a) = a\}$$

dır.(Bhaintwal, 2011)

2.5.9Tanım:

$$Z(GR(q,m)[x,r]) = \{p \in GR(q,m)[x,r] \mid \forall f \in GR(q,m)[x,r] \; için \; p.f = f.p\}$$

kümesine $GR(q,m)[x,r]$ skew polinom halkasının merkezi denir.

2.5.10 Önerme: $GR(q,m)[x,r]$ kümesinin merkezi $\mathbb{Z}_q[x^m]$ ve $GR(q,m)[x,\theta]$ nin merkezi $GR(q,d)[x^t]$dir. (Bhaintwal, 2011)

2.5.11 Lemma: $g.h \in Z(GR(q,m)[x,r])$ ise $g.h = h.g$ dir. (Bhaintwal, 2011)

İspat:

$$g.h \in GR(q,m)[x,r] \Longrightarrow \forall p \in GR(q,m)[x,r] \text{için } (g.h).p = p.(h).g$$

dir. $p = g$ seçersek

$$(g.h).p = p.(h.g) \Longrightarrow (g.h).g = g.(h.g) = (g.h).g$$

o halde $g.h = h.g$ olur.

2.5.12Not: Sonlu cisimler üzerinde skew polinom halkaları ya sağ Euclidean bölge ya da sol Euclidean bölgesidir. Galois halkaları için aynı şey söz konusu değildir.

2.5.13 Teorem: $f, g \in GR(q,m)[x,r]$ ve g polinomunun baş katsayısı birim olmak üzere

$$f = qg + r \quad r = 0 \quad \text{ya da} \quad \deg r < \deg g$$

olacak şekilde $q, r \in GR(q,m)[x,r]$ vardır.(Bhaintwal, 2011)

İspat:

$$f = \sum_{i=0}^{d} a_i x^i \quad ve \quad g = \sum_{j=0}^{e} a_j x^j$$

ve b_e birimsel eleman olmak üzere

$$h = f - \frac{a_d}{r^{d-e}(b_e)}.x^{d-e}.g$$

ve derecesi f nin derecesinden daha küçüktür. h polinomunun derecesi g nin derecesinden küçük kalana kadar işlem tekrarlanırsa q ve r polinomları elde edilir. Üstelik g polinomunun baş katsayısı birim ise q ve r tek şekilde belirlenir.

2.5.14Tanım: r, $GR(q,m)$ üzerinde tanımlı aşikar olmayan bir otomorfizma olsun. $n = s.l$,r otomorfizmasının mertebesi t ve $t \mid s$ olmak üzere aşağıdaki koşullar sağlanıyorsa C ye n uzunluğunda l indeksli skew quasi kod ya da r −skew quasi cyclic kod adı verilir.

i) $C, GR(q,m)^n \; nin \; bir$ alt modülü

ii) $Her \;\; c = (c_{0,0}, c_{0,1}, \dots, c_{0,l-1}, c_{1,0}, c_{1,1}, \dots, c_{1,l-1}, \dots, c_{s-1,0}, \dots, c_{s-1,l-1}) \in C$ iken $T_{r,l}(c) = \begin{pmatrix} r(c_{s-1,0}), \dots, r(c_{s-1,l-1}), r(c_{0,0}), \dots, r(c_{0,l-1}) \\ , \dots, r(c_{s-2,0}), \dots, r(c_{s-2,l-1}) \end{pmatrix} \in C$

2.5.15 Önerme: Toplama ve $her \;\; v \in GR(q,m)^{ls}$ ve $her \;\; f(x) \in GR(q,m)[x,r]$ için $f(x).v = f(T_{r,l})v$ şeklinde tanımlanan çarpma işlemine göre $GR(q,m)^{ls}$, bir sol $GR(q,m)[x,r]$ −modüldür.(Bhaintwal, 2011)

2.5.16 Not: C, n uzunluğunda l indeksli skew quasi kod, $T_{r,l}(C) = C$ sağlayan $GR(q,m)^{ls}$ nın bir sol $GR(q,m)[x,r]$ −alt modülüdür.

2.5.16 Önerme: $j = 0,1, \dots, l-1$ için

$$\overline{c_j(x)} = \sum_{i=0}^{s-1} c_{i,j} x^i \in R_s$$

olmak üzere

$$\emptyset \quad : \quad GR(q,m)^{sl} \longrightarrow R_s^l$$
$$c = (c_{0,0}, \dots, c_{0,l-1}, \dots, c_{s-1,l-1}) \longmapsto \emptyset(c) = (c_0(x), c_1(x), \dots, c_{l-1}(x))$$

şeklinde tanımlı dönüşüm bir izomorfizmadır.

2.5.17 Teorem: C**,** $GR(q,m)$ üzerinde n=s.l uzunluğunda l indexli bir skew quasi-cyclic kod olması için gerek ve yeter koşul $R_s = {GR(q,m)[x,r]}/{< x^s - 1 >}$ olmak üzere $\emptyset(C)$ nin R_s^lnin bir sol R_s alt modül olmasıdır. (Bhaintwal, 2011)

$C \subseteq GR(q,m)^n \quad \leftrightarrow \quad \emptyset(C) \subseteq R_s^l$

l indeksli skew quasi-cylic kod sol R_s-alt modülü

SKEW CONSTACYCLIC KODLAR

Skew Constacyclic Kodlar ilk olarak 2008 yılında $D.Boucher,\ P.Sole$ ve $F.Ulmer$ tarafından Galois halkaları üzerinde tanımlanmıştır.

2009 yılında tarafından sonlu zincir halkalarına S. Jitman, S. Ling, P. Udomkavanich tarafından genelleştirilmiştir.

2.6 Galois Halkaları Üzerinde Tanımlı Skew Constacyclic Kodlar

2.6.1 Önerme:

$$\varphi: \mathbb{Z}_4 \longrightarrow \mathbb{Z}_2 \cong IF_2$$

$$\begin{aligned} \bar{0} &\mapsto \bar{0} \\ \bar{1} &\mapsto \bar{1} \\ \bar{2} &\mapsto \bar{0} \\ \bar{3} &\mapsto \bar{1} \end{aligned}$$

şeklinde tanımlanan dönüşüm bir homomorfizmadır. Bu dönüşüm

$$\bar{\varphi}: \mathbb{Z}_4[x] \longrightarrow \mathbb{Z}_2[x] \cong IF_2[x]$$
$$f = \sum_{i=0}^{n} a_i x^i \longmapsto \bar{\varphi}(f) = \sum_{i=0}^{n} \bar{a_i} x^i = \bar{f}$$

dönüşümüne genişletilir.(Boucher, Sole,Ulmer,2008)

2.6.2 Önerme: ζ elemanı,

$$\left({}^{IF_2[x]}\!/_{<\bar{h}>} \right)^* = <\zeta>$$

olacak şekilde $\bar{h} \in IF_2[x]$ ilkel, asal polinomunun bir kökü olsun. $\bar{\varphi}^{-1}(\bar{h}) = h \in \mathbb{Z}_4[x]$, $m - inci$ dereceden monik bir polinom olmak üzere

$${}^{\mathbb{Z}_4[x]}\!/_{<h>} \cong GR(4, m)$$

Galois halkasının her bir elemanı $0 \leq i \leq m-1$ olmak üzere $a_i \in \mathbb{Z}_4$ olmak üzere

$$a_0 + a_1\zeta + \cdots + a_{m-1}\zeta^{m-1}$$

şeklinde tek şekilde yazılır.(Boucher, Sole,Ulmer,2008)

2.6.3 Önerme: $GR(4,m)$ nin herhangi bir elemanı $a, b \in \{0,1,\zeta,\ldots,\zeta^{2^m-2}\}$ olmak üzere $2a+b$ şeklinde tek şekilde yazılır ve

$$\theta: GR(4,m) \longrightarrow GR(4,m)$$
$$a + 2b \longmapsto a^2 + 2b^2$$

şeklinde tanımlı dönüşüm $m-inci$ mertebeden bir halka homomorfizmasıdır. Ayrıca $GR(4,m)$ üzerinde tanımlı otomorfizmalar kümesi θ ile üretilmiş $m-inci$ dereceden devirli bir gruptur.(Boucher, Sole, Ulmer, 2008)

2.6.4 Tanım:

$$\theta: GR(4,m) \longrightarrow GR(4,m)$$
$$a + 2b \longmapsto a^2 + 2b^2$$

şeklinde tanımlı $m-inci$ dereceden bir halka otomorfizması olmak üzere

$$GR(4,m)[x,\theta] = \{\alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n \mid \alpha_i \in GR(4,m), n \in \mathbb{N}\}$$

kümesi, polinomların toplaması ve $her\ \alpha \in GR(4,m)$ için

$$x.\alpha = \theta(\alpha).x$$

şeklinde tanımlanan çarpma işlemine göre bir halkadır. Bu halkaya skew polinom halkası denir.

2.6.5 Lemma: $GR(4,m)[x,\theta]$ skew polinom halkasının merkezi $Z(GR(4,m)[x,\theta]) = \mathbb{Z}_4[x^m]$ tir.(Boucher, Sole,Ulmer,2008)

İspat:

$$Z(GR(4,m)[x,\theta]) \subseteq \mathbb{Z}_4[x^m]$$
$$Z(GR(4,m)[x,\theta]) \supseteq \mathbb{Z}_4[x^m]$$

olduğu gösterilerek eşitlik elde edilir.

2.6.6.Not: $GR(4,m)$ halkası sıfır bölen içerdiği için, IF_q sonlu cisim olmak üzere $IF_q[x,\theta]$ halkaları için geçerli olan pek çok özellik $GR(4,m)[x,\theta]$ halkası için geçerli değildir.

2.6.7 Örnek: $x^4 - 1$ polinomunun $GR(4,2)[x,\theta]$ halkasındaki iki farklı çarpanlarına ayrılışı

$$x^4 - 1 = (x+1).(x+1).(x+2\zeta+1).(x+2\zeta+3)$$
$$x^4 - 1 = (x^2+2\zeta+1).(x^2+2\zeta+3)$$

şeklindedir.

2.6.8 Not: $GR(4,2)[x,\theta]$ halkası ne sağ ne de sol Euclidean bölgesidir. Fakat sağ yada sol bölme bazı elemanlar için tanımlanabilir.

2.6.9 Önerme: $f = \sum_{i=0}^{s} \alpha_i x^i \quad ve \quad g = \sum_{j=0}^{t} \beta_j x^j$ olsun. Eğer $s \geq t$ ve g polinomunun β_t baş katsayısı terslenebilir ise

$i)$ f polinomunun bir g sağ böleni vardır.

ii) f polinomunun bir g sol böleni vardır.

İspat: $i) f = \sum_{i=0}^{s} \alpha_i x^i , g = \sum_{j=0}^{t} \beta_j x^j$ ve β_t terslenebilir eleman olsun.

$h = f - \frac{\alpha s}{\theta^{s-t}(\beta_t)} x^{s-t} g$ polinomunun derecesi f nin derecesinden küçüktür.

h polinomunun derecesi , g nin derecesinden küçük olana kadar işlem devam edilirse $f = \tilde{q}g + \tilde{r}$ ve $\deg \tilde{r} < \deg g$ olacak şekilde $\tilde{q}$ ve $\tilde{r}$ polinomları elde edilir. $\tilde{r} = 0$ ise g ye f nin sağ böleni denir.

$ii)$ $f - g\left(\theta^{-t}\left(\frac{\alpha s}{\beta_t}\right)x^{s-t}\right)$ polinomunun derecesinin f nin derecesinden

daha küçük olduğu kullanılarak benzer şekilde yapılır.

2.6.10 Önerme: $f \in GR(4,m)[x,\theta]$ polinomunun g monik polinomuyla sağdan bölümünden kalan tektir.(Boucher, Sole,Ulmer,2008)

İspat: $f = \widetilde{q_1}g + \widetilde{r_1} = \widetilde{q_2}g + \widetilde{r_2}$ olsun. $(\widetilde{q_1} - \widetilde{q_2})g = \widetilde{r_2} - \widetilde{r_1}$ dir. $\widetilde{q_1} - \widetilde{q_2} \neq 0ise\deg g < \deg(\widetilde{r_2} - \widetilde{r_1}) < \deg g - 1$ olur. Bu çelişkidir. Dolayısıyla $\widetilde{q_1} - \widetilde{q_2} = 0$ olmalıdır. Bu durumda $\widetilde{r_1} = \widetilde{r_2}$ dir. (Sol bölme ile kalanın tekliği benzer şekilde gösterilir.)

2.6.11 Örnek: $x^2 - 1 \in GR(4,2)[x,\theta]$ olmak üzere $x^2 - 1$ in sağ böleni $x - \zeta$ dir.

$$x^2 - 1 = (x + \zeta^2).(x - \zeta)$$

2.6.12 Not: $GR(4,2)[x,\theta]$ nın sağ ve sol ideallerinin tümü esas ideal değildir. burada esas idealler dikkate alınacaktır.

$I \subset GR(4,2)[x,\theta]$ iki taraflı ideal ise $GR(4,2)[x,\theta]/I$ nın sol (sağ) idealleri $GR(4,2)[x,\theta]$ nın I yı içeren sol (sağ) idealleridir.

2.6.13 Lemma: $GR(4,m)[x,\theta]$ skewpolinom halkasının $n-inci$ dereceden monik, merkezi bir $f \in \mathbb{Z}_4[x^m]$ polinomu ile üretilen sağ yada sol ideali iki taraflı bir idealdir.(Boucher, Sole,Ulmer,2008)

2.6.14 Not: f polinomunun $r-inci$ dereceden herhangi bir g sağ böleni, $GR(4,m)[x,\theta]/(f)$ halkasının bir sol esas $(g)/(f)$ idealini üretir. Özel olarak $(g)/(f)$ idealine $GR(4,m)^n$ modülünün bir alt modülü olan bir kod karşılık gelir.

2.6.15Tanım: $f \in \mathbb{Z}_4[x^m]$ monik, merkezi bir polinom ve g, f polinomunun monik sağ böleni olmak üzere $(g)/(f)$ idealine karşılık gelen $GR(4,m)$ üzerindeki bir $\theta-$esas kodu için;

$f = x^n - 1$ ise $GR(4,m)$ üzerindeki bir $\theta-$esas koda $GR(4,m)$ üzerindeki $\theta-$cyclic kod adı verilir.

$c \in Z_4\ birim$ olmak üzere $f = x^n - c$ ise $GR(4,m)$ üzerindeki bir $\theta-$esas koda $GR(4,m)$ üzerindeki $\theta-$constacyclic kod adı verilir.

2.6.16 Önerme: $GR(4,m)$ halkası üzerindeki $\theta-$constacyclic kod, $GR(4,m)[x,\theta]/< x^n - c >$ halkasının bir sol idealine karşılık gelir.(Boucher, Sole,Ulmer,2008)

2.6.17Önerme: $f \in \mathbb{Z}_4[x^m]$, $n-inci$ dereceden bir polinom,

$$g = x^r + g_{r-1}x^{r-1} + \cdots + g_1 x + g_0 \in GR(4,m)[x,\theta]$$

f polinomunun bir böleni ise g ile üretilen sol idealine karşılık gelen $[n, n-r]$ mertebeli bir $\theta-$kodun üretici matrisi

$$G = \begin{bmatrix} g_0 & \dots\dots g_{r-1} & 1 & 0 \dots\dots\dots\dots\dots 0 \\ 0 & \theta(g_0) \dots\dots \theta(g_{r-1}) & 1 \dots\dots\dots\dots & \dots \\ & \dots\dots\dots\dots\dots\dots\dots\dots\dots & & \\ 0..0 & \theta^{n-r-1}(g_0) \dots\dots \theta^{n-r-1}(g_{r-1}) & & 1 \end{bmatrix}$$

şeklindedir.(Boucher, Sole,Ulmer,2008)

2.6.18Örnek: $GR(4,2)[x,\theta]$ halkasında (x^4-1) ideali polinomunun iki farklı şekilde çarpanlara ayrılışı

$$x^4 - 1 = (x+1).(x+1).(x+2\zeta+1).(x+2\zeta+3)$$
$$= (x^2+2\zeta+1).(x^2+2\zeta+3)$$

şeklindedir. Bu sayede 4 tane sağ bölen yardımıyla 4 tane $\theta-$cyclic kod elde edilir.

2.6.19 Örnek: $GR(4,2)[x,\theta]$ halkasında (x^2-1) ideali esas idealdir. $x-\zeta$, x^2-1 polinomunun sağ böleni olduğu için (x^2-1) ideali $(x-\zeta)$ sol ideali tarafından kapsanır. $x-\zeta$ polinomunun sol çarpanı bir sol ideal oluşturur.

2.6.20Tanım: P, $GR(4,m)[x,\theta]$ halkasının bir elemanı olmak üzere (P) sol ideali, $(P)^*$ iki taraflı idealini içeriyor ise P elemanına sınırlıdır denir. P^*aP polinomunun bir sınırı adı verilir.

2.6.21Lemma: P, derecesi n olan $GR(4,m)[x,\theta]$ halkasının bir elemanı ise$P$ polinomunun en fazla mertebesi m^2n olan bir P^* sınırı vardır.(Boucher, Sole,Ulmer,2008)

2.6.22Lemma: P, derecesi n olan $GR(4,2)[x,\theta]$ halkasının bir elemanı ise P polinomunun en fazla mertebesi $2n$ olan bir P^* sınırı vardır.(Boucher, Sole,Ulmer,2008)

2. 7 Sonlu Zincir Halkaları Üzerindeki Skew Constacyclic Kodlar

2.7.1 Tanım: R birimli, değişmeli , sonlu bir halka olsun.

$i \in I = \{0,1,2, \dots, e-1\}$ olmak üzere A_i, R halkasının idealleri olmak üzere

$$< 0 >= A_0 \subsetneq A_1 \subsetneq A_2 \subsetneq \cdots \subsetneq A_{e-1} \subsetneq < 1 >= R$$

oluyorsa R halkasına sonlu bir zincir halkası denir.

2.7.2.Önerme: R sonlu bir zincir halkası ise R nin her ideali esas idealdir ve maksimal ideali tektir. Her A_i ideali e, $\gamma^e = 0$ sağlayan en küçük pozitif tam sayı olmak üzere $A_i =< \gamma^{e-i} >$ dir. (Jitman, Ling, Udomkavanich,2009)

2.7.3Önerme: R sonlu bir zincir halkası ve γ R nin maksimal idealinin bir üreteci olsun. $K = R/< \gamma >$ rezidü cismi q elemanlı ise $|R| = q^e$dir.(Jitman, Ling, Udomkavanich,2009)

2.7.4Örnek: $\mathbb{Z}_{p^e}$ halkası, $GR(p^e, m)$Galois halkası ayrıca p asal sayı $m, e \in \mathbb{Z}^+$, $e \geq 2$ ve $u^e = 0$ olmak üzere

$$IF_{p^m} + uIF_{p^m} + \cdots + u^{e-1}IF_{p^m} \cong {}^{IF_{p^m}[u]}/_{< u^e >}$$

halkası sonlu zincir halkalarına örnektir.

2.7.5Teorem: $Aut\,(R)$, R sonlu zincir halkası üzerinde tanımlı otomorfizmalarının kümesi olsun.

i) $Aut\,(GR(p^e, m)\,)$aşikar olmayan bir grup olması için gerek ve yeter koşul $m \geq 2$ olmasıdır.

ii) $Aut\big(IF_{p^m} + uIF_{p^m} + \cdots + u^{e-1}IF_{p^m}\big)$aşikar olmayan bir grup olması için gerek ve yeter koşul ya $m \geq 2$ ya p tek asal ya da $e \geq 3$ olmasıdır.

iii) $\theta \in Aut\big(IF_{p^m}\big), \beta \in IF_{p^m}^*$ olmak üzere

$$\ominus_{\theta,\beta}: IF_{p^m} + uIF_{p^m} \longrightarrow IF_{p^m} + uIF_{p^m}$$
$$a + bu \longmapsto \theta(a) + \beta\theta(b)u$$

otomorfizması vardır ve

$$Aut\,\big(IF_{p^m} + uIF_{p^m}\big) = \big\{\ominus_{\theta,\beta} \mid \theta \in Aut\big(IF_{p^m}\big), \beta \in IF_{p^m}^*\big\}$$

eşittir.

koşulları sağlanır. (Jitman, Ling, Udomkavanich,2009)

2.7.6 Tanım: $\ominus$, R sonlu zincir halkası üzerinde tanımlı aşikar olmayan bir otomorfizma olmak üzere

$$\{a_0 + a_1x + \cdots + a_nx^n \mid a_i \in R, n \in IN \ \}$$

kümesi polinomlar kümesi üzerinde tanımlı toplama ve

$$x.a = \ominus(a).x$$

şeklinde tanımlanan çarpma işlemine göre bir halkadır. Bu halkaya skew polinom halkası, halkanın elemanlarına skew polinomlar adı verilir. $R[x,\ominus]$ değişmeli olmayan bir halkadır.

2.7.7Önerme: $- : R \longrightarrow K$ doğal izdüşüm dönüşümü verilsin. $Her \ \ r \in R$ için $\overline{\ominus}(\bar{r}) = \overline{\ominus(r)}$ olmak üzere

$$- : R[x,\ominus] \longrightarrow K\left[x,\overline{\ominus}\right]$$
$$r_0 + r_1x + \cdots + r_nx^n \longmapsto \bar{r_0} + \bar{r_1}x + \cdots + \bar{r_n}x^n$$

şeklinde tanımlanan bir dönüşüm örten bir halka epimorfizmasıdır. (Jitman, Ling, Udomkavanich,2009)

2.7.8Örnek:

$$\ominus_{id,2}: IF_3 + uIF_3 \longrightarrow IF_3 + uIF_3$$
$$a + ub \longmapsto a + 2bu$$

otomorfizması verilsin. $x^6 - 1$ polinomunun $(IF_3 + uIF_3)\left[x,\ominus_{id,2}\right]$ halkasındaki iki farklı çarpanlara ayrılışı

$$x^6 - 1 = (x+1)^3.(x+2)^3$$
$$= (x^2 + ux + 2)^3$$

şeklindedir.

2.7.9Not: $R[x,\ominus]$ skew polinom halkası ne sağ ne de sol Euclidean bölgesidir. Fakat uygun elemanlar için bölme tanımlanabilir.

2.7.10 Önerme: $f = \sum_{i=0}^{r} a_i x^i \ \ , \ \ g = \sum_{j=0}^{s} b_j x^j \in R[x,\ominus]$ olsun. Eğer $r \geq s$ ve g polinomunun b_s başkatsayısı birimsel eleman ise

i) f polinomunun bir g sağ böleni vardır.

ii) f polinomunun bir g sol böleni vardır.

(Jitman, Ling, Udomkavanich,2009)

İ**spat**: $i)\ f = \sum_{i=0}^{r} a_i x^i \quad ve\ \ g = \sum_{j=0}^{s} b_j x^j$

ve b_s birimsel eleman olsun.$h = f - a_r \ominus^{r-s} (b_s^{-1}) x^{r-s}.g$ polinomunun derecesi f nin derecesinden küçüktür. h polinomu üzerinden derece, g nin derecesinden küçük olana kadar tekrar işlem devam ettirilirse $f = qg + r$ ve $\deg r < \deg g$ olacak şekilde q ve r polinomları elde edilir. $r = 0$ ise g ye f nin sağ böleni denir.

$ii) f - g(x) \ominus^{-s} (a_r b_s^{-1}) x^{r-s}$ polinomunun derecesi f nin derecesinden daha küçük olduğu kullanılarak benzer şekilde yapılır.

2.7.11Not:$f(x) \in R[x,\ominus]$ skew polinomu için $< f(x) >$, $R[x,\ominus]$ skew polinom halkasının bir sol ideali olsun.$< f(x) >$ idealinin sağ ideal olması için aşağıdaki belirtilen koşulun sağlanması gerekir.

2.7.12Önerme:$g(x)$ merkezi bir eleman, $t \in N_0$ olmak üzere $f(x) = x^t.g(x)$ şeklinde ise $< f(x) >$, $R[x,\ominus]$ ın bir esas idealidir.(Jitman, Ling, Udomkavanich,2009)

İspat: $g(x)$ merkezi bir eleman olsun. $Her \quad \sum_{i=0}^{n} a_i x^i \in R[x,\ominus]$için

$$\left(\sum_{i=0}^{n} a_i x^i\right).\left(x^t.g(x)\right) = x^t.\sum_{i=0}^{n} \ominus^{-t} (a_i).x^i.g(x) = \left(x^t.g(x)\right).\sum_{i=0}^{n} \ominus^{-t} (a_i).x^i$$

olur. O halde $<f(x)>$ idealidir.

2.7.13Sonuç:$f(x)$, monik, merkezi ve $\deg f = n$ olan bir polinom ise

$$R[x,\ominus]\Big/_{< f(x) >} = \left\{\overline{a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}} \mid a_i \in R, \qquad n \in \mathbb{N}\right\}$$

şeklindedir.

2.7.14Önerme:$n \in \mathbb{Z}_+$ ve λ, R sonlu zincir halkasında birim olsun. Aşağıdaki ifadeler birbirine denktir.

i) $x^n - \lambda$ polinomu $R[x,\ominus]$ da merkezi bir elemandır.

ii)$< x^n - \lambda >$ bir idealdir.

iii) $|<\ominus>| \mid n$ ve $\ominus(\lambda) = \lambda$ dır.

(Jitman, Ling, Udomkavanich,2009)

İspat:i)$\Longrightarrow$ ii) üstteki önermeden görülür.

ii)⟹ iii) $< x^n - \lambda >$ ideal ve $r \in R$ olsun.

$$r(x^n - \lambda) = rx^n - r\lambda = (x^n - \lambda).s = \ominus^n (s)x^n - s\lambda$$

olacak şekilde $s \in R$ vardır. $r\lambda = s\lambda$ olur. λ birimsel olduğundan $r = s$ olur.

$rx^n - r\lambda = \ominus^n (r)x^n - r\lambda$ olduğundan n, $\ominus$ nın mertebesinin bir katıdır. Yani $|<\ominus>| \mid n$ dir. Benzer şekilde

$$\begin{aligned} x^{n+1} - \ominus (\lambda)x &= x(x^n - \lambda) \\ &= (x^n - \lambda).(ax + b) \\ &= \ominus^n (a)x^{n+1} + \ominus^n (b)x^n + a\lambda x - b\lambda \end{aligned}$$

olacak şekilde $a, b \in R$ vardır. $\ominus^n (a) = 1 \Longrightarrow a = 1$ olur. Böylece $x^{n+1} - \ominus (\lambda)x = x^{n+1} - \lambda x$ olur. Yani $\ominus (\lambda) = \lambda$ dır. $\ominus^n (b) = 0 \Longrightarrow b = 0$ olduğundan $\ominus (\lambda) = \lambda$.

iii)⟹ i) $|<\ominus>| \mid n$ ve $\ominus (\lambda) = \lambda$ olsun.

$$\begin{aligned} x(x^n - \lambda) &= x^{n+1} - \ominus (\lambda)x \\ &= x^{n+1} - \ominus (\lambda)x \\ &= (x^n - \lambda).x \end{aligned}$$

ve

$\forall t \in R$için

$$\begin{aligned} (x^n - \lambda).t &= \ominus^n (t).x^n - tx \\ &= tx^n + t\lambda \\ &= t(x^n - \lambda) \end{aligned}$$

olur. O halde $x^n - \lambda$, $R[x,\ominus]$ da merkezi bir elemanıdır.

2.7.15Önerme: $g(x)$ ve $h(x) \in R[x,\ominus]$ olsun. $h(x)g(x)$ monik, merkezi skew polinom ise $h(x).g(x) = g(x).h(x)$dır.(Jitman, Ling, Udomkavanich,2009)

2.7.16Tanım: $\ominus$, R de bir otomorfizma, λ birimsel bir eleman olsun. C, skew constacyclic kod olması için gerekli ve yeterli koşul her $c = (a_0, a_1, \dots, a_{n-1})$ için $(\lambda \ominus an{-}1, \ominus a0, \dots, \ominus an{-}2 \in C$ olmasıdır.

$\lambda = 1$ olursa C, kodu skew cyclic kod, $\lambda = -1$ olursa C, kodu skew negacyclic kod olur. $\ominus$ aşikar otomorfizma olursa C, kodu sırasıyla cyclic ve negacyclic kod olur.

$\ominus$ aşikar otomorfizma olursa C skew constacyclic kod, constacyclic kod olur.

2.7.17Teorem: C, R üzerinde n uzunluğa sahip skew constacyclic kod olması için gerekli ve yeterli koşul C kodunun polinom temsili

kümesinin $R[x,\ominus]/< x^n - \lambda >$ halkasının sol ideali olmasıdır.(Jitman, Ling, Udomkavanich,2009)

2.7.18 Önerme: $g(x) = \sum_{i=0}^{n-k-1} g_i x^i + x^{n-k}$

$x^n - \lambda$ in bir sağ böleni olsun. $g(x)$ tarafından üretilen sol idealine karşılık gelen C, kodunun üreteç matrisi

$$G = \begin{bmatrix} g_0 \dots \dots \dots \dots . \dots (g_{n-k-1}) & 1 \dots . \dots \dots \dots . 0 \dots \dots \dots \dots \dots \dots 0 \\ 0 \quad \ominus (g_0) \dots \dots \dots \dots \dots \dots \ominus (g_{n-k-1}) & 1 \dots \dots \dots \quad \dots \dots 0 \\ \vdots \qquad\qquad \vdots \qquad\qquad \vdots & \vdots \qquad\qquad \vdots \\ 0 \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \ominus^{k-1} (g_0) & \dots \dots \dots \dots \dots . \dots \dots \dots \dots 1 \end{bmatrix}$$

şeklindedir.(Jitman, Ling, Udomkavanich,2009)

III.BÖLÜM

M_2 HALKASI ÜZERİNDE TANIMLI KODLAR

2009 yılında B.Yıldız ve S. Karadeniz tarafından "Linear codes over $IF_2 + u_1IF_2 + u_2IF_2 + u_1u_2IF_2$" adlı çalışmada $u_1^2 = 0,\ u_2^2 = 0,\ u_1u_2 = u_2u_1$ olmak üzere $IF_2[u_1, u_2]/< u_1^2,\ u_2^2,\ u_1u_2 - u_2u_1 >$ halkasının yapısı analiz edilmiş ve bu halkalar üzerindeki lineer kodlar incelenmiştir. Ayrıca bu kodlar üzerinde Lee ağırlık dönüşümü ve Gray dönüşümleri tanımlanmıştır.

2010 yılında B.Yıldız ve S. Karadeniz tarafından "Cylic codes over $IF_2 + u_1IF_2 + u_2IF_2 + u_1u_2IF_2$"adlı çalışmada bu halka üzerindeki cyclic kodların yapısı "Self dual codes over $F_2 + u_1IF_2 + u_2IF_2 + u_1u_2IF_2$ " adlı çalışmada self dual kodlar incelenmiştir.

2010 yılında S Dougherty, B.Yıldız ve S. Karadeniz tarafından "Codes over R_k, Gray maps and their binary images" adlı çalışmada yapılanların bir kısmı $i = 1, \dots k,\ j = 1, \dots, k \quad için \quad u_i^2 = 0, \quad u_iu_j = u_ju_i$ olmak üzere $R_k = {IF_2[u_1, \dots, u_k]}\Big/{< u_i^2,\ u_iu_j - u_ju_i >}$ sonsuz halkalar ailesine genelleştirilmiştir.

Bu bölümde, $u_1^2 = 1, u_2^2 = 1, u_1u_2 = u_2u_1$ olmak üzere

$$M_2 = IF_2[u_1, u_2]/< u_1^2 - 1, u_2^2 - 1, u_1u_2 - u_2u_1 >$$

halkasının yapısı analiz edilmiş, bu halka üzerinde Gray dönüşümleri ve Lee ağırlık dönüşümü tanımlanmıştır. $K_4 = \{1, \alpha, \beta, \alpha\beta\}$ permütasyon grubu ile M_2 üzerinde tanımlı lineer kodların Gray dönüşümü altındaki görüntüsü arasındaki ilişki incelenmiştir. M_2 üzerindeki Euclidean self dual kodlar araştırılmış, halkanın her bir idealinin 1 uzunluğunda Euclidean self dual kod olduğu gösterilmiştir.

Ayrıca M_2 halkası üzerinde aşikar olmayan bir θ otomorfizması tanımlanarak $M_2[x, \theta]$ skew polinom halkası oluşturulmuş ve bu sayede M_2 halkası üzerinde Skew kodlar tanımlamak mümkün kılınmıştır.

3.1. M_2 Halkası ve M_2 üzerinde tanımlı Gray dönüşümleri

3.1.1Önerme:$u_1^2 = 1, u_2^2 = 1, u_1u_2 = u_2u_1$ olmak üzere

$$M_2 = IF_2[u_1, u_2]/< u_1^2 - 1, u_2^2 - 1, u_1u_2 - u_2u_1 >$$

kümesi karakteristiği 2, eleman sayısı 16 olan sonlu değişmeli bir halkadır. $X^2 = 1, Y^2 = 1, XY = YX$ olmak üzere

$$IF_2 + u_1IF_2 + u_2IF_2 + u_1u_2IF_2 \cong {}^{IF_2[X,Y]}\Big/_{< X^2 - 1, Y^2 - 1, XY - YX >}$$

dir. Ayrıca $M_1 = IF_2[u_1] /< u_1^2 - 1 >$, $u_1^2 = 1$ olmak üzere, M_2 halkası

$$M_2 \cong M_1 + u_2M_1$$

şeklinde de yazılır.

3.1.2 Önerme: M_2 halkasının birimsel elemanları kümesi,

$$M_2^* = \{1, u_1, u_2, u_1u_2, 1 + u_1 + u_2, 1 + u_1 + u_1u_2, 1 + u_2 + u_1u_2, u_1 + u_2 + u_1u_2\}$$

ve M_2 halkasının idealleri

$$I_{1+u_1+u_2+u_1u_2} = \{0,1 + u_1 + u_2 + u_1u_2\}$$

$$I_{1+u_1} = \{0,1 + u_1, u_2 + u_1u_2, 1 + u_1 + u_2 + u_1u_2\}$$

$$I_{1+u_2} = \{0,1 + u_2, u_1 + u_1u_2, 1 + u_1 + u_2 + u_1u_2\}$$

$$I_{1+u_1u_2} = \{0, u_1 + u_2, 1 + u_1u_2, 1 + u_1 + u_2 + u_1u_2\}$$

$$I_0 = \{0\} \subseteq I_{1+u_1+u_2+u_1u_2} \subseteq I_{1+u_1} \subseteq M_2$$

$$I_0 = \{0\} \subseteq I_{1+u_1+u_2+u_1u_2} \subseteq I_{1+u_2} \subseteq M_2$$

$$I_0 = \{0\} \subseteq I_{1+u_1+u_2+u_1u_2} \subseteq I_{1+u_1u_2} \subseteq M_2$$

şeklindedir

Ayrıca M_2halkası esas ideal bölgesidir. Fakat sonlu zincir halkası ve yerel halka değildir.

3.1.3Tanım: $M_1 = IF_2[u_1] /< u_1^2 - 1 >$, $u_1^2 = 1$ ve $z_i = r_i + u_1q_i$, $1 \leq i \leq n$ olmak üzere,

$$\emptyset_1 : M_1^n \longrightarrow IF_2^{2n}$$

$$z=(z_1, \dots, z_n) \mapsto \emptyset_1(z)=(r_1, \dots \dots, r_n, q_1, \dots \dots, q_n)$$

biçiminde tanımlanan dönüşüme Gray dönüşümü denir. n=1 olması durumunda Gray dönüşümü

$$\emptyset_1 : M_1 \longrightarrow IF_2^2$$
$$a + bu_1 \longmapsto (a, b)$$

biçimindedir.

3.1.4 Önerme: $\emptyset_1, M_1$ üzerinde tanımlı Gray dönüşümü ve $c_1, c_2 \in M_1$ olmak üzere M_2 üzerinde tanımlı

$$\emptyset_2 : M_2 \longrightarrow IF_2^4$$
$$c_1 + u_2 c_2 \longmapsto \big(\emptyset_1(c_1), \emptyset_1(c_2)\big)$$

dönüşümü M_2^n kümesine de genelleştirilir.

3.1.5 Not: M_1 halkası IF_2 üzerinde vektör uzayıdır ve tabanı $T = \{1, u_1\}$ dir. Benzer şekilde M_2 halkasında IF_2 üzerinde vektör uzayıdır ve tabanı

$$S = \{1, u_1, u_2, u_1 u_2\}$$

dir.

3.1.6 Önerme: M_1 ve M_2 üzerinde

$$\psi_1(1) = (0,1) \quad \psi_1(u_1) = (1,0) \text{ ve}$$

$$\psi_2(1) = (0,0,0,1) \quad \psi_2(u_2) = (0,1,0,0)$$
$$\psi_2(u_1) = (0,0,1,0) \quad \psi_2(u_1 u_2) = (1,0,0,0)$$

yardımıyla tanımlanan ψ_1 ve ψ_2 dönüşümleri Gray dönüşümleridir.

3.1.7Teorem: ψ_2 Teorem 3.1.6 daki gibi olsun. $\sigma_1, \sigma_2,$ her $(c_1, c_2, c_3, c_4) \in IF_2^4$ elemanı için $\sigma_1(c_1, c_2, c_3, c_4) = (c_2, c_1, c_4, c_3)$ ve $\sigma_2(c_1, c_2, c_3, c_4) = (c_3, c_4, c_1, c_2)$ şeklinde tanımlı permütasyonlar olmak üzere $\emptyset_2$ ve ψ_2 Gray dönüşümleri için

$$\emptyset_2 = \sigma_2\big(\sigma_1(\psi_2)\big)$$

sağlanır.

İspat: Herhangi bir $r \in M_2$ için $\emptyset_2(r) = \sigma_2\big(\sigma_1(\psi_2(r))\big)$ olduğu açıktır. O halde $\emptyset_2 = \sigma_2\big(\sigma_1(\psi_2)\big)$dir.

3.1.8 *Tanım* : M_2 halkası üzerinde $her\ s = a + bu_1 + cu_2 + du_1 u_2$ elemanı için

$$w_L(a + bu_1 + cu_2 + du_1 u_2) = w_H\big(\emptyset_2(a + bu_1 + cu_2 + du_1 u_2)\big)$$
$$= w_H(a, b, c, d)$$

biçiminde tanımlanan fonksiyona s elemanının Lee ağırlığı denir. Her $t = (t_1, \dots, t_n) \in M_2^n$ için t kod sözcüğünün Lee ağırlığı da

$$w_L(t) = \sum_{i=1}^{n} w_L(t_i)$$

biçiminde tanımlanır.

3.1.9 Not:

$1, u_1, u_2, u_1u_2$elemanlarının Lee ağırlığı 1,

$1+u_1, 1+u_2, 1+u_1u_2, u_1+u_2, u_1+u_1u_2, u_2+u_1u_2$elemanlarının Lee ağırlığı 2,

$1+u_1+u_2, u_1+u_2+u_1u_2, 1+u_1+u_1u_2, 1+u_2+u_1u_2$ elemanlarının Lee ağırlığı 3,

$1+u_1+u_2+u_1u_2$ elemanının Lee ağırlığı 4 tür.

3.1.10Tanım:M_2 üzerindeki, n uzunluğuna sahip C lineer kodu M_2^n nin bir M_2-alt modülüdür.

3.1.11Teorem: C,IF_2 üzerinde tanımlı $4n$ uzunluğunda lineer kod olsun. Herhangi bir $(\acute{a}, \acute{b}, \acute{c}, \acute{d}) \in IF_2^{4n}$ için

$$\alpha(\acute{a}, \acute{b}, \acute{c}, \acute{d}) = (\acute{b}, \acute{a}, \acute{d}, \acute{c})$$
$$\beta(\acute{a}, \acute{b}, \acute{c}, \acute{d}) = (\acute{c}, \acute{d}, \acute{a}, \acute{b})$$
$$\alpha\beta(\acute{a}, \acute{b}, \acute{c}, \acute{d}) = (\acute{d}, \acute{c}, \acute{b}, \acute{a})$$

olmak üzere $K_4 = \{1, \alpha, \beta, \alpha\beta\}$ permütasyon grubu verilsin. Bu durumda C kodunun, M_2 üzerinde tanımlı bir lineer kodun Gray dönüşümü altında görüntüsü olması için gerekli ve yeterli koşul, C nin

$$K_4 = \{1, \alpha, \beta, \alpha\beta\}$$

permütasyon grubu altında değişmez kalmasıdır.

İspat:C, M_2 üzerinde n uzunluğunda lineer D kodunun görüntüsü olsun. $\acute{x} = (\acute{a}, \acute{b}, \acute{c}, \acute{d}) \in C$ olsun. $\acute{y} = \acute{a} + \acute{b}u_1 + \acute{c}u_2 + \acute{d}u_1u_2 \in D$ kod sözcüğünün Gray dönüşümü altındaki görüntüsü $\acute{x}$ olmak üzere

$$\emptyset_2(u_1.\acute{y}) = (\acute{b}, \acute{a}, \acute{d}, \acute{c}) = \alpha(\acute{x})$$
$$\emptyset_2(u_2.\acute{y}) = (\acute{c}, \acute{d}, \acute{a}, \acute{b}) = \beta(\acute{x})$$
$$\emptyset_2(u_1u_2.\acute{y}) = (\acute{d}, \acute{c}, \acute{b}, \acute{a}) = \alpha\beta(\acute{x})$$

olduğundan, C, K_4 permütasyon grubu altında sabit kalmaktadır.

Tersine, C, IF_2üzerinde tanımlı lineer bir kod olduğundan $\alpha, \beta, \alpha\beta$, u_1, u_2 ve u_1u_2 sabit bıraktığından D de sabit kalır. O halde D, M_2 üzerinde tanımlı lineer bir koddur.

3.1.12Teorem:

$$\pi_{2,1}: M_2 \longrightarrow M_1$$
$$a + bu_1 + cu_2 + du_1u_2 \longrightarrow a + bu_1$$

izdüşüm dönüşümü olmak üzere C, M_2 üzerinde Euclidean self dual kod ise $\pi_{2,1}(C)$, M_1 üzerinde self ortogonal koddur.

İspat:C, Euclidean self dual kod olsun. O zaman $C^{\perp} = C$ dir.$\pi_{2,1}(C) = \pi_{2,1}(C^{\perp}) \subseteq \pi_{2,1}(C)^{\perp}$olduğunu görmek için, herhangibir $\pi_{2,1}(x) \in \pi_{2,1}(C^{\perp})$ alalım.

$$\pi_{2,1}(x) \in \pi_{2,1}(C^{\perp}) \Longrightarrow x = (x_1, \dots, x_n) \in C^{\perp}$$
$$\Longrightarrow \sum_{i=1}^{n} c_i x_i = 0, \qquad \forall c = (c_1, \dots, c_n) \in C$$
$$\Longrightarrow \pi_{2,1}\left(\sum_{i=1}^{n} c_i x_i\right) = \pi_{2,1}(0)$$
$$\Longrightarrow \pi_{2,1}\left(\sum_{i=1}^{n} c_i x_i\right) = 0 \qquad \forall \pi_{2,1}(c) \in \pi_{2,1}(C)$$
$$\Longrightarrow < \pi_{2,1}(c), \pi_{2,1}(x) >= 0,$$
$$\Longrightarrow \pi_{2,1}(x) \in \pi_{2,1}(C)^{\perp}$$

O halde $\pi_{2,1}(C)$, Euclidean self ortogonal koddur.

3.1.13Sonuç:C, M_1 üzerinde Euclidean self dual kod ise$\pi_{2,1}(\acute{C}) = C$ olacak şekilde M_2 üzerinde $\acute{C}$ self dual kod vardır.

3.1.14 Teorem:M_2 halkasının idealleri 1 uzunluğuna sahip self dual kodlardır.

İspat: Her $I \in M_2$ ideali için $I^{\perp} = I$ olduğundan I idealleri 1 uzunluğa sahip self dual kodlardır.

3.1.15 Lemma:E ve F, M_2 üzerinde tanımlı iki Euclidean self dual kod ise ExFde Euclidean self dual koddur.

3.1.16Teorem:M_2 üzerinde tüm uzunluklara sahip Euclidean self dual kod vardır.

İspat: 3.1.14 Teoremden Iideali1 uzunluğa sahip bir self dual kod idi.3.1.15 Lemma kullanılarak her uzunluğa sahipself dual kodun varlığı gösterilir.

3.1.17Teorem:C, M_2 üzerinde self dual kod ise C, tümbileşenleri$1 + u_1 + u_2 + u_1u_2$olan bir vektör içerir.

İspat: C self dual kod olsun. a , M_2 halkasının birimsel bir elemanı ise $a^2 = 1$ dir. b birimsel eleman değil ise $b^2 = 0$ dır. Bu yüzden c , self ortogonal vektörü çift sayıda birim içermelidir.

$$(1 + u_1 + u_2 + u_1u_2).\, a = 1 + u_1 + u_2 + u_1u_2$$
$$(1 + u_1 + u_2 + u_1u_2).\, b = 0$$

olduğundan$c$, $tümü\ 1 + u_1 + u_2 + u_1u_2$ olan vektöre ortogonaldir. Yani C, tümü $1 + u_1 + u_2 + u_1u_2$ olan bir vektörü içerir.

3.1.18Teorem: C, n uzunluğunda M_2 üzerinde lineer kod olsun. O halde

$$\emptyset_2(C^{\perp}) \subseteq \left(\emptyset_2(C)\right)^{\perp}$$

dir.

İspat:

$$\forall \emptyset_2(x) \in \emptyset_2(C^{\perp}) \Longrightarrow x \in C^{\perp}$$
$$\Longrightarrow \forall c \in C \text{ için } < x, c >= 0$$

$\acute{a}_1, \acute{b}_1, \acute{c}_1, \acute{d}_1, \acute{a}_2, \acute{b}_2, \acute{c}_2, \acute{d}_2 \in IF_2^n$olmak üzere

$x = \acute{a}_1 + u_1\acute{b}_1 + u_2\acute{c}_1 + u_1u_2\acute{d}_1,\ c = \acute{a}_2 + u_1\acute{b}_2 + u_2\acute{c}_2 + u_1u_2\acute{d}_2$elemanları için

$$\left(\acute{a}_1\acute{a}_2 + \acute{b}_1\acute{b}_2 + \acute{c}_1\acute{c}_2 + \acute{d}_1\acute{d}_2\right) = 0$$
$$\left(\acute{a}_1\acute{b}_2 + \acute{b}_1\acute{a}_2 + \acute{c}_1\acute{d}_2 + \acute{d}_1\acute{c}_2\right) = 0$$
$$\left(\acute{a}_1\acute{c}_2 + \acute{a}_2\acute{c}_1 + \acute{b}_1\acute{d}_2 + \acute{d}_1\acute{b}_2\right) = 0$$
$$\left(\acute{a}_1\acute{d}_2 + \acute{d}_1\acute{a}_2 + \acute{b}_1\acute{c}_2 + \acute{c}_1\acute{b}_2\right) = 0$$

olur. Bu yüzden $\emptyset_2(x) = \left(\acute{a}_1, \acute{b}_1, \acute{c}_1, \acute{d}_1\right)$ ve $her\ \emptyset_2(c) = \left(\acute{a}_2, \acute{b}_2, \acute{c}_2, \acute{d}_2\right) \in \emptyset_2(C)\ \ için$

$$< \emptyset_2(x), \emptyset_2(c) >= 0$$

olur. Yani

$$\emptyset_2(x) \in \left(\emptyset_2(C)\right)^{\perp}$$

olur. O halde

$$\emptyset_2(C^{\perp}) \subseteq \left(\emptyset_2(C)\right)^{\perp}$$

dir. ■

3.2 $M_2[x,\theta]$ Skewpolinom halkası

M_2 kümesi üzerinde

$$\begin{gathered}\theta: M_2 \longrightarrow M_2 \\ 0 \longrightarrow 0 \\ 1 \longrightarrow 1 \\ u_1 \longrightarrow u_2 \\ u_2 \longrightarrow u_1\end{gathered}$$

şeklinde tanımlanan dönüşüm aşikar olmayan bir otomorfizmadır. Bu sayede $M_2[x,\theta]$ skew polinom halkası tanımlanarak M_2 halkası üzerinde skewcyclic, skewQC kod tanımlanabilir. M_2 nin 1 den farklı birimleri olduğu için M_2 kümesi üzerinde skew constacyclic kod tanımlamakta mümkündür.

Bu çalışmalar $i = 1,..k,\ j = 1,...k\ için\ u_i^2 = 1,\ \ u_iu_j = u_ju_i$ olmak üzere

$$M_k = {}^{IF_2[u_1,\dots,u_k]}\Big/_{< u_i^2 - 1, u_iu_j - u_ju_i >}$$

halkası üzerine, hatta p bir asal ve $i = 1,..k,\ j = 1,...k\ için\ u_i^2 = 1,\ \ u_iu_j = u_ju_i$ olmak üzere

$$IF_p[u_1,\dots,u_k]\Big/_{< u_i^2 - 1, u_iu_j - u_ju_i >}$$

halkasına da genelleştirilebilir.

Bu şekilde halkalar üzerinde tanımlı cyclic, quasicyclic ve constacyclic kodlardan daha büyük bir sınıf elde edilir. Bu sayede minimum uzaklığı yüksek lineer kodlar elde etmek ihtimali artacaktır.

IV.BÖLÜM

F_2+vF_2 HALKASI ÜZERİNDE TANIMLI MACDONALD KODLAR

"Simplex linear codes over the ring $F_2 + vF_2$" adlı çalışmada $v^2 = v$ olmak üzere $R = F_2 + v F_2 \cong F_2[v]/\langle v^2 - v\rangle$ halkası üzerinde lineer simpleks kodlar Mohammed Al Ashker ve Ibtisam Isleem tarafından oluşturulmuştur.

Bu kısımda, bu makaledeki bilgiler ve $v^2 = v$ olmak üzere $R = F_2 + v F_2 \cong F_2[v]/\langle v^2 - v\rangle$ halkası üzerinde tanımlı simpleks kodlar yardımıyla bu halka üzerindeki MacDonald kodların oluşumu ve bu kodların bazı temel özellikleri verilmiştir.

4.1 . F_2+vF_2 HALKASI ÜZERİNDE TANIMLI LİNEER SIMPLEKS KODLAR

$F_2[v]/\langle v^2 - v\rangle = \{ a_0 + a_1 v + \langle v^2 - v\rangle \mid a_0, a_1 \in F_2\}$ halkası için $v^2 = v$ olması durumunda

$$a_0 + a_1 v + \langle 0 \rangle = \{ a_0 + a_1 v + 0.b \mid a_0, a_1 \in F_2, b \in F_2[v] \} = \{a_0 + v a_1\}$$

olacağından

$$F_2[v]/\langle v^2 - v\rangle = \{\{a_0 + v.a_1\} \mid a_0, a_1 \in F_2\}$$

bulunur. $R = F_2 + v F_2 = \{ a_0 + a_1 v \mid a_0, a_1 \in F_2\}$ de bir halkadır. Üstelik

$$f: F_2 + v F_2 \longrightarrow F_2[v]/\langle v^2 - v\rangle$$
$$a_0 + a_1 v \longrightarrow \{a_0 + a_1 v\}$$

dönüşümü bir izomorfizma olduğundan $R = F_2 + v F_2 \cong F_2[v]/\langle v^2 - v\rangle$ şeklinde yazılır. R, 4 elemanlı değişmeli bir halkadır.

4.1.1.Tanım: C, R üzerinde tanımlı bir lineer kod olsun. x kod sözcüğünün Lee ağırlığı,

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

olmak üzere

$$w_L(x)=\sum_{i=1}^{n} w_L(x_i)$$

x kod sözcüğünün Bachoc ağırlığı,

$$w_B(x_i)=\begin{cases}0 & x_i=0\\ 1 & x_i=1\\ 2 & x_i=v \quad ya\ da\ \ x_i=1+v\end{cases}$$

olmak üzere

$$\mathrm{w_B(x)}=\sum_{\boldsymbol{i=1}}^{\boldsymbol{n}} \mathrm{w_B(x_i)}$$

şeklinde tanımlanır.

4.1.2. Teorem: x *ve* y R^n kümesinin herhangi iki elemanı olmak üzere x ve y arasındaki Lee uzaklığı

$$d_{\boldsymbol{L}}\,(\mathrm{x,y})=\mathrm{w_L}\,(x-y)=\sum_{i=1}^{n} w_L(x_i-y_i)$$

dir. [Betsumiya, Harada, 2004]

4.1.3Teorem: x ve y $\mathrm{R^n}$ kümesinin herhangi iki elemanı olmak üzere x ve y arasındaki Bachoc uzaklığı

$$d_B(x,y)=w_B(x-y)=\sum_{i=1}^{n} w_B(x_i-y_i)$$

dir. (Betsumiya, Harada , Gulliver 2003)

4.1.4 Tanım: R üzerinde tanımlı C kodunun minimum Lee uzaklığı ve minimum Bachoc uzaklığı sırasıyla

$$d_L = d_L(C) = \min_{\substack{u,v \in C \\ u \neq v}} d_L(u,v)$$

$$d_B = d_B(C) = \min_{\substack{u,v \in C \\ u \neq v}} d_B(u,v)$$

şeklinde tanımlanır.

4.1.5.Tanım: x ve y F_2^n nin herhangi iki elemanı olmak üzere

$$\emptyset: F_2^n + v F_2^n \longrightarrow F_2^n \; x \; F_2^n$$
$$(x + vy) \longrightarrow (x, x + y)$$

şeklinde tanımlanan $\emptyset$ dönüşümüne Gray dönüşümü denir.

4.1.6.Teorem: Yukarıdaki gibi tanımlanan $\emptyset$ dönüşümü bir izomorfizmadır. (Betsumiya, Harada, 2004)

Bu dönüşüm $\phi : (F_2 + vF_2)^n \longrightarrow F_2^{2n}$ şeklindeki dönüşüme genişletilebilir. Ayrıca $\forall a \in (F_2 + v F_2)^n$ için $w_L(a) = w_H(\phi(a))$ dır.

4.1.7 Tanım: $w_1, w_2, \dots, w_k \; R^n$ de vektörler olsun. Eğer $\sum a_j w_j = 0$ iken her j için $a_j w_j = 0$ ise $w_1, w_2, \dots, w_k$ vektörleri doğrusal bağımsızdır denir. Eğer bazı i değerleri için $\emptyset(w_1), \emptyset(w_2), \dots, \emptyset(w_k)$ lineer bağımsızsa $w_1, w_2, \dots, w_k$ vektörlerine modüler bağımsız adı verilir.

4.1.8 Tanım: Hem doğrusal, hem de modüler bağımsız kümeye en küçük üreteç kümesi adı verilir.

4.1.8 Not: $w = (a_1, a_2, \dots, a_n)$ sıfırdan farklı bir vektör olsun. $< (a_1, a_2, \dots, a_n) >$ ya $< v >$, $< v + 1 >$ ya da R dir. $I(w) = | < (a_1, a_2, \dots, a_n) > |$ olsun. $I(w) = 2 \; ya \; da \; 4$ dir.

4.1.9Teorem: C, $\{ w_1, w_2, \dots, w_k \}$ en küçük üreteç kümesiyle üretilen kod olsun. O zaman $|C| = \prod_{i=1}^{s} I(w_i)$ dir.

4.1.10 Sonuç: $\{ w_1, w_2, \dots, w_k \}$, R üzerinde tanımlı C kodu için en küçük üreteç kümesi olsun. Bu kümenin içinde ya 1 ya da hem v hem de $v + 1$ i bulunduran k_1 tane vektör, ya sadece 0 ve v ya da sadece 0 ve $v + 1$ i bulunduran k_2 tane vektör vardır. Bu durumda $|C| = 4^{k_1} 2^{k_2}$dir.

4.1.11.Teorem: C, R üzerindeki herhangi bir kod olsun. A_i ve B_j bileşenleri F_2 cisminden alınan matrisler olmak üzere, C kodu

$$\begin{pmatrix} \boldsymbol{I_{k_1}} & \boldsymbol{vB_1} & \boldsymbol{(1+v)A_1} & \boldsymbol{(1+v)A_2+vB_2} & \boldsymbol{(1+v)A_3+\ vB_3} \\ \boldsymbol{0} & \boldsymbol{(1+v)I_{k_2}} & \boldsymbol{0} & \boldsymbol{(1+v)A_4} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{vI_{k_3}} & \boldsymbol{0} & \boldsymbol{vB_4} \end{pmatrix}$$

matrisi ile üretilen bir koda denktir. (Dougherty, Gaborit ,Harada ,Solé , 1999)

4.1.12.Tanım: H, R üzerinde tanımlı bir kod olmak üzere,

$$H^+ = \{s | \exists t \in F_2^n | (1+v)s + vt \in H\}$$

kümesine H ' ın Torsion kodu,

$$H^- = \{t | \exists s \in F_2^n | (1+v)s + vt \in H\}$$

kümesine H ın Rezidü kodu denir.

4.1.13.Teorem: H^+ ve H^-, R üzerinde tanımlı H kodunun sırasıyla Torsion ve Rezidü kodları olsun. A_i ve B_j ler bileşenleri F_2 cisminden alınan matrisler olmak üzere bu kodlar sırasıyla

$$\begin{pmatrix} I_{k_1} & 0 & A_1 & A_2 & A_3 \\ 0 & I_{k_2} & 0 & A_4 & 0 \end{pmatrix} \quad \text{ve} \quad \begin{pmatrix} I_{k_1} & B_1 & 0 & B_2 & B_3 \\ 0 & 0 & I_{k_3} & 0 & B_4 \end{pmatrix}$$

üreteç matrisleri ile üretilen kodlara denktir. (Dougherty, Gaborit, Harada, Sole, 1999)

4.1.14.Tanım: $G_1^\alpha = (0\ \ 1\ \ v\ \ w)$ ve $k \geq 2$ için

$$G_k^\alpha = \begin{pmatrix} 0\,0\,\ldots\,0 & 1\,1\,\ldots\,1 & \mathrm{v\,v\,\ldots\,v} & \mathrm{w\,w\,\ldots\,w} \\ \mathrm{G}_{\mathrm{k-1}}^{\alpha} & \mathrm{G}_{\mathrm{k-1}}^{\alpha} & \mathrm{G}_{\mathrm{k-1}}^{\alpha} & \mathrm{G}_{\mathrm{k-1}}^{\alpha} \end{pmatrix}_{\mathrm{kx2^{2k}}}$$

olsun. $k \geq 1$ için $\mathrm{G}_{\mathrm{k}}^{\alpha}$ matrisi ile üretilen koda R üzerinde tanımlı α tipi Simpleks kod adı verilir ve $\mathrm{S}_{\mathrm{k}}^{\alpha}$ ile gösterilir.

4.1.15.Teorem: S_k^{α} simpleks kodun Hamming, Lee ve Bachoc ağırlık dağılımları aşağıdaki gibidir. (Al-Ashker, Isleem, 2008)

$$A_H(0) = 1$$
$$A_H\left(2^{2k-1}\right) = 2\left(2^k - 1\right)$$
$$A_H\left(3.2^{2(k-1)}\right) = \left(2^k - 1\right)\left(2^k - 1\right)$$

$$A_L(0) = 1$$
$$A_L\left(2^{2k-1}\right) = 2\left(2^k - 1\right)$$
$$A_L\left(4^k\right) = \left(2^k - 1\right)\left(2^k - 1\right)$$

$$A_B(0) = 1$$
$$A_B\left(4^k\right) = 2(2^k - 1)$$
$$A_B\left(5.2^{2(k-1)}\right) = (2^k - 1)(2^k - 1)$$

4.1.16.Sonuç: S_k^{α} simpleks kodunun minimum Hamming, Lee, Bachoc ağırlıkları $d_H = 2^{2k-1}, d_L = 2^{2k-1}, d_B = 2^{2k}$ şeklindedir. (Al-Ashker, Isleem, 2008)

4.1.17.Not: α tipi Simpleks S_k^{α} kodunun uzunluğu çok büyüktür. Dolayısıyla G_k^{α} üreteç matrisinin bazı sütunlarını atarak *R* üzerinde tanımlı daha küçük uzunluklu iyi kodlar elde etmek mümkündür.

4.1.18.Tanım: λ_1=[1 v] ve k ≥ 2 için $\lambda_k = \begin{bmatrix} 0..0 & 1..1 & v..v & w..w \\ \lambda_{k-1} & G_{k-1}^{\alpha} & G_{k-1}^{\alpha} & \lambda_{k-1} \end{bmatrix}$ olmak üzere λ_k, $k\,x\,2^k(2^k-1)$ tipinde bir matris, S_1 = [1 w] ve k ≥ 2 için $S_k = \begin{bmatrix} 0..0 & 1..1 & v..v & w..w \\ S_{k-1} & G_{k-1}^{\alpha} & S_{k-1} & G_{k-1}^{\alpha} \end{bmatrix}$ olmak üzere S_k , $k\,x\,2^k(2^k-1)$ tipinde bir matris olsun.

$G_2^{\beta} = \begin{bmatrix} 1\,1\,1\,1 & 0 & v\,v & w\,w \\ 0\,1\,v\,w & 1 & 1\,\mathrm{w} & 1\,\mathrm{v} \end{bmatrix}$ ve k > 2 için $G_k^{\beta} = \begin{bmatrix} 0..0 & 1..1 & v..v & w..w \\ G_{k-1}^{\alpha} & G_{k-1}^{B} & S_{k-1} & \lambda_{k-1} \end{bmatrix}$ olmak üzere G_k^{β} , $k\ x\ [(2^k-1)(2^k-1)]$ tipinde bir matris olsun. k ≥ 2 olmak üzere G_k^{β} üreteç matrisi ile üretilen koda β tipi simpleks kod denir ve S_k^{β} ile gösterilir.

G_k^{β} üreteç matrisi, G_k^{α} üreteç matrisinin $2^{k+1}-1$ sütunun silinmesiyle elde edilmiştir.

4.1.19.Teorem: S_k^{β} simpleks kodunun Hamming, Lee ve Bachoc ağırlık dağılımları aşağıdaki gibidir. (Al-Ashker, Isleem ,2008)

$$A_H(0) = 1$$
$$A_H\left(2^{k-2}(3.2^k-1)-1\right) = (2^k-1)(2^k-1)$$
$$A_H\left(2^{(k-1)}(2^k-1)\right) = 2(2^k-1)$$

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

$$A_B(0) = 1$$
$$A_B\left(2^k\left[2.(2^{k-1}-1)+2^{k-2}\right]\right) = (2^k-1)(3.2^{k-1})$$
$$A_B\left(2^k(2^k-1)\right) = 2.(2^{k-3})(2^k-1)$$

4.1.20. Sonuç: S_k^{β} simpleks kodunun minimum Hamming, Lee ve Bachoc ağırlıkları

$$d_H = 2^{k-1}(2^k-1)$$
$$d_L = 2^{k-1}(2^k-1)$$
$$d_B = 2^k(2.(2^{k-1}-1)+2^{k-2})$$

dır. Ayrıca $d_H = d_L \leq \frac{d_B}{2}$ dir.

4.2. $F_2 + v F_2$ HALKASI ÜZERİNDE TANIMLI MACDONALD KODLAR

α tipi Simpleks S_k^α kodu, $G_1^\alpha = (0\ 1\ v\ w)$ ve $k \geq 2$ için

$$G_k^\alpha = \begin{pmatrix} 0..0 & 1..1 & v..v & w..w \\ G_{k-1}^\alpha & G_{k-1}^\alpha & G_{k-1}^\alpha & G_{k-1}^\alpha \end{pmatrix}$$

olmak üzere G_k^α üreteç matrisi ile üretilen lineer bir $[2^{2k}, k, 2^{2k-1}, 2^{2k-1}, 2^{2k}]$ kod idi. Bu kod yardımıyla uzunluğu daha küçük olan iyi bir kod elde etmek mümkündür.

4.2.1.Tanım:(A\B) matrisi, A matrisinden B matrisinin sütunlarının silinmesiyle elde edilen matristir. .

4.2.2.Tanım: $1 \leq u \leq k-1$ olmak üzere G_k^α matrisinden G_u^α matrisinin sütunlarının ve $(k-u)x2^{2u}$ mertebeli **0** matrisinin silinmesiyle elde edilen matrise $G_{k,u}^\alpha$ matrisi denir ve

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

şeklindedir.

4.2.3.Tanım: α tipi simpleks S_k^α kodun G_k^α üreteç matrisinden elde edilen $G_{k,u}^\alpha$ üreteç matrisine sahip koda α tipi MacDonald kod denir ve $M_{k,u}^\alpha$ ile gösterilir.

$M_{k,u}^\alpha$, $n = 2^{2k} - 2^{2u}$ uzunluğuna sahip bir koddur.

4.2.4.Lemma: $M_{k,u}^\alpha$ kodunun Torsion kodu IF_2 üzerinde tanımlı bir lineer $[2^{2k}\text{-}2^{2u}, 2k_1+k_2, 2^{2k-1}\text{-}2^{2u-1}]$-koddur ve ağırlık dağılımları aşağıdaki gibidir.

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

İspat: $w = 1 + v$ olmak üzere Torsion kodunun üreteç matrisi $w.G_{k,u}^\alpha$ matrisinde w' lar yerine 1' ler yazılarak elde edilir. k ve u ya bağlı tümevarım yapılarak ispatlanır.

4.2.5.Not: $G_{k,u}^{\alpha}$ üreteç matrisinin ilk k-u satırındaki birimsel elemanların sayısı 2^{2k-2} ve birimsel olmayan elemanların sayısı 2^{2k-1} dir. Son u satırdaki birimsel elemanların sayısı 2^{2k-2}-2^{2u-2} ve birimsel olmayan elemanların sayısı 2^{2k-1}-2^{2u-1} dir.

4.2.6.Lemma: $t \in M_{k,u}^{\alpha}, t \neq 0$ olsun. t elemanının en az bir bileşeni birim ise bu durumda 4 tip kod sözcüğü vardır.

$$I.\, w_1(t) = w_w(t) = w_v(t) = w_0(t) = 2^{2k-2} - 2^{2u-2}$$

$$II.\, w_1(t) = w_w(t) = w_v(t) = 2^{2k-2}$$

$$III.\, w_1(t) = w_w(t) = 2^{2k-2} \text{ ve } w_o(t) = w_v(t) = 2^{2k-2} - 2^{2u-1}$$

$$IV.\, w_1(t) = w_v(t) = 2^{2k-2} \text{ ve } w_o(t) = w_w(t) = 2^{2k-2} - 2^{2u-1}$$

aksi taktirde

$$I.\, w_o(t) = w_v(t) = 2^{2k-1} - 2^{2u-1}$$

$$II.\, w_o(t) = w_w(t) = 2^{2k-1} - 2^{2u-1}$$

$$III.\, w_o(t) = 2^{2k-1} - 2^{2u}, w_v(t) = 2^{2k-1}$$

$$IV.\, w_o(t) = 2^{2k-1} - 2^{2u}, w_w(t) = 2^{2k-1}$$

dir.

4.2.7Teorem: $M_{k,u}^{\alpha}$ kodunun Hamming, Lee ve Bachoc ağırlık dağılımları aşağıdaki gibidir.

$$A_H(0) = 1$$

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

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

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

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

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

$$A_L(0) = 1$$

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

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

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

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

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

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

$$A_B\left(2^{2k}\right) = \left(2^k - 2^u\right)\left(2^{1-u}\right)$$

$$A_B\left(5.2^{2(k-1)}\right) = \left(2^{k-u} - 1\right)\left(2^{k-u} - 1\right)$$

$$A_B\left(2^{2k} - 2^{2u}\right) = 2^{k-u+1}\left(2^u - 1\right)$$

$$A_B\left(5.\left(2^{2k-2} - 2^{2u-2}\right)\right) = 2^{2(k-u)}\left(2^u - 1\right)\left(2^u - 1\right)$$

$$A_B\left(5.2^{2k-2} - 2^{2u}\right) = 2^{k-u+1}\left(2^u - 1\right)\left(2^{k-u} - 1\right)$$

İspat: 4.2.6 Lemma'dan, $M_{k,u}^{\alpha}$ kodunun sıfırdan farklı her bir kod sözcüğünün Hamming ağırlığı ya $2^{2k-1} - 2^{2u-1}$, 2^{2k-1}, $3.\left(2^{2k-1} - 2^{2u-1}\right)$, 3.2^{2k-1} ya da $3.2^{2k-2} - 2^{2u-1}$ ve Lee ağırlığı ya $2^{2k-1} - 2^{2u-1}$, 2^{2k-1}, $2^{2k} - 2^{2u}$, 2^{2k} ya da $2^{2k} - 2^{2u-1}$ ve Bachoc ağırlığı ya $2^{2k} - 2^{2u}$, 2^{2k}, $5.2^{2k-2} - 2^{2u-2}$, 5.2^{2k} ya da $5.2^{2k-2} - 2^{2u}$ dur. S_k^{α} kodu için yaptığımız ağırlık hesapları ile benzer bir şekilde hesaplanır.

4.2.8.Sonuç:

Benzer çalışmada, β tipi simpleks kodlar kullanılarak β tipi MacDonald kodlar oluşturulabilir ve bu kodlarla ilgili bazı özellikler incelenebilir.

R üzerinde tanımlı Macdonald kodun Torsion kodunun boyutunu belirlemekte 4.1.9 Teorem ve 4.1.10 Sonuc' u ile bize katkıda bulunan Steven Dougherty 'e teşekkürlerimizi sunarız.

KAYNAKLAR

1. Abualrub T., Ghrayeb A., Aydın N., Şiap İ., (2010), On the construction of skew quasi cyclic codes, IEEE Transform Inform Theory, 56, Issue 5, 2080-2090.

2. Abualrub T. and Seneviratne P., (2010), "Skew cyclic codes over $IF_2 + vIF_2$, Proceeding of the International Multi Conference Of Engineers and Computer Scientists, Vol II, IMECS 2010, March 17-19 ,Hong Kong.

3. Al-Ashker M., Isleem I., (2008), Simplex Linear Codes Over The Ring IF_2+vIF_2. Islamic University Journal For Natural Science, to appear.

4.Betsumiya K. ,Harada M, (2004), Optimal Self-Dual Codes Over F_2+vF_2. IEEE Trans Inform Theory(50), 356-358.

5.Betsumiya K. ,Harada M., Aaron Gulliver,(2003), Extremal Self- Dual Codes Over F_2xF_2 Designs Codes And Cryptography (28) 171-186.

6. Bhaintwal M.,(2011), "Skew quasi cyclic codes over Galois Rings" ,**Designs, codes and Cryptography** ,**Volume 62, Number 1**, 85-101.

7. Boucher D., Geiselmann W., Ulmer F., (2007), "Skew cyclic codes", Applicable Algebra in Eng. Comm. and Computing, Vol 18, Number 4,379-389.

8.Boucher D., Sole P., Ulmer F., (2008), "Skew constacyclic codes over Galois Rings" Advances of Mathematics of Communications, Vol. 2 ,Number 3 , pp 273-292.

9. Boucher D., Ulmer F., (2007), "Coding with skew polynomial rings" , Journal of Symbolic Computation, Vol 44, Issue 12, 1644-1656.

10. Dougherty S., Yıldız B, Karadeniz S, (May. 2011), "Codes over R_k, Gray Maps and their Binary Images", Finite Fields and Applications, Vol. 17, No. 3, pp. 205-219.

11. Dougherty S., Gaborit P., Harada M., Solé P**, (**1999), Type II Codes Over F_2+uF_2. IEEE Trans Inform Theory (45) 32-45.

12. Dougherty S., Liu H., (2009), Indepence of vectors in codes over rings, *Des. Codes and Cryp.*, (51),pp 55-68.

13. Hill R.,(1986),"A First Course in Coding Theory", Clarendon Press, The Oxford University Press, Oxford, UK.

14. Jacobson N., (1943), "The theory of rings", Publication of the AMS.

15. Jitman S., Ling S., Udomkavanich P., (2009), “Skew constacyclic codes over finite chain rings”, Advance in Math. of Communication, Vol 6, No 1,39-63.

16. Ling S. and Xing C., (2004), ”Coding Theory A First Course”, Cambridge University Press.

17. McDonald B.R, (1974), “Finite Rings with identity”, Marcel Dekker Inc. New York.

18. MacWilliams F.J., Sloane N.J.A, (1977), “The Theory of Error Correcting Codes”, North-Holland Publishing Company.

19. Ore O., (1983), “Theory of non-commutative polynomials”, Annals of Math., 34 ,480-508

20. Roman S.,(1992), “Coding and Information Theory”, Graduate Texts in Mathematics, Springer Verlag.

21. Şiap İ., Abualrub T., Aydın N, Seneviratne P., (2010) “Skew cyclic codes of arbitrary length” **International Journal of Information and Coding Theory**, **Volume 2, Number 1**, 10-20.

22. Yıldız B., Karadeniz S., (2010),” Linear codes over $IF_2 + uIF_2 + vIF_2 + uvIF_2$ “ ,Designs, Codes and Cryptography , Vol. 58, No. 3, pp. 221-234

23. Yıldız B., Karadeniz S., (2010), “Cyclic codes over $IF_2 + uIF_2 + vIF_2 + uvIF_2$" , Designs, Codes and Cryptography, Vol. 54, No. 1, pp. 61-81.

24. Yıldız B., Karadeniz S.,(Dec. 2010), "Self dual codes over "$IF_2 + uIF_2 + vIF_2 + uvIF_2$", Journal of the Franklin Institute, Vol. 347, No. 10, , pp. 1888-1894

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Adı Soyadı : Abdullah DERTLİ

Uyruğu: T.C.

Doğum Tarihi ve Yeri: 10.11.1987, Alucra-Giresun

e-mail: **abdullah.dertli@hotmail.com**

EĞİTİM DURUMU

İlköğretim: Neyyir Turhan İlköğretim Okulu, İstanbul 2000

Lise: Fatih Şehremini Lisesi (YDA), İstanbul 2004

Lisans: Trakya Üniversitesi Fen Edebiyat Fakültesi Matematik Bölümü, 2009

Yüksek Lisans: Trakya Üniversitesi Fen Bilimleri Enstitüsü, 2012