T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

$\mathbf{Z_4(Z_4 + vZ_4)}$ −LİNEER VE SABİT DEVİRLİ KODLAR

YÜKSEK LİSANS TEZİ

Asuman DUMLU

Enstitü Anabilim Dalı	**:**	**MATEMATİK**
Enstitü Bilim Dalı	**:**	**CEBİR VE SAYILAR TEORİSİ**
Tez Danışmanı	**:**	**Prof. Dr. Mehmet ÖZEN**

Ağustos 2021

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

$\mathbf{Z_4(Z_4 + vZ_4)}$ −LİNEER VE SABİT DEVİRLİ KODLAR

YÜKSEK LİSANS TEZİ

Asuman DUMLU

Enstitü Anabilim Dalı : MATEMATİK

Enstitü Bilim Dalı : CEBİR VE SAYILAR TEORİSİ

Bu tez 25.08.2021 tarihinde aşağıdaki jüri tarafından oybirliği ile kabul edilmiştir.

Jüri Başkanı **Üye** **Üye**

BEYAN

Tez içindeki tüm verilerin akademik kurallar çerçevesinde tarafımdan elde edildiğini, görsel ve yazılı tüm bilgi ve sonuçların akademik ve etik kurallara uygun şekilde sunulduğunu, kullanılan verilerde herhangi bir tahrifat yapılmadığını, başkalarının eserlerinden yararlanılması durumunda bilimsel normlara uygun olarak atıfta bulunulduğunu, tezde yer alan verilerin bu üniversite veya başka bir üniversitede herhangi bir tez çalışmasında kullanılmadığını beyan ederim.

Asuman DUMLU

25.08.2021

TEŞEKKÜR

Yüksek lisans eğitimimde yaptığım çalışmalarda bilgi ve deneyimlerini benimle paylaşan, araştırma çalışmalarımın tüm adımlarında desteğini esirgemeyen,öğrencisi olmaktan onur duyduğum değerli danışman hocam Prof. Dr. Mehmet ÖZEN'e teşekkürlerimi sunarım.

Lisans eğitimim boyunca insani ve ahlaki değerleri ile örnek edindiğim, tecrübelerinden yararlandığım ve bu mesleği sayesinde sevdiğim değerli hocam sayın Prof. Dr. Ali PANCAR 'a en içten teşekkürlerimi sunarım.

Eğitim hayatım boyunca beni hiç yalnız bırakmayan, maddi ve manevi desteklerini her zaman yanımda hissettiğim canım annem, sevgili babam, kıymetli kardeşlerim ve desteğini eksik etmeyen bütün arkadaşlarıma sevgilerimi sunarım.

İÇİNDEKİLER

SİMGELER VE KISALTMALAR LİSTESİ

C : Kod

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

R : $v^2 = 1$, $Z_4[v] = Z_4 + vZ_4$ Halkası

R_1 : $\vartheta^2 = 2$, $Z_4[\vartheta] = Z_4 + \vartheta Z_4$ Halkası

C_{α} : C , $Z_4R -$ lineer kodunun ilk $\alpha -$ koordinatı

C_{β} : C , $Z_4R -$ lineer kodunun son $\beta -$ koordinatı

Çekf : f homomorfizmasının çekirdeği

$w_L(x)$: x 'in Lee ağırlığı

$w_H(x)$: x 'in Hamming ağırlığı

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

(n, M, d) : n uzunluğunda M elemanlı d minimum uzaklığına sahip bir kod

$[n, k, d]$: n uzunluğunda k boyutlu ve minimum uzaklığı d olan lineer kod

$der(f)$: f polinomunun derecesi

V :Vektör uzayı

ρ : $v^2 = 1$, $Z_4Z_4[v]$ Halkasının devirli öteleme operatörü

γ : $v^2 = 1$, $Z_4Z_4[v]$ Halkasının parçalı devirli öteleme operatörü

T_{λ} : $v^2 = 1$, $Z_4Z_4[v]$ Halkasının (λ)-Sabit devirli öteleme operatörü

ϖ : $\vartheta^2 = 2$, $Z_4Z_4[\vartheta]$ Halkasının devirli öteleme operatörü

ε : $\vartheta^2 = 2$, $Z_4Z_4[\vartheta]$ Halkasının parçalı devirli öteleme operatörü

T_{φ} : $\vartheta^2 = 2$, $Z_4Z_4[\vartheta]$ Halkasının (φ)-sabit devirli öteleme operatörü

ŞEKİLLER LİSTESİ

ÖZET

Anahtar kelimeler: Lineer kodlar,devirli kodlar,sabit devirli kodlar,toplamsal kodlar.

Bu tez 5 bölümden oluşmaktadır.

Birinci bölümde cebir ve kodlama teorisi ile ilgili temel tanım ve teoremler verilmiştir.Kodlama teorisinin temel problemi verilmiş ve günümüz, kutupsal kod inşasına uzanan ana fikri ele alınmıştır.Toplamsal kodların kuantum hata düzeltme sürecinde kullanıldığı vurgulanmıştır.Ayrıca tek hata düzelten hamming kodu için literatür araştırmasından bahsedilmiştir.İkinci bölümde, $v^2=1$ için $Z_4(Z_4+vZ_4)$- lineer kodunun yapısı tanıtılmıştır.Üçüncü bölümde $v^2=1$, $Z_4Z_4[v]-$devirli kodlar incelenmiştir. Devirli kodun üreteç polinomu ve geren kümesi belirlenmiştir. Ayrıca yeni gray dönüşümler tanımlanmış ve bazı $Z_4Z_4[v]$- devirli kodların gray görüntülerine bakılmıştır. Dördüncü bölümde $v^2=1$ ve $R=Z_4+vZ_4$ olmak üzere Z_4R-sabit devirli kodlar çalışılmıştır.Yeni gray dönüşümler tanımlanarak görüntüleri incelenmiştir.Beşinci bölümde $\vartheta^2=2$ ve $R_1=Z_4+\vartheta Z_4$ olmak üzere Z_4R_1- halkasının cebirsel yapısı incelenmiştir. Z_4R_1-sabit devirli kodlar çalışılmış,yeni ve farklı Gray dönüşümler tanımlanarak görüntülerine bakılmıştır.

Son bölümde ise sonuç ve önerilere yer verilmiştir.

$\mathbf{Z_4(Z_4 + vZ_4)}$ − LINEAR AND CONSTA CYCLIC CODES

SUMMARY

Keywords: Linear codes,cyclic codes,constacyclic codes, additive codes.

The thesis contains of five sections.

In the first section, basic definitions and theorems about algebra and coding theory are given. The basic problem of coding theory is explained and today,ıts main idea,extending to polar code construction, has been discussed. It is emphasized that additive codes are used in the quantum error correction process. In addition, literature research for single error correcting hamming code is mentioned.In the second section, the structure of the linear code $Z_4(Z_4 + vZ_4)$ where $v^2 = 1$ is introduced.In the third section, cyclic codes over $Z_4Z_4[v]$, $v^2 = 1$ is investigated. Cyclic codes over this ring are investigated and the general form of the generator and a minimal spanning set of such codes are determined.Also new gray map are defined and gray images of some cyclic codes are examined.In the fourth section, constacyclic codes over Z_4R where $v^2 = 1$ for $R = Z_4 + vZ_4$ are studied. New gray map is defined and gray images is determined.In the fifth section, the algebraic structure of the ring $Z_4R_1, \vartheta^2 = 2$ and $R_1 = Z_4 + \vartheta Z_4$ is examined. $Z_4R_1 -$ Constacycle codes have been studied, new and different gray map have been defined and their images have been examined.

In the last section, the conclusion and some recommendations are given

BÖLÜM 1. GİRİŞ

1.1. Cebirsel Tanımlar, Önermeler ve Teoremler

Tezin bu kısmında ileriki bölümlerde gerekli olan temel bilgiler verilecektir. Bu bilgiler [1,2,3,4,5,6,7,8,9,10,11,12,13,14] kaynaklarından derlenmiştir.

Tanım 1.1.1. A boştan farklı bir küme olsun. $x, y \in A$, olmak üzere her (x, y) sıralı ikilisine A'nın bir ve yalnız bir elemanını karşılık getiren fonksiyona A üzerinde bir ikili işlem denir. A kümesi üzerindeki bir ikili işlem " $\odot$ " ile gösterilecek olursa

$$\begin{aligned} &A \times A \to A \\ &(x, y) \to x \odot y \end{aligned}$$ ile tanımlanır.

Üzerinde en az bir ikili işlem tanımlanmış kümeye de cebirsel yapı denir.

Tanım 1.1.2. G boştan farklı bir küme ve " $\odot$ " G kümesi üzerinde tanımlı bir ikili işlem olsun. Aşağıdaki şartları sağlayan $(G, \odot)$ cebirsel yapısına grup denir.

i. $\forall a, b, c \in G$ için $a \odot (b \odot c)$

ii. $\forall g \in G$ için $e_G \odot g = g \odot e_G = g$

olacak şekilde bir tek $e_G \in G$ elemanı vardır ve bu elemana birim eleman denir.

iii. $\forall g \in G$ için $g \odot g^{-1} = g^{-1} \odot g = e_G$

olacak şekilde $g^{-1} \in G$ elemanı vardır ve bu elemana g'nin tersi denir .

Tanım 1.1.3. $(G,\odot)$ grubunda eğer $\forall a,b\in G$, için $a\odot b=b\odot a$ şartı sağlanıyor ise $(G,\odot)$ grubuna değişmeli (abelyen) grup denir.

Teorem 1.1.1. $(G,\odot)$ bir grup ve H kümesi G 'nin boştan farklı bir alt kümesi olsun. H kümesinin G 'nin bir alt grubu olması için gerek ve yeter şart

$\forall a,b\in H$ için $a\odot b^{-1}\in H$ olmasıdır.

Tanım 1.1.4. Boştan farklı S kümesi " + " ve " $\bullet$ " ikili işlemleri altında aşağıdaki şartları sağlıyor ise S kümesine halka denir ve $(S,+,\bullet)$ ile gösterilir. $\forall a,b,c\in S$ için

i. $(S,+)$ değişmeli gruptur.

ii. $a\bullet(b\bullet c)=(a\bullet b)\bullet c$

iii. $a\bullet(b+c)=a\bullet b+a\bullet c$ ve $(a+b)\bullet c=a\bullet c+b\bullet c$ dir.

Yazım açısından bundan sonraki bölümlerde $a\bullet b$ yerine ab yazılacaktır.

Tanım 1.1.5. $\forall a,b\in S$ için eğer $ab=ba$ şartı sağlanıyor ise S halkasına değişmeli halka denir.

Tanım 1.1.6. $\forall a\in S$ için $ae=ea=a$ olacak şekilde tek bir $e\in S$ varsa S halkasına birimli halka denir. Genel olarak halkanın birimi 1_S ile gösterilir ve birim eleman veya çarpımsal birim olarak adlandırılır.

Tanım 1.1.7. Birimli bir S halkasındaki bir $a\in S$ için $ab=ba=1_S$ olacak şekilde bir $b\in S$ varsa a elemanına terslenebilen eleman denir.

Tanım 1.1.8. Birimli ve değişmeli bir halkada sıfırdan farklı her elemanın ikinci işleme göre tersi var ise bu halkaya cisim denir.

Tanım 1.1.9. S bir halka ve $0 \neq a \in S$ olsun.Eğer bir $0 \neq b \in S$ elemanı için $ab = 0$ veya $ba = 0$ oluyor ise a elemanına sıfır bölen denir.

Tanım 1.1.10. Birimli, değişmeli ve sıfır bölensiz halkaya tamlık bölgesi denir.

Tanım 1.1.11. S halkasının boştan farklı bir R alt kümesi S'deki ikili işlemler altında kendi başına bir halka oluyor ise R kümesine S halkasının bir alt halkası denir.

Tanım 1.1.12. S bir halka olmak üzere $\forall a \in S$ için $na = 0$ şartını sağlayan en küçük pozitif n tamsayısına S halkasının karakteristiği denir ve S halkasına da sonlu karakteristiğe sahip denir.Eğer böyle bir en küçük pozitif n tamsayısı bulunamıyor ise S halkasının karakteristiği 0'dır denir. S halkasının karakteristiği $kar(R)$ ile gösterilir.

Teorem 1.1.2. Bir tamlık bölgesinin karakteristiği ya sıfırdır ya da asal sayıdır.

Tanım 1.1.13. S halkasının boştan farklı bir I alt kümesi

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

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

şartlarını sağlıyor ise I kümesine S halkasının bir sol (sağ) ideali denir. Eğer I ideali hem sağ ideal hem de sol ideal ise I kümesine S halkasının bir ideali denir. Eğer S halkası değişmeli ise sağ ve sol ideal aynı olacaktır.

Tanım 1.1.14. Bir S halkasında $I = \{0\}$ ve $I = S$ kümeleri halkanın aşikâr idealleridir. S halkasının aşikâr olmayan ideallerine has (öz) ideal denir.

Teorem 1.1.3. S birimli bir halka olmak üzere S halkasının I ideali halkanın birimini içeriyor ise $I = S$ dir.

Tanım 1.1.15. S bir halka olmak üzere I , S 'nin bir ideali ve $a,b \in S$ olsun. "$a \equiv b$ olması için gerek ve yeter şart $a-b \in I$ olmasıdır." şeklinde tanımlanan " $\equiv$ " bağıntısı S üzerinde bir denklik bağıntısıdır. Bu bağıntıya göre bütün denklik sınıflarının kümesi S/I ile gösterilirse $S / I = \{s+I : r \in I\}$ şeklindedir.

Tanım 1.1.16. S bir halka ve I da S 'nin bir ideali olsun. $\forall (r+I),(s+I) \in S/I$ için

$$(r+I)+(s+I)=(r+s)+I$$
$$(r+I).(s+I)=(rs+I)$$

şeklinde tanımlanan toplama ve çarpma işlemleri altında S/I bir halkadır. Bu S/I halkasına S 'nin I 'ya göre bölüm halkası denir. Eğer S birimli bir halka ise S/I halkasının birimi $1_S + I$ elemanıdır. Eğer S değişmeli bir halka ise S/I da değişmeli halkadır. S bir halka ve I da S 'nin bir ideali olduğunda S/I kalan sınıfının bir halka olarak tanımlanır.

Tanım 1.1.17. S değişmeli halkasındaki $P \neq R$ olacak şekildeki bir P ideali

$ab \in P \Rightarrow a \in P$ veya $b \in P$

şartını sağlıyor ise P idealine S halkasının asal ideali denir.

Tanım 1.1.18. S halkasında $M \neq S$ olacak şekilde bir M ideali olsun. Eğer S halkasında $M \subseteq I \subseteq S$ şartını sağlayan her I ideali için $I = M$ veya $I = S$ oluyor ise M idealine S halkasının maksimal ideali denir.

Teorem 1.1.4. S birimli ve değişmeli bir halka ve $P \neq S$ olacak şekilde bir I ideali olsun. S/P halkasının tamlık bölgesi olması için gerek ve yeter şart P idealinin S 'nin asal ideali olmasıdır.

Teorem 1.1.5. S birimli ve değişmeli bir halka ve $M \neq S$ olacak şekilde bir M ideali olsun. S/M halkasının cisim olması için gerek ve yeter şart M idealinin S'nin maksimal ideali olmasıdır.

Teorem 1.1.6. Birimli ve değişmeli bir S halkasında her maksimal ideal asal idealdir. Fakat tersi doğru değildir.

Tanım 1.1.19. S birimli ve değişmeli bir halka ve $m_1, m_2, m_3, ..., m_t \in S$ olmak üzere

$$\langle m_1, m_2, m_3, ..., m_t \rangle = \langle m_1 l_1 + m_2 l_2 + m_3 l_3 + ... + m_t l_t : l_1, l_2, l_3, ...l_t \in S \rangle$$

idealine S'nin $m_1, m_2, m_3, ..., m_t$ tarafından üretilen ideali denir.

Özel olarak S halkasının bir I ideali $a \in S$ olmak üzere

$$I = \langle a \rangle = \{as : s \in S\}$$

şeklinde tek bir a elemanı tarafından üretiliyor ise I idealine temel ideal denir. "a" elemanına da I idealinin üreteci denir.

Tanım 1.1.20. Her ideali temel ideal olan S halkasına temel ideal halkası denir. Her ideali temel ideal olan tamlık bölgesine ise temel ideal bölgesi denir.

Tanım 1.1.21. Tek bir maksimal ideale sahip olan halkaya lokal halka denir.

Tanım 1.1.22. Birimli ve değişmeli bir halkada tüm idealler kapsama işlemi altında bir zincir oluşturuyorsa bu halkaya zincir halkası denir.

Yani $i = 0,1,2,....., n-1$ için S halkasının tüm I_i idealleri arasında

$$\{0\} = I_0 \subset I_1 \subset I_2 \subset ..... \subset I_{n-1} = S$$

şeklinde bir ilişki varsa S halkasına zincir halkası denir.

Teorem 1.1.7. Sonlu ve değişmeli bir S halkası için aşağıdaki koşullar denktir.

i. S bir lokal halka ve S'nin M maksimal ideali temel idealdir.

ii. S bir lokal temel ideal halkasıdır.

iii. S bir zincir halkasıdır.

Tanım 1.1.23. S ve R iki halka ve $f : S \to R$ fonksiyonu verilmiş olsun. Eğer $\forall r, s \in S$ için

i. $f(s+r) = f(s) + f(r)$

ii. $f(sr) = f(s)f(r)$

şartları sağlanırsa f'ye halka homomorfizması denir.

Tanım 1.1.24. S ve R iki halka ve $f : S \to R$ bir halka homomorfizması olsun. Eğer f, birebir ve örten ise f'ye bir halka izomorfizması denir. R ve S halkalarına da birbirine izomorf denir ve $S \cong R$ şeklinde ifade edilir.

Tanım 1.1.25. S ve R iki halka ve $f : S \to R$ bir halka homomorfizması olsun.

Bu durumda

i. $Çekf = \{s \in S : f(s) = 0_r\}$ kümesine f'nin çekirdeği

ii. $\text{Im } f = \{f(s) : s \in S\}$ kümesine f'nin görüntü kümesi adı verilir.

Teorem 1.1.8. S ve R iki halka ve $f : S \to R$ bir halka homomorfizması olsun. Bu durumda

i. $Çekf$, S halkasının bir idealidir.

ii. $Çekf = \{0_S\}$ ancak ve ancak f birebirdir.

Teorem 1.1.9. S ve R iki halka ve $f : S \to R$ bir halka homomorfizması olsun. Bu durumda

$S/_{Çekf} \cong \text{Im } f$ dir.

Tanım 1.1.26. S bir halka, m pozitif tamsayı ve $0 \le k \le l$ için $a_k \in S$ olmak üzere

$$f(x) = a_0 + a_1 x + a_2 x^2 + ... + a_l x^l$$

ifadesine S'den katsayılı bir polinom denir.Bu polinomda $k \ge l+1$ olmak üzere $a_k = 0$ olduğu kabul edilecektir. $0 \le k \le l$ için a_k elemanlarına $f(x)$ polinomunun katsayıları denir. $a_k \neq 0$ olacak şekildeki en büyük k tamsayısına $f(x)$ polinomunun derecesi denir ve $d^o f(x)$ şeklinde gösterilir. Bu şartı sağlayan a_k elemanına $f(x)$ polinomunun baş katsayısı, a_0 elemanına ise $f(x)$ polinomunun sabiti denir.

Tanım 1.1.27. Katsayıları S'den olan x belirsizine göre bütün polinomların kümesi $S[x]$ ile gösterilsin. Bu küme üzerinde polinomların toplamı ve çarpımı

$$f(x) = a_0 + a_1 x + ... + a_l x^l \in S[x]$$

$$g(x) = b_0 + b_1 x + ... + b_t x^t \in S[x]$$ olmak üzere,

$$f(x) + g(x) = \sum_{i=0}^{\max(l,t)} (a_i + b_i) x^i$$

$$f(x).g(x) = \sum_{i=0}^{l+t} c_i x^i \quad \text{ve} \quad c_i = \sum_{j=0}^{i} a_j b_{i-j}$$

şeklinde tanımlanır.

Tanım 1.1.28. $S[x]$ polinomlar kümesi yukarıda tanımlanan toplama ve çarpma işlemlerine göre bir halkadır.

Teorem 1.1.10. S 'den katsayılı polinom halkası $S[x]$ olmak üzere,

i. Eğer S halkası değişmeli ise $S[x]$ polinom halkası da değişmelidir.

ii. S birimli ise S halkasının birimi aynı zamanda $S[x]$ polinom halkasının da birimidir.

iii. S tamlık bölgesi ise $S[x]$ polinom halkası da tamlık bölgesidir.

Teorem 1.1.11. S 'den katsayılı polinom halkası $S[x]$ ve

$f(x) = a_0 + a_1 x + ... + a_l x^l$ ve $g(x) = b_0 + b_1 x + ... + b_t x^t$ sırası ile m. ve n. dereceden iki polinom olsun.

Bu durumda,

$$d^o[f(x) + g(x)] \leq d^o f(x) + d^o g(x)$$

Eğer S halkası tamlık bölgesi ise

$$d^o[f(x) + g(x)] = d^o f(x) + d^o g(x)$$ olur.

Tanım 1.1.29. Baş katsayısı 1 olan polinoma monik polinom denir.

Tanım 1.1.30. Sabitten farklı bir $f(x) \in S\,[x]$ polinomu, derecesi $f(x)$ polinomundan küçük fakat sabit olmayan herhangi iki polinomun çarpımı şeklinde yazılamıyorsa $f(x)$ polinomuna indirgenemez polinom denir.

Tanım 1.1.31. Birimli ve değişmeli bir S halkası ve $a,b \in S$ olsun. Eğer $b = ac$ olacak şekilde bir $c \in R$ varsa a elemanı b'yi böler (veya a elemanı b'nin bir çarpanıdır) denir ve $\frac{a}{b}$ ile gösterilir.

Tanım 1.1.32. Birimli ve değişmeli bir S halkasında $u \in S$ elemanı eğer $u/1_S$ şartını sağlıyor ise yani S de çarpımsal terse sahip ise u elemanına birimsel eleman

ya da aritmetik birim denir.

Tanım 1.1.33. S bir halka, M bir toplamsal değişmeli grup olmak üzere

$S \times M \to M$

$(s,m) \to sm$

ile tanımlanan dış işlem $\forall s, s_1, s_2 \in S$ ve $\forall m, m_1, m_2 \in M$ için

i. $s(m_1 + m_2) = sm_1 + sm_2$

ii. $(s_1 + s_2)m = s_1 m + s_2 m$

iii. $s_1(s_2)m = (s_1 s_2)m$

iv. $1_S m = m$

koşulları sağlanıyor ise M'ye bir sol S-modül denir. Benzer şekilde sağ S-modül de tanımlanabilir. Özel olarak eğer S halkası değişmeli ise sağ S-modül aynı

zamanda sol S-modül ve bunun tersi de doğru olacağından kısaca M 'ye S-modül denir.

Tanım 1.1.34. S bir halka, M bir S-modül ve M 'nin boştan farklı bir alt kümesi N olsun.

$\forall n_1, n_2 \in N$ ve $s \in S$ için

$i.\ 0_M \in N$ $\qquad ii.\ n_1 - n_2 \in N$ $\qquad iii.\ sn_1 \in N (n_1 s \in N)$

şartları sağlanıyor ise N 'ye M 'nin bir sol (sağ) S-alt modülü denir. (0) ve M 'nin kendisi M 'nin birer S-alt modülleridir. Bu alt modüllere aşikâr alt modüller denir.

Örnek 1.1.1. S bir halka ve elemanları S 'den olan sıralı n-lilerin kümesi S^n olsun. S^n, S üzerinde bir modüldür.

Tanım 1.1.35. S bir halka, M bir S-modül ve I indis kümesi olmak üzere $D = \{y_i\}_{i \in I}$ de M 'nin bir üreteç sistemi olsun. Eğer her $m \in M$ elemanı $r_i \in S$ ve $y_i \in D$ olmak üzere, $m = \sum_{i \in I} r_i y_i$ şeklinde sonlu bir toplam olarak yazılabiliyor ve bu yazılış tek türlü oluyor ise $D = \{y_i\}_{i \in I}$ ye M 'nin bir tabanı denir. M modülüne de serbest modül denir.

Tanım1.1.36. S bir halka, M ve N de S-modül olsun. Bir $f : M \to N$ fonksiyonu her $m_1, m_2 \in S$ ve $\forall s \in S$ için

$i.\ f(m_1 + m_2) = f(m_1) + f(m_2)$

$ii.\ f(sm_1) = sf(m_1)$

koşulları sağlanıyorsa, f 'ye modül homomorfizması veya S-homomorfizması denir.

1.2. Kodlama Teorisi ile İlgili Tanımlar ve Teoremler

Kodlama teorisi ile ilgili ilk çalışmalar 1948'li yıllarda matematikçi ve elektrik mühendisi olan C.E.Shannon tarafından verilmiştir.AT&T telefon şirketinde çalışan ve enformasyon kuramının kurucusu olan Shannon iki kavram ortaya koymuştur.

i. Kanal Kapasitesi: Veri iletimi için hız sınırı.

ii. Entropi:Kayıpsız olarak veri sıkıştırması için sınır değer.

Veri(data): Semboller dizisi

Atılan bir para:YTYTYYYTTTT….

Dna dizisi: ATGCAATTGGCCC….

Her gün veri üretilir.Ve bu veriler gürültülü kanallar üzerinden alıcıya aktarılır.Gönderdiğimiz veri ile aldığımız veri arasında hatalar meydana gelmekte olup bu hataları düzeltebilmenin yolları aranır.

Gönder :01000000011111100110

Al :01110000000001100110

Yukarıda verilmiş olan örnekte bir veri dizisini gönderip alıcı kısmında hatalar olduğu görülmektedir.Gönderilen ile alınan aynı değil.O zaman ilk soru şu; Hatanın nerede meydana geldiği bulunabilir mi ve bu hatalar düzeltilebilir mi? Bu amaçla çalışılmış tüm teorilere genel olarak Hata Düzelten Kodlar Teorisi adı verilmektedir.Bu teorinin temellerinin atıldığı çalışma olarak 1948 yılında Shannon tarafından yayımlanan "A mathematical theory of communication" adlı makaledir.

Bu makalesinde gürültülü bir kanal üzerinden haberleşme yapmanın sınırlarını ve bu sınır için iletişimin nasıl yapılacağının kanıtlarını vermiştir.Makale ile hayatımıza kodlama teorisi ve bilgi güvenliği girmiş, oluşan hatalara da çözümler

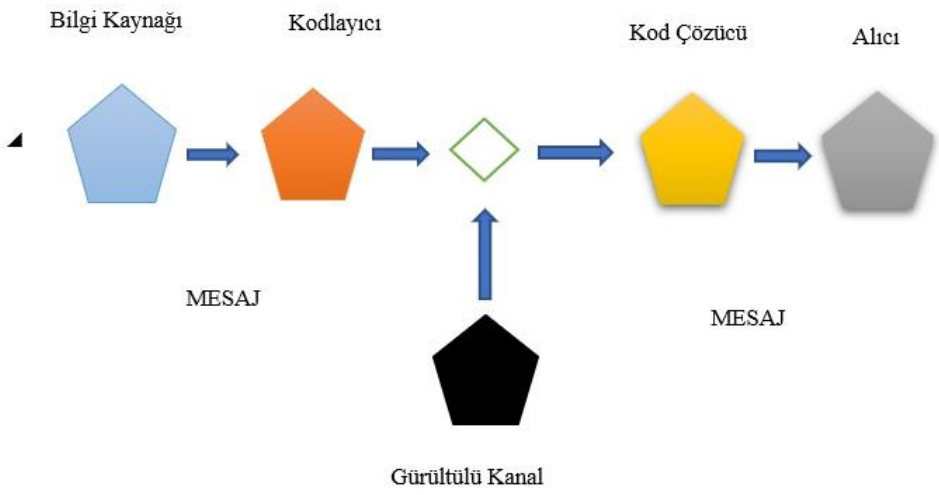
araştırılmıştır.Fakat bilgi güvenliği, kodlama teorisinin bir araştırma alanı değildir.Bilgi güvenliği kriptolojinin bir alanı olup,bu alan yapılan haberleşmenin gizliliğini sağlar.Bilgilerin ele geçirilmesi, gizli bilgilerin dinlenmesi veya değiştirilmesi gizlilik ve mahremiyet açısından önemli bir problem olup,bu problemlerin çözümünde iletilen verilerin şifrelenmesi yaygın olarak kullanılan bir yöntemdir. İletişimde amaç, gürültülü kanal üzerinden gönderilen mesajı doğruluğu yüksek bir olasılıkla alıcıya ulaştırmaktır.Mesajın iletimi için sonlu alfabe kümeleri kullanılır.Bu kümeler için cisim ya da sonlu halka alınabilir.İletilecek mesaj, oluşabilecek hatalardan korunmak üzere kodlanır. Kodlanan mesaj, kod sözcükleridir. Kanal bir telefon hattı, yüksek frekanslı bir radyo bağlantısı ya da uydu bağlantısı olabilir.Kar,yağmur,kızılötesi ışınlar,insan hatası sebebi ile mesaj iletimi sırasında hatalar meydana gelebilir.Kod çözücü, hata olup olmadığını kontrol eder, hata varsa düzeltir ve orijinal mesajı elde edip alıcıya gönderir. Tek amaç hata tespit etmek ya da düzeltmek değildir. Aynı zamanda maliyetinin az, bilgi aktarımı ve depolamasının hızlı olması istenmektedir.Daha az maliyetli ve en yüksek performanslı kodlar aranan özelliklerdendir.Bu kodlar ilk defa 1950'de Richard W. Hamming tarafından, hata düzelten kodları açıkça tanıtan çalışma olarak gösterilebilecek "Hata Tespit Eden ve Hata Düzelten Kodlar" başlıklı çalışmasını ortaya koymuştur.Günümüzde kodlama teorisinin bir sonucu olan toplamsal kodlar çalışılmakta olup bu kodlar kuantum hata düzeltme kodlarının bir sınıfı olduğu için ilgi çekmektedir. 1950-2021 yılları arasında kodlama teorisi adeta çığır açmış,Shannon'un vadettiği teorik sınırlara ulaşmak için çok önemli kodlar bulunmuştur.1960'larda bulunan Low-Density-Parity-Check (LDPC) kodları kanal kapasitesine yaklaşan kodlar olması sebebi ile kullanımda tercih edilme sebebi olmuştur.LDPC kodları bir takım eşlik denetim kodlarıdır.Daha sonra 1990'larda Turbo kodları keşfedilmiştir.Nihai hedef Shannon kapasite sınırına erişmektir.LDPC ve Turbo kodları tekniğin mevcut durumunu temsil eden iki kodlama yöntemidir.Fakat bu kodlar da ilerleyen yıllarda yeterli olmamış,içinde unsurlar barındırdığı için yeni bir tür kanal kodlama algoritması olan kutupsal kodlar bulunmuştur.Kutupsal kodlar da bir çeşit eşlik denetim kodudur. Prof Dr.Erdal Arıkan tarafından bulunan bu kodlar,Shannon kapasitesine ulaştığı matematiksel olarak kanıtlanabilen ilk ve halen kullanılan tek kodlama yöntemidir.Kutupsal kodlar 2016 yılında 5G standardına kabul edilmiştir.Pratik bakımdan önemi,kanal kapasitesine

erişilir olmaları,düşük karmaşıklı kodlama ve kod çözme algoritmasına sahip olmalarıdır.Kutupsal kodlar,5G çalışmalarında kontrol kanalı olarak kullanılmaktadır.

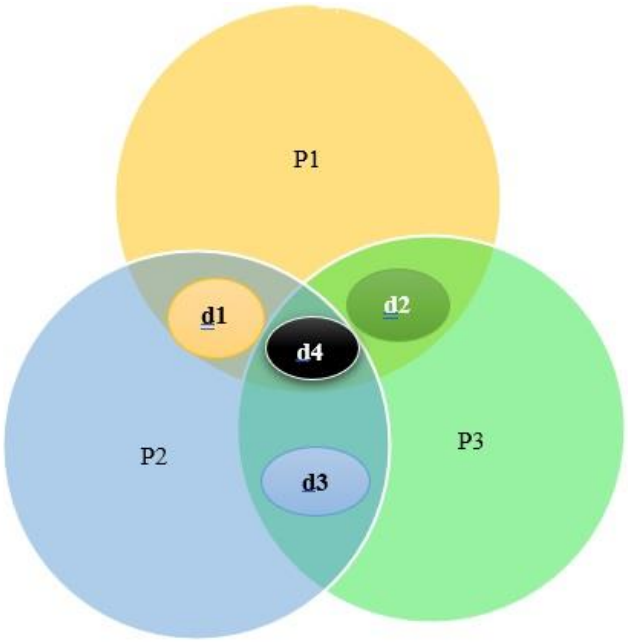
LDPC kodları yüksek veri hızı gerektiğinde tercih edilmektedir.

Fakat kutupsal kodlar düşük hacimli yüksek güvenirlikli uygulamalar için tercih edilmektedir.Turbo kodları ise karmaşık ve fazla enerji harcadıkları için 5G'ye alınmamıştır.Her geçen gün kodlama teorisi geliştirilmekte olup hem teknolojinin ilerlemesi hem insanlığın gelişmesi için önemli kodlar bulunmaktadır.Bir dijital haberleşme sisteminin ana diyagramı ve tek hata düzelten hamming kodunun çalışma yapısı ayrıca şeması aşağıda verilmiştir.

'Haberleşmenin temel problemi bir noktada meydana gelen bir mesajı (rastlantısal seçilen bir mesaj) başka bir noktaya taşımaktır.' diyor sayısal haberleşmenin kurucusu Claude Elwood Shannon.



Şekil 1.1. Shannon haberleşme modeli



Şekil 1.2. Tek hata düzelten Hamming kodu

d_1, d_2, d_3, d_4 yollanacak olan orijinal veriler olsun. Ve bu verilere 3 eşlik denetim biti eklensin.

$$p_1 = d_1 + d_2 + d_4 \equiv \mathrm{mod}(2)$$
$$p_2 = d_1 + d_3 + d_4 \equiv \mathrm{mod}(2)$$
$$p_3 = d_2 + d_3 + d_4 \equiv \mathrm{mod}(2)$$

4 orijinal bite, 3 yeni bit daha eklenince 7 bit elde edilmiş olur. Buradan varsayalım ki p_1 bloğunda hata meydana gelsin. O zaman eşlik denetimi yardımıyla;

$$p_1 + d_1 + d_2 + d_4 \equiv 0(\mathrm{mod}\,2)$$

hata meydana gelirse $\Rightarrow$ $p_1 + d_1 + d_2 + d_4 \equiv 1(\mathrm{mod}\,2)$ elde edilir.Bu şekilde tüm bloklar eşlik denetimi ile kontrol edildiğinde p_1 bloğunda hata meydana geldiği anlaşılır.Bu kod tek hataları düzeltir.Tek hata düzelten hamming kodu 2 hatayı sezebilir fakat düzeltemez. Kodlama oranı $R = 4/7$ dir.

1.2.1. Lineer kodlar

Tanım 1.2.1.1. V kümesi, p asal ve $q = p^k$ olmak üzere q elemanlı F_q cisminin elemanları ile skaler çarpım işlemlerinin tanımlı olduğu boştan farklı bir küme olsun. Eğer aşağıdaki koşullar sağlanıyor ise V kümesine F_q cismi üzerinde bir vektör uzayı denir.

i. V kümesi toplama işlemine göre değişmeli bir gruptur.

ii. $\forall a \in F_q$ ve $\forall u \in V$ için $au \in V$

iii. $\forall a \in F_q$ ve $\forall u, v \in V$ için $a(u+v) = au + av$

iv. $\forall a, \ell \in F_q$ ve $\forall u \in V$ için $(a+\ell)u = au + \ell u$

v. $\forall a, \ell \in F_q$ ve $\forall u \in V$ için $(a\ell)u = a(\ell u)$

vi. $1_{F_q}, F_q$ cisminin birim elemanı olmak üzere $\forall u \in V$ için $1_{F_q} u = u$

olur.

Teorem 1.2.1.1. F_q cismi üzerindeki V vektör uzayının boştan farklı bir C alt kümesinin V'nin alt vektör uzayı olması için gerek ve yeter şart $\forall x, y \in C$ ve $\forall a, \ell \in F_q$ için $ax + \ell y \in C$ olmasıdır.

Tanım 1.2.1.2. F_q cismi üzerinde V bir vektör uzayı ve $D = \{d_1, d_2, d_3, ..., d_t\}$ vektörler kümesi V'nin boş kümeden farklı bir alt kümesi olsun.

$$< \mathrm{D} > = \left\{ \beta_1 d_1, \beta_2 d_2, \beta_3 d_3, ..., \beta_t d_t : \beta_i \in F_q, 1 \le i \le t \right\}$$

kümesi V 'nin bir alt uzayıdır ve bu kümeye D 'nin gerdiği (ürettiği) alt uzay denir.

Verilen bir $C \subseteq V$ alt vektör uzayı ve $D \subseteq C$ alt kümesi için eğer C 'deki her eleman D 'deki elemanların bir lineer kombinasyonu şeklinde yazılabiliyorsa yani $\langle D \rangle = C$ oluyor ise D 'ye C'nin üreteç kümesi (geren kümesi) denir.

Tanım 1.2.1.3. F_q cismi üzerinde V bir vektör uzayı ve $\{v_1, v_2, ..., v_t\} \subseteq V$ olsun. Eğer ; $\chi_1 v_1 + \chi_2 v_2 + ... + \chi_t v_t = 0$ eşitliğini sağlayan hepsi aynı anda sıfırolmayan $\chi_1, \chi_2, ..., \chi_t$ sabitleri varsa $\{v_1, v_2, ..., v_t\}$ kümesine lineer bağımlı küme denir. Eğer bu eşitlik yalnızca $\chi_1 = \chi_2 = ... = \chi_t = 0$ için sağlanıyor ise $\{v_1, v_2, ..., v_t\}$ kümesine lineer bağımsız küme denir.

Tanım 1.2.1.4. F_q cismi üzerinde V bir vektör uzayı $U = \{u_1, u_2, ..., u_k\}$ vektörler kümesi V 'nin boş kümeden farklı bir alt kümesi olsun. Eğer U kümesi lineer bağımsız ve $\langle U \rangle = V$ ise U 'ya V vektör uzayının bir bazı denir.

Uyarı 1.2.1.1. Eğer $U = \{u_1, u_2, ..., u_k\}$ kümesi V vektör uzayının bir bazı ise V 'deki her vektör U 'daki vektörlerin lineer kombinasyonu olarak tek türlü yazılabilir.

Uyarı 1.2.1.2. F_q cismi üzerindeki V vektör uzayının birden fazla bazı olabilir. Fakat bütün bazlardaki eleman sayıları aynıdır.

Tanım 1.2.1.5. Bir V vektör uzayının herhangi bir bazındaki eleman sayısına V 'nin boyutu denir.

Tanım 1.2.1.6. F_q^n de $y = (y_1, y_2, ..., y_n)$ ve $z = (z_1, z_2, ..., z_n)$ iki vektör olmak üzere y ve z 'nin iç çarpımı ;

$$y.z = y_1 z_1 + y_2 z_2 + ... + y_n z_n$$

olarak tanımlanır.

Not. Bu çarpım öklid iç çarpımı olarak da bilinir.

Tanım 1.2.1.7. A alfabesi üzerindeki aynı uzunluktaki n – liler x ve y olsun. x ve y nin farklı olan bileşenlerinin sayısına x ve y arasındaki Hamming uzaklık denir ve $d(x,y)$ ile gösterilir.

Teorem 1.2.1.2. A alfabesi üzerindeki n – lilerin kümesinden alınan x, y, z için Hamming uzaklık fonksiyonu aşağıda verilen özelliklerle birlikte (A^n, d) bir metrik uzay olur.

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

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

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

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

Tanım 1.2.1.8. En az iki kod söz içeren bir C kodu için C kodunun minimum uzaklığı $d(C) = \min\{d(x,y) : x, y \in C, x \neq y\}$ olarak tanımlanır.

Tanım 1.2.1.9. C kodunun bir kod sözü $x = (x_1, x_2, ..., x_n)$ olmak üzere x kod sözünün sıfırdan farklı bileşen sayısına x 'in ağırlığı denir ve $w(x)$ ile gösterilir. Bir C kodunun minimum ağırlığı C de ki sıfırdan farklı kod sözlerin en küçük ağırlığıdır ve $w(C)$ ile gösterilir.

Bu tanımlamalardan sonra lineer kod tanımı aşağıdaki şekilde verilebilir.

Tanım 1.2.1.10. $C \subseteq F_q^n$ kodu eğer F_q^n vektör uzayının bir k boyutlu bir alt vektör uzayı ise C'ye F_q üzerinde n uzunluğunda k boyutlu bir lineer kod veya $[n,k]$ kodu denir. Eğer C kodunun minimum uzaklığı $d(C)=d$ ise bu lineer kod $[n,k,d]$kodu olarak gösterilir. n,k ve d sayılarına da lineer kodun parametreleri denir.

Teorem 1.2.1.3. Eğer C bir lineer kod ise $d(C)=w(C)$'dir.

Tanım 1.2.1.11. n uzunluğunda M elemanlı d minimum uzaklığa sahip bir C kodu (n,M,d) kodu olarak gösterilir. Buradaki n,M,d sayılarına da C kodunun parametreleri denir.

Tanım 1.2.1.12. F_q üzerinde C bir $[n,k]$ kodu olsun. Satırları C için bir baz oluşturan $k\times n$ boyutundaki bir G matrisine C'nin üreteç matrisi denir. Başka bir ifade ile $C=\{xG : x\in F_q^k\}$ olarak tanımlanabilir.

Tanım 1.2.1.13. C bir $[n,k]$ kodu olsun. C kodunun duali

$C^{\perp}=\{x\in F_q^n : x.c=0, \forall c\in C\}$ kümesi olarak tanımlanır.

Teorem 1.2.1.4 Eğer $G=(I_k \mid A)$, C $[n,k]$ – kodunun standart formdaki üreteç matrisi ise o zaman C' nin kontrol matrisi $H=(-A^T \mid I_{n-k})$ dir.

Tanım 1.2.1.14. Herhangi bir $\dot{c}\in C$ ve $\dot{c}\neq c$ için $d_L(c,\dot{c})$ iki kodsöz arasındaki Lee uzaklık olmak üzere $d_L(c,\dot{c})=w_L(c-\dot{c})$ ifadesine C'nin Lee uzaklığı denir. $d_L=\min d_L(c,\dot{c})$ ifadesine de C 'nin minimum Lee uzaklığı denir.

Tanım 1.2.1.15. S üzerinde n uzunluğunda lineer bir kod C olsun. Herhangi bir $c=(c_0,c_1,.....,c_{n-1})$ kodsözü için c 'nin Lee ağırlığı $w_L=\sum_{i=0}^{n-1} w_L(c_i)$ olarak tanımlanmaktadır.

Tanım 1.2.1.16. S^n'de n uzunluğundaki bir C kodu için, C 'nin üreteçlerinin en küçük sayısına rank denir. $Rank(C)$ ile gösterilir.

1.2.2 Devirli Kodlar

İlk olarak Eugene Prange tarafından 1957'de çalışılan lineer kodların da önemli bir sınıfı olan devirli kodlar, zengin bir cebirsel yapıya sahiptir. Devirli kodlar oldukça çok çalışılmış ve genişletilmiştir.Reed Solomon ve BCH kodları bu sınıfta çalışılmış önemli devirli kod ailelerindendir.1960 yılında bulunan Reed Solomon kodları,ikili olmayan BCH kodlarının önemli bir alt sınıfıdır.Reed Solomon kodları CD'lerde, veri depolama sistemlerinde yoğun olarak kullanılmıştır. Günümüzde ise önemli uygulama alanları mevcut olmakta bunlar; bellek elemanları,kablosuz haberleşme, uydu haberleşmesi ve modemler olmak üzere birçok yerde kullanılmaktadır. Bu sistemleri anlayabilmek için öncelikle devirli kodun tanımı verilsin.

Tanım 1.2.2.1 $C\subseteq F_q^n$ için $(c_0,c_1,c_2,.....,c_{n-1})\in C$ iken $(c_{n-1},c_0,c_1,c_2,.....,c_{n-2})\in C$ oluyorsa C lineer koduna devirli kod denir.

$$\pi \ : \ F_q^n \to \frac{F_q[x]}{x^{n-1}}$$

$(c_0,c_1,.....,c_{n-1})\to(c_0+c_1x+.....+c_{n-1}x^{n-1})$ şeklinde verilen dönüşüm ile

$C\subseteq F_q^n$ de ki $(c_0,c_1,.....,c_{n-1})$ kodsözü $F_q[x]/(x^{n-1})$ de ki polinomla ilişkilendirilebilir.

Teorem 1.2.2.1. Ω yukarıda tanımlanan lineer dönüşüm olsun. F_q^n nin boştan farklı C alt kümesinin devirli kod olması için gerek ve yeter koşul $\Omega(C)$ nin $F_q[x]/(x^{n-1})$ nin ideali olmasıdır.

Teorem 1.2.2.2. I, $F_q[x]/(x^{n-1})$ de sıfırdan farklı bir ideal olsun. $g(x)$, I 'da sıfırdan farklı derecesi en küçük olan monik polinom olsun. O zaman $g(x)$, I 'nın üretecidir. Ve $g(x), x^{n-1}$ 'i böler.

Tanım 1.2.2.2 $F_q[x]/(x^{n-1})$ in sıfırdan farklı I idealinde derecesi en küçük olan tek bir monik polinoma I nın üreteç polinomu denir. C devirli kodu için $\Omega(C)$ nin üreteç polinomuna C nin üreteç polinomu denir.

Teorem 1.2.2.3. $F_q[x]/(x^{n-1})$ in idealinin üreteç polinomu $g(x)$ olsun. Eğer $g(x)$ in derecesi $n-t$ ise devirli kodun boyutu t dir.

Teorem 1.2.2.4. $der(g(x))=n-t$ olmak üzere F_q^n de ki C devirli kodunun üreteç polinomu $g(x)=g_0+g_1x+.....+g_{n-t}x^{n-t}$ olsun. O zaman C nin üreteç matrisi

$$G=\begin{pmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{t-1}g(x) \end{pmatrix}=\begin{pmatrix} g_0 & g_1 & \dots & g_{n-t} & 0 & 0 & \dots & 0 \\ 0 & g_0 & g_1 & \dots & g_{n-t} & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & g_0 & g_1 & \dots & 0 & 0 \end{pmatrix}$$ şeklindedir.

Örnek 1.2.2.1. $C_1=\{(0,0,0),(1,0,1),(0,1,1),(1,1,0)\}\subseteq F_2^3$,

$C_2=\{(0,1,1,2),(2,0,1,1),(1,2,0,1),(1,1,2,0)\}\subseteq F_3^4$,

$C_3=\{(1,1,1,1,1)\}\subseteq F_2^5$

kodları verilsin.

C_1 bir devirli koddur.Çünkü C_1 kodundaki her bir kodsözün bir devir kayması ile oluşan eleman yine C_1 kodunun kod sözüdür.Fakat C_2 ve C_3 kodları bir devirli kod örneği değildir.Çünkü lineer kod değillerdir.

BÖLÜM 2. $Z_4\left(Z_4+vZ_4\right)-$ LİNEER KODLAR

Lineer kodların, kodlama teorisinde önemli bir yeri vardır.Lineer kodlarda vektör uzayının cebirsel özellikleri kullanıldığından kodlama teorindeki çoğu çalışma lineer kodlar üzerinedir.Kodların sistematik bir şekilde dizayn edilebilmesi için,dekodlama ve kodlamasının daha kolay yapılabilmesinde ve bu kodların yoğun kullanılmasındaki önemi kazanmasında lineer kodların büyük bir rolü vardır. Bu bölümde $v^2=1$ olmak üzere $Z_4Z_4[v]$ halkasının yapısı tanıtılacaktır.

2.1. $v^2=1$; $Z_4(Z_4+vZ_4)$ - Halkası

$v^2=1$ olmak üzere, $R=Z_4+vZ_4=Z_4[v]$ halkasını temsil etsin.

$Z_4+vZ_4=\{0,1,2,3,v,2v,3v,1+v,2+v,3+v,1+2v,1+3v,2+2v,2+3v,3+2v,3+3v\}$ halkası 16 elemanlıdır.

$\tau=\tau_i+v\tau_j$, Z_4+vZ_4 halkasının birimsel elemanlarını ifade etsin. Bu halkanın birimsel elemanlarının kümesi

$\{1,3,v,3v,1+2v,2+v,2+3v,3+2v\}$ dir.

Maksimal ideali $<2v,1+v>$ dir.

Böylece R tek maksimal ideale sahip olduğundan lokal halkadır [15].

$Z_4Z_4[v]=\{(u,\hat{u});u\in Z_4,\hat{u}\in R\}$ şeklinde tanımlanan $Z_4Z_4[v]$ halkası bilinen çarpma işlemi altında kapalı olmadığından R-modül değildir. Bu nedenle aşağıdaki tanımda verilen μ dönüşümü kullanılarak yeni bir çarpma işlemi tanımlanacaktır. Böylece bu halkanın R-modül olması sağlanacaktır.

Tanım 2.1.1. $a,b \in Z_4$, $a+vb \in R$ olmak üzere,

$\mu : R \to Z_4$

$a+vb \to a+b$ olacak şekilde tanımlansın.

$\forall a+vb, c+vd \in R$ için

$$\mu((a+vb)+(c+vd)) = \mu(a+c+v(b+d))$$
$$= a+c+(b+d) = a+c+b+d = (a+b)+(c+d)$$
$$= \mu(a+vb)+\mu(c+vd)$$

$$\mu((a+vb)(c+vd)) = \mu(ac+bd+v(ad+bc))$$
$$= ac+bd+ad+bc = a(c+d)+b(d+c)$$
$$= a(c+d)+b(c+d) = (a+b)(c+d)$$
$$= \mu(a+vb)\mu(c+vd)$$

olduğundan μ dönüşümü bir halka homomorfizmasıdır.

2.2. $Z_4Z_4[v]$ – Lineer Kodların Yapısı

Tanım 2.2.1. Herhangi bir $\tilde{r} \in R$ ve $(u,\hat{u}) \in Z_4R$ için $\tilde{r} * (u,\hat{u}) = (\mu(\tilde{r})u, \tilde{r}\hat{u})$ olarak tanımlansın. Bu çarpma $Z_4^{\alpha}R^{\beta}$ halkasına genelleştirilerek herhangi bir $\tilde{r} \in R$ ve

$w = (u_0, u_1, ..., u_{\alpha-1}, \hat{u}_0, \hat{u}_1, ..., \hat{u}_{\beta-1}) \in Z_4^{\alpha}R^{\beta}$ için

$\tilde{r}w = (\mu(\tilde{r})u_0, \mu(\tilde{r})u_1, ..., \mu(\tilde{r})u_{\alpha-1}, \tilde{r}\hat{u}_0, \tilde{r}\hat{u}_1, ..., \tilde{r}\hat{u}_{\beta-1})$ şeklindedir.

Önerme 2.2.1. $Z_4^{\alpha}R^{\beta}$ halkası yukarıda tanımlanan çarpma işlemi ile bir R-modüldür.

İspat: $\forall r, \tilde{r} \in R$ ve

$\forall w=(u_0,u_1,...,u_{\alpha-1},\hat{u}_0,\hat{u}_1,....,\hat{u}_{\beta-1})$, $\breve{w}=(u_0',u_1',....,u_{\alpha-1}',\bar{u}_0,\bar{u}_1,.....,\bar{u}_{\beta-1})\in Z_4^{\alpha}\times R^{\beta}$ için

i. $r(w+\breve{w})=$ $r(u_0+u_0'+.....+u_{\alpha-1}+u_{\alpha-1}',\hat{u}_0+\bar{u}_0+.....+\hat{u}_{\beta-1}+\bar{u}_{\beta-1})$

$=(\mu(r)(u_0+u_0')+.....+\mu(r)(u_{\alpha-1}+u_{\alpha-1}'),r(\hat{u}_0+\bar{u}_0)+...+r(\hat{u}_{\beta-1}+\bar{u}_{\beta-1}))$

$=(\mu(r)u_0,.....,\mu(r)u_{\alpha-1},r\hat{u}_0,....,r\hat{u}_{\beta-1})$ + $(\mu(r)u_0',....,\mu(r)u_{\alpha-1}',r\bar{u}_0,.....,r\bar{u}_{\beta-1})$

$=rw+r\breve{w}$

ii. $(r+\tilde{r})w=$ $(\mu(r+\tilde{r})u_0,....,\mu(r+\tilde{r})u_{\alpha-1},(r+\tilde{r})\hat{u}_0,....,(r+\tilde{r})\hat{u}_{\beta-1})$

$=((\mu(r)+\mu(\tilde{r}))u_0,....,(\mu(r)+\mu(\tilde{r}))u_{\alpha-1},r\hat{u}_0+\tilde{r}\hat{u}_0,.....,r\hat{u}_{\beta-1}+\tilde{r}\hat{u}_{\beta-1})$

$=(\mu(r)u_0,....,\mu(r)u_{\alpha-1},r\hat{u}_0,.....,r\hat{u}_{\beta-1})+(\mu(\tilde{r})u_0,.....,\mu(\tilde{r})u_{\alpha-1},\tilde{r}\hat{u}_0,....,\tilde{r}\hat{u}_{\beta-1})$

$=rw+\tilde{r}w$

iii. $r(\tilde{r})w=$ $r(\mu(\tilde{r})u_0,....,\mu(\tilde{r})u_{\alpha-1},\tilde{r}\hat{u}_0,....\tilde{r}\hat{u}_{\beta-1})$

$=(\mu(r)\mu(\tilde{r})u_0,....,\mu(r)\mu(\tilde{r})u_{\alpha-1},r\tilde{r}\hat{u}_0,.....,r\tilde{r}\hat{u}_{\beta-1})$

$=(\mu(r\tilde{r})u_0,.....,\mu(r\tilde{r})u_{\alpha-1},r\tilde{r}\hat{u}_0,.....,r\tilde{r}\hat{u}_{\beta-1})$

$=(r\tilde{r})w$

iv. Tanım 2.2.1 den $\mu(1)=1$ dir. $\forall w=(u_0,.....,u_{\alpha-1},\hat{u}_0,.....,\hat{u}_{\beta-1})\in Z_4^{\alpha}R^{\beta}$ için,

$1_R w=1_R(u_0,.....,u_{\alpha-1},\hat{u}_0,.....,\hat{u}_{\beta-1})$

$=(\mu(1_R)u_0,.....,\mu(1_R)u_{\alpha-1},\hat{u}_0,.....,\hat{u}_{\beta-1})$

$=(u_0,....,u_{\alpha-1},\hat{u}_0,.....,\hat{u}_{\beta-1})$

$=w$

elde edilir. Böylece $Z_4{}^{\alpha}R^{\beta}$ halkası yukarıda tanımlanan çarpma işlemi ile bir R-modüldür.

Tanım 2.2.2. $Z_4^{\alpha}R^{\beta}$ nın boş olmayan bir C alt kümesi $Z_4^{\alpha}R^{\beta}$ nın $R-$ alt modülü ise C' ye Z_4R-lineer kod denir.

Not. Kolayca görülür ki $\alpha=0$ ise R üzerinde bir lineer kod $\beta=0$ ise Z_4 üzerinde bir lineer koddur.

Önerme 2.2.2. $R=Z_4+vZ_4$ olsun. τ 'nin R de birimsel eleman olması için gerek ve yeter şart $\mu(\tau)$ nin Z_4 de birimsel eleman olmasıdır.

İspat: $\tau_1,\tau_2\in Z_4$ ve $\tau=\tau_1+v\tau_2$ olmak üzere τ, R 'de birimsel eleman olsun. O zaman $\exists k\in R$ vardır ve $\tau.k=k.\tau=1$ olsun. $\mu(k.\tau)=\mu(\tau.k)=1$ dir. μ halka homomorfizması ve $\mu(1)=1$ olduğundan $\mu(k).\mu(\tau)=1=\mu(\tau).\mu(k)$ olarak bulunur. Böylece $\mu(\tau)$, Z_4 de birimsel elemandır.

$\tau=2+v$ olsun. $\mu(\tau)=\tau_1+\tau_2$, Z_4 de birimsel eleman olsun. Şimdi $\tau=\tau_1+v\tau_2$, R 'de birimsel eleman olduğu gösterilmelidir. Yani, $\tau.\tau^{-1}=1$ olduğu gösterilmelidir.

Buradan ; $\tau.\tau^{-1}=(\tau_1+v\tau_2)(\tau_1+v\tau_2)^{-1}$

$=(\tau_1+v\tau_2)(\tau_1^{-1}+v\tau_3)=\tau_1\tau_1^{-1}+\tau_2\tau_3+v(\tau_1\tau_3+\tau_2\tau_1^{-1})$.....$(*)$ olarak

bulunur. $\mu(\tau)$, Z_4 de birimsel eleman olduğundan $(\tau_1+\tau_2)(\tau_1+\tau_2)^{-1}=1$ dir.Yani,

$(\tau_1+\tau_2)(\tau_1^{-1}+\tau_3)=\tau_1\tau_1^{-1}+\tau_1\tau_3+\tau_2\tau_1^{-1}+\tau_2\tau_3=1$ dir. $\tau_1\tau_1^{-1}+\tau_2\tau_3=1-\tau_1\tau_3-\tau_2\tau_1^{-1}$

eşitliği $(*)$ da yerine yazılır ve düzenlenirse, $\tau.\tau^{-1}=1+(v-1)(\tau_1\tau_3+\tau_2\tau_1^{-1})$ elde

edilir. $\tau_3 = \dfrac{-\tau_2\tau_1^{-1}}{\tau_1} = -\tau_2(\tau_1^{-1})^{-1}$ olmak üzere $\tau.\tau^1 = 1$ dir.Böylece $\tau = \tau_1 + v\tau_2$, R 'de birimsel elemandır.

BÖLÜM 3. $Z_4\left(Z_4+vZ_4\right)-$ DEVİRLİ KODLAR

Lineer kodların önemli bir sınıfı devirli kodlar ve sabit devirli kodlardır.Kodlama teorisi her ne kadar cisimlerin yapısının incelenmesi ile başlamışsa da sonraları halkalara genişletilmiş ve çeşitli halkalar üzerinde çalışmalar yapılmıştır. Son yıllarda değişmeli ve değişmeli olmayan halkalar üzerinde toplamsal devirli kodların çalışıldığı görülür.[16] çalışmasında sonlu değişmeli zincir halkaları üzerinde toplamsal devirli kodlar çalışılmıştır.[17] Galois Ring 'in dikkat çeken yapısından dolayı bu halka üzerinde de toplamsal kodlar araştırılmıştır. [18] $v^2=0,$ için $Z_2Z_2[v]$ toplamsal devirli ve sabit devirli kodları üzerinde Aydoğdu ve ark. çalışma yapmıştır.[19] Daha sonra $v^2=0$ olmak üzere $Z_4Z_4[v]-$ toplamsal devirli Ve toplamsal sabit devirli kodları Islam ve ark. tarafından çalışılmıştır.[20] Parçalı devirli kodların yapısı toplamsal devirli kodlar üzerinde incelenmiştir.[21] Aydoğdu doktora tezinde, bazı özel modüller üzerinde toplamsal kodları incelemiştir.[22] Kuantum hata düzeltme kodları için bir kodun duali önem arzettiğinden toplamsal kodlar ve onların dualleri $Z_pZ_{p^k}$ halkası üzerinde Minja ve ark. tarafından çalışılmıştır.[23]Abualrup ve ark. F_2F_4 toplamsal devirli kodları tarafından türetilen optimal ikili kodları çalışmıştır.[24] $Z_pZ_p[v]$ toplamsal kodları üzerindeki bazı sonuçları Diao ve ark. tarafından çalışılmıştır.[25] Z_2Z_4 toplamsal kodunun çekirdeği ve boyutu Borges ve ark. tarafından incelenmiştir.

Bu bölümde ise toplamsal devirli,toplamsal sabit devirli ,parçalı devirli tanımları yapılacaktır. Sonrasında ise β tek ve $v^2=1$ olmak üzere $Z_4\left(Z_4+vZ_4\right)-$ toplamsal devirli kodun üreteç polinomu ve en küçük geren kümesi verilecektir. En son olarak $Z_4(Z_4+vZ_4)-$ toplamsal devirli kodun gray görüntülerine bakılmıştır.

3.1. Temel Tanımlar ve Teoremler

Tanım 3.1.1. C bir $Z_4Z_4[v]-$toplamsal kodu ve uzunluk (α,β) olmak üzere;

i. C, $Z_4^{\alpha}\times R^{\beta}$ nın $R-$alt modülüdür. (ispatı teorem 3.1.1.'de verilmiştir.)

ii. Herhangi bir $z=(u_0,u_1,....,u_{\alpha-1},\hat{u}_0,\hat{u}_1,.....,\hat{u}_{\beta-1})\in Z_4^{\alpha}\times R^{\beta}$ için

$\sigma(z)=(u_{\alpha-1},u_0,.....,u_{\alpha-2},\hat{u}_{\beta-1},\hat{u}_0,.....,\hat{u}_{\beta-2})\in Z_4^{\alpha}\times R^{\beta}$ şeklinde bir devirsel öteleme operatörü tanımlansın. Z_4R-lineer C kodu σ devirli öteleme operatörü altında sabit kalıyorsa $\sigma(C)=C$ şartlarını sağlayan C koduna devirli kod denir.

Devirli kod çalışmalarında, kod sözleri polinomlar ile temsil ederek koda daha fazla cebirsel özellik kazandırılabilir.

Burada da $Z_4^{\alpha}\times R^{\beta}$ halkasının elemanları ile

$R_{\alpha,\beta}=Z_4[x]\Big/\left(x^{\alpha}-1\right)\times R[x]\Big/\left(x^{\beta}-1\right)$ halkasının elemanları arasında aşağıdaki gibi bir dönüşüm tanımlanabilir.

$$Z_4^{\alpha}\times R^{\beta}\rightarrow R_{\alpha,\beta}$$

$$(u_0,u_1,....,u_{\alpha-1},\hat{u}_0,\hat{u}_1,.....,\hat{u}_{\beta-1})\rightarrow(u_0+u_1x+....+u_{\alpha-1}x^{\alpha-1},\hat{u}_0+\hat{u}_1x+....+\hat{u}_{\beta-1}x^{\beta-1})=\left(u(x),\hat{u}(x)\right)$$

Tanım 3.1.2. $\tilde{r}(x)=\tilde{r}_0+\tilde{r}_1x+....+\tilde{r}_tx^t\in R[x]$ ve $\left(u(x),\hat{u}(x)\right)\in R_{\alpha,\beta}$ elemanları için $\tilde{r}(x)*\left(u(x),\hat{u}(x)\right)=\left(\mu(\tilde{r}(x))u(x),\tilde{r}(x)\hat{u}(x)\right)$ çarpımı tanımlanabilir.

Teorem 3.1.1. $C\subseteq R_{\alpha,\beta}$ kodunun Z_4R-devirli kod olması için gerek ve yeter şart C'nin $R_{\alpha,\beta}$'nın bir $R[x]-$alt modülü olmasıdır.

İspat. C, Z_4R-devirli kod ve $c(x)=(u(x),\hat{u}(x))\in C$ olsun. C, $R_{\alpha,\beta}$' nın bir alt grubu olduğundan $\bar{c}(x),\tilde{c}(x)\in C$ için $\bar{c}(x)-\tilde{c}(x)\in C$ olduğu açık olup C, Z_4R-devirli kod olduğundan $x*c(x)\in C$'dir. Devam edilirse $t\geq 0$ için $x^t*c(x)\in C$ dir.C kodunun lineerliğini kullanacak olursak $\forall k(x)\in R[x]$ için de $k(x)*c(x)\in C$ elde edilir.Görülmüş olur ki C kodu $R_{\alpha,\beta}$'nın bir $R[x]-$alt modülüdür.

Tersine , C kodu $R_{\alpha,\beta}$' nın bir $R[x]-$alt modülü olsun. Alt modül şartlarından dolayı C, $R_{\alpha,\beta}$'nın alt grubu olup $c(x)\in C$ ve $x\in R[x]$ için $x*c(x)\in C$ olacağından C kodu Z_4R-devirli koddur.

Tanım 3.1.3. $n=s.l$ ve C, $Z_4^{\alpha}\times R^{\beta}$ kümesinin bir alt kümesi olmak üzere

i. C, $Z_4^{\alpha}\times R^{\beta}$ nın bir alt uzayı,

ii. $\eta: Z_4^n\to Z_4^n$ quasi(parçalı) devirli öteleme operatörü olmak üzere ,

iii. $\eta(a_0\mid a_1\mid\ldots\mid a_{s-1})=(\sigma(a_0)\mid\sigma(a_1)\mid\ldots\mid\sigma(a_{s-1}))$, $a_i\in Z_4^l$ ve

$i=0,1,2,\ldots..,s-1$ için şartlar sağlanıyorsa C'ye $n=s.l$ uzunluğunda l indeksli parçalı devirli kod denir. $\eta(C)=C$'dir.

Not. $l=1$ alınırsa devirli kod ile parçalı devirli kod çakışır.

Tanım 3.1.4. $n_1,\ldots,n_r\in Z$ ve $R_i=\dfrac{Z_4[x]}{\langle x^{n_i}-1\rangle}$, $i=1,2,\ldots..,r$ olmak üzere herhangi bir $Z_4[x]-$modülü'n $Z_4[x]-$alt modülü $\bar{R}:=R_1\times R_2\times\ldots..\times R_r$ ye genelleştirilmiş parçalı devirli kod (GQC) denir.

i. Blok uzunluğu: $n_1,n_2,\ldots..,n_r$'dir.

ii. Eğer $n_1 = n_2 = ... = n_r$ ise quasi (parçalı) kod adını alır. Uzunluğu rn 'dir.

iii. Eğer $r = 1$ ise devirli kod adını alır.Uzunluğu n 'dir.

3.2. $Z_4(Z_4 + vZ_4) -$ Devirli Kodun Üreteç Polinomu ve En Küçük Geren Kümesi

Bu bölümde $Z_4R -$ devirli kodun üreteçleri hakkında bilgi verilip,geren kümeleri oluşturulacaktır.Bölüm boyunca C kodu, $Z_4R -$ devirli kod ve β pozitif tek tamsayı olarak alınmıştır.

Teorem 3.2.1 n pozitif tek tamsayı olmak üzere C, $Z_4 + vZ_4$ üzerinde n uzunluğunda devirli bir kod olsun. $Z_4 + vZ_4$ üzerindeki $g_2(x)$ polinomu ve Z_4 üzerindeki devirli kodların üreteç polinomları $g_1(x)$ ve $g_3(x)$ polinomları için $C = \langle g_1(x) + (1+v)g_2(x), (1+v)g_3(x) \rangle$ şeklindedir.[15]

Hem C kodu hem de $R[x] \big/ \langle x^\beta - 1 \rangle$ halkası $R_{\alpha,\beta}$'nın bir $R[x] -$ alt modülü olduğundan dönüşümü tanımlayalım;

$$\Psi : C \to R[x] \big/ \langle x^\beta - 1 \rangle$$

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

şeklinde bir $R[x] -$ modül homomorfizması tanımlanır.

Burada Ψ homomorfizmasının çekirdek kümesi

$$Çek\Psi = \left\{ (f(x) \mid 0) \in C : f(x) \in Z_4[x] \big/ \langle x^\alpha - 1 \rangle \right\}$$

olup C'nin bir alt modülüdür.

$$I = \left\{ f(x) \in {Z_4[x]}/{\langle x^\alpha - 1\rangle} : (f(x) \mid 0) \in \text{Çek}\Psi \right\}$$

şeklinde tanımlanan I kümesi ${Z_4[x]}/{\langle x^\alpha - 1\rangle}$ halkasının bir idealidir. Başka bir eyişle ${Z_4[x]}/{\langle x^\alpha - 1\rangle}$ halkasında devirli kod olup $f(x) \mid \langle x^\alpha - 1\rangle$ olacak şekilde $I = \langle f(x)\rangle$ dir. Herhangi bir $(t(x) \mid 0) \in \text{Çek}\Psi$ elemanı için $t(x) \in I$ olduğundan $t(x) = k(x) f(x)$ olacak şekilde $k(x) \in {Z_4[x]}/{\langle x^\alpha - 1\rangle}$ polinomu vardır.

Dolayısıyla

$(t(x) \mid 0) = (k(x) f(x) \mid 0) = k(x) * (f(x) \mid 0)$ olup $\text{Çek}\Psi = \langle f(x), 0\rangle$ bulunur. Diğer taraftan $\text{Im}\,\Psi$ de ${R[x]}/{\langle x^\beta - 1\rangle}$ nin bir alt modülü olduğundan $Z_4 + vZ_4$ üzerinde devirli koddur. β 'nın tek ya da çift olmasına göre Z_4R-devirli kodun üreteçleri belirlenir. β 'nın tek olduğu durumu incelenecektir.

Uyarı 3.2.1. Herhangi bir $f(x)$ polinomu kısaca f olarak gösterilecektir.

Teorem 3.2.2. C kodu Z_4R-tdevirli kod olsun. $f \mid (x^\alpha - 1)$ ve g_1, g_2, g_3 Teorem 3.2.1 de verilen polinomlar ve $l_1, l_2 \in Z_4[x]$ olmak üzere

$C = \langle (f, 0), (l_1, g_1 + (1+v)g_2, (l_2, (1+v)g_3)\rangle$ dir.

İspat. C kodu Z_4R üzerinde devirli kod olsun. $\text{Im}\,\Psi = \langle g_1 + (1+v)g_2, (1+v)g_3\rangle$ olmak üzere $\Psi(l_1, g_1 + (1+v)g_2) = g_1 + (1+v)g_2$ ve $\Psi(l_2, (1+v)g_3) = (1+v)g_3$ olacak şekilde $(l_1, g_1 + (1+v)g_2), (l_2, (1+v)g_3) \in C$ vardır. Herhangi bir $(a,b) \in C$ nin $(f,0)$, $(l_1, g_1 + (1+v)g_2)$ ve $(l_2, (1+v)g_3)$ tarafından üretildiği gösterilsin.

$d_1, d_2 \in R[x]/\langle x^\beta - 1\rangle$ elemanları vardır öyle ki ; $\Psi(a,b) = b = d_1(g_1 + (1+v)g_2) + d_2((1+v)g_3)$ şeklindedir.

$(a,b) - \left(d_1 * (l_1, g_1 + (1+v)g_2\right) + d_2 * \left(l_2, (1+v)g_3\right) = \left(a - \mu(d_1)l_1 - \mu(d_2)l_2, 0\right) \in Çek\Psi$

olup $d_3 \in Z_4[x]/\langle x^\alpha - 1\rangle$ vardır öyle ki $\left(a - \mu(d_1)l_1 - \mu(d_2)l_2, 0\right) = d_3 * (f, 0)$ olarak bulunur.

Buradan, $(a,b) = d_1 * \left(l_1, g_1 + (1+v)g_2\right) + d_2 * \left(l_2, (1+v)g_3\right) + \left(a - \mu(d_1)l_1 - \mu(d_2)l_2, 0\right)$

$= d_1 * \left(l_1, g_1 + (1+v)g_2\right) + d_2 * \left(l_2, (1+v)g_3\right) + d_3 * \left(f, 0\right)$ olup

$C \subseteq \langle (f,0), (l_1, g_1 + (1+v)g_2), (l_2, (1+v)g_3)\rangle$ elde edilir. Tersine

$C \supseteq \langle (f,0), (l_1, g_1 + (1+v)g_2), (l_2, (1+v)g_3)\rangle$ de olup

$C = \langle (f,0), (l_1, g_1 + (1+v)g_2), (l_2, (1+v)g_3)\rangle$

istenen gösterilmiş olur.

Önerme 3.2.1. C kodu $R_{\alpha,\beta}$ da devirli kod olsun. $f \mid \left(x^\alpha - 1\right)$, $C = \langle (f,0), (l_1, g_1 + (1+v)g_2), (l_2, (1+v)g_3)\rangle$ şeklinde üretilir.

Z_4R-toplamsal devirli kodu ise $der(l_1) < der(f)$, $der(l_2) < der(f)$ ve $h = \frac{x^\beta - 1}{g_1}, k = \frac{x^\beta - 1}{hg_2}$ olmak üzere $f \mid \frac{x^\beta - 1}{g_3} l_1 \bmod(1+v)$, $f \mid khl_1 \bmod(1+v)$ dir.

İspat. $der(l_1) \geq der(f)$ olsun. $l_1 = fq_1 + r_1$; $0 \leq der(r_1) < der(f)$ olacak şekilde $r_1, q_1 \in Z_4[x]/\langle x^\alpha - 1\rangle$ polinomları vardır. Şimdi $der(l_2) \geq der(f)$ olsun. O zaman

$l_2 = fq_2 + r_2$; $0 \le der(r_2) < der(f)$ olacak şekilde $r_2, q_2 \in {Z_4[x]}/{\langle x^\alpha - 1\rangle}$ vardır.

$\langle (f,0),(l_1, g_1 + (1+v)g_2),(l_2,(1+v)g_3)\rangle$

$= \langle (f,0),(fq_1 + r_1, g_1 + (1+v)g_2),(fq_2 + r_2,(1+v)g_3)\rangle$

$= \langle (f,0),(r_1, g_1 + (1+v)g_2),(r_2,(1+v)g_3)\rangle$ dir.

Böylece $der(l_1) < der(f)$, $der(l_2) < der(f)$ elde edilmiş olur.

$f \mid \frac{x^\beta - 1}{g_3} l_1 \bmod(1+v)$ olduğunu gösterelim. $\frac{x^\beta - 1}{g_3} * (l_1, g_1 + (1+v)g_2) =$

$\left(\mu\left(\frac{x^\beta - 1}{g_3}\right)l_1, \frac{x^\beta - 1}{g_3}(g_1 + (1+v)g_2)\right) = \left(\mu\left(\frac{x^\beta - 1}{g_3}\right)l_1, 0\right)$ elde edilir. Görülür ki;

$\Psi\left(\mu\left(\frac{x^\beta - 1}{g_3}\right)l_1, 0\right) = 0$ sonucuna varılır.Buradan $\left(\mu\left(\frac{x^\beta - 1}{g_3}\right)l_1, 0\right) \in Çek\Psi \subseteq C$

olduğundan $f \mid \frac{x^\beta - 1}{g_3} l_1 \bmod(1+v)$ elde edilir. Şimdi de $f \mid khl_1 \bmod(1+v)$ olduğunu

gösterelim. $kh * (l_1, g_1 + (1+v)g_2) = (\mu(kh)l_1, khg_1 + (1+v)khg_2) = (\mu(kh)l_1, 0)$ olup

$\Psi(\mu(kh)l_1, 0) = 0$ sonucuna varılır.Böylece $(\mu(kh)l_1, 0) \in Çek\Psi \subseteq C$ olduğundan

$f \mid khl_1 \bmod(1+v)$ elde edilmiş olur.Burada $h = \frac{x^\beta - 1}{g_1}, k = \frac{x^\beta - 1}{hg_2}$ kullanıldığı göz

önünde bulundurulmalıdır.

Önerme 3.2.2. $C = \langle (f,0),(l_1, g_1 + (1+v)g_2),(l_2,(1+v)g_3)\rangle$ kodu Z_4R toplamsal halkasında devirli kod olsun.Buradan;

$$S_1 = \bigcup_{i=0}^{\alpha-der(f)-1} \left\{ x^i * (f, 0) \right\}$$

$$S_2 = \bigcup_{i=0}^{\beta-der(g_1)-1} \left\{ x^i * (l_1, g_1 + (1+v)g_2) \right\}$$

$$S_3 = \bigcup_{i=0}^{der(g_1)-der(g_2)-1} \left\{ x^i * (\mu(h)l_1, (1+v)hg_2) \right\}$$

$$S_4 = \bigcup_{i=0}^{\beta-der(g_3)-1} \left\{ x^i * (l_2, (1+v)g_3 \right\}$$

olmak üzere $S = S_1 \cup S_2 \cup S_3 \cup S_4$ kümesi, C kodu için en küçük geren kümedir.

İspat. $C = \langle (f, 0), (l_1, g_1 + (1+v)g_2), (l_2, (1+v)g_3) \rangle$ ve $c \in C$ olsun.

$c_1 \in Z_4[x]$ ve $c_2, c_3 \in R[x]$ polinomları için

$$c = c_1 * (f, 0) + c_2 * (l_1, g_1 + (1+v)g_2) + c_3 * (l_2, (1+v)g_3)$$

$$= (\mu(c_1)(f, 0)) + c_2 * (l_1, g_1 + (1+v)g_2) + c_3 * (l_2, (1+v)g_3)$$ olur ki eğer

$der(\mu(c_1)) \le \alpha - der(f) - 1$ ise $\mu(c_1)(f, 0) \in SpanS_1$ dir. Aksi takdirde bölme algoritması uygulanırsa $q_3, r_3 \in Z_4[x]$, $0 \le der(r_3) \le (\alpha - der(f) - 1)$ olmak üzere, $\mu(c_1) = \frac{x^\alpha - 1}{f} q_3 + r_3$ dir. Bu yüzden $\mu(c_1)$ yerine yazılırsa,

$$\mu(c_1)(f, 0) = \left(\frac{x^\alpha - 1}{f} q_3 + r_3 \right)(f, 0) = q_3 \left(\frac{x^\alpha - 1}{f} \right)(f, 0) + r_3(f, 0) = r_3(f, 0)$$

elde edilir. $\mu(c_1)(f, 0) \in SpanS_1$ olduğu gösterilmiş olur.

Şimdi $der(c_2) \le \beta \le der(g_1) - 1$ ise $c_2 * (l_1, g_1 + (1+v)g_2) \in SpanS_2$ dir.

Aksi takdirde bölme algoritması uygulanarak, $q_4, r_4 \in Z_4[x]$,

$0 \le der(r_4) \le (\beta - der(g_1) - 1)$ için $c_2 = \frac{x^\beta - 1}{g_1} q_4 + r_4 = hq_4 + r_4$ olur ki Buradan;

$c_2 * (l_1, g_1 + (1+v)g_2) = (hq_4 + r_4) * (l_1, g_1 + (1+v)g_2) =$

$q_4 (\mu(h)l_1, hg_1 + (1+v)hg_2) + r_4 (l_1, g_1 + (1+v)g_2)$

$= q_4 (\mu(h)l_1, (1+v)hg_2) + r_4 (l_1, g_1 + (1+v)g_2)$ olur. Buradan

$0 \le der(r_4) \le \beta - der(g_1) - 1$ olduğundan $c_2 * (l_1, g_1 + (1+v)g_2) \in SpanS_2$ dir.

Şimdi $q_4 (\mu(h)l_1, (1+v)hg_2) \in SpanS_3$ olduğunu gösterelim.

$der(q_4) \le der(g_1) - der(g_2) - 1$ ise $q_4 (\mu(h)l_1, (1+v)hg_2) \in SpanS_3$ dür. Aksi takdirde bölme algoritması uygularsak , $q_5, r_5 \in Z_4[x]$, $0 \le der(r_5) \le (\beta - der(g_2) - 1)$ olmak üzere $q_4 = \frac{x^\beta - 1}{hg_2} q_5 + r_5 = kq_5 + r_5$ tir. Buradan,

$q_4 (\mu(h)l_1, (1+v)hg_2) = (kq_5 + r_5)(\mu(h)l_1, (1+v)hg_2)$

$= q_5 (k\mu(h)l_1, (1+v)hg_2 k) + r_5 (\mu(h)l_1, (1+v)hg_2)$

$= q_5 (k\mu(h)l_1, 0) + r_5 (\mu(h)l_1, (1+v)hg_2)$ olup

$0 \le der(r_5) \le (\beta - der(g_2) - 1)$ olduğundan $r_5 (\mu(h)l_1, (1+v)hg_2) \in SpanS_3$ yazılır. Önerme 3.2.2 den dolayı $fr = khl_1 \bmod(1+v)$, $q_5 (\mu(h)l_1, 0) \in SpanS_1$ dir. Buradan $c_2 * (l_1, g_1 + (1+v)g_2) \in Span(S_1 \cup S_2 \cup S_3)$ bulunur.

Son olarak $c_3 (l_2, (1+v)g_3) \in SpanS_4$ olduğunu gösterelim. $der(c_3) \le \beta - der(g_3) - 1$ ise $c_3 (l_2, (1+v)g_3) \in SpanS_4$ dür.Aksi takdirde bölme algoritması uygulanırsa,

$q_6, r_6 \in Z_4[x]$ ve $0 \le der(r_6) \le (\beta - der(g_3) - 1)$ olmak üzere, $c_3 = \frac{x^\beta - 1}{g_3} q_6 + r_6$ şeklinde olur. Dolayısıyla,

$$c_3(l_2,(1+v)g_3) = \left(\frac{x^\beta - 1}{g_3} q_6 + r_6\right)(l_2,(1+v)g_3)$$

$$= q_6\left(\mu\left(\frac{x^\beta - 1}{g_3}\right)l_2,(1+v)\frac{x^\beta - 1}{g_3} g_3\right) + r_6(l_2,(1+v)g_3)$$

$$= q_6\left(\mu\left(\frac{x^\beta - 1}{g_3}\right)l_2,0\right) + r_6(l_2,(1+v)g_3) \quad \text{olur.}$$

$0 \le der(r_6) \le (\beta - der(g_3) - 1)$ olduğundan $r_6(l_2,(1+v)g_3) \in SpanS_4$ dür. .Önerme 3.2.2. den dolayı $fw = \frac{x^\beta - 1}{g_3} l_2 \bmod(1+v)$ olup $q_6\left(\mu\left(\frac{x^\beta - 1}{g_3}\right)l_2,0\right) \in SpanS_1$ dir. Buradan $c_3(l_2,(1+v)g_3) \in Span(S_1 \cup S_4)$ bulunur. $S = S_1 \cup S_2 \cup S_3 \cup S_4$ kümesi C kodu için geren kümedir.Ayrıca S kümesindeki diğer elemanlar ile lineer bağımlı olacak şekilde bir eleman olmadığından S 'ye C için en küçük geren kümesi denir.

BÖLÜM 4. $Z_4Z_4[v]-$ SABİT DEVİRLİ KODLAR

4.1. $v^2=1,\ Z_4(Z_4+vZ_4)-$ Sabit Devirli Kodların Cebirsel Yapısı

Tanım 4.1.1. Herhangi bir $c=(u_0,u_1,....,u_{\alpha-1},\hat{u}_0,\hat{u}_1,.....,\hat{u}_{\beta-1})\in C$ için $T_\lambda-$ sabit devir ötelemesi ve $T_\lambda(c)=\left(u_{\alpha-1},u_0,....,u_{\alpha-2},\lambda\hat{u}_{\beta-1},\hat{u}_0,....,\hat{u}_{\beta-2}\right)\in C$ ise $Z_4^\alpha\times\left(Z_4+vZ_4\right)^\beta$ nin C, Z_4+vZ_4- alt modülüne $Z_4Z_4[v]-$ lineer $T_{(\lambda)}-$ sabit devirli kod denir.

Not. $\lambda=1$ ise C kodunun devirli kod olduğu açıktır.

Not. $\lambda=-1$ ise C koduna negatif devirli kod denir.

Not. $\lambda=1,3,v,3v,1+2v,2+v,2+3v,3+2v$ ise C koduna sabit devirli kod denir.Bu halka için sadece 2 birim eleman seçilerek çalışılmıştır.

$(u_0,....,u_{\alpha-1},\hat{u}_0,.....\hat{u}_{\beta-1})\in C$ kod sözü polinom cinsinden aşağıdaki gibi ifade edilebilir:

$$c(x)=(u_0+u_1x+....+u_{\alpha-1}x^{\alpha-1}\ |\ \hat{u}_0+\hat{u}_1x+....+\hat{u}_{\beta-1}x^{\beta-1})=\left(u(x),\hat{u}(x)\right)$$

$$\left(u(x),\hat{u}(x)\right)\in Z_4[x]\Big/<x^\alpha-1>\times R[x]\Big/<x^\beta-\lambda>$$

Şimdi; $\breve{r}(x)=(\breve{r}_0+\breve{r}_1x+....+\breve{r}_lx^l)\in R[x]$ ve

$\left(h(x),g(x)\right)\in Z_4[x]\Big/<x^\alpha-1>\times R[x]\Big/<x^\beta-\lambda>$ olsun.

$\mu\left(\breve{r}(x)\right)=\mu(\breve{r}_0)+.....+\mu(\breve{r}_l)x^l$ olmak üzere,

$\breve{r}(x)\left(h(x),g(x)\right)=\left(\mu(\breve{r}(x))h(x),\breve{r}(x)g(x)\right)$ elde edilir.

Tanım 4.1.2. C'nin Z_4R üzerinde (α,β) uzunluğunda $\lambda-$sabit devirli kod olması için gerek ve yeter şart C nin $R_{\alpha,\beta,\lambda}=Z_4[x]/\langle x^{\alpha}-1\rangle\times R[x]/\langle x^{\beta}-\lambda\rangle$ nın $Z_4[v][x]-$alt modülü olmasıdır.

İspat. C bir $\lambda-$toplamsal sabit devirli kod ve $c\in C$ olsun. $c(x)=(u(x),\hat{u}(x))\in C$ yazılır.Bilinir ki $x^i*(u(x),\hat{u}(x))\in C \quad i\geq 1$ için de yazılır. C nin lineerliğinden dolayı herhangi bir $s(x)\in Z_4[v][x]$ için $s(x)(u(x),\hat{u}(x))\in C$ dir. O halde C, $R_{\alpha,\beta,\lambda}$' nın $Z_4[v][x]-$alt modülüdür.Tersine C, $R_{\alpha,\beta,\lambda}$ nın $Z_4[v][x]-$alt modülü olsun.O zaman $x*c(x)\in C$ dir.Dolayısıyla C, Z_4R-toplamsal sabit devirli koddur.

4.2. $Z_4(Z_4+vZ_4)$-Sabit Devirli Kodların Gray Görüntüsü

4 yeni gray map tanımı; $s=u+v\hat{u}\in Z_4[v]$ için

$$\psi_1: Z_4[v]\to Z_4^2 \qquad \psi_2: Z_4[v]\to Z_4^2$$
$$u+v\hat{u}\to(3\hat{u},3u) \qquad u+v\hat{u}\to(3u+3\hat{u},2\hat{u}+2u)$$

$$\psi_3: Z_4[v]\to Z_4^2 \qquad \psi_4: Z_4[v]\to Z_4^2$$
$$u+v\hat{u}\to(3\hat{u},2\hat{u}+u) \qquad u+v\hat{u}\to(2u+2\hat{u},\hat{u}+u)$$

şeklinde tanımlı $\psi_1,\psi_2,\psi_3,\psi_4$ dönüşümüne $Z_4[v]$ üzerinde tanımlı **Gray dönüşüm** denir.Bu dönüşümler $Z_4[v]^{\beta}$ dan $Z_4^{2\beta}$ ya genişletilebilir.

$s_i=u_i+v\hat{u}_i\in Z_4[v], i=0,1,...,i-1$ için

$$\psi_1: Z_4[v]^{\beta}\to Z_4^{2\beta}$$
$$\psi_1(s_0,....,s_{\beta-1})\to(3\hat{u}_0,....,3\hat{u}_{\beta-1},3u_0,....,3u_{\beta-1})$$

$$\psi_2: Z_4[v]^{\beta}\to Z_4^{2\beta}$$
$$\psi_2(s_0,....,s_{\beta-1})\to(3u_0+3\hat{u}_0,....,3u_{\beta-1}+3\hat{u}_{\beta-1},2\hat{u}_0+2u_0,...,2\hat{u}_{\beta-1}+2u_{\beta-1})$$

$$\psi_3 : Z_4[v]^\beta \to Z_4^{2\beta}$$
$$\psi_3(s_0,....,s_{\beta-1}) \to (3\hat{u}_0,....,3\hat{u}_{\beta-1}, 2\hat{u}_0+u_0,....,2\hat{u}_{\beta-1}+u_{\beta-1})$$

$$\psi_4 : Z_4[v]^\beta \to Z_4^{2\beta}$$
$$\psi_4(s_0,...,s_{\beta-1}) \to (2u_0+2\hat{u}_0,....,2u_{\beta-1}+2\hat{u}_{\beta-1},\hat{u}_0+u_0,....,\hat{u}_{\beta-1}+u_{\beta-1})$$

Tanım 4.2.2. Her $c,\hat{c} \in Z_4[v]^\beta$ için $d_L(c,\hat{c}) = w_L(c-\hat{c})$ şeklinde tanımlanan d_L fonksiyonuna **Lee uzaklık** denir.

Tanım 4.2.1. w_G , Z_4^2 vektör uzayı üzerinde tanımlı Hamming ağırlık olmak üzere $c \in Z_4[v]^\beta$ için $w_L(c) = w_G\left(\psi_{1,2,3,4}(c)\right)$ şeklinde tanımlanan w_L fonksiyonuna Z_4 üzerinde **Lee ağırlığı** denir.

Not. $\psi_{1,2,3,4} = \psi_1,\psi_2,\psi_3,\psi_4$ gray dönüşümlerini kastetmektedir.

Teorem 4.2.1. $\psi_{1,2,3,4}$: $(Z_4[v]^\beta, d_L) \to (Z_4^{2\beta}, d_H)$ şeklinde tanımlanan Gray dönüşümler uzaklık koruyan dönüşümlerdir.

İspat. $\forall c_1,c_2 \in Z_4[v]^\beta$ olsun.Bu durumda $\psi_{1,2,3,4}(c_1-c_2) = \psi_{1,2,3,4}(c_1) - \psi_{1,2,3,4}(c_2)$ dir.

$$d_L(c_1,c_2) = w_L(c_1-c_2)$$
$$= w_H\left(\psi_{1,2,3,4}(c_1-c_2)\right)$$
$$= w_H\left(\psi_{1,2,3,4}(c_1) - \psi_{1,2,3,4}(c_2)\right)$$
$$= d_H\left(\psi_{1,2,3,4}(c_1), \psi_{1,2,3,4}(c_2)\right)$$

eşitliği elde edilir. O halde $\psi_{1,2,3,4}$ uzaklık koruyan dönüşümlerdir.

Önerme 4.2.1. ψ_1, $Z_4[v]^\beta$ kümesinden $Z_4^{2\beta}$ kümesine gray dönüşümü $T_\lambda - \lambda$ sabit devirli öteleme, $\lambda = v$ ve $\rho -$ devirli öteleme operatörü olmak üzere $\psi_1 T_\lambda = \rho\psi_1$ dir.

İspat. $s_i = u_i + v\hat{u}_i \in Z_4[v]$, $i = 0,1,.....,\beta-1$ için $s = (s_0, s_1, ..., s_{\beta-1}) \in Z_4[v]^\beta$ ve $\lambda = v$ olmak üzere

$$\psi_1 T_\lambda(s) = \psi_1(\lambda s_{\beta-1}, s_0, ..., s_{\beta-2})$$

$$= (3u_{\beta-1}, 3\hat{u}_0, ..., 3\hat{u}_{\beta-2}, 3u_0, ..., 3u_{\beta-2})$$

Diğer yandan;

$$\rho\psi_1(s) = \rho(3\hat{u}_0, ..., 3\hat{u}_{\beta-1}, 3u_0, ..., 3u_{\beta-1})$$

$$= (3u_{\beta-1}, 3\hat{u}_0, ..., 3\hat{u}_{\beta-2}, 3u_0, ..., 3u_{\beta-2})$$

Görülür ki $\psi_1 T_\lambda = \rho\psi_1$ dir.

Teorem 4.2.2. C kodunun $Z_4[v]$ üzerinde β uzunluğunda bir sabit devirli kod olması için , $\psi_1(C)$ kodunun Z_4 üzerinde tanımlı 2β uzunluğunda bir devirli kod olmasıdır.

İspat. C bir $\lambda-$sabit devirli kod, $T_\lambda(C) = C$ dir. (Önerme 4.2.1.'den) $\psi_1 T_\lambda(C) = \psi_1(C) = \rho\psi_1(C)$ olup $\psi_1(C)$, Z_4 üzerinde 2β uzunluğunda bir devirli koddur.

Önerme 4.2.2. ψ_2, $Z_4[v]^\beta$ kümesinden $Z_4^{2\beta}$ kümesine gray dönüşümü $T_\lambda - \lambda$ sabit devirli öteleme, $\lambda = v$ ve γ-parçalı devirli öteleme operatörü olmak üzere $\psi_2 T_\lambda = \gamma\psi_2$ dir.

İspat. $s_i = u_i + v\hat{u}_i \in Z_4[v]$, $i = 0,1,...,\beta-1$ için $s = (s_0, ..., s_{\beta-1}) \in Z_4[v]^\beta$ ve $\lambda = v$ olmak üzere

$$\psi_2 T_\lambda(s) = \psi_2(\lambda s_{\beta-1}, s_0, ..., s_{\beta-2})$$

$$(3u_{\beta-1} + 3\hat{u}_{\beta-1}, 3u_0 + 3\hat{u}_0, ..., 3u_{\beta-2} + 3\hat{u}_{\beta-2}, 2\hat{u}_{\beta-1} + 2u_{\beta-1}, ..., 2\hat{u}_{\beta-2} + 2u_{\beta-2})$$

Diğer yandan

$$\gamma\psi_2(s) = \gamma(3u_0 + 3\hat{u}_0, ..., 3u_{\beta-1} + 3\hat{u}_{\beta-1}, 2\hat{u}_0 + 2u_0, ..., 2\hat{u}_{\beta-1} + 2u_{\beta-1})$$

$$(3u_{\beta-1} + 3\hat{u}_{\beta-1}, 3u_0 + 3\hat{u}_0, ..., 3u_{\beta-2} + 3\hat{u}_{\beta-2}, 2\hat{u}_{\beta-1} + 2u_{\beta-1}, ..., 2\hat{u}_{\beta-2} + 2u_{\beta-2})$$

Görülür ki $\psi_2 T_\lambda = \gamma\psi_2$ dir.

Teorem 4.2.3. C kodunun $Z_4[v]$ üzerinde β uzunluğunda bir sabit devirli kod olması için , $\psi_2(C)$ kodunun Z_4 üzerinde tanımlı 2β uzunluğunda indeksi 2 olan bir parçalı devirli kod olmasıdır.

İspat. C bir $\lambda-$sabit devirli kod, $T_\lambda(C) = C$ dir. (Önerme 4.2.2.'den) $\psi_2 T_\lambda(C) = \psi_2(C) = \gamma\psi_2(C)$ olup Z_4, üzerinde 2β uzunluğunda indeksi 2 olan parçalı devirli bir koddur.

Önerme 4.2.3. ψ_3, $Z_4[v]^\beta$ kümesinden $Z_4^{2\beta}$ kümesine gray dönüşümü $T_\lambda - \lambda$ sabit devirli öteleme, $\lambda = 2 + 3v$ ve ρ- devirli öteleme operatörü olmak üzere $\psi_3 T_\lambda = \rho\psi_3$ dir.

İspat. $s_i = u_i + v\hat{u}_i \in Z_4[v]$, $i = 0,1,..., \beta - 1$ için $s = (s_0, ..., s_{\beta-1}) \in Z_4[v]^\beta$ ve $\lambda = 2 + 3v$ olmak üzere

$$\psi_3 T_\lambda(s) = \psi_3(\lambda s_{\beta-1}, s_0, ..., s_{\beta-2})$$

$$= (2\hat{u}_{\beta-1} + u_{\beta-1}, 3\hat{u}_0, ..., 3\hat{u}_{\beta-2}, 2\hat{u}_0 + u_0, ..., 2\hat{u}_{\beta-2} + u_{\beta-2})$$

Diğer yandan

$$\rho\psi_3(s) = \rho(3\hat{u}_0, ..., 3\hat{u}_{\beta-1}, 2\hat{u}_0 + u_0, ..., 2\hat{u}_{\beta-1} + u_{\beta-1})$$

$$= (2\hat{u}_{\beta-1} + u_{\beta-1}, 3\hat{u}_0, ..., 3\hat{u}_{\beta-2}, 2\hat{u}_0 + u_0, ..., 2\hat{u}_{\beta-2} + u_{\beta-2})$$

Görülür ki $\psi_3 T_\lambda = \rho\psi_3$ dür.

Teorem 4.2.4. C kodunun $Z_4[v]$ üzerinde β uzunluğunda bir sabit devirli kod olması için , $\psi_3(C)$ kodunun Z_4 üzerinde tanımlı 2β uzunluğunda bir devirli kod olmasıdır.

İspat. C bir $\lambda-$sabit devirli kod, $T_\lambda(C)=C$ dir. (Önerme 4.2.3.'den) $\psi_3 T_\lambda(C)=\psi_3(C)=\rho\psi_3(C)$ olup Z_4, üzerinde 2β uzunluğunda devirli bir koddur.

Önerme 4.2.4. ψ_4, $Z_4[v]^\beta$ kümesinden $Z_4^{2\beta}$ kümesine gray dönüşümü $T_\lambda-\lambda$ sabit devirli öteleme, $\lambda=2+3v$ ve γ-parçalı devirli öteleme operatörü olmak üzere $\psi_3 T_\lambda=\gamma\psi_3$ dir.

İspat. $s_i=u_i+v\hat{u}_i\in Z_4[v],\quad i=0,1,...,\beta-1$ için $s=(s_0,.....,s_{\beta-1})\in Z_4[v]^\beta$ ve $\lambda=2+3v$ olmak üzere

$$\psi_4 T_\lambda(s)=\psi_4(\lambda s_{\beta-1},s_0,.....,s_{\beta-2})$$

$$=(2u_{\beta-1}+2\hat{u}_{\beta-1},2u_0+2\hat{u}_0,....,2u_{\beta-2}+2\hat{u}_{\beta-2},\hat{u}_{\beta-1}+u_{\beta-1},\hat{u}_0+u_0,....,\hat{u}_{\beta-2}+u_{\beta-2})$$

Diğer yandan

$$\gamma\psi_4(s)=\gamma(2u_0+\hat{u}_0,....,2u_{\beta-1}+\hat{u}_{\beta-1},\hat{u}_0+u_0,....,\hat{u}_{\beta-1}+u_{\beta-1})$$

$$=(2u_{\beta-1}+2\hat{u}_{\beta-1},2u_0+2\hat{u}_0,....,2u_{\beta-2}+2\hat{u}_{\beta-2},\hat{u}_{\beta-1}+u_{\beta-1},\hat{u}_0+u_0,....,\hat{u}_{\beta-2}+u_{\beta-2})$$

Görülür ki $\psi_4 T_\lambda=\gamma\psi_4$ dir.

Teorem 4.2.5. C kodunun $Z_4[v]$ üzerinde β uzunluğunda bir sabit devirli kod olması için , $\psi_4(C)$ kodunun Z_4 üzerinde tanımlı 2β uzunluğunda indeksi 2 olan bir parçalı devirli kod olmasıdır.

İspat. C bir $\lambda-$sabit devirli kod, $T_\lambda(C)=C$ dir. (Önerme 4.2.4.'den) $\psi_4 T_\lambda(C)=\psi_4(C)=\gamma\psi_4(C)$ olup Z_4, üzerinde 2β uzunluğunda indeksi 2 olan parçalı devirli bir koddur.

Şimdi ψ_1 gray dönüşümü yardımıyla $\ddot{\psi}_1$ gray dönüşümünü tanmlıyoruz.

$$\ddot{\psi}_1 :\ Z_4 \times Z_4[v] \to Z_4^3$$

$$\ddot{\psi}_1 (c, u+v\hat{u}) \to (c, \psi_1(u+v\hat{u})) = (c, 3\hat{u}, 3u) \qquad u, \hat{u}, c \in Z_4$$

$\ddot{\psi}_1$ dönüşümünü genişletirsek,

$$\ddot{\psi}_1 :\ Z_4^\alpha \times Z_4[v]^\beta \to Z_4^{\alpha+2\beta}$$

$$\ddot{\psi}_1(c_0, c_1, ...c_{\alpha-1}, s_0, s_1, ..., s_{\beta-1})$$

$$= (c_0, ..., c_{\alpha-1}, 3\hat{u}_0, 3\hat{u}_1, ..., 3\hat{u}_{\beta-1}, 3u_0, 3u_1, ..., 3u_{\beta-1})$$

$s_i = u_i + v\hat{u}_i \in Z_4[v]$ ve $i = 0,1,....,\beta-1$ için $u_i, \hat{u}_i, c_i \in Z_4$ dir.

Teorem 4.2.6. C, $\dfrac{Z_4[x]}{\langle x^\alpha - \mu(\lambda)\rangle} \times \dfrac{R[x]}{\langle x^\beta - \lambda\rangle}$ de sabit devirli kod olsun.Bu durumda $\lambda = v$ için $\alpha = \beta$ ise $\ddot{\psi}_1(C)$, 2 indeksli parçalı devirli koddur. Eğer $\alpha \neq \beta$ ise

$\ddot{\psi}_1(C)$, 2 indeksli genelleştirilmiş parçalı devirli koddur.

İspat. C, $\dfrac{Z_4[x]}{\langle x^\alpha - \mu(\lambda)\rangle} \times \dfrac{R[x]}{\langle x^\beta - \lambda\rangle}$ de sabit devirli kod olsun.

$$c = \left(c_0, c_1, ..., c_{\alpha-1}, s_0, s_1, ..., s_{\beta-1}\right) = \left(c_0, c_1, ..., c_{\alpha-1}, u_0 + v\hat{u}_0, u_1 + v\hat{u}_1, ..., u_{\beta-1} + v\hat{u}_{\beta-1}\right) \in C$$

alalım. $\lambda = v$ için $\mu(\lambda) = 1$ dir. γ, parçalı devirli öteleme operatörü ve $T_\lambda - \lambda$ sabit

devirli öteleme operatörü olsun. C, $\frac{Z_4[x]}{\langle x^{\alpha}-1\rangle}\times\frac{R[x]}{\langle x^{\beta}-(v)\rangle}$ de sabit devirli kod olduğundan,

$$T_{\lambda}(c)=\left(\mu(v)c_{\alpha-1},c_0,....,c_{\alpha-2},(v)s_{\beta-1},s_0,....,s_{\beta-2}\right)$$

$$=\left(c_{\alpha-1},c_0,...,c_{\alpha-2},(v)(u_{\beta-1}+v\hat{u}_{\beta-1}),u_0+v\hat{u}_0,....,u_{\beta-2}+v\hat{u}_{\beta-2}\right)$$

$$=\left(c_{\alpha-1},c_0,....,c_{\alpha-2},\hat{u}_{\beta-1}+vu_{\beta-1},u_0+v\hat{u}_0,....,u_{\beta-2}+v\hat{u}_{\beta-2}\right) \quad \text{olup}$$

$\vec{\psi}_1$ uygulanarak,

$\vec{\psi}_1\left(T_{\lambda}(c)\right)=(c_{\alpha-1},c_0,...,c_{\alpha-2},3u_{\beta-1},3\hat{u}_0,....,3\hat{u}_{\beta-2},3u_0,....,3u_{\beta-2})$ elde edilir.

Diğer taraftan,

$\vec{\psi}_1(c)=(c_0,.....,c_{\alpha-1},3\hat{u}_0,3\hat{u}_1,.....,3\hat{u}_{\beta-1},3u_0,3u_1,....,3u_{\beta-1})$ dir.

Buradan,

$\gamma\left(\vec{\psi}_1(c)\right)=(c_{\alpha-1},c_0,...,c_{\alpha-2},3u_{\beta-1},3\hat{u}_0,....,3\hat{u}_{\beta-2},3u_0,....,3u_{\beta-2})$ bulunur.

Böylece $\vec{\psi}_1\left(T_{\lambda}(c)\right)=\gamma\vec{\psi}_1\left(c\right)$ dir.Eğer $\alpha=\beta$ ise $\vec{\psi}_1(C)$, 2 indeksli parçalı devirli koddur. Eğer $\alpha\neq\beta$ ise $\vec{\psi}_1(C)$, 2 indeksli genelleştirilmiş parçalı devirli koddur.

Şimdi ψ_2 gray dönüşümü yardımıyla $\vec{\psi}_2$ gray dönüşümünü tanmlıyoruz.

$\vec{\psi}_2: \quad Z_4\times Z_4[v]\rightarrow Z_4^3$

$\vec{\psi}_2\ (c,u+v\hat{u})\rightarrow(c,\psi_2(u+v\hat{u}))=(c,3u+3\hat{u},2\hat{u}+2u) \qquad u,\hat{u},c\in Z_4$

$\vec{\psi}_2$ dönüşümünü genişletirsek,

$\vec{\vec{\psi}}_2 : \ Z_4^{\alpha} \times Z_4[v]^{\beta} \to Z_4^{\alpha+2\beta}$

$\vec{\vec{\psi}}_2(c_0, c_1, ...c_{\alpha-1}, s_0, s_1, ..., s_{\beta-1})$

$= (c_0, ..., c_{\alpha-1}, 3u_0 + 3\hat{u}_0, 3u_1 + 3\hat{u}_1, ..., 3u_{\beta-1} + 3\hat{u}_{\beta-1}, 2\hat{u}_0 + 2u_0, ..., 2\hat{u}_{\beta-1} + 2u_{\beta-1})$

$s_i = u_i + v\hat{u}_i \in Z_4[v]$ ve $i = 0,1,...., \beta - 1$ için $u_i, \hat{u}_i, c_i \in Z_4$ dir.

Teorem 4.2.7. C, $\frac{Z_4[x]}{\langle x^{\alpha} - \mu(\lambda)\rangle} \times \frac{R[x]}{\langle x^{\beta} - \lambda\rangle}$ de sabit devirli kod olsun. Bu durumda $\lambda = v$ için $\alpha = \beta$ ise $\vec{\vec{\psi}}_2(C)$, 3 indeksli parçalı devirli koddur. Eğer $\alpha \neq \beta$ ise $\vec{\vec{\psi}}_2(C)$, 3 indeksli genelleştirilmiş parçalı devirli koddur.

İspat. C, $\frac{Z_4[x]}{\langle x^{\alpha} - \mu(\lambda)\rangle} \times \frac{R[x]}{\langle x^{\beta} - \lambda\rangle}$ de sabit devirli kod olsun.

$c = \left(c_0, c_1, ..., c_{\alpha-1}, s_0, s_1, ..., s_{\beta-1}\right) = \left(c_0, c_1, ..., c_{\alpha-1}, u_0 + v\hat{u}_0, u_1 + v\hat{u}_1, ..., u_{\beta-1} + v\hat{u}_{\beta-1}\right) \in C$

alalım. $\lambda = v$ için $\mu(\lambda) = 1$ dir. γ, parçalı devirli öteleme operatörü ve

$T_{\lambda} - \lambda$ sabit devirli öteleme operatörü olsun. C, $\frac{Z_4[x]}{\langle x^{\alpha} - 1\rangle} \times \frac{R[x]}{\langle x^{\beta} - (v)\rangle}$ de sabit devirli kod olduğundan,

$$T_{\lambda}(c) = \left(\mu(v)c_{\alpha-1}, c_0, ..., c_{\alpha-2}, (v)s_{\beta-1}, s_0, ..., s_{\beta-2}\right)$$

$$= \left(c_{\alpha-1}, c_0, ..., c_{\alpha-2}, (v)(u_{\beta-1} + v\hat{u}_{\beta-1}), u_0 + v\hat{u}_0, ..., u_{\beta-2} + v\hat{u}_{\beta-2}\right)$$

$$= \left(c_{\alpha-1}, c_0, ..., c_{\alpha-2}, \hat{u}_{\beta-1} + vu_{\beta-1}, u_0 + v\hat{u}_0, ..., u_{\beta-2} + v\hat{u}_{\beta-2}\right)$$

olup $\vec{\vec{\psi}}_2$ uygulanarak,

$\vec{\psi}_2\left(T_\lambda(c)\right) =$

$(c_{\alpha-1},.....,c_{\alpha-2},3u_{\beta-1}+3\hat{u}_{\beta-1},3u_0+3\hat{u}_0,.....,3u_{\beta-2}+3\hat{u}_{\beta-2},2\hat{u}_{\beta-1}+2u_{\beta-1},....,2\hat{u}_{\beta-2}+2u_{\beta-2})$

elde edilir.

Diğer taraftan,

$\vec{\psi}_2(c) = (c_0,.....,c_{\alpha-1},3u_0+3\hat{u}_0,3u_1+3\hat{u}_1,.....,3u_{\beta-1}+3\hat{u}_{\beta-1},2\hat{u}_0+2u_0,....,2\hat{u}_{\beta-1}+2u_{\beta-1})$

dir.

Buradan,

$\gamma\left(\vec{\psi}_2(c)\right) =$

$(c_{\alpha-1},.....,c_{\alpha-2},3u_{\beta-1}+3\hat{u}_{\beta-1},3u_0+3\hat{u}_0,.....,3u_{\beta-2}+3\hat{u}_{\beta-2},2\hat{u}_{\beta-1}+2u_{\beta-1},....,2\hat{u}_{\beta-2}+2u_{\beta-2})$

bulunur.

Böylece $\vec{\psi}_2\left(T_\lambda(c)\right) = \gamma\vec{\psi}_2\left(c\right)$ dir. Eğer $\alpha = \beta$ ise $\vec{\psi}_2(C)$, 3 indeksli parçalı devirli koddur.

Eğer $\alpha \neq \beta$ ise $\vec{\psi}_2(C)$, 3 indeksli genelleştirilmiş parçalı devirli koddur.Şimdi ψ_3 gray dönüşümü yardımıyla $\vec{\psi}_3$ gray dönüşümünü tanmlıyoruz.

$\vec{\psi}_3 : \ Z_4 \times Z_4[v] \rightarrow Z_4^3$

$\vec{\psi}_3\ (c, u+v\hat{u}) \rightarrow (c, \psi_3(u+v\hat{u})) = (c, 3\hat{u}, 2\hat{u}+u) \quad u,\hat{u},c \in Z_4$

$\vec{\psi}_3$ dönüşümünü genişletirsek,

$\vec{\psi}_3 : \ Z_4^\alpha \times Z_4[v]^\beta \rightarrow Z_4^{\alpha+2\beta}$ $\vec{\psi}_3(c_0,c_1,....c_{\alpha-1},s_0,s_1,.....,s_{\beta-1})$

$= (c_0,.....,c_{\alpha-1},3\hat{u}_0,3\hat{u}_1,.....,3\hat{u}_{\beta-1},2\hat{u}_0+u_0,2\hat{u}_1+u_1,....,2\hat{u}_{\beta-1}+u_{\beta-1})$

$s_i = u_i + v\hat{u}_i \in Z_4[v]$ ve $i = 0,1,....,\beta-1$ için $u_i,\hat{u}_i,c_i \in Z_4$ dir.

Teorem 4.2.8. C, $\frac{Z_4[x]}{\langle x^{\alpha}-\mu(\lambda)\rangle}\times\frac{R[x]}{\langle x^{\beta}-\lambda\rangle}$ de sabit devirli kod olsun. Bu durumda $\lambda=2+3v$ için $\alpha=\beta$ ise $\vec{\psi}_3(C)$, 2 indeksli parçalı devirli koddur.Eğer $\alpha\neq\beta$ ise $\vec{\psi}_3(C)$, 2 indeksli genelleştirilmiş parçalı devirli koddur.

İspat. C, $\frac{Z_4[x]}{\langle x^{\alpha}-\mu(\lambda)\rangle}\times\frac{R[x]}{\langle x^{\beta}-\lambda\rangle}$ de sabit devirli kod olsun.

$$c=\left(c_0,c_1,....,c_{\alpha-1},s_0,s_1,....,s_{\beta-1}\right)=\left(c_0,c_1,.....,c_{\alpha-1},u_0+v\hat{u}_0,u_1+v\hat{u}_1,...,u_{\beta-1}+v\hat{u}_{\beta-1}\right)\in C$$

alalım. $\lambda=2+3v$ için $\mu(\lambda)=1$ dir. γ, parçalı devirli öteleme operatörü ve $T_{\lambda}-\lambda$ sabit devirli öteleme operatörü olsun. C, $\frac{Z_4[x]}{\langle x^{\alpha}-1\rangle}\times\frac{R[x]}{\langle x^{\beta}-(2+3v)\rangle}$ de sabit devirli kod olduğundan,

$$T_{\lambda}(c)=\left(\mu(2+3v)c_{\alpha-1},c_0,....,c_{\alpha-2},(2+3v)s_{\beta-1},s_0,....,s_{\beta-2}\right)$$

$$=\left(c_{\alpha-1},c_0,...,c_{\alpha-2},(2+3v)(u_{\beta-1}+v\hat{u}_{\beta-1}),u_0+v\hat{u}_0,....,u_{\beta-2}+v\hat{u}_{\beta-2}\right)$$

$$=\left(c_{\alpha-1},c_0,....,c_{\alpha-2},2u_{\beta-1}+3\hat{u}_{\beta-1}+v(3u_{\beta-1}+2\hat{u}_{\beta-1}),u_0+v\hat{u}_0,....,u_{\beta-2}+v\hat{u}_{\beta-2}\right)$$

olup $\vec{\psi}_3$ uygulanarak,

$$\vec{\psi}_3\left(T_{\lambda}(c)\right)=(c_{\alpha-1},c_0,...,c_{\alpha-2},2\hat{u}_{\beta-1}+u_{\beta-1},3\hat{u}_0,....,3\hat{u}_{\beta-2},2\hat{u}_0+u_0,....,2\hat{u}_{\beta-2}+u_{\beta-2})$$

elde edilir.

Diğer taraftan,

$$\vec{\psi}_3(c)=(c_0,.....,c_{\alpha-1},3\hat{u}_0,3\hat{u}_1,.....,3\hat{u}_{\beta-1},2\hat{u}_0+u_0,2\hat{u}_1+u_1,....,2\hat{u}_{\beta-1}+u_{\beta-1})$$ dir.

Buradan,

$$\gamma\left(\vec{\psi}_3(c)\right)=(c_{\alpha-1},c_0,...,c_{\alpha-2},2\hat{u}_{\beta-1}+u_{\beta-1},3\hat{u}_0,....,3\hat{u}_{\beta-2},2\hat{u}_0+u_0,....,2\hat{u}_{\beta-2}+u_{\beta-2})$$

bulunur.

Böylece $\vec{\psi}_3(T_\lambda(c)) = \gamma(\vec{\psi}_3(c))$ dir.Eğer $\alpha = \beta$ ise $\vec{\psi}_3(C)$, 2 indeksli parçalı devirli koddur. Eğer $\alpha \neq \beta$ ise $\vec{\psi}_3(C)$, 2 indeksli genelleştirilmiş parçalı devirli koddur.

Şimdi ψ_4 gray dönüşümü yardımıyla $\vec{\psi}_4$ gray dönüşümünü tanmlıyoruz.

$$\vec{\psi}_4 : \quad Z_4 \times Z_4[v] \to Z_4^3$$

$$\vec{\psi}_4 (c, u+v\hat{u}) \to (c, \psi_4(u+v\hat{u})) = (c, 2u+2\hat{u}, \hat{u}+u) \qquad u, \hat{u}, c \in Z_4$$

$\vec{\psi}_4$ dönüşümünü genişletirsek,

$$\vec{\psi}_4 : \quad Z_4^\alpha \times Z_4[v]^\beta \to Z_4^{\alpha+2\beta}$$

$$\vec{\psi}_4(c_0, c_1, ...c_{\alpha-1}, s_0, s_1, ..., s_{\beta-1})$$

$$= (c_0, ..., c_{\alpha-1}, 2u_0 + 2\hat{u}_0, 2u_1 + 2\hat{u}_1, ..., 2u_{\beta-1} + 2\hat{u}_{\beta-1}, \hat{u}_0 + u_0, ..., \hat{u}_{\beta-1} + u_{\beta-1})$$

$s_i = u_i + v\hat{u}_i \in Z_4[v]$ ve $i = 0, 1, ..., \beta - 1$ için $u_i, \hat{u}_i, c_i \in Z_4$ dir.

Teorem 4.2.9. C, $\dfrac{Z_4[x]}{\langle x^\alpha - \mu(\lambda)\rangle} \times \dfrac{R[x]}{\langle x^\beta - \lambda\rangle}$ de sabit devirli kod olsun.Bu durumda $\lambda = 2 + 3v$ için $\alpha = \beta$ ise $\vec{\psi}_4(C)$, 3 indeksli parçalı devirli koddur.Eğer $\alpha \neq \beta$ ise $\vec{\psi}_4(C)$, 3 indeksli genelleştirilmiş parçalı devirli koddur.

İspat. C, $\dfrac{Z_4[x]}{\langle x^\alpha - \mu(\lambda)\rangle} \times \dfrac{R[x]}{\langle x^\beta - \lambda\rangle}$ de sabit devirli kod olsun.

$$c = \left(c_0, c_1, ..., c_{\alpha-1}, s_0, s_1, ..., s_{\beta-1}\right) = \left(c_0, c_1, ..., c_{\alpha-1}, u_0 + v\hat{u}_0, u_1 + v\hat{u}_1, ..., u_{\beta-1} + v\hat{u}_{\beta-1}\right) \in C$$

alalım. $\lambda = 2 + 3v$ için $\mu(\lambda) = 1$ dir. γ, parçalı devirli öteleme operatörü ve $T_\lambda - \lambda$ sabit devirli öteleme operatörü olsun. C, $\dfrac{Z_4[x]}{\langle x^\alpha - 1\rangle} \times \dfrac{R[x]}{\langle x^\beta - (2+3v)\rangle}$ de sabit devirli kod olduğundan,

$$T_\lambda(c) = \left(\mu(2+3v)c_{\alpha-1}, c_0, ..., c_{\alpha-2}, (2+3v)s_{\beta-1}, s_0, ..., s_{\beta-2}\right)$$

$$= \left(c_{\alpha-1}, c_0, ..., c_{\alpha-2}, (2+3v)(u_{\beta-1} + v\hat{u}_{\beta-1}), u_0 + v\hat{u}_0, ..., u_{\beta-2} + v\hat{u}_{\beta-2}\right)$$

$$= \left(c_{\alpha-1}, c_0, ..., c_{\alpha-2}, 2u_{\beta-1} + 3\hat{u}_{\beta-1} + v(3u_{\beta-1} + 2\hat{u}_{\beta-1}), u_0 + v\hat{u}_0, ..., u_{\beta-2} + v\hat{u}_{\beta-2}\right)$$

olup $\vec{\psi}_4$ uygulanarak,

$$\vec{\psi}_4\left(T_\lambda(c)\right) =$$
$$(c_{\alpha-1}, ..., c_{\alpha-2}, 2u_{\beta-1} + 2\hat{u}_{\beta-1}, ..., 2u_{\beta-2} + 2\hat{u}_{\beta-2}, \hat{u}_{\beta-1} + u_{\beta-1}, \hat{u}_0 + u_0, ..., \hat{u}_{\beta-2} + u_{\beta-2})$$

elde edilir.

Diğer taraftan,

$$\vec{\psi}_4(c) = (c_0, ..., c_{\alpha-1}, 2u_0 + 2\hat{u}_0, 2u_1 + 2\hat{u}_1, ..., 2u_{\beta-1} + 2\hat{u}_{\beta-1}, \hat{u}_0 + u_0, ..., \hat{u}_{\beta-1} + u_{\beta-1})$$

dir.

Buradan,

$$\gamma\left(\vec{\psi}_4(c)\right) =$$
$$(c_{\alpha-1}, ..., c_{\alpha-2}, 2u_{\beta-1} + 2\hat{u}_{\beta-1}, ..., 2u_{\beta-2} + 2\hat{u}_{\beta-2}, \hat{u}_{\beta-1} + u_{\beta-1}, \hat{u}_0 + u_0, ..., \hat{u}_{\beta-2} + u_{\beta-2})$$

bulunur.

Böylece $\vec{\psi}_4\left(T_\lambda(c)\right) = \gamma(\vec{\psi}_4(c))$ dir.Eğer $\alpha = \beta$ ise $\vec{\psi}_4(C)$, 3 indeksli parçalı devirli koddur.

Eğer $\alpha \neq \beta$ ise $\vec{\psi}_4(C)$, 3 indeksli genelleştirilmiş parçalı devirli koddur.

BÖLÜM 5. $Z_4Z_4[\vartheta]-$ SABİT DEVİRLİ KODLAR

Parçalı devirli, sabit devirli gibi devirli kod içinde birçok genelleştirme mevcuttur. Lineer kodların önemli bir sınıfı da sabit devirli kodlardır. Toplamsal halkalar üzerinde birçok farklı halkanın birim elemanı seçilerek, sabit devirli kod incelemesi yapılmıştır [16,17,18,19,20,21,22,23,24,25]. Li ve ark. $Z_2Z_2[u]-(1+u)$ toplamsal sabit devirli kodlara çalışmıştır.[26] İslam ve ark. $u^2=v^2=uv=0$ için $Z_pZ_p[u,v]$ toplamsal halkasında devirli ve sabit devirli kodları incelemiştir.[27] Bu bölümde, $\vartheta^2=2$ için $Z_4(Z_4+\vartheta Z_4)-$ halkasının yapısı verilmiştir. Daha sonra $\vartheta^2=2$ ve $R_1=Z_4+\vartheta Z_4$ olmak üzere, Z_4R_1 üzerinde uzunluğu tek olan $\vartheta-$ sabit devirli kodlar incelenip, sabit devirli kodlar için gray dönüşüm tanımlanarak görüntülerine bakılmıştır.

5.1. $\vartheta^2=2$; $Z_4(Z_4+\vartheta Z_4)$ Halkasının Yapısı

$\vartheta^2=2$ olmak üzere, $R_1=Z_4+\vartheta Z_4=Z_4[\vartheta]$ halkasını temsil etsin.

$Z_4+\vartheta Z_4\cong Z_4[\vartheta]/<\vartheta^2-2>=\{p+\vartheta q: p,q\in Z_4\}$ halkası karakteristiği 4 olan 16 elemanlı değişmeli ve sonlu bir halkadır. $Z_4+\vartheta Z_4$ halkası sonlu zincir halkasıdır ve tek maksimal ideali olduğundan ayrıca lokal halkadır.

$Z_4[\vartheta]/<\vartheta^2-2>=\{p+\vartheta q: p,q\in Z_4\}$ olup $S_4=Z_4+\vartheta Z_4=\{p+\vartheta q: p,q\in Z_4\}$ kümesi de bir halkadır.

Teorem 5.1.1. $f: Z_4+\vartheta Z_4\to Z_4[\vartheta]/<\vartheta^2-2>$

$p+\vartheta q \to f(p+\vartheta q)=\{p+\vartheta q\}$ dönüşümü bir izomorfizmadır.

İspat. Tanımlanan f dönüşümü kapalı ve iyi tanımlıdır.

$\forall p_1+\vartheta q_1, p_2+\vartheta q_2 \in S_4$ için $f(p_1+\vartheta q_1)=f(p_2+\vartheta q_2)$ olsun.

$$\{p_1+\vartheta q_1\}=\{p_2+\vartheta q_2\}=$$
$$\{p_1-p_2+\vartheta(q_1-q_2\}=0=$$
$$p_1-p_2=q_1-q_2=0=$$
$$p_1=p_2, q_1=q_2=$$
$$p_1+\vartheta q_1=p_2+\vartheta q_2$$

elde edilir.O halde f birebirdir.

$|S_4|=4^2=16$ olduğundan f örtendir.

$$f((p_1+\vartheta q_1)+(p_2+\vartheta q_2))$$
$$=f(p_1+p_2+\vartheta(q_1+q_2))$$
$$=\{p_1+\vartheta q_1\}+\{p_2+\vartheta q_2\}$$
$$=f(p_1+\vartheta q_1)+f(p_2+\vartheta q_2)$$

ve

$$\forall k \in Z_4+\vartheta Z_4$$
$$f(k(p_1+\vartheta q_1))=f(kp_1+\vartheta kq_1)$$
$$=k\{p_1+\vartheta q_1\}=kf(p_1+\vartheta q_1)$$

Olup f dönüşümü homomorfizmadır.

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

Buradan;

$Z_4 + \vartheta Z_4 \cong {Z_4[\vartheta]}\big/{< \vartheta^2 - 2 >}$ yazılır.

Bu halkanın 16 elemanı ;

$0,1,2,3,\vartheta,2\vartheta,3\vartheta,1+\vartheta,1+2\vartheta,1+3\vartheta,2+\vartheta,2+2\vartheta,2+3\vartheta,3+\vartheta,3+2\vartheta,3+3\vartheta$ olmak üzere $\varphi = \varphi_i + \vartheta\varphi_j$, $Z_4 + \vartheta Z_4$ halkasının birimsel elemanlarını ifade etsin.

Bu halkanın birimsel elemanlarının kümesi
$\{1,3,1+\vartheta,3+\vartheta,1+2\vartheta,3+2\vartheta,1+3\vartheta,3+3\vartheta\}$ dir.

Bu halkanın sıfır bölenlerinin kümesi

$\{0,2,\vartheta,2\vartheta,2+\vartheta,2+2\vartheta,3\vartheta,2+3\vartheta\}$ dir.

$Z_4 + \vartheta Z_4$ halkasının idealleri;

$I_0 = \{0\}$

$I_1 = I_3 = I_{1+\vartheta} = I_{1+2\vartheta} = I_{1+3\vartheta} = I_{3+\vartheta} = I_{3+2\vartheta} = I_{3+3\vartheta} = Z_4 + \vartheta Z_4$

$I_{2\vartheta} = \{0,\vartheta\}$

$I_2 = I_{2+2\vartheta} = \{0,2,2\vartheta,2+2\vartheta\}$

$I_\vartheta = I_{3\vartheta} = I_{2+\vartheta} = I_{2+3\vartheta} = \{0,2,\vartheta,2\vartheta,3\vartheta,2+\vartheta,2+2\vartheta,2+3\vartheta\}$

$I_0 \subseteq I_{2\vartheta} \subseteq I_2 = I_{2+2\vartheta} \subseteq I_\vartheta = I_{3\vartheta} = I_{2+\vartheta} = I_{2+3\vartheta} \subseteq Z_4 + \vartheta Z_4$ dir.

$Z_4R_1 = \{(p,q) : p \in Z_4, q \in R_1\}$ şeklinde tanımlanan $Z_4Z_4[\vartheta]$ halkası bilinen çarpma işlemi altında kapalı olmadığından R_1-modül değildir. Bu nedenle aşağıdaki tanımda verilen θ dönüşümü kullanılarak yeni bir çarpma işlemi tanımlanacaktır. Böylece bu halkanın R_1-modül olması sağlanacaktır.

Tanım 5.1.1. $p,q \in Z_4$, $P+\vartheta q \in R_1$ olmak üzere ,

$$\theta : R_1 \to Z_4$$

$$p+\vartheta q \to p$$

olacak şekilde tanımlansın.

$\forall p+\vartheta q, r+\vartheta k \in R_1$ için

$$\theta\big((p+\vartheta q)+(r+\vartheta k)\big)=\theta\big((p+r)+\vartheta(q+k)\big)=$$
$$p+r=\theta(p+\vartheta q)+\theta(r+\vartheta k)$$

$\forall t \in Z_4$ için $\theta\big(t(p+\vartheta q)\big)=\theta\big(tp+\vartheta tq\big)$
$= tp = t\theta(p+\vartheta q)$

olduğundan θ dönüşümü bir halka homomorfizmasıdır.

Şimdi bu homomorfizma yardımı ile herhangi bir $(p,q) \in Z_4 R_1$ ve $m \in R_1$ için çarpma ; $m*(p,q)=(\theta(m)p, mq)$ şeklinde tanımlansın.Bu çarpma

$Z_4^{\alpha} R_1^{\beta}$ halkasına genişletilerek herhangi bir

$m \in R_1$ ve $d=(p_0, p_1, ..., p_{\alpha-1}, q_0, ..., q_{\beta-1}) \in Z_4^{\alpha} R_1^{\beta}$ için

$md=\big(\theta(m)p_0, ..., \theta(m)p_{\alpha-1}, mq_0, ..., mq_{\beta-1}\big)$ şeklindedir.

Önerme 5.1.1. $Z_4^{\alpha} R_1^{\beta}$ halkası yukarıda tanımlanan çarma işlemi ile bir R_1-modüldür.

İspat: $\forall s, \tilde{s} \in R$ ve

$\forall w=(p_0, p_1, ..., p_{\alpha-1}, q_0, q_1, ..., q_{\beta-1})$, $\breve{w}=(\overline{p}_0, \overline{p}_1, ..., \overline{p}_{\alpha-1}, \overline{q}_0, \overline{q}_1, ..., \overline{q}_{\beta-1}) \in Z_4^{\alpha} \times R^{\beta}$
için

i. $s(w+\breve{w}) = s(p_0+\bar{p}_0+.....+p_{\alpha-1}+\bar{p}_{\alpha-1}, q_0+\bar{q}_0+.....+q_{\beta-1}+\bar{q}_{\beta-1})$

$= (\theta(s)(p_0+\bar{p}_0)+.....+\theta(s)(p_{\alpha-1}+\bar{p}_{\alpha-1}), s(q_0+\bar{q}_0)+...+s(q_{\beta-1}+\bar{q}_{\beta-1}))$

$= (\theta(s)p_0,....., \theta(s)p_{\alpha-1}, sq_0,...., sq_{\beta-1}) + (\theta(s)\bar{p}_0,...., \theta(s)\bar{p}_{\alpha-1}, s\bar{q}_0,....., s\bar{q}_{\beta-1})$

$= sw + s\breve{w}$

ii. $(s+\tilde{s})w = (\theta(s+\tilde{s})p_0,...., \theta(s+\tilde{s})p_{\alpha-1}, (s+\tilde{s})q_0,...., (s+\tilde{s})q_{\beta-1})$

$= ((\theta(s)+\theta(\tilde{s}))p_0,...., (\theta(s)+\theta(\tilde{s}))p_{\alpha-1}, sq_0+\tilde{s}q_0,....., sq_{\beta-1}+\tilde{s}q_{\beta-1})$

$= (\theta(s)p_0,...., \theta(s)p_{\alpha-1}, sq_0,....., sq_{\beta-1}) + (\theta(\tilde{s})p_0,....., \theta(\tilde{s})p_{\alpha-1}, \tilde{s}q_0,...., \tilde{s}q_{\beta-1})$

$= sw + \tilde{s}w$

iii. $s(\tilde{s})w = s(\theta(\tilde{s})p_0,...., \theta(\tilde{s})p_{\alpha-1}, \tilde{s}q_0,....\tilde{s}q_{\beta-1})$

$= (\theta(s)\theta(\tilde{s})p_0,...., \theta(s)\theta(\tilde{s})p_{\alpha-1}, s\tilde{s}q_0,....., s\tilde{s}q_{\beta-1})$

$= (\theta(s\tilde{s})p_0,....., \theta(s\tilde{s})p_{\alpha-1}, s\tilde{s}q_0,....., s\tilde{s}q_{\beta-1})$

$= (s\tilde{s})w$

iv. $\theta(1)=1$ olup $\forall w = (p_0,....., p_{\alpha-1}, q_0,....., q_{\beta-1}) \in Z_4^{\alpha}R^{\beta}$ için,

$1_{R_1} w = 1_{R_1}(p_0,....., p_{\alpha-1}, q_0,....., q_{\beta-1}) = (\theta(1_{R_1})p_0,....., \theta(1_{R_1})p_{\alpha-1}, q_0,....., q_{\beta-1})$

$= (p_0,...., p_{\alpha-1}, q_0,....q_{\beta-1}) = w$

elde edilir. Böylece $Z_4{}^{\alpha}R^{\beta}$ halkası yukarıda tanımlanan çarpma işlemi ile bir R_1-modüldür.

Tanım 5.1.2. $Z_4^{\alpha}R_1^{\beta}$ nın boş olmayan bir C alt kümesi $Z_4^{\alpha}R_1^{\beta}$ nın R_1-alt modülü ise C'ye Z_4R_1-lineer kod denir.

5.1.1 $\vartheta^2 = 2,\ Z_4 Z_4[\vartheta] - (\varphi)$ – Sabit devirli kodun gray görüntüsü

Tanım 5.1.1.1. Herhangi bir $c = (p_0, p_1, ..., p_{\alpha-1}, q_0, q_1, ..., q_{\beta-1}) \in C$ için T_φ – sabit devir ötelemesi ile $T_\varphi(c) = \left(p_{\alpha-1}, p_0, ..., p_{\alpha-2}, \varphi q_{\beta-1}, q_0, ..., q_{\beta-2}\right) \in C$ ise $Z_4^\alpha \times \left(Z_4 + \vartheta Z_4\right)^\beta$ nin C, $Z_4 + \vartheta Z_4$ – alt modülüne $Z_4 Z_4[\vartheta]$ – lineer $T_{(\varphi)}$ – sabit devirli kod denir.

Not. $\varphi = 1$ ise C kodunun devirli kod olduğu açıktır.

Not. $\varphi = -1$ ise C koduna negatif devirli kod denir.

Not. $\varphi = 3,1+\vartheta,3+\vartheta,1+2\vartheta,3+2\vartheta,1+3\vartheta,3+3\vartheta$ ise C koduna sabit devirli kod denir. Bu halkada sadece 3 birim eleman seçilerek çalışılmıştır.

$(p_0, ..., p_{\alpha-1}, q_0, ...q_{\beta-1}) \in C$ kod sözü polinom cinsinden aşağıdaki gibi ifade edilebilir:

$$c(x) = (p_0 + p_1 x + ... + p_{\alpha-1} x^{\alpha-1} \mid q_0 + q_1 x + ... + q_{\beta-1} x^{\beta-1}) = (p(x), q(x))$$

$$\left(p(x), q(x)\right) \in Z_4[x] \Big/ < x^\alpha - 1 > \times R_1[x] \Big/ < x^\beta - \varphi >$$

Şimdi; $\hat{r}(x) = (\hat{r}_0 + \hat{r}_1 x + ... + \hat{r}_l x^l) \in R_1[x]$ ve

$\left(h(x), g(x)\right) \in Z_4[x] \Big/ < x^\alpha - 1 > \times R_1[x] \Big/ < x^\beta - \varphi >$ olsun.

$\theta\left(\hat{r}(x)\right) = \theta(\hat{r}_0) + ... + \theta(\hat{r}_l) x^l$ olmak üzere,

$\hat{r}(x)\left(h(x), g(x)\right) = \left(\theta(\hat{r}(x)) h(x), \hat{r}(x) g(x)\right)$ elde edilir.

Tanım 5.1.1.2. C'nin Z_4R_1 üzerinde (α,β) uzunluğunda $\varphi-$sabit devirli kod olması için gerek ve yeter şart C nin $R_{\alpha,\beta,\varphi}=Z_4[x]/\langle x^{\alpha}-1\rangle\times R_1[x]/\langle x^{\beta}-\varphi\rangle$ nın $Z_4[\vartheta][x]-$ alt modülü olmasıdır.

İspat. C bir $\varphi-$sabit devirli kod ve $c\in C$ olsun. $c(x)=(p(x),q(x))\in C$ yazılır.Biliyoruz ki $x^i*(p(x),g(x))\in C \quad i\geq 1$ için de yazılır. C nin lineerliğinden dolayı herhangi bir $r(x)\in Z_4[\vartheta][x]$ için $r(x)(p(x),q(x))\in C$ dir. O halde C, $R_{\alpha,\beta,\varphi}$ ' nın $Z_4[\vartheta][x]-$alt modülüdür.Tersine C, $R_{\alpha,\beta,\varphi}$ nın $Z_4[\vartheta][x]-$alt modülü olsun.O zaman $x*c(x)\in C$ dir.Dolayısıyla C, Z_4R_1- sabit devirli koddur. 4 yeni gray map tanımı; $r=p+\vartheta q\in Z_4[\vartheta]$ için

$$\zeta_1: Z_4[\vartheta]\to Z_4^2 \qquad \zeta_2: Z_4[\vartheta]\to Z_4^2$$
$$p+\vartheta q\to(2q,2p+2q) \qquad p+\vartheta q\to(p+2q,2p+2q)$$

$$\zeta_3: Z_4[\vartheta]\to Z_4^2 \qquad \zeta_4: Z_4[\vartheta]\to Z_4^2$$
$$P+\vartheta q\to(2q+3p,2p) \qquad p+\vartheta q\to(2p+2q,2q)$$

şeklinde tanımlı $\zeta_1,\zeta_2,\zeta_3,\zeta_4$ dönüşümüne $Z_4[\vartheta]$ üzerinde tanımlı **Gray dönüşüm** denir.Bu dönüşümler $Z_4[\vartheta]^{\beta}$ dan $Z_4^{2\beta}$ ya genişletilebilir.

$r_i=p_i+\vartheta q_i\in Z_4[\vartheta], i=0,1,...,i-1$ için

$$\zeta_1: Z_4[\vartheta]^{\beta}\to Z_4^{2\beta}$$
$$\zeta_1(r_0,....,r_{\beta-1})\to(2q_0,....,2q_{\beta-1},2p_0+2q_0,....,2p_{\beta-1}+2q_{\beta-1})$$

$$\zeta_2: Z_4[\vartheta]^{\beta}\to Z_4^{2\beta}$$
$$\zeta_2(r_0,....,r_{\beta-1})\to(p_0+2q_0,....,p_{\beta-1}+2q_{\beta-1},2p_0+2q_0,...,2p_{\beta-1}+2q_{\beta-1})$$

$\zeta_3 : Z_4[\vartheta]^\beta \to Z_4^{2\beta}$
$\zeta_3(r_0,....,r_{\beta-1}) \to (2q_0+3p_0,....,2q_{\beta-1}+3p_{\beta-1},2p_0,...,2p_{\beta-1})$

$\zeta_4 : Z_4[\vartheta]^\beta \to Z_4^{2\beta}$
$\zeta_4(r_0,...,r_{\beta-1}) \to (2p_0+2q_0,....,2p_{\beta-1}+2q_{\beta-1},2q_0,...,2q_{\beta-1})$

Tanım 5.1.1.3. w_G , Z_4^2 vektör uzayı üzerinde tanımlı Hamming ağırlık olmak üzere $c \in Z_4[\vartheta]^\beta$ için $w_L(c) = w_G\left(\zeta_{1,2,3,4}(c)\right)$ şeklinde tanımlanan w_L fonksiyonuna Z_4 üzerinde **Lee ağırlığı** denir.

Tanım 5.1.1.4. Her $c,\hat{c} \in Z_4[\vartheta]^\beta$ için $d_L(c,\hat{c}) = w_L(c-\hat{c})$ şeklinde tanımlanan d_L fonksiyonuna **Lee uzaklık** denir.

Teorem 5.1.1.1. $\zeta_{1,2,3,4}$: $(Z_4[\vartheta]^\beta, d_L) \to (Z_4^{2\beta}, d_H)$ şeklinde tanımlanan Gray dönüşümler uzaklık koruyan dönüşümlerdir.

İspat. $\forall c_1, c_2 \in Z_4[\vartheta]^\beta$ olsun.Bu durumda $\zeta_{1,2,3,4}(c_1-c_2) = \zeta_{1,2,3,4}(c_1) - \zeta_{1,2,3,4}(c_2)$ dir.

$d_L(c_1,c_2) = w_L(c_1-c_2)$
$= w_H\left(\zeta_{1,2,3,4}(c_1-c_2)\right)$
$= w_H\left(\zeta_{1,2,3,4}(c_1) - \zeta_{1,2,3,4}(c_2)\right)$
$= d_H\left(\zeta_{1,2,3,4}(c_1), \zeta_{1,2,3,4}(c_2)\right)$

eşitliği elde edilir. O halde $\zeta_{1,2,3,4}$ uzaklık koruyan dönüşümlerdir.

Not. Burada $\zeta_{1,2,3,4} = \zeta_1, \zeta_2, \zeta_3, \zeta_4$ gray dönüşümlerini kastetmektedir.

Önerme 5.1.1.1. ζ_1, $Z_4[\vartheta]^\beta$ kümesinden $Z_4^{2\beta}$ kümesine gray dönüşümü $T_\varphi - \varphi$ sabit devirli öteleme, $\varphi = 1+\vartheta$ ve ϖ devirli öteleme operatörü olmak üzere $\zeta_1 T_\varphi = \varpi\zeta_1$ dir.

İspat. $r_i = p_i + \vartheta q_i \in Z_4[\vartheta]$, $i = 0,1,.....,\beta-1$ için $r = (r_0, r_1, ..., r_{\beta-1}) \in Z_4[\vartheta]^\beta$ ve $\varphi = 1+\vartheta$ olmak üzere

$$\zeta_1 T_\varphi(r) = \zeta_1(\varphi r_{\beta-1}, r_0, ..., r_{\beta-2})$$
$$= (2p_{\beta-1} + 2q_{\beta-1}, 2q_0, ..., 2q_{\beta-2}, 2p_0 + 2q_0, ..., 2p_{\beta-2} + 2q_{\beta-2})$$

Diğer yandan;

$$\varpi\zeta_1(r) = \varpi(3q_0, ..., 3q_{\beta-1}, 2p_0 + q_0, ..., 2p_{\beta-1} + q_{\beta-1})$$
$$= (2p_{\beta-1} + 2q_{\beta-1}, 2q_0, ..., 2q_{\beta-2}, 2p_0 + 2q_0, ..., 2p_{\beta-2} + 2q_{\beta-2})$$

Görülür ki $\zeta_1 T_\varphi = \varpi\zeta_1$ dir.

Teorem 5.1.1.2. C kodunun $Z_4[\vartheta]$ üzerinde β uzunluğunda bir sabit devirli kod olması için , $\zeta_1(C)$ kodunun Z_4 üzerinde tanımlı 2β uzunluğunda bir devirli kod olmasıdır.

İspat. C bir $\varphi-$sabit devirli kod, $T_\varphi(C) = C$ dir. (Önerme 5.1.1.1'den) $\zeta_1 T_\varphi(C) = \zeta_1(C) = \varpi\zeta_1(C)$ olup $\zeta_1(C)$, Z_4 üzerinde 2β uzunluğunda bir devirli koddur.

Önerme 5.1.1.2. ζ_2, $Z_4[\vartheta]^\beta$ kümesinden $Z_4^{2\beta}$ kümesine gray dönüşümü $T_\varphi - \varphi$ sabit devirli öteleme, $\varphi = 1+2\vartheta$ ve ε-parçalı devirli öteleme operatörü olmak üzere $\zeta_2 T_\varphi = \varepsilon\zeta_2$ dir.

İspat. $r_i = p_i + \vartheta q_i \in Z_4[\vartheta],\ i = 0,1,...,\beta-1$ için $r = (r_0, ..., r_{\beta-1}) \in Z_4[\vartheta]^\beta$ ve $\varphi = 1+2\vartheta$ olmak üzere

$$\zeta_2 T_\varphi(r) = \zeta_2(\varphi r_{\beta-1}, r_0, ..., r_{\beta-2})$$
$$= (p_{\beta-1} + 2q_{\beta-1}, p_0 + 2q_0, ..., p_{\beta-2} + 2q_{\beta-2}, 2p_{\beta-1} + 2q_{\beta-1}, 2p_0 + 2q_0, ..., 2p_{\beta-2} + 2q_{\beta-2})$$

Diğer yandan

$$\varepsilon\zeta_2(r) = \varepsilon(p_0 + 2q_0, ..., p_{\beta-1} + 2q_{\beta-1}, 2p_0 + 2q_0, ..., 2p_{\beta-1} + 2q_{\beta-1})$$

$$= (p_{\beta-1} + 2q_{\beta-1}, ..., p_{\beta-2} + 2q_{\beta-2}, 2p_{\beta-1} + 2q_{\beta-1}, ..., 2p_{\beta-2} + 2q_{\beta-2})$$

Görülür ki $\zeta_2 T_\varphi = \varepsilon\zeta_2$ dir.

Teorem 5.1.1.3. C kodunun $Z_4[\vartheta]$ üzerinde β uzunluğunda bir sabit devirli kod olması için , $\zeta_2(C)$ kodunun Z_4 üzerinde tanımlı 2β uzunluğunda indeksi 2 olan bir parçalı devirli kod olmasıdır.

İspat. C bir $\varphi-$sabit devirli kod, $T_\varphi(C) = C$ dir. (Önerme 5.1.1.2'den) $\zeta_2 T_\varphi(C) = \zeta_2(C) = \varepsilon\zeta_2(C)$ olup Z_4, üzerinde 2β uzunluğunda indeksi 2 olan parçalı devirli bir koddur.

Önerme 5.1.1.3. ζ_3, $Z_4[\vartheta]^\beta$ kümesinden $Z_4^{2\beta}$ kümesine gray dönüşümü $T_\varphi - \varphi$ sabit devirli öteleme, $\varphi = 1 + 2\vartheta$ ve ε -parçalı devirli öteleme operatörü olmak üzere $\zeta_3 T_\varphi = \varepsilon\zeta_3$ dir.

İspat. $r_i = p_i + \vartheta q_i \in Z_4[\vartheta], \quad i = 0,1,..., \beta-1$ için $r = (r_0, ..., r_{\beta-1}) \in Z_4[\vartheta]^\beta$ ve $\varphi = 1 + 2\vartheta$ olmak üzere

$$\zeta_3 T_\varphi(r) = \zeta_3(\varphi r_{\beta-1}, r_0, ..., r_{\beta-2})$$
$$= (2q_{\beta-1} + 3p_{\beta-1}, 2q_0 + 3p_0, ..., 2q_{\beta-2} + 3p_{\beta-2}, 2p_{\beta-1}, ..., 2p_{\beta-2})$$

Diğer yandan

$$\varepsilon\zeta_3(r) = \varepsilon(2q_0 + 3p_0, ..., 2q_{\beta-1} + 3p_{\beta-1}, 2p_0, 2p_1, ..., 2p_{\beta-1})$$

$$= (2q_{\beta-1} + 3p_{\beta-1}, 2q_0 + 3p_0, ..., 2q_{\beta-2} + 3p_{\beta-2}, 2p_{\beta-1}, ..., 2p_{\beta-2})$$

Görülür ki $\zeta_3 T_\varphi = \varepsilon\zeta_3$ dür.

Teorem 5.1.1.4. C kodunun $Z_4[\vartheta]$ üzerinde β uzunluğunda bir sabit devirli kod olması için , $\zeta_3(C)$ kodunun Z_4 üzerinde tanımlı 2β uzunluğunda indeksi 2 olan bir parçalı devirli kod olmasıdır.

İspat. C bir $\varphi-$sabit devirli kod, $T_\varphi(C)=C$ dir. (Önerme 5.1.1.3'den) $\zeta_3 T_\varphi(C)=\zeta_3(C)=\varepsilon\zeta_3(C)$ olup Z_4, üzerinde 2β uzunluğunda indeksi 2 olan parçalı devirli bir koddur.

Önerme 5.1.1.4. ζ_4, $Z_4[\vartheta]^\beta$ kümesinden $Z_4^{2\beta}$ kümesine gray dönüşümü $T_\varphi-\varphi$ sabit devirli öteleme, $\varphi=1+3\vartheta$ ve $\varpi-$devirli öteleme operatörü olmak üzere $\zeta_4 T_\varphi=\varpi\zeta_4$ dir.

İspat. $r_i=p_i+\vartheta q_i\in Z_4[\vartheta]$, $i=0,1,.....,\beta-1$ için $r=(r_0,r_1,.....,r_{\beta-1})\in Z_4[\vartheta]^\beta$ ve $\varphi=1+3\vartheta$ olmak üzere

$$\zeta_4 T_\varphi(r)=\zeta_4(\varphi r_{\beta-1},r_0,.....,r_{\beta-2})$$

$$=(2q_{\beta-1},2p_0+2q_0,....,2p_{\beta-2}+2q_{\beta-2},2q_0,.....,2q_{\beta-2})$$

Diğer yandan;

$$\varpi\zeta_4(r)=\varpi(2p_0+2q_0,.....,2p_{\beta-1}+2q_{\beta-1},2q_0,....,2q_{\beta-1})$$

$$=(2q_{\beta-1},2p_0+2q_0,....,2p_{\beta-2}+2q_{\beta-2},2q_0,.....,2q_{\beta-2})$$

Görülür ki $\zeta_4 T_\varphi=\varpi\zeta_4$ dir.

Teorem 5.1.1.5. C**,** kodunun $Z_4[\vartheta]$ üzerinde β uzunluğunda bir sabit devirli kod olması için , $\zeta_4(C)$ kodunun Z_4 üzerinde tanımlı 2β uzunluğunda bir devirli kod olmasıdır.

İspat. C bir $\varphi-$sabit devirli kod, $T_\varphi(C)=C$ dir. (Önerme 5.1.1.4'den) $\zeta_4 T_\varphi(C)=\zeta_4(C)=\varpi\zeta_4(C)$ olup $\zeta_4(C)$, Z_4 üzerinde 2β uzunluğunda bir devirli koddur.

Şimdi ζ_1 gray dönüşümü yardımıyla $\ddot{\zeta}_1$ gray dönüşümünü tanmlıyoruz.

$$\ddot{\zeta}_1 :\ Z_4\times Z_4[\vartheta]\to Z_4^3$$

$$\ddot{\zeta}_1(c,p+\vartheta q)\to(c,\zeta_1(p+\vartheta q))=(c,2q,2p+2q)\qquad p,q,c\in Z_4$$

$\ddot{\zeta}_1$ dönüşümünü genişletirsek,

$$\ddot{\zeta}_1 :\ Z_4^\alpha\times Z_4[\vartheta]^\beta\to Z_4^{\alpha+2\beta}$$

$$\ddot{\zeta}_1(c_0,c_1,....c_{\alpha-1},r_0,r_1,.....,r_{\beta-1})$$

$$=(c_0,.....,c_{\alpha-1},2q_0,2q_1,.....,2q_{\beta-1},2p_0+2q_0,....,2p_{\beta-1}+2q_{\beta-1})$$

$r_i=p_i+\vartheta q_i\in Z_4[\vartheta]$ ve $i=0,1,....,\beta-1$ için $p_i,q_i,c_i\in Z_4$ dir.

Teorem 5.1.1.6. C**,** $\dfrac{Z_4[x]}{\langle x^\alpha-\theta(\varphi)\rangle}\times\dfrac{R_1[x]}{\langle x^\beta-\varphi\rangle}$ de sabit devirli kod olsun.Bu durumda $\varphi=1+\vartheta$ için $\alpha=\beta$ ise $\ddot{\zeta}_1(C)$, 2 indeksli parçalı devirli koddur.Eğer $\alpha\neq\beta$ ise $\ddot{\zeta}_1(C)$, 2 indeksli genelleştirilmiş parçalı devirli koddur.

İspat. C, $\dfrac{Z_4[x]}{\langle x^\alpha-\theta(\varphi)\rangle}\times\dfrac{R_1[x]}{\langle x^\beta-\varphi\rangle}$ de sabit devirli kod olsun.

$c=\left(c_0,c_1,....,c_{\alpha-1},r_0,r_1,....,r_{\beta-1}\right)=\left(c_0,c_1,.....,c_{\alpha-1},p_0+\vartheta q_0,p_1+\vartheta q_1,...,p_{\beta-1}+\vartheta q_{\beta-1}\right)\in C$ alalım. $\varphi=1+\vartheta$ için $\theta(\varphi)=1$ dir. ε, parçalı devirli öteleme operatörü ve $T_\varphi-\varphi$ sabit devirli öteleme operatörü olsun. C, $\frac{Z_4[x]}{\langle x^\alpha-1\rangle}\times\frac{R_1[x]}{\langle x^\beta-(1+\vartheta)\rangle}$ de sabit devirli kod olduğundan,

$$T_\varphi(c)=\left(\theta(1+\vartheta)c_{\alpha-1},c_0,....,c_{\alpha-2},(1+\vartheta)r_{\beta-1},r_0,....,r_{\beta-2}\right)$$

$$=\left(c_{\alpha-1},c_0,...,c_{\alpha-2},(1+\vartheta)(p_{\beta-1}+\vartheta q_{\beta-1}),p_0+\vartheta q_0,....,p_{\beta-2}+\vartheta q_{\beta-2}\right)$$

$$=\left(c_{\alpha-1},c_0,....,c_{\alpha-2},p_{\beta-1}+2q_{\beta-1}+\vartheta(p_{\beta-1}+q_{\beta-1}),p_0+\vartheta q_0,....,p_{\beta-2}+\vartheta q_{\beta-2}\right)$$

olup $\ddot{\zeta}_1$ uygulanarak,

$$\ddot{\zeta}_1\left(T_\varphi(c)\right)=$$
$$(c_{\alpha-1},c_0,.....,c_{\alpha-1},2p_{\beta-1}+2q_{\beta-1},2q_0,...,2q_{\beta-2},2p_0+2q_0,....,2p_{\beta-2}+2q_{\beta-2})$$

elde edilir.Diğer taraftan,

$$\ddot{\zeta}_1(c)=(c_0,.....,c_{\alpha-1},2q_0,2q_1,.....,2q_{\beta-1},2p_0+2q_0,2p_1+2q_1,....,2p_{\beta-1}+2q_{\beta-1})$$ dir.

Buradan,

$$\varepsilon\left(\ddot{\zeta}_1(c)\right)=(c_{\alpha-1},c_0,.....,c_{\alpha-2},2p_{\beta-1}+2q_{\beta-1},2q_0,...,2q_{\beta-2},2p_0+2q_0,....,2p_{\beta-2}+2q_{\beta-2})$$
bulunur.

Böylece $\ddot{\zeta}_1\left(T_\varphi(c)\right)=\varepsilon\ddot{\zeta}_1(c)$ dir.Eğer $\alpha=\beta$ ise $\ddot{\zeta}_1(C)$, 2 indeksli parçalı devirli koddur. Eğer $\alpha\neq\beta$ ise $\ddot{\zeta}_1(C)$, 2 indeksli genelleştirilmiş parçalı devirli koddur.

Şimdi ζ_2 gray dönüşümü yardımıyla $\ddot{\zeta}_2$ gray dönüşümünü tanmlayalım.

$\ddot{\zeta}_2 :\ \ Z_4 \times Z_4[\vartheta] \to Z_4^3$

$\ddot{\zeta}_2(c, p+\vartheta q) \to (c, \zeta_2(p+\vartheta q)) = (c, p+2q, 2p+2q) \qquad p,q,c \in Z_4$

$\ddot{\zeta}_2$ dönüşümünü genişletirsek,

$\ddot{\zeta}_2 :\ \ Z_4^{\alpha} \times Z_4[\vartheta]^{\beta} \to Z_4^{\alpha+2\beta}$

$\ddot{\zeta}_2(c_0, c_1, ...c_{\alpha-1}, r_0, r_1, ..., r_{\beta-1})$

$= (c_0, ..., c_{\alpha-1}, p_0 + 2q_0, ..., p_{\beta-1} + 2q_{\beta-1}, 2p_0 + 2q_0, ..., 2p_{\beta-1} + 2q_{\beta-1})$

$r_i = p_i + \vartheta q_i \in Z_4[\vartheta]$ ve $i = 0,1,....,\beta-1$ için $p_i, q_i, c_i \in Z_4$ dir.

Teorem 5.1.1.7. C, $\dfrac{Z_4[x]}{\langle x^{\alpha} - \theta(\varphi)\rangle} \times \dfrac{R_1[x]}{\langle x^{\beta} - \varphi\rangle}$ de sabit devirli kod olsun.Bu durumda $\varphi = 1+2\vartheta$ için $\alpha = \beta$ ise $\ddot{\zeta}_2(C)$, 3 indeksli parçalı devirli koddur.Eğer $\alpha \neq \beta$ ise $\ddot{\zeta}_2(C)$, 3 indeksli genelleştirilmiş parçalı devirli koddur.

İspat. C, $\dfrac{Z_4[x]}{\langle x^{\alpha} - \theta(\varphi)\rangle} \times \dfrac{R_1[x]}{\langle x^{\beta} - \varphi\rangle}$ de sabit devirli kod olsun.

$c = \left(c_0, c_1, ..., c_{\alpha-1}, r_0, r_1, ..., r_{\beta-1}\right) = \left(c_0, c_1, ..., c_{\alpha-1}, p_0 + \vartheta q_0, p_1 + \vartheta q_1, ..., p_{\beta-1} + \vartheta q_{\beta-1}\right) \in C$ alalım. $\varphi = 1+2\vartheta$ için $\theta(\varphi) = 1$ dir. ε, parçalı devirli öteleme operatörü ve $T_{\varphi} - \varphi$ sabit devirli öteleme operatörü olsun. C, $\dfrac{Z_4[x]}{\langle x^{\alpha} - 1\rangle} \times \dfrac{R_1[x]}{\langle x^{\beta} - (1+2\vartheta)\rangle}$ de sabit devirli kod olduğundan,

$T_{\varphi}(c) = \left(\theta(1+2\vartheta)c_{\alpha-1}, c_0, ..., c_{\alpha-2}, (1+2\vartheta)r_{\beta-1}, r_0, ..., r_{\beta-2}\right)$

$= \left(c_{\alpha-1}, c_0, ..., c_{\alpha-2}, (1+2\vartheta)(p_{\beta-1} + \vartheta q_{\beta-1}), p_0 + \vartheta q_0, ..., p_{\beta-2} + \vartheta q_{\beta-2}\right)$

$$=\left(c_{\alpha-1},c_0,....,c_{\alpha-2},p_{\beta-1}+\vartheta(2p_{\beta-1}+q_{\beta-1}),p_0+\vartheta q_0,....,p_{\beta-2}+\vartheta q_{\beta-2}\right)$$

olup $\ddot{\zeta}_2$ uygulanarak,

$$\ddot{\zeta}_2\left(T_\varphi(c)\right)=$$

$$(c_{\alpha-1},...,c_{\alpha-2},p_{\beta-1}+2q_{\beta-1},.....,p_{\beta-2}+2q_{\beta-2},2p_{\beta-1}+2q_{\beta-1},....,2p_{\beta-2}+2q_{\beta-2})$$

elde edilir.

Diğer taraftan,

$\ddot{\zeta}_2(c)=(c_0,.....,c_{\alpha-1},p_0+2q_0,...,p_{\beta-1}+2q_{\beta-1},2p_0+2q_0,....,2p_{\beta-1}+2q_{\beta-1})$ dir.

$$\varepsilon\left(\ddot{\zeta}_2(c)\right)=$$

$(c_{\alpha-1},...,c_{\alpha-2},p_{\beta-1}+2q_{\beta-1},.....,p_{\beta-2}+2q_{\beta-2},2p_{\beta-1}+2q_{\beta-1},....,2p_{\beta-2}+2q_{\beta-2})$ bulunur.

Böylece $\ddot{\zeta}_2\left(T_\varphi(c)\right)=\varepsilon\ddot{\zeta}_2(c)$ dir.Eğer $\alpha=\beta$ ise $\ddot{\zeta}_2(C)$, 3 indeksli parçalı devirli koddur.

Eğer $\alpha\neq\beta$ ise $\ddot{\zeta}_2(C)$, 3 indeksli genelleştirilmiş parçalı devirli koddur.

Şimdi ζ_3 gray dönüşümü yardımıyla $\ddot{\zeta}_3$ gray dönüşümünü tanmlayalım.

$\ddot{\zeta}_3$: $Z_4\times Z_4[\vartheta]\rightarrow Z_4^3$

$\ddot{\zeta}_3(c,p+\vartheta q)\rightarrow(c,\zeta_3(p+\vartheta q))=(c,2q+3p,2p)\quad p,q,c\in Z_4$

$\ddot{\zeta}_3$ dönüşümünü genişletirsek,

$\ddot{\zeta}_3$: $Z_4^\alpha\times Z_4[\vartheta]^\beta\rightarrow Z_4^{\alpha+2\beta}$

$\ddot{\zeta}_3(c_0,c_1,....c_{\alpha-1},r_0,r_1,.....,r_{\beta-1})$

$$= (c_0, c_1, ..., c_{\alpha-1}, 2q_0 + 3p_0, ..., 2q_{\beta-1} + 3p_{\beta-1}, 2p_0, 2p_1, ..., 2p_{\beta-1})$$

$r_i = p_i + \vartheta q_i \in Z_4[\vartheta]$ ve $i = 0,1,...., \beta - 1$ için $p_i, q_i, c_i \in Z_4$ dir.

Teorem 5.1.1.8. C, $\frac{Z_4[x]}{\langle x^\alpha - \theta(\varphi)\rangle} \times \frac{R_1[x]}{\langle x^\beta - \varphi\rangle}$ de sabit devirli kod olsun.Bu durumda

$\varphi = 1 + 2\vartheta$ için $\alpha = \beta$ ise $\ddot{\zeta}_3(C)$, 3 indeksli parçalı devirli koddur.Eğer $\alpha \neq \beta$ ise $\ddot{\zeta}_3(C)$, 3 indeksli genelleştirilmiş parçalı devirli koddur.

İspat. C, $\frac{Z_4[x]}{\langle x^\alpha - \theta(\varphi)\rangle} \times \frac{R_1[x]}{\langle x^\beta - \varphi\rangle}$ de sabit devirli kod olsun.

$$c = \left(c_0, c_1, ..., c_{\alpha-1}, r_0, r_1, ..., r_{\beta-1}\right) = \left(c_0, c_1, ..., c_{\alpha-1}, p_0 + \vartheta q_0, p_1 + \vartheta q_1, ..., p_{\beta-1} + \vartheta q_{\beta-1}\right) \in C$$

alalım. $\varphi = 1 + 2\vartheta$ için $\theta(\varphi) = 1$ dir. ε, parçalı devirli öteleme operatörü ve $T_\varphi - \varphi$ sabit devirli öteleme operatörü olsun. C, $\frac{Z_4[x]}{\langle x^\alpha - 1\rangle} \times \frac{R_1[x]}{\langle x^\beta - (1 + 2\vartheta)\rangle}$ de sabit devirli kod olduğundan,

$$T_\varphi(c) = \left(\theta(1 + 2\vartheta)c_{\alpha-1}, c_0, ..., c_{\alpha-2}, (1 + 2\vartheta)r_{\beta-1}, r_0, ..., r_{\beta-2}\right)$$

$$= \left(c_{\alpha-1}, c_0, ..., c_{\alpha-2}, (1 + 2\vartheta)(p_{\beta-1} + \vartheta q_{\beta-1}), p_0 + \vartheta q_0, ..., p_{\beta-2} + \vartheta q_{\beta-2}\right)$$

$$= \left(c_{\alpha-1}, c_0, ..., c_{\alpha-2}, p_{\beta-1} + \vartheta(2p_{\beta-1} + q_{\beta-1}), p_0 + \vartheta q_0, ..., p_{\beta-2} + \vartheta q_{\beta-2}\right)$$

olup $\ddot{\zeta}_3$ uygulanarak,

$$\ddot{\zeta}_3\left(T_\varphi(c)\right)$$

$$= (c_{\alpha-1}, c_0, ..., c_{\alpha-2}, 2q_{\beta-1} + 3p_{\beta-1}, 2q_0 + 3p_0, ..., 2q_{\beta-2} + 3p_{\beta-2}, 2p_{\beta-1}, ..., 2p_{\beta-2})$$

elde edilir.

Diğer taraftan,

$\ddot{\zeta}_3(c) = (c_0, c_1, ..., c_{\alpha-1}, 2q_0 + 3p_0, ..., 2q_{\beta-1} + 3p_{\beta-1}, 2p_0, 2p_1, ..., 2p_{\beta-1})$ dir.

$\varepsilon\left(\ddot{\zeta}_3(c)\right) =$

$(c_{\alpha-1}, c_0, ..., c_{\alpha-2}, 2q_{\beta-1} + 3p_{\beta-1}, 2q_0 + 3p_0, ..., 2q_{\beta-2} + 3p_{\beta-2}, 2p_{\beta-1}, ..., 2p_{\beta-2})$ bulunur.

Böylece $\ddot{\zeta}_3\left(T_\varphi(c)\right) = \varepsilon\ddot{\zeta}_3(c)$ dir.Eğer $\alpha = \beta$ ise $\ddot{\zeta}_3(C)$, 3 indeksli parçalı devirli koddur. Eğer $\alpha \neq \beta$ ise $\ddot{\zeta}_3(C)$, 3 indeksli genelleştirilmiş parçalı devirli koddur.

Şimdi ζ_4 gray dönüşümü yardımıyla $\ddot{\zeta}_4$ gray dönüşümünü tanmlayalım.

$\ddot{\zeta}_4 : \quad Z_4 \times Z_4[\vartheta] \to Z_4^3$

$\ddot{\zeta}_4(c, p + \vartheta q) \to (c, \zeta_4(p + \vartheta q)) = (c, 2p + 2q, 2q) \qquad p, q, c \in Z_4$

$\ddot{\zeta}_4$ dönüşümünü genişletirsek,

$\ddot{\zeta}_4 : \quad Z_4^\alpha \times Z_4[\vartheta]^\beta \to Z_4^{\alpha+2\beta}$

$\ddot{\zeta}_4(c_0, c_1, ...c_{\alpha-1}, r_0, r_1, ..., r_{\beta-1})$

$= (c_0, ..., c_{\alpha-1}, 2p_0 + 2q_0, ..., 2p_{\beta-1} + 2q_{\beta-1}, 2q_0, 2q_1, ..., 2q_{\beta-1})$

$r_i = p_i + \vartheta q_i \in Z_4[\vartheta]$ ve $i = 0,1,...., \beta - 1$ için $p_i, q_i, c_i \in Z_4$ dir.

Teorem 5.1.1.9. C, $\dfrac{Z_4[x]}{\langle x^\alpha - \theta(\varphi)\rangle} \times \dfrac{R_1[x]}{\langle x^\beta - \varphi\rangle}$ de sabit devirli kod olsun.Bu durumda $\varphi = 1 + 3\vartheta$ için $\alpha = \beta$ ise $\ddot{\zeta}_4(C)$, 2 indeksli parçalı devirli koddur.Eğer $\alpha \neq \beta$ ise $\ddot{\zeta}_4(C)$, 2 indeksli genelleştirilmiş parçalı devirli koddur.

İspat. C, $\dfrac{Z_4[x]}{\langle x^{\alpha}-\theta(\varphi)\rangle}\times\dfrac{R_1[x]}{\langle x^{\beta}-\varphi\rangle}$ de sabit devirli kod olsun.

$$c=\left(c_0,c_1,....,c_{\alpha-1},r_0,r_1,....,r_{\beta-1}\right)=\left(c_0,c_1,.....,c_{\alpha-1},\,p_0+\vartheta q_0,\,p_1+\vartheta q_1,...,\,p_{\beta-1}+\vartheta q_{\beta-1}\right)\in C$$

alalım. $\varphi=1+3\vartheta$ için $\theta(\varphi)=1$ dir. ε, parçalı devirli öteleme operatörü ve $T_{\varphi}-\varphi$ sabit devirli öteleme operatörü olsun. C, $\dfrac{Z_4[x]}{\langle x^{\alpha}-1\rangle}\times\dfrac{R_1[x]}{\langle x^{\beta}-(1+3\vartheta)\rangle}$ de sabit devirli kod olduğundan,

$$T_{\varphi}(c)=\left(\theta(1+3\vartheta)c_{\alpha-1},c_0,....,c_{\alpha-2},(1+3\vartheta)r_{\beta-1},r_0,....,r_{\beta-2}\right)$$

$$=\left(c_{\alpha-1},c_0,...,c_{\alpha-2},(1+3\vartheta)(p_{\beta-1}+\vartheta q_{\beta-1}),\,p_0+\vartheta q_0,....,\,p_{\beta-2}+\vartheta q_{\beta-2}\right)$$

$$=\left(c_{\alpha-1},c_0,....,c_{\alpha-2},\,p_{\beta-1}+2q_{\beta-1}+\vartheta(3p_{\beta-1}+q_{\beta-1}),\,p_0+\vartheta q_0,....,\,p_{\beta-2}+\vartheta q_{\beta-2}\right)$$

olup $\ddot{\zeta}_4$ uygulanarak,

$$\ddot{\zeta}_4\left(T_{\varphi}(c)\right)=(c_{\alpha-1},c_0,...,c_{\alpha-2},2q_{\beta-1},2p_0+2q_0,.....,2p_{\beta-2}+2q_{\beta-2},2q_0,.....,2q_{\beta-2})$$

elde edilir.

Diğer taraftan,

$$\ddot{\zeta}_4(c)=(c_0,.....,c_{\alpha-1},2p_0+2q_0,....,2p_{\beta-1}+2q_{\beta-1},2q_0,2q_1,...,2q_{\beta-1})$$ dir.

Buradan,

$$\varepsilon\left(\ddot{\zeta}_4(c)\right)=(c_{\alpha-1},c_0,...,c_{\alpha-2},2q_{\beta-1},2p_0+2q_0,.....,2p_{\beta-2}+2q_{\beta-2},2q_0,.....,2q_{\beta-2})$$ bulunur.

Böylece $\vec{\vec{\zeta}}_4\left(T_\varphi(c)\right)=\varepsilon\vec{\vec{\zeta}}_4\left(c\right)$ dir. Eğer $\alpha=\beta$ ise $\vec{\vec{\zeta}}_4(C)$, 2 indeksli parçalı devirli koddur.

Eğer $\alpha\neq\beta$ ise $\vec{\vec{\zeta}}_4(C)$, 2 indeksli genelleştirilmiş parçalı devirli koddur.

BÖLÜM 6. SONUÇ VE ÖNERİLER

$v^2=1$ ve $R=Z_4+vZ_4$ olmak üzere Z_4R- lineer kodlar çalışıldı.

$v^2=1$ olmak üzere $R=Z_4+vZ_4$ için Z_4R- devirli kodlar çalışıldı. $Z_4Z_4[v]$ halkası üzerindeki devirli kodların üreteçleri araştırılıp geren kümeleri oluşturuldu.

$v^2=1$ olmak üzere, β tek olması durumunda $Z_4(Z_4+vZ_4)-(v)$ sabit devirli kodlar çalışıldı. 4 farklı gray dönüşüm tanımlandı. $(v)-$ sabit devirli kodların ikisinin gray görüntüsünün genelleştirilmiş parçalı devirli koda eşit olduğu, diğer ikisinin gray görüntüsünün parçalı devirli koda eşit olduğu ispatlandı.Ayrıca R üzerindeki sabit devirli kodlarda çalışıldı.

$\vartheta^2=2$ ve $R_1=Z_4+\vartheta Z_4$ olmak üzere $Z_4R_1-(\vartheta)$ sabit devirli kodlar çalışıldı. β tek olmak üzere 4 farklı gray dönüşüm tanımlandı. R_1 üzerindeki sabit devirli kodlar araştırıldı. $\vartheta^2=2$ için $Z_4(Z_4+\vartheta Z_4)$ halkasında skew sabit devirli kodlar araştırılabilir ve çalışılabilir.

KAYNAKLAR

[1] Fraleigh, J. B. 2003. A first course in abstract algebra. Pearson Education India.

[2] Çallıalp, F. 2001. Örneklerle Soyut Cebir, Birsen Yayınevi.

[3] Çallıalp, F., & Tekir, Ü. 2009. Değişmeli Halkalar ve Modüller. Birsen Yayınevi.

[4] Dinh, H. Q., & López-Permouth, S. R. 2004. Cyclic and negacyclic codes over finite chain rings. IEEE Transactions on Information Theory, *50*(8)**:** 1728-1744.

[5] Dougherty, S. T., & Liu, H. 2009. Independence of vectors in codes over rings. Designs, Codes and Cryptography, 51(1): 55-68.

[6] Shannon, C. E. 1948. A mathematical theory of communication. The Bell System Technical Journal, 27(3)**:** 379-423.

[7] Hamming, R. W. 1950. Error detecting and error correcting codes. The Bell System Technical journal, 29(2): 147-160.

[8] Arikan, E. 2009. Channel polarization, A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels. IEEE Transactions on İnformation Theory, 55(7): 3051-3073.

[9] Roman, S. 1992. Coding and information theory, Vol. 134. Springer Science & Business Media.

[10] Ling, S., & Xing, C. 2004. Coding theory, A first course. Cambridge University Press.

[11] Roman, S. 1992. Coding and information theory, Vol. 134. Springer Science & Business Media.

[12] Dertli, A., Cengellenmis, Y., & Eren, S. 2014. On Quantum Codes Obtained From Cyclic Codes Over F_2+ vF_2+ v^ 2F_2. arXiv preprint arXiv:1407.1232.

[13] Dougherty, S. T. And Shiromoto, K. 2001. Maximum distance codes over rings of order 4, IEEE Transactions on Information Theory, 47(1): 400-404

[14] Prange, E. 1957. Cyclic error-correcting codes in two symbols. Air Force Cambridge Research Center, Cambridge. 57-103.

[15] Özen, M., Uzekmek, F. Z., Aydin, N., & Özzaim, N. T. 2016. Cyclic and some constacyclic codes over the ring Z4. Finite Fields and their Applications, 38: 27-39.

[16] Martinez-Moro, E., Otal, K., & Özbudak, F. 2018. Additive cyclic codes over finite commutative chain rings. Discrete Mathematics, *341*(7):1873-1884.

[17] Mahmoudi, S., & Samei, K. 2019. Additive codes over Galois rings. Finite Fields and Their Applications, 56: 332-350.

[18] Aydogdu, I., Abualrub, T., & Siap, I. 2016. $\mathbb {Z} _ {2}\mathbb {Z} _ {2}[u] $–cyclic and constacyclic codes. IEEE Transactions on Information Theory, 63(8): 4883-4893.

[19] Islam, H., Prakash, O., & Solé, P. 2020. Z 4 Z 4 [u]-Addıtıve cyclıc and constacyclıc codes. Advances in Mathematics of Communications.

[20] Güneri, C., Özdemir, F., & Solé, P. 2018. On the additive cyclic structure of quasi-cyclic codes. Discrete Mathematics, 341(10): 2735-2741.

[21] [21] Aydoğdu, İ. 2014. Bazı özel modüller üzerinde toplamsal kodlar.

[22] Shi, M., Wu, R., & Krotov, D. S. 2018. On $ Z_p Z_ {p^ k} $-Additive codes and their duality. IEEE Transactions on Information Theory, 65(6): 3841-3847.

[23] Abualrub, T., Aydin, N., & Aydoğdu, İ. 2020. Optimal binary codes derived from F2F4-additive cyclic codes. Journal of Applıed Mathematıcs and Computıng , 64:71-87.

[24] Diao, L., Gao, J., & Lu, J. 2020. Some results on\begin {document} $\mathbb {Z} _p\mathbb {Z} _p [v] $\end {document}-additive cyclic codes. Advances in Mathematics of Communications, 14(4): 555.

[25] Borges, J., Dougherty, S. T., Fernández-Córdoba, C., & Ten-Valls, R. 2018. ${\mathbb {Z} _ {2}\mathbb {Z} _ {4}} $-Additive cyclic codes, Kernel and rank. IEEE Transactions on Information Theory, 65(4): 2119-2127.

[26] Li, P., Dai, W., & Kai, X. 2016. On Z 2 Z 2[u]−(1+ u)-additive constacyclic. arXiv preprint arXiv:1611.03169.

[27] Islam, H., & Prakash, O. 2019. On ZpZp [u, v]-additive cyclic and constacyclic codes. arXiv preprint arXiv:1905.06686.

ÖZGEÇMİŞ

Adı Soyadı : Asuman DUMLU

ÖĞRENİM DURUMU

Derece	Eğitim Birimi	Mezuniyet Yılı
Yüksek Lisans	Sakarya Üniversitesi / Fen Bilimleri Enstitüsü / Matematik Bölümü	2021
Lisans	Ondokuz Mayıs Üniversitesi /Fen Edebiyat Fakültesi / Matematik Bölümü	2016
Lise	Şehit Öğretmen Necmeddin Kuyucu Anadolu Lisesi	2012

YABANCI DİL

İngilizce