T.C.

TRAKYA ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

HADAMARD KODLARI VE HALKALAR ÜZERİNDEKİ KODLAR

MUSTAFA ÖZKAN

DOKTORA TEZİ

MATEMATİK ANABİLİM DALI

Tez Danışmanı: Doç. Dr. FİGEN ÖKE

EDİRNE-2016

T.Ü. Fen Bilimleri Enstitüsü onayı

Prof. Dr. Murat YURTCAN
Fen Bilimleri Enstitüsü Müdürü

Bu tezin Doktora tezi olarak gerekli şartları sağladığını onaylarım.

Prof. Dr. Hülya İŞCAN
Anabilim Dalı Başkanı Y.

Bu tez tarafımızca okunmuş, kapsamı ve niteliği açısından bir Doktora tezi olarak kabul edilmiştir.

Doç. Dr. Figen ÖKE
Tez Danışmanı

Bu tez, tarafımızca okunmuş, kapsam ve niteliği açısından Matematik Anabilim Dalında bir Doktora tezi olarak oybirliği ile kabul edilmiştir.

Jüri Üyeleri	İmza
Doç. Dr. Figen ÖKE (Danışman)	
Prof. Dr. Ahmet Sinan ÇEVİK	
Prof. Dr. Mustafa ÖZCAN	
Doç. Dr. Gökhan SOYDAN	
Doç. Dr. Yasemin ÇENGELLENMİŞ	

Tarih: 14.10.2016

T.Ü. FEN BİLİMLERİ ENSTİTÜSÜ
MATEMATİK DOKTORA PROGRAMI
DOĞRULUK BEYANI

İlgili tezin akademik ve etik kurallara uygun olarak yazıldığını ve kullanılan tüm literatür bilgilerinin kaynak gösterilerek ilgili tezde yer aldığını beyan ederim.

14/09/2016

Mustafa ÖZKAN

Doktora Tezi

Hadamard Kodları ve Halkalar Üzerindeki Kodlar

T.Ü. Fen Bilimleri Enstitüsü

Matematik Anabilim Dalı

ÖZET

Bu tezin amacı yeni ve iyi kodların varlığını ortaya koymaktır. Tez çalışmasında önce kodlama teorisi ile ilgili ön bilgiler verilmiştir. Belirli halkalar üzerinde özel üreteçler oluşturulmuş, bu üreteçler ile özel kodlar yazılmış ve bu kodların Hadamard kodları ile bağlantısı ifade edilmiştir. Quasi-cyclic kod olan Hadamard kodlar tespit edilmiştir. Hadamard kodlara eşit ya da denk olan tek kod, çift kod gibi farklı kodlar bulunmuştur. Ardından p bir asal sayı olmak üzere $u^3 = v^2 = 0, u.v = v.u = 0$ iken $\mathbb{F}_p[u,v] \big/ < u^3, v^2, u.v >$ tipinde yeni halkalar yazılmış ve bu halkaların üzerinde ağırlık fonksiyonları tanımlanmıştır. Ayrıca yeni Gray dönüşümleri verilerek bu halkaların bilinen halkalar ve Galois cisimleri ile ilişkisi gösterilmiştir. Burada $p = 2$ durumu için 16 elemanlı halkada constacyclic kodlar çalışılmıştır. $p \geq 3$ olan asal sayılar için ise p^4 elemanlı halkalar için cyclic kodlar çalışılmıştır. Bu tip halkalarda yazılan kodlar için yeni sonuçlar elde edilmiştir. Son bölümde ise elde edilmiş olan tüm yeni sonuçlar özet olarak sunulmuştur.

Yıl : 2016

Sayfa Sayısı : 82

Anahtar Kelimeler : Hadamard Kodlar, Lineer Kodlar, Halkalar Üzerindeki Kodlar, Gray dönüşümü, Cyclic kodlar, Lee Ağırlığı, Hamming Ağırlığı, Hadamard Matrisi, Quasi-Cyclic Kodlar, Constacyclic Kodlar, Galois Cismi.

Ph. D. Thesis

Hadamard Codes and Codes Over Rings
Trakya University Institute of Natural Sciences

Department of Mathematics

ABSTRACT

The aim of this thesis is to show the existence of new and good codes. In this thesis basic knowledge on coding theory is given. Special generators over certain rings are constructed, especial codes are written with these generators and the relation between these codes and Hadamard codes is established. Hadamard codes which are quasi-cyclic codes are obtained. Different codes which are equal or equivalent to Hadamard codes such as odd code, even code are found. Then new rings in type $\mathbb{F}_p[u,v]/_{<u^3,\ v^2,u.v>}$ are written in case of $u^3=v^2=0,\ u.v=v.u=0$ where p is a prime number and weight function over these rings are defined. Writing new Gray maps, the relations among these rings, another known rings and Galois fields are shown. For the case $p=2$, constacyclic codes over the ring which has 16 elements. For the case p is prime number such that $p\geq 3$, cyclic codes are studied over the ring which has p^4 elements. The new consequences are obtained for the codes writing over these kind rings are submitted and proofs are shown. In the last chapter all new consequences obtained are presented as a summary.

Year : 2016

Number of Pages : 82

Keywords : Hadamard Codes, Linear Codes, Codes Over Rings, Gray Map, Cyclic Codes, Lee Weight, Hamming Weight, Hadamard Matrix, Quasi-Cyclic Codes, Constacyclic Codes, Galois Field.

ÖNSÖZ

Bu çalışmanın üçüncü bölümünde Hadamard kodları ile ilgili yeni sonuçlar verilmiştir. Dördüncü bölümde ise yeni halkalar yazılmış ve bu halkalar üzerindeki kodlarla ilgili bazı önemli sonuçlar literatüre kazandırılmıştır.

Çalışmalarım boyunca benimle yakından ilgilenen, hiçbir yardımı esirgemeyen değerli hocam Sayın Doç. Dr. Figen ÖKE'ye en derin saygı ve teşekkürlerimi sunarım.

Akademik yaşamımda bilgisini ve desteğini esirgemeyen değerli hocam Sayın Prof. Dr. Hülya İŞCAN'a teşekkür ederim.

Bu sürecin her aşamasında bana daha fazla sevgi, güç ve destek olan Annem Yüksel ÖZKAN'a, Babam Ramazan ÖZKAN'a, Ablam Sibel ÖZKAN'a ve Kardeşim Recep ÖZKAN'a sonsuz teşekkür ederim.

MUSTAFA ÖZKAN

İÇİNDEKİLER

SİMGELER DİZİNİ

$GF(p), \mathbb{F}_p$	: p elemanlı Galois cismi
$(n, M, d)\_$ Kod	: uzunluğu n, eleman sayısı M ve minimum uzaklığı d olan bir kod
$C^{\perp}$	: bir C kodunun duali
$P(C)$	: bir C kodunun polinom gösterimi
$w_R(r)$	: R halkası üzerinde bir elemanın ağırlığı
$w_R(C)$	: R halkası üzerinde bir C kodunun ağırlığı
$w_L(C)$	: bir C kodunun Lee ağırlığı
$w_{\text{hom}}(C)$	: bir C kodunun homogeneous ağırlığı
$w_H(C)$	: bir C kodunun Hamming ağırlığı
G	: Üreteç matrisi
H	: Parity-check matrisi
M	: Hadamard matrisi
B_n	: İkili Hadamard matrisi
M_n	: Normalleştirilmiş Hadamard matrisi
A_n	: İkili normalleştirilmiş Hadamard matrisi
${}_1C$	: birinci tekrarlı oluşum kodu
${}_2C$	: ikinci tekrarlı oluşum kodu
$odd(C)$	: tek kod
$even(C)$	: çift kod
$C_1 \otimes C_2$	: C_1 ve C_2 kodlarının direkt çarpımı
$C_1 \oplus C_2$	: C_1 ve C_2 kodlarının direkt toplamı

BÖLÜM 1

GİRİŞ

Bir kod tanımı; uzunluğu n, eleman sayısı M ve minimum uzaklığı d olmak üzere (n, M, d) parametreleri ile verilir. Kodun parametreleri için kod sözcükleri şifrelenmiş mesajlar olduğundan kod sözcüğünün iletiminin hızlı olması için uzunluğu kısa olmalıdır. Tersine kodun eleman sayısının fazla ve minimum uzaklığının büyük olması istenir. Kodun eleman sayısı fazla olursa daha çok mesaj şifrelenebilir ve kodun minimum uzaklığının da büyük olması kodun hata tespit etme ve hata düzeltme kapasitesini arttırır. Bu üç parametreyi daha iyi duruma getirmek kodlama teorisinin problemlerindendir. n, M ve d parametrelerini optimize etmek iyi ve yeni kodlar bulunmasını sağlayacaktır. Cebir ve sayılar teorisi alanında önemli bir yer tutan kodlama teorisi son dönemlerde literatüre bir çok çalışma kazandırmıştır. Kodlama teorisinde temel problemlerden biri yeni kodlar yazmaktır. Yeni kodlar yazmak farklı metodlar ile yapılmaktadır. Bu metodlardan bir tanesi var olan kodlardan yeni kodlar yazılmasıdır. Tezin 3. bölümünde bu durum gerçekleştirilmiştir. Tezin 4. bölümünde ise kodlama teorisinde literatürde daha önce yer almamış yeni halkalar üzerinde belirli kod tipleri tanımlanmış ve bilinen kodlar ile ilişkisi inşa edilmiştir. Böylece kodlama teorisine zenginlik kazandırılmıştır.

1948 yılında Claude Elwood Shannon'un " A Mathematical Theory of Communication" [1] isimli makalesinin yayınlanması matematiksel olarak kodlama teorisinin başlangıcı oldu.

1972 yılında Ian F. Blake'nin " Codes Over Certain Rings" [2] başlıklı makalesi ile halkalar üzerinde kodlar yayınlanmaya başlandı. Devam eden yıllarda ise farklı halkalar üzerinde kodlar yazılmaya devam edildi ve bu kodların cisimler üzerindeki kodlar ile ilişkileri kuruldu.

1999 yılında Wolfmann tarafından $\mathbb{Z}_4$ halkası üzerinde cyclic ve negacyclic kodların yapısı ele alınmış ve bu kodların Gray görüntüleri alınarak literatürde birçok çalışmaya referans gösterilmiştir [3].

2000 yılında D. S. Krotov, yine $\mathbb{Z}_4$ halkası üzerindeki çalışmalara farklılık katarak "$\mathbb{Z}_4$ – lineer Perfect Codes" [4] isimli makalesi ile $\mathbb{Z}_4$ halkasının elemanlarının kullanarak özel matrisler oluşturmuş ve bu matrislerin ürettiği kodlar ile $\mathbb{Z}_2$ üzerinde mükemmel kod ilişkisini ortaya koymuştur. D. S. Krotov 2001 yılında bu çalışmasını genişleterek $\mathbb{Z}_4$ üzerinde lineer Hadamard kodların yazılacağını belirlemiştir [5].

2006 yılında Qian, Zhang ve Zhu [6], [7] nolu makalelerinde $u^2 = 0$ olmak üzere $\mathbb{F}_2 + u\mathbb{F}_2$ ve $u^3 = 0$ olmak üzere $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$ sonlu zincir halkalarını kullanarak bu halkalarda constacyclic kodları ele alıp binary kodlardaki karşılıklarını değerlendirmişlerdir.

2010 ve sonraki yıllarda B. Yıldız ve S. Karadeniz [8] ve [9] nolu makalelerinde $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ Frobenious halkasını kullanarak lineer kodlar ve constacyclic kodlar üzerine çalışmalar yapmışlardır. Bu çalışmaları ile halkalar üzerindeki kodlara zenginlik kazandırmışlardır. 2013 yılında Xiaofang, bu çalışmalardaki $u.v = v.u = 0$ koşulunu alarak $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2$ halkasında constacyclic kodları çalışmıştır [10].

Üçüncü bölümde bu çalışmalar doğrultusunda belirli halkaların elemanları ile özel matrisler inşa edilmiştir. Bu matrislerin ürettiği kodlar sınıflandırılmış ve Hadamard kodları ile ilişkisi bulunmuştur. $u^2 = 0$ iken $\mathbb{F}_2 + u\mathbb{F}_2$, $v^2 = 1$ iken $\mathbb{F}_2 + v\mathbb{F}_2$, $v^2 = v$ iken $\mathbb{F}_2 + v\mathbb{F}_2$, $u^3 = 0$ iken $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$ ve $u^{m+1} = 0$ iken de ise $\mathbb{F}_2 + u\mathbb{F}_2 + ... + u^m\mathbb{F}_2$ halkalarında yazılan bu kodların ve dual kodların parametreleri hesaplanarak iyi kodlar bulunması sağlanmıştır. Ayrıca Hadamard kodların Hadamard matrisleri kullanılmadan da elde edilebileceği ortaya konulmuştur. Yine quasi-cyclic kod olan Hadamard kodların varlığı tespit edilmiştir. Bu çalışmalar genişletilerek direkt toplam, direkt çarpım kodları, tek kodlar, çift kodlar ve tekrarlı oluşum kodlarının Hadamard kodlar ile ilişkisi ortaya konulmuştur.

Literatürde sonlu zincir halkaları, Frobenious Halkaları gibi halkalarda cyclic, quasi-cyclic ve constacyclic kodlar üzerine bazı çalışmalar mevcuttur. Tezin dördüncü bölümünde böyle halkalar dışında idealleri bir kurala göre oluşturulmayan farklı

halkalar bulunmuş, bunların üzerinde cyclic, quasi-cyclic ve constacyclic kodları çalışılmış ve bu kod tiplerinin Galois cisimlerinde bu kodlar ile bağlantısı kurulmuştur. Buradan $u^3=0,\ v^2=0$ ve $u.v=v.u=0$ koşulları sabit tutularak $\mathbb{F}_p[u,v]\big/_{<u^3,\ v^2,u.v>}$ halkaları $\mathbb{F}_p+v\mathbb{F}_p+u\mathbb{F}_p+u^2\mathbb{F}_p$ halkalarına izomorftur. $\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2+u^2\mathbb{F}_2$ halkasında constacyclic kodlar ile $\mathbb{F}_2$ Galois cisminde quasi-cyclic kodlar inşa edilmiştir. $p\geq 3$ asal sayı olmak üzere $\mathbb{F}_p+v\mathbb{F}_p+u\mathbb{F}_p+u^2\mathbb{F}_p$ halkalarında ise cyclic kodlar ile $\mathbb{F}_p$ Galois cisminde quasi-cyclic kodlar ele alınmıştır.

Tezin son bölümünde üçüncü ve dördüncü bölümlerde elde edilen sonuçlar özet halinde sunulmuştur.

BÖLÜM 2

KODLAMA TEORİSİ

Bu bölümde kod kavramı ve diğer bölümlerde kullanılacak temel tanım, önerme ve teoremlere yer verilecektir.

2.1. Kod ile ilgili temel kavramlar

Bu alt bölümde kodlama teorisinde kullanılan bazı temel kavramlar verilecektir.

2.1.1. TANIM ([11]): q elemanlı bir $A=\{a_1,a_2,...,a_q\}$ kümesine kod alfabesi ve elemanlarına kod sembolleri denir.

(i) $i=1,2,...,n$, her $w_i \in A$ için n uzunluğunda bir $q-$ary sözcüğü $w=(w_1,w_2,...,w_n)$ olarak tanımlanır.

(ii) A kümesi üzerindeki n uzunluklu $q-$ary sözcüklerinin oluşturduğu C kümesine bir $q-$ary kod denir.

(iii) C kodunun bir elemanına kod sözcüğü denir.

(iv) C deki kod sözcüğü sayısı $|C|=M$ ile gösterilir ve C nin boyutu olarak adlandırılır.

(v) C kodunun bilgi iletim hızı $\dfrac{\log_q M}{n}$ dir.

(vi) n uzunluğunda M elemanlı bir kod $(n,M)\_$ kod olarak tanımlanır.

2.1.2. TANIM ([11]): $i=1,2,...,n$, için $x_i,\ y_i \in A$ olsun. $x=(x_1,x_2,...,x_n)$, $y=(y_1,y_2,...,y_n)$ sözcükleri arasındaki uzaklık $d(x,y)=\left|\{\ i \mid x_i \neq y_i\ \}\right|$ olarak tanımlanır. Burada $d(x_i,y_i)=\begin{cases}0 & ;x_i=y_i\\ 1 & ;x_i\neq y_i\end{cases}$ olmak üzere

$d(x,y) = d(x_1,y_1) + d(x_2,y_2) + ... + d(x_n,y_n)$ şeklinde tanımlanır.

2.1.3. ÖNERME ([11]): x, y, z, A üzerinde n uzunluğunda sözcükler olsun.

(i) $0 \le d(x,y) \le n$

(ii) $d(x,y) = 0 \Leftrightarrow x = y$

(iii) $d(x,y) = d(y,x)$

(iv) $d(x,z) \le d(x,y) + d(y,z)$

koşulları sağlanır.

2.1.4. TANIM ([11]): Bir C kodunun minimum uzaklığı $d(C) = \min\{\, d(x,y) \mid x \neq y,\ x,y \in C \,\}$ biçiminde tanımlanır.

2.1.5. TANIM ([12]): C koduna uzunluğu n, eleman sayısı M ve minimum uzaklığı d olan bir $(n,M,d)\_$ parametreli kodu adı verilir.

2.1.6. TANIM ([12]): C_1, C_2 iki kod olsun.

C_2 kodundaki her bir kod sözcüğünün aynı bileşenine permütasyon uygulanması veya C_2 kodundaki her bir kod sözcüğünün herhangi iki bileşeninin yer değiştirilmesi ile C_1 kodu elde edilirse C_1 ve C_2 kodları birbirine denktir denir.

2.1.7. TANIM ([11]): $d = 2t+1,\ t \in \mathbb{N}$ olmak üzere bir q- ary $(n,M,d)_$kodu için $m.\left\{ \binom{n}{0} + \binom{n}{1}.(q-1) + ... + \binom{n}{t}.(q-1)^t \right\} = q^n$ eşitliği sağlanıyorsa bu koda mükemmel kod denir.

2.1.8. TANIM ([5]): A ve B sıralı iki küme olsun. Her $(a_1,b_1), (a_2,b_2) \in A \times B$ için $(a_1,b_1) \le (a_2,b_2) \Leftrightarrow a_1 < a_2$ veya ($a_1 = a_2$ ve $b_1 \le b_2$) şeklinde tanımlı $\le$ sıralama bağıntısı Lexicographically sıralama olarak adlandırılır.

2.1.9. TANIM ([13]): p bir asal sayı, $t \in \mathbb{Z}_+$ olmak üzere $q = p^t$ yazılsın, f, $\mathbb{Z}_p[x]$ de t. dereceden asal bir polinom olmak üzere $\mathbb{F}_q \cong \mathbb{Z}_p[x] \big/ (f)$ biçiminde yazılan q elemanlı $\mathbb{F}_q$ cismine bir Galois cismi denir. $t = 1$ iken $\mathbb{F}_p \cong \mathbb{Z}_p$ olur. Galois cismi $GF(q)$ ya da $\mathbb{F}_q$ olarak gösterilir.

2.1. Lineer kodlar

2.2.1. TANIM ([11]): $\mathbb{F}_q^n$, $\mathbb{F}_q$ üzerinde bir vektör uzayı olsun. $\mathbb{F}_q^n$ nin her alt uzayı $\mathbb{F}_q$ cismi üzerinde n uzunluklu bir lineer kod olarak tanımlanır.

R bir halka olmak üzere R^n , R üzerinde bir modül olsun. R^n nin her alt modülü R halkası üzerinde n uzunluklu bir lineer kod olarak tanımlanır.

2.2.2. TANIM ([11]): C , $\mathbb{F}_q^n$ vektör uzayının k boyutlu bir alt uzayı ise C koduna bir $[n,k]_$kod adı verilir. Eğer C kodunun minimum Hamming uzaklığı $d(C)=d$ ile gösterilirse C bir lineer $[n,k,d]_$koddur denir.

2.2.3. TANIM ([11]): Her $x=(x_1,x_2,...,x_n)\in \mathbb{F}_q^n$ için

$w(x)=\left|\ \{\ i\ \ \middle|\ \ x_i\neq 0, i=1,2,...,n\ ,\ x_i\in IF_q\}\ \right|$ sayısına x elemanının Hamming ağırlığı denir. Eğer C, $\mathbb{F}_q$ üzerinde bir lineer kod ise

$w(C)=\min\{\ w(x)\ \ \middle|\ \ x_i\neq 0\ ,\ x\in C\ \}$ sayısına C kodunun Hamming ağırlığı denir.

Cisimler üzerindeki kodlar için Hamming ağırlığı verilirken, halkalar üzerindeki kodlar için farklı halkalarda tanımlanan kodlarda farklı ağırlık fonksiyonları verilir. 3. ve 4. bölümde farklı halkalar için ağırlık fonksiyonları verilmiştir.

2.2.4. ÖNERME ([13]): Her $x,y\in \mathbb{F}_q^n$ için $d(x,y)=w(x-y)$ dir.

2.2.5. TEOREM ([13]): C, $\mathbb{F}_q$ cismi üzerinde bir n uzunluğunda lineer kod ise $d(C)=w(C)$ sağlanır.

2.2.6. TANIM ([12]): C bir lineer $[n,k]_$kod olsun. C nin tabanındaki k tane eleman kullanılarak elde edilen $k\times n$ tipindeki matrise C kodunun üretici matrisi denir ve G ile gösterilir.

2.2.7. TANIM ([13]): C bir $q_$ary $[n,k]_$kod olsun.

$C^{\perp}=\{v\in \mathbb{F}_q^n\ \ \middle|\ \ u.v=0\ ,\ \forall\ u\in C\ \}$ kümesine C kodunun duali denir.

2.2.8. ÖNERME ([14]): C, $\mathbb{F}_q$ üzerinde bir lineer $[n,k]_$kod ise $C^{\perp}$ de $\mathbb{F}_q$ üzerinde bir lineer $[n,n-k]_$koddur.

2.2.9. TANIM ([14]): C bir $[n,k]\_$ kod ise $C^{\perp}$ nin üretici matrisine parity-check matrisi denir ve H ile gösterilir. H, $(n-k)\times n$ tipinde $G.H^{\mathrm{T}}=0$ koşulunu sağlayan bir matristir. Bir C lineer $[n,k]\_$ kodunun parity-check matrisi H ise $C=\{x=(x_1,x_2,...,x_n)\in \mathbb{F}_q^n \mid [\, x_1\, x_2\, ...\, x_n\,]_{1\times n}.H^{\mathrm{T}}{}_{n\times(n-k)}=[0]_{1\times(n-k)}\}$ biçiminde ifade edilir.

2.2.10. TANIM: R bir halka, $C\subseteq R^n$ bir lineer kod olmak üzere

$$\tau: \quad R^n \longrightarrow R^n$$

$$(c_0,c_1,...,c_{n-1})\mapsto \tau(c_0,c_1,...,c_{n-1})=(c_{n-1},c_0,...,c_{n-2})$$

dönüşümü için $\tau(C)=C$ oluyorsa C koduna R üzerinde bir cyclic kod denir.

Bu tanım R halkası yerine $\mathbb{F}_q$ cismi üzerinde de verilebilir.

2.2.11. TEOREM ([13]): $\mathbb{F}_q$ üzerinde,

$$\rho:\mathbb{F}_q^n \longrightarrow \mathbb{F}_q[x]\Big/_{<x^n-1>}$$

$$a=(a_0,a_1,...,a_{n-1})\mapsto \rho(a)=a_0+a_1x+...+a_{n-1}x^{n-1}+<x^n-1>$$

lineer dönüşümü verilsin. $C\subseteq\mathbb{F}_q^n$ nin cyclic kod olması için gerekli ve yeterli koşul $\rho(C)\subseteq \mathbb{F}_q[x]\Big/_{<x^n-1>}$ nin bir ideali olmasıdır.

Bu teorem $\mathbb{F}_q$ cismi yerine R halkası üzerinde de gerçeklenir.

2.2.12. TANIM: R bir halka ve $\lambda\in R$ olsun, $C\subseteq R^n$ bir lineer kod olmak üzere

$$\nu: \quad R^n \longrightarrow R^n$$

$$(c_0,c_1,...,c_{n-1})\mapsto \nu(c_0,c_1,...,c_{n-1})=(\lambda.c_{n-1},c_0,...,c_{n-2})$$

dönüşümü için $\nu(C)=C$ oluyorsa C koduna R üzerinde bir λ-constacyclic kod denir.

2.2.13. TANIM: $\mathbb{F}_q$ cismi üzerinde C, $a.n$ uzunluğunda bir lineer kod olsun.

$$\sigma^{\otimes a}: \mathbb{F}_q{}^{n.a} \longrightarrow \mathbb{F}_q{}^{n.a}$$

$$(d_1,d_2,...,d_{n.a})\mapsto \sigma^{\otimes a}(d_1,d_2,...,d_{n.a})=(d_a,d_1,...,d_{a-1},d_{2a},d_{a+1},...,d_{2a-1},$$
$$d_{3a},d_{2a+1},...,d_{3a-1},...,d_{n.a},d_{(n-1).a+1},...,d_{n.a-1})$$

permütasyonu için $\sigma^{\otimes a}(C)=C$ koşulu sağlanıyorsa C koduna $\mathbb{F}_q$ üzerinde $a.$ mertebeden bir quasi-cyclic kod denir.

Benzer tanım R halkası üzerinde de verilebilir.

2.3. Hadamard kodların yapısı

Bu alt bölümde Hadamard matrisleri ve Hadamard kodları ile temel bilgiler verilecektir.

2.3.1. TANIM ([15]): M , $n\times n$ mertebeden bir matris ve M^t, M matrisinin transpozu olsun. M matrisinin her bir bileşeni sadece -1 ya da 1 den oluşuyorsa ve $M.M^t = n.I_n$ eşitliği sağlanıyorsa M matrisine bir Hadamard matrisi denir.

2.3.2. LEMMA ([15]): M , $n\times n$ lik bir Hadamard matrisi ise M terslenebilir bir matristir ve M^t matrisi de bir Hadamard matrisidir.

2.3.3. LEMMA ([15]): M , $n\times n$ lik bir Hadamard matrisi olsun. $R_1, R_2, ..., R_n$ matrisleri M nin satırları olmak üzere M nin herhangi bir satırı -1 ile çarpıldığında elde edilen matris yine Hadamard matrisidir.

2.3.4. LEMMA([15]) :

(i) Bir Hadamard matrisi için ilk satır ve ilk sütundaki tüm bileşenler 1 olacak biçimde düzenlendiğinde yine bir Hadamard matrisi elde edilir.

(ii) Bir Hadamard matrisinde herhangi iki satır ya da iki sütun yer değiştirdiğinde elde edilen matris bir Hadamard matristir.

2.3.5. TANIM([15]): İlk satır ve ilk sütundaki tüm bileşenleri 1 olan Hadamard matrisine normalleştirilmiş Hadamard matrisi denir ve M_n ile gösterilir.

2.3.4. Lemmadan; bir Hadamard matrisi varsa normalleştirilmiş Hadamard matrisi de vardır.

2.3.6. ÖNERME([15]): M $n\times n$ lik bir Hadamard matrisi ise $\begin{bmatrix} M & M \\ M & -M \end{bmatrix}$, $2n\times 2n$ lik bir Hadamard matrisidir.

2.3.7. TEOREM ([15]): $n\times n$ lik bir Hadamard matrisi var ise $n = 1, 2$ ya da 4 ün bir katı olur.

2.3.8. TANIM([15]): İki Hadamard matrisi için birinin satırları ya da sütunları -1 ile çarpıldığında veya satırları ya da sütunlarına permütasyon uygulandığında diğeri elde edilebiliyorsa bu iki Hadamard matrisi denktir denir.

2.3.9. TANIM([15]): M $n\times n$ lik bir Hadamard matrisi olsun. M matrisinin tüm bileşenleri 1 ler yerine 0, -1 ler yerine 1 yazılarak yeniden düzenlendiğinde elde edilen $n\times n$ lik matrise ikili Hadamard matrisi denir ve B_n ile gösterilir. $n\times n$ lik bir M_n normalleştirilmiş Hadamard matrisi 1 ler yerine 0, -1 ler yerine 1 yazılarak yeniden düzenlendiğinde elde edilen $n\times n$ lik matrise ikili normalleştirilmiş Hadamard matrisi denir ve A_n ile gösterilir.

A_n matrisinin herhangi iki satırı ortagonal ise A_n in herhangi iki satırı $\frac{n}{2}$ yerde aynıdır. A_n in herhangi iki satırı $\frac{n}{2}$ yerde farklıdır. A_n in herhangi iki satırı arasındaki Hamming uzaklığı $\frac{n}{2}$ dir. A_n in sıfırdan farklı herhangi bir satırının ağırlığı $\frac{n}{2}$ dir.

2.3.10. TANIM([15]): A_n $n\times n$ lik bir ikili normalleştirilmiş Hadamard matrisi olsun. A_n matrisinin ilk sütunu silinerek ile satırları bir ∂_n kümesine yazılsın. ∂_n kümesinin elemanları; $n-1$ uzunluğunda, n tane elemana sahip ve iki eleman arasındaki minimum uzaklığı $\frac{n}{2}$ olan elemanlardır. ∂_n kümesinin tüm elemanları ve her bir elemanın tümleyenleri bir β_n kümesine yazılsın. β_n kümesinin elemanları; $n-1$ uzunluğunda, $2n$ tane elemana sahip ve iki eleman arasındaki minimum uzaklığı $\frac{n}{2}-1$ ($n>2$ için) olan elemanlardır. A_n matrisinin her bir satırı ve bunların tümleyenleri bir $\Im_n$ kümesine yazılsın. $\Im_n$ kümesinin elemanları; n uzunluğunda , $2n$

tane elemana sahip ve iki eleman arasındaki minimum uzaklığı $\frac{n}{2}$ olan elemanlardır. Yukarıda ifade edilen ∂_n, β_n ve $\Im_n$ kümelerine Hadamard küme denir.

2.3.11. TANIM([15]): Bir $n \times n$ lik B_n binary Hadamard matrisinde tüm satırları ve bu satır vektörlerinin tümleyenleri de ilave edilerek yeni bir küme oluşturulsun. Bu kümedeki tüm vektörler kendileri, tümleyenleri ve tamamlayıcıları olarak düzenlendiğinde elde edilen $(2n, 4n, n)$ parametreli kümeye Hadamard kod denir.

BÖLÜM 3

HADAMARD KODLAR

Bu bölümde; belirli halkaların elemanları kullanılarak özel matrisler oluşturulmuştur. Üreteç matrisleri bu matrisler olan olarak kullanarak özel kodlar elde edilmiştir. Elde edilen kodlar için Gray görüntüleri alınarak Hadamard kodlar yazılmıştır. Böylece Hadamard kodların sadece Hadamard matrisler ile değil aynı zamanda burada verilen metod ile de elde edilebileceği sonucuna varılmıştır. Ayrıca Hadamard kodlarının cyclic kodlar ve quasi-cyclic kodlar ile ilişkisi tespit edilmiştir. Bunlara ilave olarak tanımlanan özel kodların hangi tip Hadamard kodlarına karşılık geldiği belirlenmiştir.

Bu çalışmada $u^2=0$ iken $\mathbb{F}_2+u\mathbb{F}_2$ halkası, $v^2=1$ ve $v^2=v$ iken $\mathbb{F}_2+v\mathbb{F}_2$ halkalarında, $u^3=0$ iken $\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2$ halkası ve $u^{m+1}=0$ iken de $\mathbb{F}_2+u\mathbb{F}_2+...+u^m\mathbb{F}_2$ halkaları kullanılarak Hadamard kodları ele alınmıştır. Bu bölüm Hadamard kodlar ile ilgili orijinal sonuçlar içerir.[25]

3.1. Hadamard Kodlar ile $\mathbb{F}_2+u\mathbb{F}_2$ Üzerindeki Özel Kodlar Arasındaki İlişki ve Hadamard Kodlar üzerine Sonuçlar

Bu bölümde önce $u^2=0$ durumda $\mathbb{F}_2+u\mathbb{F}_2$ halkası ile bilgi verilmiş, bu halka üzerinde bazı özel matrisler ve kodlar yazılmıştır. Sonra Hadamard kodlar tanımlanmış ve tipleri ortaya konulmuştur. Dahası bu kodlar yardımıyla tek kod, çift kod ve tekrarlı oluşum kodları yazılmış, bunların hangi tip Hadamard kodlara karşılık geldiği belirlenmiştir. Bu özel kodların direkt toplam ve direkt çarpımları üzerine yeni sonuçlar verilmiştir. Ayrıca değişik tipteki tüm kodların dualleri de elde edilmiştir.

$u^2 = 0$ olması durumunda $\mathbb{F}_2[u] \Big/ _{<u^2>} = \{ a_0 + a_1.u + <u^2> \mid a_0, a_1 \in \mathbb{F}_2 \}$ halkası $\mathbb{F}_2 + u\mathbb{F}_2$ halkasına izomorftur. $\mathbb{F}_2 + u\mathbb{F}_2 = \{0,1,u,1+u\}$, aşığıda tanımlanan + ve • işlemleri ile bir halkadır.

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

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

$R = \mathbb{F}_2 + u\mathbb{F}_2$ halkasının üç ideali vardır. Bu idealler $\langle 0 \rangle$, $\langle 1 \rangle$ ve $\langle u \rangle$ olup $\langle 0 \rangle \subseteq \langle u \rangle \subseteq \langle 1 \rangle = R$ sağlanır.

3.1.1. TANIM : $R = \mathbb{F}_2 + u\mathbb{F}_2$ halkası üzerinde;

her $r \in R$ için $w_L(r) = \begin{cases} 0 & , r = 0 \\ 1 & , r = 1, 1+u \\ 2 & , r = u \end{cases}$

biçiminde tanımlanan fonksiyona, R üzerinde Lee ağırlık fonksiyonu denir.

Bu durumda her $r = (r_1, r_2, ..., r_n) \in R^n$ için $w_L(r) = \sum_{i=1}^{n} w_L(r_i)$ eşitliği gerçeklenir.

3.1.2. TANIM : $\mathbb{F}_2$ cismi üzerinde;

her $c \in \mathbb{F}_2$ için $w_H(c) = \begin{cases} 0 & , c = 0 \\ 1 & , c = 1 \end{cases}$ biçiminde tanımlanan fonksiyona $\mathbb{F}_2$ üzerinde Hamming ağırlık fonksiyonu denir. Bu durumda her $c = (c_1, c_2, ..., c_n) \in \mathbb{F}_2^n$ için $w_H(c) = \sum_{i=1}^{n} w_H(c_i)$ olur.

3.1.3. TANIM : Her $a, b \in R^n$, $a \neq b$ vektörleri arasındaki uzaklık $d_L(a,b) = w_L(a-b)$ olmak üzere, bir C kodunun minimum Lee uzaklığı $d_L(C) = \min\{d_L(a,b) \mid a,b \in C, a \neq b\}$ biçiminde tanımlanır.

$\mathbb{F}_2^n$ de Lee ağırlığı yerine Hamming ağırlığı yazılarak benzer tanım verilir. $\mathbb{F}_2^n$ üzerinde bir C kodunun minimum Hamming uzaklığı $d_H(C)$ ile gösterilir.

3.1.4. TANIM : $R = \mathbb{F}_2 + u\mathbb{F}_2$ halkası üzerinde bir C, $[n,k,d]\_$ kodunun üreteç matrisi $G = \begin{bmatrix} G_1 \\ u.G_2 \end{bmatrix}$ biçimindedir. Burada G_1 matrisi, bileşenleri $\mathbb{F}_2 + u\mathbb{F}_2$ halkasında olan $k_1 \times n$ boyutlu bir matris, G_2 matrisi de bileşenleri $\mathbb{F}_2$ cisminde olan $k_2 \times n$ boyutlu bir matristir. Dolayısı ile $|C| = 2^{2k_1+k_2}$ dir. Burada G matrisi ile üretilen kod $C = \{\ c = (c_1, c_2).\begin{bmatrix} G_1 \\ u.G_2 \end{bmatrix} \Big|\ c_1 \in R^{k_1},\ c_2 \in \mathbb{F}_2^{k_2}\ \}$ biçiminde tanımlanır ve bu kod $4^{k_1}.2^{k_2}$ tipinde bir koddur.

3.1.5. TANIM : $R = \mathbb{F}_2 + u\mathbb{F}_2$ halkası üzerinde bir C, $[n,k,d]\_$ kodunun parity-check matrisi $H = \begin{bmatrix} H_1 \\ u.H_2 \end{bmatrix}$ biçimindedir. Burada H_1 matrisi, bileşenleri $\mathbb{F}_2 + u\mathbb{F}_2$ halkasında olan $(n-k_1-k_2)\times n$ boyutlu bir matris, H_2 matrisi de bileşenleri $\mathbb{F}_2$ cisminde olan $k_2 \times n$ boyutlu bir matristir. Burada H matrisi ile üretilen C kodunun duali $C^{\perp} = \left\{ c_1 \in R^n \Big|\ H.c_1^T = 0 \right\}$ biçiminde tanımlanır.

3.1.6. TANIM : $R = \mathbb{F}_2 + u\mathbb{F}_2$ olmak üzere;

$$\Phi :\ R^n \longrightarrow \mathbb{F}_2^{2n}$$

$$(r_1, r_2, ..., r_n) \mapsto \Phi(r_1, r_2, ..., r_n) = (b_1, b_2, ..., b_n, a_1 + b_1, a_2 + b_2, ..., a_n + b_n)$$

biçiminde tanımlanan dönüşüme R halkası üzerindeki Gray dönüşümü denir. Burada $1 \le i \le n$, $a_i, b_i \in \mathbb{F}_2$ için $r_i = a_i + ub_i \in R$ dır.

Bu tanım ile $\mathbb{F}_2 + u\mathbb{F}_2$ üzerindeki n uzunluğunda bir kodun Gray görüntüsü $2n$ uzunluğunda bir binary kod olduğu görülür. R^n üzerinde tanımlanan Lee uzaklığı ve $\mathbb{F}_2^{2n}$ üzerinde tanımlanan Hamming uzaklığı arasında her $a, b \in R^n$ için $d_L(a,b) = d_H(\Phi(a), \Phi(b))$ ilişkisi vardır. Bu Gray dönüşümünün bir izometri olduğunu göstermektedir.

3.1.7. TANIM : $R = \mathbb{F}_2 + u\mathbb{F}_2$ halkası üzerinde;

$\alpha_1, \alpha_2 \in \mathbb{Z}_+ \cup \{0\}$ için ilk satır bileşenleri $\{1\}$ kümesinden, diğer satır elemanları $\alpha_2 = 0$ iken $\{0,1,u,1+u\}$ kümesinden ve $\alpha_1 = 0$ iken $\{0,u\}$ kümesinden seçilmek üzere, sütunları da lexicographically sıralama bağıntısına göre sıralanmış olacak biçimde N^{α_1,α_2} matrisleri yazılsın ve satır sayısı $\alpha_1 + \alpha_2 + 1$ olan özel olarak oluşturulan bu N^{α_1,α_2} matrisine üreteç matrisi denir.

Aşağıda N^{α_1,α_2} matrisleri için birkaç örnek verilmiştir.

$$N^{0,0} = \begin{bmatrix} 1 \end{bmatrix},\ N^{0,1} = \begin{bmatrix} 1 & 1 \\ 0 & u \end{bmatrix},\ N^{0,2} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & u & u \\ 0 & u & 0 & u \end{bmatrix},$$

$$N^{0,3} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & u & u & u & u \\ 0 & 0 & u & u & 0 & 0 & u & u \\ 0 & u & 0 & u & 0 & u & 0 & u \end{bmatrix},\ N^{1,0} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & u & 1+u \end{bmatrix},$$

$$N^{2,0} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & u & u & u & u & 1+u & 1+u & 1+u & 1+u \\ 0 & 1 & u & 1+u & 0 & 1 & u & 1+u & 0 & 1 & u & 1+u & 0 & 1 & u & 1+u \end{bmatrix},$$

$$N^{1,1} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & u & u & 1+u & 1+u \\ 0 & u & 0 & u & 0 & u & 0 & u \end{bmatrix}.$$

3.1.8. TANIM : $R = \mathbb{F}_2 + u\mathbb{F}_2$ halkası üzerinde; her $\alpha_1, \alpha_2 \geq 0$ tamsayıları için $C^{\alpha_1,\alpha_2} = \{ (c_1,c_2).N^{\alpha_1,\alpha_2} \mid c_1 \in R^{\alpha_1+1}, c_2 \in \mathbb{F}_2^{\alpha_2} \}$ biçiminde yazılan koda N^{α_1,α_2} üreteç matrisi ile üretilmiş, uzunluğu $n = 2^{2\alpha_1+\alpha_2}$ olan $(n,4n,n)$ parametreli kod denir.

3.1.9. TEOREM : Φ, R^n üzerinde bir Gray dönüşümü olsun. C^{α_1,α_2}, N^{α_1,α_2} üreteç matrisi ile yazılan kod olmak üzere $\Phi(C^{\alpha_1,\alpha_2})$ kodu, $\mathbb{F}_2$ üzerinde $(2n,4n,n)$ parametreli bir Hadamard kodudur.

Kanıt: Boyutu $(\alpha_1 + \alpha_2 + 1) \times n$ olan N^{α_1,α_2} üreteç matrisi ile oluşturulan kod $C^{\alpha_1,\alpha_2} = \{ (c_1,c_2).N^{\alpha_1,\alpha_2} \mid c_1 \in R^{\alpha_1+1}, c_2 \in \mathbb{F}_2^{\alpha_2} \}$ biçimindedir. Tanımlanan bu kodun uzunluğu

$n = 2^{2\alpha_1+\alpha_2}$ dir. $C^{\alpha_1,\alpha_2} \subseteq R^n$ olan bu kodun bir tekrar kodu olduğu ve eleman sayısının da $4n$ olduğu açıktır. Buradan $\Phi(C^{\alpha_1,\alpha_2}) \subseteq \mathbb{F}_2^{2n}$ olduğundan $\Phi(C^{\alpha_1,\alpha_2})$, $(2n,4n,n)$ parametreli bir binary Hadamard kodu belirtir.

3.1.10. SONUÇ : $\alpha_1 = \alpha_2 = 0$ dışında; $(C^{\alpha_1,\alpha_2})^{\perp}$, C^{α_1,α_2} kodunun duali olmak üzere, $(C^{\alpha_1,\alpha_2})^{\perp}$ dual kodun parametresi $(n, \frac{4^n}{4n}, 4)$ olur. Ayrıca $\Phi((C^{\alpha_1,\alpha_2})^{\perp})$ kodu $(2n, \frac{4^n}{4n}, 4)$ _ parametreli bir kod olur.

Kanıt: C^{α_1,α_2} kodunun üreteç matrisi olan N^{α_1,α_2} matrisinin boyutu $(\alpha_1 + \alpha_2 + 1) \times n$ dir. Aynı zamanda $(C^{\alpha_1,\alpha_2})^{\perp}$ kodu için parity-check matrisidir. $(C^{\alpha_1,\alpha_2})^{\perp}$ kodunun bir elemanı, $N^{\alpha_1,\alpha_2}.c^T = 0$ koşulunu sağlar. Bu koşulu sağlayan sözcük sayısının $\frac{4^n}{4n}$ olduğu görülür. Kod sözcüklerinin en küçük ağırlığının 4 olduğu açıktır. Böylece $(C^{\alpha_1,\alpha_2})^{\perp}$ kodu $(n, \frac{4^n}{4n}, 4)$ parametresine sahip olur. Buradan $\Phi((C^{\alpha_1,\alpha_2})^{\perp})$ kodunun da $(2n, \frac{4^n}{4n}, 4)$ parametreli kod olduğu görülür.

3.1.11. TANIM : $n = 2^{2\alpha_1+\alpha_2}$ olmak üzere C^{α_1,α_2}, R üzerinde n uzunluğunda bir lineer kod olsun.

$$\tau : R^n \longrightarrow R^n$$

$$(c_1, c_2, ..., c_n) \mapsto \tau(c_1, c_2, ..., c_n) = (c_n, c_1, ..., c_{n-1})$$

permütasyonu için $\tau(C^{\alpha_1,\alpha_2}) = C^{\alpha_1,\alpha_2}$ koşulu sağlanıyorsa C^{α_1,α_2} koduna R üzerinde bir cyclic kod denir.

3.1.12. TANIM : $n = 2^{2\alpha_1+\alpha_2}$ olmak üzere D^{α_1,α_2}, $\mathbb{F}_2$ üzerinde $2n$ uzunluğunda bir lineer kod olsun.

$$\sigma^{\otimes 2} : \mathbb{F}_2^{2n} \longrightarrow \mathbb{F}_2^{2n}$$

$$(d_1, d_2, ..., d_{2n}) \mapsto \sigma^{\otimes 2}(d_1, d_2, ..., d_{2n}) = (d_n, d_1, ..., d_{n-1}, d_{2n}, d_{n+1}, ...d_{2n-1})$$

permütasyonu için $\sigma^{\otimes 2}(D^{\alpha_1,\alpha_2}) = D^{\alpha_1,\alpha_2}$ koşulu sağlanıyorsa D^{α_1,α_2} koduna $\mathbb{F}_2$ üzerinde 2. mertebeden bir quasi-cyclic kod denir.

3.1.13. ÖNERME : τ dönüşümü R^n üzerinde bir permütasyon, $\sigma^{\otimes 2}$ dönüşümü $\mathbb{F}_2^{2n}$ üzerinde bir permütasyon ve Φ, R^n den $\mathbb{F}_2^{2n}$ e yukarıda tanımlanan Gray dönüşümünü ise $\sigma^{\otimes 2} \circ \Phi = \Phi \circ \tau$ eşitliği sağlanır.

Kanıt: Her $1 \le i \le n$ için $c_i = a_i + ub_i \in R$ olmak üzere $c = (c_1, c_2, ..., c_n) \in R^n$ olsun. Bu durumda $c \in R^n$ in Gray görüntüsünü

$$\Phi(c) = \Phi(c_1, c_2, ..., c_n) = \Phi(a_1 + ub_1, a_2 + ub_2, ..., a_n + ub_n)$$
$$= (b_1, b_2, ..., b_n, a_1 + b_1, a_2 + b_2, ..., a_n + b_n)$$

olarak bulunur. Buradan $\sigma^{\otimes 2}(\Phi(c)) = (b_n, b_1, ..., b_{n-1}, a_n + b_n, a_1 + b_1, ..., a_{n-1} + b_{n-1})$.
elde edilir. Diğer taraftan,

$\tau(c_1, c_2, ..., c_n) = (c_n, c_1, ..., c_{n-1})$ dir. Böylece

$$\Phi(\tau(c)) = \Phi(\tau(c_1, c_2, ..., c_n)) = \Phi(c_n, c_1, ..., c_{n-1})$$
$$= (b_n, b_1, ..., b_{n-1}, a_n + b_n, a_1 + b_1, ..., a_{n-1} + b_{n-1})$$

elde edilir. Dolayısıyla istenen eşitlik görülmüş olur.

3.1.14. TEOREM : $\alpha_2 \neq 0$ olmak üzere, N^{α_1, α_2} üreteç matrisi ile elde edilen bir Hadamard kod $2.$mertebeden bir quasi-cyclic koddur.

Kanıt: $\alpha_2 \neq 0$ olsun. N^{α_1, α_2} üreteç matrisler ile elde edilen bir C^{α_1, α_2} kodunun uzunluğu $n = 2^{2\alpha_1 + \alpha_2}$ dir. Buradan bir C^{α_1, α_2} kodunun $\mathbb{F}_2$ cismi üzerinde Gray görüntüsü olan $\Phi(C^{\alpha_1, \alpha_2})$ kodunun uzunluğunun $2^{2\alpha_1 + \alpha_2 + 1}$ olduğu görülür. Bu durumda Hadamard matrisleri ile elde edilen Hadamard kodlarının $\Phi(C^{\alpha_1, \alpha_2})$ kodlarına eşit olduğu sonucuna varılır. 3.1.13. Önerme kullanılarak $\sigma^{\otimes 2}(\Phi(C^{\alpha_1, \alpha_2})) = \Phi(\tau(C^{\alpha_1, \alpha_2})) = \Phi(C^{\alpha_1, \alpha_2})$ eşitliği elde edilir. Φ bire-bir fonksiyon olduğundan $\sigma^{\otimes 2}(\Phi(C^{\alpha_1, \alpha_2})) = \Phi(C^{\alpha_1, \alpha_2})$ bulunur. Sonuç olarak $\Phi(C^{\alpha_1, \alpha_2})$ Hadamard kodu $2.$mertebeden bir quasi-cyclic koddur.

3.1.15. ÖRNEK : $C^{0,1}$ kodunu belirlemek için $N^{0,1}$ üreteç matrisini yazalım. $N^{0,1}$ matrisi $\begin{bmatrix} 1 & 1 \\ 0 & u \end{bmatrix}$ dir. Buradan $C^{0,1}$ kodunun elemanları $c_1 \in R$, $c_2 \in \mathbb{F}_2$ olmak üzere $c = (c_1, c_2).N^{0,1}$ biçimindeki elemanlardır.

$C^{0,1}=\{00,11,uu,1+u1+u,0u,11+u,u0u+11\}\subseteq R^2$ kodu için $d_L(C^{0,1})=2$ ve $\left|C^{0,1}\right|=8$ dir. Dolayısı ile $C^{0,1}$ kodunun parametresi $(2,8,2)$ olur.

Buradan $C^{0,1}$ kodunun Gray görüntüsü alındığında

$\Phi(C^{0,1})=\{0000,0011,1111,1100,0101,0110,1010,1001\}\subseteq\mathbb{F}_2^4$ kodu elde edilir. $\Phi(C^{0,1})$ kodu $(4,8,2)$ parametreli bir Hadamard koddur. Diğer taraftan $M=\begin{bmatrix}1 & 1\\ -1 & 1\end{bmatrix}$ bir normalleştirilmiş Hadamard matrisi olmak üzere, M Hadamard matrisinde 1 yerine 0 ve -1 yerine 1 yazılarak M marisinin satırlarından, 00 ve 10 vektörleri elde edilir. Bu vektörlerin tamamlayıcıları da ilave edilerek $00,10,11,01$ vektörleri oluşturulur. Bu 4 vektörün tamamlayıcıları alınır ve tekrarlayıcıları ile yeniden düzenlenirse $0000,0011,1111,1100,0101,0110,1010,1001$ vektörleri elde edilir. Bu vektörlerin oluşturduğu küme bir ikili kod belirtir. Bu kodun uzunluğu 4, eleman sayısı 8 ve Hamming ağırlığı 2 dir. Böylece M Hadamard matrisi ile bir Hadamard kodu elde edilir. Bulunan kod $(4,8,2)\_$ parametreli $\Phi(C^{0,1})$ koduna eşittir.

Ayrıca $(C^{0,1})^{\perp}=\{00,uu\}$ ve $\Phi((C^{0,1})^{\perp})=\{0000,1111\}$ olur. Bunun dışında $C^{0,1}$ kodu, $\tau(C^{0,1})=C^{0,1}$ koşulunu sağladığından bir cyclic koddur. Benzer biçimde $\sigma^{\otimes 2}(\Phi(C^{0,1}))=\Phi(C^{0,1})$ sağlandığından $\Phi(C^{0,1})$ kodu, 2. mertebeden bir quasi-cyclic koddur.

3.1.16. ÖRNEK : $C^{0,2}$ kodunu belirlemek için $N^{0,2}$ üreteç matrisini yazalım.

$N^{0,2}$ matrisi $\begin{bmatrix}1 & 1 & 1 & 1\\ 0 & 0 & u & u\\ 0 & u & 0 & u\end{bmatrix}$ dir. Buradan $C^{0,2}$ kodunun elemanları $c_1\in R$, $c_2\in\mathbb{F}_2^2$ olmak üzere $c=(c_1,c_2).N^{0,2}$ biçimindeki elemanlardır.

$C^{0,2}=\{\,0000,0u0u,00uu,0uu0,1111,11+u11+u,111+u1+u,11+u1+u1,\ uuuu,$
$u0u0,uu00,u00u,1+u1+u1+u1+u,1+u11+u1,1+u1+u11,1+u111+u\,\}\subseteq R^4$

olur. Bu kod için $d_L(C^{0,2})=4$ ve $\left|C^{0,2}\right|=16$ dır. Yani $C^{0,2}$ kodu bir $(4,16,4)\_$ koddur.

Buradan $C^{0,2}$ kodunun Gray görüntüsü

$$\Phi(C^{0,2}) = \{00000000, 01010101, 00110011, 01100110,$$
$$00001111, 01011010, 00111100, 01101001,$$
$$11111111, 10101010, 11001100, 10011001,$$
$$11110000, 10100101, 11000011, 10010110\} \subseteq \mathbb{F}_2^8$$

kodu olur. $\Phi(C^{0,2})$ kodu $(8,16,4)$ parametreli bir Hadamard koddur. Diğer taraftan $M = \begin{bmatrix} 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 1 \\ -1 & -1 & -1 & 1 \end{bmatrix}$ normalleştirilmiş bir Hadamard matrisi olmak üzere M Hadamard matrisinde 1 yerine 0 ve -1 yerine 1 yazılarak M marisinin satırlarından, $0000, 1010, 1100$ ve 0110 vektörleri elde edilir. Bu vektörlerin tamamlayıcılarını da ilave edilerek $0000, 1010, 1100$, 0110 , $1111, 0101, 0011$ ve 1001 vektörleri oluşturulur. Bu 8 vektörün tamamlayıcıları alınır ve tekrarlayıcıları ile yeniden düzenlenirse

$00000000, 01010101, 00110011, 01100110$, 11111111, $10101010, 11001100, 10011001,$

$00001111, 01011010, 00111100, 01101001, 11110000, 10100101, 11000011, 10010110$

vektörleri elde edilir. Bu vektörlerin oluşturduğu küme bir ikili kod oluşturur. Bu kodun uzunluğu 8, eleman sayısı 16 ve Hamming ağırlığı 4 tür. Böylece M Hadamard matrisi ile Hadamard kodu elde edilir. Bulunan kod $(8,16,4)$ _ parametreli $\Phi(C^{0,2})$ koduna eşittir. $(C^{0,2})^{\perp} = C^{0,2}$ olduğu için $C^{0,2}$ kodu self-dual koddur. Ayrıca $C^{0,2}$ kodu, $\tau(C^{0,2}) = C^{0,2}$ koşulunu sagladığından bir cyclic koddur. Benzer biçimde $\sigma^{\otimes 2}(\Phi(C^{0,2})) = \Phi(C^{0,2})$ saglandığından $\Phi(C^{0,2})$ kodu, 2. mertebeden bir quasi-cyclic koddur.

Aşağıda C^{α_1,α_2} kodları için tek kodlar çift kodlar ve tekrarlı oluşum kodları alınmıştır. Bu kodların C^{α_1,α_2} kodları için sınıflandırılması ve örnekleri verilmiştir.

3.1.17. TANIM : $\alpha_1, \alpha_2 \geq 0$ ve $n = 2^{2\alpha_1+\alpha_2}$ olmak üzere

$C^{\alpha_1,\alpha_2} = \{ (c_1, c_2).N^{\alpha_1,\alpha_2} \mid c_1 \in R^{\alpha_1+1}, c_2 \in \mathbb{F}_2^{\alpha_2} \}$, R halkası üzerinde bir $(n,4n,n)$ kod, $S' = \{00...0, uu...u\}$ R halkası üzerinde bir $(n,2,2n)$ kod,

$S''=\{00...0,11...1,uu...u,1+u1+u...1+u\}$ R halkası üzerinde bir $(n,4,n)$ kod olsun. S', S'' ve C^{α_1,α_2} kodları kullanılarak R halkası üzerinde elde edilen ${}_1C^{\alpha_1,\alpha_2}=\{\ (a,a+b)\ \big|\ a\in C^{\alpha_1,\alpha_2},\ b\in S'\}$ koduna $(2n,8n,2n)$ parametreli 1. tekrarlı oluşum kodu denir. Yine S', S'' ve C^{α_1,α_2} kodları kullanılarak elde edilen, R halkası üzerindeki ${}_2C^{\alpha_1,\alpha_2}=\{\ (a,a+b,a+u.b,a+(1+u).b)\ \big|\ a\in C^{\alpha_1,\alpha_2},\ b\in S''\}$ koduna $(4n,16n,4n)$ parametreli 2. tekrarlı oluşum kodu denir.

3.1.18. ÖNERME : $\alpha_1,\ \alpha_2\geq 0$ olmak üzere ${}_1C^{\alpha_1,\alpha_2}$ kodu C^{α_1,α_2+1} koduna denktir. Özel olarak $\alpha_1=0$ olduğunda ${}_1C^{0,\alpha_2}=C^{0,\alpha_2+1}$ dir.

Kanıt: ${}_1C^{\alpha_1,\alpha_2}=\{\ (a,a+b)\ \big|\ a\in C^{\alpha_1,\alpha_2},\ b\in S'\}$ kodunu ele alınsın. Burada $b=00...0$ veya $b=uu...u$ elemanlarıdır. Her $a\in C^{\alpha_1,\alpha_2}$ kod sözcüğü için $n=2^{2\alpha_1+\alpha_2}$ olmak üzere $x=(a,a+b)\in_1 C^{\alpha_1,\alpha_2}$ kod sözcüğü $2n$ uzunluğunda olur. Burada $2n=2.2^{2\alpha_1+\alpha_2}=2^{2\alpha_1+(\alpha_2+1)}$ dir. Benzer biçimde C^{α_1,α_2} kodunun elemanlarını S' kodu ile düzenlediğimizde eleman sayısı 2 katına çıkacaktır. $d_L(b)=0$ veya $d_L(b)=2n$ olduğundan $d_L(a)=n$, $d_L(a+b)=n$ olur. Her $x\in_1 C^{\alpha_1,\alpha_2}$ olmak üzere $d_L(x)=2n$ bulunur. Böylece uzunluğu $2^{2\alpha_1+(\alpha_2+1)}$ olan bu kod her zaman $C^{\alpha_1,\alpha_2+1}=\{\ (c_1,c_2).N^{\alpha_1,\alpha_2+1}\ \big|\ c_1\in R^{\alpha_1+1},\ c_2\in\mathbb{F}_2^{\alpha_2+1}\}$ koduna denk olur. Özel olarak $\alpha_1=0$ alındığında N^{0,α_2} matrisinin 1. satır bileşenleri haricinde sadece 0 ve u bileşenleri bulunur. Bu kodlar benzer biçimde yazıldığında C^{0,α_2+1} kodu elde edilir.

3.1.19. ÖNERME : $\alpha_1,\ \alpha_2\geq 0$ olmak üzere ${}_2C^{\alpha_1,\alpha_2}$ kodu C^{α_1+1,α_2} koduna denktir. Özel olarak $\alpha_1=0$ olduğunda ${}_2C^{\alpha_1,\alpha_2}\approx C^{\alpha_1+1,\alpha_2}$ dir.

Kanıt: ${}_2C^{\alpha_1,\alpha_2}=\{\ (a,a+b,a+u.b,a+(1+u).b)\ \big|\ a\in C^{\alpha_1,\alpha_2},\ b\in S''\}$ kodunun uzunluğu n uzunluğundaki C^{α_1,α_2} kodunun 4 katı uzunluğunda olduğundan $4n=2^2.2^{2\alpha_1+\alpha_2}=2^{2(\alpha_1+1)+\alpha_2}$ olacağından 3.1.18. Önermenin kanıtına benzer biçimde gözükmektedir.

3.1.20. ÖRNEK : 3.1.15. Örnekte oluşturulan $(2,8,2)_$parametreli $C^{0,1}=\{\ (c_1,c_2).N^{0,1}\ \big|\ c_1\in R,\ c_2\in\mathbb{F}_2\ \}=\{00,11,uu,1+u1+u,0u,u0,11+u,1+u1\}\subseteq R^2$, kodu alınsın. $S'=\{00,uu\}$ olmak üzere ${}_1C^{0,1}=\{\ (a,a+b)\ \big|\ a\in C^{0,1},b\in S'\}$

$$=\begin{Bmatrix}0000,uuuu,0u0u,u0u0,1111,1+u1+u1+u1+u,11+u11+u,1+u11+u1\\00uu,uu00,0uu0,u00u,111+u1+u,1+u1+u11,11+u1+u1,1+u111+u\end{Bmatrix}\subseteq R^4$$

bir $(4,16,4)_$koddur. Aynı zamanda bu ${}_1C^{0,1}$ kodu 3.1.16. Örnekte oluşturulan $N^{0,2}$ matrisi ile elde edilen $C^{0,2}$ koduna eşit olur.

${}_2C^{0,1}=\{\ (a,a+b,a+ub,a+(1+u).b)\ \big|\ a\in C^{0,1},b\in S''\}$ kodu da $N^{1,1}$ matrisi ile üretilen $(8,32,8)$ parametreli $C^{1,1}$ koduna eşit bulunur.

3.1.21. ÖRNEK : $N^{1,0}=\begin{bmatrix}1&1&1&1\\0&1&u&1+u\end{bmatrix}$ üreteç matrisi ile üretilen

$C^{1,0}=\{\ c_1.N^{0,1}\ \big|\ c_1\in R^2\ \}$

$=\{\ 0000,1111,uuuu,1+u1+u1+u1+u,01u1+u,101+uu,u1+u01,1+uu10,$
$0u0u,11+u11+u,u0u0,1+u11+u1,01+uu1,1u1+u0,u101+u,1+u01u\ \}$

kodunun parametresi $(4,16,4)$ dir. Buradan

$${}_1C^{1,0}=\{\ 00000000,0000uuuu,01u1+u01u1+u,01u1+uu1+u01,$$
$$0u0u0u0u,0u0uu0u0,01+uu101+uu1,01+uu1u101+u,$$
$$11111111,11111+u1+u1+u1+u,101+uu101+uu,101+uu1+uu10,$$
$$1+u1+u1+u1+u1+u1+u1+u1+u,1+u1+u1+u1+u1111,$$
$$1+uu101+uu10,1+uu10101+uu,11+u11+u11+u11+u,$$
$$11+u11+u1+u11+u1,1u1+u01u1+u0,1u1+u01+u01u,$$
$$1+u11+u11+u11+u1,1+u11+u111+u11+u,1+u01u1+u01u,$$
$$1+u01u1u1+u0,uuuuuuuu,u0u0u0u0,uu1+u1+u0011,u01+u10u11+u,$$
$$uu00uu00,u00uu00u,uu11001+u1+u,u011+u0u1+u1\ \}\subseteq R^8$$

bulunur. Böylece uygun bileşenlerin yer değiştirmesi ve permütasyon uygulanması ile $C^{1,1}$ kodu elde edilir. Dolayısı ile ${}_1C^{1,0}$ kodunun $C^{1,1}$koduna, ayrıca ${}_2C^{1,0}$ kodunun $C^{2,0}$ koduna denk olduğu görülür.

3.1.22. TANIM : $\alpha_1,\ \alpha_2\geq 0$ ve $n=2^{2\alpha_1+\alpha_2}$ olmak üzere $C^{\alpha_1,\alpha_2}\subseteq R^n$ bir kod olsun. R halkası üzerinde $even(C^{\alpha_1,\alpha_2})=\{\ (c_0,c_2,...,c_{n-2})\in R^{\frac{n}{2}}\ \big|\ (c_0,c_1,...,c_{n-1})\in C^{\alpha_1,\alpha_2}\ \}$

biçiminde tanımlanan koda C^{α_1,α_2} nin <u>çift kodu</u> denir. R halkası üzerinde $odd(C^{\alpha_1,\alpha_2}) = \{ (c_1, c_3, ..., c_{n-1}) \in R^{\frac{n}{2}} \mid (c_0, c_1, ..., c_{n-1}) \in C^{\alpha_1,\alpha_2} \}$ biçiminde tanımlanan koda C^{α_1,α_2} nin <u>tek kodu</u> denir. Çift ve tek kod tanımları $\mathbb{F}_2$ cismi üzerinde benzer biçimde verilir.

3.1.23. ÖNERME : $C^{\alpha_1,\alpha_2} \subseteq R^n$ bir kod olmak üzere

i) $\alpha_1 \geq 1,\ \alpha_2 \geq 0$ için $even(C^{\alpha_1,\alpha_2}) = odd(C^{\alpha_1,\alpha_2}) = C^{\alpha_1-1,\alpha_2+1}$ dir

ii) $\alpha_1 \geq 0,\ \alpha_2 \geq 1$ için $even(C^{\alpha_1,\alpha_2}) \approx odd(C^{\alpha_1,\alpha_2}) = C^{\alpha_1,\alpha_2-1}$ dir.

3.1.24. ÖNERME : $C^{\alpha_1,\alpha_2} \subseteq R^n$ bir kod olsun. Φ , R halkası üzerinde bir Gray dönüşümü olsun. Bu durumda $even(\Phi(C^{\alpha_1,\alpha_2})) = \Phi(even(C^{\alpha_1,\alpha_2}))$ sağlanır.

Kanıt: $0 \leq i \leq n$ ve $c_i = r_i + uq_i$ olmak üzere, her $c = (c_0, c_1, ..., c_{n-1}) \in C^{\alpha_1,\alpha_2}$ için

$$\Phi(c) = \Phi(c_0, c_1, ..., c_{n-1}) = \Phi(r_0 + uq_0, r_1 + uq_1, ..., r_{n-1} + uq_{n-1})$$
$$= (q_0, q_1, ..., q_{n-1}, r_0 + q_0, r_1 + q_1, ..., r_{n-1} + q_{n-1}) \in \Phi(C^{\alpha_1,\alpha_2})$$

bulunur. Buradan $(q_0, q_2, ..., q_{n-2}, r_0 + q_0, r_2 + q_2, ..., r_{n-2} + q_{n-2}) \in even(\Phi(C^{\alpha_1,\alpha_2}))$ dir. Diğer taraftan $c' = (c_0, c_2, ..., c_{n-2}) = (r_0 + uq_0, r_2 + uq_2, ..., r_{n-2} + uq_{n-2}) \in even(C^{\alpha_1,\alpha_2})$ olsun. Gray görüntüsünü alındığında

$\Phi(c') = (q_0, q_2, ..., q_{n-2}, r_0 + q_0, r_2 + q_2, ..., r_{n-2} + q_{n-2}) \in \Phi(even(C^{\alpha_1,\alpha_2}))$ olur.

3.1.24. Önerme tek kodlar için de verilebilir.

3.1.25. ÖRNEK : 3.1.16. Örnekte $C^{0,2}$ kodu aşagıdaki biçimde bulunmuştur.

$$C^{0,2} = \{ 0000, 0u0u, 00uu, 0uu0, 1111, 11+u11+u, 111+u1+u, 11+u1+u1, uuuu,$$
$$u0u0, uu00, u00u, 1+u1+u1+u1+u, 1+u11+u1, 1+u1+u11, 1+u111+u \} \subseteq R^4,$$

dir.bu kodun çift kodu $even(C^{0,2}) = \{00, u0, 0u, uu, 11, 11+u, 1+u1, 1+u1+u\}$ olur. Bu kodun Gray görüntüsü $\Phi(even(C^{0,2})) = \{0000, 0011, 1111, 1100, 0101, 0110, 1010, 1001\}$ olarak bulunur. Ayrıca $C^{0,2}$ kodunun Gray görüntüsü

$$\Phi(C^{0,2}) = \{00000000, 01010101, 00110011, 01100110, 00001111, 01011010, 00111100, 01101001,$$
$$11111111, 10101010, 11001100, 10011001, 11110000, 10100101, 11000011, 10010110\}$$

olur. Böylece $even(\Phi(C^{0,2})) = \Phi(even(C^{0,2}))$ eşitliği elde edilir.

3.1.26. ÖRNEK : 3.1.21. Örnekte $C^{1,0}$ kodu için çift kod ile tek kod eşittir. Ayrıca bu kodlar $C^{0,1}$ koduna eşit olur. Buradan

$even(C^{1,0}) = \{00, u0, 11, 11+u, uu, u0, 1+u1+u, 1+u1\} = odd(C^{1,0}) = C^{0,1}$ dir.

3.1.27. ÖRNEK : $C^{1,1} = \{ (c_1, c_2).N^{1,1} \mid c_1 \in R^2, c_2 \in \mathbb{F}_2 \}$ kodunun parametresi $(8, 32, 8)$ dir. Buradan $C^{1,1}$ in çift kodu

$$even(C^{1,0}) = \{ 0000, 0u0u, 00uu, 0uu0, 1111, 11+u11+u, 111+u1+u,$$
$$11+u1+u1, 1+u1+u1+u1+u, 1+u11+u1, 1+u1+u11,$$
$$1+u111+u, uuuu, u0u0, u101+u, u1+u01 \} \subseteq R^4.$$

olarak bulunur. Bu kodun parametresi $(4, 16, 4)$ olur. Bu koda uygun yer değiştirme ve bir permütasyon uygulandığında

$$C^{1,0} = \{ 0000, 1111, uuuu, 1+u1+u1+u1+u, 01u1+u, 101+uu, u1+u01, 1+uu10,$$
$$0u0u, 11+u11+u, u0u0, 1+u11+u1, 01+uu1, 1u1+u0, u101+u, 1+u01u \}$$

kodu elde edilir.

Bundan sonra yukarıda elde edilen bu C^{α_1,α_2} kodlarının direkt çarpım ve direkt toplam kodları belirlenmiştir. Direkt çarpım ve direkt toplam kodlarının bu kodlar ve bu kodların Gray görüntüleri ile ilişkisi gösterilmiştir. Ayrıca dual kodlar ile ilgili incelemeler yapılmıştır. Dolayısı ile yukarıdaki şekilde elde edilen Hadamard kodların sonuçları ortaya konulmuştur.

$A, B \subseteq R^n$ olsun. Buradan $A \otimes B = \{(a,b) \mid a \in A, b \in B\}$ ve $A \oplus B = \{a+b \mid a \in A, b \in B\}$ biçiminde tanımlanır. C^{α_1,α_2} , R üzerinde n uzunluğunda bir kod olmak üzere $C_1^{\alpha_1,\alpha_2} = \{ x \in \mathbb{F}_2^n \mid \exists y \in \mathbb{F}_2 \ni x+uy \in C^{\alpha_1,\alpha_2} \}$ ve $C_2^{\alpha_1,\alpha_2} = \{ x+y \in \mathbb{F}_2^n \mid x+uy \in C^{\alpha_1,\alpha_2} \}$ binary kodlardır.

3.1.28. ÖNERME : $C_1^{\alpha_1,\alpha_2}$, $C_2^{\alpha_1,\alpha_2}$ kodlar $\mathbb{F}_2$ cismi üzerinde ise $C^{\alpha_1,\alpha_2+1} \subseteq C^{\alpha_1,\alpha_2} \otimes C^{\alpha_1,\alpha_2}$ dir.

Kanıt: $C^{\alpha_1,\alpha_2+1} \subseteq R^n$ kodunun uzunluğu $n = 2^{2\alpha_1+\alpha_2+1}$ dir. Buradan Her $c = (c_0, c_1, ..., c_{n-1}) \in C^{\alpha_1,\alpha_2+1}$ için

$$c = (c_0, c_1, ..., c_{n-1}) = (c_0, c_1, ..., c_{2^{2\alpha_1+\alpha_2+1}}) = (c_0, c_1, ..., c_{2^{2\alpha_1+\alpha_2}}, c_{2^{2\alpha_1+\alpha_2}+1}, ..., c_{2^{2\alpha_1+\alpha_2+1}}) \in C^{\alpha_1,\alpha_2} \otimes C^{\alpha_1,\alpha_2}$$

elde edilir.

3.1.29. TEOREM : C^{α_1,α_2} , R halkası zerinde $n = 2^{2\alpha_1+\alpha_2}$ uzunluğunda bir kod ise $C_1^{\alpha_1,\alpha_2} \otimes C_2^{\alpha_1,\alpha_2} \approx \Phi(C^{\alpha_1,\alpha_2})$ dir. Ayrıca $|C^{\alpha_1,\alpha_2}| = |C_1|.|C_2|$ dir.

Kanıt : $i = 1,...,n$ için $c_i = r_i + uq_i$ olmak üzere

$(r_1, r_2, ..., r_n, q_1 + r_1, q_2 + r_2, ..., q_n + r_n) \in \Phi(C^{\alpha_1,\alpha_2})$ dir. Φ bire-bir ve örten bir fonksiyon olduğundan $c = (c_1, c_2, ..., c_n) \in C^{\alpha_1,\alpha_2}$ olur. $C_1^{\alpha_1,\alpha_2}$ ve $C_2^{\alpha_1,\alpha_2}$ nin tanımları kullanılarak $(r_1, r_2, ..., r_n) \in C_1^{\alpha_1,\alpha_2}, (q_1 + r_1, q_2 + r_2, ..., q_n + r_n) \in C_2^{\alpha_1,\alpha_2}$ elde edilir. Böylece $(r_1, r_2, ..., r_n, q_1 + r_1, q_2 + r_2, ..., q_n + r_n) \in C_1^{\alpha_1,\alpha_2} \otimes C_2^{\alpha_1,\alpha_2}$ olur. Buradan $\Phi(C^{\alpha_1,\alpha_2})$, $C_1^{\alpha_1,\alpha_2} \otimes C_2^{\alpha_1,\alpha_2}$ nin bir alt koduna denktir. Benzer şekilde $C_1^{\alpha_1,\alpha_2} \otimes C_2^{\alpha_1,\alpha_2}$, $\Phi(C^{\alpha_1,\alpha_2})$ nin bir alt koduna denktir.

3.1.30. SONUÇ : $\Phi(C^{\alpha_1,\alpha_2}) \approx C_1^{\alpha_1,\alpha_2} \otimes C_2^{\alpha_1,\alpha_2}$ olsun. Buradan

i) $\alpha_1 = 0$ ise $C^{\alpha_1,\alpha_2} = C_1^{\alpha_1,\alpha_2} \oplus (u) C_2^{\alpha_1,\alpha_2}$ dir

ii) $\alpha_1 \neq 0$ ise $C^{\alpha_1,\alpha_2} \subseteq C_1^{\alpha_1,\alpha_2} \oplus (u) C_2^{\alpha_1,\alpha_2}$ dir.

3.1.31. ÖNERME : C^{α_1,α_2} , R halkası üzerinde bir kod olsun. Bu durumda $d_H = d_L = \min\left\{ d_H(C_1^{\alpha_1,\alpha_2}), d_H(C_2^{\alpha_1,\alpha_2}) \right\}$ sağlanır.

Kanıt : Φ Gray dönüşümü uzaklığı koruduğu için, $d_L(C^{\alpha_1,\alpha_2}) = d_H(\Phi(C^{\alpha_1,\alpha_2}))$ olur. Buradan $\Phi(C^{\alpha_1,\alpha_2}) \approx C_1^{\alpha_1,\alpha_2} \otimes C_2^{\alpha_1,\alpha_2}$ olduğundan $d_H(\Phi(C^{\alpha_1,\alpha_2})) = d_H(C_1^{\alpha_1,\alpha_2} \otimes C_2^{\alpha_1,\alpha_2}) = \min\left\{ d_H(C_1^{\alpha_1,\alpha_2}), d_H(C_2^{\alpha_1,\alpha_2}) \right\}$ eşitliği elde edilir.

3.1.32. ÖNERME : $C^{0,0}$ ve $C^{0,1}$ kodları hariç olmak üzere, tüm C^{α_1,α_2} kodarı self ortogonal kodlardır. Özel olarak $C^{1,0}$ ve $C^{0,2}$ kodları self dual kodlardır.

Kanıt : C^{α_1,α_2} kodunun uzunluğu $n = 2^{2\alpha_1+\alpha_2}$ dir. C^{α_1,α_2} kodunun eleman sayısı $4n$ olduğuna göre C^{α_1,α_2} kodunun duali $(C^{\alpha_1,\alpha_2})^{\perp}$ nin eleman sayısı $\frac{4^n}{4.n}$ dir. Buradan $(\alpha_1, \alpha_2) = (0,0)$ ve $(\alpha_1, \alpha_2) = (0,1)$ durumları dışında $4n \leq \frac{4^n}{4.n}$ olur. Böylece $C^{\alpha_1,\alpha_2} \subseteq (C^{\alpha_1,\alpha_2})^{\perp}$ elde edilir.

3.1.33. ÖNERME : $\Phi(C^{0,0})$ ve $\Phi(C^{0,1})$ kodları hariç olmak üzere, tüm $\Phi(C^{\alpha_1,\alpha_2})$ kodları self ortagonal kodlardır. Özel olarak $\Phi(C^{0,1})$ ve $\Phi(C^{0,\alpha_2})$ kodları self dual kodlardır.

Kanıt : Bu önermenin kanıtı 3.1.32. Önermenin kanıtına benzer biçimde elde edilir.

3.1.34. ÖNERME : $C_1^{\alpha_1,\alpha_2}$ kodu için, $(\alpha_1,\alpha_2)=(0,0)$ ve $(\alpha_1,\alpha_2)=(0,1)$ durumları hariç olmak üzere $(C_1^{\alpha_1,\alpha_2})^{\perp}=C_1^{\alpha_1,\alpha_2}$ dir. $C_2^{\alpha_1,\alpha_2}$ kodu için ya $(C_2^{\alpha_1,\alpha_2})^{\perp}=C_2^{\alpha_1,\alpha_2}$ ya da $(C_2^{\alpha_1,\alpha_2})^{\perp}$, $\mathbb{F}_2$ üzerinde bir tekrar koduna eşittir.

3.2. $v^2=1$ ve $v^2=v$ İken $\mathbb{F}_2+v\mathbb{F}_2$ Üzerindeki Kodlardan Hadamard Kodların Elde Edilmesi

Bu bölümde, 3.1. bölümde verilen $u^2=0$ durumda $\mathbb{F}_2+u\mathbb{F}_2$ halkası üzerinde özel matrisler için elde edilen yapılandırma hem $v^2=1$ durumu için hemde $v^2=v$ durumu için $\mathbb{F}_2+v\mathbb{F}_2$ halkası üzerinde çalışılmıştır. Ayrıca, bu iki halka üzerinde tanımlanan kodların Hadamard kodlar ve quasi-cyclic kodlar ile ilişkisi verilmiştir.

Buradan, $v^2=1$ olması durumnunda $\mathbb{F}_2[v]/\langle v^2-1\rangle$ halkası $\mathbb{F}_2+v\mathbb{F}_2$ halkasına izomorftur. $v^2=1$ koşulu ile $\mathbb{F}_2+v\mathbb{F}_2$, aşığıda tanımlanan + ve • işlemleri ile bir halkadır.

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

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

$v^2=1$ durumunda $R=\mathbb{F}_2+v\mathbb{F}_2$ halkasının idealleri $\langle 0\rangle=\{0\}$, $\langle 1+v\rangle=\{0,1+v\}$ ve $\langle v\rangle=\langle 1\rangle=R$ dir. Bu halkanın idealleri arasında $\langle 0\rangle\subseteq\langle 1+v\rangle\subseteq\langle v\rangle\subseteq\langle 1\rangle=R$ ilişkisi vardır ve R bir yerel halkadır.

3.2.1. TANIM : $R=\mathbb{F}_2+v\mathbb{F}_2$ halkası üzerinde;

her $x\in R$ için $w_{L_R}(x)=\begin{cases}0 & ; \quad x=0\\ 1 & ; \quad x=1,v\\ 2 & ; \quad x=1+v\end{cases}$

biçiminde tanımlanan fonksiyona, R üzerinde Lee ağırlık fonksiyonu denir.

Bu durumda her $r=(r_1,r_2,...,r_n)\in R^n$ için $w_{L_R}(r)=\sum_{i=1}^{n} w_{L_R}(r_i)$ eşitliği gerçeklenir.

$v^2=v$ iken $\mathbb{F}_2[v]/\langle v^2-v\rangle$ halkası $\mathbb{F}_2+v\mathbb{F}_2$ halkasına izomorftur. $v^2=v$ koşulu ile $\mathbb{F}_2+v\mathbb{F}_2$, aşığıda tanımlanan $+$ ve $\bullet$ işlemleri ile halkadır.

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

$.$	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	$1+v$

$v^2=v$ iken $S=\mathbb{F}_2+v\mathbb{F}_2$ halkasının idealleri $\langle 0\rangle=\{0\}$, $\langle v\rangle=\{0,v\}$, $\langle 1+v\rangle=\{0,1+v\}$ ve $\langle 1\rangle=S$ dir. Bu halkanın idealleri arasında $\langle 0\rangle\subseteq\langle 1+v\rangle\subseteq\langle 1\rangle=S$ ve $\langle 0\rangle\subseteq\langle v\rangle\subseteq\langle 1\rangle=S$ ilişkisi vardır ve R bir yerel halka değildir.

3.2.2. TANIM : $S=\mathbb{F}_2+v\mathbb{F}_2$ halkası üzerinde;

her $x\in S$ için $w_{L_S}(x)=\begin{cases}0 & ; \ x=0\\ 1 & ; \ x=v,1+v\\ 2 & ; \ x=1\end{cases}$

biçiminde tanımlanan fonksiyona, S üzerinde Lee ağırlık fonksiyonu denir.

Bu durumda her $s=(s_1,s_2,...,s_n)\in S^n$ için $w_{L_S}(s)=\sum_{i=1}^{n} w_{L_R}(s_i)$ eşitliği gerçeklenir.

3.2.3. TANIM : $\mathbb{F}_2$ cismi üzerinde; $w_H(0)=0, w_H(1)=1$ biçiminde tanımlanan w_H fonksiyonuna $\mathbb{F}_2$ üzerinde Hamming ağırlık fonksiyonu denir. Bu durumda her $c=(c_1,c_2,...,c_n)\in\mathbb{F}_2^n$ için $w_H(c)=\sum_{i=1}^{n} w_H(c_i)$ olur.

3.2.4. TANIM : R^n (ya da S^n) üzerinde iki vektör arasındaki uzaklık $a, b\in R^n$ (ya da S^n), $a\neq b$ için $d_{L_R}(a,b)=w_{L_R}(a-b)$ (ya da $d_{L_S}(a,b)=w_{L_S}(a-b)$) olmak üzere bir C kodunun minimum Lee uzaklığı

$d_{L_R}(C) = \min\{d_{L_R}(a,b) \mid a,b \in C, a \neq b\}$ (ya da $d_{L_S}(C) = \min\{d_{L_S}(a,b) \mid a,b \in C, a \neq b\}$) biçiminde tanımlanır. $\mathbb{F}_2^n$ de Lee ağırlığı yerine Hamming ağırlığı yazılarak benzer tanım verilir. $\mathbb{F}_2^n$ üzerinde bir C kodunun minimum Hamming uzaklığı $d_H(C)$ ile gösterilir.

3.2.5. TANIM : $v^2 = 1$ durumunda $R = \mathbb{F}_2 + v\mathbb{F}_2$ olmak üzere;

$\Phi_1 : R^n \longrightarrow \mathbb{F}_2^{2n}$

$(r_1, r_2, ..., r_n) \mapsto \Phi(r_1, r_2, ..., r_n) = (a_1, a_2, ..., a_n, b_1, b_2, ..., b_n)$

biçiminde tanımlanan dönüşüme R halkası üzerindeki Gray dönüşümü denir. Burada $1 \leq i \leq n$, $a_i, b_i \in \mathbb{F}_2$ için $r_i = a_i + vb_i \in R$ dır.

3.2.6. TANIM : $v^2 = v$ durumunda $S = \mathbb{F}_2 + v\mathbb{F}_2$ olmak üzere;

$\Phi_2 : S^n \longrightarrow \mathbb{F}_2^{2n}$

$(s_1, s_2, ..., s_n) \mapsto \Phi(s_1, s_2, ..., s_n) = (c_1, c_2, ..., c_n, c_1 + d_1, c_2 + d_2, ..., c_n + d_n)$

biçiminde tanımlanan dönüşüme S halkası üzerindeki Gray dönüşümü denir. Burada $1 \leq i \leq n$, $c_i, d_i \in \mathbb{F}_2$ için $s_i = c_i + vd_i \in S$ dır.

Bu tanım ile birlikte $v^2 = 1$ durumunda $\mathbb{F}_2 + v\mathbb{F}_2$ halkası üzerindeki n uzunluğunda bir kodun, Φ_1 Gray dönüşümü altındaki görüntüsü $2n$ uzunluğunda bir binary koddur. R^n üzerinde tanımlanan d_{L_R} Lee uzaklığı ve $\mathbb{F}_2^{2n}$ üzerinde tanımlanan d_H Hamming uzaklığı arasında her $a, b \in R^n$ için $d_{L_R}(a,b) = d_H(\Phi_1(a), \Phi_1(b))$ ilişkisi vardır. Yine $v^2 = v$ koşulu ile $\mathbb{F}_2 + v\mathbb{F}_2$ halkası üzerindeki n uzunluğunda bir kodunun, Φ_2 Gray dönüşümü altındaki görüntüsü $2n$ uzunluğunda bir binary koddur. S^n üzerinde tanımlanan d_{L_S} Lee uzaklığı ve $\mathbb{F}_2^{2n}$ üzerinde tanımlanan d_H Hamming uzaklığı arasında, her $a', b' \in S^n$ için $d_{L_S}(a', b') = d_H(\Phi_2(a'), \Phi_2(b'))$ ilişkisi vardır. Buradan Φ_1 ve Φ_2 Gray dönüşümlerinin birer izometri olduğunu görülür.

3.2.7. TANIM : $v^2 = 1$ durumnda $R = \mathbb{F}_2 + v\mathbb{F}_2$ halkası üzerinde;

$\alpha_1, \alpha_2 \in \mathbb{Z}_+ \cup \{0\}$ olmak üzere ilk satır bileşenleri $\{1\}$ kümesinden, diğer satır elemanları $\alpha_2 = 0$ iken $\{0, 1, v, 1+v\}$ kümesinden ve $\alpha_1 = 0$ iken $\{0, 1+v\}$

kümesinden seçilerek, sütunları da lexicographically sıralama bağıntısına göre sıralanmış ve satır sayısı $\alpha_1+\alpha_2+1$ olacak şekilde özel olarak oluşturulan $N_R{}^{\alpha_1,\alpha_2}$ matrisine R üzerinde üreteç matrisi denir.

Aşağıda $N_R{}^{\alpha_1,\alpha_2}$ matrisleri için birkaç örnek verilmiştir.

$$N_R{}^{0,0}=\begin{bmatrix}1\end{bmatrix} \quad , \quad N_R{}^{0,1}=\begin{bmatrix}1 & 1\\ 0 & 1+v\end{bmatrix} \quad , \quad N_R{}^{0,2}=\begin{bmatrix}1 & 1 & 1 & 1\\ 0 & 0 & 1+v & 1+v\\ 0 & 1+v & 0 & 1+v\end{bmatrix},$$

$$N_R{}^{0,3}=\begin{bmatrix}1 & 1 & 1 & 1 & 1 & 1 & 1 & 1\\ 0 & 0 & 0 & 0 & 1+v & 1+v & 1+v & 1+v\\ 0 & 0 & 1+v & 1+v & 0 & 0 & 1+v & 1+v\\ 0 & 1+v & 0 & 1+v & 0 & 1+v & 0 & 1+v\end{bmatrix}, \quad N_R{}^{1,0}=\begin{bmatrix}1 & 1 & 1 & 1\\ 0 & 1 & v & 1+v\end{bmatrix},$$

$$N_R{}^{2,0}=\begin{bmatrix}1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1\\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & v & v & v & v & 1+v & 1+v & 1+v & 1+v\\ 0 & 1 & v & 1+v & 0 & 1 & v & 1+v & 0 & 1 & v & 1+v & 0 & 1 & v & 1+v\end{bmatrix},$$

$$N_R{}^{1,1}=\begin{bmatrix}1 & 1 & 1 & 1 & 1 & 1 & 1 & 1\\ 0 & 0 & 1 & 1 & v & v & 1+v & 1+v\\ 0 & 1+v & 0 & 1+v & 0 & 1+v & 0 & 1+v\end{bmatrix}.$$

3.2.8. TANIM : $v^2=1$ durumnda $R=\mathbb{F}_2+v\mathbb{F}_2$ halkası üzerinde;

her $\alpha_1,\alpha_2\geq 0$ tamsayıları için $C_R{}^{\alpha_1,\alpha_2}=\{\ (c_1,c_2).N_R{}^{\alpha_1,\alpha_2}\ \big|\ c_1\in R^{\alpha_1+1}, c_2\in\mathbb{F}_2^{\alpha_2}\ \}$ biçiminde yazılan kod $n=2^{2\alpha_1+\alpha_2}$ uzunluğundadır ve bu koda $N_R{}^{\alpha_1,\alpha_2}$ üreteç matrisi ile üretilmiş, $(n,4n,n)$ parametreli kod denir.

3.2.9. TANIM : $v^2=v$ durumunda $S=\mathbb{F}_2+v\mathbb{F}_2$ halkası üzerinde;

$\alpha_1,\ \alpha_2\in\mathbb{Z}_+\cup\{0\}$ olmak üzere ilk satır bileşenleri {1} kümesinden, diğer satır elemanları $\alpha_2=0$ iken $\{0,1,v,1+v\}$ kümesinden ve $\alpha_1=0$ iken $\{0,1\}$ kümesinden seçilerek, sütunları da lexicographically sıralama bağıntısına göre sıralanmış ve satır sayısı $\alpha_1+\alpha_2+1$ olacak şekilde özel olarak oluşturulan $N_S{}^{\alpha_1,\alpha_2}$ matrisine S üzerinde üreteç matrisi denir.

Aşağıda $N_S{}^{\alpha_1,\alpha_2}$ matrisleri için birkaç örnek verilmiştir.

$$N_S{}^{0,0} = [1], \qquad N_S{}^{0,1} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \qquad N_S{}^{0,2} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix},$$

$$N_S{}^{0,3} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}, \qquad N_S{}^{1,0} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & v & 1+v \end{bmatrix},$$

$$N_S{}^{2,0} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & v & v & v & v & 1+v & 1+v & 1+v & 1+v \\ 0 & 1 & v & 1+v & 0 & 1 & v & 1+v & 0 & 1 & v & 1+v & 0 & 1 & v & 1+v \end{bmatrix},$$

$$N_S{}^{1,1} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & v & v & 1+v & 1+v \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

3.2.10. TANIM : $v^2 = v$ durumnda $S = \mathbb{F}_2 + v\mathbb{F}_2$ halkası üzerinde;

her $\alpha_1, \alpha_2 \geq 0$ tamsayıları için $C_S{}^{\alpha_1,\alpha_2} = \{ (c_1, c_2).N_S{}^{\alpha_1,\alpha_2} \mid c_1 \in R^{\alpha_1+1}, c_2 \in \mathbb{F}_2^{\alpha_2} \}$ biçiminde yazılan kod $n = 2^{2\alpha_1+\alpha_2}$ uzunluğundadır ve bu koda $N_S{}^{\alpha_1,\alpha_2}$ üreteç matrisi ile üretilmiş $(n, 4n, n)$ parametreli kod denir.

3.2.11. TEOREM : Φ_1 , R^n üzerinde bir Gray dönüşümü olsun. $C_R{}^{\alpha_1,\alpha_2}$, $N_R{}^{\alpha_1,\alpha_2}$ üreteç matrisi ile yazılan bir kod olmak üzere $\Phi_1(C_R{}^{\alpha_1,\alpha_2})$ kodu, $\mathbb{F}_2$ cismi üzerinde $(2n, 4n, n)$ parametreli bir Hadamard kodudur.

Kanıt: Boyutu $(\alpha_1 + \alpha_2 + 1) \times n$ olan $N_R{}^{\alpha_1,\alpha_2}$ üreteç matrisi ile oluşturulan kod $C_R{}^{\alpha_1,\alpha_2} = \{ (c_1, c_2).N_R{}^{\alpha_1,\alpha_2} \mid c_1 \in R^{\alpha_1+1}, c_2 \in \mathbb{F}_2^{\alpha_2} \}$ biçimindedir. Tanımlanan bu kodun uzunluğu $n = 2^{2\alpha_1+\alpha_2}$ dir. $C_R{}^{\alpha_1,\alpha_2} \subseteq R^n$ olan bu kodun bir tekrar kod olduğu ve eleman sayısının da $4n$ olduğu açıktır. Buradan $\Phi_1(C_R{}^{\alpha_1,\alpha_2}) \subseteq \mathbb{F}_2^{2n}$ olduğundan $\Phi_1(C_R{}^{\alpha_1,\alpha_2}), (2n, 4n, n)$ parametreli bir binary Hadamard koddur.

3.2.12. SONUÇ : $\alpha_1 = \alpha_2 = 0$ durumu dışında; $(C_R{}^{\alpha_1,\alpha_2})^{\perp}$ dual kodunun parametresi $(n, \frac{4^n}{4n}, 4)$ dür. Ayrıca $\Phi_1((C_R{}^{\alpha_1,\alpha_2})^{\perp})$ kodu da $(2n, \frac{4^n}{4n}, 4)$_ parametreli bir koddur.

Kanıt: $C_R{}^{\alpha_1,\alpha_2}$ kodunun üreteç matrisi olan $N_R{}^{\alpha_1,\alpha_2}$ matrisi $(C_R{}^{\alpha_1,\alpha_2})^{\perp}$ kodunun aynı zamanda parity-check matrisidir. $(C_R{}^{\alpha_1,\alpha_2})^{\perp}$ kodunun elemanları, boyutu $(\alpha_1 + \alpha_2 + 1) \times n$ olan $N_R{}^{\alpha_1,\alpha_2}$ üreteç matrisi yardımıyla $N_R{}^{\alpha_1,\alpha_2}.c^T = 0$ koşulunu sağlayan $c \in R^n$ elemanlarıdır. Bu koşulu sağlayan sözcük sayısı $\frac{4^n}{4n}$ dir. Bu kod sözcüklerinin en küçük ağırlığının 4 olduğu açıktır. Böylece $(C_R{}^{\alpha_1,\alpha_2})^{\perp}$ kodu $(n, \frac{4^n}{4n}, 4)$ parametresine sahip olur. Buradan $\Phi_1((C_R{}^{\alpha_1,\alpha_2})^{\perp})$ kodunun da $(2n, \frac{4^n}{4n}, 4)$ parametreli olduğu görülür.

3.2.13. TEOREM : Φ_2, S^n üzerinde bir Gray dönüşümü olsun. $C_S{}^{\alpha_1,\alpha_2}$, $N_S{}^{\alpha_1,\alpha_2}$ üreteç matrisi ile yazılan kod olmak üzere $\Phi_2(C_S{}^{\alpha_1,\alpha_2})$ kodu, $\mathbb{F}_2$ cismi üzerinde $(2n, 4n, n)$ parametreli bir Hadamard kodudur.

Kanıt: $N_R{}^{\alpha_1,\alpha_2}$ üreteç matrisleri yerine $N_S{}^{\alpha_1,\alpha_2}$ üreteç matrisleri kullanılarak 3.2.11. Teoreme benzer biçimde kanıtlanır.

3.2.14. SONUÇ : $\alpha_1 = \alpha_2 = 0$ durumu dışında; $(C_s{}^{\alpha_1,\alpha_2})^{\perp}$ dual kodunun parametresi $(n, \frac{4^n}{4n}, 4)$ dür. Ayrıca $\Phi_2((C_s{}^{\alpha_1,\alpha_2})^{\perp})$ kodu $(2n, \frac{4^n}{4n}, 4)$_ parametreli koddur.

Kanıt: 3.2.12. Sonucun kanıtına benzer biçimde görülür.

3.2.15. TANIM : $n = 2^{2\alpha_1+\alpha_2}$ olmak üzere $C_R{}^{\alpha_1,\alpha_2}$, $R = \mathbb{F}_2 + v\mathbb{F}_2$ $(v^2 = 1)$ halkası üzerinde n uzunluğunda bir lineer kod olsun.

$\tau_1 : R^n \longrightarrow R^n$

$(c_1, c_2, ..., c_n) \mapsto \tau_1(c_1, c_2, ..., c_n) = (c_n, c_1, ..., c_{n-1})$

permütasyonu için $\tau_1(C_R{}^{\alpha_1,\alpha_2}) = C_R{}^{\alpha_1,\alpha_2}$ koşulu sağlanıyorsa $C_R{}^{\alpha_1,\alpha_2}$ koduna R üzerinde bir cyclic kod denir.

3.2.16. TANIM : $n = 2^{2\alpha_1+\alpha_2}$ olmak üzere ${C_S}^{\alpha_1,\alpha_2}$, $S = \mathbb{F}_2 + v\mathbb{F}_2$ ($v^2 = v$) halkası üzerinde n uzunluğunda bir lineer kod olsun.

$$\tau_2 : S^n \longrightarrow S^n$$

$$(c_1, c_2, ..., c_n) \mapsto \tau_2(c_1, c_2, ..., c_n) = (c_n, c_1, ..., c_{n-1})$$

permütasyonu için $\tau_2({C_S}^{\alpha_1,\alpha_2}) = {C_S}^{\alpha_1,\alpha_2}$ sağlanıyorsa ${C_S}^{\alpha_1,\alpha_2}$ koduna S üzerinde bir cyclic kod denir.

3.2.17. TANIM : $n = 2^{2\alpha_1+\alpha_2}$ olmak üzere D^{α_1,α_2}, $\mathbb{F}_2$ üzerinde $2n$ uzunluğunda bir lineer kod olsun.

$$\sigma^{\otimes 2} : {\mathbb{F}_2}^{2n} \longrightarrow {\mathbb{F}_2}^{2n}$$

$$(d_1, d_2, ..., d_{2n}) \mapsto \sigma^{\otimes 2}(d_1, d_2, ..., d_{2n}) = (d_n, d_1, ..., d_{n-1}, d_{2n}, d_{n+1}, ...d_{2n-1})$$

permütasyonu için $\sigma^{\otimes 2}(D^{\alpha_1,\alpha_2}) = D^{\alpha_1,\alpha_2}$ sağlanıyorsa D^{α_1,α_2} koduna $\mathbb{F}_2$ üzerinde 2. mertebeden bir quasi-cyclic kod denir.

3.2.18. ÖNERME : τ_1 dönüşümü R^n üzerinde bir permütasyon, $\sigma^{\otimes 2}$ dönüşümü ${\mathbb{F}_2}^{2n}$ üzerinde bir permütasyon ve Φ_1, R^n den ${\mathbb{F}_2}^{2n}$ e yukarıda tanımlanan Gray dönüşümünü ise $\sigma^{\otimes 2} \circ \Phi_1 = \Phi_1 \circ \tau_1$ eşitliği sağlanır.

Kanıt: Her $1 \le i \le n$ için $c_i = a_i + vb_i \in R$ olmak üzere her $c = (c_1, c_2, ..., c_n) \in R^n$ olsun. Bu durumda $\tau_1(c_1, c_2, ..., c_n) = (c_n, c_1, ..., c_{n-1})$ sağlanır.

Buradan,

$$\Phi_1(\tau_1(c)) = \Phi_1(\tau_1(c_1, c_2, ..., c_n)) = \Phi_1(c_n, c_1, ..., c_{n-1}) = (a_n, a_1, ..., a_{n-1}, b_n, b_1, ..., b_{n-1})$$

elde edilir. Diğer taraftan, her $c \in R^n$ için

$$\Phi_1(c) = \Phi_1(c_1, c_2, ..., c_n) = \Phi_1(a_1 + vb_1, a_2 + vb_2, ..., a_n + vb_n)$$

$$= (a_1, a_2, ..., a_n, b_1, b_2, ..., b_n) \text{ dir.}$$

Böylece $\sigma^{\otimes 2}(\Phi_1(c)) = (a_n, a_1, ..., a_{n-1}, b_n, b_1, ..., b_{n-1})$ olduğu görülür.

3.2.19. ÖNERME : τ_2 dönüşümü S^n üzerinde bir permütasyon, $\sigma^{\otimes 2}$ dönüşümü ${\mathbb{F}_2}^{2n}$ üzerinde bir permütasyon ve Φ_2, S^n den ${\mathbb{F}_2}^{2n}$ e yukarıda tanımlanan Gray dönüşümünü ise $\sigma^{\otimes 2} \circ \Phi_2 = \Phi_2 \circ \tau_2$ eşitliği sağlanır.

Kanıt: Her $1 \le i \le n$ için $c_i = a_i + vb_i \in S$ olmak üzere her $c = (c_1, c_2, ..., c_n) \in S^n$ olsun. Bu durumda

$$\Phi_2(c) = \Phi_2(c_1, c_2, ..., c_n) = \Phi_2(a_1 + vb_1, a_2 + vb_2, ..., a_n + vb_n)$$
$$= (a_1, a_2, ..., a_n, a_1 + b_1, a_2 + b_2, ..., a_n + b_n)$$

dir. Böylece $\sigma^{\otimes 2}(\Phi_2(c)) = (a_n, a_1, ..., a_{n-1}, a_n + b_n, b_1, ..., a_{n-1} + b_{n-1})$ elde edilir.

Diğer taraftan, $c = (c_1, c_2, ..., c_n) \in S^n$ için $\tau_2(c_1, c_2, ..., c_n) = (c_n, c_1, ..., c_{n-1})$ dir.

Buradan $\Phi_2(\tau_2(c)) = \Phi_2(\tau_2(c_1, c_2, ..., c_n)) = \Phi_2(c_n, c_1, ..., c_{n-1})$

$$= (a_n, a_1, ..., a_{n-1}, a_n + b_n, b_1, ..., a_{n-1} + b_{n-1})$$

bulunur.

3.2.20. TEOREM : $\alpha_2 \neq 0$ olmak üzere, $N_R{}^{\alpha_1,\alpha_2}$ üreteç matrisi ile elde edilen Hadamard kodu 2. mertebeden bir quasi-cyclic koddur.

Kanıt: $\alpha_2 \neq 0$ olsun. $N_R{}^{\alpha_1,\alpha_2}$ üreteç matrisi ile elde edilen $C_R{}^{\alpha_1,\alpha_2}$ kodunun uzunluğu $n = 2^{2\alpha_1+\alpha_2}$ dir. Buradan bir $C_R{}^{\alpha_1,\alpha_2}$ kodunun Gray görüntüsü $\Phi_1(C_R{}^{\alpha_1,\alpha_2})$ kodunun $\mathbb{F}_2$ cismi üzerinde uznuluğunun $2^{2\alpha_1+\alpha_2+1}$ olduğu görülür. Bu durumda bir Hadamard matrisi ile elde edilen bir Hadamard kodunun $\Phi_1(C_R{}^{\alpha_1,\alpha_2})$ koduna eşit olduğu sonucuna varılır. 3.2.18. Önerme kullanılarak $\sigma^{\otimes 2}(\Phi_1(C_R{}^{\alpha_1,\alpha_2})) = \Phi_1(\tau_1(C_R{}^{\alpha_1,\alpha_2})) = \Phi_1(C_R{}^{\alpha_1,\alpha_2})$ eşitliği elde edilir. Φ bire-bir bir fonksiyon olduğundan $\sigma^{\otimes 2}(\Phi_1(C_R{}^{\alpha_1,\alpha_2})) = \Phi_1(C_R{}^{\alpha_1,\alpha_2})$ bulunur. Sonuç olarak $\Phi_1(C_R{}^{\alpha_1,\alpha_2})$ Hadamard kodları 2. mertebeden bir quasi-cyclic koddur.

3.2.21. TEOREM : $\alpha_2 \neq 0$ olmak üzere, $N_s{}^{\alpha_1,\alpha_2}$ üreteç matrisi ile elde edilen bir Hadamard kodu 2. mertebeden bir quasi-cyclic koddur.

Kanıt: 3.2.21. Teoremin kanıtına benzer biçimde görülür.

3.2.22. ÖRNEK : $C_R{}^{0,1}$ kodunu belirleyen $N_R{}^{0,1}$ üreteç matrisi $N_R{}^{0,1} = \begin{bmatrix} 1 & 1 \\ 0 & 1+v \end{bmatrix}$ biçimindedir. Buradan $C_R{}^{0,1}$ kodunun elemanları $c_1 \in R$, $c_2 \in \mathbb{F}_2$ olmak üzere $c = (c_1, c_2).N_R{}^{0,1}$ biçimindeki elemanlardır. Buradan

$C_R{}^{0,1} = \{\, 0\ 0, 0\ 1+v, 1\ 1, 1\ v, v\ v, v\ 1, 1+v\ 1+v, 1+v\ \ 0 \,\} \subseteq R^2$ kodu için

$d_{L_R}(C_R{}^{0,1}) = 2$ ve $\left|C_R{}^{0,1}\right| = 8$ dir. Dolayısı ile $C_R{}^{0,1}$ kodunun parametresi $(2,8,2)$ olur.

Buradan $C_R{}^{0,1}$ kodunun Φ_1 Gray görüntüsü

$\Phi_1(C_R{}^{0,1}) = \{0000, 0011, 1111, 1100, 0101, 0110, 1010, 1001\} \subseteq \mathbb{F}_2^4$ kodudur. $\Phi_1(C_R{}^{0,1})$ kodu $(4,8,2)$ parametreli bir Hadamard koddur. Diğer taraftan $M = \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$ normalleştirilmiş bir Hadamard matrisi olmak üzere M Hadamard matrisinde 1 yerine 0 ve -1 yerine 1 yazılarak M marisinin satırlarından, 00 ve 10 vektörleri elde edilir. Bu vektörlerin tamamlayıcıları da ilave edilerek $00, 10, 11, 01$ vektörleri oluşturulur. Bu dört vektörün tamamlayıcıları alınır ve tekrarlayıcıları ile yeniden düzenlenlenirse $0000, 0011, 1111, 1100, 0101, 0110, 1010, 1001$ vektörleri elde edilir. Bu vektörlerin oluşturduğu küme bir ikili kod belirtir. Bu kodun uzunluğu 4, eleman sayısı 8 ve Hamming ağırlığı 2 dir. Böylece M Hadamard matrisi ile elde edilen bir Hadamard kodu $(4,8,2)\_$ parametreli $\Phi_1(C_R{}^{0,1})$ koduna eşittir.

Ayrıca $(C_R{}^{0,1})^{\perp} = \{\, 0\ 0\ ,\ 1+v\ 1+v\,\}$ ve $\Phi((C_R{}^{0,1})^{\perp}) = \{0000, 1111\}$ olur. Bunun dışında $\tau_1(C_R{}^{0,1}) = C_R{}^{0,1}$ sagladığından $C_R{}^{0,1}$ bir cyclic koddur. Benzer biçimde $\sigma^{\otimes 2}(\Phi_1(C_R{}^{0,1})) = \Phi_1(C_R{}^{0,1})$ saglandığından $\Phi_1(C_R{}^{0,1})$ kodu, 2. mertebeden bir quasi-cyclic koddur.

3.2.23. ÖRNEK : $C_S{}^{0,2}$ kodunu belirleyen $N_S{}^{0,2}$ üreteç matrisi $N_S{}^{0,2} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}$ dir. Buradan $c_1 \in R,\ c_2 \in \mathbb{F}_2^2$ olmak üzere $C_S{}^{0,2}$ kodunun elemanları $c = (c_1, c_2).N_S{}^{0,2}$ biçimindeki elemanlardır. Bu durumda

$C_S{}^{0,2} = \{\, 0000, 0101, 0011, 0110, 1111, 1010, 1100, 1001, vvvv, v\ 1+v\ v\ 1+v, vv1+v1+v,$
$v1+v1+vv, 1+v1+v1+v1+v, 1+v\ v1+vv, 1+v1+vvv, 1+v\ vv1+v\} \subseteq S^4$

dur. Bu kod için $d_{L_S}(C_S{}^{0,2}) = 4$ ve $\left|C_S{}^{0,2}\right| = 16$ olduğundan $C_S{}^{0,2}$ kodu bir $(4,16,4)\_$ koddur. $C_S{}^{0,2}$ kodunun Gray görüntüsü alınarak

$$\Phi_2(C_S{}^{0,2}) = \{00000000, 01010101, 00110011, 01100110,$$
$$11111111, 10101010, 11001100, 10011001,$$
$$00001111, 01011010, 00111100, 01101001,$$
$$11110000, 10100101, 11000011, 10010110\} \subseteq \mathbb{F}_2^8$$

kodu elde edilir. $\Phi_2(C_S{}^{0,2})$ kodu $(8,16,4)$ parametreli bir Hadamard koddur. Diğer taraftan $M = \begin{bmatrix} 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 1 \\ -1 & -1 & -1 & 1 \end{bmatrix}$ normalleştirilmiş bir Hadamard matrisi olmak üzere M Hadamard matrisinde 1 yerine 0 ve -1 yerine 1 yazılarak M marisinin satırlarından, $0000, 1010, 1100$ ve 0110 vektörleri elde edilir. Bu vektörlerin tamamlayıcıları da eklenerek $0000, 1010, 1100$, 0110 , $1111, 0101, 0011$ ve 1001 vektörleri oluşturulur. Bu vektörlerin tamamlayıcıları alınır ve tekrarlayıcıları ile yeniden düzenlenirse

$00000000, 01010101, 00110011, 01100110$, 11111111, $10101010, 11001100, 10011001$,

$00001111, 01011010, 00111100, 01101001, 11110000, 10100101, 11000011, 10010110$

vektörleri elde edilir. Bu vektörlerin oluşturduğu küme bir ikili kod oluşturur. Bu kodun uzunluğu 8, eleman sayısı 16 ve Hamming ağırlığı 4 tür. Böylece M Hadamard matrisi ile elde edilen Hadamard kodu $(8,16,4)$_ parametreli $\Phi_2(C_S{}^{0,2})$ koduna eşittir.

Ayrıca $(C_S{}^{0,2})^{\perp} = C_S{}^{0,2}$ olduğu için $C_S{}^{0,2}$ bir self-dual koddur. $\tau_2(C_S{}^{0,2}) = C_S{}^{0,2}$ sağladığından $C_S{}^{0,2}$ bir cyclic koddur. Benzer biçimde $\sigma^{\otimes 2}(\Phi_2(C_S{}^{0,2})) = \Phi_2(C_S{}^{0,2})$ saglandığından $\Phi_2(C_S{}^{0,2})$ kodu, 2 . mertebeden bir quasi-cyclic koddur.

3.3. $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$ Üzerindeki Kodlardan Hadamard Kodların Bulunması ve Hadamard Kodların Özel Durumları

Bu bölümde $u^3 = 0$ iken $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$ halkası üzerinde yazılan özel matrisler ve bu matrislerin üretmiş olduğu kodlar verilmiştir. Bu kodların Hadamard kodları ile ilişkilendirilmiştir. Bu halka üzerinde Hadamard kodun cyclic kod, quasi-cyclic kod, tek kod ve çift kod ile verdiği sonuçlar ortaya konulmuştur.

$\mathbb{F}_2[u]/\langle u^3\rangle = \{ a_0 + a_1.u + a_2.u^2 + \langle u^3\rangle \mid a_i \in \mathbb{F}_2, i = 0,1,2 \}$ halkası $u^3 = 0$ alınması durumda $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$ halkasına izomorf olur.

$\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 = \{0,1,u,u^2,1+u,1+u^2,u+u^2,1+u+u^2\}$ aşığıda tanımlanan $+$ ve $\bullet$ işlemleri ile halkadır.

$+$	0	1	u	u^2	$1+u$	$1+u^2$	$u+u^2$	$1+u+u^2$
0	0	1	u	u^2	$1+u$	$1+u^2$	$u+u^2$	$1+u+u^2$
1	1	0	$1+u$	$1+u^2$	u	u^2	$1+u+u^2$	$u+u^2$
u	u	$1+u$	0	$u+u^2$	1	$1+u+u^2$	u^2	$1+u^2$
u^2	u^2	$1+u^2$	$u+u^2$	0	$1+u+u^2$	1	u	$1+u$
$1+u$	$1+u$	u	1	$1+u+u^2$	0	$u+u^2$	$1+u^2$	u^2
$1+u^2$	$1+u^2$	u^2	$1+u+u^2$	1	$u+u^2$	0	$1+u$	u
$u+u^2$	$u+u^2$	$1+u+u^2$	u^2	u	$1+u^2$	$1+u$	0	1
$1+u+u^2$	$1+u+u^2$	$u+u^2$	$1+u^2$	$1+u$	u^2	u	1	0

$\bullet$	0	1	u	u^2	$1+u$	$1+u^2$	$u+u^2$	$1+u+u^2$
0	0	0	0	0	0	0	0	0
1	0	1	u	u^2	$1+u$	$1+u^2$	$u+u^2$	$1+u+u^2$
u	0	u	u^2	0	$u+u^2$	u	u^2	$u+u^2$
u^2	0	u^2	0	0	u^2	u^2	0	u^2
$1+u$	0	$1+u$	$u+u^2$	u^2	$1+u^2$	$1+u+u^2$	u	1
$1+u^2$	0	$1+u^2$	u	u^2	$1+u+u^2$	1	$u+u^2$	$1+u$
$u+u^2$	0	$u+u^2$	u^2	0	u	$u+u^2$	u^2	u
$1+u+u^2$	0	$1+u+u^2$	$u+u^2$	u^2	1	$1+u$	u	$1+u^2$

$R_2 = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$ halkasının idealleri $(0) = \{0\}$, $(u^2) = \{0, u^2\}$, $(u) = (u+u^2) = \{0, u, u^2, u+u^2\}$, $(1) = (1+u) = (1+u^2) = (1+u+u^2) = R_2$ biçimdedir ve $(0) \subset (u^2) \subset (u) = (u+u^2) \subset (1+u) = (1+u^2) = (1+u+u^2) = (1) = R_2$ ilişkisi sağlanır.

3.3.1. TANIM : $R_2 = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$ halkası üzerinde;

her $r \in R_2$ için $w_L(r) = \begin{cases} 0 & , r = 0 \\ 4 & , r = u^2 \\ 2 & , \textit{otherwise} \end{cases}$

biçiminde tanımlanan fonksiyona, R_2 üzerinde Lee ağırlık fonksiyonu denir.

Bu durumda her $r = (r_o, r_1, ..., r_{n-1}) \in R_2^n$ için $w_L(r) = \sum_{i=0}^{n-1} w_L(r_i)$ eşitliği gerçeklenir.

3.3.2. TANIM : $\mathbb{F}_2$ cismi üzerinde; her $c \in \mathbb{F}_2$ için $w_H(c) = \begin{cases} 0 & , c = 0 \\ 1 & , c = 1 \end{cases}$

biçiminde tanımlanan fonksiyona $\mathbb{F}_2$ üzerinde Hamming ağırlık fonksiyonu denir. Bu durumda her $c = (c_0, c_1, ..., c_{n-1}) \in \mathbb{F}_2^n$ için $w_H(c) = \sum_{i=0}^{n-1} w_H(c_i)$ olur.

3.3.3. TANIM : $R_2{}^n$ üzerinde iki vektör arasındaki uzaklık; $x, y \in R_2^n$, $x \neq y$ için $d_L(x,y) = w_L(x-y)$ olarak tanımlandığından bir C kodunun minimum Lee uzaklığı $d_L(C) = \min\{d_L(x,y) \mid x, y \in C, x \neq y\}$ biçiminde tanımlanır.

$\mathbb{F}_2^n$ de Lee ağırlığı yerine Hamming ağırlığı yazılarak benzer tanım verilir. $\mathbb{F}_2^n$ üzerinde bir C kodunun minimum Hamming uzaklığı $d_H(C)$ ile gösterilir.

3.3.4. TANIM : $R_2 = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$ olmak üzere;

$$\Phi : R_2^n \longrightarrow IF_2^{4n}$$

$$(r_1, r_2, ..., r_n) \mapsto \Phi(r_1, r_2, ..., r_n) = (c_1, c_2, ..., c_n, a_1 + c_1, a_2 + c_2, ..., a_n + c_n, b_1 + c_1,$$
$$b_2 + c_2, ..., b_n + c_n, a_1 + b_1 + c_1, a_2 + b_2 + c_2, ..., a_n + b_n + c_n)$$

biçiminde tanımlanan dönüşüme R_2 halkası üzerindeki Gray dönüşümü denir. Burada $1 \leq i \leq n$ için $a_i, b_i, c_i \in \mathbb{F}_2$ olmak üzere $r_i = a_i + b_i.u + c_i.u^2 \in R_2$ dır.

$R_2 = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$ halkası üzerindeki n uzunluğunda bir kodun 3.3.4. Tanımdaki Gray dönüşümü altındaki görüntüsü $4n$ uzunluğunda bir binary koddur. $R_2{}^n$ üzerinde tanımlanan Lee uzaklığı ve $\mathbb{F}_2^{4n}$ üzerinde tanımlanan Hamming uzaklığı arasında her $x, y \in R_2^n$ için $d_L(x,y) = d_H(\Phi(x), \Phi(y))$ ilişkisi vardır. Bu Gray dönüşümünün bir izometri olduğunu göstermektedir.

3.3.5. TANIM : $R_2 = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$ halkası üzerinde;

$\alpha_1, \alpha_2 \in \mathbb{Z}_+ \cup \{0\}$ için ilk satır bileşenleri $\{1\}$ kümesinden, diğer satır elemanları $\alpha_2 = 0$ iken $\{0, 1, u, u^2, 1+u, 1+u^2, u+u^2, 1+u+u^2\}$ kümesinden, $\alpha_1 = 0$ iken $\{0, u^2\}$ kümesinden seçilen ve sütunları da lexicographically sıralama bağıntısına göre sıralanmış olan satır sayısı $\alpha_1 + \alpha_2 + 1$ olacak şekilde özel olarak oluşturulan M^{α_1,α_2} matrisine üreteç matrisi denir.

Aşağıda M^{α_1,α_2} matrisleri için birkaç örnek verilmiştir.

$$M^{0,0} = [1]_{1x1} \ , \ M^{0,1} = \begin{bmatrix} 1 & 1 \\ 0 & u^2 \end{bmatrix}_{2x2} \ , \ M^{0,2} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & u^2 & u^2 \\ 0 & u^2 & 0 & u^2 \end{bmatrix}_{3x4} \ ,$$

$$M^{0,3}=\begin{bmatrix}1&1&1&1&1&1&1&1\\0&0&0&0&u^2&u^2&u^2&u^2\\0&0&u^2&u^2&0&0&u^2&u^2\\0&u^2&0&u^2&0&u^2&0&u^2\end{bmatrix}_{4x8},$$

$$M^{1,0}=\begin{bmatrix}1&1&1&1&1&1&1&1\\0&1&u&u^2&1+u&1+u^2&u+u^2&1+u+u^2\end{bmatrix}_{2x8},$$

$$M^{1,1}=\begin{bmatrix}1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\0&0&1&1&u&u&u^2&u^2&1+u&1+u&1+u^2&1+u^2&u+u^2&u+u^2&1+u+u^2&1+u+u^2\\0&u^2&0&u^2&0&u^2&0&u^2&0&u^2&0&u^2&0&u^2&0&u^2\end{bmatrix}_{3x16}$$

.

3.3.6. TANIM : $R_2=\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2$ halkası üzerinde;

her $\alpha_1,\ \alpha_2\geq 0$ tamsayıları için $C^{\alpha_1,\alpha_2}=\{\ (c_1,c_2).M^{\alpha_1,\alpha_2}\ \big|\ c_1\in R_2^{\alpha_1+1},\ c_2\in\mathbb{F}_2^{\alpha_2}\}$ biçiminde yazılan koda M^{α_1,α_2} üreteç matrisi ile üretilmiş, uzunluğu $n=2^{3\alpha_1+\alpha_2}$ olan $(n,8n,2n)$ parametreli kod denir.

3.3.7. TEOREM : Φ , R_2^n üzerinde bir Gray dönüşümü olsun. C^{α_1,α_2}, M^{α_1,α_2} üreteç matrisi ile yazılan kod olmak üzere $\Phi(C^{\alpha_1,\alpha_2})$ kodu, $\mathbb{F}_2$ üzerinde $(4n,8n,2n)$ parametreli bir Hadamard kodudur.

Kanıt: Boyutu $(\alpha_1+\alpha_2+1)\times n$ olan M^{α_1,α_2} üreteç matrisi ile oluşturulan kod $C^{\alpha_1,\alpha_2}=\{\ (c_1,c_2).M^{\alpha_1,\alpha_2}\ \big|\ c_1\in R_2^{\alpha_1+1},c_2\in\mathbb{F}_2^{\alpha_2}\}$ biçimindedir. Tanımlanan bu kodun uzunluğu $n=2^{3\alpha_1+\alpha_2}$ dir. $C^{\alpha_1,\alpha_2}\subseteq {R_2}^n$ olan bu kodun bir tekrar kod olduğu ve eleman sayısının da $8n$ olduğu açıktır. $\Phi(C^{\alpha_1,\alpha_2})\subseteq {\mathbb{F}_2}^{4n}$ olduğundan $\Phi(C^{\alpha_1,\alpha_2})$, $(4n,8n,2n)$ parametreli bir binary Hadamard koddur.

3.3.8. SONUÇ : $\alpha_1=\alpha_2=0$ durumu dışında; $(C^{\alpha_1,\alpha_2})^{\perp}$ dual kodunun parametresi $(n,\frac{8^n}{8n},4)$ olur. Ayrıca $\Phi((C^{\alpha_1,\alpha_2})^{\perp})$, $(4n,\frac{8^n}{8n},4)$ parametreli bir koddur.

Kanıt: C^{α_1,α_2} kodunun üreteç matrisi olan M^{α_1,α_2} matrisi $(C^{\alpha_1,\alpha_2})^{\perp}$ kodu için parity-check matrisidir. $(C^{\alpha_1,\alpha_2})^{\perp}$ kodunun elemanları, boyutu $(\alpha_1+\alpha_2+1)\times n$ olan M^{α_1,α_2} üreteç matrisi yardımıyla $M^{\alpha_1,\alpha_2}.c^T=0$ koşulunu sağlayan $c\in R_2^n$

elemanlarıdır. Bu koşulu sağlayan sözcük sayısı $\frac{8^n}{8n}$ dir. $\frac{8^n}{8n}$ sayıda yazılan kod sözcüklerinin en küçük ağırlığının 4 olduğu açıktır. Böylece $(C^{\alpha_1,\alpha_2})^{\perp}$ kodu $(n,\frac{8^n}{8n},4)$ parametresine sahip olur. Buradan $\Phi((C^{\alpha_1,\alpha_2})^{\perp})$ kodunun da $(4n,\frac{8^n}{8n},4)$ parametreli bir kod olduğu görülür.

3.3.9. TANIM : $n=2^{3\alpha_1+\alpha_2}$ olmak üzere C^{α_1,α_2}, R_2^n üzerinde n uzunluğunda bir lineer kod olsun.

$$\tau : R_2^n \longrightarrow R_2^n$$

$$(c_1,c_2,...,c_n) \mapsto \tau(c_1,c_2,...,c_n)=(c_n,c_1,...,c_{n-1})$$

permütasyonu için $\tau(C^{\alpha_1,\alpha_2})=C^{\alpha_1,\alpha_2}$ sağlanıyorsa C^{α_1,α_2} koduna R_2 üzerinde bir cyclic kod denir.

3.3.10. TANIM : $n=2^{3\alpha_1+\alpha_2}$ olmak üzere D^{α_1,α_2}, $\mathbb{F}_2$ üzerinde $4n$ uzunluğunda bir lineer kod olsun.

$$\sigma^{\otimes 4} : \mathbb{F}_2^{4n} \longrightarrow \mathbb{F}_2^{4n}$$

$$(d_1,d_2,...,d_{4n}) \mapsto \sigma^{\otimes 4}(d_1,d_2,...,d_{4n}) = (d_n,d_1,...,d_{n-1},d_{2n},d_{n+1},...d_{2n-1},$$
$$d_{3n},d_{2n+1},...d_{3n-1},d_{4n},d_{3n+1},...d_{4n-1})$$

permütasyonu için $\sigma^{\otimes 4}(D^{\alpha_1,\alpha_2})=D^{\alpha_1,\alpha_2}$ sağlanıyorsa D^{α_1,α_2} koduna $\mathbb{F}_2$ üzerinde 4. mertebeden bir quasi-cyclic kod denir.

3.3.11. ÖNERME : τ dönüşümü R_2^n üzerinde, $\sigma^{\otimes 4}$ dönüşümü $\mathbb{F}_2^{4n}$ üzerinde bir permütasyon ve Φ, R_2^n den $\mathbb{F}_2^{4n}$ e yukarıda tanımlanan Gray dönüşümünü ise $\Phi\circ\tau=\sigma^{\otimes 4}\circ\Phi$ eşitliği sağlanır.

Kanıt: Her $1\le i\le n$ için $x_i=a_i+ub_i+u^2c_i \in R_2$ olmak üzere $x=(x_1,x_2,...,x_n)\in R_2^n$ olsun. Bu durumda $x\in R_2^n$ in Gray görüntüsünü

$$\Phi(x)=\Phi(x_1,x_2,...,x_n)=\Phi(a_1+ub_1+u^2c_1,a_2+ub_2+u^2c_2,...,a_n+ub_n+u^2c_n)$$
$$=(c_1,c_2,...,c_n,a_1+c_1,a_2+c_2,...,a_n+c_n,b_1+c_1,b_2+c_2,...,$$
$$b_n+c_n,a_1+b_1+c_1,a_2+b_2+c_2,...,a_n+b_n+c_n)$$

olarak bulunur. Buradan

$$\sigma^{\otimes 4}(\Phi(x)) = (c_n, c_1, c_2, ..., c_{n-1}, a_n + c_n, a_1 + c_1, a_2 + c_2, ..., a_{n-1} + c_{n-1}, b_n + c_n,$$
$$b_1 + c_1, b_2 + c_2, ..., b_{n-1} + c_{n-1}, a_n + b_n + c_n, a_1 + b_1 + c_1, a_2 + b_2 + c_2, ..., a_{n-1} + b_{n-1} + c_{n-1})$$

elde edilir. Diğer taraftan,

$\tau(x) = \tau(x_1, x_2, ..., x_n) = (x_n, x_1, ..., x_{n-1})$ dir. Böylece

$$\Phi(\tau(x)) = \Phi(\tau(x_1, x_2, ..., x_n)) = \Phi(x_n, x_1, ..., x_{n-1})$$

$$= \Phi(a_n + ub_n + u^2 c_n, a_1 + ub_1 + u^2 c_1, a_2 + ub_2 + u^2 c_2, ..., a_{n-1} + ub_{n-1} + u^2 c_{n-1})$$

$$= (c_n, c_1, c_2, ..., c_{n-1}, a_n + c_n, a_1 + c_1, a_2 + c_2, ..., a_{n-1} + c_{n-1}, b_n + c_n,$$
$$b_1 + c_1, b_2 + c_2, ..., b_{n-1} + c_{n-1}, a_n + b_n + c_n, a_1 + b_1 + c_1, a_2 + b_2 + c_2, ..., a_{n-1} + b_{n-1} + c_{n-1}).$$

elde edilir.

3.3.12. TEOREM : $\alpha_2 \neq 0$ olmak üzere, M^{α_1,α_2} üreteç matrisi ile elde edilen bir Hadamard kodu 4. mertebeden bir quasi-cyclic koddur.

Kanıt: $\alpha_2 \neq 0$ olsun. M^{α_1,α_2} üreteç matrisleri ile elde edilen bir C^{α_1,α_2} kodunun uzunluğu $n = 2^{3\alpha_1+\alpha_2}$ dir. Buradan C^{α_1,α_2} kodunun Gray görüntüsü $\Phi(C^{\alpha_1,\alpha_2})$ kodunun $\mathbb{F}_2$ cismi üzerinde uznuluğunun $2^{3\alpha_1+\alpha_2+2}$ olduğu görülür. Bu durumda Hadamard matrisi ile elde edilen Hadamard kodu $\Phi(C^{\alpha_1,\alpha_2})$ koduna eşit olduğu sonucuna varılır. 3.3.11. Önerme kullanılarak $\sigma^{\otimes 4}(\Phi\ (C^{\alpha_1,\alpha_2})) = \Phi(\tau(C^{\alpha_1,\alpha_2})) = \Phi\ (C^{\alpha_1,\alpha_2})$ eşitliği elde edilir. Φ bire-bir bir fonksiyon olduğundan $\sigma^{\otimes 4}(\Phi\ (C^{\alpha_1,\alpha_2})) = \Phi(C^{\alpha_1,\alpha_2})$ bulunur. Sonuç olarak $\Phi(C^{\alpha_1,\alpha_2})$ Hadamard kodu 4. mertebeden bir quasi-cyclic koddur.

3.3.13. TANIM : $\alpha_1, \alpha_2 \geq 0$ ve $n = 2^{3\alpha_1+\alpha_2}$ olsun. $C^{\alpha_1,\alpha_2} \subseteq R_2^{\ n}$ bir kod olmak üzere $even(C^{\alpha_1,\alpha_2}) = \{\ (c_1, c_3, ..., c_{n-1}) \in R_2^{\frac{n}{2}} \mid (c_1, c_3, ..., c_{n-1}) \in C^{\alpha_1,\alpha_2}\}$ biçiminde tanımlanan koda R_2 halkası üzerinde <u>çift kod</u> denir. $odd(C^{\alpha_1,\alpha_2}) = \{\ (c_2, c_4, ..., c_n) \in R_2^{\frac{n}{2}} \mid (c_2, c_4, ..., c_n) \in C^{\alpha_1,\alpha_2}\}$ biçiminde tanımlanan koda R_2 halkası üzerinde <u>tek kod</u> denir. Çift ve tek kod tanımları $\mathbb{F}_2$ cismi üzerinde de benzer biçimde verilir.

3.3.14. ÖNERME : $C^{\alpha_1,\alpha_2} \subseteq R_2^{\ n}$ bir kod olmak üzere,

i) $\alpha_1 \geq 1, \alpha_2 = 0$ ise $even(C^{\alpha_1,\alpha_2}) = odd(C^{\alpha_1,\alpha_2}) = C^{\alpha_1-1,2}$ dir

ii) $\alpha_1 \geq 0, \alpha_2 \geq 1$ ise $even(C^{\alpha_1,\alpha_2}) \approx odd(C^{\alpha_1,\alpha_2}) = C^{\alpha_1,\alpha_2-1}$ dir.

3.3.15. ÖNERME : $C^{\alpha_1,\alpha_2} \subseteq R_2^{\,n}$ bir kod, Φ , R_2 halkası üzerinde Gray dönüşümü olsun. Bu durumda $even(\Phi(C^{\alpha_1,\alpha_2})) = \Phi(even(C^{\alpha_1,\alpha_2}))$ sağlanır.

Kanıt: $1 \le i \le n$ ve $r_i = a_i + b_i.u + c_i.u^2 \in R_2$ olmak üzere, her $r = (r_1, r_2, ..., r_n) \in C^{\alpha_1,\alpha_2}$ için

$$\Phi(r) = \Phi(r_1, r_2, ..., r_n) = \Phi(a_1 + b_1.u + c_1.u^2, a_2 + b_2.u + c_2.u^2, ..., a_n + b_n.u + c_n.u^2)$$
$$= (c_1, c_2, ..., c_n, a_1 + c_1, a_2 + c_2, ..., a_n + c_n, b_1 + c_1, b_2 + c_2, ...,$$
$$b_n + c_n, a_1 + b_1 + c_1, a_2 + b_2 + c_2, ..., a_n + b_n + c_n) \in \Phi(C^{\alpha_1,\alpha_2})$$

bulunur. Buradan

$$(c_1, c_3, ..., c_{n-1}, a_1 + c_1, a_3 + c_3, ..., a_{n-1} + c_{n-1}, b_1 + c_1, b_3 + c_3, ..., b_{n-1} + c_{n-1},$$
$$a_1 + b_1 + c_1, a_3 + b_3 + c_3, ..., a_{n-1} + b_{n-1} + c_{n-1}) \in even(\Phi(C^{\alpha_1,\alpha_2}))$$

dir. Diğer taraftan

$r' = (r_1, r_3, ..., r_{n-1}) = (a_1 + b_1.u + c_1.u^2, a_3 + b_3.u + c_3.u^2, ..., a_{n-1} + b_{n-1}.u + c_{n-1}.u^2) \in even(C^{\alpha_1,\alpha_2})$ olsun. Gray görüntüsünü alındığında

$$\Phi(r') = (c_1, c_3, ..., c_{n-1}, a_1 + c_1, a_3 + c_3, ..., a_{n-1} + c_{n-1}, b_1 + c_1, b_3 + c_3, ..., b_{n-1} + c_{n-1},$$
$$a_1 + b_1 + c_1, a_3 + b_3 + c_3, ..., a_{n-1} + b_{n-1} + c_{n-1}) \in \Phi(even(C^{\alpha_1,\alpha_2}))$$

bulunur 3.3.17. Önerme tek kodlar için de verilebilir.

3.3.16. ÖRNEK : $C^{0,1}$ kodunu belirlemek için $M^{0,1}$ üreteç matrisini yazalım.

$M^{0,1}$ matrisi $\begin{bmatrix} 1 & 1 \\ 0 & u^2 \end{bmatrix}_{2x2}$ dir. Buradan $C^{0,1}$ kodunun elemanları $c_1 \in R_2$, $c_2 \in \mathbb{F}_2$ olmak üzere $c = (c_1, c_2).M^{0,1}$ biçimindeki elemanlardır.

$$C^{0,1} = \{\, 0\ 0, 0\ u^2, 11, 11 + u^2, u\ u, u\ u + u^2, u^2\ u^2, u^2\ 0, 1 + u1 + u, 1 + u1 + u + u^2, 1 + u^2 1 + u^2$$
$$1 + u^2 1, u + u^2\ u + u^2, u + u^2\ u, 1 + u + u^2 1 + u + u^2, 1 + u + u^2 1 + u \} \subseteq R_2^2$$

kodu için $d_L(C^{0,1}) = 4$ ve $\left|C^{0,1}\right| = 16$ dir. Dolayısı ile $C^{0,1}$ kodunun parametresi $(2, 16, 4)$ olur.

Buradan $C^{0,1}$ kodunun Gray görüntüsü alınırsa

$$\Phi(C^{0,1}) = \{\, 00000000, 01010101, 00110011, 01100110,$$
$$11111111, 10101010, 11001100, 10011001,$$
$$00001111, 01011010, 00111100, 01101001,$$
$$11110000, 10100101, 11000011, 10010110 \} \subseteq \mathbb{F}_2^8$$

kodu elde edilir. $\Phi(C^{0,1})$ kodu $(8,16,4)$ parametreli bir Hadamard kodudur. Diğer taraftan $M=\begin{bmatrix} 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 1 \\ -1 & -1 & -1 & 1 \end{bmatrix}_{4x4}$ normalleştirilmiş bir Hadamard matrisi olmak üzere M Hadamard matrisinde 1 yerine 0 ve -1 yerine 1 yazılarak M marisinin satırlarından, $0000, 1010, 1100$ ve 0110 vektörleri elde edilir. Bu vektörlerin tamamlayıcıları da ilave edilerek $0000, 1010, 1100, 0110, 1111, 0101, 0011$ ve 1001 vektörleri oluşturulur. Bu vektörlerin tamamlayıcıları alınır ve tekrarlayıcıları ile yeniden düzenlenlenirse

$00000000, 01010101, 00110011, 01100110, 11111111, 10101010, 11001100, 10011001,$

$00001111, 01011010, 00111100, 01101001, 11110000, 10100101, 11000011, 10010110$

vektörleri elde edilir. Bu vektörlerin oluşturduğu küme bir ikili koddur. Bu kodun uzunluğu 8, eleman sayısı 16 ve Hamming ağırlığı da 4 tür. Böylece M Hadamard matrisi ile Hadamard kodu elde edilir. Bulunan kod $(8,16,4)\_$ parametreli $\Phi(C^{0,1})$ koduna eşittir. Ayrıca $(C^{0,1})^{\perp}=\{00, uu, u^2u^2, u+u^2u+u^2\} \subseteq \mathbb{F}_2^2$ ve $\Phi((C^{0,1})^{\perp})=\{00000000, 00001111, 11111111, 11110000\} \subseteq IF_2^8$ olur. Bunun dışında $C^{0,1}$ kodu, $\tau(C^{0,1})=C^{0,1}$ koşulunu sagladığından bir cyclic koddur. Benzer biçimde $\sigma^{\otimes 4}(\Phi(C^{0,1}))=\Phi(C^{0,1})$ saglandığından $\Phi(C^{0,1})$ kodu, 4. mertebeden bir quasi-cyclic koddur. Ayrıca $even(C^{0,1})=\{0,1,u,u^2,1+u,1+u^2,u+u^2,1+u+u^2\}=C^{0,0}=R_2$ elde edilir. Bu durumda $\Phi(even(C^{0,1}))=\{0000, 0011, 1111, 1100, 0101, 0110, 1010, 1001\}$ bulunur. Buradan $even(\Phi(C^{0,2}))=\Phi(even(C^{0,2}))$ eşitliği gerçeklenir.

3.4. $\mathbb{F}_2+u\mathbb{F}_2+...+u^m\mathbb{F}_2$ Üzerindeki Kodlar ile Hadamard Kodların İlişkisi

Bu bölümde, 3.1. ve 3.3. bölümlerde verilen halkalar üzerindeki çalışmalar $u^{m+1}=0$ durumunda $\mathbb{F}_2+u\mathbb{F}_2+...+u^m\mathbb{F}_2$ halkası üzerinde genişletilmiştir. Burada

$$\mathbb{F}_2[u]/_{<u^{m+1}>}=\{x_0+x_1.u+...+x_m.u^m+<u^{m+1}> \mid \ x_i \in \mathbb{F}_2,\ 0\le i\le m,\ m\ge 1,\ m\in\mathbb{Z}\}$$

halkası $u^{m+1}=0$ alınması durumunda $m\ge 1,\ m\in\mathbb{Z}$ olmak üzere

$R_m = \mathbb{F}_2 + u\mathbb{F}_2 + ... + u^m\mathbb{F}_2$ halkasına izomorftur. R_m halkasının mertebesi 2^{m+1} dir. Bu halkanın idealleri arasında $I_0 = (0) \subset I_{u^m} = (u^m) \subset ... I_{u^2} = (u^2) \subset I_u = (u) \subset R_m$ ilişkisi vardır.

3.4.1. TANIM : $R_m = \mathbb{F}_2 + u\mathbb{F}_2 + ... + u^m\mathbb{F}_2$ halkası üzerinde;

her $r \in R_m$ için $w_{\text{hom}}(r) = \begin{cases} 0 & , r = 0 \\ 2^m & , r = u^m \\ 2^{m-1} & , \textit{otherwise} \end{cases}$

biçiminde tanımlanan fonksiyona, R_m üzerinde homogeneous ağırlık fonksiyonu denir.

Bu durumda her $r = (r_o, r_1, ..., r_{n-1}) \in R_m^n$ için $w_{\text{hom}}(r) = \sum_{i=0}^{n-1} w_{\text{hom}}(r_i)$ eşitliği gerçeklenir.

3.4.2. TANIM : $\mathbb{F}_2$ cismi üzerinde;

her $c \in \mathbb{F}_2$ için $w_H(c) = \begin{cases} 0 & , c = 0 \\ 1 & , c = 1 \end{cases}$ biçiminde tanımlanan fonksiyona $\mathbb{F}_2$ üzerinde Hamming ağırlık fonksiyonu denir. Bu durumda her $c = (c_o, c_1, ..., c_{n-1}) \in \mathbb{F}_2^n$ için $w_H(c) = \sum_{i=0}^{n-1} w_H(c_i)$ olur.

3.4.3. TANIM : R_m^n üzerinde iki vektör arasındaki uzaklık $a, b \in R_m^n$, $a \neq b$ için $d_{\text{hom}}(a,b) = w_{\text{hom}}(a-b)$ olmak üzere bir C kodunun minimum homogeneous uzaklığı $d_{\text{hom}}(C) = \min\{d_{\text{hom}}(a,b) \mid a,b \in C, a \neq b\}$ biçiminde tanımlanır. $\mathbb{F}_2^n$ de homogeneous ağırlığı yerine Hamming ağırlığı yazılarak benzer tanım verilir. $\mathbb{F}_2^n$ üzerinde bir C kodunun minimum Hamming uzaklığı $d_H(C)$ ile gösterilir.

3.4.4. TANIM : $R_m = \mathbb{F}_2 + u\mathbb{F}_2 + ... + u^m\mathbb{F}_2$ olmak üzere;

$$\Phi : R_m^n \longrightarrow \mathbb{F}_2^{2^m.n}$$

$$a_0 + a_1.u + ... + a_m.u^m \mapsto \Phi(a_0 + a_1.u + ... + a_m.u^m)$$

$$\Phi(a_0 + a_1.u + ... + a_m.u^m) = (a_m, a_m + a_0, a_m + a_1, ..., a_m + a_{m-1}, a_m + a_0 + a_1, a_m + a_0 + a_2, ...,$$
$$a_m + a_0 + a_{m-1}, a_m + a_1 + a_2, ..., a_m + a_1 + a_{m-1}, a_m + a_2 + a_3, ..., a_m + a_2 + a_{m-1}, ...,$$
$$a_m + a_{m-2} + a_{m-1}, a_m + a_0 + a_1 + a_2, ..., a_m + a_0 + a_1 + a_{m-1}, ...,$$
$$a_m + a_{m-3} + a_{m-2} + a_{m-1}, a_m + a_0 + a_1 + a_2 + a_3, ...,$$
$$a_m + a_{m-4} + a_{m-3} + a_{m-2} + a_{m-1}, ..., ..., a_m + a_0 + a_1 + ... + a_{m-1})$$

biçiminde tanımlanan dönüşüme, R_m halkası üzerindeki Gray dönüşümü denir. Burada $0 \le i \le m$ için $a_i \in \mathbb{F}_2^n$ dir.

Bu tanım ile birlikte $R_m = \mathbb{F}_2 + u\mathbb{F}_2 + ... + u^m\mathbb{F}_2$ üzerindeki n uzunluğunda bir kodun Gray görüntüsü $2^m.n$ uzunluğunda bir binary koddur. R_m^n üzerinde tanımlanan homogeneous uzaklığı ile $\mathbb{F}_2^{2^m n}$ üzerinde tanımlanan Hamming uzaklığı arasında, her $a, b \in R_m^n$ için $d_{\text{hom}}(a,b) = d_H(\Phi(a), \Phi(b))$ ilişkisi vardır. Bu Gray dönüşümünün bir izometri olduğunu göstermektedir.

3.4.5. TANIM : $R_m = \mathbb{F}_2 + u\mathbb{F}_2 + ... + u^m\mathbb{F}_2$ halkası üzerinde;

α , $\beta \in \mathbb{Z}_+ \cup \{0\}$ için ilk satır bileşenleri $\{1\}$ kümesinden, diğer satır elemanları $\beta = 0$ iken $\{0, 1, u, ..., u^m, 1+u, ..., 1+u^m, ..., 1+u+...+u^m\}$ kümesinden, $\alpha = 0$ iken $\{0, u^m\}$ kümesinden seçilen, sütunları lexicographically sıralama bağıntısına göre sıralanmış olarak ve satır sayısı $\alpha + \beta + 1$ olacak şekilde özel olarak oluşturulan $G^{\alpha,\beta}$ matrisine üreteç matrisi denir.

Aşağıda $G^{\alpha,\beta}$ matrisleri için birkaç örnek verilmiştir.

$$G^{0,0} = [1]_{1x1} \ , \ G^{0,1} = \begin{bmatrix} 1 & 1 \\ 0 & u^m \end{bmatrix}_{2x2} \ , \ G^{0,2} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & u^m & u^m \\ 0 & u^m & 0 & u^m \end{bmatrix}_{3x4} \ ,$$

$$G^{0,3} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & u^m & u^m & u^m & u^m \\ 0 & 0 & u^m & u^m & 0 & 0 & u^m & u^m \\ 0 & u^m & 0 & u^m & 0 & u^m & 0 & u^m \end{bmatrix}_{4x8} \ ,$$

$$G^{1,0} = \begin{bmatrix} 1 & 1 & 1 & 1 & . & . & . & 1 & . & . & . & 1 \\ 0 & 1 & u & 1+u & . & . & . & 1+u^m & . & . & . & 1+u+...+u^m \end{bmatrix}_{2\times 2^{m+1}} .$$

3.4.6. TANIM : $R_m = \mathbb{F}_2 + u\mathbb{F}_2 + ... + u^m\mathbb{F}_2$ halkası üzerinde;

her $\alpha, \beta \ge 0$ tamsayıları için $C^{\alpha,\beta} = \{ (c_1, c_2).G^{\alpha,\beta} \mid c_1 \in R_m^{\alpha+1}, c_2 \in \mathbb{F}_2^{\beta} \}$ biçiminde yazılan koda $G^{\alpha,\beta}$ üreteç matrisi ile üretilmiş, uzunluğu $n = 2^{(m+1).\alpha+\beta}$ olan $(n, 2^{m+1}.n, 2^{m-1}.n)$ parametreli kod denir.

3.4.7. TEOREM : Φ , R_m^n üzerinde bir Gray dönüşümü olsun. $C^{\alpha,\beta}$, $G^{\alpha,\beta}$ üreteç matrisi ile yazılan kod olmak üzere $\Phi(C^{\alpha,\beta})$ kodu, $\mathbb{F}_2$ üzerinde $(2^m.n, 2^{m+1}.n, 2^{m-1}.n)$ parametreli bir Hadamard kodudur.

Kanıt: Boyutu $(\alpha+\beta+1)\times n$ olan $G^{\alpha,\beta}$ üreteç matrisi ile oluşturulan kod $C^{\alpha,\beta} = \{ (c_1, c_2).G^{\alpha,\beta} \mid c_1 \in R_m^{\alpha+1}, c_2 \in \mathbb{F}_2^{\beta} \}$ biçimindedir. Tanımlanan bu kodun uzunluğu $n = 2^{(m+1).\alpha+\beta}$ dir. $C^{\alpha,\beta} \subseteq R_m^n$ olan bu kodun bir tekrar kodu olduğu ve eleman sayısının da $2^{m+1}.n$ olduğu açıktır. Buradan $\Phi(C^{\alpha,\beta}) \subseteq \mathbb{F}^{2^m.n}$ olduğundan $\Phi(C^{\alpha,\beta})$, $(2^m.n, 2^{m+1}.n, 2^{m-1}.n)$ parametreli bir binary Hadamard kodudur.

3.4.8. SONUÇ : $\alpha = \beta = 0$ durumu dışında; $(C^{\alpha,\beta})^{\perp}$ dual kodunun parametresi $(n, \frac{(2^{m+1})^n}{2^{m+1}.n}, 4)$ dür. Ayrıca $\Phi((C^{\alpha,\beta})^{\perp})$ da $(2^m.n, \frac{(2^{m+1})^n}{2^{m+1}.n}, 4)$ parametreli bir koddur.

Kanıt: $C^{\alpha,\beta}$ kodunun üreteç matrisi olan $G^{\alpha,\beta}$ matrisi, $(C^{\alpha,\beta})^{\perp}$ kodu parity-check matrisidir. Boyutu $(\alpha+\beta+1)\times n$ olan $(C^{\alpha,\beta})^{\perp}$ kodunun elemanları; $G^{\alpha,\beta}$ üreteç matrisi olmak üzere $G^{\alpha,\beta}.x^T = 0$ koşulunu sağlayan $x \in R_m^n$ elemanlarıdır. Bu koşulu sağlayan sözcük sayısı $\frac{(2^{m+1})^n}{2^{m+1}.n}$ dir. Bu tip kod sözcüklerinin en küçük ağırlığının 4 olduğu açıktır. Böylece $(C^{\alpha,\beta})^{\perp}$ kodu $(n, \frac{(2^{m+1})^n}{2^{m+1}.n}, 4)$ parametresine sahip olur. Buradan $\Phi((C^{\alpha,\beta})^{\perp})$ kodunun da $(2^m.n, \frac{(2^{m+1})^n}{2^{m+1}.n}, 4)$ parametreli kod olduğu görülür.

3.4.9. TANIM : $n = 2^{(m+1).\alpha+\beta}$ olmak üzere $C^{\alpha,\beta}$, R_m üzerinde n uzunluğunda bir lineer kod olsun.

$$\tau : R_m^n \longrightarrow R_m^n$$

$$(c_1, c_2, ..., c_n) \mapsto \tau(c_1, c_2, ..., c_n) = (c_n, c_1, ..., c_{n-1})$$

permütasyonu tanımlansın $\tau(C^{\alpha,\beta}) = C^{\alpha,\beta}$ sağlanıyorsa $C^{\alpha,\beta}$ koduna R_m üzerinde bir cyclic kod denir.

3.4.10. TANIM : $n = 2^{(m+1).\alpha+\beta}$ olmak üzere

$$\sigma : \mathbb{F}_2^{\,n} \longrightarrow \mathbb{F}_2^{\,n}$$

$$(x_1, x_2, ..., x_n) \mapsto \sigma(x_1, x_2, ..., x_n) = (x_n, x_1, ..., x_{n-1})$$

dönüşümüne $\mathbb{F}_2$ üzerinde cyclic permütasyonu denir.

3.4.11. TANIM : $n = 2^{(m+1).\alpha+\beta}$ olmak üzere $D^{\alpha,\beta}$, $\mathbb{F}_2$ üzerinde $2^m.n$ uzunluğunda bir lineer kod olsun. $a \in \mathbb{F}_2^{2^m.n}$ elemanı $i = 1, 2, ..., 2^m$ için $a^{(i)} \in \mathbb{F}_2^n$ olmak üzere $a = (a_1, a_2, ..., a_{2^m.n}) = (a^{(1)} \mid a^{(2)} \mid \ ... \mid a^{(2^m)})$ biçiminde yazılır. $\sigma^{\otimes 2^m}$, $\mathbb{F}_2^{2^m.n}$ den $\mathbb{F}_2^{2^m.n}$ ye $\sigma^{\otimes 2^m}(a) = (\sigma(a^{(1)}) \mid \sigma(a^{(2)}) \mid ... \mid \sigma(a^{(2^m)}))$ biçiminde tanımlanan permütasyon olmak üzere $\sigma^{\otimes 2^m}(D^{\alpha,\beta}) = D^{\alpha,\beta}$ koşulunu sağlıyorsa $D^{\alpha,\beta}$ koduna, $\mathbb{F}_2$ üzerinde 2^m. mertebeden bir quasi-cyclic kod denir.

3.4.12. ÖNERME : τ dönüşümü R_m^n üzerinde bir permütasyon, $\sigma^{\otimes 2^m}$ dönüşümü $\mathbb{F}_2^{2^m.n}$ üzerinde bir permütasyon ve Φ, R_m^n den $\mathbb{F}_2^{2^m.n}$ e yukarıda tanımlanan Gray dönüşümünü ise $\Phi \circ \tau = \sigma^{\otimes 2^m} \circ \Phi$ eşitliği sağlanır.

Kanıt: Her $1 \le i \le n$ için $x_i = a_{0_i} + u.a_{1_i} + ... + u^m.a_{m_i} \in R_m$ olmak üzere $x = (x_1, x_2, ..., x_n) \in R_m^n$ olsun. Bu durumda $x \in R_m^n$ in Gray görüntüsünü aldığımızda

$$\Phi(x) = \Phi(x_1, x_2, ..., x_n)$$
$$= \Phi(a_{0_1} + u.a_{1_1} + ... + u^m.a_{m_1}, a_{0_2} + u.a_{1_2} + ... + u^m.a_{m_2}, ..., a_{0_n} + u.a_{1_n} + ... + u^m.a_{m_n})$$
$$= (a_{m_1}, ..., a_{m_{n-1}}, a_{m_n}, a_{m_1} + a_{0_1}, ..., a_{m_{n-1}} + a_{0_{n-1}}, a_{m_n} + a_{0_n},$$
$$a_{m_1} + a_{1_1}, ..., a_{m_{n-1}} + a_{1_{n-1}}, a_{m_n} + a_{1_n}, a_{m_1} + a_{m-1_1}, ..., a_{m_{n-1}} + a_{m-1_{n-1}}, a_{m_n} + a_{m-1_n},$$
$$a_{m_1} + a_{0_1} + a_{1_1}, ..., a_{m_{n-1}} + a_{0_{n-1}} + a_{1_{n-1}}, a_{m_n} + a_{0_n} + a_{1_n},$$
$$a_{m_1} + a_{0_1} + a_{2_1}, ..., a_{m_{n-1}} + a_{0_{n-1}} + a_{2_{n-1}}, a_{m_n} + a_{0_n} + a_{2_n}, ...,$$
$$a_{m_1} + a_{0_1} + a_{m-1_1}, ..., a_{m_{n-1}} + a_{0_{n-1}} + a_{m-1_{n-1}}, a_{m_n} + a_{0_n} + a_{m-1_n},$$
$$a_{m_1} + a_{1_1} + a_{2_1}, ..., a_{m_{n-1}} + a_{1_{n-1}} + a_{2_{n-1}}, a_{m_n} + a_{1_n} + a_{2_n}, ..., a_{m_1} + a_{1_1} + a_{m-1_1}, ...,$$
$$a_{m_{n-1}} + a_{1_{n-1}} + a_{m-1_{n-1}}, a_{m_n} + a_{1_n} + a_{m-1_n}, a_{m_1} + a_{2_1} + a_{3_1}, ..., a_{m_{n-1}} + a_{2_{n-1}} + a_{3_{n-1}}, a_{m_n} + a_{2_n} + a_{3_n}, ...,$$
$$a_{m_1} + a_{2_1} + a_{m-1_1}, ..., a_{m_{n-1}} + a_{2_{n-1}} + a_{m-1_{n-1}}, a_{m_n} + a_{2_n} + a_{m-1_n}, ..., a_{m_1} + a_{m-2_1} + a_{m-1_1}, ...,$$
$$a_{m_{n-1}} + a_{m-2_{n-1}} + a_{m-1_{n-1}}, a_{m_n} + a_{m-2_n} + a_{m-1_n}, a_{m_1} + a_{0_1} + a_{1_1} + a_{2_1}, ..., a_{m_{n-1}} + a_{0_{n-1}} + a_{1_{n-1}} + a_{2_{n-1}},$$
$$a_{m_n} + a_{0_n} + a_{1_n} + a_{2_n}, ..., a_{m_1} + a_{0_1} + a_{1_1} + a_{m-1_1}, ..., a_{m_{n-1}} + a_{0_{n-1}} + a_{1_{n-1}} + a_{m-1_{n-1}},$$
$$a_{m_n} + a_{0_n} + a_{1_n} + a_{m-1_n}, ..., a_{m_1} + a_{m-3_1} + a_{m-2_1} + a_{m-1_1}, ..., a_{m_{n-1}} + a_{m-3_{n-1}} + a_{m-2_{n-1}} + a_{m-1_{n-1}},$$

$a_{m_n} + a_{m-3_n} + a_{m-2_n} + a_{m-1_n}, a_{m_1} + a_{0_1} + a_{1_1} + a_{2_1} + a_{3_1}, ..., a_{m_{n-1}} + a_{0_{n-1}} + a_{1_{n-1}} + a_{2_{n-1}} + a_{3_{n-1}},$

$a_{m_n} + a_{0_n} + a_{1_n} + a_{2_n} + a_{3_n}, ..., a_{m_1} + a_{m-4_1} + a_{m-3_1} + a_{m-2_1} + a_{m-1_1}, ...,$

$a_{m_{n-1}} + a_{m-4_{n-1}} + a_{m-3_{n-1}} + a_{m-2_{n-1}} + a_{m-1_{n-1}}, a_{m_n} + a_{m-4_n} + a_{m-3_n} + a_{m-2_n} + a_{m-1_n}, ...,$

$..., a_{m_1} + a_{0_1} + a_{1_1} + ... + a_{m-1_1}, ..., a_{m_{n-1}} + a_{0_{n-1}} + a_{1_{n-1}} + ... + a_{m-1_{n-1}}, a_{m_n} + a_{0_n} + a_{1_n} + ... + a_{m-1_n})$

olarak bulunur. Buradan

$\sigma^{\otimes 2^m}(\Phi(x)) = (a_{m_n}, a_{m_1}, ..., a_{m_{n-1}}, a_{m_n} + a_{0_n}, a_{m_1} + a_{0_1}, ..., a_{m_{n-1}} + a_{0_{n-1}},$

$a_{m_n} + a_{1_n}, a_{m_1} + a_{1_1}, ..., a_{m_{n-1}} + a_{1_{n-1}}, a_{m_n} + a_{m-1_n}, a_{m_1} + a_{m-1_1}, ..., a_{m_{n-1}} + a_{m-1_{n-1}},$

$a_{m_n} + a_{0_n} + a_{1_n}, a_{m_1} + a_{0_1} + a_{1_1}, ..., a_{m_{n-1}} + a_{0_{n-1}} + a_{1_{n-1}},$

$a_{m_n} + a_{0_n} + a_{2_n}, a_{m_1} + a_{0_1} + a_{2_1}, ..., a_{m_{n-1}} + a_{0_{n-1}} + a_{2_{n-1}}, ...,$

$a_{m_n} + a_{0_n} + a_{m-1_n}, a_{m_1} + a_{0_1} + a_{m-1_1}, ..., a_{m_{n-1}} + a_{0_{n-1}} + a_{m-1_{n-1}},$

$a_{m_n} + a_{1_n} + a_{2_n}, a_{m_1} + a_{1_1} + a_{2_1}, ..., a_{m_{n-1}} + a_{1_{n-1}} + a_{2_{n-1}}, ...,$

$a_{m_n} + a_{1_n} + a_{m-1_n}, a_{m_1} + a_{1_1} + a_{m-1_1}, ..., a_{m_{n-1}} + a_{1_{n-1}} + a_{m-1_{n-1}},$

$a_{m_n} + a_{2_n} + a_{3_n}, a_{m_1} + a_{2_1} + a_{3_1}, ..., a_{m_{n-1}} + a_{2_{n-1}} + a_{3_{n-1}}, ...,$

$a_{m_n} + a_{2_n} + a_{m-1_n}, a_{m_1} + a_{2_1} + a_{m-1_1}, ..., a_{m_{n-1}} + a_{2_{n-1}} + a_{m-1_{n-1}}, ...,$

$a_{m_n} + a_{m-2_n} + a_{m-1_n}, a_{m_1} + a_{m-2_1} + a_{m-1_1}, ..., a_{m_{n-1}} + a_{m-2_{n-1}} + a_{m-1_{n-1}},$

$a_{m_n} + a_{0_n} + a_{1_n} + a_{2_n}, a_{m_1} + a_{0_1} + a_{1_1} + a_{2_1}, ..., a_{m_{n-1}} + a_{0_{n-1}} + a_{1_{n-1}} + a_{2_{n-1}}, ...,$

$a_{m_n} + a_{0_n} + a_{1_n} + a_{m-1_n}, a_{m_1} + a_{0_1} + a_{1_1} + a_{m-1_1}, ..., a_{m_{n-1}} + a_{0_{n-1}} + a_{1_{n-1}} + a_{m-1_{n-1}}, ...,$

$a_{m_n} + a_{m-3_n} + a_{m-2_n} + a_{m-1_n}, a_{m_1} + a_{m-3_1} + a_{m-2_1} + a_{m-1_1}, ..., a_{m_{n-1}} + a_{m-3_{n-1}} + a_{m-2_{n-1}} + a_{m-1_{n-1}},$

$a_{m_n} + a_{0_n} + a_{1_n} + a_{2_n} + a_{3_n}, a_{m_1} + a_{0_1} + a_{1_1} + a_{2_1} + a_{3_1}, ..., a_{m_{n-1}} + a_{0_{n-1}} + a_{1_{n-1}} + a_{2_{n-1}} + a_{3_{n-1}} ...,$

$a_{m_n} + a_{m-4_n} + a_{m-3_n} + a_{m-2_n} + a_{m-1_n}, a_{m_1} + a_{m-4_1} + a_{m-3_1} + a_{m-2_1} + a_{m-1_1}, ...,$

$a_{m_{n-1}} + a_{m-4_{n-1}} + a_{m-3_{n-1}} + a_{m-2_{n-1}} + a_{m-1_{n-1}}, ...,$

$..., a_{m_n} + a_{0_n} + a_{1_n} + ... + a_{m-1_n}, .., a_{m_1} + a_{0_1} + a_{1_1} + ... + a_{m-1_1}, ..., a_{m_{n-1}} + a_{0_{n-1}} + a_{1_{n-1}} + ... + a_{m-1_{n-1}}).$

elde edilir. Diğer taraftan,

$\tau(x) = \tau(x_1, x_2, ..., x_n) = (x_n, x_1, ..., x_{n-1})$ dir. Böylece

$\Phi\,\tau(x) = \Phi(\tau(x_1, x_2, ..., x_n)) = \Phi(x_n, x_1, ..., x_{n-1})$

$= \Phi(a_{0_n} + u.a_{1_n} + ... + u^m.a_{m_n}, a_{0_1} + u.a_{1_1} + ... + u^m.a_{m_1}, ..., a_{0_{n-1}} + u.a_{1_{n-1}} + ... + u^m.a_{m_{n-1}})$

$= (a_{m_n}, a_{m_1}, ..., a_{m_{n-1}}, a_{m_n} + a_{0_n}, a_{m_1} + a_{0_1}, ..., a_{m_{n-1}} + a_{0_{n-1}},$

$a_{m_n} + a_{1_n}, a_{m_1} + a_{1_1}, ..., a_{m_{n-1}} + a_{1_{n-1}}, a_{m_n} + a_{m-1_n}, a_{m_1} + a_{m-1_1}, ..., a_{m_{n-1}} + a_{m-1_{n-1}},$

$a_{m_n}+a_{0_n}+a_{1_n}, a_{m_1}+a_{0_1}+a_{1_1},...,a_{m_{n-1}}+a_{0_{n-1}}+a_{1_{n-1}},$

$a_{m_n}+a_{0_n}+a_{2_n}, a_{m_1}+a_{0_1}+a_{2_1},...,a_{m_{n-1}}+a_{0_{n-1}}+a_{2_{n-1}},...,$

$a_{m_n}+a_{0_n}+a_{m-1_n}, a_{m_1}+a_{0_1}+a_{m-1_1},...,a_{m_{n-1}}+a_{0_{n-1}}+a_{m-1_{n-1}},$

$a_{m_n}+a_{1_n}+a_{2_n}, a_{m_1}+a_{1_1}+a_{2_1},...,a_{m_{n-1}}+a_{1_{n-1}}+a_{2_{n-1}},...,$

$a_{m_n}+a_{1_n}+a_{m-1_n}, a_{m_1}+a_{1_1}+a_{m-1_1},...,a_{m_{n-1}}+a_{1_{n-1}}+a_{m-1_{n-1}},$

$a_{m_n}+a_{2_n}+a_{3_n}, a_{m_1}+a_{2_1}+a_{3_1},...,a_{m_{n-1}}+a_{2_{n-1}}+a_{3_{n-1}},...,$

$a_{m_n}+a_{2_n}+a_{m-1_n}, a_{m_1}+a_{2_1}+a_{m-1_1},...,a_{m_{n-1}}+a_{2_{n-1}}+a_{m-1_{n-1}},...,$

$a_{m_n}+a_{m-2_n}+a_{m-1_n}, a_{m_1}+a_{m-2_1}+a_{m-1_1},...,a_{m_{n-1}}+a_{m-2_{n-1}}+a_{m-1_{n-1}},$

$a_{m_n}+a_{0_n}+a_{1_n}+a_{2_n}, a_{m_1}+a_{0_1}+a_{1_1}+a_{2_1},...,a_{m_{n-1}}+a_{0_{n-1}}+a_{1_{n-1}}+a_{2_{n-1}},...,$

$a_{m_n}+a_{0_n}+a_{1_n}+a_{m-1_n}, a_{m_1}+a_{0_1}+a_{1_1}+a_{m-1_1},...,a_{m_{n-1}}+a_{0_{n-1}}+a_{1_{n-1}}+a_{m-1_{n-1}},...,$

$a_{m_n}+a_{m-3_n}+a_{m-2_n}+a_{m-1_n}, a_{m_1}+a_{m-3_1}+a_{m-2_1}+a_{m-1_1},...,a_{m_{n-1}}+a_{m-3_{n-1}}+a_{m-2_{n-1}}+a_{m-1_{n-1}},$

$a_{m_n}+a_{0_n}+a_{1_n}+a_{2_n}+a_{3_n}, a_{m_1}+a_{0_1}+a_{1_1}+a_{2_1}+a_{3_1},...,a_{m_{n-1}}+a_{0_{n-1}}+a_{1_{n-1}}+a_{2_{n-1}}+a_{3_{n-1}}...,$

$a_{m_n}+a_{m-4_n}+a_{m-3_n}+a_{m-2_n}+a_{m-1_n}, a_{m_1}+a_{m-4_1}+a_{m-3_1}+a_{m-2_1}+a_{m-1_1},...,$

$a_{m_{n-1}}+a_{m-4_{n-1}}+a_{m-3_{n-1}}+a_{m-2_{n-1}}+a_{m-1_{n-1}},...,$

$...,a_{m_n}+a_{0_n}+a_{1_n}+...+a_{m-1_n},..,a_{m_1}+a_{0_1}+a_{1_1}+...+a_{m-1_1},...,a_{m_{n-1}}+a_{0_{n-1}}+a_{1_{n-1}}+...+a_{m-1_{n-1}})$

elde edilir.

3.4.13. TEOREM : $\beta \neq 0$ olmak üzere, $G^{\alpha,\beta}$ üreteç matrisi ile elde edilen Hadamard kodu $2.$mertebeden bir quasi-cyclic koddur.

Kanıt: $\alpha_2 \neq 0$ olsun. $G^{\alpha,\beta}$ üreteç matrisi ile elde edilen $C^{\alpha,\beta}$ kodunun uzunluğu $n=2^{(m+1).\alpha+\beta}$ dir. Bu durumda $C^{\alpha,\beta}$ kodunun Gray görüntüsü $\Phi(C^{\alpha,\beta})$, $\mathbb{F}_2$ cismi üzerinde uzunluğu $n=2^{(m+1).\alpha+\beta+m}$ olan bir koddur. Dolayısıyla bir Hadamard matrisi ile elde edilen Hadamard kodunun $\Phi(C^{\alpha,\beta})$ koduna eşit olduğu sonucuna varılır. 3.4.12. Önerme kullanılarak $\sigma^{\otimes 2^m}(\Phi(C^{\alpha,\beta}))=\Phi(\tau(C^{\alpha,\beta}))=\Phi(C^{\alpha,\beta})$ eşitliği elde edilir. Φ bire-bir bir fonksiyon olduğundan $\sigma^{\otimes 2^m}(\Phi(C^{\alpha,\beta}))=\Phi(C^{\alpha,\beta})$ bulunur. Sonuç olarak $\Phi(C^{\alpha,\beta})$ Hadamard kodu 2^m. mertebeden bir quasi-cyclic kodudur.

BÖLÜM 4

HALKALAR ÜZERİNDEKİ KODLAR

Bu bölümde, p bir asal sayı, $u^3 = 0, v^2 = 0$ ve $u.v = v.u = 0$ iken $\mathbb{F}_p[u,v] \Big/ < u^3,\ v^2, u.v >$ ve $\mathbb{F}_p + v\mathbb{F}_p + u\mathbb{F}_p + u^2\mathbb{F}_p$ halkaları üzerindeki kodlar çalışılmıştır. Yeni tanımlamış olduğumuz bu iki halka birbirine izomorftur. p^4 elemanlı bu halkalarda cyclic kodların yapısı, bu kodların Gray görüntüleri ve bu halkalar üzerinde ağırlık fonksiyonları verilmiştir. Bu yeni halkalar üzerindeki kodlar ile sonlu zincir halkaları üzerindeki kodlar ilişkilendirilmiştir.

Önce $p = 2$ alınarak, $\mathbb{F}_2[u,v] \Big/ < u^3,\ v^2, u.v >$ halkası üzerindeki $(1+v)-$constacyclic kodlar çalışılmıştır. Daha sonra p herhangi bir tek asal sayı olmak üzere, bu halka üzerindeki cyclic kodlar incelenmiş, özel olarak $p = 3$ durumu için cyclic kodlar ele alınmıştır. Bu halkalar üzerinde yazılan tüm kodların Gray görüntülerinin cisimler üzerinde quasi-cyclic kodlar olduğu gösterilmiştir.

Yine bu bölüm orijinal sonuçlar içermektedir ve bu sonuçlar kodlama teorisi literatürüne kazandırılmıştır. [26], [27]

4.1. $\mathbb{F}_2[u,v] \Big/ < u^3,\ v^2, u.v >$ Halkasının Yapısı ve $(1+v)-$Constacyclic Kodların Gray Görüntüleri

4.1. bölümde ilk olarak $\mathbb{F}_2[u,v] \Big/ < u^3,\ v^2, u.v >$ halkası tanımlanmış ve yapısı incelenmiştir. Bu halkadan $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$ sonlu zincir halkasına yeni bir Gray dönüşümü ile bu halkada yeni bir ağırlık fonksiyonu tarafımızca tanımlanmıştır. Ayrıca cyclic kod, constacyclic kod ve quasi-cyclic kod tanımlarına yer verilmiştir. [27]

$\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$ nin $+$ ve $\cdot$ işlemleri ile bir halka olduğu ve $u^3 = 0$ olmak üzere $\mathbb{F}_2[u] \big/ < u^3 >$ halkasına izomorf olduğu bilinmektedir. Burada $\mathbb{F}_2$ cismi yerine $v^2 = 0$ olmak üzere $R' = \mathbb{F}_2 + v\mathbb{F}_2$ halkası alındığında, $u^3 = 0$ olmak üzere $R' + uR' + u^2R'$ kümesi elde edilir. Daha açık yazılırsa bu kümenin

$$R' + uR' + u^2R' = (\mathbb{F}_2 + v\mathbb{F}_2) + u.(\mathbb{F}_2 + v\mathbb{F}_2) + u^2.(\mathbb{F}_2 + v\mathbb{F}_2)$$
$$= \mathbb{F}_2 + v\mathbb{F}_2 + u\mathbb{F}_2 + uv\mathbb{F}_2 + u^2\mathbb{F}_2 + u^2v\mathbb{F}_2$$

olduğu görülür. $(\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2, +, \cdot)$ halkasında $u^3 = 0$ olması ve $(R', +, \cdot)$ halkasında $v^2 = 0$ olması koşullarına ilave olarak $u.v = v.u = 0$ koşulu konulursa $u^2.v = (u.u).v = u.(u.v) = u.0 = 0$ olacağından $R' + uR' + u^2R'$ kümesi $R = \mathbb{F}_2 + v\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$ kümesine eşit olacaktır.

$u^3 = 0, v^2 = 0$ ve $u.v = v.u = 0$ olmak üzere

$$R = \mathbb{F}_2 + v\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 = \{0, 1, v, u, u^2, 1+v, 1+u, 1+u^2, v+u, v+u^2, u+u^2,$$
$$1+v+u, 1+v+u^2, 1+u+u^2, v+u+u^2, 1+v+u+u^2\}$$

kümesi aşağıda tanımlanan $\oplus$ ve $\otimes$ işlemleri ile koşulları altında bir halka yapısı taşır ve bu halka $\mathbb{F}_2[u, v] \big/ < u^3 = 0,\ v^2 = 0, u.v = v.u = 0 >$ halkasına izomorftur.

$\oplus$	0	1	v	u	u^2	$1+v$	$1+u$	$1+u^2$	$v+u$	$v+u^2$	$u+u^2$	$1+v+u$	$1+v+u^2$	$1+u+u^2$	$v+u+u^2$	$1+v+u+u^2$
0	0	1	v	u	u^2	$1+v$	$1+u$	$1+u^2$	$v+u$	$v+u^2$	$u+u^2$	$1+v+u$	$1+v+u^2$	$1+u+u^2$	$v+u+u^2$	$1+v+u+u^2$
1	1	0	$1+v$	$1+u$	$1+u^2$	v	u	u^2	$1+v+u$	$1+v+u^2$	$1+u+u^2$	$v+u$	$v+u^2$	$u+u^2$	$1+v+u+u^2$	$v+u+u^2$
v	v	$1+v$	0	$v+u$	$v+u^2$	1	$1+v+u$	$1+v+u^2$	u	u^2	$v+u+u^2$	$1+u$	$1+u^2$	$1+v+u+u^2$	$u+u^2$	$1+u+u^2$
u	u	$1+u$	$v+u$	0	$u+u^2$	$1+v+u$	1	$1+u+u^2$	v	$v+u+u^2$	u^2	$1+v$	$1+v+u+u^2$	$1+u^2$	$v+u^2$	$1+v+u^2$
u^2	u^2	$1+u^2$	$v+u^2$	$u+u^2$	0	$1+v+u^2$	$1+u+u^2$	1	$v+u+u^2$	v	u	$1+v+u+u^2$	$1+v$	$1+u$	$v+u$	$1+v+u$
$1+v$	$1+v$	v	1	$1+v+u$	$1+v+u^2$	0	$v+u$	$v+u^2$	$1+u$	$1+u^2$	$1+v+u+u^2$	u	u^2	$v+u+u^2$	$1+u+u^2$	$u+u^2$
$1+u$	$1+u$	u	$1+v+u$	1	$1+u+u^2$	$v+u$	0	$u+u^2$	$1+v$	$1+v+u+u^2$	$1+u^2$	v	$v+u+u^2$	u^2	$1+v+u^2$	$v+u^2$
$1+u^2$	$1+u^2$	u^2	$1+v+u^2$	$1+u+u^2$	1	$v+u^2$	$u+u^2$	0	$1+v+u+u^2$	$1+v$	$1+u$	$v+u+u^2$	v	u	$1+v+u$	$v+u$
$v+u$	$v+u$	$1+v+u$	u	v	$v+u+u^2$	$1+u$	$1+v$	$1+v+u+u^2$	0	$u+u^2$	$v+u^2$	1	$1+u+u^2$	$1+v+u^2$	u^2	$1+u^2$
$v+u^2$	$v+u^2$	$1+v+u^2$	u^2	$v+u+u^2$	v	$1+u^2$	$1+v+u+u^2$	$1+v$	$u+u^2$	0	$v+u$	$1+u+u^2$	1	$1+v+u$	u	$1+u$
$u+u^2$	$u+u^2$	$1+u+u^2$	$v+u+u^2$	u^2	u	$1+v+u+u^2$	$1+u^2$	$1+u$	$v+u^2$	$v+u$	0	$1+v+u^2$	$1+v+u$	1	v	$1+v$
$1+v+u$	$1+v+u$	$v+u$	$1+u$	$1+v$	$1+v+u+u^2$	u	v	$v+u+u^2$	1	$1+u+u^2$	$1+v+u^2$	0	$u+u^2$	$v+u^2$	$1+u^2$	u^2
$1+v+u^2$	$1+v+u^2$	$v+u^2$	$1+u^2$	$1+v+u+u^2$	$1+v$	u^2	$v+u+u^2$	v	$1+u+u^2$	1	$1+v+u$	$u+u^2$	0	$v+u$	$1+u$	u
$1+u+u^2$	$1+u+u^2$	$u+u^2$	$1+v+u+u^2$	$1+u^2$	$1+u$	$v+u+u^2$	u^2	u	$1+v+u^2$	$1+v+u$	1	$v+u^2$	$v+u$	0	$1+v$	v
$v+u+u^2$	$v+u+u^2$	$1+v+u+u^2$	$u+u^2$	$v+u^2$	$v+u$	$1+u+u^2$	$1+v+u^2$	$1+v+u$	u^2	u	v	$1+u^2$	$1+u$	$1+v$	0	1
$1+v+u+u^2$	$1+v+u+u^2$	$v+u+u^2$	$1+u+u^2$	$1+v+u^2$	$1+v+u$	$u+u^2$	$v+u^2$	$v+u$	$1+u^2$	$1+u$	$1+v$	u^2	u	v	1	0

$\otimes$	0	1	v	u	u^2	$1+v$	$1+u$	$1+u^2$	$v+u$	$v+u^2$	$u+u^2$	$1+v+u$	$1+v+u^2$	$1+u+u^2$	$v+u+u^2$	$1+v+u+u^2$
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	v	u	u^2	$1+v$	$1+u$	$1+u^2$	$v+u$	$v+u^2$	$u+u^2$	$1+v+u$	$1+v+u^2$	$1+u+u^2$	$v+u+u^2$	$1+v+u+u^2$
v	0	v	0	0	0	v	v	v	0	0	0	v	v	v	0	v
u	0	u	0	u^2	0	u	$u+u^2$	u	u^2	0	u^2	$u+u^2$	u	$u+u^2$	u^2	$u+u^2$
u^2	0	u^2	0	0	0	u^2	u^2	u^2	0	0	0	u^2	u^2	u^2	0	u^2
$1+v$	0	$1+v$	v	u	u^2	1	$1+v+u$	$1+v+u^2$	$v+u$	$v+u^2$	$u+u^2$	$1+u$	$1+u^2$	$1+v+u+u^2$	$v+u+u^2$	$1+u+u^2$
$1+u$	0	$1+u$	v	$u+u^2$	u^2	$1+v+u$	$1+u^2$	$1+u+u^2$	$v+u+u^2$	$v+u^2$	u	$1+v+u^2$	$1+v+u+u^2$	1	$v+u$	$1+v$
$1+u^2$	0	$1+u^2$	v	u	u^2	$1+v+u^2$	$1+u+u^2$	1	$v+u$	$v+u^2$	$u+u^2$	$1+v+u+u^2$	$1+v$	$1+u$	$v+u+u^2$	$1+v+u$
$v+u$	0	$v+u$	0	u^2	0	$v+u$	$v+u+u^2$	$v+u$	u^2	0	u^2	$v+u+u^2$	$v+u$	$v+u+u^2$	u^2	$v+u+u^2$
$v+u^2$	0	$v+u^2$	0	0	0	$v+u^2$	$v+u^2$	$v+u^2$	0	0	0	$v+u^2$	$v+u^2$	$v+u^2$	0	$v+u^2$
$u+u^2$	0	$u+u^2$	0	u^2	0	$u+u^2$	u	$u+u^2$	u^2	0	u^2	u	$u+u^2$	u	u^2	u
$1+v+u$	0	$1+v+u$	v	$u+u^2$	u^2	$1+u$	$1+v+u^2$	$1+v+u+u^2$	$v+u+u^2$	$v+u^2$	u	$1+u^2$	$1+u+u^2$	$1+v$	$v+u$	1
$1+v+u^2$	0	$1+v+u^2$	v	u	u^2	$1+u^2$	$1+v+u+u^2$	$1+v$	$v+u$	$v+u^2$	$u+u^2$	$1+u+u^2$	1	$1+v+u$	$v+u+u^2$	$1+u$
$1+u+u^2$	0	$1+u+u^2$	v	$u+u^2$	u^2	$1+v+u+u^2$	1	$1+u$	$v+u+u^2$	$v+u^2$	u	$1+v$	$1+v+u$	$1+u^2$	$v+u$	$1+v+u^2$
$v+u+u^2$	0	$v+u+u^2$	0	u^2	0	$v+u+u^2$	$v+u$	$v+u+u^2$	u^2	0	u^2	$v+u$	$v+u+u^2$	$v+u$	u^2	$v+u$
$1+v+u+u^2$	0	$1+v+u+u^2$	v	$u+u^2$	u^2	$1+u+u^2$	$1+v$	$1+v+u$	$v+u+u^2$	$v+u^2$	u	1	$1+u$	$1+v+u^2$	$v+u$	$1+u^2$

4.1.1. TANIM : $R=\mathbb{F}_2+v\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2$ ve $R_1=\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2$ olmak üzere;

$$\Phi : R \longrightarrow R_1^2$$
$$a+bv+cu+du^2 \mapsto \Phi\ (a+bv+cu+du^2)=\Phi(r+qv)=(q,q+r)$$

biçiminde tanımlanan dönüşüme R halkası üzerindeki Gray dönüşümü denir. Burada $r=a+cu+du^2$ $q=b+au+(a+c)u^2$, $a,b,c\in\mathbb{F}_2$ dır.

Φ dönüşümünü, $\Phi\ (t_o,t_1,...,t_{n-1})=(q_0,q_1,...,q_{n-1},q_0+r_0,q_1+r_1,...,q_{n-1}+r_{n-1})$ biçiminde R^n e genişletilebilir.

Burada $i=0,1,...,n-1$ için $t_i=r_i+q_iv$, $r_i=a_i+c_iu+d_iu^2$, $q_i=b_i+a_iu+(a_i+c_i)u^2$ biçimindedir.

4.1.2. TANIM : $R_1=\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2$, $x,y,z\in\mathbb{F}_2$ olmak üzere;

$$\Phi_1 : R_1 \longrightarrow \mathbb{F}_2^4$$
$$x+yu+zu^2 \mapsto \Phi_1(x+yu+zu^2)=(z,x+z,y+z,x+y+z)$$

biçiminde tanımlanan dönüşüme R_1 halkası üzerindeki Gray dönüşümü denir.

Φ_1 dönüşümünü, R_1^n e aşağıdaki biçimde genişletilebilir.

$$\Phi_1 : R_1^n \longrightarrow \mathbb{F}_2^{4n}$$
$$\begin{aligned}(b_o,b_1,...,b_{n-1}) \mapsto \Phi(b_o,b_1,...,b_{n-1}) =(&z_o,z_1,...,z_{n-1},x_0+z_o,x_1+z_1,...,\\ &x_{n-1}+z_{n-1},y_0+z_o,y_1+z_1,...,\\ &y_{n-1}+z_{n-1},x_o+y_0+z_o,x_1+y_1+z_1,\\ &...,x_{n-1}+y_{n-1}+z_{n-1})\end{aligned}$$

Burada $i=0,1,...,n-1$ için $b_i=x_i+y_iu+z_iu^2$, $x_i,\ y_i,\ z_i\in\mathbb{F}_2$ biçimindedir.

4.1.3. TANIM : $R=\mathbb{F}_2+v\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2$ halkası üzerinde;

her $s\in R$ için $w_R(s)=\begin{cases}0 & , s=0\\ 2 & , s=1+v+u\\ 6 & , s=u,u+u^2,1+v+u+u^2\\ 4 & , \textit{diğer durumlar}\end{cases}$

biçiminde tanımlanan fonksiyon R üzerinde bir ağırlık fonksiyonu olarak adlandırılır.

Bu durumda her $s=(s_o,s_1,...,s_{n-1})\in R^n$ için $w_R(s)=\sum_{i=0}^{n-1}w_R(s_i)$ dir.

4.1.4. TANIM : $R_1 = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$ halkası üzerinde;

her $t \in R_1$ için $w_L(t) = \begin{cases} 0 & ; \ t = 0 \\ 4 & ; \ t = u^2 \\ 2 & ; \ diğer\ durumlar \end{cases}$

biçiminde tanımlanan fonksiyona, R_1 üzerinde Lee ağırlık fonksiyonu denir.

Bu durumda her $t = (t_o, t_1, ..., t_{n-1}) \in R_1^n$ için $w_L(t) = \sum_{i=0}^{n-1} w_L(t_i)$ eşitliği gerçeklenir.

4.1.5. TANIM : $\mathbb{F}_2$ cismi üzerinde;

$w_H(0) = 0, w_H(1) = 1$ biçiminde tanımlanan fonksiyona $\mathbb{F}_2$ üzerinde Hamming ağırlık fonksiyonu denir.

Bu durumda her $c = (c_o, c_1, ..., c_{n-1}) \in \mathbb{F}_2^n$ için $w_H(c) = \sum_{i=0}^{n-1} w_H(c_i)$ olur.

4.1.6. TANIM : Her $x, y \in R^n$, $x \neq y$ için x ve y arasındaki d_R uzaklığı $w_R(x-y)$ olarak tanımlanır. C, R^n üzerinde bir kod olmak üzere, C kodunun minimum uzaklığı her $x, y \in C$, $x \neq y$ için; $d_R(C) = \min\{d_R(x,y)\}$ biçiminde tanımlanır.

R^n üzerinde yazılan 4.1.6. Tanım benzer biçimde R_1^n ve $\mathbb{F}_2^n$ üzerinde de verilir. Burada R_1^n ve $\mathbb{F}_2^n$ üzerinde C kodunun minimum uzaklığı sırasıyla $d_L(C)$ ve $d_H(C)$ ile gösterilir.

4.1.7. ÖNERME : Φ ve Φ_1 dönüşümleri 4.1.1. Tanım ve 4.1.2. Tanımdaki gibi olsun. Φ dönüşümü (R^n, d_R) den (R_1^{2n}, d_L) e, Φ_1 dönüşümü de (R_1^{2n}, d_L) den $(\mathbb{F}_2^{8n}, d_H)$ e birer izometridir. Bunun sonucu olarak $\Phi_1 \circ \Phi$ dönüşümü de (R^n, d_R) den $(\mathbb{F}_2^{8n}, d_H)$ e bir izometridir.

Kanıt : Her $x, y \in R^n$, $x \neq y$ için $x = a + bv + cu + du^2$, $y = a' + b'v + c'u + d'u^2$ $a, a', b, b', c, c', d, d' \in \mathbb{F}_2^n$ olsun. $r = a + cu + du^2 \in R_1^n$, $q = b + au + (a+c)u^2 \in R_1^n$, $r' = a' + c'u + d'u^2 \in R_1^n$, $q' = b' + a'u + (a'+c')u^2 \in R_1^n$ olarak alındığında $x = a + bv + cu + du^2 = r + qv$ ve $y = a' + b'v + c'u + d'u^2 = r' + q'v$ biçiminde yazılır.

$$
\begin{aligned}
d_R(x,y) &= w_R(x-y) \\
&= w_R((a+bv+cu+du^2)-(a'+b'v+c'u+d'u^2)) \\
&= w_R((r+vq)-(r'+vq')) \\
&= w_R((r-r')+v(q-q')) \\
&= w_L((q-q'),(q-q')+(r-r')) \\
&= w_L((b+au+(a+c)u^2)-(b'+a'u+(a'+c')u^2)) \\
&= w_L((b+au+(a+c)u^2)-(b'+a'u+(a'+c')u^2), \\
&\qquad (b+au+(a+c)u^2)-(b'+a'u+(a'+c')u^2)+(a+cu+du^2)-(a'+c'u+d'u^2)) \\
&= w_L((b-b')+(a-a')u+(a-a'+c-c')u^2,(a-a'+b-b') \\
&\qquad +(a-a'+c-c')u-(a-a'+c-c'+d-d')u^2) \\
&= w_H(a-a'+c-c',a-a'+c-c'+d-d',a-a'+b-b'+c-c', \\
&\quad b-b'+c-c'+d-d',c-c',d-d',b-b'+c-c',a-a'+b-b'+d-d')
\end{aligned}
$$

elde edilir. Buradan $s \in R^n$ için $w_R(s) = w_L(\Phi(s)) = w_H(\Phi_1(\Phi(s)))$ eşitliği görülür. Dolayısıyla $d_R(x,y) = d_L(\Phi(x),\Phi(y)) = d_H((\Phi_1 \circ \Phi)(x),(\Phi_1 \circ \Phi)(y))$ olur.

4.1.8. TANIM : C, $R = \mathbb{F}_2 + v\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$ halkası üzerinde n uzunluğunda bir lineer kod olsun.

$$\sigma : R^n \longrightarrow R^n$$

$$(c_o, c_1, ..., c_{n-1}) \mapsto \sigma(c_o, c_1, ..., c_{n-1}) = (c_{n-1}, c_0, ..., c_{n-2})$$

permütasyonu için $\sigma(C) = C$ koşulu sağlanıyorsa, C koduna R üzerinde bir cyclic kod denir.

4.1.9. TANIM : C, $R = \mathbb{F}_2 + v\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$ halkası üzerinde n uzunluğunda bir lineer kod olsun.

$$\gamma : R^n \longrightarrow R^n$$

$$(c_o, c_1, ..., c_{n-1}) \mapsto \gamma(c_o, c_1, ..., c_{n-1}) = ((1+v).c_{n-1}, c_0, ..., c_{n-2})$$

permütasyonu için $\gamma(C) = C$ koşulu sağlanıyorsa C koduna R üzerinde bir $(1+v)-$constacyclic kod adı verilir.

C, R halkası üzerinde bir kod olmak üzere, n uzunlugundaki bir $c=(c_o,c_1,...,c_{n-1})$ kod sözcüğü $R[x]$ halkası üzerinde $c(x)=\sum_{i=0}^{n-1} c_i.x^i$ biçimde gösterilebilir. Bu notasyon R_1 halkası ve $\mathbb{F}_2$ cismi üzerinde de benzer biçimde kullanılabilir.

4.1.10. ÖNERME : C, R halkası üzerinde n uzunluğunda bir lineer kod olmak üzere, bu kodun polinom gösterimi $P(C)=\{\sum_{i=0}^{n-1} r_i.x^i \mid (r_0,r_1,...,r_{n-1})\in C\}$ biçimindedir. Buradan;

i) C nin R halkası üzerinde bir cyclic kod olması için gerekli ve yeterli koşul $P(C)$ nin $R[x]/\langle x^n-1\rangle$ in bir ideali olmasıdır.

ii) C nin R halkası üzerinde bir $(1+v)-$constacyclic kod olması için gerekli ve yeterli koşul $P(C)$ nin $R[x]/\langle x^n-(1+v)\rangle$ in bir ideali olmasıdır.

Kanıt : Bu önermenin kanıtı halka olarak $R=\mathbb{F}_2+v\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2$ alınarak [11] de yapılan kanıta benzer biçimde görülür.

4.1.11. TANIM : D, R_1 halkası üzerinde $2n$ uzunluğunda bir lineer kod olsun.

$$\tau : R_1^{2n} \longrightarrow R_1^{2n}$$

$$(d_o,d_1,...,d_{2n-1}) \mapsto \tau(d_o,d_1,...,d_{2n-1})=(d_{2n-1},d_0,...,d_{2n-2})$$

permütasyonu için $\tau(D)=D$ koşulu sağlanıyorsa, D koduna R_1 üzerinde bir cyclic kod denir.

4.1.12. TANIM : D, R_1 halkası üzerinde $2n$ uzunluğunda bir lineer kod olsun.

$$\upsilon : R_1^{2n} \longrightarrow R_1^{2n}$$

$$(d_o,d_1,...,d_{2n-1}) \mapsto \upsilon(d_o,d_1,...,d_{2n-1})=((1+u^2).d_{2n-1},d_0,...,d_{2n-2})$$

permütasyonu için $\upsilon(D)=D$ koşulu sağlanıyorsa D koduna R_1 üzerinde bir $(1+u^2)-$constacyclic kod denir.

4.1.13. ÖNERME ([7]) : D, R_1 halkası üzerinde $2n$ uzunluğunda bir lineer kod olmak üzere, bu kodun polinom gösterimi $P_1(D) = \{ \sum_{i=0}^{2n-1} s_i.x^i \mid (s_0, s_1, ..., s_{2n-1}) \in D \}$ dir. Buradan;

i) D nin R_1 halkası üzerinde bir cyclic kod olması için gerekli ve yeterli koşul $P_1(D)$ nin $R_1[x] \big/ \langle x^n - 1 \rangle$ in bir ideali olmasıdır.

ii) D nin R_1 halkası üzerinde bir $(1+u^2)-$constacyclic kod olması için gerekli ve yeterli koşul $P_1(D)$ nin $R_1[x] \big/ \langle x^n - (1+v) \rangle$ nin bir ideali olmasıdır.

4.1.14. TANIM : C', $\mathbb{F}_2$ cismi üzerinde $8n$ uzunluğunda bir lineer kod olsun.

$$\sigma^{\otimes 2} : \mathbb{F}_2^{8n} \longrightarrow \mathbb{F}_2^{8n}$$

$$(d_o, d_1, ..., d_{8n-1}) \mapsto \sigma^{\otimes 2}(d_o, d_1, ..., d_{8n-1}) = (d_{4n-1}, d_0, ..., d_{4n-2}, d_{8n-1}, d_{4n}, ..., d_{8n-2})$$

permütasyonu için $\sigma^{\otimes 2}(C') = C'$ koşulu sağlanıyorsa C' koduna $\mathbb{F}_2$ üzerinde 2.mertebeden bir quasi-cyclic kod denir.

n bir tek sayı olduğunda $(1+v)^n = (1+v)$ ve n bir çift sayı olduğunda $(1+v)^n = 1$ olduğundan bu bölümde 4.2. başlığına kadar n bir tek doğal sayı olarak alınacaktır.

4.1.15. ÖNERME : $\mu : R[x] \big/ \langle x^n - 1 \rangle \longrightarrow R[x] \big/ \langle x^n - (1+v) \rangle$

$$r(x) \mapsto r((1+v).x)$$

dönüşümü tanımlansın. n tek doğal sayı olduğunda μ dönüşümü bir halka izomorfizmasıdır.

Kanıt: n bir tek sayı ise $(1+v)^n = (1+v)$ olduğunu biliniyor. $a(x) \equiv b(x) \pmod{x^n - 1}$ olsun. Buradan $a(x) - b(x) = (x^n - 1).q(x)$, $q(x) \in R[x]$ dir ve x yerine $(1+v).x$ yazıldığında aşağıdaki eşitlik elde edilir.

$$a((1+v).x) - b((1+v).x) = ((1+v)^n.x^n - 1).q((1+v).x), \; q((1+v).x) \in R[x]$$

$$= ((1+v).x^n - 1).q((1+v).x)$$

$$= ((1+v).x^n - (1+v)^2).q((1+v).x)$$

$$= (1+v).(x^n - (1+v)).q((1+v).x)$$

$$= (x^n - (1+v)).q((1+v).x).(1+v)$$

$$= (x^n - (1+v)).p(x)\ ,\ p(x) \in R[x].$$

Böylece $a((1+v).x) = b((1+v).x) \pmod{(x^n - (1+v))}$ olduğu görülür.

Bu durum da aşağıdaki sonuç elde edilir.

4.1.16. SONUÇ : I nın $R[x] \big/ \langle x^n - 1 \rangle$ nin bir ideali olması için gerekli ve yeterli koşul $\mu(I)$ nın $R[x] \big/ \langle x^n - (1+v) \rangle$ nin bir ideali olmasıdır.

Kanıt : Bu sonucun kanıtı için [6] da halka $R = \mathbb{F}_2 + v\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$ alındığında kanıt açık bir biçimde görülür.

4.1.17. TEOREM : $\bar{\mu} : R^n \to R^n$

$$(r_o, r_1, ..., r_{n-1}) \mapsto (r_o, (1+v).r_1, ..., (1+v)^i.r_i, (1+v)^{n-1} r_{n-1})$$

dönüşümü verilsin. C nin R üzerinde n uzunluğunda bir cyclic kod olması için gerekli yeterli koşul $\bar{\mu}(C)$ nin R üzerinde n uzunluğunda bir $(1+v)-$constacyclic kod olmasıdır.

Kanıt : Bu teoremin kanıtı için [6] da halka olarak $R = \mathbb{F}_2 + v\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$ alındığında kanıtı kolayca görülür.

Aşağıda, R halkası üzerindeki $(1+v)-$constacyclic kodların Gray görüntülerinin R_1 halkası üzerinde çift uzunluklu kodlar olduğu gösterilmiştir

4.1.18. ÖNERME : γ dönüşümü R^n üzerinde bir permütasyon, τ dönüşümü R_1^{2n} üzerinde bir permütasyon ve Φ, R^n den R_1^{2n} e yukarıda tanımlanan Gray dönüşümünü ise $\Phi \circ \gamma = \tau \circ \Phi$ eşitliği sağlanır.

Kanıt: Her $0 \le i \le n-1$ için $c_i = r_i + q_i v$ olmak üzere $c = (c_0, c_1, ..., c_{n-1}) \in R^n$ olsun. Bu durumda $c \in R^n$ in Gray görüntüsünü

$$\Phi(c) = \Phi(c_0, c_1, ..., c_{n-1}) = \Phi(r_0 + q_0 v, r_1 + q_1 v, ..., r_{n-1} + q_{n-1} v)$$

$$= (q_0, q_1, ..., q_{n-1}, q_0 + r_0, q_1 + r_1, ..., q_{n-1} + r_{n-1})$$

olarak bulunur. Buradan $\tau(\Phi(c)) = \tau(q_0, q_1, ..., q_{n-1}, q_0 + r_0, q_1 + r_1, ..., q_{n-1} + r_{n-1})$

$$= (q_{n-1} + r_{n-1}, q_0, q_1, ..., q_{n-1}, q_0 + r_0, ..., q_{n-2} + r_{n-2})$$

elde edilir. Diğer taraftan,

$\gamma(c) = \gamma(c_0, c_1, ..., c_{n-1}) = ((1+v).c_{n-1}, c_0, ..., c_{n-2})$ dir. $(1+v).c_{n-1} = r_{n-1} + (q_{n-1} + r_{n-1})v$ olduğundan

$$\Phi(\gamma(c)) = \Phi(r_{n-1} + (q_{n-1} + r_{n-1})v, r_0 + q_0 v, q_1, ..., r_{n-2} + q_{n-2}v)$$
$$= (q_{n-1} + r_{n-1}, q_0, q_1, ..., q_{n-1}, q_0 + r_0, ..., q_{n-2} + r_{n-2})$$

elde edilir.

4.1.19. TEOREM : C kodunun R halkası üzerinde n uzunluğunda bir $(1+v)-$constacyclic kod olması için gerekli ve yeterli koşul $\Phi(C)$ nin R_1 halkası üzerinde $2n$ uzunluğunda bir cyclic kod olmasıdır.

Kanıt : C, R halkası üzerinde bir $(1+v)-$constacyclic kod olsun. Bu durumda $\gamma(C) = C$ olur. Eşitliğin her iki tarafının Φ görüntüsü alındığında $\Phi(\gamma(C)) = \Phi(C)$ elde edilir. 4.1.18. Önermeden $\tau(\Phi(C)) = \Phi(\gamma(C)) = \Phi(C)$ bulunur. Böylece $\Phi(C)$ nin cyclic kod olduğu görülür. Tersine $\Phi(C)$ cyclic kod olsun. Bu durumda $\tau(\Phi(C)) = \Phi(C)$ elde edilir. 4.1.18. Önermeden $\tau(\Phi(C)) = \Phi(\gamma(C)) = \Phi(C)$ bulunur. Φ bire-bir fonksiyon olduğundan $\gamma(C) = C$ olur. Öyleyse C bir $(1+v)-$constacyclic koddur.

4.1.20. ÖNERME : υ dönüşümü R_1^{2n} üzerinde bir permütasyon, $\sigma^{\otimes 2}$ dönüşümü $\mathbb{F}_2^{8n}$ üzerinde bir permütasyon ve Φ_1, R_1^{2n} den $\mathbb{F}_2^{8n}$ e yukarıda tanımlanan Gray dönüşümü ise $\sigma^{\otimes 2} \circ \Phi_1 = \Phi_1 \circ \upsilon$ eşitliği sağlanır.

Kanıt : Her $0 \le i \le n-1$ için $t_i = x_i + y_i u + z_i u^2$ olmak üzere $t = (t_0, t_1, ..., t_{n-1}) \in R_1^{2n}$ olsun.

$\upsilon(t) = \upsilon(t_0, t_1, ..., t_{2n-1}) = ((1+u^2).t_{2n-1}, t_0, ..., t_{2n-2})$ dir.

Burada $(1+u^2).t_{2n-1}$ bileşeni düzenlendiğinde

$(1+u^2).t_{2n-1} = (1+u^2).(x_{2n-1} + y_{2n-1}u + z_{2n-1}u^2) = x_{2n-1} + y_{2n-1}u + (x_{2n-1} + z_{2n-1})u^2$ bulunur.

Gray görüntüsü alınarak

$$\Phi_1(\nu(t)) = \Phi_1((1+u^2).t_{2n-1}, t_0, ..., t_{2n-2})$$
$$= \Phi_1(x_{2n-1} + y_{2n-1}u + (x_{2n-1} + z_{2n-1})u^2, x_0 + y_0 u + z_0 u^2, ..., x_{2n-2} + y_{2n-2}u + z_{2n-2}u^2)$$

$$= (x_{2n-1} + z_{2n-1}, z_0, z_1, ..., z_{2n-1}, x_0 + z_0, , ..., x_{2n-2} + z_{2n-2}, x_{2n-1} + y_{2n-1} + z_{2n-1}, y_0 + z_0, ...,$$
$$y_{2n-1} + z_{2n-1}, x_0 + y_0 + z_0, ..., x_{2n-2} + y_{2n-2} + z_{2n-2}).$$

elde edilir. Diğer taraftan

$$\Phi_1(t) = \Phi_1(t_0, t_1, ..., t_{2n-1}) = (z_0, z_1, ..., z_{2n-1}, x_0 + z_0, , ..., x_{2n-1} + z_{2n-1}, y_0 + z_0, ...,$$
$$y_{2n-1} + z_{2n-1}, x_0 + y_0 + z_0, ..., x_{2n-1} + y_{2n-1} + z_{2n-1})$$

olur. Buradan

$$\sigma^{\otimes 2}.\Phi_1(t) = \sigma^{\otimes 2}(t_0, t_1, ..., t_{2n-1}) = (z_0, z_1, ..., z_{2n-1}, x_0 + z_0, , ..., x_{2n-1} + z_{2n-1}, y_0 + z_0, ...,$$
$$y_{2n-1} + z_{2n-1}, x_0 + y_0 + z_0, ..., x_{2n-1} + y_{2n-1} + z_{2n-1})$$
$$= (x_{2n-1} + z_{2n-1}, z_0, z_1, ..., z_{2n-1}, x_0 + z_0, , ...,$$
$$x_{2n-2} + z_{2n-2}, x_{2n-1} + y_{2n-1} + z_{2n-1}, y_0 + z_0, ...,$$
$$y_{2n-1} + z_{2n-1}, x_0 + y_0 + z_0, ..., x_{2n-2} + y_{2n-2} + z_{2n-2})$$

elde edilir.

4.1.21. TEOREM : C nin R_1 halkası üzerinde $2n$ uzunluğunda bir $(1+u^2)-$constacyclic kod olması için gerekli ve yeterli koşul $\Phi_1(C)$ nin $\mathbb{F}_2$ cismi üzerinde $8n$ uzunluğunda 2. mertebeden bir quasi-cyclic kod olmasıdır.

Kanıt : C bir $(1+u^2)-$constacyclic kod ise $\upsilon(C) = C$ dir. Eşitliğin her iki tarafının Φ görüntüsü alındığında $\Phi_1(\upsilon(C)) = \Phi_1(C)$ elde edilir. 4.1.20. Önermeden $\sigma^{\otimes 2}(\Phi_1(C)) = \Phi_1(\upsilon(C)) = \Phi_1(C)$ bulunur. Böylece $\Phi_1(C)$ nin, 2. mertebeden bir quasi-cyclic kod olduğu görülür. Tersine $\Phi_1(C)$, 2. mertebeden bir quasi-cyclic kod ise $\sigma^{\otimes 2}(\Phi_1(C)) = \Phi_1(C)$ sağlanır. 4.1.20. Önermeden $\sigma^{\otimes 2}(\Phi_1(C)) = \Phi_1(\upsilon(C)) = \Phi_1(C)$ bulunur. Φ bire-bir bir fonksiyon olduğundan $\upsilon(C) = C$ olur. Dolayısıyla C nin bir $(1+u^2)-$constacyclic kod olduğu görülür.

4.1.22. SONUÇ : C nin R halkası üzerinde n uzunluğunda bir $(1+v)-$constacyclic kod olması için gerekli ve yeterli koşul $\Phi_1(\Phi(C))$ nin $\mathbb{F}_2$ cismi üzerinde $8n$ uzunluğunda, 2. mertebeden bir quasi-cyclic kod olmasıdır.

Kanıt : C kodunun önce Φ görüntüsü sonra Φ_1 görüntüsü alındığında 4.1.19. Teorem ve 4.1.21. Teoremleri ile kolayca görülür.

4.2. $\mathbb{F}_p[u,v]/_{<u^3,\ v^2,uv>}$ Halkası Üzerindeki Cyclic Kodlar

Bu bölümde $p>3$ bir asal sayı olmak üzere $\mathbb{F}_p[u,v]/_{<u^3,\ v^2,u.v>}$ halkası üzerinde çalışılmıştır. Bu alt bölümde verilen tanımlar 4.1. bölümdeki tanımlar ile isim olarak benzerlik gösterse de her alt bölümdeki tanımlar ilgili kısımla sınırlıdır. Burada, söz konusu $\mathbb{F}_p[u,v]/_{<u^3,\ v^2,u.v>}$ halkası $u^3=0, v^2=0$ ve $u.v=v.u=0$ koşulları altında eleman sayısı p^4 olan $\mathbb{F}_p+v\mathbb{F}_p+u\mathbb{F}_p+u^2\mathbb{F}_p$ halkasına izomorftur.

4.2. bölümde $u^3=0, v^2=0$ ve $u.v=v.u=0$ koşulları ile $\mathbb{F}_p[u,v]/_{<u^3,\ v^2,u.v>}$ halkasının yapısı incelenmiş bu halka üzerinde ağırlık fonksiyonu tanımlanmıştır. Böylece bu halka üzerinde lineer kodların yazılabildiği gösterilmiştir. Bu halka üzerinde tanımlanan bir cyclic kodun Gray görüntüsünün $\mathbb{F}_p+v\mathbb{F}_p$ halkası üzerinde 2. mertebeden quasi-cyclic kod olduğu gösterilmiştir. $\mathbb{F}_p+v\mathbb{F}_p$ halkası üzerinden $\mathbb{F}_p$ cismine bir başka Gray dönüşümü daha tanımlanmıştır. Böylece yeni tanımlanan $\mathbb{F}_p+v\mathbb{F}_p+u\mathbb{F}_p+u^2\mathbb{F}_p$ halkası üzerindeki cyclic kodlar ile $\mathbb{F}_p$ cismi üzerinde quasi-cyclic kodlar arasındaki ilişki elde edilmiştir. Bu alt bölümde $u^3=0, v^2=0$ ve $u.v=v.u=0$ koşulları ile $\mathbb{F}_p+v\mathbb{F}_p+u\mathbb{F}_p+u^2\mathbb{F}_p$ halkası R ve $u^3=0$ koşulu ile $\mathbb{F}_p+u\mathbb{F}_p+u^2\mathbb{F}_p$ halkası S ile gösterilecektir. $\mathbb{F}_p+v\mathbb{F}_p+u\mathbb{F}_p+u^2\mathbb{F}_p$ halkası üzerinde yazılan ağırlık fonksiyonu ve Gray dönüşümü tarafımızca tanımlanmıştır.

4.2.1. TANIM : $\mathbb{F}_p$ cismi üzerinde;

Her $c\in\mathbb{F}_p$ için $w_H(c)=\begin{cases}0\ , c=0\\ 1\ , c\neq 0\end{cases}$ biçiminde tanımlanan fonksiyona $\mathbb{F}_p$ cismi üzerinde Hamming ağırlık fonksiyonu denir.

Bu durumda her $c=(c_o,c_1,...,c_{n-1})\in\mathbb{F}_p^n$ için $w_H(c)=\sum_{i=0}^{n-1}w_H(c_i)$ dir.

4.2.2. TANIM : $S = \mathbb{F}_p + u\mathbb{F}_p + u^2\mathbb{F}_p$ halkası üzerinde;

her $s \in S$ için $w_{\text{hom}}(s) = \begin{cases} p^2 - p & , \ s \in S - S.u^2 \\ p^2 & , \ s \in S.u^2 - \{0\} \\ 0 & , \ s = 0 \end{cases}$

biçiminde tanımlanan fonksiyona S üzerinde homogeneous ağırlık fonksiyonu denir.

Bu durumda her $s = (s_0, s_1, ..., s_{n-1}) \in S^n$ için $w_{\text{hom}}(s) = \sum_{i=0}^{n-1} w_{\text{hom}}(s_i)$ dir.

4.2.3. TANIM : $R = \mathbb{F}_p + v\mathbb{F}_p + u\mathbb{F}_p + u^2\mathbb{F}_p$ halkası üzerinde;

her $r \in R$ için $w_R(r) = \begin{cases} 0 & , \ r = 0 \\ 2p^2 - 2p & , \ r \in R - S.u \\ 2p^2 - p & , \ r \in S.u - S.u^2 \\ p^2 & , \ r \in S.u^2 - \{0\} \end{cases}$

biçiminde tanımlanan fonksiyon R üzerinde bir ağırlık fonksiyonu olarak tanımlanır.

Dolayısıyla her $r = (r_0, r_1, ..., r_{n-1}) \in R^n$ için $w_R(r) = \sum_{i=0}^{n-1} w_R(r_i)$ dir.

4.2.4. TANIM : Her $x, y \in R^n$, $x \neq y$ için x ve y arasındaki d_R uzaklığı $w_R(x - y)$ olarak tanımlanır. C, R^n üzerinde bir kod olmak üzere, C kodunun minimum uzaklığı her $x, y \in C$, $x \neq y$ için; $d_R(C) = \min\{d_R(x, y)\}$ biçiminde tanımlanır.

R^n üzerinde yazılan 4.2.4. Tanım, benzer biçimde S^n ve $\mathbb{F}_p^n$ üzerinde de verilir. Burada S^n ve $\mathbb{F}_p^n$ üzerinde C kodunun minimum uzaklığı sırasıyla $d_{\text{hom}}(C)$ ve $d_H(C)$ ile gösterilir.

4.2.5. TANIM : $R = \mathbb{F}_p + v\mathbb{F}_p + u\mathbb{F}_p + u^2\mathbb{F}_p$ ve $S = \mathbb{F}_p + u\mathbb{F}_p + u^2\mathbb{F}_p$ olmak üzere;

$$\varphi_1 : R \longrightarrow S^2$$

$$a + bv + cu + du^2 \mapsto \varphi_1(a + bv + cu + du^2)$$

$$\varphi_1(a + bv + cu + du^2) = \varphi_1(r + qv) = ((p-1).q, q + (p-1).r)$$

$$= ((p-1).b + (p-1).au + ((p-1).a + (p-1).c)u^2,$$
$$(b + (p-1).a) + (a + (p-1).c)u + (a + c + (p-1).d)u^2)$$

biçiminde tanımlanan dönüşüme R üzerindeki Gray dönüşümü denir. Burada $r = a + cu + du^2$ ve $q = b + au + (a+c)u^2$ $a,b,c,d \in \mathbb{F}_p$ dır.

φ_1 dönüşümünü

$$\varphi_1(t_0, t_1, ..., t_{n-1}) = ((p-1)q_0, (p-1)q_1, ..., (p-1)q_{n-1}, q_0 + (p-1)r_0, \\ q_1 + (p-1)r_1, ..., q_{n-1} + (p-1)r_{n-1})$$

biçiminde R^n e genişletilebilir.

Burada $i = 0,1,...,n-1$ için $t_i = r_i + q_i v$ olmak üzere $r_i = a_i + c_i u + d_i u^2$, $q_i = b_i + a_i u + (a_i + c_i)u^2$ biçimindedir.

4.2.6. TANIM : $S = \mathbb{F}_p + u\mathbb{F}_p + u^2\mathbb{F}_p$, $x, y, z \in \mathbb{F}_p$ olmak üzere;

$$\varphi_2 : S \longrightarrow \mathbb{F}_p^{p^2}$$
$$x + yu + zu^2 \mapsto \varphi_2(x + yu + zu^2)$$

biçiminde tanımlanan dönüşüme S halkası üzerindeki Gray dönüşümü denir. Burada her $i = 0,1,..., p-1$ için $m_i \in \mathbb{F}_p^p$ olmak üzere $\varphi_2(x + yu + zu^2) = (m_0 \,|\, m_1 \,|\, ... \,|\, m_{p-1})$ yazılır. Buradan $m_0 = (z, y+z, 2y+z, ..., (p-1)y + z)$,

$m_1 = (x+z, x+y+z, ..., x+(p-1)y+z), \ldots,$

$m_{p-1} = ((p-1)x+z, (p-1)x+y+z, ..., (p-1)x+(p-1)y+z)$.

biçimindedir. φ_2 dönüşümü uygun biçimde S^n e genişletilebilir.

4.2.7. ÖNERME : φ_1 ve φ_2 dönüşümleri 4.2.5. Tanım ve 4.2.6. Tanım daki gibi olsun. φ_1 dönüşümü (R^n, d_R) den (S^{2n}, d_{hom}) ye φ_2 dönüşümü de (S^{2n}, d_{hom}) den $(\mathbb{F}_p^{p^2 \cdot n}, d_H)$ ye birer izometridir. Bunun sonucu olarak $\varphi_2 \circ \varphi_1$ dönüşümü de (R^n, d_R) den $(\mathbb{F}_p^{p^2 \cdot n}, d_H)$ ye bir izometridir.

Kanıt: Her $x, y \in R^n$, $x \neq y$ alınsın.

$$d_R(x,y) = w_R(x-y) = w_L(\varphi_1(x-y)) \\ = w_L(\varphi_1(x) - \varphi_1(y))) \\ = d_L(\varphi_1(x), \varphi_1(y)) \\ = w_H(\varphi_2(\varphi_1(x) - \varphi_1(y)))$$

$$= w_H(\varphi_2(\varphi_1(x-y)))$$
$$= w_H((\varphi_2 \circ \varphi_1)(x-y))$$
$$= w_H((\varphi_2 \circ \varphi_1)(x) - (\varphi_2 \circ \varphi_1)(y))$$
$$= d_H((\varphi_2 \circ \varphi_1)(x), (\varphi_2 \circ \varphi_1)(y))$$

elde edilir.

4.2.8. TANIM : C, R halkası üzerinde n uzunluğunda bir lineer kod olsun.

$$\sigma : R^n \longrightarrow R^n$$

$$(c_o, c_1, ..., c_{n-1}) \mapsto \sigma(c_o, c_1, ..., c_{n-1}) = (c_{n-1}, c_0, ..., c_{n-2})$$

permütasyonu için $\sigma(C) = C$ koşulu sağlanıyorsa C koduna R üzerinde bir cyclic kod denir. S halkası ve $\mathbb{F}_p$ cismi üzerinde de aynı tanım verilir.

4.2.9. TANIM : C', S halkası üzerinde $2n$ uzunluğunda bir lineer kod olsun. Her $i = 0,1$ ve $a \in S^{2n}$ için $a = (a_0, a_1, ..., a_{2n-1}) = (a^{(0)} \,|\, a^{(1)}), a^{(i)} \in S^n$ olmak üzere

$$\sigma^{\otimes 2} : S^{2n} \longrightarrow S^{2n}$$

$$a \mapsto \sigma^{\otimes 2}(a) = (\sigma(a^{(0)}) \,|\, \sigma(a^{(1)}))$$

biçiminde tanımlanan permütasyonu için $\sigma^{\otimes 2}(C') = C'$ koşulu sağlanıyorsa C' koduna S üzerinde 2. mertebeden bir quasi-cyclic kod denir. Burada σ permütasyonu S^n de tanımlıdır.

4.2.10. TANIM : D, S halkası üzerinde $2n$ uzunluğunda bir lineer kod olsun.

$$\tau : S^{2n} \longrightarrow S^{2n}$$

$$(d_o, d_1, ..., d_{2n-1}) \mapsto \tau(d_o, d_1, ..., d_{2n-1}) = (d_{2n-1}, d_0, ..., d_{2n-2})$$

permütasyonu için $\tau(D) = D$ koşulu sağlanıyorsa D koduna S üzerinde bir cyclic kod adı verilir.

4.2.11. TANIM : $D', \mathbb{F}_p$ cismi üzerinde $2p^2n$ uzunluğunda bir lineer kod olsun. Her $i = 0,1,..., p^2 - 1$, $a \in \mathbb{F}_p^{2p^2n}$ için

$a = (a_0, a_1, ..., a_{2p^2n-1}) = (a^{(0)} \,|\, a^{(1)} \,|\, a^{(2)} \,|\, ... \,|\, a^{(p^2-1)}), a^{(i)} \in \mathbb{F}_p^{2n}$ olmak üzere

$$\sigma^{\otimes p^2} : \mathbb{F}_p^{2p^2n} \longrightarrow \mathbb{F}_p^{2p^2n}$$

$$a \mapsto \sigma^{\otimes p^2}(a) = (\sigma(a^{(0)}) \,|\, \sigma(a^{(1)}) \,|\, \sigma(a^{(2)}) \,|\, ... \,|\, \sigma(a^{(p^2-1)}))$$

biçiminde tanımlanan permütasyonu için $\sigma^{\otimes p^2}(D') = D'$ koşulu sağlanıyorsa D' koduna $\mathbb{F}_p$ üzerinde p^2. mertebeden bir quasi-cyclic kod denir. Burada σ permütasyonu $\mathbb{F}_p^{2n}$ de tanımlıdır.

Aşağıdaki kısımda R halkası üzerindeki bir cyclic kodun S halkası üzerinde 2. mertebeden bir quasi-cyclic kod olduğu gösterilmiştir. Ayrıca S halkası üzerinde çift uzunluklu bir cyclic kodun $\mathbb{F}_p$ cismi üzerinde mertebesi p^2 olan bir quasi-cyclic kod olduğu gösterilmiştir.

4.2.12. ÖNERME : σ dönüşümü R^n üzerinde bir permütasyon, $\sigma^{\otimes 2}$ dönüşümü S^{2n} üzerinde bir permütasyon ve φ_1, R^n den S^{2n} ye yukarıda tanımlanan Gray dönüşümü olsun. Bu durumda $\sigma^{\otimes 2} \circ \varphi_1 = \varphi_1 \circ \sigma$ eşitliği sağlanır.

Kanıt: Her $0 \le i \le n-1$ için $c_i = r_i + q_i v$ olmak üzere $c = (c_0, c_1, ..., c_{n-1}) \in R^n$ olsun. Bu durumda $c \in R^n$ in Gray görüntüsünü

$$\varphi_1(c) = \varphi_1(c_0, c_1, ..., c_{n-1}) = \varphi_1(r_0 + q_0 v, r_1 + q_1 v, ..., r_{n-1} + q_{n-1} v)$$
$$= ((p-1)q_0, (p-1)q_1, ..., (p-1)q_{n-1}, q_0 + (p-1)r_0,$$
$$q_1 + (p-1)r_1, ..., q_{n-1} + (p-1)r_{n-1})$$

olarak bulunur. Buradan

$$\sigma^{\otimes 2}(\varphi_1(c)) = ((p-1)q_{n-1}, (p-1)q_0, ..., (p-1)q_{n-2}, q_{n-1} + (p-1)r_{n-1},$$
$$q_0 + (p-1)r_0, ..., q_{n-2} + (p-1)r_{n-2})$$

elde edilir. Diğer taraftan,

$\sigma(c) = \sigma(c_0, c_1, ..., c_{n-1}) = (c_{n-1}, c_0, ..., c_{n-2})$ dir. Bu ifadenin Gray görüntüsü alındığında

$$\varphi_1(\sigma(c)) = \varphi_1(\sigma(c_0, c_1, ..., c_{n-1})) = \varphi_1(c_{n-1}, c_0, ..., c_{n-2})$$
$$= \varphi_1(r_{n-1} + v q_{n-1}, r_0 + v q_0, ..., r_{n-2} + v q_{n-2})$$
$$= ((p-1)q_{n-1}, (p-1)q_0, ..., (p-1)q_{n-2},$$
$$q_{n-1} + (p-1)r_{n-1}, q_0 + (p-1)r_0, ..., q_{n-2} + (p-1)r_{n-2})$$

elde edilir.

4.2.13. TEOREM : C kodunun R halkası üzerinde n uzunluğunda bir cyclic kod olması için gerekli ve yeterli koşul $\varphi_1(C)$ nin S halkası üzerinde $2n$ uzunluğunda, $2.$mertebeden bir quasi-cyclic kod olmasıdır.

Kanıt : C, R halkası üzerinde bir cyclic kod olsun. Bu durumda $\sigma(C) = C$ olur. Eşitliğin her iki tarafının φ_1 görüntüsü alındığında $\varphi_1(\sigma(C)) = \varphi_1(C)$ elde edilir. 4.2.12. Önermeden $\sigma^{\otimes 2}(\varphi_1(C)) = \varphi_1(\sigma(C)) = \varphi_1(C)$ bulunur. Böylece $\varphi_1(C)$ nin $2.$mertebeden bir quasi-cyclic kod olduğu görülür. Tersine $\varphi_1(C)$ $2.$mertebeden bir quasi-cyclic kod ise $\sigma^{\otimes 2}(\varphi_1(C)) = \varphi_1(C)$ elde edilir. 4.2.12. Önermeden $\sigma^{\otimes 2}(\varphi_1(C)) = \varphi_1(\sigma(C)) = \varphi_1(C)$ bulunur. Böylece φ_1 bire-bir fonksiyon olduğu için $\sigma(C) = C$ olur. O halde C bir cyclic koddur.

4.2.14. ÖNERME : τ dönüşümü S^{2n} üzerinde bir permütasyon, $\sigma^{\otimes p^2}$ dönüşümü $\mathbb{F}_p^{2p^2n}$ üzerinde bir permütasyon ve φ_2, S^{2n} den $\mathbb{F}_p^{2p^2n}$ e yukarıda tanımlanan Gray dönüşümü olsun. Bu durumda $\sigma^{\otimes p^2} \circ \varphi_2 = \varphi_2 \circ \tau$ eşitliği sağlanır.

Kanıt : 4.1.12. Önermenin kanıtı ile benzer biçinde görülür.

4.2.15. TEOREM : D kodunun S halkası üzerinde $2n$ uzunluğunda bir cyclic kod olması için gerekli ve yeterli koşul $\varphi_2(D)$ nin $\mathbb{F}_p$ cismi üzerinde $2p^2n$ uzunluğunda mertebesi p^2 olan bir quasi-cyclic kod olmasıdır.

Kanıt : D bir cyclic kod ise $\tau(D) = D$ dir. Eşitliğin her iki tarafının φ_2 görüntüsü alındığında $\varphi_2(\tau(D)) = \varphi_2(D)$ elde edilir. 4.2.14. Önermeden $\sigma^{\otimes p^2}(\varphi_2(D)) = \varphi_2(\tau(D)) = \varphi_2(D)$ bulunur. Böylece $\varphi_2(D)$ nin, mertebesi p^2 olan bir quasi-cyclic kod olduğu görülür. Tersine $\varphi_2(C)$, mertebesi p^2 olan bir quasi-cyclic kod ise $\sigma^{\otimes p^2}(\varphi_2(D)) = \varphi_2(D)$ sağlanır. 4.2.14. Önermeden

$\sigma^{\otimes p^2}(\varphi_2(D)) = \varphi_2(\tau(D)) = \varphi_2(D)$ bulunur. φ_2 bire-bir bir fonksiyon olduğundan $\tau(D) = D$ olur. Dolayısıyla D nin bir cyclic kod olduğu görülür.

Yukarıdaki teoremler kullanılarak elde edilen temel sonuç aşağıda verilmiştir.

4.2.16. SONUÇ : C nin R halkası üzerinde n uzunluğunda bir cyclic kod olması için gerekli ve yeterli koşul $\varphi_2(\varphi_1(C))$ nin $\mathbb{F}_p$ cismi üzerinde $2p^2n$ uzunluğunda, mertebesi p^2 olan bir quasi-cyclic kod olmasıdır.

Kanıt : C kodunun önce φ_1 altında görüntüsü sonra φ_2 altında görüntüsü alındığında 4.2.13. Teorem ve 4.2.15. Teoremleri ile kanıt kolayca görülür.

4.3. $\mathbb{F}_3[u,v]/_{<u^3,\ v^2,uv>}$ Halkası Üzerindeki Cyclic Kodlar

4.2. bölümünde $\mathbb{F}_p[u,v]/_{<u^3,\ v^2,u.v>}$ halkasının $u^3=0, v^2=0$ ve $u.v=v.u=0$ koşulları ile izomorf olduğu $\mathbb{F}_p+v\mathbb{F}_p+u\mathbb{F}_p+u^2\mathbb{F}_p$ halkası için, özel olarak $p=3$ asal sayısı alınarak çalışılmıştır ([26]). Dolayısı ile $u^3=0, v^2=0$ ve $u.v=v.u=0$ koşulları ile $\mathbb{F}_3[u,v]/_{<u^3,\ v^2,u.v>}$ halkası $\mathbb{F}_p[u,v]/_{<u^3,\ v^2,u.v>}$ halkasının özel bir durumudur. Burada $\mathbb{F}_3[u,v]/_{<u^3,\ v^2,u.v>}$ halkasının $u^3=0, v^2=0$ ve $u.v=v.u=0$ koşulları altında izomorf olduğu $\mathbb{F}_3+v\mathbb{F}_3+u\mathbb{F}_3+u^2\mathbb{F}_3$ halkası R ile gösterilmiştir. $u^3=0$ koşulu ile $\mathbb{F}_3[u]/_{<u^3>}$ halkasına izomorf olan $\mathbb{F}_3+u\mathbb{F}_3+u^2\mathbb{F}_3$ halkası R_1 ile gösterilmiştir.

4.3.1. TANIM : $\mathbb{F}_3$ cismi üzerinde; $w_H(0)=0, w_H(1)=1, w_H(2)=1$ biçiminde tanımlanan w_H fonksiyonuna $\mathbb{F}_3$ cismi üzerinde Hamming ağırlık fonksiyonu denir.

Bu durumda her $c=(c_o,c_1,...,c_{n-1})\in\mathbb{F}_3^n$ için $w_H(c)=\sum_{i=0}^{n-1} w_H(c_i)$ dir.

4.3.2. TANIM : $R_1=\mathbb{F}_3+u\mathbb{F}_3+u^2\mathbb{F}_3$ halkası üzerinde;

her $s\in R_1$ için $w_{\text{hom}}(s)=\begin{cases}6 & , \ s\in R_1-R_1.u^2\\ 9 & , \ s\in R_1.u^2-\{0\}\\ 0 & , \ s=0\end{cases}$

biçiminde tanımlanan fonksiyona R_1 üzerinde homogeneous ağırlık fonksiyonu denir.

Bu durumda her $s=(s_0,s_1,...,s_{n-1})\in R_1$ için $w_{\text{hom}}(s)=\sum_{i=0}^{n-1} w_{\text{hom}}(s_i)$ dir.

4.3.3. TANIM : $R = \mathbb{F}_3 + v\mathbb{F}_3 + u\mathbb{F}_3 + u^2\mathbb{F}_3$ halkası üzerinde;

her $r \in R$ için $w_R(r) = \begin{cases} 12 & , \ r \in R - R_1.u \\ 15 & , \ r \in R_1.u - R_1.u^2 \\ 9 & , \ r \in R_1.u^2 \\ 0 & , \ r = 0 \end{cases}$

biçiminde tanımlanan fonksiyon R üzerinde bir ağırlık fonksiyonudur.

Dolayısıyla her $r = (r_0, r_1, ..., r_{n-1}) \in R^n$ için $w_R(r) = \sum_{i=0}^{n-1} w_R(r_i)$ dir.

4.3.4. TANIM : Her $x, y \in R^n$, $x \neq y$ için x ve y arasındaki d_R uzaklığı $w_R(x-y)$ olarak tanımlanır. C, R^n üzerinde bir kod olmak üzere, C kodunun minimum uzaklığı her $x, y \in C$, $x \neq y$ için; $d_R(C) = \min\{d_R(x, y)\}$ biçiminde tanımlanır.

R^n üzerinde yazılan 4.3.4. Tanım, benzer biçimde R_1^n ve $\mathbb{F}_3^n$ üzerinde de verilir. Burada R_1^n ve $\mathbb{F}_3^n$ üzerinde C kodunun minimum uzaklığı sırasıyla $d_{\text{hom}}(C)$ ve $d_H(C)$ olarak gösterilir.

4.3.5. TANIM : $R = \mathbb{F}_3 + v\mathbb{F}_3 + u\mathbb{F}_3 + u^2\mathbb{F}_3$ ve $R_1 = \mathbb{F}_3 + u\mathbb{F}_3 + u^2\mathbb{F}_3$ olmak üzere;

$$\Phi_1 : R \longrightarrow R_1^2$$

$$a + bv + cu + du^2 \mapsto \Phi_1(a + bv + cu + du^2)$$

$$\begin{aligned} \Phi_1(a + bv + cu + du^2) &= \Phi_1(r + qv) \\ &= (2q, q + 2r) \\ &= (2b + 2au + (2a + 2c)u^2, (b + 2a) + (a + 2c)u + (a + c + 2d)u^2) \end{aligned}$$

biçiminde tanımlanan dönüşüme R üzerindeki Gray dönüşümü denir. Burada $r = a + cu + du^2$ ve $q = b + au + (a + c)u^2$, $a, b, c, d \in \mathbb{F}_3$ dür.

Φ_1 dönüşümünü

$\Phi_1(t_1, t_2, ..., t_n) = (q_1, q_2, ..., q_n, q_1 + r_1, q_2 + r_2, ..., q_n + r_n)$ biçiminde R^n e genişletilebilir.

Burada $i = 1, 2, ..., n$ için $t_i = r_i + q_i v$ olmak üzere $r_i = a_i + c_i u + d_i u^2$ ve $q_i = b_i + a_i u + (a_i + c_i)u^2$ biçimindedir.

4.3.6. TANIM : $R_1 = \mathbb{F}_3 + u\mathbb{F}_3 + u^2\mathbb{F}_3$, $x, y, z \in \mathbb{F}_3$ olmak üzere;

$$\Phi_2 : R_1 \longrightarrow \mathbb{F}_3^9$$
$$x + yu + zu^2 \mapsto \Phi_2(x + yu + zu^2)$$
$$\Phi_2(x + yu + zu^2) = (z, y+z, 2y+z, x+z, x+y+z, x+2y+z, 2x+z, 2x+y+z, 2x+2y+z)$$

biçiminde tanımlanan dönüşüme R_1 halkası üzerindeki Gray dönüşümü denir. Buradan Φ_2 dönüşümü

$$\begin{aligned}\Phi_2(b_1, b_2, ..., b_n) = (&z_1, z_2, ..., z_n, y_1 + z_1, y_2 + z_2, ..., y_n + z_n, 2y_1 + z_1, 2y_2 + z_2, ..., 2y_n + z_n,\\ &x_1 + z_1, x_2 + z_2, ..., x_n + z_n, x_1 + y_1 + z_1, x_2 + y_2 + z_2, ..., x_n + y_n + z_n,\\ &x_1 + 2y_1 + z_1, x_2 + 2y_2 + z_2, ..., x_n + 2y_n + z_n, 2x_1 + z_1, 2x_2 + z_2, ..., 2x_n + z_n,\\ &2x_1 + y_1 + z_1, 2x_2 + y_2 + z_2, ..., 2x_n + y_n + z_n, 2x_1 + 2y_1 + z_1, 2x_2 + 2y_2 + z_2, ...,\\ &2x_n + 2y_n + z_n)\end{aligned}$$

biçiminde R_1^n e genişletilebilir. Burada $i = 1, 2, ..., n$ için $x_i, y_i, z_i \in \mathbb{F}_3$ olmak üzere, $b_i = x_i + y_i u + z_i u^2$ biçimindedir.

4.3.7. ÖNERME : Φ_1 ve Φ_2 dönüşümleri 4.3.5. Tanım ve 4.3.6. Tanım daki gibi olsun. Φ_1 dönüşümü (R^n, d_R) ile $(R_1^{2n}, d_{\text{hom}})$, Φ_2 dönüşümü de $(R_1^{2n}, d_{\text{hom}})$ ile $(\mathbb{F}_3^{9n}, d_H)$ arasında birer izometridir. Bunun sonucu olarak $\Phi_2 \circ \Phi_1$ dönüşümü de (R^n, d_R) ile $(\mathbb{F}_3^{9n}, d_H)$ arasında bir izometridir.

Kanıt: 4.2.12. Önermenin kanıtına benzer biçimde görülür.

4.3.8. TANIM : C, R halkası üzerinde n uzunluğunda bir lineer kod olsun.

$$\sigma : R^n \longrightarrow R^n$$
$$(c_o, c_1, ..., c_{n-1}) \mapsto \sigma(c_o, c_1, ..., c_{n-1}) = (c_{n-1}, c_0, ..., c_{n-2})$$

permütasyonu için $\sigma(C) = C$ koşulu sağlanıyorsa C koduna R üzerinde bir cyclic kod denir. R_1 halkası ve $\mathbb{F}_3$ cismi üzerinde de aynı tanım verilir.

4.3.9. TANIM : D, R_1 halkası üzerinde $2n$ uzunluğunda bir lineer kod olsun. Her $i = 0, 1$, $a \in R_1^{2n}$ için $a = (a_0, a_1, ..., a_{2n-1}) = (a^{(0)} \,|\, a^{(1)})$, $a^{(i)} \in R_1^n$ olmak üzere

$$\sigma^{\otimes 2} : R_1^{2n} \longrightarrow R_1^{2n}$$
$$a \mapsto \sigma^{\otimes 2}(a) = (\sigma(a^{(0)}) \,|\, \sigma(a^{(1)}))$$

biçiminde tanımlanan permütasyonu için $\sigma^{\otimes 2}(D) = D$ koşulu sağlanıyorsa D koduna R_1 üzerinde 2. mertebeden bir quasi-cyclic kod denir. Burada σ permütasyonu R_1^n de tanımlıdır.

4.3.10. TANIM : $\tilde{D}$, R_1 halkası üzerinde $2n$ uzunluğunda bir lineer kod olsun.

$$\tau : R_1^{2n} \longrightarrow R_1^{2n}$$

$$(d_o, d_1, ..., d_{2n-1}) \mapsto \tau(d_o, d_1, ..., d_{2n-1}) = (d_{2n-1}, d_0, ..., d_{2n-2})$$

permütasyonu için $\tau(\tilde{D}) = \tilde{D}$ koşulu sağlanıyorsa $\tilde{D}$ koduna R_1 üzerinde bir cyclic kod adı verilir.

4.3.11. TANIM : C_1, $\mathbb{F}_3$ cismi üzerinde $18n$ uzunluğunda bir lineer kod olsun. Her $i = 0,1,...,8$, $a \in \mathbb{F}_3^{18n}$ için

$a = (a_0, a_1, ..., a_{18n-1}) = (a^{(0)} \,|\, a^{(1)} \,|\, a^{(2)} \,|\, ... \,|\, a^{(8)}), a^{(i)} \in \mathbb{F}_3^{2n}$ olmak üzere

$$\sigma^{\otimes 9} : \mathbb{F}_3^{18n} \longrightarrow \mathbb{F}_3^{18n}$$

$$a \mapsto \sigma^{\otimes 9}(a) = (\sigma(a^{(0)}) \,|\, \sigma(a^{(1)}) \,|\, \sigma(a^{(2)}) \,|\, ... \,|\, \sigma(a^{(8)}))$$

biçiminde tanımlanan permütasyonu için $\sigma^{\otimes 9}(C_1) = C_1$ koşulu sağlanıyorsa C_1 koduna $\mathbb{F}_3$ üzerinde 9. mertebeden bir quasi-cyclic kod denir. Burada σ permütasyonu $\mathbb{F}_3^{2n}$ de tanımlıdır.

Aşağıdaki kısımda R halkası üzerindeki bir cyclic kod alındığında bu kodun R üzerinde tanımlı Gray dönüşümü yardımı ile R_1 halkası üzerinde 2. mertebeden bir quasi-cyclic kod elde edildiği gösterilmiştir. Buna ilaveten R_1 halkası üzerinde uzunluğu çift sayı olan bir cyclic kodun R_1 üzerinde tanımlı Gray dönüşümü yardımı ile $\mathbb{F}_3$ cismi üzerinde 9. mertebeden bir quasi-cyclic koda karşılık geldiği gösterilmiştir.

4.3.12. ÖNERME : σ dönüşümü R^n üzerinde bir permütasyon, $\sigma^{\otimes 2}$ dönüşümü R_1^{2n} üzerinde bir permütasyon ve Φ_1, R^n den R_1^{2n} e yukarıda tanımlanan Gray dönüşümü olsun. Bu durumda $\Phi_1 \circ \sigma = \sigma^{\otimes 2} \circ \Phi_1$ eşitliği sağlanır.

Kanıt: Her $0 \le i \le n-1$ için $c_i = r_i + q_i v$ olmak üzere $c = (c_0, c_1, ..., c_{n-1}) \in R^n$ olsun. Bu durumda $c \in R^n$ in Gray görüntüsünü

$$\Phi_1(c) = \Phi_1(c_0, c_1, ..., c_{n-1}) = \Phi_1(r_0 + q_0 v, r_1 + q_1 v, ..., r_{n-1} + q_{n-1} v)$$
$$= (2q_0, 2q_1, ..., 2q_{n-1}, q_0 + 2r_0, q_1 + 2r_1, ..., q_{n-1} + 2r_{n-1})$$

olarak bulunur. Buradan

$$\sigma^{\otimes 2}(\Phi_1(c)) = (2q_{n-1}, 2q_0, ..., 2q_{n-2}, q_{n-1} + 2r_{n-1}, q_0 + 2r_0, ..., q_{n-2} + 2r_{n-2})$$

elde edilir. Diğer taraftan,

$\sigma(c) = \sigma(c_0, c_1, ..., c_{n-1}) = (c_{n-1}, c_0, ..., c_{n-2})$ dir. Bu ifadenin Gray görüntüsü alındığında

$$\Phi_1(\sigma(c)) = \Phi_1\,\sigma(c_0, c_1, ..., c_{n-1}) = \Phi_1(c_{n-1}, c_0, ..., c_{n-2})$$
$$= \Phi_1(r_{n-1} + vq_{n-1}, r_0 + vq_0, ..., r_{n-2} + vq_{n-2})$$
$$= (2q_{n-1}, 2q_0, ..., 2q_{n-2}, q_{n-1} + 2r_{n-1}, q_0 + 2r_0, ..., q_{n-2} + 2r_{n-2})$$

elde edilir.

4.3.13. TEOREM : C kodunun R halkası üzerinde n uzunluğunda bir cyclic kod olması için gerekli ve yeterli koşul $\Phi_1(C)$ nin R_1 halkası üzerinde $2n$ uzunluğunda 2. mertebeden bir quasi-cyclic kod olmasıdır.

Kanıt : C, R halkası üzerinde bir cyclic kod olsun. Bu durumda $\sigma(C) = C$ olur. Eşitliğin her iki tarafının Φ_1 görüntüsü alındığında $\Phi_1(\sigma(C)) = \Phi_1(C)$ elde edilir. 4.3.12. Önermeden $\sigma^{\otimes 2}(\Phi_1(C)) = \Phi_1(\sigma(C)) = \Phi_1(C)$ bulunur. Böylece $\Phi_1(C)$ nin 2. mertebeden bir quasi-cyclic kod olduğu görülür. Tersine $\Phi_1(C)$, 2. mertebeden bir quasi-cyclic kod ise $\sigma^{\otimes 2}(\Phi_1(C)) = \Phi_1(C)$ elde edilir. 4.3.12. Önermeden $\sigma^{\otimes 2}(\Phi_1(C)) = \Phi_1(\sigma(C)) = \Phi_1(C)$ bulunur. Böylece Φ_1 bire-bir fonksiyon olduğu için $\sigma(C) = C$ olur. O halde C bir cyclic koddur.

4.3.14. ÖNERME : τ dönüşümü R_1^{2n} üzerinde bir permütasyon, $\sigma^{\otimes 9}$ dönüşümü $\mathbb{F}_3^{18n}$ üzerinde bir permütasyon ve Φ_2, R_1^{2n} den $\mathbb{F}_3^{18n}$ e yukarıda tanımlanan Gray dönüşümü olsun. Bu durumda $\sigma^{\otimes 9} \circ \Phi_2 = \Phi_2 \circ \tau$ eşitliği sağlanır.

Kanıt : Her $0 \le i \le 2n-1$ için $t_i = x_i + y_i u + z_i u^2$ olmak üzere $t = (t_0, t_1, ..., t_{2n-1}) \in R_1^{2n}$ olsun. Burada $\tau(t) = \nu(t_0, t_1, ..., t_{2n-1}) = (t_{2n-1}, t_0, ..., t_{2n-2})$ dir. Bu ifadenin Gray görüntüsü alındığında

$$\Phi_2.\tau(t) = \Phi_2(t_{2n-1}, t_0, ..., t_{2n-2})$$

$$\begin{aligned}
&= (z_{2n-1}, z_0, ..., z_{2n-2}, y_{2n-1} + z_{2n-1}, y_0 + z_0, ..., y_{2n-2} + z_{2n-2}, 2y_{2n-1} + z_{2n-1},\\
&\quad y_0 + z_0, ..., 2y_{2n-2} + z_{2n-2}, x_{2n-1} + z_{2n-1}, x_0 + z_0, ..., x_{2n-2} + z_{2n-2},\\
&\quad x_{2n-1} + y_{2n-1} + z_{2n-1}, x_0 + y_0 + z_0, ..., x_{2n-2} + y_{2n-2} + z_{2n-2},\\
&\quad x_{2n-1} + 2y_{2n-1} + z_{2n-1}, x_0 + 2y_0 + z_0, ..., x_{2n-2} + 2y_{2n-2} + z_{2n-2},\\
&\quad 2x_{2n-1} + z_{2n-1}, 2x_0 + z_0, ..., 2x_{2n-2} + z_{2n-2},\\
&\quad 2x_{2n-1} + y_{2n-1} + z_{2n-1}, 2x_0 + y_0 + z_0, ..., 2x_{2n-2} + y_{2n-2} + z_{2n-2},\\
&\quad 2x_{2n-1} + 2y_{2n-1} + z_{2n-1}, 2x_0 + 2y_0 + z_0, ..., 2x_{2n-2} + 2y_{2n-2} + z_{2n-2})
\end{aligned}$$

elde edilir. Diğer taraftan $t \in R_1^{2n}$ in Gray görüntüsü

$$\begin{aligned}
\Phi_2(t) &= \Phi_2(t_0, t_1, ..., t_{2n-1})\\
&= (z_0, z_1, ..., z_{2n-1}, y_0 + z_0, y_1 + z_1, ..., y_{2n-1} + z_{2n-1}, 2y_0 + z_0, 2y_1 + z_1, ..., 2y_{2n-1} + z_{2n-1},\\
&\quad x_0 + z_0, x_1 + z_1, ..., x_{2n-1} + z_{2n-1}, x_0 + y_0 + z_0, x_1 + y_1 + z_1, ..., x_{2n-1} + y_{2n-1} + z_{2n-1},\\
&\quad x_0 + 2y_0 + z_0, x_1 + 2y_1 + z_1, ..., x_{2n-1} + 2y_{2n-1} + z_{2n-1}, 2x_0 + z_0, 2x_1 + z_1, ..., 2x_{2n-1} + z_{2n-1},\\
&\quad 2x_0 + y_0 + z_0, 2x_1 + y_1 + z_1, ..., 2x_{2n-1} + y_{2n-1} + z_{2n-1},\\
&\quad 2x_0 + 2y_0 + z_0, 2x_1 + 2y_1 + z_1, ..., 2x_{2n-1} + 2y_{2n-1} + z_{2n-1})
\end{aligned}$$

olarak bulunur. Buradan

$$\sigma^{\otimes 9}.\Phi_2(t) = \sigma^{\otimes 9}(t_0, t_1, ..., t_{2n-1})$$

$$\begin{aligned}
&= (z_{2n-1}, z_0, ..., z_{2n-2}, y_{2n-1} + z_{2n-1}, y_0 + z_0, ..., y_{2n-2} + z_{2n-2}, 2y_{2n-1} + z_{2n-1},\\
&\quad y_0 + z_0, ..., 2y_{2n-2} + z_{2n-2}, x_{2n-1} + z_{2n-1}, x_0 + z_0, ..., x_{2n-2} + z_{2n-2},\\
&\quad x_{2n-1} + y_{2n-1} + z_{2n-1}, x_0 + y_0 + z_0, ..., x_{2n-2} + y_{2n-2} + z_{2n-2},\\
&\quad x_{2n-1} + 2y_{2n-1} + z_{2n-1}, x_0 + 2y_0 + z_0, ..., x_{2n-2} + 2y_{2n-2} + z_{2n-2},\\
&\quad 2x_{2n-1} + z_{2n-1}, 2x_0 + z_0, ..., 2x_{2n-2} + z_{2n-2},\\
&\quad 2x_{2n-1} + y_{2n-1} + z_{2n-1}, 2x_0 + y_0 + z_0, ..., 2x_{2n-2} + y_{2n-2} + z_{2n-2},\\
&\quad 2x_{2n-1} + 2y_{2n-1} + z_{2n-1}, 2x_0 + 2y_0 + z_0, ..., 2x_{2n-2} + 2y_{2n-2} + z_{2n-2})
\end{aligned}$$

elde edilir.

4.3.15. TEOREM : D kodunun R_1 halkası üzerinde $2n$ uzunluğunda bir cyclic kod olması için gerekli ve yeterli koşul $\Phi_2(D)$ nin $\mathbb{F}_3$ cismi üzerinde $18n$ uzunluğunda 9 . mertebeden bir quasi-cyclic kod olmasıdır.

Kanıt : D bir cyclic kod ise $\tau(D) = D$ dir. Eşitliğin her iki tarafının Φ_2 görüntüsü alındığında $\Phi_2(\tau(D)) = \Phi_2(D)$ elde edilir. 4.3.14. Önermeden $\sigma^{\otimes 9}(\Phi_2(D)) = \Phi_2(\tau(D)) = \Phi_2(D)$ bulunur. Böylece $\Phi_2(D)$, 9 . mertebeden bir quasi-cyclic kod olduğu görülür. Tersine $\Phi_2(D)$, 9. mertebeden bir quasi-cyclic kod ise

$\sigma^{\otimes 9}(\Phi_2(D)) = \Phi_2(D)$ sağlanır. 4.3.14. Önermeden $\sigma^{\otimes 9}(\Phi_2(D)) = \Phi_2(\tau(D)) = \Phi_2(D)$ bulunur. Φ_2 bire-bir bir fonksiyon olduğundan $\tau(D) = D$ olur. Dolayısıyla D nin bir cyclic kod olduğu görülür.

Yukarıdaki teoremler kullanılarak elde edilen temel sonuç aşağıda verilmiştir.

4.3.16. SONUÇ : C nin R halkası üzerinde n uzunluğunda bir cyclic kod olması için gerekli ve yeterli koşul $\Phi_2(\Phi_1(C))$ nin $\mathbb{F}_3$ cismi üzerinde $18n$ uzunluğunda, 9. mertebeden bir quasi-cyclic kod olmasıdır.

Kanıt : C kodunun önce Φ_1 görüntüsü sonra Φ_2 görüntüsü alındığında 4.3.13. Teorem ve 4.3.15. Teoremleri ile kolayca görülür.

BÖLÜM 5

SONUÇLAR

Bu çalışmada; Hadamard kodların yapısı, Hadamard kodların bilinen kodlar ile ilişkisi, bulunan yeni kodlar ve yeni halkalar hakkında bulunan orijinal sonuçlar tartışılmıştır.

Üçüncü bölümde $u^2 = 0$ durumunda $\mathbb{F}_2 + u\mathbb{F}_2$ halkası üzerinde tanımlanan özel matrisler ile kodlar yazılmıştır. Bu halkadan Galois cismine tanımlanan Gray dönüşümü ile birlikte kodların Gray görüntülerinin Hadamard kod olduğu sonucu 3.1.9.Teorem ile kanıtlanmıştır. Devamında Hadamard kodlarının 2. mertebeden quasi-cyclic kod olduğu teorisi 3.1.14.Teorem ile gösterilmiştir. Bunlara ilaveten bulunan C^{α_1,α_2} kodları için ${}_1C^{\alpha_1,\alpha_2}$, ${}_2C^{\alpha_1,\alpha_2}$, $even(C^{\alpha_1,\alpha_2})$ ve $odd(C^{\alpha_1,\alpha_2})$ kodları tanımlanmış ve bunların Hadamard kodları ile sınıflandırılması yapılmıştır. $\mathbb{F}_2 + u\mathbb{F}_2$ halkasında $C_1^{\alpha_1,\alpha_2}$ ve $C_2^{\alpha_1,\alpha_2}$ kodları verilerek bunların direkt çarpımlarının Hadamard kodlara denk olduğu teorisi 3.1.27.Teoremde kanıtlanmıştır. Bunların self dual ve self ortogonal olanlarının ayrıca sınıflandırılması 3.1. bölümde gösterilmiştir.

3.1. bölümde $u^2 = 0$ durumunda $\mathbb{F}_2 + u\mathbb{F}_2$ halkasındaki özel matrisler ile yazılan kodlar, 3.2. bölümünde $v^2 = 1$ ve $v^2 = v$ durumlarında $\mathbb{F}_2 + v\mathbb{F}_2$ halkalarında, 3.3. bölümünde $u^3 = 0$ durumunda $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$ halkasında ve bu genişletilerek 3.4. bölümde $u^{m+1} = 0$ durumunda $\mathbb{F}_2 + u\mathbb{F}_2 ... + u^m\mathbb{F}_2$ halkasında da bulunmuştur. Dolayısı ile farklı halkalarda Hadamard kodların varlığının ortaya konulabileceği sonucuna varılmıştır. Buradan Hadamard kodların farklı mertebeden quasi-cyclic kodlar olduğu sonucu belirlenilmiştir.

Dördüncü bölümün 4.1. bölümünde 16 elemanlı yeni bir halka tanımlanmıştır. Bu halka $u^3=0,\ v^2=0,\ u.v=v.u=0$ koşulları ile $\mathbb{F}_2[u,v]/_{<u^3,\ v^2,u.v>}$ dir. Yeni tanımladığımız bu halka üzerinde kod yazabilmek için Ağırlık fonksiyonu tanımlanmıştır. Burada 4.1.19.Teorem ve 4.1.21.Teoremlerin ispatlanması bu halka üzerinde $(1+v)-$constacyclic kodun $\mathbb{F}_2$ cisminde 2. mertebeden quasi-cyclic kod olduğu sonucuna varılmıştır.

4.2. bölümde ise; $\mathbb{F}_p[u,v]/_{<u^3,\ v^2,u.v>}$ ifadesi ile tanımlanan halka inşa edilmiştir. Bu halka üzerinde özel bir Ağırlık fonksiyonu tanımlanarak kodlar yazılması sağlanılmıştır. Ayrıca bu halkadan bilinen halkaya Gray dönüşümü verilmiştir. Bu bilgiler neticesinde bu halkalar üzerinde cyclic kodlar ele alınmış ve 4.2.13.Teorem ile 4.2.15.Teoremin ispatları neticesinde 4.2.16. Sonucunda $\mathbb{F}_p[u,v]/_{<u^3,\ v^2,u.v>}$ halkasındaki bir cyclic kodun olması için gerekli ve yeterli koşulun p^2 inci mertebeden bir quasi-cyclic kod olması gösterilmiştir.

4.3. bölümde ise; 4.2. bölümde bulunan halka özelleştirilerek $p=3$ alınması ile elde edilen benzer sonuçlara yer verilmiştir.

KAYNAKLAR

[1] C.E. Shannon, ***A Mathematical Theory of Communication***, The Bell System Technical Journal, Vol.27, 379-423, (1948)

[2] I.F. Blanke, ***Codes Over Certain Rings***, Information and Control, Vol. 20, 396-404, (1972)

[3] J.Wolfmann, ***Negacyclic and cyclic codes over*** $\mathbb{Z}_4$, IEEE Trans. Inf. Theory, Vol. 45, 2527-2532, (1999)

[4] D. S. Krotov, ***Z4-linear perfect codes***, Diskretn. Anal. Issled. Oper., Vol.**7**, 4, 78–90, (2000)

[5] D. S. Krotov, ***Z4-linear Hadamard and extended perfect codes***, Proc. of the International Workshop on Coding and Cryptography, Paris, 329-334, (2001)

[6] J. Qian, L. Zhang and S. Zhu, $(1+u)$***_cyclic and cyclic codes over the ring*** $\mathbb{F}_2+u\mathbb{F}_2$, Applied Mathematics Letters, Vol.19, 820-823, (2006)

[7] J. Qian, L. Zhang and S. Zhu, ***Constacyclic and cycliccodes over*** $\mathbb{F}_2+u\mathbb{F}_2+u^2\mathbb{F}_2$, IEICE Trans. Fundamentals, Vol.89, 6, 1863-1865, (2006)

[8] B.Yıldız, S.Karadeniz, ***Linear codes over*** $\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2+uv\mathbb{F}_2$, Des. Codes Cryptgr., Vol.54, 61-71, (2010)

[9] S.Karadeniz, B.Yıldız, ***On*** $(1+v)$***-constacyclic codes over*** $\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2+uv\mathbb{F}_2$, Journal of the Franklin Institude, Vol.348, 2625-2632, (2011)

[10] X. Xioafang, $(1+v)$***-constacyclic codes over*** $\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2$, Computer Engineering and Applications, Vol.49,12,77-79, (2013)

[11] S. Ling, C. Xing, ***Coding Theory A First Course*** , (Cambridge University Pres, 2004)

[12] F.J. MacWilliams, N.J.A. Sloane, ***The Theory of Error Correcting Codes***, (North-Holland Publishing Company, 1977)

[13] S. Roman, ***Coding and Information Theory***, (Springer Verlag, 1992)

[14] W. C. Huffman, V. Pless, ***Fundamentals of Error Correcting Codes***, (Cambridge, 2003)

[15] L. R. Vermani, ***Elements of Algebraic Coding Theory***, (Chapman Hall, India, 1996)

[16] A. Bonnecaze, P. Udaya, ***Cyclic codes and self dual codes*** $\mathbb{F}_2+u\mathbb{F}_2$, IEEE Trans. Inf. Theory , Vol. 45, 1250-1255, (1999)

[17] S. Zhu, Y. Wang, M. Shi, ***Some Result On Cyclic Codes over*** $\mathbb{F}_2+v\mathbb{F}_2$, IEEE Trans. Inf. Theory , Vol.56, 4, 1680-1684, (2010)

[18] M. Al-Ashker, M.Hamoudeh, ***Cylic codes over*** $\mathbb{Z}_2+u\mathbb{Z}_2+u^2\mathbb{Z}_2+...+u^{k-1}\mathbb{Z}_2$, Turk Journal of Math., Vol.35, 737-749, (2011)

[19] P. Udomkavanich, S. Jitman, ***On the Gray Image of (***$1-u^m$***)-Cyclic Codes*** $\mathbb{F}_{p^k}+u\mathbb{F}_{p^k}+...+u^m\mathbb{F}_{p^k}$, Int. J. Contemp. Math. Sciences, Vol.26, 4, 1265-1272, (2009)

[20] S. Ling, J.T. Blackford, $\mathbb{Z}_{p^{k+1}}$ ***_ Lineer Codes***, IEEE Trans. On Inform. Theory, Vol.45, 9, 2592-2605, (2002)

[21] M.C. Amarra, F.R.Nemenzo, ***On*** $(1-u)$***−cyclic codes over*** $\mathbb{F}_{p^k}+u\mathbb{F}_{p^k}$, Applied Mathematics Letters, Vol.21, 1129-1133, (2008)

[22] Y. Çengellenmiş, F. Öke, ***On (***$1-u^2$***)-Cyclic Codes over*** $\mathbb{F}_{p^k}+u\mathbb{F}_{p^k}+u^2\mathbb{F}_{p^k}$, Advances and Applications in Discrete Mathematics, Vol.4, 1,11-16, (2009)

[23] T. Abualrub, İ. Şiap, ***Cyclic codes over the rings*** Z_2+uZ_2 ***and*** $Z_2+uZ_2+u^2Z_2$, Desings, Codes and Cryptography,Vol.24, 3, 273-287, (2007)

[24] T. Abualrub, İ. Şiap, ***Constacyclic codes over*** $\mathbb{F}_2+u\mathbb{F}_2$, Journal of the Franklin Institude, Vol.346, 520-529, (2009)

[25] M. Özkan, F. Öke, ***A relation between Hadamard codes and some special codes over*** $\mathbb{F}_2+u\mathbb{F}_2$, App. Mathematics and Inf. Sci.,Vol.10, 2, 701-704, (2016)

[26] M. Özkan, F. Öke, ***Some Special Codes Over*** $\mathbb{F}_3+v\mathbb{F}_3+u\mathbb{F}_3+u^2\mathbb{F}_3$, Mathematical Sciences and Applications E-Notes, Vol.4, 1, 40-44, (2016)

[27] M. Özkan, F. Öke, **Gray images of (1 + v)-constacyclic codes over a particular ring** , Palestine Journal of Mathematics, (Yayına kabul edildi.)

ÖZGEÇMİŞ

08.02.1985 tarihinde Kadıköy-İstanbulda doğdum. İlkokulu ve ortaokulu III. Selim İlköğretim Okulu Üsküdar-İstanbul'da, liseyi Üsküdar Burhan Felek Lisesi Üsküdar-İstanbul'da okudum. 2002 yılında kayıt olduğum Trakya Üniversitesi Fen-Edebiyat Fakültesi Matematik Bölümü'nden Haziran 2006 döneminde mezun oldum. Temmuz 2006 yılında Trakya Üniversitesi Fen-Edebiyat Fakültesi Matematik Bölüm'ünde açılan Araştırma Görevlisi sınavını kazanarak göreve başladım. 2009 yılında Trakya Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalı'nda Yüksek Lisansımı tamamladım. Halen Trakya Üniversitesi Fen Fakültesi Matematik Bölümünde Araştırma Görevlisi olarak görevimi sürdürmekteyim.

BİLİMSEL YAYIN FAALİYETLERİ

Yayınlanmış Makalenin,

Adı : A relation between Hadamard codes and some special codes over $\mathbb{F}_2 + u\mathbb{F}_2$

Yazarları : Mustafa ÖZKAN, Figen ÖKE

Yayınlandığı Dergi : App.Mathematics and Inf. Sci.

Yılı : 2016

Yayınlanmış Makalenin,

Adı : Some Special Codes Over $\mathbb{F}_3 + v\mathbb{F}_3 + u\mathbb{F}_3 + u^2\mathbb{F}_3$

Yazarları : Mustafa ÖZKAN, Figen ÖKE

Yayınlandığı Dergi : Mathematical Sciences and Applications E-Notes.

Yılı : 2016

Yayınlanmış Makalenin,

Adı : Gray images of (1 + v)-constacyclic codes over a particular ring

Yazarları : Mustafa ÖZKAN, Figen ÖKE

Yayınlandığı Dergi : Palestine Journal of Mathematics.

Yılı : Yayına kabul edildi

Katıldığı Kongre : International Congress in Honour of Professor Ravi P. Agarwal 23-26 Haziran 2014 Bursa-TÜRKİYE

Bildiri Adı : Certain quasi-cyclic codes which are Hadamard codes (Sözlü Bildiri)

Düzenleyen Kuruluş : Uludağ Üniversitesi

Katıldığı Kongre : 3rd International Eurasian Conference On Mathematical Sciences and Applications 25 - 28 Ağustos 2014 Viyana-AVUSTURYA

Bildiri Adı : A relation between Hadamard codes and some special codes over $\mathbb{F}_2 + u\mathbb{F}_2$ (Sözlü Bildiri)

Düzenleyen Kuruluş : Viyana Teknoloji Üniversitesi ve Sakarya Üniversitesi

Katıldığı Kongre : The 28th International Conference of Jangjeon Mathematical Society 15 - 19 Mayıs 2015 Antalya-TÜRKİYE

Bildiri Adı : On Hadamard codes constructed over $\mathbb{F}_2 + u\mathbb{F}_2 + ... + u^m\mathbb{F}_2$ (Sözlü Bildiri)

Düzenleyen Kuruluş : Akdeniz Üniversitesi

Katıldığı Kongre : Öğr. Matematik Çalıştayı 17 Nisan 2015 İstanbul-TÜRKİYE

Bildiri Adı : Yeni bir halka üzerinde constacylic kodların yapısı (Poster Bildiri)

Düzenleyen Kuruluş : İstanbul Üniversitesi

Katıldığı Kongre : 4th International Eurasian Conference On Mathematical Sciences and Applications 31 Ağustos – 3 Eylül 2015 Atina- YUNANİSTAN

Bildiri Adı : On the Codes Over the Ring $\mathbb{F}_2 + v\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$ (Sözlü Bildiri)

Düzenleyen Kuruluş : Sakarya Üniversitesi

Katıldığı Kongre : 4th International Eurasian Conference On Mathematical Sciences and Applications 31 Ağustos – 3 Eylül 2015 Atina- YUNANİSTAN

Bildiri Adı : Some Special Codes Over $\mathbb{F}_3 + v\mathbb{F}_3 + u\mathbb{F}_3 + u^2\mathbb{F}_3$ (Sözlü Bildiri)

Düzenleyen Kuruluş : Sakarya Üniversitesi

Katıldığı Kongre : 3rd International Conference On Recent Advances in Pure and Applied Mathematics 19-23 Mayıs 2016 Bodrum-Muğla-TÜRKİYE

Bildiri Adı : Results On Hadamard Codes and Codes Over Rings (Sözlü Bildiri)

Düzenleyen Kuruluş : İstanbul Ticaret Üniversitesi ve İstanbul Medeniyet Üniversitesi

Katıldığı Kongre : 5th International Eurasian Conference On Mathematical Sciences and Applications 16-19 Ağustos 2016 Belgrad- SIRBİSTAN

Bildiri Adı : Codes defined via especial matrices over the ring and Hadamard codes (Sözlü Bildiri)

Düzenleyen Kuruluş : Sakarya Üniversitesi ve Nis Üniversitesi

Katıldığı Kongre	: 5th International Eurasian Conference On Mathematical Sciences and Applications 16-19 Ağustos 2016 Belgrad- SIRBİSTAN
Bildiri Adı	: Cyclic codes over the new ring (Sözlü Bildiri)
Düzenleyen Kuruluş	: Sakarya Üniversitesi ve Nis Üniversitesi