T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BAZI SONLU HALKALAR ÜZERİNDEKİ LİNEER KODLAR, SABİT DEVİRLİ KODLAR VE SKEW SABİT DEVİRLİ KODLAR

YÜKSEK LİSANS TEZİ

Ceyda CEBE

Enstitü Anabilim Dalı : **MATEMATİK**

Enstitü Bilim Dalı : **CEBİR VE SAYILAR TEORİSİ**

Tez Danışmanı : **Prof. Dr. Mehmet ÖZEN**

Temmuz 2020

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.

Ceyda CEBE

13.07.2020

TEŞEKKÜR

Yüksek lisans eğitimimde yaptığım çalışmalarda bilgi ve deneyimlerini benimle paylaşan, araştırma çalışmalarımın tüm adımlarında desteğini esirgemeyen değerli danışman hocam Prof. Dr. Mehmet ÖZEN'e teşekkürlerimi sunarım. Bilgisine başvurduğumda benden yardımını esirgemeyen bölümümüz doktora öğrencisi Fatma Zehra Uzekmek'e teşekkür ederim. Bugüne kadar bana her zaman destek olan, beni teşvik eden ve ilgisini benden esirgemeyen değerli aileme ve arkadaşlarıma teşekkürlerimi sunarım.

İÇİNDEKİLER

SİMGELER VE KISALTMALAR LİSTESİ

C : Kod

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

R : $v^2 = 1$, $\mathbb{Z}_2[v] = \mathbb{Z}_2 + v\mathbb{Z}_2$ halkası

R_1 : $v^2 = 1$, $\mathbb{Z}_4[v] = \mathbb{Z}_4 + v\mathbb{Z}_4$ halkası

C_μ : C, $\mathbb{Z}_4 R_1 -$ lineer kodunun ilk μ koordinatı

C_η : C, $\mathbb{Z}_4 R_1 -$ lineer kodunun son η koordinatı

$R_1[x;\theta]$: R_1 üzerindeki polinomların kümesi

∂ : Devirli öteleme operatörü

$\overline{\partial}$: Parçalı devirli (quasicyclic) öteleme operatörü

$\Im$: $(v)-$ sabit devirli öteleme operatörü

ξ : Skew $(\varpi)-$ sabit devirli öteleme operatörü

$\wp$: Skew quasi twisted öteleme operatörü

ÖZET

Anahtar kelimeler: Lineer kodlar, devirli kodlar, sabit devirli kodlar, skew sabit devirli kodlar, skew polinom halkası

Bu tezde $v^2=1$ olmak üzere $\mathbb{Z}_2\mathbb{Z}_2[v]-$ lineer kodlar çalışılmıştır. $\mathbb{Z}_2\mathbb{Z}_2[v]-$ lineer kodların üreteç ve kontrol matrisinin standart formu elde edilmiştir. Sonra $\mathbb{Z}_2\mathbb{Z}_2[v]-(v)-$ sabit devirli kodların üreteç polinomları ve en küçük geren kümesi belirlenmiştir. Devirli kodlar ve sabit devirli kodlar arasındaki birebir ilişki verilmiştir. Böylece, devirli kodların dolayısıyla sabit devirli kodların dualinin yapısı incelenmiştir. $\mathbb{Z}_2\mathbb{Z}_2[v]$ de $(v)-$ sabit devirli kodun $\mathbb{Z}_2-$ görüntüsünün 2- indeksli parçalı devirli (quasicyclic) kod olduğu ispatlanmıştır. Son olarak $v^2=1$ ve $R_1=\mathbb{Z}_4+v\mathbb{Z}_4$ olmak üzere R_1 ve $\mathbb{Z}_4R_1$ de skew sabit devirli kodlar çalışılmıştır. Bu halkalar üzerindeki kodların üreteç polinomları verilmiştir. R_1 de farklı otomorfizmalar ve farklı gray dönüşümler verilmiştir. Ayrıca $\mathbb{Z}_4R_1$ üzerindeki double skew sabit devirli kodlar verilmiştir.

LINEAR CODES, CONSTACYCLIC CODES AND SKEW CONSTACYCLIC CODES OVER SOME FINITE RINGS

SUMMARY

Keywords: Linear codes, cyclic codes, constacyclic codes, skew constacyclic codes, skew polynomial ring

In this thesis, $\mathbb{Z}_2\mathbb{Z}_2[v]-$ linear codes are studied, where $v^2=1$. The standart form of the generator matrix and parity- check matrix of $\mathbb{Z}_2\mathbb{Z}_2[v]-$ linear codes are obtained. After, generator polynomials of $\mathbb{Z}_2\mathbb{Z}_2[v]-(v)-$ constacyclic codes and their minimal spanning set are determined. The one-to-one relationship between cyclic codes and constacylic codes is given. Hence, the structure of dual codes of cyclic codes and therefore constacyclic codes are investigated. The $\mathbb{Z}_2-$ image of $(v)-$ constacyclic code over $\mathbb{Z}_2\mathbb{Z}_2[v]-$ is quasi cyclic code with 2- index is proved. Finally, skew constacyclic codes over R_1 and $\mathbb{Z}_4R_1$ are studided, where $v^2=1$ and $R_1=\mathbb{Z}_4+v\mathbb{Z}_4$. The generator polynomials of the codes over this ring are given. Different automorphisms and different gray maps over R_1 are given. Also, double skew constacyclic codes over $\mathbb{Z}_4R_1$ are given.

BÖLÜM 1. GİRİŞ

1.1. Cebirsel Tanımlar, Önermeler ve Teoremler

Tezin bu kısmında ileriki bölümlerde gerekli olan temel bilgiler verilecektir.

Tanım 1.1.1. G boştan farklı bir küme olsun. $g_1, g_2 \in G$ için $G \times G$ den alınan her sıralı ikiliyi G kümesinde bir ve yalnız bir elemana götüren fonksiyona G'de bir ikili işlem denir. Yani, $*$, G de ki ikili işlemi göstermek üzere,

$G \times G \to G$

$(g_1, g_2) \to g_1 * g_2$

şeklinde tanımlanır [1].

Tanım 1.1.2. Üzerinde en az bir ikili işlem tanımlı boştan farklı bir kümeye cebirsel yapı denir. G kümesi üzerinde tanımlı bir $*$ ikili işlemi varsa bu cebirsel yapı $(G,*)$ ile gösterilir [2].

Tanım 1.1.3. G boş olmayan bir küme ve $*$, G kümesinde tanımlı bir ikili işlem olsun. $(G,*)$ cebirsel yapısına aşağıda verilen aksiyomları sağlıyorsa grup denir.

$G1$. $*$, G de bir ikili işlemdir.

$G2$. $*$ işleminin G de birleşme özelliği vardır. Yani, $\forall g_1, g_2, g_3 \in G$ için, $g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3$ tür.

$G3$. $*$ işleminin G de birim elemanı vardır. Yani, $\forall g_1 \in G$ için,

$g_1 * e = e * g_1 = g_1$ olacak şekilde $\exists e \in G$ vardır.

$G4.$ $*$ işlemine göre, G deki her elemanın bir tersi vardır. Yani, $\forall g_1 \in G$ için, $g_1 * g_1^{-1} = g_1^{-1} * g_1 = e$ olacak şekilde $\exists g_1^{-1} \in G$ bulunabilir $[2]$.

Tanım 1.1.4. $(G,*)$ bir grup ve $\forall g_1, g_2 \in G$ için $g_1 * g_2 = g_2 * g_1$ değişme özelliği de sağlanıyor ise $(G,*)$ grubuna değişmeli grup veya abel grubu denir $[2]$.

Tanım 1.1.5. G bir grup ve H, G nin boş olmayan bir alt kümesi olsun. H kümesi, G de ki işleme göre kendi başına bir grup oluyorsa H kümesine G nin bir alt grubu denir $[2]$.

Tanım 1.1.6. F kümesi G grubunun bir alt kümesi olsun. F yi kapsayan, G nin bütün alt gruplarının arakesitine F nin ürettiği alt grup denir. $\langle F \rangle$ ile gösterilir. F sonlu bir küme ise G ye sonlu üretilmiş grup ve $F = \{a\}$ tek elemanlı bir küme ise G ye a tarafından üretilmiş devirli grup denir. $G = \langle a \rangle$ ile gösterilir $[2]$.

Tanım 1.1.7. R boş olmayan bir küme olsun. $+$ ve $.$ ikili işlemleri ile aşağıda verilen aksiyomları sağlayan $(R,+,.)$ cebirsel yapısına halka denir.

1. $(R,+)$ değişmeli bir gruptur.
2. $.$ işleminin R de birleşme özelliği vardır. Yani, $\forall r_1, r_2, r_3 \in R$ için, $(r_1.r_2).r_3 = r_1.(r_2.r_3)$ tür.
3. $.$ işleminin $+$ işlemi üzerine sağdan ve soldan dağılma özellikleri vardır. Yani, $\forall r_1, r_2, r_3 \in R$ için $r_1.(r_2 + r_3) = r_1.r_2 + r_1.r_3$ ve $(r_1 + r_2).r_3 = r_1.r_3 + r_2.r_3$ tür.

Ayrıca,

4. R halkasının $.$ işlemine göre değişme özelliği sağlanıyorsa yani, $\forall r_1, r_2 \in R$ için $r_1.r_2 = r_2.r_1$ oluyorsa R halkasına değişmeli halka denir.

5. R halkasının . işlemine göre etkisiz elemanı varsa yani, $\forall r_1 \in R$ için $1_R.r_1 = r_1.1_R = r_1$ olacak şekilde $1_R \in R$ varsa R halkasına birimli halka denir. 1_R de halkanın birim elemanı olarak adlandırılır [3].

Tanım 1.1.8. R halkası birimli bir halka olsun. $r_1 \in R$ için $r_1.r_2 = r_2.r_1 = 1_R$ şartını sağlayan bir $r_2 \in R$ varsa r_1 e birimsel eleman denir.

Tanım 1.1.9. R halkasında sıfırdan farklı alınan bir $r_1 \in R$ için, $r_1.r_2 = 0_R$ veya $r_2.r_1 = 0_R$ şartını sağlayan sıfırdan farklı $\exists r_2 \in R$ varsa r_1 e sıfır bölen denir [2].

Tanım 1.1.10. Birimli, değişmeli, sıfır bölensiz (tam) halkaya tamlık bölgesi denir [2].

Tanım 1.1.11. R bir halka ve S, R nin boş olmayan bir alt kümesi olsun. S, R halkasındaki işlemlere göre kendi başına bir halka ise S ye R halkasının bir alt halkası denir [2].

Tanım 1.1.12. R bir halka ve $P \subset R$ olsun. R halkasının P yi kapsayan bütün alt halkalarının arakesitine P nin ürettiği alt halka ($\langle P \rangle$) denir. P nin elemanları $\langle P \rangle$ nin üreteçleri olarak adlandırılır [2].

Tanım 1.1.13. R bir halka ve $\varnothing \neq I \subset R$ olsun.

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

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

ise I ya R nin bir sol (veya sağ) ideali denir. Hem sol hem de sağ ideale iki taraflı ideal veya kısaca ideal denir [2].

Tanım 1.1.14. R bir halka ve $P \subset R$ olsun. R nin, P yi kapsayan bütün ideallerinin arakesitine P nin ürettiği ideal ((P)) denir. Eğer $P = \{p\}$ tek elemanlı bir küme ise P nin ürettiği ideale temel ideal denir. (p) ile gösterilir [2].

Tanım 1.1.15. Her ideali bir temel ideal olan halkaya, bir temel ideal halkası denir. Her ideali bir temel ideal olan tamlık bölgesine temel ideal bölgesi denir [4].

Tanım 1.1.16. R değişmeli ve birimli halkasında $M \neq R$ şartını sağlayan bir M ideali olsun. R nin, M yi kapsayan M ve R den başka hiçbir ideali yoksa, M ye R nin bir maksimal ideali denir [2].

Tanım 1.1.17. Tek maksimal ideale sahip olan birimli değişmeli bir halkaya lokal halka denir [3].

Tanım 1.1.18. I , R halkasının bir ideali olsun. $\forall r_1, r_2 \in R$ için,

$r_1 \equiv r_2 (\mathrm{mod}\, I) \Leftrightarrow r_1 - r_2 \in I$

denklik bağıntısına göre oluşan bütün denklik sınıflarının kümesi R/I ile gösterilirse, R/I ,

$(r+I)+(s+I)=(r+s)+I$,

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

işlemleri ile bir halka oluşturur. Bu halkaya, I ya göre bölüm halkası denir [4].

Tanım 1.1.19. R ve S iki halka, $f : R \to S$ bir fonksiyon olsun. $\forall r_1, r_2 \in R$ için;

i. $f(r_1 + r_2) = f(r_1) + f(r_2)$ ve

ii. $f(r_1 r_2) = f(r_1)\, f(r_2)$

ise f ye, R den S ye bir halka homomorfizması denir [2].

Tanım 1.1.20. $f:R\to S$ halka homomorfizması birebir ve örten ise f ye halka izomorfizması denir. R ve S halkalarına izomorf halkalar ($R\cong S$) denir. $f:R\to R$ izomorfizma ise f ye otomorfizma denir [1].

Tanım 1.1.21. $f:R\to S$ halka homomorfizması olsun.

i. f nin çekirdeği, $Çek\ f=\{r\in R\mid f(r)=0_S\}$ dir.

ii. f nin görüntüsü, $\mathrm{Im}\ f=\{s\in S\mid r\in R\ için\ s=f(r)\}$ dir [3].

Tanım 1.1.22. R bir halka, x bir bilinmeyen ve $a_0,a_1,\ldots,a_n$ ler R halkasının elemanları olmak üzere, $a_0+a_1x+\ldots+a_nx^n$ şeklindeki ifadeye R den katsayılı bir polinom denir. R den katsayılı tüm polinomlar kümesi $R[x]$ ile gösterilir. $p(x)=a_0+a_1x+\ldots+a_nx^n\in R[x]$ ve $a_n\neq 0$ ise a_n ye polinomun baş katsayısı ve n ye de polinomun derecesi denir. $p(x)$ polinomunun derecesi $d^0p(x)$ ile gösterilir [2].

Önerme 1.1.1. R bir halka ise $R[x]$ de bir halkadır [2].

Önerme 1.1.2. R bir halka olmak üzere,

i. R halkası birimli ise $R[x]$ de birimlidir.

ii. R halkası değişmeli ise $R[x]$ de değişmelidir.

iii. R halkası tamlık bölgesi ise $R[x]$ de tamlık bölgesidir [2].

Teorem 1.1.1. R değişmeli bir halka ve $f(x),g(x)\in R[x]$ olsun. $g(x)\neq 0$ ve $g(x)$ polinomunun baş katsayısı terslenebilsin. O zaman;

$f(x)=q(x)g(x)+r(x)$ ve $d^0r(x)<d^0g(x)$

olacak şekilde tek türlü olarak belirli $\exists q(x),r(x)\in R[x]$ polinomları bulunabilir [2].

Tanım 1.1.23. Baş katsayısı 1 olan polinoma monik polinom denir $[2]$.

Tanım 1.1.24. $(M,+)$ bir değişmeli grup, R de değişmeli bir halka olmak üzere, M grubundaki elemanların, R değişmeli halkasındaki elemanlarla skaler çarpımı, $R\times M\to M$ fonksiyonu,

i. $\forall r\in R,\ \forall m,\bar{m}\in M$ için, $r(m+\bar{m})=rm+r\bar{m}$,

ii. $\forall r,\bar{r}\in R,\ \forall m\in M$ için, $(r+\bar{r})m=rm+\bar{r}m$,

iii. $\forall r,\bar{r}\in R,\ \forall m\in M$ için, $(r\bar{r})m=r(\bar{r}m)$,

iv. $\forall m\in M$ için, $1_R m=m$.

şeklinde verilen koşulları sağlıyorsa, M ye R üzerinde bir modül veya kısaca $R-$ modül denir $[4]$.

Tanım 1.1.25. R bir halka, M bir $R-$ modül ve N, M nin boş olmayan bir alt kümesi olsun. Eğer N de kendi başına bir $R-$ modül oluyorsa N ye, M nin bir alt modülü veya kısaca $R-$ alt modülü denir. M modülünün kendisi ve sıfırından ibaret $\{0_M\}=0$ alt kümesi M nin bir alt modülüdür $[4]$.

Önerme 1.1.3. $R-$ modül M nin, boştan farklı bir $N\subseteq M$ alt kümesinin alt modül olması için gerek ve yeter koşul $\forall r,\bar{r}\in R$ ve $\forall m,\bar{m}\in N$ için, $rm+\bar{r}\bar{m}\in N$ olmasıdır $[4]$.

Tanım 1.1.26. R değişmeli halka, M bir $R-$ modül ve $\{x_1,x_2,...,x_n\}\in M$ olsun. Eğer her $x\in M$ elemanı $a_1,a_2,...,a_n\in R$ olmak üzere, $x=a_1x_1+a_2x_2+...+a_nx_n$ şeklinde tek türlü olarak ifade edilebiliyorsa M ye n ranklı serbest $R-$ modül denir ve $\{x_1,x_2,...,x_n\}$ e M nin serbest tabanı denir $[5]$.

Tanım 1.1.27. R bir halka, M ve N nin her ikisi de $R-$ modül olsun. Bir $f:M\to N$ fonksiyonu, aşağıda verilen koşulları sağlıyorsa, f ye bir modül homomorfizması veya $R-$ homomorfizma denir. $\forall m,\bar{m}\in M$ ve $\forall r\in R$ için,

i. $f(m+\bar{m}) = f(m) + f(\bar{m})$

ii. $f(rm) = r f(m)$ dir $[4]$.

Tanım 1.1.28. $\mathbb{F}_{q^m} = GF(q^m)$ bir cisim ve bu cisim üzerinde tanımlanan otomorfizma $\theta : \alpha \to \alpha^q$ olmak üzere,

$\mathbb{F}_{q^m}[x,\theta] = \left\{ f(x) = a_0 + a_1 x + ... + a_{n-1} x^{n-1} : a_i \in F_{q^m} \ \ ve \ \ i = 0,1,...,n-1 \right\}$ kümesinin polinom halkasındaki standart toplama işlemi ve $(ax^i) * (bx^j) = a\theta^i(b) x^{i+j}$ ile tanımlı çarpma işlemine göre belirttiği halkaya skew polinom halkası denir $[6]$.

Tanım 1.1.29. Eğer $R-$ modül olan R halkası birebir ise sonlu değişmeli olan R halkasına Frobenius halkası denir $[7]$.

1.2. Lineer Kodlar

Bu bölümde öncelikle lineer cebirden ve kodlama teorisinden gerekli olan bazı tanımlar ve teoremler verilecektir.

Tanım 1.2.1. F_q sonlu cisim olsun. Vektörel toplam $+$ ile ve F_q nun elemanları ile skaler çarpım işlemlerinin tanımlı olduğu boş olmayan bir V kümesine, eğer aşağıdaki şartların tümü sağlanıyorsa F_q üzerinde vektör uzayı denir. Her $u, v, w \in V$ ve her $q_1, q_2 \in F_q$ için:

i. V kümesi toplama işlemine göre değişmeli bir gruptur.

ii. $q_1 v \in V$ dir.

iii. $q_1(u+v) = q_1 u + q_1 v,\ (q_1 + q_2)u = q_1 u + q_2 u$ dur.

iv. $(q_1 q_2)u = q_1(q_2 u)$ dur.

v. Eğer F_q nun birim elemanı 1 ise o zaman $1u = u$ dur $[8]$.

Tanım 1.2.2. V vektör uzayının boş olmayan bir C alt kümesi V de tanımlı olan vektörel toplam ve skaler çarpım ile kendi başına vektör uzayı ise C ye V nin alt uzayı denir [8].

Teorem 1.2.1. F_q üzerinde V vektör uzayının boş olmayan bir C alt kümesinin alt uzay olması için gerek ve yeter şart aşağıdaki koşulun sağlanmasıdır:
$x, y \in C$ ve $q_1, q_2 \in F_q$ ise $q_1 x + q_2 y \in C$ dir [8].

Tanım 1.2.3. V, F_q üzerinde vektör uzayı ve $S = \{v_1, v_2, ..., v_r\}$, V nin boştan farklı bir alt kümesi olsun. $\langle S \rangle = \{q_1 v_1 + ... + q_r v_r : q_i \in F_q\}$ kümesine S nin ürettiği (gerdiği) alt uzay denir. $\langle S \rangle$, V nin alt uzayıdır. V nin C alt uzayı ve C nin S alt kümesi için eğer $C = \langle S \rangle$ ise S ye C nin üreteç kümesi (geren kümesi) denir [8].

Tanım 1.2.4. V, F_q üzerinde vektör uzayı olsun. Eğer $q_1 v_1 + ... + q_r v_r = 0$ olacak şekilde hepsi aynı anda sıfır olmayan $q_1, ..., q_r \in F_q$ varsa V de ki $\{v_1, ..., v_r\}$ vektörlerinin kümesi lineer bağımlıdır denir. Eğer $q_1 v_1 + ... + q_r v_r = 0 \Rightarrow q_1 = ... = q_r = 0$ oluyor ise V de ki $\{v_1, ..., v_r\}$ vektörlerinin kümesi lineer bağımsızdır denir [8].

Tanım 1.2.5. $S = \{v_1, v_2, ..., v_r\}$, V de ki vektörler kümesi olsun. Eğer S lineer bağımsız küme ve S , V yi geren küme ise S ye V nin bazı (tabanı) denir [9].

Tanım 1.2.6. V vektör uzayının herhangi bir bazındaki eleman sayısına V nin boyutu denir [9].

Tanım 1.2.7. $P = \{p_1, ..., p_q\}$ sonlu kümesine kod alfabesi denir. P^n , P üzerinde $n-$ lilerin kümesi olsun. P^n nin boş olmayan herhangi bir C alt kümesine $q-$ lu blok

kod denir. C de ki her bir elemana kod söz denir. Eğer $C \subset P^n$, M tane eleman içeriyor ise C ye n uzunluğunda M elemanlı kod ya da $(n, M)-$ kod denir [10].

Tanım 1.2.8. 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 [8].

Teorem 1.2.2. A alfabesi üzerindeki $n-$ lilerin kümesinden alınan x, y, z için Hamming uzaklık fonksiyonu aşağıda verilen özelliklere sahiptir.

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

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

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

iv. $d(x, z) \le d(x, y) + d(y, z)$ [8].

Tanım 1.2.9. 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 [8].

Tanım 1.2.10. n uzunluklu, M elemanlı ve minimum uzaklığı d olan bir kod $(n, M, d)-$ kod olarak gösterilir. n, M, d sayılarına kodun parametreleri denir [8].

Tanım 1.2.11. $x = (x_1, ..., x_n)$ kod sözünün ağırlığı x in sıfırdan farklı bileşen sayısıdır 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 [10].

Tanım 1.2.12. Bileşenleri F_q dan alınan ve $n-$ lilerden oluşan vektör uzayı $V(n, q)$ olmak üzere, $C \subset V(n, q)$ kodu eğer $V(n, q)$ vektör uzayının bir alt uzayı ise C ye bir lineer kod denir. Eğer C , $V(n, q)$ üzerinde k boyuta sahip ise C ye $[n, k]-$ kod denir. Eğer C kodunun minimum uzaklığı d ise C ye $[n, k, d]-$ kod denir [10].

Teorem 1.2.3. Eğer C bir lineer kod ise $d(C)=w(C)$ dir $[10]$.

Tanım 1.2.13. C bir $[n,k]-$ kod olsun. Satırları C kodu için baz oluşturan $k\times n$ boyutlu bir G matrisine C nin üreteç matrisi denir. $C=\{xG \mid x\in V(k,q)\}$ dir $[10]$. I_k, k boyutlu birim matris olmak üzere $G=(I_k \mid A)$ biçimindeki üreteç matrise standart formdadır denir $[10]$.

Tanım 1.2.14. $v=(v_1,...,v_n), w=(w_1,...,w_n)\in F_q^n$ olsun.

i. v ve w nın skaler çarpımı (nokta çarpımı ya da Öklid iç çarpımı olarak da bilinir) $v.w=v_1w_1+...+v_nw_n\in F_q$ olarak tanımlanır.

ii. Eğer $v.w=0$ ise v vektörü w vektörüne diktir (ortogonaldir) denir $[8]$.

Tanım 1.2.15. C bir lineer $[n,k]-$ kod olsun. C nin dual kodu $C^{\perp}=\{v\in V(n,q) \mid v.c=0, \forall c\in C\}$ kümesidir $[10]$.

Teorem 1.2.4.

i. Eğer G , C için üreteç matris ise $C^{\perp}=\{v\in V(n,q) \mid v.G^T=0\}$ dır.

ii. Lineer $[n,k]-$ kodunun duali $C^{\perp}$ lineer $[n,n-k]-$ koddur.

iii. Herhangi C lineer kodu için $(C^{\perp})^{\perp}=C$ dir $[10]$.

Tanım 1.2.16. C lineer kodunun kontrol matrisi H , $C^{\perp}$ dual kodunun üreteç matrisidir $[8]$.

Teorem 1.2.5. Eğer $G=(I_k \mid A)$, C $[n,k]-$ kodunun standart formdaki üreteç matrisi ise o zaman C nin kontrol matrisi $H=(-A^T \mid I_{n-k})$ dır$[8]$.

1.3.Devirli Kodlar

Tanım 1.3.1. $C \subseteq F_q^n$ için $(c_0, c_1, ..., c_{n-1}) \in C$ iken $(c_{n-1}, c_0, ..., c_{n-2}) \in C$ oluyorsa C lineer koduna devirli kod denir [8].

$$\begin{aligned} \ell : \quad & F_q^n \quad \rightarrow \quad F_q[x]/(x^n - 1) \\ & (c_0, c_1, ..., c_{n-1}) \quad \rightarrow (c_0 + c_1 x + ... + c_{n-1} x^{n-1}) \end{aligned}$$

şeklinde verilen dönüşüm ile $C \subseteq F_q^n$ de ki $(c_0, c_1, ..., c_{n-1})$ kod sözü $F_q[x]/(x^n - 1)$ de ki polinomla ilişkilendirilebilir [8].

Teorem 1.3.1. ℓ yukarıda tanımlanan lineer dönüşüm olsun. F_q^n nin boştan farklı C alt kümesinin devirli kod olması için gerek ve yeter koşul $\ell(C)$ nin $\frac{F_q[x]}{\langle x^n - 1 \rangle}$ in ideali olmasıdır [8].

Teorem 1.3.2. 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 [8].

Teorem 1.3.3. $F_q[x]/(x^n - 1)$ in sıfırdan farklı I idealinde derecesi en küçük olan tek bir monik polinom vardır. (Bu monik polinom Teorem 1.3.2.den I nın üretecidir) [8].

Tanım 1.3.2. $F_q[x]/(x^n - 1)$ in sıfırdan farklı I idealinde derecesi en küçük olan tek bir monik polinoma I nın üreteç polinomu denir. C devirli kodu için $\ell(C)$ nin üreteç polinomuna C nin üreteç polinomu denir [8].

Teorem 1.3.4. $F_q[x]/(x^n-1)$ in idealinin üreteç polinomu $g(x)$ olsun. Eğer $g(x)$ in derecesi $n-k$ ise devirli kodun boyutu k dir [8].

Teorem 1.3.5. $der(g(x))=n-k$ olmak üzere F_q^n de ki C devirli kodunun üreteç polinomu $g(x)=g_0+g_1x+...+g_{n-k}x^{n-k}$ olsun. O zaman C nin üreteç matrisi

$$G=\begin{pmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{k-1}g(x) \end{pmatrix}=\begin{pmatrix} g_0 & g_1 & \dots & g_{n-k} & 0 & 0 & 0 & ... & 0 \\ 0 & g_0 & g_1 & ... & g_{n-k} & 0 & 0 & ... & 0 \\ \vdots & & & & & & & & \vdots \\ 0 & 0 & ... & g_0 & g_1 & \dots & & & g_{n-k} \end{pmatrix}$$ şeklindedir [8].

Tanım 1.3.3. $h(x)=\sum_{i=0}^{k}a_ix^i$, F_q üzerinde k dereceli $(a_k\neq 0)$ polinom olsun. $h(x)$ in reciprocal polinomu $h_R(x)$, $h_R(x):=x^kh(1/x)=\sum_{i=0}^{k}a_{k-i}x^i$ olarak tanımlanır [8].

Teorem 1.3.6. C, $q-$ lu $[n,k]-$ devirli kodunun üreteç polinomu $g(x)$ olsun. $h(x)=(x^n-1)/g(x)$ ile ifade edilsin. $h(x)$ in sabit terimi h_0 olmak üzere $h_0^{-1}h_R(x)$ e $C^{\perp}$ in üreteç polinomu denir [8].

Tanım 1.3.4. C, n uzunluğunda $q-$ lu devirli kod olsun. $h(x)=(x^n-1)/g(x)$ ile ifade edilsin. $h(x)$ in sabit terimi h_0 olmak üzere $h_0^{-1}h_R(x)$ e C nin kısmi kontrol polinomu denir [8].

Sonuç 1.3.1. C, $q-$ lu $[n,k]-$ devirli kodunun üreteç polinomu $g(x)$ olsun. $h(x)=(x^n-1)/g(x)$ ile ifade edilsin. $h(x)=h_0+h_1x+...+h_kx^k$ olsun. O halde C nin kısmi kontrol matrisi,

$$H=\begin{pmatrix} h_R(x) \\ xh_R(x) \\ \vdots \\ x^{n-k-1}h_R(x) \end{pmatrix}=\begin{pmatrix} h_k & h_{k-1} & \dots & h_0 & 0 & 0 & 0 & \dots & 0 \\ 0 & h_k & h_{k-1} & \dots & h_0 & 0 & 0 & \dots & 0 \\ \vdots & & & & & & & & \\ 0 & 0 & \dots & h_k & h_{k-1} & & \dots & & h_0 \end{pmatrix}$$ şeklindedir [8].

BÖLÜM 2. $\mathbb{Z}_2\mathbb{Z}_2[v]-$ LİNEER KODLAR

Cisimler üzerinde yapılan çalışmaların yanı sıra halkalar üzerinde de birçok çalışma yapılmıştır. Brouwer ve ark.$[11]$ tarafından farklı iki alfabe üzerindeki kodların çalışması yapılmıştır. Sonrasında Borges ve ark.$[12]$ tarafından $\mathbb{Z}_2\mathbb{Z}_4-$toplamsal kodlar sunulmuştur. Ayrıca bu kodlar için çeşitli çalışmalar yapılmıştır$[13,14,15,16]$. Daha sonra bu kodlar $\mathbb{Z}_2\mathbb{Z}_{2^s}$ $(s\geq 2)$ toplamsal kodlara Aydoğdu ve ark. $[17]$ tarafından genişletilmiştir. Aydoğdu ve ark. $[18]$ tarafından $u^2=0$ olmak üzere $\mathbb{Z}_2\mathbb{Z}_2[u]-$ toplamsal kodlar çalışılmıştır.

Tezin bu bölümünde öncelikle $v^2=1$ olmak üzere $\mathbb{Z}_2+v\mathbb{Z}_2$ halkası hakkında bilgi verilecektir. Daha sonra $\mathbb{Z}_2\mathbb{Z}_2[v]$ kümesi tanımlanarak $\mathbb{Z}_2\mathbb{Z}_2[v]-$ lineer kodların yapısı çalışılacaktır. Bu kodların üreteç matrislerinin ve kontrol matrislerinin standart formu belirlenecektir.

2.1. $v^2=1;\ \mathbb{Z}_2[v]=\mathbb{Z}_2+v\mathbb{Z}_2$ Halkası

$v^2=1$ olmak üzere, $\mathbb{Z}_2[v]=\mathbb{Z}_2+v\mathbb{Z}_2=\{0,1,v,1+v\}$ halkası dört elemanlı bir halkadır. Bu halka kısaca R sembolü ile gösterilsin. R nin terslenebilen elemanları $\{1,v\}$ dir. A_1,A_2,B_1,B_2 matrisleri $\mathbb{Z}_2$ üzerinde matrisler olmak üzere, R halkası üzerindeki C lineer koduna permütasyon denk olan üreteç matris,

$$G=\begin{bmatrix} I_{k_1} & A_1 & B_1+vB_2 \\ 0 & (1+v)I_{k_2} & (1+v)A_2 \end{bmatrix} \tag{2.1}$$

biçimindedir $[19]$.

Tanım 2.1.1. $\begin{matrix}\varphi : R \to \mathbb{Z}_2^{\,2} \\ (a+vb) \to (a,b)\end{matrix}$ olacak şekilde φ gray dönüşümü tanımlansın. Burada, $\varphi(0)=(0,0), \varphi(1)=(1,0), \varphi(v)=(0,1), \varphi(1+v)=(1,1)$ dir $[20]$.

2.2. $\mathbb{Z}_2\mathbb{Z}_2[v]-$ Lineer Kodların Yapısı

$\mathbb{Z}_2\mathbb{Z}_2[v]=\{(s,t)\,|\,s\in\mathbb{Z}_2, t\in R\}$ şeklinde tanımlanan $\mathbb{Z}_2\mathbb{Z}_2[v]$ halkası bilinen toplama işlemi altında kapalıdır. Fakat $v\in R$ için çarpma işlemi altında kapalı olmadığından bilinen çarpma işlemine göre $R-$ modül değildir. Bu nedenle aşağıdaki tanımda verilen τ dönüşümü kullanılarak yeni bir çarpma işlemi tanımlanacaktır. Böylece $\mathbb{Z}_2\mathbb{Z}_2[v]$ halkasının $R-$ modül olması sağlanarak, cebirsel yapısı daha iyi bir konuma gelir $[20]$.

Tanım 2.2.1. $a,b\in\mathbb{Z}_2, a+vb\in R$ olmak üzere,

$\begin{matrix}\tau : R \to \mathbb{Z}_2 \\ (a+vb) \to a+b\end{matrix}$ dönüşümü tanımlansın. Burada,

$\tau(0)=0, \tau(1)=1, \tau(v)=1, \tau(1+v)=0$ dır $[20]$.

Tanımlanan τ dönüşümü halka homomorfizmasıdır.

Yukarıda açıklandığı gibi yeni bir çarpma işlemi aşağıdaki gibi tanımlanır.

Tanım 2.2.2. Herhangi bir $r\in R, c=(s_0,s_1,...,s_{\mu-1},t_0,t_1,...,t_{\eta-1})\in\mathbb{Z}_2^{\,\mu}\times(\mathbb{Z}_2+v\mathbb{Z}_2)^{\eta}$ için,

$$rc=(\tau(r)s_0,\tau(r)s_1,...,\tau(r)s_{\mu-1},rt_0,rt_1,...,rt_{\eta-1}) \tag{2.2}$$

şeklindedir.

Önerme 2.2.1. $\mathbb{Z}_2^{\,\mu}\times(\mathbb{Z}_2+v\mathbb{Z}_2)^{\eta}$ halkası (2.2) ile verilen çarpma işlemi ile bir $R-$ modüldür $[20]$.

Tanım 2.2.3. Bir C lineer kodu (2.2) ile verilen çarpma işlemi altında $\mathbb{Z}_2{}^{\mu}\times\left(\mathbb{Z}_2+v\mathbb{Z}_2\right)^{\eta}$ nın bir $\mathbb{Z}_2+v\mathbb{Z}_2$ alt modülü ise C ye $\mathbb{Z}_2\mathbb{Z}_2[v]-$ lineer kod denir.

Tanım 2.2.4. Tanım 2.1.1 de verilen gray dönüşüm genişletilerek,

$\forall s=\left(s_0,s_1,...,s_{\mu-1}\right)\in\mathbb{Z}_2{}^{\mu}$ ve $\forall t=\left(t_0,t_1,...,t_{\eta-1}\right)\in R^{\eta}$ $\left(t_i=a_i+vb_i;0\le i\le\eta-1\right)$

için, $k=\mu+2\eta$ olmak üzere,

$$\sigma:\mathbb{Z}_2{}^{\mu}\times\left(\mathbb{Z}_2+v\mathbb{Z}_2\right)^{\eta}\to\mathbb{Z}_2{}^{k}$$
$$(s,t)\ \to\left(s_0,...,s_{\mu-1},a_0,...,a_{\eta-1},b_0,...,b_{\eta-1}\right)$$

elde edilir [20].

2.3. $\mathbb{Z}_2\mathbb{Z}_2[v]-$ Lineer Kodların Üreteç Matrislerinin Standart Formu

Bir C kodunun hangi tipte olduğunun belirlenmesinde ve eleman sayısının bulunmasında standart forma sahip üreteç matris önem kazanmaktadır. Bu nedenle bu bölümde $\mathbb{Z}_2\mathbb{Z}_2[v]-$ lineer kodların üreteç matrislerinin standart formu belirlenmiştir.

Teorem 2.3.1. C kodu $\left(\mu,\eta,k_0,k_1,k_2\right)$ tipinde bir $\mathbb{Z}_2\mathbb{Z}_2[v]-$ lineer kod olsun. A_1,A_2,B_1,B_2,D,D_1,E, $\mathbb{Z}_2$ üzerinde verilen matrisler olmak üzere, C kodunun üreteç matrisinin standart hali,

$$G=\begin{bmatrix} I_{k_0} & D & 0 & 0 & (1+v)D_1 \\ 0 & E & I_{k_1} & A_1 & B_1+vB_2 \\ 0 & 0 & 0 & (1+v)I_{k_2} & (1+v)A_2 \end{bmatrix} \tag{2.3}$$

biçimindeki $\mathbb{Z}_2\mathbb{Z}_2[v]-$ lineer koda permütasyon denktir.

İspat: C, $\mathbb{Z}_2\mathbb{Z}_2[v]-$ lineer kodunun η uzunluğundaki kısmı R^{η} üzerinde lineer koddur. Dolayısıyla C için üreteç matris (2.1) de verilen matris kullanılarak aşağıdaki gibi yazılabilir.

$\begin{bmatrix} R_1 & R_2 & I_{k_1} & F & E_1+vE_2 \\ R_3 & R_4 & 0 & (1+v)I_k & (1+v)F' \end{bmatrix}$. Burada R_i $(1 \le i \le 4)$ matrisleri, $\mathbb{Z}_2$ üzerindeki matrislerdir. Bu matrisin $\mathbb{Z}_2$ kısmındaki son satırında, varsa içindeki sıfırlar ayrılarak $\begin{bmatrix} R_1 & R_2 & I_{k_1} & F & E_1+vE_2 \\ R_{31} & R_{41} & 0 & (1+v)I_r & (1+v)M \\ 0 & 0 & 0 & (1+v)I_{k_2} & (1+v)A_2 \end{bmatrix}$ biçimindeki matris elde edilir. Buradan bu matrisin $\mathbb{Z}_2$ üzerindeki kısmında gerekli olan satır işlemleri yapılırsa,

$\begin{bmatrix} R_1 & R_2 & I_{k_1} & H & S_1+vS_2 \\ I_{k_0} & T_1 & 0 & (1+v)T_2 & (1+v)N \\ 0 & 0 & 0 & (1+v)I_{k_2} & (1+v)A_2 \end{bmatrix}$ biçimindeki matris bulunur. Böylece $\mathbb{Z}_2$ üzerinde bulunan I_{k_0} birim matrisi yardımıyla R_1 matrisi sıfırlanarak ve matrisin R üzerindeki kısmında da gerekli olan işlemler yapılarak aşağıdaki matris elde edilir.

$\begin{bmatrix} 0 & R_2 & I_{k_1} & H' & S_1'+vS_2' \\ I_{k_0} & T_1 & 0 & 0 & (1+v)N' \\ 0 & 0 & 0 & (1+v)I_{k_2} & (1+v)A_2 \end{bmatrix}$. Böylece son bir düzenleme ile C, $\mathbb{Z}_2\mathbb{Z}_2[v]-$ lineer kodunun standart formdaki üreteç matrisi:

$\begin{bmatrix} I_{k_0} & D & 0 & 0 & (1+v)D_1 \\ 0 & E & I_{k_1} & A_1 & B_1+vB_2 \\ 0 & 0 & 0 & (1+v)I_{k_2} & (1+v)A_2 \end{bmatrix}$ dir.

Örnek 2.3.1. $\mu=\eta=3$ olmak üzere,

$G=\begin{bmatrix} 0 & 1 & 1 & 1 & 1 & v \\ 0 & 1 & 0 & 1+v & v & 1 \\ 1 & 0 & 1 & v & 1 & v \end{bmatrix}$ ile verilen matris C, $\mathbb{Z}_2\mathbb{Z}_2[v]-$ lineer kodunun üreteç matrisi olsun.

$$\begin{bmatrix} 0 & 1 & 1 & 1 & 1 & v \\ 0 & 1 & 0 & 1+v & v & 1 \\ 1 & 0 & 1 & v & 1 & v \end{bmatrix} \overset{H_{21}(1+v)}{\sim} \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & v \\ 0 & 1 & 0 & 0 & 1 & v \\ 1 & 0 & 1 & v & 1 & v \end{bmatrix} \overset{H_{12}(1)}{\sim} \begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & v \\ 1 & 0 & 1 & v & 1 & v \end{bmatrix} \overset{H_{32}(1)}{\sim}$$

$$\begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & v \\ 1 & 1 & 1 & v & 0 & 0 \end{bmatrix} \overset{H_{31}(v)}{\sim} \begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & v \\ 1 & 1 & 0 & 0 & 0 & 0 \end{bmatrix} \overset{H_1 \to H_3}{\sim} \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & v \\ 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix} \overset{H_2 \to H_3}{\sim}$$

$$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & v \end{bmatrix}.$$

Buradan, G ile verilen üreteç matrisin $\mathbb{Z}_2\mathbb{Z}_2[v]-$ lineer koda permütasyon denk olan standart formdaki üreteç matrisi:

$G' = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & v \end{bmatrix} = \begin{bmatrix} I_{k_0} & D & 0 & (1+v)D_1 \\ 0 & E & I_{k_1} & B_1 + vB_2 \end{bmatrix}$ olarak bulunur. Dolayısıyla C kodunun hangi tipte olduğu ve eleman sayısı kolaylıkla söylenebilir. k_0, k_1, k_2 sırasıyla 1,2,0 dır ve $\mu = \eta = 3$ olduğundan C, $\mathbb{Z}_2\mathbb{Z}_2[v]-$ lineer kodu $(3,3;1,2,0)$ tipindedir. $|C| = 2^1 2^{2.2} = 32$ dir.

2.4. $\mathbb{Z}_2\mathbb{Z}_2[v]-$ Lineer Kodların Dual Uzayı

Bu bölümde öncelikle $\mathbb{Z}_2{}^{\mu} \times R^{\eta}$ de verilen iki elemanın iç çarpımı tanımlanacaktır. Daha sonra $\mathbb{Z}_2\mathbb{Z}_2[v]-$ lineer kodların dualinin bulunması için gerekli olan dönüşümler ve bu dönüşümler yardımıyla önermeler verilecektir. Buradan elde edilen sonuçlar **2. 5.** de kullanılacaktır.

Tanım 2.4.1. Herhangi $c=\left(s_0,s_1,...,s_{\mu-1},t_0,t_1,...,t_{\eta-1}\right)\in \mathbb{Z}_2{}^{\mu}\times R^n$,

$c'=\left(s_0{}',s_1{}',...,s_{\mu-1}{}',t_0{}',t_1{}',...,t_{\eta-1}{}'\right)\in \mathbb{Z}_2{}^{\mu}\times R^n$ elemanlarının iç çarpımı $[12]$ de ki tanımlamadan $\langle c,c'\rangle=\left((1+v)\left(\sum_{i=0}^{\mu-1}s_is_i'\right)+\sum_{j=0}^{\eta-1}t_jt_j'\right)\in \mathbb{Z}_2+v\mathbb{Z}_2$ şeklindedir.

Şimdi bu iç çarpım kullanılarak dual tanımı verilecektir. Ayrıca $C^{\perp};C,\ \mathbb{Z}_2\mathbb{Z}_2[v]-$ lineer kodunun dualini göstermektedir ve $C^{\perp}$ de $\mathbb{Z}_2\mathbb{Z}_2[v]-$ lineer koddur.

Tanım 2.4.2. C nin duali, $C^{\perp}=\left\{c'\in \mathbb{Z}_2{}^{\mu}\times R^{\eta}\mid \langle c,c'\rangle=0,\forall c\in C\right\}$ şeklinde tanımlanır.

Tanım 2.4.3. $\alpha:\mathbb{Z}_2\to\mathbb{Z}_2+v\mathbb{Z}_2$ olmak üzere $\alpha(0)=0,\ \alpha(1)=1+v$,

$\forall x\in \mathbb{Z}_2+v\mathbb{Z}_2$ için

$\beta:\mathbb{Z}_2+v\mathbb{Z}_2\to\mathbb{Z}_2$ olmak üzere $\beta(x)=\begin{cases}0,\ x\in\{0,1+v\}\\ 1,\ x\in\{1,\ v\}\end{cases}$ ve

$\gamma:\mathbb{Z}_2\to\mathbb{Z}_2+v\mathbb{Z}_2$ olmak üzere $\gamma(0)=0,\ \gamma(1)=1$ olacak şekilde tanımlansın.

Tanımlanan α,β,γ dönüşümleri,

$(\alpha,I_d):\mathbb{Z}_2{}^{\mu}\times(\mathbb{Z}_2+v\mathbb{Z}_2)^{\eta}\to(\mathbb{Z}_2+v\mathbb{Z}_2)^{\mu}\times(\mathbb{Z}_2+v\mathbb{Z}_2)^{\eta}$,

$(\beta,I_d):(\mathbb{Z}_2+v\mathbb{Z}_2)^{\mu}\times(\mathbb{Z}_2+v\mathbb{Z}_2)^{\eta}\to\mathbb{Z}_2{}^{\mu}\times(\mathbb{Z}_2+v\mathbb{Z}_2)^{\eta}$,

$(\gamma,I_d):\mathbb{Z}_2{}^{\mu}\times(\mathbb{Z}_2+v\mathbb{Z}_2)^{\eta}\to(\mathbb{Z}_2+v\mathbb{Z}_2)^{\mu}\times(\mathbb{Z}_2+v\mathbb{Z}_2)^{\eta}$ şeklinde genişletilebilir.

Önerme 2.4.1. $\langle,\rangle_v$, R de ki bilinen çarpma işlemini göstermek üzere,

$s\in\mathbb{Z}_2{}^{\mu}\times R^{\eta}$ ve $t\in R^{\mu+\eta}$ için $\langle\alpha(s),t\rangle_v=\langle s,\beta(t)\rangle$ dir.

İspat: $s \in \mathbb{Z}_2{}^{\mu} \times R^{\eta}$ ve $t \in R^{\mu+\eta}$ olsun.

$$\begin{aligned}\langle \alpha(s), t \rangle_v &= \sum_{i=1}^{\mu} \big((1+v)s_i\big)t_i + \sum_{j=\mu+1}^{\mu+\eta} s_j t_j \\ &= \sum_{i=1}^{\mu} \big((1+v)s_i\big)\big(t_i \left(\bmod(1+v)\right)\big) + \sum_{j=\mu+1}^{\mu+\eta} s_j t_j \\ &= \langle s, \beta(t) \rangle\end{aligned}$$

olarak bulunur.

Sonuç 2.4.1. $s, t \in \mathbb{Z}_2{}^{\mu} \times R^{\eta}$ olmak üzere $\langle \alpha(s), \gamma(t) \rangle_v = \langle s, t \rangle$ dir.

İspat: Önerme 2.4.1. i kullanarak, $\langle \alpha(s), \gamma(t) \rangle_v = \langle s, \beta(\gamma(t)) \rangle = \langle s, t \rangle$ bulunur.

Önerme 2.4.2. $C, (\mu, \eta; k_0, k_1, k_2)$ tipindeki $\mathbb{Z}_2\mathbb{Z}_2[v]-$ lineer kodu için C kodunun duali, $C^{\perp} = \beta\left(\alpha(C)^{\perp}\right)$ dir.

İspat: $t \in C^{\perp}$ olsun. Böylece $\forall s \in C$ için $\langle s, t \rangle = 0$ yazılabilir. Bu eşitlik ve Sonuç 2.4.1. den $\langle s, t \rangle = \langle \alpha(s), \gamma(t) \rangle_v = 0$ olacağı açıktır. $\beta(\gamma(t)) = t \in \beta\left(\alpha(C)^{\perp}\right)$ dir. O halde, $C^{\perp} \subseteq \beta\left(\alpha(C)^{\perp}\right)$ dir.

$t \in \alpha(C)^{\perp}$ olsun. $\forall s \in C$ için $\langle \alpha(s), t \rangle_v = 0$ dır. Önerme 2. 4. 1. kullanılarak, $\langle \alpha(s), t \rangle_v = \langle s, \beta(t) \rangle = 0$ bulunur. O halde, $\beta\left(\alpha(C)^{\perp}\right) \subseteq C^{\perp}$ dir.

Dolayısıyla, $C^{\perp} = \beta\left(\alpha(C)^{\perp}\right)$ dir.

2.5. $\mathbb{Z}_2\mathbb{Z}_2[v]-$ Lineer Kodların Kontrol Matrislerinin Standart Formu

Teorem 2.5.1. $C,(\mu,\eta;k_0,k_1,k_2)$ tipindeki $\mathbb{Z}_2\mathbb{Z}_2[v]-$lineer kodunun standart formdaki üreteç matrisi (2.3) te verildiği gibi olsun. $C^{\perp},\mathbb{Z}_2\mathbb{Z}_2[v]-$lineer kodunun standart formdaki üreteç matrisi, dolayısıyla $C,\mathbb{Z}_2\mathbb{Z}_2[v]-$lineer kodunun kontrol matrisi:

$$H=\begin{bmatrix} -D^t & I_{\mu-k_0} & -(1+v)E^t & 0 & 0 \\ -D_1^t & 0 & -(B_1+vB_2)^t+A_2{}^tA_1^t & -A_2{}^t & I_{\eta-k_1-k_2} \\ 0 & 0 & -(1+v)A_1^t & (1+v)I_{k_2} & 0 \end{bmatrix} \tag{2.4}$$

şeklindedir.

İspat: (2.4) ile verilen matrisin, $C,\mathbb{Z}_2\mathbb{Z}_2[v]-$lineer kodunun kontrol matrisi olduğunu göstermek için Önerme 2.4.2. de verilen $C^{\perp}=\beta\left(\alpha(C)^{\perp}\right)$ eşitliği kullanılacaktır. C kodunun üreteç matrisinin standart formu:

$G=\begin{bmatrix} I_{k_0} & D & 0 & 0 & (1+v)D_1 \\ 0 & E & I_{k_1} & A_1 & B_1+vB_2 \\ 0 & 0 & 0 & (1+v)I_{k_2} & (1+v)A_2 \end{bmatrix}$ olsun. O halde öncelikle $\alpha(C)$ kodunun üreteç matrisi yazılmalıdır. Bu üreteç matris aşağıda verilen $G_{\alpha(C)}$ matrisidir.

$$G_{\alpha(C)}=\begin{bmatrix} (1+v)I_{k_0} & (1+v)D & 0 & 0 & (1+v)D_1 \\ 0 & (1+v)E & I_{k_1} & A_1 & B_1+vB_2 \\ 0 & 0 & 0 & (1+v)I_{k_2} & (1+v)A_2 \end{bmatrix}$$

Dikkat edilirse $\alpha(C)$ kodu $R^{\mu+\eta}$ üzerinde lineer bir koddur. R de ki C lineer koduna permütasyon denk olan üreteç matris:

$\begin{bmatrix} I_{k_1} & A_1 & B_1+vB_2 \\ 0 & (1+v)I_{k_2} & (1+v)A_2 \end{bmatrix}$ şeklindedir. O zaman $G_{\alpha(C)}$ matrisi de bu formda yazılabilir.

$$\begin{bmatrix} (1+v)I_{k_0} & (1+v)D & 0 & 0 & (1+v)D_1 \\ 0 & (1+v)E & I_{k_1} & A_1 & B_1+vB_2 \\ 0 & 0 & 0 & (1+v)I_{k_2} & (1+v)A_2 \end{bmatrix} \overset{H_1 \leftrightarrow H_2}{\sim}$$

$$\begin{bmatrix} 0 & (1+v)E & I_{k_1} & A_1 & B_1+vB_2 \\ (1+v)I_{k_0} & (1+v)D & 0 & 0 & (1+v)D_1 \\ 0 & 0 & 0 & (1+v)I_{k_2} & (1+v)A_2 \end{bmatrix} \overset{K_1 \leftrightarrow K_3}{\sim}$$

$$\begin{bmatrix} I_{k_1} & (1+v)E & 0 & A_1 & B_1+vB_2 \\ 0 & (1+v)D & (1+v)I_{k_0} & 0 & (1+v)D_1 \\ 0 & 0 & 0 & (1+v)I_{k_2} & (1+v)A_2 \end{bmatrix} \overset{K_2 \leftrightarrow K_4}{\sim}$$

$$\begin{bmatrix} I_{k_1} & A_1 & 0 & (1+v)E & B_1+vB_2 \\ 0 & 0 & (1+v)I_{k_0} & (1+v)D & (1+v)D_1 \\ 0 & (1+v)I_{k_2} & 0 & 0 & (1+v)A_2 \end{bmatrix} \overset{H_2 \leftrightarrow H_3}{\sim}$$

$$\begin{bmatrix} I_{k_1} & A_1 & 0 & (1+v)E & B_1+vB_2 \\ 0 & (1+v)I_{k_2} & 0 & 0 & (1+v)A_2 \\ 0 & 0 & (1+v)I_{k_0} & (1+v)D & (1+v)D_1 \end{bmatrix} = G'_{\alpha(C)}$$

olsun. Burada, $\begin{bmatrix} (1+v)I_{k_2} & 0 \\ 0 & (1+v)I_{k_0} \end{bmatrix} = (1+v)I'_{k'_2}$,

$\begin{bmatrix} A_1 & 0 \end{bmatrix} = A'_1$, $\begin{bmatrix} (1+v)E & B_1+vB_2 \end{bmatrix} = B'_1+vB'_2$ ve $\begin{bmatrix} 0 & (1+v)A_2 \\ (1+v)D & (1+v)D_1 \end{bmatrix} = (1+v)A'_2$

olsun. Buradan, $\begin{bmatrix} I_{k_1} & A'_1 & B'_1+vB'_2 \\ 0 & (1+v)I'_{k'_2} & (1+v)A'_2 \end{bmatrix}$, $G'_{\alpha(C)}$ matrisinin $R^{\mu+\eta}$ da standart formda yazılmış halidir. Bu matrisin kontrol matrisi,

$$\begin{bmatrix} -(B'_1+vB'_2)^t + A'^t_2 A'^t_1 & -A'^t_2 & I_{\mu+\eta-k_1-k'_2} \\ -(1+v)A'^t_1 & (1+v)I'_{k'_2} & 0 \end{bmatrix}$$

şeklinde yazılabilir. Buradan $(B'_1+vB'_2)$, A'_2, A'_1 ve $(1+v)I'_{k'_2}$ matrisleri yerlerine yazılarak, $\alpha(C)^{\perp}$ için üreteç matris

$$\begin{bmatrix} -(1+v)E^t & 0 & -D^t & I_{\mu+\eta-k_0-k_1-k_2} \\ -(B_1+vB_2)^t + A_2^t A_1^t & -A_2{}^t & -D_1{}^t & 0 \\ -(1+v)A_1^t & (1+v)I_{k_2} & 0 & 0 \\ 0 & 0 & (1+v)I_{k_0} & 0 \end{bmatrix}$$

olarak bulunur. Şimdi gerekli düzenlemeler yapılırsa,

$$\begin{bmatrix} -(1+v)E^t & 0 & -D^t & I_{\mu-k_0} & 0 \\ -(B_1+vB_2)^t + A_2{}^t A_1^t & -A_2{}^t & -D_1{}^t & 0 & I_{\eta-k_1-k_2} \\ -(1+v)A_1^t & (1+v)I_{k_2} & 0 & 0 & 0 \\ 0 & 0 & (1+v)I_{k_0} & 0 & 0 \end{bmatrix}$$

matrisi elde edilir. $K_2 \leftrightarrow K_4$ ve $K_1 \leftrightarrow K_3$ şeklinde yapılan sütun permütasyonlarının geri alınmasıyla aşağıdaki matris bulunur.

$$H' = \begin{bmatrix} -D^t & I_{\mu-k_0} & -(1+v)E^t & 0 & 0 \\ -D_1{}^t & 0 & -(B_1+vB_2)^t + A_2{}^t A_1^t & -A_2{}^t & I_{\eta-k_1-k_2} \\ 0 & 0 & -(1+v)A_1^t & (1+v)I_{k_2} & 0 \\ (1+v)I_{k_0} & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Son adımda β dönüşümü uygulanarak,

$$\beta(H') = \begin{bmatrix} -D^t & I_{\mu-k_0} & -(1+v)E^t & 0 & 0 \\ -D_1{}^t & 0 & -(B_1+vB_2)^t + A_2{}^t A_1^t & -A_2{}^t & I_{\eta-k_1-k_2} \\ 0 & 0 & -(1+v)A_1^t & (1+v)I_{k_2} & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} = H$$

olarak bulunur.

Sonuç 2.5.1. C, $\mathbb{Z}_2\mathbb{Z}_2[v]-$ lineer kodu $(\mu,\eta;k_0,k_1,k_2)$ tipinde ise, Teorem 2.5.1. de elde edilen kontrol matrisi doğrultusunda $C^{\perp}$ lineer dual kodu $(\mu,\eta;\mu-k_0,\eta-k_1-k_2,k_2)$ tipindedir.

Örnek 2.5.1. $G' = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & v \end{bmatrix} = \begin{bmatrix} I_{k_0} & D & 0 & (1+v)D_1 \\ 0 & E & I_{k_1} & B_1 + vB_2 \end{bmatrix}$

Örnek 2.3.1. de verilen üreteç matrisin $\mathbb{Z}_2\mathbb{Z}_2[v]-$ lineer koda permütasyon denk olan standart formdaki üreteç matrisi olarak bulunmuştu. Böylece,

$D = [1 \quad 0]$, $D_1 = [0]$, $E = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, $B_1 + vB_2 = \begin{bmatrix} 0 \\ v \end{bmatrix}$ dir. Buradan C, $\mathbb{Z}_2\mathbb{Z}_2[v]-$ lineer kodunun kontrol matrisi,

$$H = \begin{bmatrix} -D^t & I_{\mu-k_0} & -(1+v)E^t & 0 & 0 \\ -D_1^t & 0 & -(B_1+vB_2)^t + A_2{}^t A_1^t & -A_2^t & I_{\eta-k_1-k_2} \\ 0 & 0 & -(1+v)A_1^t & (1+v)I_{k_2} & 0 \end{bmatrix}$$

$$= \begin{bmatrix} -1 & 1 & 0 & 0 & -(1+v) & 0 \\ 0 & 0 & 1 & -(1+v) & 0 & 0 \\ 0 & 0 & 0 & 0 & -v & 1 \end{bmatrix}$$

olarak bulunur. Böylece $C^\perp$, $(3,3;2,1,0)$ tipindedir ve $|C^\perp| = 2^2.2^{2.1} = 16$ adet kod söze sahiptir.

BÖLÜM 3. $\mathbb{Z}_2\mathbb{Z}_2[v]-(v)-$ SABİT DEVİRLİ KODLAR

Devirli ve sabit devirli kodlar lineer kodların önemli birer sınıfını oluşturmaktadır. $\mathbb{Z}_2\mathbb{Z}_4-$toplamsal devirli kodlar ve duali için çalışmalar yapılmıştır$[21,22]$. $u^2=0$ olmak üzere $\mathbb{Z}_2+u\mathbb{Z}_2$ halkası üzerindeki devirli kodlar için birçok çalışma yapıldı $[23,24,25]$. Ayrıca $u^2=0$ olmak üzere $\mathbb{Z}_2\mathbb{Z}_2[u]-$devirli ve sabit devirli kodlar Aydoğdu ve ark. $[26]$ tarafından çalışılmıştır.

η tek ve $v^2=1$ olmak üzere, bu bölümde $\mathbb{Z}_2\mathbb{Z}_2[v]-(v)-$sabit devirli kodun üreteç polinomu ve en küçük geren kümesi verilmiştir. Daha sonra devirli ve sabit devirli kodların arasındaki ilişkiden yola çıkılarak, $\mathbb{Z}_2\mathbb{Z}_2[v]-(v)-$sabit devirli kodun dual kodu belirlenmiştir. Ayrıca C sabit devirli kod olduğunda, tanımlanan gray fonksiyonu ile görüntüsü parçalı devirli (quasicylic) olan örnekler verilmiştir.

3.1. $\mathbb{Z}_2\mathbb{Z}_2[v]-(v)-$ Sabit Devirli Kodların Cebirsel Yapısı

Tanım 3.1.1. Herhangi bir $c=(s_0,s_1,...,s_{\mu-1},t_0,t_1,...,t_{\eta-1})\in C$ için $(v)-$sabit devir ötelemesi, $T_{(v)}(c)=(s_{\mu-1},s_0,...,s_{\mu-2},vt_{\eta-1},t_0,...,t_{\eta-2})\in C$ ise $\mathbb{Z}_2{}^{\mu}\times(\mathbb{Z}_2+v\mathbb{Z}_2)^{\eta}$ nın C, $\mathbb{Z}_2+v\mathbb{Z}_2-$alt modülüne $\mathbb{Z}_2\mathbb{Z}_2[v]-$lineer $T_{(v)}-$sabit devirli kod denir.

Herhangi $c,c'\in\mathbb{Z}_2{}^{\mu}\times R^{\eta}$ elemanlarının iç çarpımı Tanım 2.4.1. de verilmişti. Şimdi bu çarpma dikkate alınarak C nin duali tanımlansın.

Tanım 3.1.2. C, $\mathbb{Z}_2\mathbb{Z}_2[v]-$sabit devirli kod olsun.

$C^{\perp}=\{c'\in\mathbb{Z}_2{}^{\mu}\times R^{\eta}\mid\langle c,c'\rangle=0,\forall c\in C\}$ şeklinde tanımlanır.

Önerme 3.1.1. $C,\ \mathbb{Z}_2\mathbb{Z}_2[v]-$ lineer sabit devirli kod ise $C^{\perp}$ de sabit devirli koddur.

İspat: $C,\ \mathbb{Z}_2\mathbb{Z}_2[v]-$ lineer sabit devirli kod olsun.

$c'=\left(s_0',s_1',...,s_{\mu-1}',t_0',t_1',...,t_{\eta-1}'\right)\in C^{\perp}$ olsun. $T_{(v)}(c')\in C^{\perp}$ olduğu gösterilmelidir.

$c'\in C^{\perp}$ olduğundan, herhangi $c=\left(s_0,s_1,...,s_{\mu-1},t_0,t_1,...,t_{\eta-1}\right)\in C$ için,

$$c.c'=(1+v)s_0s_0'+(1+v)s_1s_1'+...+(1+v)s_{\mu-1}s_{\mu-1}'$$
$$+t_0t_0'+t_1t_1'+....+t_{\eta-1}t_{\eta-1}'\pmod 2$$
$$=\left((1+v)\left(\sum_{i=0}^{\mu-1}s_is_i'\right)+\sum_{j=0}^{\eta-1}t_jt_j'\right)$$
$$=0\pmod 2 \text{ yazılabilir.}$$

$ekok(\mu,\eta)=m$ olsun. Herhangi $c\in\mathbb{Z}_2^{\mu}\times R^{\eta}$ için $T_{(v)}^{m}(c)=c$ dir. $T_{(v)}^{m-1}(c)=\left(s_1,...,s_{\mu-1}s_0,t_1,...,t_{\eta-1},vt_0\right)=d$ olsun. $C,\ \mathbb{Z}_2\mathbb{Z}_2[v]-$ lineer sabit devirli kod olduğundan, $d\in C$ dir. Buradan,

$$0=d.c'=(1+v)\left(s_1s_0'+...+s_{\mu-1}s_{\mu-2}'+s_0s_{\mu-1}'\right)+\left(t_1t_0'+...+t_{\eta-1}t_{\eta-2}'+vt_0t_{\eta-1}'\right)$$
$$=(1+v)\left(s_0s_{\mu-1}'+s_1s_0'+...+s_{\mu-1}s_{\mu-2}'\right)+\left(vt_0t_{\eta-1}'+t_1t_0'+...+t_{\eta-1}t_{\eta-2}'\right)$$
$$=c.T_{(v)}(c') \text{ olarak bulunur.}$$

Böylece $T_{(v)}(c')\in C^{\perp}$ dir ve $C^{\perp}$ de sabit devirli koddur.

$S_{\mu,\eta}=\mathbb{Z}_2[x]/\left(x^{\mu}-1\right)\times R[x]/\left(x^{\eta}-v\right)$ ve

$c=\left(s_0,s_1,...,s_{\mu-1},t_0,t_1,...,t_{\eta-1}\right)\in\mathbb{Z}_2{}^{\mu}\times\left(\mathbb{Z}_2+v\mathbb{Z}_2\right)^{\eta}$ olsun. Bu kod söz $S_{\mu,\eta}$ üzerinde $c(x)=\left(s_0+s_1x+...+s_{\mu-1}x^{\mu-1},t_0+t_1x+...+t_{\eta-1}x^{\eta-1}\right)=(s(x),t(x))$ biçiminde polinomlar cinsinden ifade edilebilir. τ, Tanım 2.2.1. de verilen dönüşüm olmak üzere, $r(x)=r_0+r_1x+...+r_lx^l\in R[x]$ ve $(s(x),t(x))\in S_{\mu,\eta}$ olsun.

$\tau(r(x)) = \tau(r_0) + \tau(r_1)x + ... + \tau(r_l)x^l$ olmak üzere,

$r(x) * (s(x), t(x)) = (\tau(r(x))s(x), r(x)t(x))$ olacak şekilde tanımlanır.

Teorem 3.1.1. $S_{\mu,\eta}$ yukarıda tanımlanan çarpma işlemine göre $R[x]-$ modüldür.

İspat: $\forall r(x), r'(x) \in R[x]$, $\forall (s(x), t(x)), ((s'(x), t'(x)) \in S_{\mu,\eta}$ için,

$$\begin{aligned} i.\ r * [(s,t) + (s',t')] &= r * (s + s', t + t') \\ &= (\tau(r)(s + s'), r(t + t')) \\ &= (\tau(r)s, rt) + (\tau(r)s', rt') \\ &= r * (s,t) + r * (s',t') \end{aligned}$$

$$\begin{aligned} ii.\ (r + r') * (s,t) &= (\tau(r + r')s, (r + r')t) \\ &= (\tau(r)s + \tau(r')s, rt + r't) \\ &= (\tau(r)s, rt) + (\tau(r')s, r't) \\ &= r * (s,t) + r' * (s,t) \end{aligned}$$

$$\begin{aligned} iii.\ r * [r' * (s,t)] &= r * [\tau(r')s, r't] \\ &= (\tau(r)\tau(r')s, rr't) \\ &= (\tau(rr')s, rr't) \\ &= (rr') * (s,t) \end{aligned}$$

$$iv.\ 1_{S[x]} * (s,t) = (\tau(1_{S[x]})s, t) = (s,t)$$

elde edilir. Böylece $S_{\mu,\eta}$ yukarıda tanımlanan çarpma işlemine göre $R[x]-$ modüldür.

$C \subseteq \mathbb{Z}_2{}^{\mu} \times R^{\eta}$, $T_{(v)} -$ sabit devirli kod için, C den alınan $c = (s_0, s_1, ..., s_{\mu-1}, t_0, t_1, ..., t_{\eta-1})$ kod sözü $c(x) = (s_0 + s_1x + ...s_{\mu-1}x^{\mu-1}, t_0 + t_1x + ... + t_{\eta-1}x^{\eta-1}) \in S_{\mu,\eta}$ şeklinde polinom olarak gösterilebilir.

Dikkat edilirse, $T_{(v)}(c) = (s_{\mu-1}, s_0, ..., s_{\mu-2}, vt_{\eta-1}, t_0, ..., t_{\eta-2}) \in C$,

$x * c(x) = (s_{\mu-1} + s_0x + ... + s_{\mu-2}x^{\mu-1}, vt_{\eta-1} + t_0x + ... + t_{\eta-2}x^{\eta-1}) \in C$ ye dönüşen bir özelliktir.

Teorem 3.1.2. Bir C kodunun $\mathbb{Z}_2\mathbb{Z}_2[v]-$lineer $T_{(v)}-$sabit devirli kod olması için gerekli ve yeter şart C nin $S_{\mu,\eta}$ nın $R[x]-$alt modülü olmasıdır.

İspat: C, $\mathbb{Z}_2\mathbb{Z}_2[v]-$lineer $T_{(v)}-$sabit devirli kod olsun. $c(x)=(s(x),t(x))\in C$ olsun. $c'(x),c''(x)\in C$ için $c'(x)-c''(x)\in C$ dir. C, $T_{(v)}-$sabit devirli kod olduğundan $x*c(x)\in C$ ve $x^2*c(x)\in C$ olarak bulunur. Benzer şekilde $k\geq 0$ için $x^k*c(x)\in C$ elde edilir. Ayrıca C lineer olduğundan $\forall r(x)\in R[x]$ için $r(x)*c(x)\in C$ dir. Böylece C, $S_{\mu,\eta}$ nın $R[x]-$alt modülüdür.

Aksine C, $S_{\mu,\eta}$ nın $R[x]-$alt modülü olsun. $c(x)\in C$ ve $x\in R[x]$ olsun. Buradan $x*c(x)\in C$ bulunur. Böylece C, $\mathbb{Z}_2\mathbb{Z}_2[v]-$lineer $T_{(v)}-$sabit devirli koddur.

3.2. $\mathbb{Z}_2\mathbb{Z}_2[v]-$ Sabit Devirli Kodların Üreteç Polinomları Ve En Küçük Geren Kümesi

Bu bölümde $\mathbb{Z}_2\mathbb{Z}_2[v]-$sabit devirli kodun üreteç polinomunu bulmak için $[27]$ de verilen Teorem 3 den yararlanılmıştır. η tek pozitif tam sayı olarak alınmıştır.

C, $\mathbb{Z}_2\mathbb{Z}_2[v]-$ lineer $T_{(v)}-$sabit devirli kod olsun. C kodu ve $R[x]/\langle x^\eta - v\rangle$, $R[x]-$ modül olduğundan,

$\chi: \quad C \rightarrow R[x]/\langle x^\eta - v\rangle$
$(f(x),f'(x)) \rightarrow f'(x)$ olacak şekilde tanımlanan χ dönüşümü $R[x]-$modül homomorfizmasıdır. $Çek\,\chi=\{(f(x),0)\in C: f(x)\in\mathbb{Z}_2[x]/\langle x^\mu-1\rangle\}$, C nin bir alt modülü olup, $\mathrm{Im}\,\chi$, $R[x]/\langle x^\eta - v\rangle$ nin bir alt modülüdür.

Aşağıda tanımlanan π dönüşümü R de ki devirli ve sabit devirli kodlar arasındaki ilişkiyi vermektedir.

Önerme 3.2.1. $\pi : R[x]/\langle x^{\eta}-1\rangle \to R[x]/\langle x^{\eta}-v\rangle$
$r(x) \to r(vx)$

olacak şekilde π dönüşümü tanımlansın. η tek olduğunda π dönüşümü halka izomorfizmasıdır.

İspat: i. $\forall r(x), r'(x) \in R[x]/\langle x^{\eta}-1\rangle$ için $r(x) = r'(x)\left(\mathrm{mod}\,(x^{\eta}-1)\right)$ iken $\pi(r(x)) = \pi(r'(x))\left(\mathrm{mod}(x^{\eta}-v)\right)$ mi?

$r(x) = r'(x)\left(\mathrm{mod}\, x^{\eta}-1\right)$ ise $r(x) = \left(x^{\eta}-1\right).q(x) + r'(x)$ dir. Bu eşitlikte x yerine vx yazılırsa, $r(vx) = \left((vx)^{\eta}-1\right).q(vx) + r'(vx)$

$= \left(v^{\eta}x^{\eta}-v^{2}\right).q(vx) + r'(vx)$; η tek ise $v^{\eta} = v$ olduğundan,

$= v\left(x^{\eta}-v\right).q(vx) + r'(vx)$ bulunur. Yani,

$r(vx) = v\left(x^{\eta}-v\right).q(vx) + r'(vx)$ dir. O halde, $\pi(r(x)) = \pi(r'(x))\left(\mathrm{mod}(x^{\eta}-v)\right)$ dir. Buradan, π iyi tanımlıdır.

ii. $\forall r(x), r'(x) \in R[x]/\langle x^{\eta}-1\rangle$ için $\pi(r(x)) = \pi(r'(x))\left(\mathrm{mod}(x^{\eta}-v)\right)$ ise $r(x) = r'(x)\left(\mathrm{mod}(x^{\eta}-1)\right)$ mi?

$\pi(r(x)) = \pi(r'(x))$ ise $r(vx) = r'(vx)\left(\mathrm{mod}(x^{\eta}-v)\right)$ dir. Buradan, $r(vx) = \left(x^{\eta}-v\right).q(vx) + r'(vx)\left(\mathrm{mod}(x^{\eta}-v)\right)$ yazılabilir. Bu eşitlikte x yerine vx yazılırsa, $r(x) = \left((vx)^{\eta}-v\right).q(x) + r'(x)$

$= \left((v)^{\eta}x^{\eta}-v\right).q(x) + r'(x)$; η tek ise $v^{\eta} = v$ olduğundan,

$= \left(vx^{\eta}-v\right).q(x) + r'(x)$

$= v\left(x^{\eta}-1\right).q(x) + r'(x)$ bulunur. Yani, $r(x) = r'(x)\left(\mathrm{mod}\, x^{\eta}-1\right)$ dir. Buradan, π birebirdir.

iii. Sonlu ve birebir olduğundan örtendir.

iv. $\forall r(x), r'(x) \in R[x]/\langle x^{\eta}-1\rangle$ için,

$a)\pi(r(x)+r'(x)) = \pi(r(x)) + \pi(r'(x))$ ve $b)\pi(r(x).r'(x)) = \pi(r(x)).\pi(r'(x))$ mi?

$\forall r(x), r'(x) \in R[x]/\langle x^{\eta}-1\rangle$ için,

$$a)\pi(r(x)+r'(x)) = \pi((r+r')(x)) = (r+r')(vx) = r(vx)+r'(vx)$$
$$= \pi(r(x)) + \pi(r'(x))$$

$$b)\pi(r(x).r'(x)) = \pi((r.r')(x)) = (r.r')(vx) = r(vx).r'(vx) = \pi(r(x)).\pi(r'(x))$$

bulunur.

Buradan, π halka homorfizmasıdır.

Böylece, i. ii. iii. ve iv. den π bir halka izomorfizmasıdır.

Sonuç 3.2.1. I nın $R[x]/\langle x^{\eta}-1\rangle$ in ideali olması için gerek ve yeter şart $\pi(I)$ nın $R[x]/\langle x^{\eta}-v\rangle$ nin ideali olmasıdır.

İspat: $(\Rightarrow)$: I, $R[x]/\langle x^{\eta}-1\rangle$ ideali olsun. O zaman,

i. $\forall a(x), b(x) \in I$ için $a(x)-b(x) \in I$ ve

ii. $\forall a(x) \in I$, $\forall r(x) \in R[x]/\langle x^{\eta}-1\rangle$ için $a(x)r(x) \in I$, $r(x)a(x) \in I$ dır.

Şimdi $\pi(I)$ nın $R[x]/\langle x^{\eta}-v\rangle$ nin ideali olduğu gösterilsin.

i. $\forall a(x), b(x) \in I$ ve $\forall \pi(a(x)) = a(vx)$, $\pi(b(x)) = b(vx) \in \pi(I)$ için,
$\pi(a(x)-b(x)) = \pi(a(x)) - \pi(b(x)) \in \pi(I)$ dır.

ii. $\forall \pi(a(x)) = a(vx) \in \pi(I)$ ve $\forall r(x) \in R[x]/\langle x^{\eta}-v\rangle$ için,
$\pi(a(x)r(x)) = \pi(a(x))r(x) \in \pi(I)$ ve $\pi(r(x)a(x)) = r(x)\pi(a(x)) \in \pi(I)$
dır.

Böylece i. ve ii. den $\pi(I)$, $R[x]/\langle x^{\eta}-v\rangle$ nin bir idealidir.

$(\Leftarrow)$: $\pi(I)$, $R[x]/\langle x^{\eta}-v\rangle$ nin ideali olsun. O zaman,

i. $\forall \pi(a(x)), \pi(b(x)) \in \pi(I)$ için $\pi(a(x)) - \pi(b(x)) \in \pi(I)$ ve

ii. $\forall \pi(a(x)) \in \pi(I)$, $\forall r(x) \in R[x]/\langle x^{\eta}-v \rangle$ için $\pi(a(x))r(x) \in I$ ve $r(x)\pi(a(x)) \in I$ dır.

Şimdi I nın $R[x]/\langle x^{\eta}-1 \rangle$ in ideali olduğu gösterilsin.

$\pi(a(x)-b(x)) = \pi(a(x)) - \pi(b(x)) \in \pi(I)$ ve $\pi(a(x)r(x)) = \pi(a(x))r(x) \in \pi(I)$ dır. Buradan,

$\forall a(x), b(x) \in I$ için $a(x)-b(x) \in I$ ve $r(x)a(x) \in I$ dır.

$\pi(r(x)a(x)) = r(x)\pi(a(x)) \in \pi(I)$ ise $a(x)r(x) \in I$ dır.

Böylece I, $R[x]/\langle x^{\eta}-1 \rangle$ in bir idealidir.

Teorem 3.2.1. C kodu $S_{\mu,\eta}$ da $T_{(v)}$ – sabit devirli kod olsun. $f(x) \mid (x^{\mu}-1) \pmod 2$, $a(x) \mid g(x) \mid (x^{\eta}-v) \pmod 2$ ve $l(x)$ ikili polinom olmak üzere $C = \langle (f(x),0), (l(x), g(x)+(1+v)a(x)) \rangle$ şeklindedir. $der(l(x)) < der(f(x))$ ve $f(x) \mid \left(\frac{x^{\eta}-v}{a(x)}\right) l(x) \bmod (1+v)$ dir.

İspat: C kodu $S_{\mu,\eta}$ da $T_{(v)}$ – sabit devirli kod olmak üzere,

$\mathrm{Im}\,\chi = \langle g(x)+(1+v)a(x) \rangle$ olsun. Böylece $(l(x), g(x)+(1+v)a(x)) \in C$ vardır öyle ki $\chi(l(x), g(x)+(1+v)a(x)) = g(x)+(1+v)a(x)$ dir. Öncelikle $(s(x),t(x)) \in C$ nin $(f(x),0)$ ve $(l(x), g(x)+(1+v)a(x))$ tarafından üretildiği gösterilsin. $\chi(s(x),t(x)) = t(x) = w_1(x)(g(x)+(1+v)a(x))$ şartını sağlayan $w_1(x) \in R[x]/\langle x^{\eta}-v \rangle$ vardır.

$$(s(x),t(x)) - w_1(x) * (l(x), g(x)+(1+v)a(x)) = (s(x)-\tau(w_1(x))l(x), 0) \in Çek\,\chi \qquad (3.1)$$

dir. Dolayısıyla, $(s(x)-\tau(w_1(x))l(x),0) = w_2(x)(f(x),0)$ şartını sağlayan $w_2(x) \in \mathbb{Z}_2[x]/\langle x^{\mu}-1 \rangle$ vardır.

(3.1) den,

$$(s(x),t(x)) = w_1(x) * (l(x), g(x) + (1+v)a(x)) + (s(x) - \tau(w_1(x))l(x), 0)$$

$$= w_1(x) * (l(x), g(x) + (1+v)a(x)) + w_2(x)(f(x), 0) \text{ olduğundan,}$$

$C \subseteq \langle (f(x),0), (l(x), g(x) + (1+v)a(x)) \rangle$ bulunur.

Tersine, $C \supseteq \langle (f(x),0), (l(x), g(x) + (1+v)a(x)) \rangle$ olduğundan,

$C = \langle (f(x),0), (l(x), g(x) + (1+v)a(x)) \rangle$ elde edilir.

Şimdi, $der(l(x)) \geq der(f(x))$ olsun. $l(x) = f(x)q(x) + r(x)$;

$0 \leq der(r(x)) < der(f(x))$ şartını sağlayan $q(x), r(x) \in \mathbb{Z}_2[x] / \langle x^{\mu} - 1 \rangle$ vardır.

$$\langle (f(x),0), (l(x), g(x) + (1+v)a(x)) \rangle = \langle (f(x),0), (f(x)q(x) + r(x), g(x) + (1+v)a(x)) \rangle$$

$$= \langle (f(x),0), (r(x), g(x) + (1+v)a(x)) \rangle \text{ dir.}$$

Böylece, $der(l(x)) < der(f(x))$ bulunur.

Son olarak, $f(x) \mid \left(\frac{x^{\eta} - v}{a(x)} \right) l(x) \pmod{1+v}$ olduğu gösterilsin.

$$\frac{x^{\eta} - v}{a(x)} * (l(x), g(x) + (1+v)a(x)) = \left(\tau\left(\frac{x^{\eta} - v}{a(x)} \right) l(x), \frac{x^{\eta} - v}{a(x)} (g(x) + (1+v)a(x)) \right)$$

$$= \left(\tau\left(\frac{x^{\eta} - v}{a(x)} \right) l(x), 0 \right) \text{dır.}$$

$\chi\left(\tau\left(\frac{x^{\eta} - v}{a(x)} \right) l(x), 0 \right) = 0$ bulunur. $\left(\tau\left(\frac{x^{\eta} - v}{a(x)} \right) l(x), 0 \right) \in Çek\chi \subseteq C$ dir. Dolayısıyla,

$f(x) \mid \left(\frac{x^{\eta} - v}{a(x)} \right) l(x) \pmod{1+v}$ elde edilir.

Sonuç 3.2.2. Eğer $ebob\left(f(x), \frac{x^{\eta} - v}{a(x)} \right) = 1 \pmod{1+v}$ ise $l(x) = 0$ dır.

İspat: $f(x)\left|\left(\frac{x^{\eta}-v}{a(x)}\right)l(x)\ (\mathrm{mod}1+v)\right.$ ve $ebob\left(f(x),\frac{x^{\eta}-v}{a(x)}\right)=1\ (\mathrm{mod}1+v)$ olduğundan $f(x)\,|\,l(x)$ tir. Ancak $der(l(x))<der(f(x))$ olduğundan $l(x)=0$ dır.

Uyarı 3.2.1. Aşağıda verilen teorem ve ispatta alınan herhangi bir $f(x)$ polinomu f şeklinde verilecektir.

Teorem 3.2.2. f,a,g,l polinomları Teorem 3.2.1. de verilen polinomlar olmak üzere, $C=\langle(f,0),(l,g+(1+v)a)\rangle$, $S_{\mu,\eta}$ da $T_{(v)}-$sabit devirli kod olsun.

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

$$S_2=\bigcup_{i=0}^{\eta-der(g)-1}\{x^i*(l,g+(1+v)a)\},$$

$$S_3=\bigcup_{i=0}^{der(g)-der(a)-1}\{x^i*(\tau(k)l,(1+v)ka)\}.$$

için $S=S_1\cup S_2\cup S_3$, C için en küçük geren kümedir ve C kodunun $2^{\mu-der(f)}4^{\eta-der(g)}2^{der(g)-der(a)}$ tane kod sözü vardır.

İspat: $C=\langle(f,0),(l,g+(1+v)a)\rangle$ ve $c\in C$ olsun. $w_1,w_2\in R[x]$ olmak üzere, $c=\tau(w_1)(f,0)+w_2*(l,g+(1+v)a)\in S_{\mu,\eta}$ yazılabilir. Eğer, $der(\tau(w_1))\le\mu-der(f)-1$ ise $\tau(w_1)(f,0)\in\langle S_1\rangle$ dir. Aksi taktirde bölme algoritması uygulanarak, $q_1,r_1\in R[x]$ ve $0\le der(\tau(r_1))\le\mu-der(f)-1$ olmak üzere, $\tau(w_1)=\left(\frac{x^{\mu}-1}{f}\tau(q_1)\right)+\tau(r_1)$ dir.

Dolayısıyla, $\tau(w_1)(f,0)=\left(\frac{x^{\mu}-1}{f}\tau(q_1)+\tau(r_1)\right)(f,0)$

$$=\tau(r_1)(f,0)\text{ dır.}$$

$der(\tau(r_1)) \le \mu - der(f) - 1$ olduğundan, $\tau(r_1)(f,0) \in \langle S_1 \rangle$ dir. Eğer, $der(w_2) \le \eta - der(g) - 1$ ise $w_2 * (l, g + (1+\nu)a) \in \langle S_2 \rangle$ dir. Aksi taktirde bölme algoritması uygulanarak, $0 \le der(r_2) \le \eta - der(g) - 1$ olmak üzere,

$w_2 = \dfrac{x^\eta - \nu}{g} q_2 + r_2 = kq_2 + r_2$ dir. Buradan,

$$\begin{aligned} w_2 * (l, g + (1+\nu)a) &= (kq_2 + r_2) * (l, g + (1+\nu)a) \\ &= q_2(\tau(k)l, kg + (1+\nu)ka) + r_2(l, g + (1+\nu)a) \\ &= q_2(\tau(k)l, (1+\nu)ka) + r_2(l, g + (1+\nu)a) \text{ olur.} \end{aligned}$$

$0 \le der(r_2) \le \eta - der(g) - 1$ olduğundan, $r_2(l, g + (1+\nu)a) \in \langle S_2 \rangle$ dir. Şimdi $q_2(\tau(k)l, (1+\nu)ka) \in \langle S \rangle$ olduğu ispatlansın. $a \mid g \mid (x^\eta - \nu)$ olduğundan $g = ab$ olacak şekilde $b \in R[x]$ vardır. Buradan, $x^\eta - \nu = gk = abk$ dir. Eğer $der(q_2) \le der(g) - der(a) - 1$ ise $q_2(\tau(k)l, (1+\nu)ka) \in \langle S_3 \rangle$ tür. Aksi taktirde bölme algoritması uygulanarak, $0 \le der(r_3) \le der(g) - der(a) - 1$ olmak üzere,

$q_2 = \dfrac{x^\eta - \nu}{ka} q_3 + r_3$ tür. Buradan,

$$\begin{aligned} q_2(\tau(k)l, (1+\nu)ka) &= \left(\frac{x^\eta - \nu}{ka} q_3 + r_3 \right)(\tau(k)l, (1+\nu)ka) \\ &= \left(\frac{x^\eta - \nu}{ka} q_3 \tau(k)l, \frac{x^\eta - \nu}{ka} q_3 (1+\nu)ka \right) + r_3(\tau(k)l, (1+\nu)ka) \\ &= \left(\frac{x^\eta - \nu}{ka} q_3 \tau(k)l, 0 \right) + r_3(\tau(k)l, (1+\nu)ka) \text{ dır.} \end{aligned}$$

$0 \le der(r_3) \le der(b) - 1$ olduğundan $r_3(\tau(k)l, (1+\nu)ka) \in \langle S_3 \rangle$ tür.

$f \mid \dfrac{x^\eta - \nu}{a} l \pmod{1+\nu}$ olduğundan bazı m polinomu için $\dfrac{x^\eta - \nu}{a} l = fm \pmod{1+\nu}$ yazılabilir.

Dolayısıyla, $\left(\dfrac{x^\eta - \nu}{ka} q_3 \tau(k)l, 0 \right) \in \langle S_1 \rangle$ dir.

Sonuç olarak, $S = S_1 \cup S_2 \cup S_3$ kümesi C için geren kümedir ve S kümesindeki diğer elemanlar ile lineer bağımlı olacak şekilde eleman olmadığından S kümesi C için en küçük geren kümedir. Dolayısıyla, C kodu $2^{\mu-der(f)}4^{\eta-der(g)}2^{der(g)-der(a)}$ tane kod söze sahiptir.

3.3. $\mathbb{Z}_2\mathbb{Z}_2[v]-$ Devirli Ve Sabit Devirli Kodların Dualinin Yapısı

Tezin bu bölümünde $v^2 = 1$ olmak üzere $\mathbb{Z}_2\mathbb{Z}_2[v]-$ devirli kodların dualinin yapısı belirlenecektir. $R_{\mu,\eta} = \mathbb{Z}_2[x]/(x^\mu - 1) \times R[x]/(x^\eta - 1)$ olsun. $R_{\mu,\eta}$ üzerindeki devirli kodlar ve $S_{\mu,\eta}$ üzerindeki sabit devirli kodlar arasındaki birebir ilişki π dönüşümü ile verildiğinden $\mathbb{Z}_2\mathbb{Z}_2[v]-$ sabit devirli kodun dualinin yapısı da belirlenmiş olacaktır.

Öncelikle $\mathbb{Z}_2{}^\mu \times R^\eta$ da ki elemanlar ile $R_{\mu,\eta}$ da ki elemanlar arasındaki diklik ilişkisi verilsin.

$f(x) = a_0 + a_1 x + ... + a_{n-1}x^{n-1} \in \mathbb{Z}_2[x]/(x^n - 1)$ olsun.

$f^*(x) = x^{n-1} f\left(\frac{1}{x}\right) = a_{n-1} + a_{n-2}x + ... + a_0 x^{n-1}$ olmak üzere, $a_{n-1} \neq 0$ ise $f^*(x)$, $f(x)$ in reciprocal polinomudur.

$\mathbb{Z}_2{}^\mu \times R^\eta$ dan alınan $(s_0, s_1, ..., s_{\mu-1}, t_0, t_1, ..., t_{\eta-1})$ kod sözlerinin devir ötelemesi $T(s,t) = (s_{\mu-1}, s_0, ..., s_{\mu-2}, t_{\eta-1}, t_0, ..., t_{\eta-2})$ şeklindedir.

$m = ekok(\mu, \eta)$ olsun. $\{(s,t), T(s,t), T^2(s,t), ..., T^{m-1}(s,t)\}$ kümesi (s,t) nin tüm devir ötelemelerini üretir.

Tanım 3.3.1. $\mathbb{Z}_2{}^\mu \times R^\eta$ den alınan herhangi $A = (s_0, s_1, ..., s_{\mu-1}, t_0, t_1, ..., t_{\eta-1})$ ve $B = (w_0, w_1, ..., w_{\mu-1}, z_0, z_1, ..., z_{\eta-1})$ elemanlarının iç çarpımı:

$$\langle A, B \rangle = \left((1+v) \sum_{i=0}^{\mu-1} s_i w_i + \sum_{j=0}^{\eta-1} t_j z_j \right) \in \mathbb{Z}_2 + v\mathbb{Z}_2 \text{ dir.}$$

İç çarpım ile polinom çarpımı arasındaki ilişki $\mathbb{Z}_2{}^{\mu}R^{\eta}$ de ki devir ötelemesine dayanmaktadır.

$A=(s_0,s_1,s_2,s_3,s_4,t_0,t_1)$, $B=(w_0,w_1,w_2,w_3,w_4,z_0,z_1)\in\mathbb{Z}_2^5R^2$ olsun.

$$A.T(B)=(1+v)s_0w_4+(1+v)s_1w_0+(1+v)s_2w_1+(1+v)s_3w_2+(1+v)s_4w_3+t_0z_1+t_1z_0$$
$$=(1+v)\delta_0+\Delta_0$$

$$A.T^2(B)=(1+v)s_0w_3+(1+v)s_1w_4+(1+v)s_2w_0+(1+v)s_3w_1+(1+v)s_4w_2+t_0z_0+t_1z_1$$
$$=(1+v)\delta_1+\Delta_1$$

$$A.T^3(B)=(1+v)s_0w_2+(1+v)s_1w_3+(1+v)s_2w_4+(1+v)s_3w_0+(1+v)s_4w_1+t_0z_1+t_1z_0$$
$$=(1+v)\delta_2+\Delta_0$$

$$A.T^4(B)=(1+v)s_0w_1+(1+v)s_1w_2+(1+v)s_2w_3+(1+v)s_3w_4+(1+v)s_4w_0+t_0z_0+t_1z_1$$
$$=(1+v)\delta_3+\Delta_1$$

$$A.T^5(B)=(1+v)s_0w_0+(1+v)s_1w_1+(1+v)s_2w_2+(1+v)s_3w_3+(1+v)s_4w_4+t_0z_1+t_1z_0$$
$$=(1+v)\delta_4+\Delta_0$$

$$A.T^6(B)=(1+v)s_0w_4+(1+v)s_1w_0+(1+v)s_2w_1+(1+v)s_3w_2+(1+v)s_4w_3+t_0z_0+t_1z_1$$
$$=(1+v)\delta_0+\Delta_1$$

$$A.T^7(B)=(1+v)s_0w_3+(1+v)s_1w_4+(1+v)s_2w_0+(1+v)s_3w_1+(1+v)s_4w_2+t_0z_1+t_1z_0$$
$$=(1+v)\delta_1+\Delta_0$$

$$A.T^8(B)=(1+v)s_0w_2+(1+v)s_1w_3+(1+v)s_2w_4+(1+v)s_3w_0+(1+v)s_4w_1+t_0z_0+t_1z_1$$
$$=(1+v)\delta_2+\Delta_1$$

$$A.T^9(B)=(1+v)s_0w_1+(1+v)s_1w_2+(1+v)s_2w_3+(1+v)s_3w_4+(1+v)s_4w_0+t_0z_1+t_1z_0$$
$$=(1+v)\delta_3+\Delta_0$$

$$A.T^{10}(B)=(1+v)s_0w_0+(1+v)s_1w_1+(1+v)s_2w_2+(1+v)s_3w_3+(1+v)s_4w_4+t_0z_0+t_1z_1$$
$$=(1+v)\delta_4+\Delta_1$$

olarak bulunur.

$A(x)=(s_0+s_1x+s_2x^2+s_3x^3+s_4x^4,t_0+t_1x)$,

$B^*(x)=(w_4+w_3x+w_2x^2+w_1x^3+w_0x^4,z_1+z_0x)\in R_{\mu,\eta}$ olsun. $m=ekok(\mu,\eta)$ olmak üzere,

$$G(x)=\left((1+v)\delta_0+\Delta_0\right)+\left((1+v)\delta_1+\Delta_1\right)x+\left((1+v)\delta_2+\Delta_0\right)x^2$$
$$+\left((1+v)\delta_3+\Delta_1\right)x^3+\left((1+v)\delta_4+\Delta_0\right)x^4+\left((1+v)\delta_0+\Delta_1\right)x^5$$
$$+\left((1+v)\delta_1+\Delta_0\right)x^6+\left((1+v)\delta_2+\Delta_1\right)x^7+\left((1+v)\delta_3+\Delta_0\right)x^8+\left((1+v)\delta_4+\Delta_1\right)x^9$$
$$=\left((1+v)\delta_0+(1+v)\delta_1x+(1+v)\delta_2x^2+(1+v)\delta_3x^3+(1+v)\delta_4x^4\right)$$
$$+\left((1+v)\delta_0+(1+v)\delta_1x+(1+v)\delta_2x^2+(1+v)\delta_3x^3+(1+v)\delta_4x^4\right)x^5$$
$$+\left(\Delta_0+\Delta_1x\right)+\left(\Delta_0+\Delta_1x\right)x^2+\left(\Delta_0+\Delta_1x\right)x^4+\left(\Delta_0+\Delta_1x\right)x^6+\left(\Delta_0+\Delta_1x\right)x^8$$
$$=\left((1+v)\delta_0+(1+v)\delta_1x+(1+v)\delta_2x^2+(1+v)\delta_3x^3+(1+v)\delta_4x^4\right)\left(1+x^5\right)$$
$$+\left(\Delta_0+\Delta_1x\right)\left(1+x^2+x^4+x^6+x^8\right)$$
$$=\left((1+v)\delta_0+(1+v)\delta_1x+(1+v)\delta_2x^2+(1+v)\delta_3x^3+(1+v)\delta_4x^4\right)\left(\frac{x^{10}-1}{x^5-1}\right)$$
$$+\left(\Delta_0+\Delta_1x\right)\left(\frac{x^{10}-1}{x^2-1}\right)$$

$$G(x)=\left((1+v)s(x)w^*(x)\bmod(x^\mu-1)\right)\left(\frac{x^m-1}{x^\mu-1}\right)+\left(t(x)z^*(x)\bmod(x^\eta-1)\right)\left(\frac{x^m-1}{x^\eta-1}\right)$$

şeklindedir. Bu örnek herhangi μ, η için genelleştirilebilir.

$\mu\le\eta$ ve $A=\left(s_0,s_1,...,s_{\mu-1},t_0,t_1,...,t_{\eta-1}\right)$, $B=\left(w_0,w_1,...,w_{\mu-1},z_0,z_1,...,z_{\eta-1}\right)\in\mathbb{Z}_2^\mu R^\eta$ olsun.

$$A.T(B)=(1+v)s_0w_{\mu-1}+(1+v)s_1w_0+...+(1+v)s_{\mu-1}w_{\mu-2}+t_0z_{\eta-1}+t_1z_0+...+t_{\eta-1}z_{\eta-2}$$
$$=(1+v)\delta_0+\Delta_0.$$

$m=ekok(\mu,\eta)$ olmak üzere, her $i=1,2,...,m$ için genel olarak,

$$A.T^i(B)=(1+v)s_0w_{\mu-i}+(1+v)s_1w_{\mu-i+1}+...+(1+v)s_{\mu-1}w_{\mu-i-1}$$
$$+t_0z_{\eta-i}+t_1z_{\eta-i+1}+...+t_{\eta-1}z_{\eta-i-1}$$
$$=(1+v)\delta_{(i-1)}\bmod\mu+\Delta_{(i-1)}\bmod\eta$$

şeklindedir. Şimdi $G(x)$ polinomu oluşturulsun:

$$G(x)=\left((1+v)\delta_0+\Delta_0\right)+\left((1+v)\delta_1+\Delta_1\right)x+\ldots+\left((1+v)\delta_{(\mu-1)}+\Delta_{(\mu-1)\bmod\eta}\right)x^{\mu-1}$$
$$+\left((1+v)\delta_{\mu}+\Delta_{\mu\bmod\eta}\right)x^{\mu}+\ldots+\left((1+v)\delta_{(\eta-1)\bmod\mu}+\Delta_{(\eta-1)\bmod\eta}\right)x^{\mu-1}$$
$$+\left((1+v)\delta_{\eta\bmod\mu}+\Delta_{\eta\bmod\eta}\right)x^{\eta}+\ldots+\left((1+v)\delta_{(m-1)\bmod\mu}+\Delta_{(m-1)\bmod\eta}\right)x^{m-1}.$$

O halde,

$$G(x)=\left((1+v)s(x)w^*(x)\bmod(x^{\mu}-1)\right)\left(\frac{x^m-1}{x^{\mu}-1}\right)+\left(t(x)z^*(x)\bmod(x^{\eta}-1)\right)\left(\frac{x^m-1}{x^{\eta}-1}\right)$$

şeklindedir.

Teorem 3.3.1. $A=\left(s_0,s_1,\ldots,s_{\mu-1},t_0,t_1,\ldots,t_{\eta-1}\right)\in\mathbb{Z}_2{}^{\mu}R^{\eta}$ ve $B=\left(w_0,w_1,\ldots,w_{\mu-1},z_0,z_1,\ldots,z_{\eta-1}\right)\in\mathbb{Z}_2{}^{\mu}R^{\eta}$ olsun. A nın B ye ve B nin tüm devir ötelemelerine dik olması için gerekli ve yeter şart

$$G(x)=\left[(1+v)s(x)w^*(x)\bmod\left(x^{\mu}-1\right)\right]\left(\frac{x^m-1}{x^{\mu}-1}\right)$$
$$+\left[t(x)z^*(x)\bmod\left(x^{\eta}-1\right)\right]\left(\frac{x^m-1}{x^{\eta}-1}\right)=0\bmod\left(x^m-1\right)$$

olmasıdır.

Uyarı 3.3.1. Alınan herhangi bir $f(x)$ polinomu f şeklinde verilecektir.

Teorem 3.3.2. $f\mid\left(x^{\mu}-1\right)\pmod 2$, $a\mid g\mid\left(x^{\eta}-1\right)\pmod 2$, l ikili polinom ve $t_1=ebob\left(f,\frac{x^{\eta}-1}{g}l\right)$ olmak üzere, $der(f)=a_1$, $der(g)=a_2$, $der(a)=a_3$, $der(t_1)=a_4$ olsun. $C=\left\langle(f,0),\left(l,g+(1+v)a\right)\right\rangle$, $R_{\mu,\eta}$ da devirli kod olsun. C kodu $\left(\mu,\eta;\mu-a_4,\eta-a_2,a_2+a_4-a_1-a_3\right)$ tipindedir.

İspat: [28] de ki Teorem 4. 9. a benzer şekilde ispatlanır.

Teorem 3.3.3. $C, \mathbb{Z}_2\mathbb{Z}_2[v]-$ devirli kodu, $(\mu,\eta;\mu-a_4,\eta-a_2,a_2+a_4-a_1-a_3)$ tipinde ise $C^{\perp}$ dual kodu $\left(\mu,\eta;k_0',k_1',k_2'\right)$ tipindedir. Burada,

$k_0'=a_4,\ k_1'=a_1+a_3-a_4,\ k_2'=a_2+a_4-a_1-a_3$ tür.

İspat: $(\mu,\eta;k_0,k_1,k_2)$ tipindeki C, $\mathbb{Z}_2\mathbb{Z}_2[v]-$ lineer kodu için $C^{\perp}$ dual kodu $(\mu,\eta;\mu-k_0,\eta-k_1-k_2,k_2)$ tipindedir. Dolayısıyla ispat buradan sağlanmaktadır.

Önerme 3.3.1. $g=ab$ ve $f\mid\left(\frac{x^{\eta}-1}{a}l\right)$ olmak üzere, $C=\left\langle(f,0),\left(l,g+(1+v)a\right)\right\rangle$, $R_{\mu,\eta}$ da devirli kod olsun. $t_1=ebob\left(f,\frac{x^{\eta}-1}{g}l\right)$, $t=ebob(l,f)$, $f=t_1t_2$ olsun. O halde, $t\mid t_1$ ve $t_2\mid b$ dir.

İspat: $t_1=ebob\left(f,\frac{x^{\eta}-1}{g}l\right)$, $t=ebob(l,f)$ olduğundan $t\mid t_1$ dir. Buradan $t_1=tw$ dır. $t=b_1l+b_2f$, $f=t_1t_2$, $l=tt_4$, $\frac{x^{\eta}-1}{g}l=t_1w_1$, $t_1=b_3\frac{x^{\eta}-1}{g}l+b_4f$ olsun. $f\mid\left(\frac{x^{\eta}-1}{a}l\right)$ olduğundan $\left(\frac{x^{\eta}-1}{a}l\right)=fh$ yazılabilir. Buradan

$fh=\left(\frac{x^{\eta}-1}{a}l\right)=\left(\frac{x^{\eta}-1}{ab}l\right)b=\frac{x^{\eta}-1}{g}lb=t_1w_1b$ bulunur. $f=t_1t_2$ olduğundan $t_1t_2h=t_1w_1b$ dir. O halde $t_2h=w_1b$ dir. $t_1=ebob\left(f,\frac{x^{\eta}-1}{g}l\right)$ ve $f=t_1t_2$, $\frac{x^{\eta}-1}{g}l=t_1w_1$ olduğundan, $ebob(t_2,w_1)=1$ ve $t_2v_1+w_1v_2=1$ olarak bulunur. Eşitliğin her iki tarafı b ile çarpılırsa,

$b=bt_2v_1+bw_1v_2=bt_2v_1+t_2hv_2=t_2(bv_1+hv_2)=t_2t_3$ elde edilir. Yani $t_2\mid b$ dir.

Böylece ispat tamamlanır.

$f \mid x^{\mu}-1$ ve $f = t_1 t_2$ olduğundan $x^{\mu}-1 = fs_1 = t_1 t_2 s_1$ yazılabilir.

$$\frac{x^{\eta}-1}{a} t_1 = \frac{x^{\eta}-1}{a}\left(b_3 \frac{x^{\eta}-1}{g} l + b_4 f \right)$$

$$= b_3 \frac{x^{\eta}-1}{g} fh + b_4 \frac{x^{\eta}-1}{a} f$$

$$= f\left(b_3 \frac{x^{\eta}-1}{g} h + b_4 \frac{x^{\eta}-1}{a} \right) \text{ bulunur.}$$

$b_3 \frac{x^{\eta}-1}{g} h + b_4 \frac{x^{\eta}-1}{a} = \lambda_1$ olsun. Buradan,

$$\frac{x^{\eta}-1}{a} t_1 = f\lambda_1$$

$$\left(x^{\eta}-1\right) t_1 = fa\lambda_1 = t_1 t_2 a\lambda_1$$

$\left(x^{\eta}-1\right) = t_2 a\lambda_1$ bulunur.

O halde, λ_1, $x^{\eta}-1$ in çarpanıdır.

Şimdi $t = b_1 l + b_2 f$ nin her iki tarafı $\frac{x^{\eta}-1}{g}$ ile çarpılırsa,

$$\frac{x^{\eta}-1}{g} t = \frac{x^{\eta}-1}{g}\left(b_1 l + b_2 f\right)$$

$$= b_1 t_1 w_1 + b_2 \frac{x^{\eta}-1}{g} t_1 t_2$$

$$= t_1\left(b_1 w_1 + b_2 \frac{x^{\eta}-1}{g} t_2 \right) \text{ elde edilir.}$$

$b_1 w_1 + b_2 \frac{x^{\eta}-1}{g} t_2 = \lambda_2$ olsun. Buradan,

$$\frac{x^{\eta}-1}{g} t = t_1 \lambda_2$$

$$\left(x^{\eta}-1\right) t = t_1 g\lambda_2 = twg\lambda_2$$

$\left(x^{\eta}-1\right) = wg\lambda_2$ bulunur.

O halde, λ_2, $x^{\eta}-1$ in çarpanıdır.

Önerme 3.3.2. $g=ab$ ve $f\mid\left(\frac{x^{\eta}-1}{a}l\right)$ olmak üzere, $C=\langle(f,0),(l,g+(1+v)a)\rangle$ $R_{\mu,\eta}$ da devirli kod olsun. $t_1=ebob\left(f,\frac{x^{\eta}-1}{g}l\right)$, $t=ebob(l,f)$, $f=t_1t_2$ olsun.

O halde C kodu $D=\left\langle\left(\left(\frac{x^{\mu}-1}{t}\right)^{*},0\right),\left(\left(b_1(ws_1+t_2s_1)\right)^{*},\left(\lambda_1+(1+v)\lambda_2\right)^{*}\right)\right\rangle$ koduna diktir.

İspat: $g=ab$ ve $f\mid\left(\frac{x^{\eta}-1}{a}l\right)$ olmak üzere, $C=\langle(f,0),(l,g+(1+v)a)\rangle$ $\mathbb{Z}_2\mathbb{Z}_2[v]-$ devirli kod olsun. $t_1=ebob\left(f,\frac{x^{\eta}-1}{g}l\right)$, $t=ebob(l,f)$, $f=t_1t_2$ olsun.

$$\left(\frac{x^{\mu}-1}{t},0\right)*(f,0)=\left((1+v)\frac{x^{\mu}-1}{t}f \bmod\left(x^{\mu}-1\right)\right)\frac{x^{m}-1}{x^{\mu}-1}$$

$$=0\bmod\left(x^{m}-1\right).$$

$$\left(\frac{x^{\mu}-1}{t},0\right)*\left(l,g+(1+v)a\right)=\left((1+v)\frac{x^{\mu}-1}{t}l \bmod\left(x^{\mu}-1\right)\right)\frac{x^{m}-1}{x^{\mu}-1}$$

$$=\left((1+v)\frac{x^{\mu}-1}{t}tt_4 \bmod\left(x^{\mu}-1\right)\right)\frac{x^{m}-1}{x^{\mu}-1}$$

$$=0\bmod\left(x^{m}-1\right).$$

$$\left(b_1(ws_1+t_2s_1),\lambda_1+(1+v)\lambda_2\right)*(f,0)=(1+v)\left(b_1(ws_1+t_2s_1)f \bmod\left(x^{\mu}-1\right)\right)\frac{x^{m}-1}{x^{\mu}-1}$$

$$=\left((1+v)\left(b_1ws_1f+b_1t_2s_1f\right)\bmod\left(x^{\mu}-1\right)\right)\frac{x^{m}-1}{x^{\mu}-1}$$

$$=0\bmod\left(x^{m}-1\right).$$

$$\begin{aligned}\left(b_1\left(ws_1+t_2s_1\right),\lambda_1+\left(1+v\right)\lambda_2\right)*\left(l,g+\left(1+v\right)a\right)&=\left(\left(1+v\right)\left(lb_1ws_1+b_1lt_2s_1\right)\bmod\left(x^{\mu}-1\right)\right)\left(\frac{x^m-1}{x^{\mu}-1}\right)\\&+\left(\left(\lambda_1+\left(1+v\right)\lambda_2\right)\left(g+\left(1+v\right)a\right)\right)\bmod\left(x^{\eta}-1\right)\left(\frac{x^m-1}{x^{\eta}-1}\right)\\&=\left(\left(1+v\right)\left(\left(t+b_2f\right)ws_1+\left(t+b_2f\right)t_2s_1\right)\right)\frac{x^m-1}{x^{\mu}-1}\\&+\left(\left(\lambda_1+\left(1+v\right)\lambda_2\right)\left(g+\left(1+v\right)a\right)\right)\left(\frac{x^m-1}{x^{\eta}-1}\right)\\&=\left(\left(1+v\right)tws_1\right)\left(\frac{x^m-1}{x^{\mu}-1}\right)+\left(\left(1+v\right)tt_2s_1\right)\left(\frac{x^m-1}{x^{\mu}-1}\right)\\&+\left(\lambda_1g+\left(1+v\right)\lambda_1a+\left(1+v\right)\lambda_2g\right)\left(\frac{x^m-1}{x^{\eta}-1}\right).\end{aligned}$$

Şimdi son eşitliğin 0 a eşit olduğu gösterilsin.

$$\lambda_1g=\left(b_3\frac{x^{\eta}-1}{g}h+b_4\frac{x^{\eta}-1}{a}g\right)=0\bmod\left(x^m-1\right).$$

$$\begin{aligned}\left(1+v\right)\lambda_1a\left(\frac{x^m-1}{x^{\eta}-1}\right)&=\left(1+v\right)\left(\frac{\left(x^{\eta}-1\right)t_1}{fa}\right)a\left(\frac{x^m-1}{x^{\eta}-1}\right)\\&=\left(1+v\right)\frac{\left(x^{\eta}-1\right)t_1}{f}\left(\frac{x^m-1}{x^{\eta}-1}\right)\\&=\left(1+v\right)\frac{\left(x^{\eta}-1\right)t_1s_1}{x^{\mu}-1}\left(\frac{x^m-1}{x^{\eta}-1}\right)\\&=\left(1+v\right)t_1s_1\left(\frac{x^m-1}{x^{\mu}-1}\right)\\&=\left(1+v\right)tws_1\left(\frac{x^m-1}{x^{\mu}-1}\right).\end{aligned}$$

$$\begin{aligned}\left(1+v\right)\lambda_2g\left(\frac{x^m-1}{x^{\eta}-1}\right)&=\left(\left(1+v\right)\frac{x^{\eta}-1}{g}\frac{t}{t_1}\right)g\left(\frac{x^m-1}{x^{\eta}-1}\right)\\&=\left(\left(1+v\right)\frac{x^{\eta}-1}{g}\frac{t_2ts_1}{t_2t_1s_1}\right)g\left(\frac{x^m-1}{x^{\eta}-1}\right)\\&=\left(1+v\right)t_2ts_1\left(\frac{x^m-1}{x^{\mu}-1}\right).\end{aligned}$$

Böylece, $\left(b_1\left(ws_1+t_2s_1\right),\lambda_1+\left(1+v\right)\lambda_2\right)*\left(l,g+\left(1+v\right)a\right)=0\bmod\left(x^m-1\right)$ bulunur. Dolayısıyla C kodu D koduna diktir.

Önerme 3.3.3. $K=b_1\left(ws_1+t_2s_1\right)$ olmak üzere, $C=\left\langle\left(f,0\right),\left(l,g+\left(1+v\right)a\right)\right\rangle$, $R_{\mu,\eta}$ da devirli kod ve $D=\left\langle\left(\left(\frac{x^\mu-1}{t}\right),0\right),\left(K,\left(\lambda_1+\left(1+v\right)\lambda_2\right)\right)\right\rangle$ olsun.

i. $\frac{x^\mu-1}{t}\mid x^\mu-1$ dir. Ayrıca $\lambda_2\mid\lambda_1\mid x^\eta-1$ dir.

ii. $\frac{x^\mu-1}{t}\mid\left(\left(\frac{x^\eta-1}{\lambda_2}\right)K\right)$ dir.

iii. D kodunun $2^{dert}4^{(\eta-der\lambda_1)}2^{(der\lambda_1-der\lambda_2)}$ tane kod sözü vardır.

İspat: i. $\frac{x^\mu-1}{t}$ nin $\left(x^\mu-1\right)$ in çarpanı olduğu açıktır. $\frac{x^\eta-1}{a}t_1=f\lambda_1$ de $f=t_1t_2$ yazılırsa $\left(x^\eta-1\right)=t_2a\lambda_1$ bulunur. Ayrıca $\left(x^\eta-1\right)=wg\lambda_2$ olduğundan λ_1 ve λ_2, $\left(x^\eta-1\right)$ in çarpanlarıdır.

$\lambda_1=\frac{\left(x^\eta-1\right)}{t_2a}$ ve $\lambda_2=\frac{\left(x^\eta-1\right)}{wg}=\frac{\left(x^\eta-1\right)}{wab}=\frac{\left(x^\eta-1\right)}{wat_2t_3}$ yazılabilir. Buradan,

$\lambda_1=\frac{\left(x^\eta-1\right)}{t_2a}=\frac{\left(x^\eta-1\right)}{wt_2at_3}wt_3=\lambda_2wt_3$ bulunur. Yani $\lambda_2\mid\lambda_1$ dir.

ii. $\left(\left(\frac{x^\eta-1}{\lambda_2}\right)K\right)=\left(\frac{x^\eta-1}{\lambda_2}\right)b_1\left(ws_1+t_2s_1\right)$ dir. $\frac{x^\mu-1}{t}=\frac{x^\mu-1}{t_1}w$ ve $\frac{\left(x^\eta-1\right)}{\lambda_2}=wg$ yazılabilir. Böylece,

$$\left(\left(\frac{x^\eta-1}{\lambda_2}\right)K\right)=\left(\frac{x^\eta-1}{\lambda_2}\right)b_1\left(ws_1+t_2s_1\right)$$

$$=wgb_1\left(ws_1+t_2s_1\right)$$

$$\left(\left(\frac{x^{\eta}-1}{\lambda_2}\right)K\right) = wb_1\left(wab\frac{x^{\mu}-1}{f} + gt_2\frac{x^{\mu}-1}{f}\right)$$

$$= wb_1\left(wat_2t_3\frac{x^{\mu}-1}{t_1t_2} + gt_2\frac{x^{\mu}-1}{t_1t_2}\right)$$

$$= wb_1\left(wat_3\frac{x^{\mu}-1}{t_1} + g\frac{x^{\mu}-1}{t_1}\right)$$

$$= w\frac{x^{\mu}-1}{t_1}\left(b_1wat_3 + g\right) \text{ bulunur.}$$

Yani $\frac{x^{\mu}-1}{t} \mid \left(\left(\frac{x^{\eta}-1}{\lambda_2}\right)K\right)$ dir.

iii. D kodunun üreteçleri, Teorem 3.2.2. de ki C kodunun üreteçleri ile aynı özelliklere sahip olduğundan, sonuç Teorem 3.2.2. den sağlanır.

Önerme 3.3.4. $C = \langle (f,0), (l, g+(1+v)a) \rangle$, $R_{\mu,\eta}$ da devirli kod ve

$D = \left\langle \left(\left(\frac{x^{\mu}-1}{t}\right),0\right), \left(K, \left(\lambda_1 + (1+v)\lambda_2\right)\right)\right\rangle$ olsun. $k = \mu + 2\eta$ olmak üzere,

$|C||D| = 2^k$ dır.

İspat: $|C| = 2^{\mu - derf}4^{\eta - derg}2^{derg - dera}$, $|D| = 2^{dert}4^{(\eta - der\lambda_1)}2^{(der\lambda_1 - der\lambda_2)}$ ve $\frac{x^{\eta}-1}{af}t_1 = \lambda_1$,

$\frac{x^{\eta}-1}{gt_1}t = \lambda_2$ olduğundan,

$$\eta - der\lambda_1 = \eta - (\eta + dert_1 - dera - derf)$$

$$= dera - dert_1 + derf \text{ dir.}$$

$$der\lambda_1 - der\lambda_2 = (\eta + dert_1 - dera - derf) - (\eta + dert - derg - dert_1)$$

$$= 2dert_1 - dera - derf - dert + derg \text{ dir.}$$

$|C||D| = 2^p$ olsun. Dolayısıyla,

$$p = \mu - derf + 2\eta - 2derg + derg - dera + dert + 2\eta - 2der\lambda_1 + der\lambda_1 - der\lambda_2$$

$= \mu - derf + 2\eta - 2derg + derg - dera + dert + 2dera - 2dert_1 + 2derf$

$+2dert_1 - dera - derf - dert + derg$

$= \mu + 2\eta$ bulunur.

Buradan $|C||D| = 2^k$ dir.

Bu bilgiler doğrultusunda aşağıdaki teorem verilebilir.

Teorem 3.3.4. $C = \langle (f,0), (l, g + (1+v)a) \rangle$, $\mathbb{Z}_2\mathbb{Z}_2[v]$ – devirli kod olsun.

$k_0' = a_4$, $k_1' = a_1 + a_3 - a_4$, $k_2' = a_2 + a_4 - a_1 - a_3$ olmak üzere,

$D = \left\langle \left(\left(\frac{x^\mu - 1}{t} \right), 0 \right), \left(\left(b_1 (ws_1 + t_2 s_1) \right), \left(\lambda_1 + (1+v)\lambda_2 \right) \right) \right\rangle$ kodu $\left(\mu, \eta; k_0', k_1', k_2' \right)$

tipindedir. Ayrıca $C^\perp = \left\langle \left(\left(\frac{x^\mu - 1}{t} \right)^*, 0 \right), \left(\left(b_1 (ws_1 + t_2 s_1) \right)^*, \left(\lambda_1 + (1+v)\lambda_2 \right)^* \right) \right\rangle$ dır.

Sonuç 3.3.1. $R_{\mu,\eta}$ da ki devirli kodlar ve $S_{\mu,\eta}$ da ki sabit devirli kodlar arasındaki birebir ilişki π dönüşümü ile verilmişti. Dolayısıyla C kodu sabit devirli kod olduğunda, $C^\perp$ dual kodu,

$C^\perp = \left\langle \left(\left(\frac{x^\mu - 1}{t} \right)^*, 0 \right), \left(\left(b_1 (ws_1 + t_2 s_1) \right)^*, \left(\lambda_1 + (1+v)\lambda_2 \right)^* \right) \right\rangle$ şeklindedir.

3.4. $\mathbb{Z}_2\mathbb{Z}_2[v]$ – Sabit Devirli Kodların Gray Dönüşümü

$\forall s = (s_0, s_1, ..., s_{\mu-1}) \in \mathbb{Z}_2{}^\mu$ ve $\forall t = (t_0, t_1, ..., t_{\eta-1}) \in R^\eta$ $(t_i = a_i + vb_i ; 0 \le i \le \eta - 1)$

için, $k = \mu + 2\eta$ olmak üzere,

$$\sigma : \mathbb{Z}_2{}^\mu \times (\mathbb{Z}_2 + v\mathbb{Z}_2)^\eta \to \mathbb{Z}_2{}^k$$
$$(s,t) \to (s_0, ..., s_{\mu-1}, a_0, ..., a_{\eta-1}, b_0, ..., b_{\eta-1})$$

olacak şekilde daha önce tanımlanan σ gray dönüşümü doğrultusunda aşağıda verilen teorem sağlanır.

Teorem 3.4.1 C, $S_{\mu,\eta}$ da sabit devirli kod olsun.

i. Eğer $\mu = 2\eta$ ise $\sigma(C)$, $2-$ indeksli $QC-$ koddur.

ii. Eğer $\mu \neq 2\eta$ ise $\sigma(C)$, $2-$ indeksli genelleştirilmiş $QC-$ koddur.

İspat: C, $S_{\mu,\eta}$ da sabit devirli kod ve

$c = (s_0, s_1, ..., s_{\mu-1}, t_0, t_1, ..., t_{\eta-1}) = (s_0, s_1, ..., s_{\mu-1}, a_0 + vb_0, a_1 + vb_1, ..., a_{\eta-1} + vb_{\eta-1}) \in C$ olsun. $\bar{\partial}$, parçalı devirli (quasicyclic) öteleme operatörü ve $\Im$, sabit devirli öteleme operatörü olsun. C, $S_{\mu,\eta}$ da sabit devirli kod olduğundan,

$$\Im(c) = (s_{\mu-1}, s_0, ..., s_{\mu-2}, v(a_{\eta-1} + b_{\eta-1}), a_0 + vb_0 + ... + a_{\eta-1} + vb_{\eta-1})$$
$$= (s_{\mu-1}, s_0, ..., s_{\mu-2}, b_{\eta-1} + va_{\eta-1}, a_0 + vb_0, ..., a_{\eta-2} + vb_{\eta-2}) \text{ dir.}$$

Böylece σ uygulanarak,

$\sigma(\Im(c)) = (s_{\mu-1}, s_0, ..., s_{\mu-2}, b_{\eta-1}, a_0, ..., a_{\eta-2}, a_{\eta-1}, b_0, ..., b_{\eta-2})$ elde edilir.

Diğer taraftan, $\sigma(c) = (s_0, s_1, ..., s_{\mu-1}, a_0, a_1, ..., a_{\eta-1}, b_0, b_1, ..., b_{\eta-1})$ dir. Buradan, $\bar{\partial}\sigma(c) = (s_{\mu-1}, s_0, ..., s_{\mu-2}, b_{\eta-1}, a_0, ..., a_{\eta-2}, a_{\eta-1}, b_0, ..., b_{\eta-2})$ bulunur.

Böylece $\sigma(\Im(c)) = \bar{\partial}\sigma(c)$ dir. Eğer $\mu = 2\eta$ ise $\sigma(C)$, $2-$indeksli $QC-$koddur. Eğer $\mu \neq 2\eta$ ise $\sigma(C)$, $2-$indeksli genelleştirilmiş $QC-$koddur.

BÖLÜM 4. $\mathbb{Z}_4\mathbb{Z}_4[v]-$ LİNEER SKEW SABİT DEVİRLİ KODLAR

Son yıllarda değişmeli olmayan halkalar üzerinde skew devirli kodlar ve skew sabit devirli kodlar çalışılmıştır. Skew devirli kodlar için birçok çalışma bulunmaktadır $[29,30,31,32]$. Skew quasi devirli kodların çalışması da M. Özen ve ark. $[33]$ tarafından yapılmıştır. Sonlu zincir halkaları üzerindeki skew sabit devirli kodlar Jitman ve ark. $[34]$ tarafından çalışılmıştır. $u^2=0$ olmak üzere $\mathbb{Z}_4+u\mathbb{Z}_4$ de ki skew sabit devirli kodlar $[35]$ de çalışılmıştır. Ayrıca $u^2=0$ olmak üzere $\mathbb{Z}_q\left(\mathbb{Z}_q+u\mathbb{Z}_q\right)-$ lineer skew sabit devirli kodların çalışılması $[36]$ da yapılmıştır.

Tezin bu bölümünde $v^2=1$, $R_1=\mathbb{Z}_4+v\mathbb{Z}_4$ ve θ, R_1 de otomorfizma olmak üzere, R_1 ve $\mathbb{Z}_4R_1$ de skew sabit devirli kodlar çalışılmıştır. Bu kodların üreteç polinomları verilmiştir. Daha sonra $\varpi=\varpi_i+v\varpi_j$, $\mathbb{Z}_4+v\mathbb{Z}_4$ halkasının birimsel elemanlarını ifade etmek üzere C_η, R_1 de η uzunluğunda skew $(\varpi)-$ sabit devirli kod olduğunda tanımlanan iki gray fonksiyonu ile görüntüsü; devirli kod, 2 indeksli parçalı devirli kod ve 2 indeksli skew quasi twisted kod olan örnekler verilmiştir. Bu kısımda ayrıca R_1 de θ_1 otomorfizması verilerek tanımlanan gray fonksiyonu ile görüntüsü; devirli kod, 2 indeksli parçalı devirli kod ve 2 indeksli skew quasi twisted kod olan örnekler verilmiştir. C, $\mathbb{Z}_4[x]/\langle x^\mu-\varepsilon(\varpi)\rangle\times R_1[x;\theta]/\langle x^\eta-(\varpi)\rangle$ de skew sabit devirli kod olduğunda θ otomorfizması ve tanımlanan iki gray fonksiyonu ile görüntüsü; 2 ve 3 indeksli parçalı devirli kod ve 3 indeksli skew quasi twisted kod olan örnekler verilmiştir. Son olarak, $\mathbb{Z}_4R_1$ de double skew sabit devirli kodlar verilmiştir.

4.1. $\mathbb{Z}_4\mathbb{Z}_4[v]-$ Lineer Skew Sabit Devirli Kodların Yapısı

$v^2=1$ olmak üzere, $R_1=\mathbb{Z}_4[v]=\mathbb{Z}_4+v\mathbb{Z}_4$ halkasını temsil etsin. $\mathbb{Z}_4+v\mathbb{Z}_4=\{0,1,2,3,v,2v,3v,1+v,1+2v,1+3v,2+v,2+2v,2+3v,3+v,3+2v,3+3v\}$ halkası 16 elemanlıdır. $\varpi=\varpi_i+v\varpi_j$, $\mathbb{Z}_4+v\mathbb{Z}_4$ 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 $\langle 2v,1+v\rangle$ dir. Böylece R_1 tek maksimal ideale sahip olduğundan lokal halkadır $[37]$.

$\mathbb{Z}_4\mathbb{Z}_4[v]=\{(p,q)\,|\,p\in\mathbb{Z}_4, q\in R_1\}$ şeklinde tanımlanan $\mathbb{Z}_4\mathbb{Z}_4[v]$ halkası bilinen çarpma işlemi altında kapalı olmadığından R_1- modül değildir. Bu nedenle aşağıdaki tanımda verilen ε dönüşümü kullanılarak yeni bir çarpma işlemi tanımlanacaktır. Böylece bu halkanın R_1- modül olması sağlanacaktır.

Tanım 4.1.1. $a,b\in\mathbb{Z}_4, a+vb\in R_1$ olmak üzere,

$\varepsilon: R_1\to\mathbb{Z}_4$

$(a+vb)\to a+b$

olacak şekilde tanımlansın.

Tanım 4.1.2. Herhangi bir $\overline{r}\in R_1$ ve $(p,q)\in\mathbb{Z}_4R_1$ için $\overline{r}*(p,q)=(\varepsilon(\overline{r})p,\overline{r}q)$ olarak tanımlansın. Bu çarpma $\mathbb{Z}_4^{\mu}R_1^{\eta}$ halkasına genelleştirilerek herhangi bir $\overline{r}\in R_1$ ve $w=(p_0,p_1,...,p_{\mu-1},q_0,q_1,...,q_{\eta-1})\in\mathbb{Z}_4{}^{\mu}R_1^{\eta}$ için

$\overline{r}w=(\varepsilon(\overline{r})p_0,\varepsilon(\overline{r})p_1,...,\varepsilon(\overline{r})p_{\mu-1},\overline{r}q_0,\overline{r}q_1,...,\overline{r}q_{\eta-1})$ şeklindedir.

Önerme 4.1.1. $\mathbb{Z}_4{}^{\mu}R_1^{\eta}$ halkası yukarıda tanımlanan çarpma işlemi ile bir R_1- modüldür.

İspat: $\forall r, \bar{r} \in R$ ve

$\forall w = \left(p_0, p_1, ..., p_{\mu-1}, q_0, q_1, ..., q_{\eta-1}\right), \bar{w} = \left(\bar{p}_0, \bar{p}_1, ..., \bar{p}_{\mu-1}, \bar{q}_0, \bar{q}_1, ..., \bar{q}_{\eta-1}\right) \in \mathbb{Z}_4{}^{\mu} \times R_1^{\eta}$ için,

$$
\begin{aligned}
i.\ r(w+\bar{w}) &= r\left(p_0+\bar{p}_0, ..., p_{\mu-1}+\bar{p}_{\mu-1}, q_0+\bar{q}_0, ..., q_{\eta-1}+\bar{q}_{\eta-1}\right) \\
&= \left(\varepsilon(r)(p_0+\bar{p}_0), ..., \varepsilon(r)(p_{\mu-1}+\bar{p}_{\mu-1}), r(q_0+\bar{q}_0), ..., r(q_{\eta-1}+\bar{q}_{\eta-1})\right) \\
&= \left(\varepsilon(r)p_0, ..., \varepsilon(r)p_{\mu-1}, rq_0, ..., rq_{\eta-1}\right) + \left(\varepsilon(r)\bar{p}_0, ..., \varepsilon(r)\bar{p}_{\eta-1}, r\bar{q}_0, ..., r\bar{q}_{\eta-1}\right) \\
&= rw + r\bar{w}
\end{aligned}
$$

$$
\begin{aligned}
ii.\ (r+\bar{r})w &= \left(\varepsilon(r+\bar{r})p_0, ..., \varepsilon(r+\bar{r})p_{\mu-1}, (r+\bar{r})q_0, ..., (r+\bar{r})q_{\eta-1}\right) \\
&= \left((\varepsilon(r)+\varepsilon(\bar{r}))p_0, ..., (\varepsilon(r)+\varepsilon(\bar{r}))p_{\mu-1}, rq_0+\bar{r}q_0, ..., rt_{\mu-1}+\bar{r}q_{\mu-1}\right) \\
&= \left(\varepsilon(r)p_0, ..., \varepsilon(r)p_{\mu-1}, rq_0, ..., rq_{\eta-1}\right) + \left(\varepsilon(\bar{r})p_0, ..., \varepsilon(\bar{r})p_{\mu-1}, \bar{r}q_0, ..., \bar{r}q_{\eta-1}\right) \\
&= rw + \bar{r}w
\end{aligned}
$$

$$
\begin{aligned}
iii.\ r(\bar{r}w) &= r\left(\varepsilon(\bar{r})p_0, ..., \varepsilon(\bar{r})p_{\mu-1}, \bar{r}q_0, ..., \bar{r}q_{\eta-1}\right) \\
&= \left(\varepsilon(r)\varepsilon(\bar{r})p_0, ..., \varepsilon(r)\varepsilon(\bar{r})p_{\mu-1}, r\bar{r}q_0, ..., r\bar{r}q_{\eta-1}\right) \\
&= \left(\varepsilon(r\bar{r})p_0, ..., \varepsilon(r\bar{r})p_{\mu-1}, r\bar{r}q_0, ..., r\bar{r}q_{\eta-1}\right) \\
&= (r\bar{r})w
\end{aligned}
$$

iv. Tanım 4.1.1. den $\varepsilon(1) = 1$ dir. $\forall w = \left(p_0, p_1, ..., p_{\mu-1}, q_0, q_1, ..., q_{\eta-1}\right) \in \mathbb{Z}_4{}^{\mu} R_1^{\eta}$ için,

$$
\begin{aligned}
1_{R_1} w &= 1_{R_1}\left(p_0, ..., p_{\mu-1}, q_0, ..., q_{\eta-1}\right) \\
&= \left(\varepsilon(1_{R_1})p_0, ..., \varepsilon(1_{R_1})p_{\mu-1}, q_0, ..., q_{\eta-1}\right) \\
&= \left(p_0, ..., p_{\mu-1}, q_0, ..., q_{\eta-1}\right) \\
&= w
\end{aligned}
$$

elde edilir. Böylece $\mathbb{Z}_4{}^{\mu} R_1^{\eta}$ halkası yukarıda tanımlanan çarpma işlemi ile bir $R_1 -$modüldür.

Tanım 4.1.3. $\mathbb{Z}_4{}^{\mu} R_1^{\eta}$ nın boş olmayan bir C alt kümesi, $\mathbb{Z}_4{}^{\mu} R_1^{\eta}$ nın $R_1 -$alt modülü ise C ye $\mathbb{Z}_4 R_1 -$ lineer kod denir.

Önerme 4.1.2. $\mathbb{Z}_4$, R_1 in alt halkası olmak üzere, $R_1 = \mathbb{Z}_4 + v\mathbb{Z}_4$ olsun. ϖ nin R_1 de birimsel eleman olması için gerek ve yeter şart $\varepsilon(\varpi)$ nin $\mathbb{Z}_4$ de birimsel eleman olmasıdır.

İspat: $\varpi_1, \varpi_2 \in \mathbb{Z}_4$ ve $\varpi = \varpi_1 + v\varpi_2$ olmak üzere ϖ, R_1 de birimsel eleman olsun. Buradan $\varpi.z = z.\varpi = 1$ dir. $\varepsilon(\varpi.z) = \varepsilon(z.\varpi) = \varepsilon(1)$ dir. ε halka homomorfizması ve $\varepsilon(1) = 1$ olduğundan $\varepsilon(\varpi).\varepsilon(z) = \varepsilon(z).\varepsilon(\varpi) = 1$ olarak bulunur. Böylece $\varepsilon(\varpi)$, $\mathbb{Z}_4$ de birimsel elemandır.

Tersine, $\varepsilon(\varpi) = \varpi_1 + \varpi_2$, $\mathbb{Z}_4$ de birimsel eleman olsun. Şimdi $\varpi = \varpi_1 + v\varpi_2$ nin R_1 de birimsel eleman olduğu gösterilmelidir. Yani, $\varpi.\varpi^{-1} = 1$ olduğu gösterilmelidir. Buradan, $\varpi.\varpi^{-1} = (\varpi_1 + v\varpi_2)(\varpi_1 + v\varpi_2)^{-1}$

$= (\varpi_1 + v\varpi_2)(\varpi_1^{-1} + v\varpi_3)$

$= \varpi_1\varpi_1^{-1} + \varpi_2\varpi_3 + v(\varpi_1\varpi_3 + \varpi_2\varpi_1^{-1})...(*)$ olarak bulunur.

$\varepsilon(\varpi) = \varpi_1 + \varpi_2$, $\mathbb{Z}_4$ de birimsel eleman olduğundan $(\varpi_1 + \varpi_2)(\varpi_1 + \varpi_2)^{-1} = 1$ dir. Yani, $(\varpi_1 + \varpi_2)(\varpi_1^{-1} + \varpi_3) = \varpi_1\varpi_1^{-1} + \varpi_1\varpi_3 + \varpi_2\varpi_1^{-1} + \varpi_2\varpi_3 = 1$ dir.

$\varpi_1\varpi_1^{-1} + \varpi_2\varpi_3 = 1 - \varpi_1\varpi_3 - \varpi_2\varpi_1^{-1}$ eşitliği $(*)$ da yerine yazılır ve düzenlenirse,

$\varpi.\varpi^{-1} = 1 + (v-1)(\varpi_1\varpi_3 + \varpi_2\varpi_1^{-1})$ elde edilir. $\varpi_3 = \dfrac{-\varpi_2\varpi_1^{-1}}{\varpi_1} = -\varpi_2(\varpi_1^{-1})^2$ olmak üzere $\varpi.\varpi^1 = 1$ dir. Böylece $\varpi = \varpi_1 + v\varpi_2$, R_1 de birimsel elemandır.

4.2. $R_1[x;\theta]$ Skew Polinom Halkası

θ otomorfizması aşağıdaki gibi tanımlansın.

$\theta : \mathbb{Z}_4 + v\mathbb{Z}_4 \to \mathbb{Z}_4 + v\mathbb{Z}_4$

$a + vb \to a + (2 + 3v)b$

θ otomorfizması $\mathbb{Z}_4$ ün her elemanını sabit bırakır. θ nın sabit bıraktığı elemanların oluşturduğu küme $Z' = \{0, 1, 2, 3, 2v, 1 + 2v, 2 + 2v, 3 + 2v\}$ dir. θ otomorfizmasının mertebesi 2 dir.

Tanım 4.2.1. $R_1[x;\theta]$, R_1 üzerindeki polinomların kümesidir. $R_1[x;\theta]$ değişmeli olmayan halkasına, polinomların toplamı ve $(ax^i)(bx^j) = a\theta^i(b)x^{i+j}$ ile tanımlanan çarpma işlemine göre skew polinom halkası denir.

Tanım 4.2.2. $f(x) = q(x)g(x)$ olacak şekilde $q(x) \in R_1[x;\theta]$ varsa $g(x) \in R_1[x;\theta]$ ya $f(x)$ in sağ böleni denir. Bu durumda $f(x)$ e $g(x)$ in sol çarpanı denir. Benzer şekilde $f(x)$ in sol böleni tanımlanabilir.

Önerme 4.2.1. [6] $f(x), g(x) \in R_1[x;\theta]$ olsun öyle ki $g(x)$ in baş katsayısı birimdir. O zaman $r(x) = 0$ *ya da* $der(r(x)) < der(g(x))$ olmak üzere $q(x), r(x) \in R_1[x;\theta]$ vardır öyle ki $f(x) = q(x)g(x) + r(x)$ dir.

Tanım 4.2.3. $\forall r(x) \in R_1[x;\theta]$ için, $f(x)r(x) = r(x)f(x)$ ise $f(x) \in R_1[x;\theta]$ polinomuna merkez polinomu denir.

Teorem 4.2.1. θ otomorfizmasının mertebesi 2 olmak üzere, $R_1[x;\theta]$ nın $Z(R_1[x;\theta])$ merkezi $Z'[x^2]$ kümesidir.

İspat: θ, $\mathbb{Z}_4$ ün her elemanını serbest bırakmalıdır. θ nın mertebesi 2 olduğundan herhangi $a \in R_1$ için, $x^{2i}a = (\theta^2)^i(a)x^{2i} = ax^{2i}$ dir. O halde x^{2i}, $R_1[x;\theta]$ nın $Z(R_1[x;\theta])$ merkezindedir. Yani, $\varsigma_i \in R_1$ olmak üzere, $f(x) = \varsigma_0 + \varsigma_1 x^2 + \varsigma_2 x^4 + ... + \varsigma_k x^{2k}$ merkezindedir.

Tersine, $i = 0,1,...,l$ için $\varsigma_i \in R_1$ olmak üzere, $f(x) = \varsigma_0 + \varsigma_1 x + \varsigma_2 x^2 + ... + \varsigma_l x^l$, $R_1[x;\theta]$ nın merkezinde olsun. Böylece herhangi $a \in R_1$ için $af(x) = f(x)a$ dır.

Dolayısıyla,

$$f(x)a = af(x)$$

$$\left(\varsigma_0+\varsigma_1x+\varsigma_2x^2+...+\varsigma_lx^l\right)a = a\left(\varsigma_0+\varsigma_1x+\varsigma_2x^2+...+\varsigma_lx^l\right)$$

$$a\varsigma_0+\varsigma_1\theta(a)x+\varsigma_2\theta^2(a)x^2+...+\varsigma_l\theta^l(a)x^l = a\varsigma_0+a\varsigma_1x+a\varsigma_2x^2+...+a\varsigma_lx^l$$

dir. Buradan, her i için $\varsigma_i\theta^i(a)=\varsigma_i a$ bulunur. Her $a\in R_1$ için $\theta^i(a)=a$ olduğundan $2\,|\,i$ dir. Yani, $f(x)=\varsigma_0+\varsigma_1x^2+\varsigma_2x^4+...+\varsigma_kx^{2k}$ dır. Böylece merkezin herhangi elemanı $Z'[x^2]$ dedir.

Sonuç 4.2.1. $f(x)=x^\eta-1$ olsun. $f(x)\in Z\left(R_1[x;\theta]\right)$ ancak ve ancak $2\,|\,\eta$ dır. Ayrıca, $x^\eta-(\varpi)\in Z\left(R_1[x;\theta]\right)$ ancak ve ancak $2\,|\,\eta$ dır ve θ, (ϖ) i sabit bırakır.

4.3. R_1 Üzerindeki Skew $(\varpi)-$Sabit Devirli Kodlar

Tanım 4.3.1. R_1^η nın C_η alt kümesi,

i. C_η, R_1^η nın R_1-alt modülüdür.

ii. $(c_0,c_1,...,c_{\eta-1})\in C_\eta$ iken $\left((\varpi)\theta(c_{\eta-1}),\theta(c_0),...,\theta(c_{\eta-2})\right)\in C_\eta$ dır.

şartlarını sağlıyorsa C_η ya η uzunluğunda skew $(\varpi)-$sabit devirli kod denir. $(c_0,c_1,...,c_{\eta-1})\in C_\eta$ kod sözü polinom cinsinden aşağıdaki gibi ifade edilebilir: $c_0+c_1x+...+c_{\eta-1}x^{\eta-1}\in R_1[x;\theta]/\left(x^\eta-(\varpi)\right)$.

Önerme 4.3.1. $2\,|\,\eta$ ve θ nın mertebesi 2 olmak üzere, C_η, R_1 de η uzunluğunda skew $(\varpi)-$sabit devirli kod olsun. O zaman $C_\eta^{\perp}$, R_1 de η uzunluğunda skew $(\varpi)^{-1}-$sabit devirli koddur.

İspat: $q=(q_0,q_1,...,q_{\eta-1})\in C_\eta$ ve $\overline{q}=(\overline{q}_0,\overline{q}_1,...,\overline{q}_{\eta-1})\in C_\eta^{\perp}$ olsun.

$\left((\varpi)\theta^{\eta-1}(q_1),(\varpi)\theta^{\eta-1}(q_2),...,(\varpi)\theta^{\eta-1}(q_{\eta-1}),\theta^{\eta-1}(q_0)\right)\in C_\eta$ olduğundan,

$$0=\left\langle\left((\varpi)\theta^{\eta-1}(q_1),(\varpi)\theta^{\eta-1}(q_2),...,(\varpi)\theta^{\eta-1}(q_{\eta-1}),\theta^{\eta-1}(q_0)\right),\overline{q}\right\rangle$$
$$=\left\langle\left((\varpi)\theta^{\eta-1}(q_1),...,(\varpi)\theta^{\eta-1}(q_{\eta-1}),\theta^{\eta-1}(q_0)\right),\left(\overline{q}_0,\overline{q}_1,...,\overline{q}_{\eta-1}\right)\right\rangle$$
$$=(\varpi)\left\langle\left(\theta^{\eta-1}(q_1),...,\theta^{\eta-1}(q_{\eta-1}),\theta^{\eta-1}\left((\varpi)^{-1}q_0\right)\right),\left(\overline{q}_0,\overline{q}_1,...,\overline{q}_{\eta-1}\right)\right\rangle$$
$$=(\varpi)\left(\theta^{\eta-1}\left((\varpi)^{-1}q_0\right)\overline{q}_{\eta-1}+\sum_{k=1}^{\eta-1}\theta^{\eta-1}(q_k)\overline{q}_{k-1}\right)$$

dir.

η, θ nın mertebesinin katıdır ve θ, $(\varpi)^{-1}$ i sabit bırakır.

$$0=\theta\left((\varpi)\left(\theta^{\eta-1}\left((\varpi)^{-1}q_0\right)\overline{q}_{\eta-1}+\sum_{k=1}^{\eta-1}\theta^{\eta-1}(q_k)\overline{q}_{k-1}\right)\right)$$
$$=(\varpi)\left(q_0\theta\left((\varpi)^{-1}\overline{q}_{\eta-1}\right)+\sum_{k=1}^{\eta-1}q_k\theta(\overline{q}_{k-1})\right)$$
$$=(\varpi)\left\langle\left(\theta\left((\varpi)^{-1}\overline{q}_{\eta-1}\right),\theta(\overline{q}_0),...,\theta(\overline{q}_{\eta-2})\right),\left(q_0,q_1,...,q_{\eta-1}\right)\right\rangle$$

dir.

Böylece, $\left(\theta\left((\varpi)^{-1}\overline{q}_{\eta-1}\right),\theta(\overline{q}_0),...,\theta(\overline{q}_{\eta-2})\right)\in C_\eta^{\perp}$ dir.

Teorem 4.3.1. C_η kodunun R_1 üzerinde η uzunluğunda skew $(\varpi)-$ sabit devirli kod olması için gerek ve yeter şart C_η kodunun $R_1[x;\theta]/\left\langle x^\eta-(\varpi)\right\rangle$ nin sol $R_1[x;\theta]-$ alt modülü olmasıdır.

İspat: $c(x)=c_0+c_1x+...+c_{\eta-1}x^{\eta-1}\in C_\eta$ olsun.

$xc(x)=(\varpi)\theta(c_{\eta-1})+\theta(c_0)x+...+\theta(c_{\eta-2})x^{\eta-1}$

$=\left((\varpi)\theta(c_{\eta-1}),\theta(c_0),...,\theta(c_{\eta-2})\right)\in C_\eta$ dır. Tekrarlama ve lineerlikten, her $r(x)\in R_1[x;\theta]/\left\langle x^\eta-(\varpi)\right\rangle$ için $r(x)c(x)\in C_\eta$ dır. O halde C_η, $R_1[x;\theta]/\left\langle x^\eta-(\varpi)\right\rangle$ nin sol $R_1[x;\theta]-$ alt modülüdür.

Tersine, C_η, $R_1[x;\theta]/\left\langle x^\eta-(\varpi)\right\rangle$ nin sol $R_1[x;\theta]-$ alt modülü olsun. O halde $xc(x)\in C_\eta$ dır. Dolayısıyla, C_η, skew $(\varpi)-$ sabit devirli koddur.

Teorem 4.3.2. C_η, baş katsayısı birimsel eleman olan minimum dereceli $g_\eta(x)$ polinomunu içeren, R_1 üzerinde η uzunluğunda skew $(\varpi)-$ sabit devirli kod ise C_η serbest koddur öyle ki $C_\eta = \langle g_\eta(x) \rangle$ ve $g_\eta(x) \mid x^\eta - (\varpi)$ dir. Ayrıca C_η için baz $\left\{ g_\eta(x), x g_\eta(x), ..., x^{\eta - der(g_\eta(x))-1} g_\eta(x) \right\}$ şeklindedir. $|C_\eta| = |R_1|^{\eta - der(g_\eta(x))}$ dir.

İspat: [35] de ki Teorem 4 ün ispatına benzer şekilde ispatlanır.

Teorem 4.3.3. C_η serbest kod ve tek eleman tarafından üretilen, R_1 üzerinde η uzunluğunda skew $(\varpi)-$ sabit devirli kod olsun. O zaman baş katsayısı birimsel eleman olan $g_\eta(x) \in C_\eta$ minimal dereceli polinomu vardır öyle ki $C_\eta = \langle g_\eta(x) \rangle$ ve $g_\eta(x) \mid x^\eta - (\varpi)$ dir.

İspat: [35] de ki Teorem 5 in ispatına benzer şekilde ispatlanır.

4.4. R_1 Üzerindeki Skew Sabit Devirli Kodların Gray Görüntüleri

Tanım 4.4.1. $a_i, b_i \in \mathbb{Z}_4$, $q_i = a_i + v b_i \in R_1$ $(i = 0,1,...,\eta-1)$ ve ρ_1, ρ_2 iki farklı gray dönüşüm olmak üzere ,

$$\rho_1 : R_1^\eta \to \mathbb{Z}_4^{2\eta}$$
$$(q_0, q_1, ..., q_{\eta-1}) \to (a_0 + 3b_0, ..., a_{\eta-1} + 3b_{\eta-1}, b_0 + 3a_0, ..., b_{\eta-1} + 3a_{\eta-1})$$

ve

$$\rho_2 : R_1^\eta \to \mathbb{Z}_4^{2\eta}$$
$$(q_0, q_1, ..., q_{\eta-1}) \to (a_0 + b_0, ..., a_{\eta-1} + b_{\eta-1}, 3a_0 + 3b_0, ..., 3a_{\eta-1} + 3b_{\eta-1})$$

olacak şekilde tanımlansın.

Önerme 4.4.1. Eğer C_η, R_1 de η uzunluğunda skew $(\varpi)-$ sabit devirli kod ise ,

i. $\varpi = 3, \varpi = v, \varpi = 1+2v, \varpi = 2+3v$ olmak üzere $\rho_1(C_\eta)$, $\mathbb{Z}_4$ üzerinde 2η uzunluğunda devirli koddur,

ii. $\varpi = 3v, \varpi = 2+v, \varpi = 3+2v$ olmak üzere $\rho_1(C_\eta)$, $\mathbb{Z}_4$ üzerinde 2η uzunluğunda 2 indeksli $QC-$ koddur.

iii. $\varpi = 3$ olmak üzere $\rho_1(C_\eta)$, $\mathbb{Z}_4$ üzerinde 2η uzunluğunda 2 indeksli skew $QT-$ koddur.

İspat: C_η, R_1 de η uzunluğunda skew $(\varpi)-$ sabit devirli kod ve

$q = (q_0, q_1, ..., q_{\eta-1}) = (a_0 + vb_0, a_1 + vb_1, ..., a_{\eta-1} + vb_{\eta-1}) \in C_\eta$ olsun.

i. $\varpi = 3$ olsun.

∂, devirli öteleme operatörü ve ξ, skew sabit devirli öteleme operatörü olsun. C_η, R_1 de skew 3- sabit devirli kod olduğundan,

$$\xi(q) = (3\theta(q_{\eta-1}), \theta(q_0), ..., \theta(q_{\eta-2}))$$

$$= \left(3\left(a_{\eta-1} + (2+3v)b_{\eta-1}\right), \left(a_0 + (2+3v)b_0\right), ..., \left(a_{\eta-2} + (2+3v)b_{\eta-2}\right)\right)$$

$$= \left(3a_{\eta-1} + 2b_{\eta-1} + vb_{\eta-1}, a_0 + 2b_0 + 3vb_0, ..., a_{\eta-2} + 2b_{\eta-2} + 3vb_{\eta-2}\right) \text{ dir.}$$

Böylece ρ_1 uygulanarak,

$$\rho_1(\xi(q)) = \left(3a_{\eta-1} + b_{\eta-1}, a_0 + 3b_0, ..., a_{\eta-2} + 3b_{\eta-2}, a_{\eta-1} + 3b_{\eta-1}, 3a_0 + b_0, ..., 3a_{\eta-2} + b_{\eta-2}\right)$$

elde edilir. Diğer taraftan,

$\rho_1(q) = \left(a_0 + 3b_0, a_1 + 3b_1 + ... + a_{\eta-1} + 3b_{\eta-1}, b_0 + 3a_0, b_1 + 3a_1, ..., b_{\eta-1} + 3a_{\eta-1}\right)$ dir. Buradan,

$$\partial\rho_1(q) = \left(b_{\eta-1} + 3a_{\eta-1}, a_0 + 3b_0, ..., a_{\eta-2} + 3b_{\eta-2}, a_{\eta-1} + 3b_{\eta-1}, b_0 + 3a_0, ..., b_{\eta-2} + 3a_{\eta-2}\right)$$

bulunur.

Böylece $\rho_1(\xi(q)) = \partial\rho_1(q)$ dır.

$\varpi = v, \varpi = 1+2v, \varpi = 2+3v$ için ispat benzer şekilde görülmektedir.

ii. $\varpi = 3v$ olsun.

$\bar{\partial}$, parçalı devirli öteleme operatörü ve ξ, skew sabit devirli öteleme operatörü olsun. C_η, R_1 de skew $(3v)-$ sabit devirli kod olduğundan,

$$\xi(q) = \left(3v\theta(q_{\eta-1}), \theta(q_0), ..., \theta(q_{\eta-2})\right)$$

$$= \left(3v\left(a_{\eta-1} + (2+3v)b_{\eta-1}\right), \left(a_0 + (2+3v)b_0\right), ..., \left(a_{\eta-2} + (2+3v)b_{\eta-2}\right)\right)$$

$$= \left(b_{\eta-1} + v(3a_{\eta-1} + 2b_{\eta-1}), a_0 + 2b_0 + 3vb_0, ..., a_{\eta-2} + 2b_{\eta-2} + 3vb_{\eta-2}\right) \text{ dir.}$$

Böylece ρ_1 uygulanarak,

$$\rho_1(\xi(q)) = \left(a_{\eta-1} + 3b_{\eta-1}, a_0 + 3b_0, ..., a_{\eta-2} + 3b_{\eta-2}, 3a_{\eta-1} + b_{\eta-1}, 3a_0 + b_0, ..., +3a_{\eta-2} + b_{\eta-2}\right)$$

elde edilir. Diğer taraftan,

$$\rho_1(q) = \left(a_0 + 3b_0, a_1 + 3b_1 + ... + a_{\eta-1} + 3b_{\eta-1}, b_0 + 3a_0, b_1 + 3a_1, ..., b_{\eta-1} + 3a_{\eta-1}\right) \text{ dir.}$$

Buradan,

$$\bar{\partial}\rho_1(q) = \left(a_{\eta-1} + 3b_{\eta-1}, a_0 + 3b_0, ..., a_{\eta-2} + 3b_{\eta-2}, b_{\eta-1} + 3a_{\eta-1}, b_0 + 3a_0, ..., +b_{\eta-2} + 3a_{\eta-2}\right)$$

bulunur.

Böylece $\rho_1(\xi(q)) = \bar{\partial}\rho_1(q)$ dir.

$\varpi = 2+v, \varpi = 3+2v$ için ispat benzer şekilde görülmektedir.

iii. $\varpi = 3$ olsun.

$\wp$, skew quasi twisted öteleme operatörü ve ξ, skew sabit devirli öteleme operatörü olsun. i den:

$\rho_1(\xi(q)) = \left(3a_{\eta-1} + b_{\eta-1}, a_0 + 3b_0, ..., a_{\eta-2} + 3b_{\eta-2}, a_{\eta-1} + 3b_{\eta-1}, 3a_0 + b_0, ..., 3a_{\eta-2} + b_{\eta-2}\right)$ olarak bulunmuştu. Diğer taraftan,

$\rho_1(q) = \left(a_0 + 3b_0, a_1 + 3b_1, ..., a_{\eta-1} + 3b_{\eta-1}, b_0 + 3a_0, b_1 + 3a_1, ..., b_{\eta-1} + 3a_{\eta-1}\right)$ dir. Buradan,

$\wp\rho_1(q) = \left(3a_{\eta-1} + b_{\eta-1}, a_0 + 3b_0, ..., a_{\eta-2} + 3b_{\eta-2}, a_{\eta-1} + 3b_{\eta-1}, b_0 + 3a_0, ..., b_{\eta-2} + 3a_{\eta-2}\right)$ bulunur.

Böylece $\rho_1(\xi(q)) = \wp\rho_1(q)$ dir.

Önerme 4.4.2. Eğer C_η, R_1 de η uzunluğunda skew $(\varpi)-$ sabit devirli kod ise,

i. $\varpi=3,\varpi=3v,\varpi=1+2v,\varpi=2+v$ olmak üzere $\rho_2(C_\eta)$, $\mathbb{Z}_4$ üzerinde 2η uzunluğunda devirli koddur.

ii. $\varpi=v,\varpi=2+3v,\varpi=3+2v$ olmak üzere $\rho_2(C_\eta)$, $\mathbb{Z}_4$ üzerinde 2η uzunluğunda 2 indeksli $QC-$koddur.

iii. $\varpi=3$ olmak üzere $\rho_2(C_\eta)$, $\mathbb{Z}_4$ üzerinde 2η uzunluğunda 2 indeksli skew $QT-$koddur.

İspat: C_η, R_1 de η uzunluğunda skew $(\varpi)-$ sabit devirli kod ve

$q=(q_0,q_1,...,q_{\eta-1})=(a_0+vb_0,a_1+vb_1,...,a_{\eta-1}+vb_{\eta-1})\in C_\eta$ olsun.

i. $\varpi=3$ olsun.

∂, devirli öteleme operatörü ve ξ, skew sabit devirli öteleme operatörü olsun. C_η, R_1 de skew 3- sabit devirli kod olduğundan,

$$\xi(q)=(3\theta(q_{\eta-1}),\theta(q_0),...,\theta(q_{\eta-2}))$$
$$=(3(a_{\eta-1}+(2+3v)b_{\eta-1}),(a_0+(2+3v)b_0),...,(a_{\eta-2}+(2+3v)b_{\eta-2}))$$
$$=(3a_{\eta-1}+2b_{\eta-1}+vb_{\eta-1},a_0+2b_0+3vb_0,...,a_{\eta-2}+2b_{\eta-2}+3vb_{\eta-2}) \text{ dir.}$$

Böylece ρ_2 uygulanarak,

$$\rho_2(\xi(q))=(3a_{\eta-1}+3b_{\eta-1},a_0+b_0,...,a_{\eta-2}+b_{\eta-2},a_{\eta-1}+b_{\eta-1},3a_0+3b_0,...,3a_{\eta-2}+3b_{\eta-2})$$

elde edilir. Diğer taraftan,

$\rho_2(q)=(a_0+b_0,a_1+b_1+...+a_{\eta-1}+b_{\eta-1},3a_0+3b_0,3a_1+3b_1,...,3a_{\eta-1}+3b_{\eta-1})$ dir. Buradan,

$$\partial\rho_2(q)=(3a_{\eta-1}+3b_{\eta-1},a_0+b_0,...,a_{\eta-2}+b_{\eta-2},a_{\eta-1}+b_{\eta-1},3a_0+3b_0,...,3a_{\eta-2}+3b_{\eta-2})$$

bulunur.

Böylece $\rho_2(\xi(q))=\partial\rho_2(q)$ dır.

$\varpi=3v,\varpi=1+2v,\varpi=2+v$ için ispat benzer şekilde görülmektedir.

ii. $\varpi = v$ olsun.

$\bar{\partial}$, parçalı devirli öteleme operatörü ve ξ, skew sabit devirli öteleme operatörü olsun. C_η, R_1 de skew $v-$ sabit devirli kod olduğundan,

$$\xi(q) = \left(v\theta(q_{\eta-1}), \theta(q_0), ..., \theta(q_{\eta-2})\right)$$

$$= \left(v\left(a_{\eta-1} + (2+3v)b_{\eta-1}\right), \left(a_0 + (2+3v)b_0\right), ..., \left(a_{\eta-2} + (2+3v)b_{\eta-2}\right)\right)$$

$$= \left(3b_{\eta-1} + v(a_{\eta-1} + 2b_{\eta-1}), a_0 + 2b_0 + 3vb_0, ..., a_{\eta-2} + 2b_{\eta-2} + 3vb_{\eta-2}\right) \text{ dir.}$$

Böylece ρ_2 uygulanarak,

$$\rho_2\left(\xi(q)\right) = \left(a_{\eta-1} + b_{\eta-1}, a_0 + b_0, ..., a_{\eta-2} + b_{\eta-2}, 3a_{\eta-1} + 3b_{\eta-1}, 3a_0 + 3b_0, ..., +3a_{\eta-2} + 3b_{\eta-2}\right)$$

elde edilir. Diğer taraftan,

$$\rho_2(q) = \left(a_0 + b_0, a_1 + b_1 + ... + a_{\eta-1} + b_{\eta-1}, 3a_0 + 3b_0, 3a_1 + 3b_1, ..., 3a_{\eta-1} + 3b_{\eta-1}\right) \text{ dir.}$$

Buradan,

$$\bar{\partial}\rho_2(q) = \left(a_{\eta-1} + b_{\eta-1}, a_0 + b_0, ..., a_{\eta-2} + b_{\eta-2}, 3a_{\eta-1} + 3b_{\eta-1}, 3a_0 + 3b_0, ..., +3a_{\eta-2} + 3b_{\eta-2}\right)$$

bulunur.

Böylece $\rho_2\left(\xi(q)\right) = \bar{\partial}\rho_2(q)$ dir.

$\varpi = 2+3v, \varpi = 3+2v$ için ispat benzer şekilde görülmektedir.

iii. $\varpi = 3$ olsun.

$\wp$, skew quasi twisted öteleme operatörü ve ξ, skew sabit devirli öteleme operatörü olsun. i den :

$\rho_2\left(\xi(q)\right) = \left(3a_{\eta-1} + 3b_{\eta-1}, a_0 + b_0, ..., a_{\eta-2} + b_{\eta-2}, a_{\eta-1} + b_{\eta-1}, 3a_0 + 3b_0, ..., 3a_{\eta-2} + 3b_{\eta-2}\right)$ olarak bulunmuştu. Diğer taraftan,

$\rho_2(q) = \left(a_0 + b_0, a_1 + b_1 + ... + a_{\eta-1} + b_{\eta-1}, 3a_0 + 3b_0, 3a_1 + 3b_1, ..., 3a_{\eta-1} + 3b_{\eta-1}\right)$ dir. Buradan,

$$\wp\rho_2(q) = \left(3a_{\eta-1} + 3b_{\eta-1}, a_0 + b_0, ..., a_{\eta-2} + b_{\eta-2}, a_{\eta-1} + b_{\eta-1}, 3a_0 + 3b_0, ..., 3a_{\eta-2} + 3b_{\eta-2}\right)$$

bulunur.

Böylece $\rho_2\left(\xi(q)\right) = \wp\rho_2(q)$ dir.

Ayrıca,

$$\theta_1 : \mathbb{Z}_4 + v\mathbb{Z}_4 \to \mathbb{Z}_4 + v\mathbb{Z}_4$$
$$a + vb \to a + 3vb$$

olacak şekilde θ_1 otomorfizması ve $a_i, b_i \in \mathbb{Z}_4$, $q_i = a_i + vb_i \in R_1$ $(i = 0,1,...,\eta - 1)$,

$$\rho_3 : R_1^{\eta} \to \mathbb{Z}_4^{2\eta}$$
$$(q_0, q_1, ..., q_{\eta-1}) \to (2a_0, ..., 2a_{\eta-1}, 2b_0, ..., 2b_{\eta-1})$$

olacak şekilde ρ_3 gray dönüşüm tanımlansın. θ_1 ve ρ_3 kullanılarak Önerme 4.4.3. sağlanır.

Önerme 4.4.3. Eğer C_η, R_1 de η uzunluğunda skew $(\varpi)-$sabit devirli kod ise,

i. $\varpi = v, \varpi = 3v, \varpi = 2 + v, \varpi = 2 + 3v$ olmak üzere $\rho_3(C_\eta)$, $\mathbb{Z}_4$ üzerinde 2η uzunluğunda devirli koddur.

ii. $\varpi = 3, \varpi = 1 + 2v, \varpi = 3 + 2v$ olmak üzere $\rho_3(C_\eta)$, $\mathbb{Z}_4$ üzerinde 2η uzunluğunda 2 indeksli $QC-$kod ve 2 indeksli skew $QT-$koddur.

İspat: C_η, R_1 de η uzunluğunda skew $(\varpi)-$sabit devirli kod ve

$q = (q_0, q_1, ..., q_{\eta-1}) = (a_0 + vb_0, a_1 + vb_1, ..., a_{\eta-1} + vb_{\eta-1}) \in C_\eta$ olsun.

i. $\varpi = v$ olsun.

∂, devirli öteleme operatörü ve ξ, skew sabit devirli öteleme operatörü olsun. C_η, R_1 de skew $v-$sabit devirli kod olduğundan,

$$\xi(q) = (v\theta(q_{\eta-1}), \theta(q_0), ..., \theta(q_{\eta-2}))$$
$$= (v(a_{\eta-1} + 3vb_{\eta-1}), (a_0 + 3vb_0), ..., (a_{\eta-2} + 3vb_{\eta-2}))$$
$$= (3b_{\eta-1} + va_{\eta-1}, a_0 + 3vb_0, ..., a_{\eta-2} + 3vb_{\eta-2}) \text{ dir.}$$

Böylece ρ_3 uygulanarak,

$\rho_3(\xi(q)) = (2b_{\eta-1}, 2a_0, ..., 2a_{\eta-2}, 2a_{\eta-1}, 2b_0, ..., 2b_{\eta-2})$ elde edilir. Diğer taraftan, $\rho_3(q) = (2a_0, 2a_1, ..., 2a_{\eta-1}, 2b_0, 2b_1, ..., 2b_{\eta-1})$ dir. Buradan,

$\partial\rho_3(q)=\left(2b_{\eta-1},2a_0,...,2a_{\eta-2},2a_{\eta-1},2b_0,...,2b_{\eta-2}\right)$ bulunur.

Böylece $\rho_3(\xi(q))=\partial\rho_3(q)$ dır.

$\varpi=3v,\varpi=2+v,\varpi=2+3v$ için ispat benzer şekilde görülmektedir.

ii. $\varpi=3$ olsun.

$\bar{\partial}$, parçalı devirli öteleme operatörü, $\wp$, skew quasi twisted öteleme operatörü ve ξ, skew sabit devirli öteleme operatörü olsun. C_η, R_1 de skew 3- sabit devirli kod olduğundan,

$\xi(q)=\left(3\theta(q_{\eta-1}),\theta(q_0),...,\theta(q_{\eta-2})\right)$

$=\left(3\left(a_{\eta-1}+3vb_{\eta-1}\right),\left(a_0+3vb_0\right),...,\left(a_{\eta-2}+3vb_{\eta-2}\right)\right)$

$=\left(3a_{\eta-1}+vb_{\eta-1},a_0+3vb_0,...,a_{\eta-2}+3vb_{\eta-2}\right)$ dir. Böylece ρ_3 uygulanarak,

$\rho_3(\xi(q))=\left(2a_{\eta-1},2a_0,...,2a_{\eta-2},2b_{\eta-1},2b_0,...,2b_{\eta-2}\right)$ elde edilir. Diğer taraftan,

$\rho_3(q)=\left(2a_0,2a_1,...,2a_{\eta-1},2b_0,2b_1,...,2b_{\eta-1}\right)$ dir. Buradan,

$\bar{\partial}\rho_3(q)=\left(2a_{\eta-1},2a_0,...,2a_{\eta-2},2b_{\eta-1},2b_0,...,2b_{\eta-2}\right)$ ve

$\wp\rho_3(q)=\left(2a_{\eta-1},2a_0,...,2a_{\eta-2},2b_{\eta-1},2b_0,...,2b_{\eta-2}\right)$ bulunur.

Böylece $\rho_3(\xi(q))=\bar{\partial}\rho_3(q)$ ve $\rho_3(\xi(q))=\wp\rho_3(q)$ dir.

$\varpi=1+2v,\varpi=3+2v$ için ispat benzer şekilde görülmektedir.

4.5. $\mathbb{Z}_4R_1-$ Lineer Skew $(\varpi)-$ Sabit Devirli Kodlar

Tanım 4.5.1. θ, R_1 de otomorfizma olsun. ${\mathbb{Z}_4}^\mu{R_1}^\eta$ da

i. C, ${\mathbb{Z}_4}^\mu{R_1}^\eta$ nın R_1-alt modülüdür.

ii. $i=0,1,..,.\mu-1$ için $\theta(p_i)=p_i$ $(p_i\in\mathbb{Z}_4)$ olmak üzere $\left(p_0,p_1,...,p_{\mu-1},q_0,q_1,...,q_{\eta-1}\right)\in C$ iken $\left(\varepsilon(\varpi)\theta(p_{\mu-1}),\theta(p_0),...,\theta(p_{\mu-2}),\varpi\theta(q_{\eta-1}),\theta(q_0),...,\theta(q_{\eta-2})\right)\in C$

şartlarını sağlayan C lineer koduna skew sabit devirli kod denir.

$(p_0, p_1, ..., p_{\mu-1}, q_0, q_1, ..., q_{\eta-1}) \in C$ kod sözü polinom cinsinden aşağıdaki gibi ifade edilebilir:

$$c(x) = \begin{pmatrix} p_0 + p_1 x + ... + p_{\mu-1} x^{\mu-1} \\ q_0 + q_1 x + ... + q_{\eta-1} x^{\eta-1} \end{pmatrix} = (p(x), q(x)) \in \mathbb{Z}_4[x] / \langle x^\mu - \varepsilon(\varpi) \rangle \times R_1[x;\theta] / \langle x^\eta - \varpi \rangle.$$

$r(x) = r_0 + r_1 x + ... + r_l x^l \in R_1[x;\theta]$,

$(f(x), g(x)) \in \mathbb{Z}_4[x] / \langle x^\mu - \varepsilon(\varpi) \rangle \times R_1[x;\theta] / \langle x^\eta - \varpi \rangle$ olsun.

$\varepsilon(r(x)) = \varepsilon(r_0) + \varepsilon(r_1) x + ... + \varepsilon(r_l) x^l$ olmak üzere,

$r(x)(f(x), g(x)) = (\varepsilon(r(x)) f(x), r(x) g(x))$ elde edilir.

Önerme 4.5.1. C nin $\mathbb{Z}_4 R_1$ üzerinde (μ, η) uzunluğunda skew $(\varpi)-$sabit devirli kod olması için gerek ve yeter şart C nin $\mathbb{Z}_4[x] / \langle x^\mu - \varepsilon(\varpi) \rangle \times R_1[x;\theta] / \langle x^\eta - (\varpi) \rangle$ nin sol $R_1[x;\theta]-$alt modülü olmasıdır.

İspat: C skew $(\varpi)-$sabit devirli kod ve $c \in C$ olsun. $c(x) = (p(x), q(x))$ yazılabilir. C skew $(\varpi)-$sabit devirli kod olduğundan, $xc(x) \in C$ dir. C nin lineerliğinden, herhangi $r(x) \in R_1[x;\theta]$ için $r(x)c(x) \in C$ dir. O halde C, $\mathbb{Z}_4[x] / \langle x^\mu - \varepsilon(\varpi) \rangle \times R_1[x;\theta] / \langle x^\eta - (\varpi) \rangle$ nin sol $R_1[x;\theta]-$ alt modülüdür.

Tersine, C, $\mathbb{Z}_4[x] / \langle x^\mu - \varepsilon(\varpi) \rangle \times R_1[x;\theta] / \langle x^\eta - (\varpi) \rangle$ nin sol $R_1[x;\theta]-$alt modülü olsun. O halde $xc(x) \in C$ dir. Dolayısıyla, C skew $(\varpi)-$sabit devirli koddur.

Teorem 4.5.1. C_μ, μ uzunluğunda $\mathbb{Z}_4$ de lineer kod, C_η, η uzunluğunda R_1 de lineer kod olmak üzere, $C = C_\mu \times C_\eta$ kodu (μ, η) uzunluğunda $\mathbb{Z}_4 R_1$ de lineer kod olsun. C kodunun skew $(\varpi)-$sabit devirli kod olması için gerek ve yeter şart C_μ nün $\mathbb{Z}_4$ de $\varepsilon(\varpi)-$sabit devirli kod ve C_η nın R_1 de skew $(\varpi)-$sabit devirli kod olmasıdır.

İspat: $(p_0, p_1, ..., p_{\mu-1}) \in C_\mu$, $(q_0, q_1, ..., q_{\eta-1}) \in C_\eta$ ve C, skew $(\varpi)-$sabit devirli kod olsun. Buradan,

$(\varepsilon(\varpi)\theta(p_{\mu-1}), \theta(p_0), ..., \theta(p_{\mu-2}), (\varpi)\theta(q_{\eta-1}), \theta(q_0), ..., \theta(q_{\eta-2})) \in C$ dir. Yani,

$(\varepsilon(\varpi)\theta(p_{\mu-1}), \theta(p_0), ..., \theta(p_{\mu-2})) = (\varepsilon(\varpi)(p_{\mu-1}), (p_0), ..., (p_{\mu-2})) \in C_\mu$ ve

$((\varpi)\theta(q_{\eta-1}), \theta(q_0), ..., \theta(q_{\eta-2})) \in C_\eta$ dır. O halde C_μ , $\mathbb{Z}_4$ de $\varepsilon(\varpi)-$sabit devirli kod ve C_η , R_1 de skew $(\varpi)-$sabit devirli koddur.

Diğer taraftan, C_μ , $\mathbb{Z}_4$ de $\varepsilon(\varpi)-$sabit devirli kod ve C_η , R_1 de skew $(\varpi)-$sabit devirli kod olsun. Böylece,

$(\varepsilon(\varpi)\theta(p_{\mu-1}), \theta(p_0), ..., \theta(p_{\mu-2})) = (\varepsilon(\varpi)(p_{\mu-1}), (p_0), ..., (p_{\mu-2})) \in C_\mu$ ve

$((\varpi)\theta(q_{\eta-1}), \theta(q_0), ..., \theta(q_{\eta-2})) \in C_\eta$ dır. Buradan $C = C_\mu \times C_\eta$ olduğundan

$(\varepsilon(\varpi)\theta(p_{\mu-1}), \theta(p_0), ..., \theta(p_{\mu-2}), (\varpi)\theta(q_{\eta-1}), \theta(q_0), ..., \theta(q_{\eta-2})) \in C$ bulunur.

Böylece C, $\mathbb{Z}_4 R_1$ de skew $(\varpi)-$sabit devirli koddur.

4.6. $\mathbb{Z}_4 R_1$ – Skew Sabit Devirli Kodların Üreteç Polinomu ve Geren Kümesi

Bu bölümde $\mathbb{Z}_4\mathbb{Z}_4[v]-$skew sabit devirli kodun üreteç polinomunu bulmak için aşağıda verilen teoremden yararlanılacaktır.

Teorem 4.6.1. [37] n pozitif tek tamsayı olmak üzere C, $\mathbb{Z}_4 + v\mathbb{Z}_4$ üzerinde n uzunluğunda devirli bir kod olsun. $\mathbb{Z}_4 + v\mathbb{Z}_4$ üzerindeki $g_2(x)$ polinomu ve $\mathbb{Z}_4$ 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.

C kodu $\mathbb{Z}_4\mathbb{Z}_4[v]-$skew sabit devirli kod olsun. C kodu ve $R_1[x;\theta]/\langle x^\eta - \varpi \rangle$, $R_1[x;\theta]-$modül olduğundan;

$$\gamma: \quad C \quad \to R_1[x;\theta]/\langle x^{\eta}-\varpi\rangle$$
$$(f(x),\overline{f}(x))\to \quad \overline{f}(x)$$

olacak şekilde tanımlanan γ dönüşümü modül homomorfizmasıdır.

Çek $\gamma=\{(f(x),0)\in C: f(x)\in\mathbb{Z}_4[x]/\langle x^{\mu}-\varepsilon(\varpi)\rangle\}$ kümesi C kodunun bir alt modülüdür ve Im γ, $R[x]/\langle x^{\eta}-\varpi\rangle$ nin $R_1[x;\theta]$ alt modülüdür.

Uyarı 4.6.1. Alınan herhangi bir $f(x)$ polinomu f şeklinde verilecektir.

Önerme 4.6.1. C kodu $\mathbb{Z}_4R_1$ üzerinde skew sabit devirli kod olsun. $f\,|\,(x^{\mu}-\varepsilon(\varpi))$ ve g_1,g_2,g_3 Teorem 4.6.1. de verilen polinomlar 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 $\mathbb{Z}_4R_1$ üzerinde skew sabit devirli kod olsun.

Im $\gamma=\langle g_1+(1+v)g_2,(1+v)g_3\rangle$ olmak üzere $\gamma(l_1,g_1+(1+v)g_2)=g_1+(1+v)g_2$ ve $\gamma(l_2,(1+v)g_3)=(1+v)g_3$ olacak şekilde $(l_1,g_1+(1+v)g_2),(l_2,(1+v)g_3)\in C$ vardır. Herhangi bir $(p,q)\in C$ nin $(f,0)$, $(l_1,g_1+(1+v)g_2)$ ve $(l_2,(1+v)g_3)$ tarafından üretildiği gösterilsin. $r_1,r_2\in R_1[x;\theta]$ elemanları vardır öyle ki $\gamma(p,q)=q=r_1(g_1+(1+v)g_2)+r_2((1+v)g_3)$ şeklindedir.

$(p,q)-(r_1*(l_1,g_1+(1+v)g_2)+r_2*(l_2,(1+v)g_3))=(p-\varepsilon(r_1)l_1-\varepsilon(r_2)l_2,0)\in Çek\gamma$ olduğundan $r_3\in\mathbb{Z}_4[x]$ vardır öyle ki $(p-\varepsilon(r_1)l_1-\varepsilon(r_2)l_2,0)=r_3*(f,0)$ olarak bulunur. Böylece,

$$\begin{aligned}(p,q)&=r_1*(l_1,g_1+(1+v)g_2)+r_2*(l_2,(1+v)g_3)+(p-\varepsilon(r_1)l_1-\varepsilon(r_2)l_2,0)\\&=r_1*(l_1,g_1+(1+v)g_2)+r_2*(l_2,(1+v)g_3)+r_3*(f,0)\end{aligned}$$

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

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

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

Önerme 4.6.2. $f \mid (x^{\mu}-\varepsilon(\varpi))$ olsun. Eğer

$C = \langle (f,0),(l_1, g_1+(1+v)g_2),(l_2,(1+v)g_3)\rangle$ kodu $\mathbb{Z}_4R_1-$skew sabit devirli kod ise

$der(l_1) < der(f)$, $der(l_2) < der(f)$ ve $f \mid \dfrac{x^{\eta}-\varpi}{g_3} l_1 \bmod (1+3v)$, $f \mid a\bar{g}l_1 \bmod (1+3v)$

şeklindedir. Burada $\bar{g} = \dfrac{x^{\eta}-\varpi}{g_1}$ ve $a = \dfrac{x^{\eta}-\varpi}{\bar{g}g_2}$ dir.

İspat: $der(l_1) \geq der(f)$ olsun. $l_1 = fq_1 + r_1$; $0 \leq der(r_1) < der(f)$ şartını sağlayan $q_1, r_1 \in \mathbb{Z}_4[x]/\langle x^{\mu}-\varepsilon(\varpi)\rangle$ vardır. $der(l_2) \geq der(f)$ olsun. $l_2 = fq_2 + r_2$;

$0 \leq der(r_2) < der(f)$ şartını sağlayan $q_2, r_2 \in \mathbb{Z}_4[x]/\langle x^{\mu}-\varepsilon(\varpi)\rangle$ vardır. Buradan,

$$\langle (f,0),(l_1, g_1+(1+v)g_2),(l_2,(1+v)g_3)\rangle = \langle (f,0),(fq_1+r_1, g_1+(1+v)g_2),(fq_2+r_2,(1+v)g_3)\rangle$$
$$= \langle (f,0),(r_1, g_1+(1+v)g_2),(r_2,(1+v)g_3)\rangle$$

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

$f \mid \dfrac{x^{\eta}-\varpi}{g_3} l_1 \bmod (1+3v)$ olduğu gösterilsin.

$$\frac{x^{\eta}-\varpi}{g_3} * (l_1, g_1+(1+v)g_2) = \left(\varepsilon\left(\frac{x^{\eta}-\varpi}{g_3}\right)l_1, \frac{x^{\eta}-\varpi}{g_3}(g_1+(1+v)g_2)\right) = \left(\varepsilon\left(\frac{x^{\eta}-\varpi}{g_3}\right)l_1, 0\right)$$

elde edilir. $\gamma\left(\varepsilon\left(\dfrac{x^{\eta}-\varpi}{g_3}\right)l_1, 0\right) = 0$ olarak bulunur. Böylece

$\left(\varepsilon\left(\dfrac{x^{\eta}-\varpi}{g_3}\right)l_1, 0\right) \in Çek\gamma \subseteq C$ olduğundan $f \mid \dfrac{x^{\eta}-\varpi}{g_3} l_1 \bmod (1+3v)$ elde edilir.

$f \mid a\bar{g}l_1 \bmod (1+3v)$ olduğu gösterilsin.

$$a\bar{g} * (l_1, g_1+(1+v)g_2) = (\varepsilon(a\bar{g})l_1, a\bar{g}g_1+(1+v)a\bar{g}g_2) = (\varepsilon(a\bar{g})l_1, 0)$$

elde edilir. $\gamma\left(\varepsilon\left(a\bar{g}\right)l_1,0\right)=0$ olarak bulunur. Böylece $\left(\varepsilon\left(a\bar{g}\right)l_1,0\right)\in Çek\gamma\subseteq C$ olduğundan $f\mid a\bar{g}l_1 \bmod\left(1+3v\right)$ elde edilir.

Teorem 4.6.2. $f\mid\left(x^{\mu}-\varepsilon\left(\varpi\right)\right)$ olsun. Teorem 4.6.1. de verilen g_1,g_2,g_3 polinomları $der\left(g_1\right)>der\left(g_2\right)$ şartını sağlayan polinomlar olmak üzere $C=\left\langle\left(f,0\right),\left(l_1,g_1+\left(1+v\right)g_2\right),\left(l_2,\left(1+v\right)g_3\right)\right\rangle$ kodu $\mathbb{Z}_4\mathbb{Z}_4\left[v\right]$halkasında skew sabit devirli kod olsun. O halde

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

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

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

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

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

İspat: $C=\left\langle\left(f,0\right),\left(l_1,g_1+\left(1+v\right)g_2\right),\left(l_2+\left(1+v\right)g_3\right)\right\rangle$ ve $c\in C$ olsun. $b_1,b_2,b_3\in R_1\left[x;\theta\right]$ olmak üzere, $c=\varepsilon\left(b_1\right)\left(f,0\right)+b_2\left(l_1,g_1+\left(1+v\right)g_2\right)+b_3\left(l_2,\left(1+v\right)g_3\right)$ yazılabilir. Eğer $der\left(\varepsilon\left(b_1\right)\right)\le\mu-der\left(f\right)-1$ ise $\varepsilon\left(b_1\right)\left(f,0\right)\in\left\langle S_1\right\rangle$ dir. Aksi taktirde bölme algoritması uygulanarak, $d_1,r_1\in R_1\left[x;\theta\right]$ ve $0\le der\left(\varepsilon\left(r_1\right)\right)\le\mu-der\left(f\right)-1$ olmak üzere, $\varepsilon\left(b_1\right)=\left(\frac{x^{\mu}-\varepsilon\left(\varpi\right)}{f}\varepsilon\left(d_1\right)\right)+\varepsilon\left(r_1\right)$ dir. Dolayısıyla,

$$\begin{aligned}\varepsilon\left(b_1\right)\left(f,0\right)&=\left(\frac{x^{\mu}-\varepsilon\left(\varpi\right)}{f}\varepsilon\left(d_1\right)+\varepsilon\left(r_1\right)\right)\left(f,0\right)\\&=\varepsilon\left(d_1\right)\left(\frac{x^{\mu}-\varepsilon\left(\varpi\right)}{f}f,0\right)+\varepsilon\left(r_1\right)\left(f,0\right)\\&=\varepsilon\left(r_1\right)\left(f,0\right)\end{aligned}$$

bulunur. Buradan, $\varepsilon(b_1)(f,0)\in\langle S_1\rangle$ dir.

Eğer $der(b_2)\le\eta-der(g_1)-1$ ise $b_2(l_1,g_1+(1+v)g_2)\in\langle S_2\rangle$ dir. Aksi taktirde bölme algoritması uygulanarak, $d_2,r_2\in\mathbb{Z}_4[x]$ ve $0\le der(r_2)\le\eta-der(g_1)-1$ olmak üzere, $b_2=\dfrac{x^\eta-\varpi}{g_1}d_2+r_2=\bar{g}d_2+r_2$ dir. Buradan,

$$\begin{aligned}b_2(l_1,g_1+(1+v)g_2)&=(\bar{g}d_2+r_2)(l_1,g_1+(1+v)g_2)\\&=d_2(\varepsilon(\bar{g})l_1,\bar{g}g_1+(1+v)\bar{g}g_2)+r_2(l_1,g_1+(1+v)g_2)\\&=d_2(\varepsilon(\bar{g})l_1,(1+v)\bar{g}g_2)+r_2(l_1,g_1+(1+v)g_2)\end{aligned}$$

olur. $0\le der(r_2)\le\eta-der(g_1)-1$ olduğundan, $r_2(l_1,g_1+(1+v)g_2)\in\langle S_2\rangle$ dir. Şimdi $d_2(\varepsilon(\bar{g})l_1,(1+v)\bar{g}g_2)\in\langle S\rangle$ olduğu ispatlansın. Eğer $der(d_2)\le der(g_1)-der(g_2)-1$ ise $d_2(\varepsilon(\bar{g})l_1,(1+v)\bar{g}g_2)\in\langle S_3\rangle$ tür. Aksi taktirde bölme algoritması uygulanarak, $d_3,r_3\in\mathbb{Z}_4[x]$ ve $der(r_3)\le der(g_1)-der(g_2)-1$ olmak üzere, $d_2=\dfrac{x^\eta-\varpi}{\bar{g}g_2}d_3+r_3=ad_3+r_3$ tür. Buradan,

$$\begin{aligned}d_2(\varepsilon(\bar{g})l_1,(1+v)\bar{g}g_2)&=(ad_3+r_3)(\varepsilon(\bar{g})l_1,(1+v)\bar{g}g_2)\\&=d_3(a\varepsilon(\bar{g})l_1,(1+v)a\bar{g}g_2)+r_3(\varepsilon(\bar{g})l_1,(1+v)\bar{g}g_2)\\&=d_3(a\varepsilon(\bar{g})l_1,0)+r_3(\varepsilon(\bar{g})l_1,(1+v)\bar{g}g_2)\end{aligned}$$

dir.

$0\le der(r_3)\le der(g_1)-der(g_2)-1$ olduğundan $r_3(\varepsilon(\bar{g})l_1,(1+v)\bar{g}g_2)\in\langle S_3\rangle$ tür. Önerme 4.6.2. den $ft=a\bar{g}l_1 \mod (1+3v)$ olduğundan $d_3(a\varepsilon(\bar{g})l_1,0)\in\langle S_1\rangle$ dir. Buradan $b_2(l_1,g_1+(1+v)g_2)\in\langle S_1\cup S_2\cup S_3\rangle$ olarak bulunur.

Şimdi $b_3(l_2,(1+v)g_3)\in\langle S_4\rangle$ olduğu ispatlansın. $der(b_3)\le\eta-der(g_3)-1$ ise $b_3(l_2,(1+v)g_3)\in\langle S_4\rangle$ tür. Aksi taktirde bölme algoritması uygulanarak, $d_4,r_4\in\mathbb{Z}_4[x]$ ve $0\le der(r_4)\le\eta-der(g_3)-1$ olmak üzere, $b_3=\dfrac{x^\eta-\varpi}{g_3}d_4+r_4$ şeklindedir. Dolayısıyla,

$$b_3\left(l_2,(1+v)g_3\right)=\left(\frac{x^\eta-\varpi}{g_3}d_4+r_4\right)\left(l_2,(1+v)g_3\right)$$
$$=d_4\left(\varepsilon\left(\frac{x^\eta-\varpi}{g_3}\right)l_2,\frac{x^\eta-\varpi}{g_3}(1+v)g_3\right)+r_4\left(l_2,(1+v)g_3\right)$$
$$=d_4\left(\varepsilon\left(\frac{x^\eta-\varpi}{g_3}\right)l_2,0\right)+r_4\left(l_2,(1+v)g_3\right)$$

dir. $0\le der(r_4)\le\eta-der(g_3)-1$ olduğundan, $r_4\left(l_2,(1+v)g_3\right)\in\langle S_4\rangle$ tür. Önerme 4.6.2. den $\tilde{ff}=\frac{x^\eta-\varpi}{g_3}l_1 \mod (1+3v)$ olduğundan $d_4\left(\varepsilon\left(\frac{x^\eta-\varpi}{g_3}\right)l_2,0\right)\in\langle S_1\rangle$ dir. Buradan, $b_3\left(l_2,(1+v)g_3\right)\in\langle S_1\cup S_4\rangle$ olarak bulunur. O halde, $S=S_1\cup S_2\cup S_3\cup S_4$, C kodu için geren kümedir ve S de ki diğer elemanlar ile lineer bağımlı olacak şekilde eleman olmadığı için S kümesi C kodu için en küçük geren kümedir.

4.7. $\mathbb{Z}_4R_1$ Üzerindeki Skew Sabit Devirli Kodların Gray Görüntüleri

Tanım 4.7.1. $a_i,b_i\in\mathbb{Z}_4$, $q_i=a_i+vb_i\in R_1$ $(i=0,1,...,\eta-1)$ ve ϕ_1,ϕ_2 iki farklı gray dönüşüm olmak üzere ,

$$\phi_1:{\mathbb{Z}_4}^\mu{R_1}^\eta\to{\mathbb{Z}_4}^{\mu+2\eta}$$
$$\left(p_0,p_1,...,p_{\mu-1},q_0,q_1,...,q_{\eta-1}\right)\to\left(p_0,p_1,...,p_{\mu-1},a_0+3b_0,...,a_{\eta-1}+3b_{\eta-1},b_0+3a_0,...,b_{\eta-1}+3a_{\eta-1}\right)$$

ve

$$\phi_2:{\mathbb{Z}_4}^\mu{R_1}^\eta\to{\mathbb{Z}_4}^{\mu+2\eta}$$
$$\left(p_0,p_1,...,p_{\mu-1},q_0,q_1,...,q_{\eta-1}\right)\to\left(p_0,p_1,...,p_{\mu-1},a_0+b_0,...,a_{\eta-1}+b_{\eta-1},3a_0+3b_0,...,3a_{\eta-1}+3b_{\eta-1}\right)$$

olacak şekilde tanımlansın.

Teorem 4.7.1. C, $\mathbb{Z}_4[x]/\langle x^\mu-\varepsilon(\varpi)\rangle\times R_1[x;\theta]/\langle x^\eta-\varpi\rangle$ de skew sabit devirli kod olsun. Bu durumda,

i. $\varpi=v,\varpi=2+3v$ olmak üzere eğer $\mu=\eta$ ise $\phi_1(C)$, 2 indeksli $QC-$ koddur. Eğer $\mu\neq\eta$ ise $\phi_1(C)$, 2 indeksli genelleştirilmiş $QC-$koddur.

ii. $\varpi = 3+2v$ olmak üzere eğer $\mu = \eta$ ise $\phi_1(C)$, 3 indeksli $QC-$koddur. Eğer $\mu \neq \eta$ ise $\phi_1(C)$, 3 indeksli genelleştirilmiş $QC-$koddur.

iii. $\varpi = 3$ olmak üzere eğer $\mu = \eta$ ise $\phi_1(C)$, 3 indeksli skew $QT-$koddur. Eğer $\mu \neq \eta$ ise $\phi_1(C)$, 3 indeksli genelleştirilmiş skew $QT-$koddur.

İspat: C, $\mathbb{Z}_4[x]/\langle x^\mu - \varepsilon(\varpi)\rangle \times R_1[x;\theta]/\langle x^\eta - (\varpi)\rangle$ de skew sabit devirli kod ve $c = (p_0, p_1, ..., p_{\mu-1}, q_0, q_1, ..., q_{\eta-1}) = (p_0, p_1, ..., p_{\mu-1}, a_0 + vb_0, a_1 + vb_1, ..., a_{\eta-1} + vb_{\eta-1}) \in C$ olsun.

i. $\varpi = v$ olsun. $\varepsilon(v) = 1$ dir.

$\bar{\partial}$, parçalı devirli öteleme operatörü ve ξ, skew sabit devirli öteleme operatörü olsun. C, $\mathbb{Z}_4[x]/\langle x^\mu - 1\rangle \times R_1[x;\theta]/\langle x^\eta - v\rangle$ de skew sabit devirli kod olduğundan,

$$\begin{aligned}\xi(c) &= (\varepsilon(v)\, p_{\mu-1}, p_0, ..., p_{\mu-2}, v\theta(q_{\eta-1}), \theta(q_0), ..., \theta(q_{\eta-2})) \\ &= (p_{\mu-1}, p_0, ..., p_{\mu-2}, v(a_{\eta-1} + (2+3v)b_{\eta-1}), (a_0 + (2+3v)b_0), ..., (a_{\eta-2} + (2+3v)b_{\eta-2})) \\ &= (p_{\mu-1}, p_0, ..., p_{\mu-2}, va_{\eta-1} + 2vb_{\eta-1} + 3b_{\eta-1}, a_0 + 2b_0 + 3vb_0, ..., a_{\eta-2} + 2b_{\eta-2} + 3vb_{\eta-2}) \\ &= (p_{\mu-1}, p_0, ..., p_{\mu-2}, 3b_{\eta-1} + v(a_{\eta-1} + 2b_{\eta-1}), a_0 + 2b_0 + 3vb_0, ..., a_{\eta-2} + 2b_{\eta-2} + 3vb_{\eta-2})\end{aligned}$$

dir. Böylece ϕ_1 uygulanarak,

$$\phi_1(\xi(c)) = (p_{\mu-1}, p_0, ..., p_{\mu-2}, 3a_{\eta-1} + b_{\eta-1}, a_0 + 3b_0, ..., a_{\eta-2} + 3b_{\eta-2}, a_{\eta-1} + 3b_{\eta-1}, 3a_0 + b_0, ..., 3a_{\eta-2} + b_{\eta-2})$$

elde edilir. Diğer taraftan,

$\phi_1(c) = (p_0, p_1, ..., p_{\mu-1}, a_0 + 3b_0, a_1 + 3b_1, ..., a_{\eta-1} + 3b_{\eta-1}, b_0 + 3a_0, b_1 + 3a_1, ..., b_{\eta-1} + 3a_{\eta-1})$ dir. Buradan,

$$\bar{\partial}\phi_1(c) = (p_{\mu-1}, p_0, ..., p_{\mu-2}, b_{\eta-1} + 3a_{\eta-1}, a_0 + 3b_0, ..., a_{\eta-2} + 3b_{\eta-2}, a_{\eta-1} + 3b_{\eta-1}, b_0 + 3a_0, ..., b_{\eta-2} + 3a_{\eta-2})$$

bulunur.

Böylece $\phi_1(\xi(c)) = \bar{\partial}\phi_1(c)$ dir. Eğer $\mu = \eta$ ise $\phi_1(C)$, 2 indeksli $QC-$koddur. Eğer $\mu \neq \eta$ ise $\phi_1(C)$, 2 indeksli genelleştirilmiş $QC-$koddur.

$\varpi = 2+3v$ için ispat benzer şekilde görülmektedir.

ii. $\varpi = 3+2v$ olsun. $\varepsilon(3+2v)=1$ dir.

$\bar{\partial}$, parçalı devirli öteleme operatörü ve ξ, skew sabit devirli öteleme operatörü olsun. C, $\mathbb{Z}_4[x]/\langle x^{\mu}-1\rangle \times R_1[x;\theta]/\langle x^{\eta}-(3+2v)\rangle$ de skew sabit devirli kod olduğundan,

$$\begin{aligned}\xi(c) &= \left(\varepsilon(3+2v)\, p_{\mu-1}, p_0, ..., p_{\mu-2}, (3+2v)\theta(q_{\eta-1}), \theta(q_0), ..., \theta(q_{\eta-2})\right)\\ &= \left(p_{\mu-1}, p_0, ..., p_{\mu-2}, (3+2v)\left(a_{\eta-1}+(2+3v)b_{\eta-1}\right), \left(a_0+(2+3v)b_0\right), ..., \left(a_{\eta-2}+(2+3v)b_{\eta-2}\right)\right)\\ &= \left(p_{\mu-1}, p_0, ..., p_{\mu-2}, 3a_{\eta-1}+v\left(2a_{\eta-1}+b_{\eta-1}\right), a_0+2b_0+3vb_0, ..., a_{\eta-2}+2b_{\eta-2}+3vb_{\eta-2}\right)\end{aligned}$$

dir. Böylece ϕ_1 uygulanarak,

$$\phi_1(\xi(c)) = \left(p_{\mu-1}, p_0, ..., p_{\mu-2}, a_{\eta-1}+3b_{\eta-1}, a_0+3b_0, ..., a_{\eta-2}+3b_{\eta-2}, 3a_{\eta-1}+b_{\eta-1}, 3a_0+b_0, ..., 3a_{\eta-2}+b_{\eta-2}\right)$$

elde edilir. Diğer taraftan,

$\phi_1(c) = \left(p_0, p_1, ..., p_{\mu-1}, a_0+3b_0, a_1+3b_1, ..., a_{\eta-1}+3b_{\eta-1}, b_0+3a_0, b_1+3a_1, ..., b_{\eta-1}+3a_{\eta-1}\right)$ dir.

Buradan,

$$\bar{\partial}\phi_1(c) = \left(p_{\mu-1}, p_0, ..., p_{\mu-2}, a_{\eta-1}+3b_{\eta-1}, a_0+3b_0, ..., a_{\eta-2}+3b_{\eta-2}, b_{\eta-1}+3a_{\eta-1}, b_0+3a_0, ..., b_{\eta-2}+3a_{\eta-2}\right)$$

bulunur.

Böylece $\phi_1(\xi(c)) = \bar{\partial}\phi_1(c)$ dir. Eğer $\mu=\eta$ ise $\phi_1(C)$, 3 indeksli $QC-$koddur. Eğer $\mu\neq\eta$ ise $\phi_1(C)$, 3 indeksli genelleştirilmiş $QC-$koddur.

iii. $\varpi = 3$ olsun. $\varepsilon(3)=3$ tür.

$\wp$, skew quasi twisted öteleme operatörü ve ξ, skew sabit devirli öteleme operatörü olsun. C, $\mathbb{Z}_4[x]/\langle x^{\mu}-3\rangle \times R_1[x;\theta]/\langle x^{\eta}-3\rangle$ de skew sabit devirli kod olduğundan,

$$\begin{aligned}\xi(c) &= \left(\varepsilon(3)\, p_{\mu-1}, p_0, ..., p_{\mu-2}, 3\theta(q_{\eta-1}), \theta(q_0), ..., \theta(q_{\eta-2})\right)\\ &= \left(3p_{\mu-1}, p_0, ..., p_{\mu-2}, 3\left(a_{\eta-1}+(2+3v)b_{\eta-1}\right), \left(a_0+(2+3v)b_0\right), ..., \left(a_{\eta-2}+(2+3v)b_{\eta-2}\right)\right)\\ &= \left(3p_{\mu-1}, p_0, ..., p_{\mu-2}, 3a_{\eta-1}+2b_{\eta-1}+vb_{\eta-1}, a_0+2b_0+3vb_0, ..., a_{\eta-2}+2b_{\eta-2}+3vb_{\eta-2}\right)\end{aligned}$$

dir. Böylece ϕ_1 uygulanarak,

$$\phi_1(\xi(c)) = \left(3p_{\mu-1}, p_0, ..., p_{\mu-2}, 3a_{\eta-1}+b_{\eta-1}, a_0+3b_0, ..., a_{\eta-2}+3b_{\eta-2}, a_{\eta-1}+3b_{\eta-1}, 3a_0+b_0, ..., 3a_{\eta-2}+b_{\eta-2}\right)$$

elde edilir. Diğer taraftan,

$\phi_1(c)=(p_0,p_1,...,p_{\mu-1},a_0+3b_0,a_1+3b_1,...,a_{\eta-1}+3b_{\eta-1},b_0+3a_0,b_1+3a_1,...,b_{\eta-1}+3a_{\eta-1})$ dir.

Buradan,

$\wp\phi_1(c)=(3p_{\mu-1},p_0,...,p_{\mu-2},3a_{\eta-1}+b_{\eta-1},a_0+3b_0,...,a_{\eta-2}+3b_{\eta-2},a_{\eta-1}+3b_{\eta-1},3a_0+b_0,...,3a_{\eta-2}+b_{\eta-2})$

bulunur.

Böylece $\phi_1(\xi(c))=\wp\phi_1(c)$ dir. Eğer $\mu=\eta$ ise $\phi_1(C)$, 3 indeksli skew $QT-$ koddur. Eğer $\mu\neq\eta$ ise $\phi_1(C)$, 3 indeksli genelleştirilmiş skew $QT-$koddur.

Teorem 4.7.2. C, $\mathbb{Z}_4[x]/\langle x^{\mu}-\varepsilon(\varpi)\rangle\times R_1[x;\theta]/\langle x^{\eta}-\varpi\rangle$ de skew sabit devirli kod olsun. Bu durumda,

i. $\varpi=v,\varpi=2+3v$ olmak üzere eğer $\mu=\eta$ ise $\phi_2(C)$, 3 indeksli $QC-$ koddur. Eğer $\mu\neq\eta$ ise $\phi_2(C)$, 3 indeksli genelleştirilmiş $QC-$koddur.

ii. $\varpi=3$ olmak üzere eğer $\mu=\eta$ ise $\phi_2(C)$, 3 indeksli skew $QT-$ koddur. Eğer $\mu\neq\eta$ ise $\phi_2(C)$, 3 indeksli genelleştirilmiş skew $QT-$ koddur.

İspat: Teorem 4.7.1. e benzer şekilde ispatlanır.

4.8. $\mathbb{Z}_4R_1$ Üzerindeki Double Skew Sabit Devirli Kodlar

$k'=k_1+k_2$ olacak şekilde $k_1=\mu+2\eta$ ve $k_2=\bar{\mu}+2\bar{\eta}$ olsun. $\Re_{\mu,\eta,\bar{\mu},\bar{\eta}}$ aşağıda verilen halkayı temsil etsin.

$\mathbb{Z}_4[x]/\langle x^{\mu}-\varepsilon(\varpi)\rangle\times R_1[x;\theta]/\langle x^{\eta}-(\varpi)\rangle\times\mathbb{Z}_4[x]/\langle x^{\bar{\mu}}-\varepsilon(\varpi)\rangle\times R_1[x;\theta]/\langle x^{\bar{\eta}}-(\varpi)\rangle.$

Tanım 4.8.1.

i. C, $\Re_{\mu,\eta,\bar{\mu},\bar{\eta}}$ nin $R-$alt modülüdür.

ii. $\varpi=(\varpi_i+v\varpi_j)$ olsun. $i=0,1,...,\mu-1$ ve $\bar{i}=0,1,...,\bar{\mu}-1$ için $\theta(p_i)=p_i$, $\theta(\bar{p}_{\bar{i}})=\bar{p}_{\bar{i}}$, $(p_i,\bar{p}_{\bar{i}}\in\mathbb{Z}_4)$ olmak üzere eğer

$\left(p_0, p_1, ..., p_{\mu-1}, q_0, q_1, ..., q_{\eta-1}, \overline{p}_0, \overline{p}_1, ..., \overline{p}_{\overline{\mu}-1}, \overline{q}_0, \overline{q}_1, ..., \overline{q}_{\overline{\eta}-1}\right) \in C$ ise,

$$\begin{pmatrix} \varepsilon(\varpi)\theta(p_{\mu-1}), \theta(p_0), ..., \theta(p_{\mu-2}), \varpi\theta(q_{\eta-1}), \theta(q_0), ..., \theta(q_{\eta-2}) \\ \varepsilon(\varpi)\theta(\overline{p}_{\overline{\mu}-1}), \theta(\overline{p}_0), ..., \theta(\overline{p}_{\overline{\mu}-2}), \varpi\theta(\overline{q}_{\overline{\eta}-1}), \theta(\overline{q}_0)..., \theta(\overline{q}_{\overline{\eta}-2}) \end{pmatrix} \in C \text{ dir.}$$

i. ve ii. şartlarını sağlayan $\mathbb{Z}_4 R_1$ üzerinde k' uzunluğundaki C lineer koduna double skew sabit devirli kod denir.

$c = \left(p_0, p_1, ..., p_{\mu-1}, q_0, q_1, ..., q_{\eta-1}, \overline{p}_0, \overline{p}_1, ..., \overline{p}_{\overline{\mu}-1}, \overline{q}_0, \overline{q}_1, ..., \overline{q}_{\overline{\eta}-1}\right)$ kod sözü polinomlar cinsinden aşağıdaki şekilde yazılabilir.

$$c(x) = \begin{pmatrix} p_0 + p_1 x + ... + p_{\mu-1} x^{\mu-1}, \\ q_0 + q_1 x + ... + q_{\eta-1} x^{\eta-1}, \\ \overline{p}_0 + \overline{p}_1 x + ... + \overline{p}_{\overline{\mu}-1} x^{\overline{\mu}-1}, \\ \overline{q}_0 + \overline{q}_1 x + ... + \overline{q}_{\overline{\eta}-1} x^{\overline{\eta}-1} \end{pmatrix} = \left(p(x), q(x), \overline{p}(x), \overline{q}(x)\right) \in \mathfrak{R}_{\mu,\eta,\overline{\mu},\overline{\eta}}.$$

$r(x) = r_0 + r_1 x + ... + r_\alpha x^\alpha \in R_1[x;\theta]$, $\left(p(x), q(x), \overline{p}(x), \overline{q}(x)\right) \in \mathfrak{R}_{\mu,\eta,\overline{\mu},\overline{\eta}}$ olsun.

$\varepsilon(r(x)) = \varepsilon(r_0) + \varepsilon(r_1)x + ... + \varepsilon(r_\alpha)x^\alpha$ olmak üzere,

$r(x)\left(p(x), q(x), \overline{p}(x), \overline{q}(x)\right) = \left(\varepsilon(r(x))\, p(x), r(x) q(x), \varepsilon(r(x))\, \overline{p}(x), r(x)\overline{q}(x)\right)$

dir.

$c(x) = \left(p(x), q(x), \overline{p}(x), \overline{q}(x)\right)$ ise $xc(x)$, c nin $k_1 k_2$-skew sabit devir ötelemesidir.

Teorem 4.8.1. Bir C lineer kodunun double skew sabit devirli kod olması için gerek ve yeter şart C nin $\mathfrak{R}_{\mu,\eta,\overline{\mu},\overline{\eta}}$ nin sol $R_1[x;\theta]$ alt modülü olmasıdır.

İspat: [36] da ki Teorem 6. 4. ün ispatına benzer şekilde ispatlanır.

BÖLÜM 5. TARTIŞMA VE SONUÇ

$v^2=1$ olmak üzere, $\mathbb{Z}_2\mathbb{Z}_2[v]-$ lineer kodlar çalışılmıştır. Bu kodların üreteç ve kısmi kontrol matrisleri belirlenerek standart form elde edilmiştir.

$v^2=1$ olmak üzere, η tek olma durumunda $\mathbb{Z}_2\mathbb{Z}_2[v]-(v)-$ sabit devirli kodun üreteç polinomu ve en küçük geren kümesi verilmiştir. Ayrıca devirli ve sabit devirli kodların arasındaki ilişkiden yola çıkılarak, $\mathbb{Z}_2\mathbb{Z}_2[v]-(v)-$ sabit devirli kodun dual kodu belirlenmiştir.

$v^2=1$olmak üzere, $R_1=\mathbb{Z}_4+v\mathbb{Z}_4$ için R_1 ve $\mathbb{Z}_4R_1$ de skew sabit devirli kodlar çalışılmıştır. Bu kodların üreteç polinomları verilmiştir. Ayrıca $\mathbb{Z}_4R_1$ üzerindeki double skew sabit devirli kodlar verilmiştir.

KAYNAKLAR

[1] Fraleigh, J. B., A First Course in Abstract Algebra. Pearson Education, Boston, 2003.

[2] Çallıalp, F., Örneklerle Soyut Cebir, Birsen Yayınevi, 2013.

[3] Hungerford, Thomas W., Algebra, Springer, 2000.

[4] Çallıalp, F., Değişmeli Halkalar ve Modüller, Birsen Yayınevi, 2009.

[5] Wan, Zhe X., Finite Fields and Galois Rings, World Scientific, Singapore, 2003.

[6] MacDonald, Bernard R., Dekker, M., Finite Rings With Identity, New York, 1974.

[7] Dougherty, S.T., Liu, H., Independence of vectors in codes over rings, Des. Codes Cryptogr. 51: 55-68, 2009.

[8] Ling, S., Xing C., Coding Theory A First Course, Cambridge University Press, 2004.

[9] Roman, S., Advanced Lineer Algebra, Graduate Texts in Mathematics, Springer, 2000.

[10] Roman, S., Coding and Information Theory, Graduate Texts in Mathematics, Springer Verlag, 1992.

[11] Brouwer, A.E., Hamalainen, H. O., Ostergard, P. R. J., Sloane, N. J. A., Bounds on mixed binary / ternary codes, IEEE Trans. Inform. Theory, 44(1): 140-161, 1998.

[12] Borges, J., Fernandez - Cordoba, C., Pujol, J., Ri'fa, J., Villanueva, M., $\mathbb{Z}_2\mathbb{Z}_4$ – linear codes: generator matrices and duality, Des. Codes Cryptogr. 54: 167-179, 2010.

[13] Bilal, M., Borges, J., Dougherty, S.T., Fernandez – Cordoba, C., Optimal codes over $\mathbb{Z}_2 \times \mathbb{Z}_4$, VII Jornadas de Matematica Discreta y Algoritmica Castro Urdiales, Cantabria, 7-9 de julio de 2010.

[14] Fernandez – Cordoba, C., Pujol, J., Villanueva, M., $\mathbb{Z}_2\mathbb{Z}_4$ – linear codes: rank and kernel, Des. Codes Crypt. 56: 43-59, 2010.

[15] Bilal, M., Borges, J., Dougherty, S.T., Fernandez – Cordoba, C., Maximum distance seperable codes over $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_4$, Des. Codes Crypt. 61: 31-40, 2011.

[16] Rifa – Pous, H., Rifa J., Ronquillo, L., $\mathbb{Z}_2\mathbb{Z}_4$ – Additive perfect codes in steganography, Adv. Math. Commun., 5(3): 425-433, 2011.

[17] Aydoğdu, İ., Şiap., İ., The Structure of $\mathbb{Z}_2\mathbb{Z}_{2^s}$ – additive codes: bounds on the minimum distance, Appl. Math. Inform. Sci. 7(6): 2271-2278, 2013.

[18] Aydoğdu, İ., Abualrub, T., Şiap., İ., On $\mathbb{Z}_2\mathbb{Z}_2[u]$ – additive codes, International Journal of Computer Mathematics, 92(9): 1806-1814, 2015.

[19] Wan, Zhe X., Quaternary codes, İçinde: Quaternary Linear Codes and Their Generator Matrices, World Scientific Publishing Co. Pte. Ltd., 1-8.

[20] Özzaim, N. T., Sonlu halkalar üzerindeki kodların yapısından yararlanarak yeni lineer kodların bulunması. Sakarya Üniversitesi, Fen Bilimleri Enstitüsü, Matematik Bölümü, Doktora Tezi, 2017.

[21] Borges, J., Fernandez-Cordoba, C., Ten – Valls R., $\mathbb{Z}_2\mathbb{Z}_4$ – Additive cyclic codes, generator polynomials and dual codes. IEEE Trans. Inf. Theory, 62(11): 6348-6354, 2016.

[22] Abualrub, T., Şiap, İ., Aydın, N., $\mathbb{Z}_2\mathbb{Z}_4$ – Additive cyclic codes. IEEE Trans. Inf. Theory, 60(3): 1508 – 1514, 2014.

[23] Abualrub, T., and Şiap İ., Cyclic codes over the rings $\mathbb{Z}_2 + u\mathbb{Z}_2$ and $\mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2$, Des. Codes Cryptogr.,42: 273-287, 2007

[24] Al – Ashker, M., and Hamoudeh, M., Cyclic codes over $\mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2 + ... + u^{k-1}\mathbb{Z}_2$, Turk. J. Math., 35: 737-749, 2011.

[25] Bonnecaze, A., Udaya, P., Cyclic codes and self dual codes over $\mathbb{F}_2+u\mathbb{F}_2$, IEEE Trans. Inf. Theory, 45(4): 1250-1255, 1999.

[26] Aydoğdu, İ., Abualrub, T., Şiap, İ., $\mathbb{Z}_2\mathbb{Z}_2[u]-$ Cyclic and constacyclic codes, IEEE Trans. Inf. Theory, 63(8): 4883-4893, 2017.

[27] Şiap, İ.,Abualrub, T., Ghrayeb, A., Cyclic DNA codes over the ring $\mathbb{F}_2[u]/\langle u^2-1\rangle$ based on the deletion distance. Journal of Franklin Institue, 346: 731-740, 2009.

[28] Srinivasulu, B., Bhaintwal, M., $\mathbb{Z}_2(\mathbb{Z}_2+u\mathbb{Z}_2)-$Additive cyclic codes and their duals. Discrete Mathematics, Algorithms and Applications, 8(2), 2016.

[29] Boucher, D., Geiselmann, W., Ulmer, F., Skew cyclic codes. AAECC, 18(4): 379-389, 2007.

[30] Şiap, İ., Abualrub, T., Aydın, N., Seneviratne, P., Skew cyclic codes of arbitrary length. Int. J. Inf. and Coding Theory, 2(1): 10-20, 2011.

[31] Gao, J., Skew cyclic codes over $\mathbb{F}_p+v\mathbb{F}_p$. Journal of Applied Mathematics and Informatics, 31(3-4): 337-342, 2013.

[32] Gürsoy, F., Şiap, İ., Yıldız, B., Construction of skew cyclic codes over $\mathbb{F}_q+v\mathbb{F}_q$. Advances in Math. of Communication, 8(3): 313-322, 2014.

[33] Özen, M., Özzaim, N.T., İnce, H., Skew quasi cyclic codes over $\mathbb{F}_q+v\mathbb{F}_q$, Journal of Algebra and Its Applications 18(04), 2019.

[34] Jitman, S., Ling. S., Udomkavanich, P., Skew constacyclic over finite chain rings, Adv. Math. Commun. , 6(1), 2010.

[35] Sharma, A., Bhaintwal, M., A class of skew- constacyclic codes over $\mathbb{Z}_4+u\mathbb{Z}_4$, Int. J. Information and Coding Theory,4(4): 289-303, 2017.

[36] Melakhessou, A., Aydın, N., Hebbache, Z., Guenda, K., $\mathbb{Z}_q(\mathbb{Z}_q+u\mathbb{Z}_q)-$ linear skew constacyclic codes, J. Algebra Comb. Discrete Appl., 7(1): 85-101, 2019.

[37] Özen, M., Uzekmek, F. Z., Aydın, N., Özzaim, N.T., Cyclic and some constacyclic codes over the ring $\frac{\mathbb{Z}_4[u]}{\langle u^2-1\rangle}$, Finite Fields Appl., 38: 27-39, 2016.

ÖZGEÇMİŞ

Ceyda Cebe, 18. 09. 1994 de Sakarya'da doğdu. İlk, orta ve lise eğitimini Sakarya'da tamamladı. 2012 yılında Hacı Zehra Akkoç Kız Lisesi'nden mezun oldu. 2013 yılında başladığı Sakarya Üniversitesi Fen Edebiyat Fakültesi Matematik Bölümü'nü 2017 yılında bölüm ikincisi olarak bitirdi. Aynı yıl içerisinde Sakarya Üniversitesi Matematik Anabilim Dalında Cebir ve Sayılar Teorisi Bilim Dalında yüksek lisansa başladı.