T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

MANNHEİM METRİĞİNE GÖRE GAUSS TAM SAYILAR HALKASI ÜZERİNDE LİNEER KODLARIN YAPISI

YÜKSEK LİSANS TEZİ

Murat GÜZELTEPE

Enstitü Anabilim Dalı : MATEMATİK

Tez Danışmanı : Yrd. Doç. Dr. Mehmet ÖZEN

Haziran 2007

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

MANNHEİM METRİĞİNE GÖRE GAUSS TAM SAYILAR HALKASI ÜZERİNDE LİNEER KODLARIN YAPISI

YÜKSEK LİSANS TEZİ

Murat GÜZELTEPE

Enstitü Anabilim Dalı : MATEMATİK

Bu tez 19/ 06 /2007 tarihinde aşağıdaki jüri tarafından Oybirliği ile kabul edilmiştir.

Yrd. Doç. Dr. Mehmet ÖZEN	Doç. Dr. İrfan ŞİAP	Yrd. Doç. Dr. Yalçın YILMAZ
Jüri Başkanı	Üye	Üye

TEŞEKKÜR

Tezin hazırlanması aşamasında bana her türlü desteği veren danışman hocam Sayın Yrd. Doç. Dr. Mehmet ÖZEN `e ve bölümümdeki hocalarıma teşekkürü bir borç bilirim.

Ayrıca eğitim hayatım boyunca maddi ve manevi desteklerini esirgemeyen aileme ve eşim Süheyla GÜZELTEPE' ye de teşekkür ediyorum.

İÇİNDEKİLER

SİMGELER VE KISALTMALAR

$\sigma(z)$: Hata tespit polinomu

$\mathbb{Z}$: Tamsayılar Kümesi

π : Kompleks sayı

π^* : π nin eşleniği

F_q : q elemanlı sonlu cisim

$ord(a)$: a nın mertebesi

$\phi(n)$: Euler ϕ fonksiyonu

OMEC : Bir Mannheim hatasını düzeltebilen kodlar

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

ÖZET

Anahtar Kelimeler: Lineer kodlar, devirli kodlar, Mannheim metrik, bazı halkalar üzerinde Mannheim metriği ile lineer kodlar.

Üç bölüm halinde düzenlenen bu çalışmanın birinci bölümünde cebirsel tanım ve teoremler, Hamming metriğine göre lineer kodlar ve dekodlamaları ve yine bu metrik kullanılarak sonlu cisimler üzerinde t hata düzelten BCH kodları verilmektedir.

İkinci bölümde cisimler üzerinde Mannheim metriği kullanılarak t hata düzelten BCH kodları, dekodlamaları ve bu kodların ağırlık sayaçları verilmektedir.

Üçüncü bölümde Mannheim metriği kullanılarak bazı sonlu halkalar üzerinde devirli kodlar bulundu ve bu kodlara örnekler verildi.

STRUCTURE OF LINEAR CODES OVER GAUSSIAN INTEGERS RING WITH RESPECT TO MANNHEIM METRIC

SUMMARY

Keywords: Linear codes, cyclic codes, Mannheim metrice, linear codes over some rings with Mannheim metrices

This study consists of three chapters. First chapter includes algebric definitions and theorems, linear codes and decoding, t error correcting BHC codes over finite fields with respect to Hamming metric.

In the second chapter, t-error correcting BCH codes are introduced and decoding with respect to Mannheim metric is studied.

In the third chapter, cyclic codes over some finite rings with respect to Mannheim metric are studied and some examples are worked out.

BÖLÜM 1 GİRİŞ

1.1. Cebirsel Tanımlar

Tanım 1.1.1: S boş olmayan herhangi bir küme olsun. S kümesinin elemanlarından oluşan her sıralı ikiliye S de bir ve yalnız bir eleman karşılık getiren bir fonksiyona S üzerinde bir ikili işlem denir. Bu işlem $*$ sembolü ile gösterildiğinde;

$$S \text{ x } S \to S$$
$$(a,b) \to a * b$$

ile tanımlanır.

Tanım 1.1.2: G bir küme ve $*$, G de tanımlı bir ikili işlem olsun. Eğer aşağıdaki özellikler * işlemi tarafından sağlanıyorsa (G, $*$) ikilisine bir grup denir.

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

ii. $\forall a \in G$ için $a*e = e*a = a$ olacak biçimde $e \in$ G vardır.(e etkisiz eleman)

iii. $a \in G$ için $a * a' = a' * a = e$ olacak biçimde $a' \in G$ vardır.(a', a'nın tersidir)

Ayrıca, G bir grup ve $\forall a,b,c \in G$ için $a*b = b*a$ sağlanıyorsa G ye bir değişmeli (Abel) grup denir.

Tanım 1.1.3: G bir grup ve $\varnothing \neq H \subseteq G$ olsun. H, G deki işleme göre kapalı ise H ye G nin bir alt grubu denir ve $H \leq G$ ile gösterilir. G sonlu bir grup ise G nin elemanlarının sayısına G nin mertebesi denir.

Tanım 1.1.4: $R \neq \varnothing$ kümesi üzerinde tanımlı iki ikili işlem '+' ve '.' olsun. Aşağıdaki aksiyomları sağlayan (R,+,.) cebirsel yapısına bir halka denir.

H1: (R,+) bir değişmeli gruptur.
H2: '.' işleminin R de birleşme özelliği vardır.
H3: '.' işleminin + işlemi üzerine sağdan ve soldan dağılma özellikleri vardır.

Tanım 1.1.5: R ve R' iki halka olsun. $\phi : R \to R'$ fonksiyonu;

i. birebir ve örten,
ii. $\forall a, b \in R$, $\phi(a+b) = \phi(a) + \phi(b)$ ve $\phi(a.b) = \phi(a).\phi(b)$

koşullarını sağlarsa, ϕ ye R den R' ne bir izomorfizma denir ve $R \cong R'$ ile gösterilir.

Tanım1.1.6: Bir halkada çarpma işlemi değişmeli ise bu halkaya değişmeli halka denir. Bir R halkasında $\forall x \in R$ için 1.x=x.1=x olacak biçimde 1 elemanı varsa R ye birimli halka denir. R birimli bir halka olsun. $u \in R$ nin, R de tersi varsa u ya R nin bir tersinir (birimsel) elemanı denir.

Tanım 1.1.7: R değişmeli, birimli bir halka ve $\forall u \in R-\{0\}$ elemanı tersinir ise R ye bir cisim denir.

Tanım 1.1.8: R bir halka ve $S \subseteq R$ olsun. S, R deki işlemlere göre bir halka ise S ye R nin bir alt halkası denir.

Tanım 1.1.9: $a,b \in R$ için $a \neq 0$ ve $b \neq 0$ olduğunda ab=0 oluyorsa, a ve b ye R nin sıfır bölenleri denir. Eğer $\forall a,b \in R$ için ab=0 iken a= 0 veya b=0 ise R ye sıfır bölensiz halka denir.

Teorem 1.1.1: [1] $\mathbb{Z}_n$ halkasının sıfır bölenleri n ile aralarında asal olmayan elemanlardır.

Tanım 1.1.10: Bir R halkasında $\forall a \in R$ için na=0 sağlayan pozitif n tamsayılarının en küçüğüne halkanın karakteristiği denir ve kar(R)=n ile gösterilir. Eğer böyle bir n tamsayısı yoksa R ye sıfır karakteristikli halka denir.

Teorem 1.1.2: [1] $\mathbb{Z}$ de (n,b)=1ve (n,c)=1 aralarında asal ise (n,bc)=1 dir.

Tanım 1.1.11: R bir halka ve $\varnothing \neq I \subseteq R$ olsun. I alt kümesi

i. $\forall a,b \in I$ için $a-b \in I$
ii. $\forall a \in I$ ve $\forall r \in R$ için $ra \in I$ veya $ar \in I$ özelliklerini sağlıyorsa I ya R nin bir

ideali denir.

Tanım 1.1.12: $\mathbb{Z}[i] = \{a+bi : a,b \in \mathbb{Z}\}$ tamlık bölgesine Gauss tamsayılar bölgesi denir.

Önerme 1.1.1: [1] $\mathbb{Z}[i]$ Gauss tamsayılar bölgesi bir Euclid bölgesidir.

Tanım 1.1.13: R değişmeli ve birimli bir halka ve M de R nin (1) den farklı bir ideali olsun. R nin, M yi kapsayan M ve R den başka hiçbir ideali yoksa, M ye R nin bir maksimal ideali denir.

Önerme 1.1.2: [1] Birimli ve değişmeli bir R halkasının bir M idealinin maksimal olması için gerek ve yeter koşul R/M bölüm halkasının bir cisim olmasıdır.
M nin bir maksimal ideal olması için gerek ve yeter koşul R/M nin bir cisim olmasıdır.

Tanım 1.1.14: R bir halka, x bir bilinmeyen ve $a_0, a_1, a_2, ..., a_n$ ler R nin elemanları olmak üzere,

$$a_0 + a_1 x + a_2 x^2 + ... + a_n x^n$$

şeklindeki bir ifadeye R den katsayılı bir polinom denir. R den katsayılı tüm polinomların kümesi R[x] ile gösterilir.

Önerme1.1.3: [1] R bir halka ise R[x] de bir halkadır.

Önerme1.1.4: [1] F bir cisim ve $f \in F[x]$, $d^0 f \geq 1$ olsun. $(f) = f(x)F[x]$ temel ideali için $\frac{F[x]}{(f)}$ bölüm halkasının tam temsilciler sistemi olarak $d^0 r < d^0 f$ olan $r \in F[x]$ polinomları alınabilir.

Tanım 1.1.15: $0 \neq$ f(x), $0 \neq$ h(x) $\in$ F[x] olsun. g(x) $|$ f(x) ve g(x) $|$ h(x) ise g(x) polinomuna, f(x) ve h(x) polinomlarının ortak böleni denir. Yine

i. d(x) $|$ f(x) ve d(x) $|$ h(x)

ii. g(x) $|$ f(x) ve g(x) $|$ h(x) $\Rightarrow$ g(x) $|$ d(x)

ise o zaman d(x) polimonuna f(x) ve h(x) polinomlarının en büyük ortak böleni (ebob) denir ve (f(x),h(x))=d(x) biçiminde gösterilir.

Teorem 1.1.3: [1] F[x] içinde (f(x),h(x))=d(x) olsun. Buna göre

d(x)=s(x)f(x)+t(x)h(x)

olacak biçimde s(x),t(x) $\in$ F[x] vardır.

Tanım 1.1.16: (f(x),h(x))=1 ise f(x) ve h(x) aralarında asaldır.

Tanım 1.1.17: $f(x) \in$ F[x] olsun. $f(x)$ polinomu F[x] içinde pozitif dereceli polinomların çarpımı olarak yazılabilirse $f(x)$, F[x]de çarpanlarına ayrılabilir denir.

$$f(x) = p_1(x)p_2(x)...p_m(x)$$

biçiminde ise $p_1(x), p_2(x), ..., p_m(x)$ polinomlarına çarpan, $f(x) = p_1(x)p_2(x)...p_m(x)$ ifadesine de f(x) polinomunun F[x] de çarpanlara ayrılışı denir.

Teorem 1.1.4: [1] F[x] içindeki pozitif dereceli her polinomun bir indirgenemez çarpanlara ayrılışı vardır.

Teorem 1.1.5: [1] p(x),f(x), g(x) $\in$F[x] ve p(x), F[x] de indirgenemez olsun. Buna göre,

p (x)|f(x).g(x) $\Rightarrow$p(x)|f(x) veya p(x)|g(x)

dir.

Teorem 1.1.6: [1] F[x] in bir $\langle p(x)\rangle \neq 0$ idealinin maksimum olması için gerek ve yeter şart $p(x)$ in F üzerinde indirgenemez (asal) olmasıdır.

Tanım 1.1.18: R bir halka ve M bir toplamsal değişmeli grup olsun. Modül çarpımı

$$M \times R \to M$$
$$(m, r) \to mr$$

dönüşümü aşağıdaki şartları sağlarsa M ye bir sağ R-modül denir.

i. $\forall m \in M, \forall r_1, r_2 \in R \quad için \quad (mr_1)r_2 = m(r_1r_2)$

ii. $\forall m_1, m_2 \in M, \forall r \in R \quad için \quad (m_1 + m_2)r = m_1r + m_2r$

iii. $\forall m \in M, \forall r_1, r_2 \in R \quad için \quad m(r_1 + r_2) = mr_1 + mr_2$

Ayrıca

iv. $1_R \in R \quad ve \quad m.1_R = m, \forall m \in M$

sağlıyorsa M ye birimli R-modül denir.

1.2. Lineer Kodlar ve Dualleri

Bu kısımda, hata düzelten kodlar teorisinde çok önemli bir sınıf teşkil eden lineer kodlar hakkında bilgi verilecek. $V(n,q)$, q elemanlı sonlu bir cisim olan F_q üzerinde tanımlanmış n uzunluğundaki vektör uzayı olsun.

Tanım 1.2.1: $V(n,q), F_q$ üzerinde n zunluğundaki bütün vektörlerin kümesi olsun. Bu küme bir vektör uzaydır. $C \subset V(n,q)$ ve C, $V(n,q)$ nun k boyutlu bir alt vektör uzayı ise C ye n uzunluğunda, k boyutlu bir lineer kod denir ve kısaca [n , k] ile gösterilir.

C nin elemanlarına ise kodsöz denir. Bir kodsözdeki sıfırdan farklı bileşenlerin sayısına o kodsözün ağırlığı denir. İki kodsözün farklarının ağırlığına ise bu iki kodsöz arasındaki uzaklık denir. C deki kodsözlerin sıfırdan farklı en küçük ağırlığına C nin Hamming ağırlığı denir ve $w(C)$ ile gösterilir. Ayrıca C deki sıfırdan farklı en küçük uzaklığa ise C nin minimum uzaklığı denir ve $d(C)$ ile gösterilir. Lineer kodlarda $d(C) = w(C)$ dir. Eğer C kodunun minimum mesafesi d ise bu kod kısaca [n , k , d] şeklinde gösterilir.

Bir lineer kodun üreteç matrisi:

Bir lineer kod bir vektör uzay olduğundan, lineer kod vektör uzayın tabanı kullanılarak tanımlanabilir.

Tanım 1.2.2: C bir [n,k] kodu olsun. Satırları C nin bir tabanı olan k x n tipindeki D matrisine C kodunun üreteç matrisi denir.
Elementer satır işlemlerini (satırların yerlerini değiştirmek, satırları sıfırdan farklı bir sakaler ile çarpmak ve sakalerle çarpılmış bir satırı diğerine eklemek) bir matrise uygularsak, bu matrisin satır uzayı (satırların lineer kombinasyonlarından oluşan vektör uzay) değişmaz.

Teorem 1.2.1: [2] C bir lineer [n,k] kodu olsun. Herhangi bir k koordinat yerleri verilsin, bu yerler üzerinde C ye denk olan sistematik bir kod vardır.

Teorem 1.2.2: [2] C_1 ve C_2 kodu, sırası ile D_1 ve D_2 üreteç matrislerine sahip iki lineer kod olsun. C_1 in C_2 ye denk olması için gerek ve yeter şart D_1 matrisinin D_2 matrisine denk olmasıdır.

Tanım 1.2.3: C kodunu üreten D matrisi elementer satır veya sütun işlemleri yapılarak G=(I_k|A) şeklinde yazılabilir. D ye denk olan bu G matrisine C kodunu üreten standart form matrisi denir. Burada I_k, k boyutlu birim matristir.

Bir lineer kodun duali:

$V(n,q)$ bir vektör uzay ve $u=(u_1,u_2,...,u_n), v=(v_1,v_2,...,v_n)\in V(n,q)$ olmak üzere u ile v nin iç çarpımı;

$$<u,v>=u_1v_1+...+u_nv_n$$

şeklinde tanımlanır.

Tanım 1.2.4: C bir [n,k] lineer kodu olsun.

$$C^{\perp}=\{x\in V(n,q):<x,c>=0,\forall c\in C\}$$

kümesine C nin dual kodu denir.

Teorem 1.2.3: [2]

1) G matrisi C kodu için bir üreteç matrisi ise

$C^{\perp}=\{x\in V(n,q):<x,c>=0,\forall c\in C\}$

olur.

2) Bir lineer [n,k] kodunun duali olan $C^{\perp}$ kodu da bir [n,n-k] lineer koddur.

3) Her lineer C kodu için $(C^{\perp})^{\perp}=C$ olur.

Tanım 1.2.5: Eğer C [n,k] lineer kodunun üreteç matrisi $k \times n$ boyutlu G matrisinin standart formu G=($I_k \mid A$) ise $C^{\perp}$ in üreteci H=(-$A^T \mid I_{n-k}$) olur. H matrisine C kodun kontrol (parity check) matrisi denir.

1.3. Lineer Kodlarda Dekodlama

Sendrom dekodlaması:

Tanım 1.3.1: C bir [n,k] kodu ve H da bu kodun kontrol matrisi olsun. Her $x \in$ V(n,q) için $x \,.\, H^T$ ye x in sendromu denir.

Sendromun özellikleri [2]

x in sendromu S= $x \,.\, H^T$ olarak hesaplanırsa;

I. S bir n-k boyutlu sütun matrisidir,

II. S=0 olması için gerek ve yeter koşul x in bir kodsöz olmasıdır.

III. Sendrom kontrol matrisinin t. sütununa eşitse bu kodsözde bir hata vardır. Bu hata kodsözün t. bileşeninde meydana gelmiştir.

1.4. Devirli ve BCH Kodları

Devirli kodlar:

Tanım 1.4.1 $C \subset V(n,q)$ lineer kodu için, eğer

$$c_0 c_1 ... c_{n-1} \in C \text{ iken } c_{n-1} c_0 c_1 ... c_{n-2} \in C$$

oluyorsa bu lineer koda bir devirli kod denir.

F_q üzerinde $n.$ dereceden polinomlar ile n uzunluğunadaki q elemanlı vektör uzayı arasında bir izomorfizma kurulabilir. $R_n = F_q[x] / \langle x^n - 1 \rangle$ olmak üzere $\Phi : V(n,q) \to R_n$, $\Phi((c_0, c_1, ..., c_{n-1})) = c_0 + c_1 x + ... + c_{n-1} x^{n-1}$ şeklinde tanımlanan Φ fonksiyonu $V(n,q)$ ile R_n arasında bir izomorfizmadır. Eğer C

$$R_n = \frac{F_q[x]}{\langle x^n - 1 \rangle}$$

halkasının bir ideali ise bir devirli kod olur.

R_n, F_q üzerinde derecesi n den küçük olan tüm polinomların kümesidir. R_n de toplama polinomların toplamı ve çarpma da polinomların çarpımıdır. Tüm polinomlar $x^n - 1$ modülosuna göre olacaktır. Eğer

$$c_0 c_1 ... c_{n-1} \to c_{n-1} c_0 c_1 ... c_{n-2}$$

devirli kaydırma (shift) altında C lineer kodu kapalı ise devirli koddur. Bu durumda ise C bütün kaydırmalar altında kapalıdır. Yani

$$c_0 c_1 ... c_{n-1} \to c_k ... c_{n-1} c_0 c_1 ... c_{k-1}$$

olur.

Bir devirli kodun üreteç polinomu:

Teorem 1.4.1: [2] C, R_n de bir ideal olsun. Bu durumda C, n uzunluğunda bir devirli kod olur.

1) C de derecesi minimum olan tek bir monik polinom (g(x)) vardır. Bu polinom C=$\langle g(x) \rangle$ şeklinde C yi üretir ve bu polinoma C nin üreteç polinomu denir.

2) Üreteç polinomu olan g(x), x^n -1 i böler.

3) Eğer der(g(x))=r ise C'nin boyutu n-r olur. Yani

C=$\langle g(x) \rangle$ ={r(x)g(x): der(r(x))<n-r}

dir.

4) Eğer $g(x) = g_0 + g_1 x + \cdots + g_r x^r$ ise bu durumda $g_0 \neq 0$ ve C nin üreteç matrisi

$$G = \begin{pmatrix} g_0 & g_1 & g_2 & \cdots & g_r & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & g_2 & \cdots & g_r & 0 & \cdots & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & \cdots & g_r & & \vdots \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & & \ddots & 0 \\ 0 & 0 & \cdots & 0 & g_0 & g_1 & g_2 & \cdots & g_r \end{pmatrix}$$

olur.

Bir devirli kodun kontrol polinomu

Eğer g(x) polinomu R_n de bir [n,n-r] devirli kodunun üreteç polinomu ise g(x), x^n -1 i böler. Yani

x^n -1=g(x)h(x)

olur. Burada h(x) derecesi $n-r$ olan bir polinomdur ve bu polinoma C nin kontrol polinomu denir.

Teorem 1.4.2: [2] h(x) R_n de C devirli kodunun kontrol (parity-check) polinomu olsun.

1) C kodu;

C=$\{p(x) \in R_n : p(x)h(x) \equiv 0 \mod x^n - 1\}$

şeklinde tanımlanır.

2) Eğer $h(x) = h_0 + h_1 x + \cdots + h_{n-r} x^{n-r}$ ise bu durumda C nin kontrol (parity check) matrisi

$$H = \begin{pmatrix} h_{n-r} & \cdots & h_0 & 0 & 0 & \cdots & 0 \\ 0 & h_{n-r} & \cdots & h_0 & 0 & \cdots & 0 \\ 0 & 0 & h_{n-r} & \cdots & h_0 & & \vdots \\ \vdots & \vdots & \ddots & \ddots & \cdots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & h_{n-r} & \cdots & h_0 \end{pmatrix}$$

olur.

3) C nin diki olan $C^{\perp}$ kodunun boyutu r dir ve devirlidir. $C^{\perp}$ devirli kodunun üreteç polinomu;

$$h^{\perp} = h_0^{-1} x^{n-r} h(x^{-1}) = h_0^{-1}(h_0 x^{n-r} + h_1 x^{n-r-1} + \cdots + h_{n-r})$$

dir.

BCH kodları:

Bir devirli kod, bu kodu üreten üreteç polinomunun sıfırları (kökleri) cinsinden yazılabilir. Eğer $\alpha_1, \alpha_2, \alpha_3, ..., \alpha_u$ F_q üzerinde birimin n. dereceden kökleri ise o zaman bu kod;

$$C = \{p(x) \in R_n : p(\alpha_1) = 0, ..., p(\alpha_u) = 0\}$$

bir devirli koddur ve bu kodun g(x) üreteç polinomu F_q üzerinde $\alpha_1, \alpha_2, \alpha_3, ..., \alpha_u$ nun farklı minimal polinomlarının çarpımıdır. Böylece g(x) in sıfırları için birimin n. dereceden kökleri kullanılarak kodlar oluşturulabilir. F_q üzerinde indirgenemez çarpanlarda

$$x^n - 1 = \prod_i m_i(x)$$

x^n-1 in çarpımsal şeklidir ve eğer α, F_q üzerinde birimin n. dereceden ilkel bir kökü (bkn sayfa 49) ise bu durumda $m_i(x)$ polinomunun kökleri aşağıdaki gibi eşleniktir:

$$\{\alpha^i, \alpha^{iq}, ..., \alpha^{iq^{d-1}}\}.$$

Burada d, $iq^d \equiv i$ mod n olacak şekilde en küçük tamsayıdır. Bu

$$C_i = \{i, qi, .., q^{d-1}i\}$$

kümesine n modülüne göre q nun i. devresel denklik sınıfı (cyclotomic coset) denir. Böylece

$$m_i(x) = \prod_{j \in C_i} (x - \alpha^j)$$

olur.

Teorem 1.4.3: [2] (BCH Sınırı) α , F_q üzerinde birimin n. dereceden kökü olsun. C, R_n de bir devirli kod ve bu kodun üreteç polinomu olan g(x), F_q üzerinde en küçük dereceli monik polinom olsun. $b \geq 0$ olmak üzere ardışık $\delta - 1$ sayıdaki

$$\alpha, \alpha^{b+1}, ..., \alpha^{b+\delta-2}$$

elemanları g(x) polinomunun sıfırları arasında ise C devirli kodun minimum uzaklığı en az δ kadardır.

Teorem 1.4.4: [2] α , F_q üzerinde birimin n. dereceden kökü ise C, R_n de bir devirli kod ve bu kodun üreteç polinomu olan g(x), F_q üzerinde en küçük dereceli monik polinom olsun. r ve n aralarında asal ve $b \geq 0$ olmak üzere p(x) polinomunun δ-1 tane sıfırı vardır. g(x) in sıfırları

$$\alpha^b, \alpha^{b+r}, ..., \alpha^{b+(\delta-2)r}$$

dır. Bu durumda C kodunun minimum mesafesi en az δ olur.

Tanım 1.4.2: (BCH Kod) α , F_q üzerinde ilkel bir kök, p(x), F_q üzerinde en küçük dereceli bir monik polinom ve p(x) polinomunun köklerinin sayısı $\delta - 1$ tane $\{\alpha^b, \alpha^{b+r}, ..., \alpha^{b+(\delta-2)r}\}$ $b \geq 0, \delta \geq 1$ olsun. Bu durumda

$$\text{g(x)= } okek\{m_b(x), m_{b+1}(x), ..., m_{b+\delta-2}(x)\}$$

olur. Üreteç polinomu g(x) olan n uzunluğundaki $B_q(n, \delta, \alpha, b)$ q-lu devirli koduna dizayn mesafesi δ olan BCH kodu denir.b=1 ise $B_q(n, \delta, \alpha) = B_q(n, \delta, \alpha, 1)$ ifadesi sınırlı bir BCH kod olur. α cismin bir ilkel elemanı ise $s \geq 1$ için $n = q^s - 1$ olur ve bu durumda $B_q(n, \delta, \alpha, b)$ ya bir ilkel BCH kod denir.

Teorem 1.4.5: [2] δ dizayn mesafeli, n uzunluğundaki q-lu bir BCH kod için boy($B_q(n,\delta,\alpha,b)$) $\geq n-(\delta-1)o_n(q)$ ve $d(B_q(n,\delta,\alpha,b)) \geq \delta$ parametrelerine sahiptir. Burada $o_n(q)$ modn ye göre q nun mertebesidir. BCH kodun tanımından

$$B_q(n,\delta,\alpha,b)=\{p(x)\in R_n : p(\alpha^b)=p(\alpha^{b+1})=\cdots=p(\alpha^{b+\delta-2})=0\}$$

olur ve eğer $[\alpha^i]$, F_q^s de bir sütun vektörü, x^n-1 in F_{q^s} cisim genişlemesindeki α^i elemanı ile benzer ise bu durumda $s(\delta-1)$ satırlı

$$H=\begin{pmatrix} 1 & [\alpha^b] & [\alpha^{2b}] & \cdots & [\alpha^{(n-1)b}] \\ 1 & [\alpha^{b+1}] & [\alpha^{b(b+1)}] & \cdots & [\alpha^{(b+1)(n-1)}] \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & [\alpha^{b+\delta-2}] & [\alpha^{2(b+\delta-2)}] & \cdots & [\alpha^{(n-1)(b+\delta-2)}] \end{pmatrix}$$

matrisi kontrol matrislerinin tüm kümeleri formundadır ve herhangi bir bağımlı satır çıkarıldığında geriye kalan matris $B_q(n,\delta,\alpha,b)$ için bir kontrol matrisidir.

1.5. BCH Kodlarını Dekodlama

C, bir [n,k,d] binary BCH kod ve δ dizayn mesafesi bir tek sayı olsun. Gelen kodsöz $c = c_0 c_1 ... c_{n-1}$ transferinde bozulan vektör y=c+e olarak ulaşsın. Burada e= $e_0 e_1 ... e_{n-1}$ hata vektörüdür. Dekodlama 3 aşamada yapılabilir.

1. Sendromun hesaplanması,
2. Hatanın yerini tespit eden $\sigma(z)$ polinomunun bulunuşu,
3. $\sigma(z)$ nin köklerinin bulunuşu.

1. Sendromun hesabı: [2] Kontrol matrisi

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^3 & \alpha^6 & \cdots & \alpha^{3(n-1)} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & \alpha^{\delta-2} & \alpha^{2(\delta-2)} & \cdots & \alpha^{(\delta-2)(n-1)} \end{bmatrix}$$

şeklindedir. $c(x) = \sum c_i x^i$, $e(x) = \sum e_i x^i$ ve $y(x) = \sum y_i x^i$ olsun. y nin sendromu

$$S = H.y^{tr} = H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^3 & \alpha^6 & \cdots & \alpha^{3(n-1)} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & \alpha^{\delta-2} & \alpha^{2(\delta-2)} & \cdots & \alpha^{(\delta-2)(n-1)} \end{bmatrix} \begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_{n-1} \end{bmatrix}$$

$$= \begin{bmatrix} \sum y_i \alpha^i \\ \sum y_i \alpha^{3i} \\ \vdots \\ \sum y_i \alpha^{(\delta-2)i} \end{bmatrix} = \begin{bmatrix} y(\alpha) \\ y(\alpha^3) \\ \vdots \\ y(\alpha\delta - 2) \end{bmatrix} = \begin{bmatrix} A_1 \\ A_3 \\ \vdots \\ A_{\delta-2} \end{bmatrix}$$

şeklinde hesaplanır. Burada $A_l = y(\alpha^l)$ ve $A_{2r} = y(\alpha^{2r}) = y(\alpha^r)^2 = A_r^2$ dir. Dekoder y(x) den kolayca A_l yi hesaplayabilir. y(x), α^l nin minimal polinomu olan $m_1(x)$ ile

bölünür. Yani $y(x) = Q(x)m_1(x) + R(x)$ $der(R(x)) < der(m_1(x))$ yazılır. Bu durumda $x = \alpha^l$ olduğunda, $A_l = y(\alpha^l)$ $R(x)$ e eşit olur.

2. Hatanın yerini tespit eden $\sigma(z)$ polinomunun bulunuşu: e hatasının ağırlığı w olsun ve $e_{i_1} e_{i_2} ... e_{i_w}$ bileşenlerinde sıfır olmasın. Bu durumda $i_1 i_2 ... i_w$ hatadaki y nin koordinatlarıdır. Hatanın yerleri

$$X_r = \alpha^{ir}, \quad r = 1, 2, ..., w$$

ile gösterilsin. Bu durumda

$$\sigma(z) = \prod_{i=1}^{w} (1 - X_i z) = \sum_{i=0}^{w} \sigma_i z^i$$

olur. Böylece

$$A_l = y(\alpha^l) = c(\alpha^l) + e(\alpha^l) = e(\alpha^l) \quad 1 \le l \le \delta - 1$$

ve buradan $A_l = \sum_{i=1}^{w} X_i^l$ elde edilir.

İki hata düzeltme [3], [2]

Sendrom $S = \begin{bmatrix} A_1 \\ A_3 \end{bmatrix}$ olur. Bu durumda:

i. Eğer $A_1 = A_3 = 0$ ise $\sigma(z)$=0 olur. Yani hata yoktur.

ii. Eğer $A_1 \neq 0, \quad A_3 = A_1^3$ ise bir hata vardır ve $\sigma(z) = 1 + A_1 z$ $(\sigma(z) = z = A_1)$ olur.

iii. Eğer $A_1 \neq 0, \quad A_3 \neq A_1^3$ ise bu durumda iki hata vardır ve

$$\sigma(z) = z^2 + A_1 z + (\frac{A_3}{A_1} + A_1^2)$$

olur.

iv: Eğer $A_1 = 0, \quad A_3 \neq 0$ ise bu durumda en az 3 hata oluşmuştur.

Örnek 1.6.1: $\mathbb{Z}_2$ üzerinde $x^{15} - 1$ polinomunun parçalanışından $x^4 + x + 1$ polinomu alınsın. Bu polinom indirgenemez bir monik polinomdur. α ; $\alpha^4 + \alpha + 1 = 0$ olacak biçimde bir ilkel kök olsun. Bu ilkel kökten yararlanarak kontrol matrisi şöyle yazılır:

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} \end{bmatrix}$$

Burada α nın kuvvetleri;

$$\alpha^0 = 1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \ \alpha^1 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \ \alpha^2 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \ \alpha^3 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \text{ ve } \alpha^4 = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

olur. $\alpha^4 + \alpha + 1 = 0$ olduğundan;

$$\alpha^5 = \alpha.\alpha^4 = \alpha(\alpha + 1) = \alpha^2 + \alpha \ = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix},$$

$$\alpha^6 = \alpha.\alpha^5 = \alpha(\alpha^2 + \alpha) = \alpha^3 + \alpha^2 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix},$$

$$\alpha^7 = \alpha.\alpha^6 = \alpha(\alpha^3 + \alpha^2) = \alpha^4 + \alpha^3 = 1 + \alpha \ + \alpha^3 = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix}, \ldots,$$

$$\alpha^{14} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

dir. Böylece

$$H = \left[\begin{array}{cccccccccccccc} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ \hline 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \end{array}\right]$$

olur. c=(0 0 0 1 0 0 1 1 0 1 0 1 1 1 1) bir kodsözdür. $x^4 + x + 1$ polinomu $x^{15} - 1$ polinomunu böler. Yani;

$$x^{15} - 1 = (x^4 + x + 1).(x^{11} + x^8 + x^7 + x^5 + x^3 + x^2 + x + 1)$$

dir. Burada $x^{11} + x^8 + x^7 + x^5 + x^3 + x^2 + x + 1$ polinomu kodun üreteç polinomudur ve bu kod devirlidir. Üstelik bu devirli kod bir BCH koddur ve iki hata düzeltebilir.

c=(0 0 0 1 0 0 1 1 0 1 0 1 1 1 1)

kodsözünün birinci bileşeninde 1 hata yapılsın. Bu durumda

r=(100100110101111)

olur. Sendrom;

$$r\,.\,H^{tr}=(100100110101111)\left[\begin{array}{cccccccccccccc}1&0&0&0&1&0&0&1&1&0&1&0&1&1&1\\0&1&0&0&1&1&0&1&0&1&1&1&1&0&0\\0&0&1&0&0&1&1&0&1&0&1&1&1&1&0\\0&0&0&1&0&0&1&1&0&1&0&1&1&1&1\\\hline 1&0&0&0&1&1&0&0&0&1&1&0&0&0&1\\0&0&0&1&1&0&0&0&1&1&0&0&0&1&1\\0&0&1&0&1&0&0&1&0&1&0&0&1&0&1\\0&1&1&1&1&0&1&1&1&1&0&1&1&1&1\end{array}\right]^{tr}$$

$$=\left(\begin{array}{c}1\\0\\0\\\hline 0\\1\\0\\0\\0\end{array}\right)$$

olarak hesaplanır. Burada $A_3=A_1^3=(\alpha^0)^3$ olur. Yani bir hata vardır.

$\sigma(z)=1+A_1z=0$ ise

$$1+\begin{pmatrix}1\\0\\0\\0\end{pmatrix}^{tr}.\begin{pmatrix}1\\0\\0\\0\end{pmatrix}=0$$

olur. Böylece z=α^0 olur. Yani hatanın yeri 1. bileşendedir ve bu bileşene 1 eklenerek hata düzeltilir. Şimdi yukarıda c kodsözünün 1. ve 2. bileşenlerinde 2 hata yapılsın. Yani

r=(1101000110101111)

olsun. Sendrom;

$$r\,.\,H^{tr}=(1101001101011111)\left[\begin{array}{cccccccccccccc}1&0&0&0&1&0&0&1&1&0&1&0&1&1&1\\0&1&0&0&1&1&0&1&0&1&1&1&1&0&0\\0&0&1&0&0&1&1&0&1&0&1&1&1&1&0\\0&0&0&1&0&0&1&1&0&1&0&1&1&1&1\\\hline1&0&0&0&1&1&0&0&0&1&1&0&0&0&1\\0&0&0&1&1&0&0&0&1&1&0&0&0&1&1\\0&0&1&0&1&0&0&1&0&1&0&0&1&0&1\\0&1&1&1&1&0&1&1&1&1&0&1&1&1&1\end{array}\right]^{tr}$$

$$=\left(\begin{array}{c}1\\1\\0\\0\\\hline1\\0\\0\\1\end{array}\right)$$

olarak hesaplanır. Burada $A_1=\alpha^4$, $A_3=\alpha^{14}$ ve

$$\sigma(z)=z^2+A_1z+(\frac{A_3}{A_1}+A_1^2)=0 \quad [\,(\frac{A_3}{A_1}+A_1^2)=\alpha^{10}+\alpha^8=\left(\begin{array}{c}1\\1\\1\\0\end{array}\right)+\left(\begin{array}{c}1\\0\\1\\0\end{array}\right)=\left(\begin{array}{c}0\\1\\0\\0\end{array}\right)=\alpha\,]$$

$z^2+\alpha^4\,z+\alpha=0$ ise

$(z+\alpha^0).(z+\alpha^1)=0$

dır. Yani bu denklemin kökleri hataların yerini vermektedir. Bu hatalar 1. ve 2. bileşende olmuştur. Bileşenler $\mathbb{Z}_2$ den seçildiği için buradaki bileşenlere 1 eklenerek hata düzeltilir.

BÖLÜM 2. GAUSS TAMSAYILARI ÜZERİNDE KODLAR

Klaus Huber 1994 yılında Gauss tamsayıları üzerinde Mannheim metriğini ve Mannheim ağırlığını tanımladı ve bir Mannheim ağırlığındaki hataları düzelten lineer kodlar elde etti. Bu kodların dizaynı 4n+1 oldu. [4]

Klaus Huber yine 1994 de Mannheim metriği ile Gauss tamsayılarını kullanarak elde ettiği kodları Eisenstein-Jacobi tamsayılarına aktardı ve bu kodların dizaynı 6n+1 oldu. [5]

Klaus Huber 1997 de iki boyutlu modül metriği için (Mannheim metriği) MacWilliams teoremini ispatladı. [6]

T.P. da Nobrega Neto 2001 yılında 4. ve 5. makalede belirtilen kodları Mannheim metriğini kullanarak $\mathbb{Q}\sqrt{d}$, $d=-1,-2,-3,-7,-11$ Euclid bölgesi üzerinde yeni kodlar elde etti. [7]

Y. Fan ve Y. Gao 2004 yılında Mannheim metriğini kullanarak devirsel (cyclotomic) cisimler üzerindeki cebirsel tamsayı halkalarına uyguladılar ve kendi Mannheim ağırlığını kullanarak 1 hata düzelten lineer kodlar elde ettiler. [8]

Bu bölümde Mannheim metriği incelendi ve kendi örneklerimizle pekiştirildi.

2.1. Gauss Tamsayıları

Gauss tamsayıları gerçek ve imajiner kısımları tamsayı olan kompleks sayıların bir altkümesi ve $\mathbb{Z}[i]$ Euclid bölgesi olan bir tamlık bölgesidir. Fermat'ın meşhur iki kare teoremine göre $p \equiv 1 \bmod 4$ formundaki asal sayılar iki tam sayının karelerinin toplamı olarak tek türlü yazılabilir. Bundan dolayı p bir kompleks Gauss tamsayısı ile eşleniğinin çarpımıdır. Yani

$$p = a^2 + b^2 = \pi.\pi^*$$

burada $\pi = a + ib$, $\pi^* = a - ib$ dir.

G, Gauss tamsayılarını ve G_π'de mod π ye göre G'nin kalan sınıflarının kümesini göstersin. Burada modül fonksiyonu

$$\mu(\varepsilon) = \varepsilon \mod \pi = \eta = \varepsilon - [\frac{\varepsilon.\pi^*}{\pi.\pi^*}].\pi$$

şeklinde tanımlanır.(Burada [.] işlemi en yakın tamsayıya yuvarlama olarak tanımlanır. Gauss tamsayılarını yuvarlama [a+ib]=[a]+i[b] şeklindedir). Tamsayılarda olduğu gibi $1 = u.\pi + v.\pi^*$ eşitliğini sağlayan u ve v yi hesaplamak için Gauss tamsayılarında da Euclid algoritması kullanılabilir. [4]

Tablo 2.1.1 de $p \equiv 1 \bmod 4$ ve $p \leq 113$ için π, u ve v verilmiştir. Modül fonksiyonu GF(p) den G_π'ye şöyle tanımlanır: [4]

$$\mu(g) = g \pmod n = \gamma = g - [\frac{g.\pi^*}{p}].\pi . \qquad (2)$$

$1 = u\pi + v\pi^*$ eşitliği kullanılarak μ^{-1};

$$g = \mu^{-1}(\gamma) = \gamma.(v\pi^*) + \gamma^*.(u\pi) \bmod p$$

olarak elde edilir. Eğer g, GF(p) de bir tamsayı ise o zaman $g = k.\pi + \gamma$ ve $g = g^* = k^*.\pi^* + \gamma^*$ olur. Bundan dolayı

$$\gamma.(v\pi^*) + \gamma^*.(u\pi) = (g - k\pi).(v\pi^*) + (g - k^*\pi^*).(u\pi) \equiv g.(v\pi^* + u\pi) \bmod p$$

olur. Bu da g ye eşittir.

$$\mu(g_1 + g_2) = \mu(g_1) + \mu(g_2) \text{ ve } \mu(g_1.g_2) = \mu(g_1).\mu(g_2)$$

olduğundan μ nün bir izomorfizma olduğu açıktır.

GF(p) ve G_π nin matematiksel olarak eşitliği ile birlikte ikinci bölümde iki boyutlu uzay üzerinde kodlama açısından GF(p), G_π olarak belirtildiğinde önemli teknik avantajlar sağlar.

Tablo 2.1.1 $P \le 113$ için p, π, α, u, v, $d_{\max}$ değerleri

P	π	α	$d_{\max}$	u,	v
5	2+i	-i	1	-1	1+i
13	3+2i	2	2	-2	1+2i
17	4+i	-l-i	3	-2	2+i
29	5+2i	2	4	-2+2i	3
37	6+i	2	5	-3	3+i
41	5+4i	-3+i	4	-4	1+4i
53	7+2i	2	6	-4-i	3+3i
61	6+5i	2	5	6i	6-i
73	8+3i	-3-3i	7	-3+4i	5-i
89	8+5i	3	7	-3+4i	5+i
97	9+4i	5	8	-4+3i	5+i
101	10+i	2	9	-5	5+i
109	10+3i	-4-3i	9	-3+8i	7-5i
113	8+7i	3	7	8i	8-i

Örnek 2.1.1: $\mathbb{Z}_5$ ile G_{2+i} arasında birebir bir fonksiyon olduğu gösterildi [4]. Şekil 2.1.1 de G_{2+i} nin elemanlarının düzlemdeki yerleri gösterilmiştir.

Burada p=5 π=2+i ve π^*=2-i ve $\mathbb{Z}_5=\{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4}\}$dır.

g=0 için $\gamma = g-[\frac{g.\pi^*}{p}].\pi = 0-0=0 \in G_\pi$,

g=1 için $\gamma = 1-[\frac{1.(2-i)}{5}].(2+i) = 1-0=1 \in G_\pi$,

g=2 için $\gamma = 2-[\frac{2.(2-i)}{5}].(2+i) = 2-[\frac{4-2i}{5}].(2+i) = 2-(2+i) = -i \in G_\pi$,ve

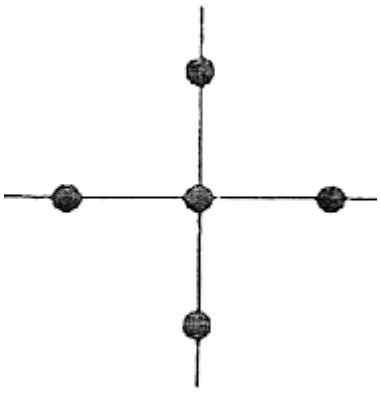
aynı yolla

g=3 için γ=i$\in G_\pi$ ve g=4 için γ=-1$\in G_\pi$

olur. Yani

$$\frac{G}{<2+i>} = G_\pi = \{0,1,-1,i,-i\}$$

dir.



Şekil 2.1.1 G_{2+i} nin elemanlarının kompleks düzlemdeki yerleri

2.2. Bir Hata Düzelten Mannheim Kodlar (OMEC)

Mannheim mesafesi şöyle tanımlanır : $\alpha, \beta \in G_\pi$ ve $\gamma = \beta - \alpha \mod \pi$ olsun. γ nın Mannheim ağırlığı;

$$\omega_m(\gamma) = \left|\mathrm{Re}(\gamma)\right| + \left|\mathrm{Im}(\gamma)\right|$$

olarak tanımlanır [4]. Kodlar lineer kod olduğu için α ile β arasındaki Mannheim uzaklığı d_m ise

$$d_m(\alpha, \beta) = W_m(\gamma)$$

şeklinde olur. $\alpha \in G_\pi$ olmak üzere $d_m(\alpha, 0)$ alındığında Mannheim uzaklığı Manhattan olarak adlandırılan uzaklığa eşittir.

G_π üzerinde $x = (x_0, x_1, ..., x_{n-1})$ vektörünün Mannheim ağırlığı

$$W_m(x) = \sum_{j=0}^{n-1} w_m(x_j)$$

olarak hesaplanır ve x ile y nin Mannheim uzaklığı $W_m(y - x)$ şeklinde gösterilir. Manhattan uzaklığı gibi olan Mannheim uzaklığı bir metrik tanımlar. Eğer $x = y$ ise $\mathrm{d}(x, y) = 0$ ve $\mathrm{d}(x, y) = \mathrm{d}(y, x)$, $\mathrm{d}(x, y) \geq 0$ eşitlikleri olur ve $\mathrm{d}(x, z) \leq \mathrm{d}(x, y) + \mathrm{d}(y, z)$ dir. G_π nin sahip olduğu iki elemanı arasındaki maksimum Mannheim mesafesi;

$$d_{\max} = \max\{d_m(\gamma, 0) : \gamma \in G_\pi\}$$

şeklinde tanımlanır. Böylece

$$d_{\max} = \max\{a,b\} - 1$$

elde edilir. Öncelikle $d_{\max} \le \max\{a,b\} - 1$ olduğunda $\forall x \in G_\pi$ için $[x\pi^* / p]$=0 olduğu not edilir. Genelliği bozmadan a>b≥0 olsun. O zaman x=(a-b-1)/2+i(a+b-1)/2$\in G_\pi$ olur. (p tek olduğunda ya a çift, b tek yada a tek b çift olduğu hatırlanmalıdır). Tablo2.1.1 de $p \equiv 1 \pmod 4$ ve $p \le 113$ olmak üzere tüm asallar için $d_{\max}$ verilmiştir.

Kod üzerinde oluşan bir ağırlığındaki Mannheim ağırlığına sahip bir hata şöyle düzeltilir:

$n = (p-1)/4$ uzunluğuna sahip kodlar Mannheim ağırlığı 1 olan kod sözler olur. Ağırlığı 1 olan Mannheim hatasının değeri $\pm 1, \pm i$ olan dört sayıdan birini verir ($0 \le l \le n-1$). $\alpha \in G_\pi$ derecesi p-1 olan bir eleman olsun. OMEC kodların kontrol matrisi aşağıdaki gibi oluşturulur.

$$H = (\alpha^0, \alpha^1, ..., \alpha^{\frac{p-1}{4}-1})$$

$H.C^T = 0$ olan c=($c_0, c_1, ..., c_{n-1}$) tüm vektörler kodsözlerdir. Üreteç matrisine ise

$$G = \begin{pmatrix} -\alpha^1 & 1 & 0 & \cdots & 0 \\ -\alpha^2 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ -\alpha^{((p-1)/4)-1} & 0 & 0 & \cdots & 1 \end{pmatrix}$$

matrisi karşılık gelir.

Yukarıdaki H matrisi ile oluşturulan C kodu 1 ağırlığındaki her Mannheim hatasını düzeltebilir. Burada $\{\alpha^n, \alpha^{2n}, \alpha^{3n}, \alpha^{4n}\} = \{\pm 1, \pm i\}$ dir. {1,-1,i,-i} den her hata farklı bir sendrom üretecektir. Dekodlama açıktır. Vektör $r = c + e$ olarak alınır ve sendrom S=$H.r^T$ ile hesaplanır. Burada vektörün hatası birdir ve değeri $s.\alpha^{-l}$ ile hesaplanır. Ayrıca $l = \log_\alpha s \mod n$ ile hesaplanır.

OMEC kodları çok hızlı ve verimli çalışırlar ancak yalnız bir hatalı (1 ağırlığındaki) vektörlerin hatasını düzeltirler.

Şimdi bu kodlara basit bir örnek verilsin.

Örnek 2.2.1: p=17, $\pi = 4+i$ ve $\alpha = 1-i$ olsun. $n = \frac{17-1}{4} = 4$ olur ve α'nın kuvvetleri Tablo 2.2.1 de gösterilmiştir. Şekil 2.2.1 de G_{3+2i} nin elemanları düzlem üzerinde gösterilmiştir. α nın kuvvetleri;

$$\begin{aligned}
&\alpha^0 = 1\\
&\alpha^1 = \alpha = 1-i\\
&\alpha^2 = (1-i)^2 = -2i\\
&\alpha^3 = -2i(1-i) = -2-2i \equiv 2-i \mod(4+i)\\
&\alpha^4 = (2-i)(1-i) = 1-3i \equiv i \mod(4+i)\\
&\vdots\\
&\alpha^{15} \equiv -1-2i \mod(4+i)\\
&\alpha^{16} = (-1-2i)(1-i) = -3-i\\
&\qquad\qquad \equiv -3-i+4+i = 1 \mod(4+i)
\end{aligned}$$

olarak hesaplanır. Bu durumda

$$H = (\alpha^0, \alpha^1, ..., \alpha^{\frac{p-1}{4}-1})$$

$$H = (1, 1\text{-}i, -2i, 2\text{-}i)$$

ve

$$G = \begin{pmatrix} -\alpha^1, & 1, & 0, & \cdots, & 0 \\ -\alpha^2, & 0, & 1, & \cdots, & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ -\alpha^{(p-1/4)-1}, & 0, & 0, & \cdots, & 1 \end{pmatrix}$$

$$G=\begin{pmatrix} -1+i & 1 & 0 & 0 \\ 2i & 0 & 1 & 0 \\ 2-i & 0 & 0 & 1 \end{pmatrix}$$

yazılır. Dekodere gelen söz r=(-1+i,1,1,0) olsun. Sendrom;

$$S = H.r^T = (1,1-i,-2i,2-i).\begin{pmatrix} -1+i \\ 1 \\ 1 \\ 0 \end{pmatrix} = -1+i+1-i-2i = -2i \equiv \alpha^2 \bmod 4+i$$

$$2 \equiv 2 \bmod 4+i$$

olduğundan;

$$S.\alpha^{-l} = -2i.\frac{1}{-2i} = 1$$

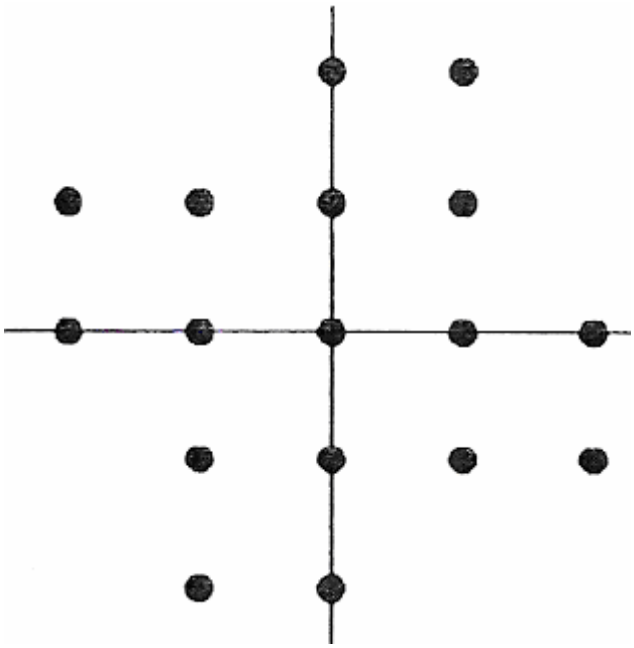
olur ve e=(0,0,1,0) elde edilir. Böylece hatalı kodsöz

c=r-e=(-1+i,1,1,0,)-(0,0,1,0)=(-1+i,1,0,0)

şeklinde düzeltilir.

Tablo 2.2.1 G_{4+i} bölüm uzayında α =1-i nin kuvvetleri

s	α^s		s	α^s		s	α^s		s	α^s		s	α^s
0	1		4	İ		8	-1		12	-i		16	1
1	1-i		5	1+i		9	-1+i		13	-1-i		17	1-i
2	-2i		6	2		10	2i		14	-2		18	-2i
3	2-i		7	1+2i		11	-2+i		15	-1-2i		19	2-i



Şekil 2.2.1 G_{4+i} nin elemanlarının kompleks düzlemdeki yerleri

Örnek 2.2.2: p=29, $\pi = 5+2i$ ve $\alpha = 2$ olsun. α'nın kuvvetleri mod 5+2i ye göre Tablo 2.2.2 de gösterilmiştir. Şekil 2.2.2 de G_{5+2i} nin elemanları düzlem üzerinde gösterilmiştir. Kontrol matrisi;

$$H = \begin{pmatrix} 1 & 2 & -1-2i & 1+3i & -1-i & -2-2i & 1-2i \end{pmatrix}$$

ve üreteç matrisi;

$$G = \begin{pmatrix} -2 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1+2i & 0 & 1 & 0 & 0 & 0 & 0 \\ -1-3i & 0 & 0 & 1 & 0 & 0 & 0 \\ 1+i & 0 & 0 & 0 & 1 & 0 & 0 \\ 2+2i & 0 & 0 & 0 & 0 & 1 & 0 \\ -1+2i & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

olur. Hatalı kodsöz $r = \begin{pmatrix} -2 & 1 & i & 0 & 0 & 0 & 0 \end{pmatrix}$ olsun. Bu durumda sendrom;

$$S = H.r^{tr} = \begin{pmatrix} 1 & 2 & -1-2i & 1+3i & -1-i & -2-2i & 1-2i \end{pmatrix}. \begin{pmatrix} -2 \\ 1 \\ i \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$= 2 - i = \alpha^9$$

olarak hesaplanır. $9 \equiv 2 \bmod 7$ olduğundan kodsözün 3. bileşeninde hata vardır ve bu hatanın değeri;

$$s.\alpha^{-l} = (2-i).\frac{1}{\alpha^2} = \frac{2-i}{-1-2i} = i$$

olur. Böylece c=r-e=(-2 1 i 0 0 0 0)-(0 0 i 0 0 0 0)=(-2 1 0 0 0 0 0) olarak dekodlanır.

$H = (\alpha^0, \alpha^1, ..., \alpha^{\frac{p-1}{4}-1})$ kontrol matrisi ile tanımlanan $n = (p^r - 1)/4$ uzunluğundaki kodlar, BCH ve Berlekamp ın negacyclic kodları ile benzeşen ilkel uzunluklu kodlara genelleştirilebilir. Böylece kontrol matrisi

$$H = (\alpha^0, \alpha^1, ..., \alpha^{[(p^r-1)/4]-1})$$

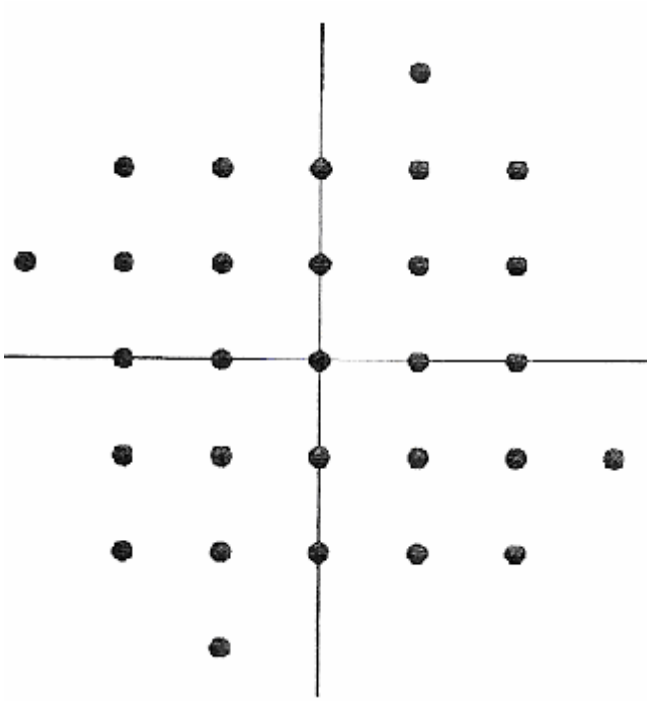
olur. Burada $\pi \in G_{\pi^r}$ ve α'nın derecesi $p^r - 1$ dir. G_{π^r}, GF(p^r)'ye izomorftur. Benzer bir şekilde Hamming mesafeli kodları hata düzelten lineer Mannheim kodlarının $[n, k, d_m]$ üçlüsü ile niteleyebiliriz. Burada n uzunluk k boyut ve kodun minimum Mannheim mesafesi

$$d_m = \min\{w_m(c) : c \neq 0, c \in C\}$$

dir.

Tablo 2.2.2 $\alpha = 2$ nin G_{5+2i} de kuvvetleri

s	α^s		s	α^s		s	α^s		s	α^s		s	α^s
0	1		6	1-2i		12	2-2i		18	1+i		24	3-i
1	2		7	i		13	2+i		19	2+2i		25	-1+i
2	-1-2i		8	2i		14	-1		20	-1+2i		26	-2+2i
3	1+3i		9	2-i		15	-2		21	-i		27	-2-i
4	-1-i		10	-3+i		16	1+2i		22	-2i		28	1
5	-2-2i		11	1-i		17	-1-3i		23	-2+i		29	2



Şekil 2.2.2 G_{5+2i} nin elemanlarının kompleks düzlemdeki yerleri

Tanım 2.2.1: $p \equiv 1 \bmod 4$ için $n = (p^r - 1)/4$ uzunluğunda ve k=n-r boyutlu minimum Mannheim uzunluğu $d_m = 3$ olan ve H=$(\alpha^0, \alpha^1, ..., \alpha^{[(p^r-1)/4]-1})$ kontrol matrisi ile tanımlanan [n,n-r,3] OMEC kodları G_π üzerinde blok kodlardır.

Aşağıdaki örnekte G_{π^r} uzayı üzerinde yapılan başka bir örnek göz önüne alınmaktadır.

Örnek 2.2.3: p=5, $\pi = 2+i$ ve r=2 olsun. G_{π^2} 'de asal polinom olarak $p(x) = x^2 - x - i$ olsun. α nın kuvvetleri Tablo 2.2.3 de gösterilmiştir. $p(x) = x^2 - x - i$ polinomunun kökü α ise;

$$\alpha^2 - \alpha - i = 0$$

olur. Bu kullanılarak α nın kuvvetleri şöyle yazılabilir:

$$\begin{aligned}
&\alpha^0 = 1 = (0,1)\\
&\alpha^1 = \alpha = (1,0)\\
&\alpha^2 = \alpha + i \quad \Rightarrow\\
&\alpha^3 = \alpha\ \alpha^2 = \alpha\ (\alpha\ + i) = \alpha^2 + \alpha i\\
&\qquad\qquad = \alpha + i + \alpha i = \alpha(1+i) + i = (1+i, i)\\
&\alpha^4 = \alpha[(1+i)\alpha + i)] = \alpha^2(1+i) + \alpha i\\
&\qquad\qquad\qquad = (-1+i)\alpha + (-1+i)\\
&\qquad\qquad\qquad = (-1+i, -1+i)\\
&\vdots\\
&\alpha^{23} = -i\alpha\ + i = (-i, i).
\end{aligned}$$

Kontrol matris;

$$H = (\alpha^0, \alpha^1, ..., \alpha^{\frac{p-1}{4}-1})$$

$$H = \begin{pmatrix} 0 & 1 & 1 & 1+i & -1+i & -1 \\ 1 & 0 & i & i & -1+i & -1-i \end{pmatrix}$$

olur. Bu [6,4,3] şeklinde bir OMEC koddur. r=(-i,0,1,1,1+i,-i) gelen vektörde bir hata oluşsun. Bu durumda sendrom;

$$H.r^T = \begin{pmatrix} 1 \\ i \end{pmatrix} = \alpha^2$$

olur. $2 \equiv 2 \bmod 6$ ve $\alpha^0 = 1$ olduğundan

c=r-e=(-i,0,1,1,1+i,-i)-(0,0,1,0,0,0)=(-i,0,0,1,1+i,-i)

olarak hata düzeltilir.

Tablo 2.2.3 $p(x) = x^2 - x - i$ polinomunu α kökünün G_{2+i} üzerinde kuvvetleri

s	α^s		s	α^s		s	α^s		s	α^s		s	α^s
0	(0,1)		4	(-1+i,-1+i)		8	(-i,1)		12	(0,-1)		16	(1-i,1-i)
1	(1,0)		5	(-1,-1-i)		9	(1-i,1)		13	(-1,0)		17	(1,1+i)
2	(1,i)		6	(0-i)		10	(-1,1+i)		14	(-1,-i)		18	(0,i)
3	(1+i,i)		7	(-i,0)		11	(i,-i)		15	(-1-i,-i)		19	(i,0)

2.3. $d_m \geq 3$ İçin Hata Düzelten Mannheim Kodlar

Bu bölümde, hatanın ağırlığı 1 den büyük olan hata düzelten Mannheim kodları incelenecektir. Bu nedenle C kodunun aşağıdaki H kontrol matrisi;

$$H = \begin{pmatrix} \beta^0, & \beta^1, & \cdots & ,\beta^{n-1} \\ \beta^0, & \beta^5, & \cdots & ,\beta^{(n-1)/5} \\ \vdots & \vdots & \ddots & \vdots \\ \beta^0, & \beta^{(4t+1)}, & \cdots & \beta^{(n-1)(4t+1)} \end{pmatrix}$$

şeklinde alınsın. β derecesi 4n, $\beta^n = i$ ve $\beta \in G_{\pi^r}$ olsun. β nın 4t+1 nci kuvvetlerini kullanarak kontrol matrisinin satırları yazılır. Eğer $\varepsilon \in \{\mp 1, \mp i\}$ ise $\varepsilon^{4t+1} = \varepsilon$ olur. Eğer $c = (c_0, c_1, ..., c_{n-1})$ C nin bir kodsözü ise o zaman $c = c(x) = \sum c_j x^j$ polinomu yazılır. Böylece $c(\beta^{4k+1}) = 0$, $k = 0,1,2,...,t$ olur. Buradan c(x) polinomu $x^n - i$ polinomunu bölen g(x) polinomunun bir çarpanıdır. Bu nedenle C bir i-devirsel (i-cyclic) koddur [4]. Örneğin eğer

$$\begin{aligned} c(x) \in C \Rightarrow x(c_0 + c_1 x + ... + c_{n-1} x^{n-1}) \\ = ic_{n-1} + c_0 x + c_1 x^2 + ... + c_{n-2} x^{n-1} \\ = (i.c_{n-1}, c_0, c_1, ..., c_{n-2}) \end{aligned}$$

olur. Böylece c(x) i $x^n - i$ modülüne göre x ile çarpmak aşağıdaki sonuçları verir.

i. Devirli kodlar 1 kaydırılarak kodsözler elde edilir.

ii. En büyük katsayı c_{n-1} kompleks düzlemde 90^0 döndürülür ve c_0 elde edilir.

Uyarı 2.3.1: Eğer $\beta^n = -i$ ise nega-icyclic kodlar elde edilir. h(x) kontrol polinomu

$$x^n - i = g(x).h(x)$$

ile tanımlanır.

Tanım 2.3.1: θ, G de bir birimsel eleman olmak üzere eğer $(c_0, c_1, ..., c_{n-1})$ kodsözü C de iken $(\theta c_{n-1}, c_0, ..., c_{n-2})$ kodsözü de C de ise G_π üzerinde C koduna constadevirli (constacyclic) ya da θ-devirli (θ-cyclic) kod denir.

Tanım 2.3.2: G_{π^r} üzerindeki i-devirsel (nega i-devirsel) kodlar, kodsözleri

$$x^n - i \,(\text{veya}\, x^n + i)$$

polinomunu bölen bir g(x) polinomunun ürettiği kodlardır. Böylece i-devirsel kodlar constadevirli kod sınıfının bir üyesidir.

İcyclic kodların (veya nega-icyclic kodların) minimum Mannheim mesafesini doğru hesaplamak yukarıda da görüldüğü gibi zor bir problem tanımlar. Bu yüzden daha çok, basit durumlar üzerinde durulacaktır. t=0 OMEC kodları verir. Bu yüzden t=1 olsun. Bu durumda iki Mannheim hatasını düzelten H kontrol matrisi;

$$H = \begin{pmatrix} \beta^0, & \beta^1, & \beta^2, & \cdots & \beta^{n-1} \\ \beta^0, & \beta^5, & \beta^{10}, & \cdots & \beta^{(n-1).5} \end{pmatrix} \tag{2.1}$$

olur. $r = c + e$ bir girdi vektörü olsun. İlk önce sendrom s;

$$s = \begin{pmatrix} s_1 \\ s_5 \end{pmatrix} = H.r^T$$

olarak hesaplanır. $l_{1,2}$ deki Mannheim hatasının değeri $\beta^{L_{1,2}-l_{1,2}} \in \{\mp 1, \mp i\}$ olsun. Bu durumda hatayı hesaplayan polinom $\sigma(z)$ şöyle hesaplanır:

$$\begin{aligned}\sigma(z) &= (z-\beta^{L_1}).(z-\beta^{L_2}) \\ &= z^2-(\beta^{L_1}+\beta^{L_2})z+\beta^{L_1}.\beta^{L_2} \\ &\Rightarrow \sigma(z) = z^2-s_1z+\varepsilon.\end{aligned}$$

Burada ε sendromlardan hesaplanır. $\sigma(z)$ polinomuna hata hesaplayan polinom demekten ziyade hatanın yerini tespit eden polinom denir. Burada $\beta^{L_{1,2}}$ bilgisi hem hatanın yerini $l_{1,2}=L_{1,2}$ modn, hem de hatanın değerini $\beta^{L_{1,2}-l_{1,2}}$ belirler. $s_1=\beta^{L_1}+\beta^{L_2}$, $s_5=\beta^{5L_1}+\beta^{5L_2}$ ve $\varepsilon=\beta^{L_1}+\beta^{L_2}$ den

$$\begin{aligned}\frac{s_1^5-s_5}{5s_1} &= (\beta^{L_1+4L_2}+2\beta^{2L_1+3L_2}+2\beta^{3L_1+2L_2}+\beta^{4L_1+L_2})/\beta^{L_1}+\beta^{L_2} \\ &= (\varepsilon+\beta^{3L_2}+2\varepsilon^2.\beta^{L_2}+2\varepsilon^2.\beta^{L_1}+\varepsilon.\beta^{3L_1})/\beta^{L_1}+\beta^{L_2} \\ &= \varepsilon.\frac{\beta^{3L_2}+\beta^{3L_1}}{\beta^{L_1}+\beta^{L_2}}+2\varepsilon^2 \\ &= \varepsilon.(\beta^{2L_2}-\beta^{L_1+L_2}+\beta^{2L_2})+2\varepsilon^2 \\ &= \varepsilon.(s_1^2-3.\varepsilon)+2\varepsilon^2\end{aligned}$$

elde edilir. Buradan ikinci dereceden

$$\varepsilon^2-s_1^2.\varepsilon+\frac{s_1^5-s_5}{5s_1}=0 \ (\bmod \pi)$$

denklem elde edilir ve buradan da

$$\varepsilon_{1,2}=\frac{s_1^2}{2}\left(1\mp\sqrt{\frac{s_1^5+4s_5}{5s_1^5}}\right)$$

olur. Bu hata hesaplayan polinomda yerine yazılırsa;

$$z_{1,2}=\frac{s_1}{2}\left(1\mp\sqrt{-1-2.\sqrt{\frac{s_1^5+4s_5}{5s_1^5}}}\right)$$

veya

$$z_{1,2} = \frac{s_1}{2}\left(1 \mp \sqrt{-1 + 2.\sqrt{\frac{s_1^5 + 4s_5}{5s_1^5}}}\right)$$

olur [4].

Bundan dolayı genelde (2.1) deki kontrol matrisi ile oluşturulan kodların iki hata ağırlıklı Mannheim hatasını düzeltmemesinde bir belirsizlik vardır. Bununla birlikte yukarıdaki formülle dekodlanan kod örnekleri Tablo 2.3.1 de mevcuttur. [4] ($d_m \geq 5$ için). OMEC kodlar yukarıdaki kodları kapsadığı için $d_m \geq 3$ olur. Minimum mesafenin 3 olabileceği aşağıdaki örnekte gösterilmektedir.

Örnek 2.3.1: p=13, r=1 n=3, $\alpha = 1 + i$ olsun. Bu durumda Tablo 2.3.2 den

$$g(x) = (x - \alpha).(x - \alpha^5) = x^2 + i.x - 1$$

elde edilir . (Şekil 2.3.1 de G_{3+2i} nin elemanları düzlem üzerinde gösterilmiştir). Buradan $d_m = 3$ olduğu ve g(x)'in [3,1,3] kodunu tanımladığı görülür.

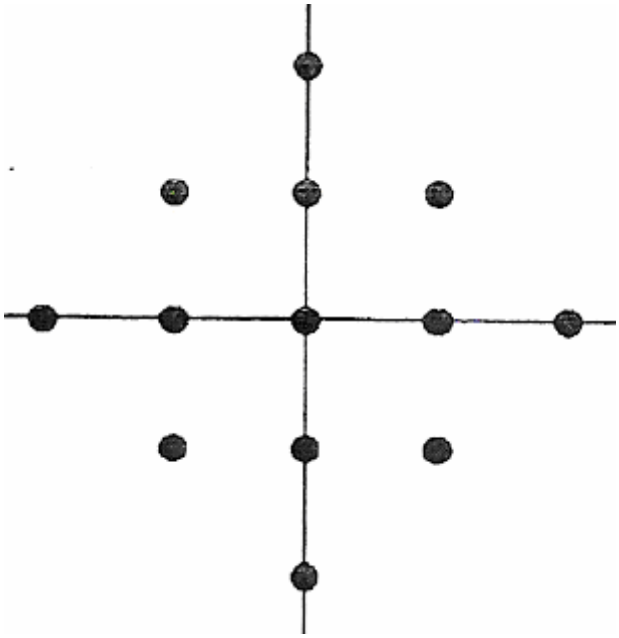
Şimdi (1) deki kontrol matrisine göre daha büyük Mannheim mesafeleri düşünülür.

Tablo 2.3.1 $g(x) = (x-\beta).(x-\beta^5)$ ile üretilen bazı kod örnekleri

P	$[n,k,d_m]$	İlkelliği	β_1	β_2
13	[3,1,4]	İlkel	-i	-i
17	[4,2,4]	İlkel	l+i	-1+ i
	[3,1,4]	İlkel	l+i	– l+i
29	[7,5,41	İlkel	2	-2 - i2
	[6.4,4]	İlkel	2	-2 - i2
	[5,3,5]	İlkel	2	-2 - i2
	[4,2,5]	İlkel	2	-2 - i2
	[3,1,7]	değil	-1-2i	-3+ i
37	[9,7,4]	İlkel	2	l+i
	[8,6,4]	İlkel	2	l+i
	[7,5,4]	İlkel	2	l+i
	[6.4,4]	İlkel	2	l +i
	[5.3.5]	İlkel	2	l+i
	[4,2,5]	İlkel	2	l+i
	[3.1,7]	İlkel	2	l+i
41	[10,9.3]	İlkel	-1-3i	-3
	[10,8,41	İlkel	-1-3i	-3
	[5.,3,6]	değil	4i	i
	[5,3,4]	İlkel	-1-3i	-3
	[4,2.61	değil	4i	i
	[4.2,51	İlkel	l –2 i	-3i
	[3,1,5]	İlkel	– l –3 i	-3
	[3,1.6]	değil	-4i	i

Tablo 2.3.2 α =1+i nin G_{3+2i} deki kuvvetleri

s	α^s	s	α^s	s	α^s	s	α^s
0	1	3	- i	6	-1	9	i
1	1+i	4	1- i	7	-1- i	10	-1+ i
2	2 i	5	2	8	i·2	11	-2



Şekil 2.3.1 G_{3+2i} nin elemanlarının kompleks düzlemdeki yerleri

Teorem 2.3.1: [4] $p \equiv 5 \mod 12$ ve $n = (p-1)/4$ için (2.1) kontrol matrisi ile $d_m \geq 4$ olan kod tanımlanır.

İspat: Dekoderin bir ve iki hatayı çözdüğü gösterilir. Hatanın Mannheim ağırlığı 1 olsun. Bu durumda $s_1 = s_5 \neq 0$ olur ve, ya

$$z_{1,2} = \begin{cases} 0 \\ s_1 \end{cases}$$

ya da

$$z_{3,4} = \frac{s_1}{2}(1 \pm \sqrt{-3})$$

elde edilir. $z_1 = 0$ olmaz ise, $z_2 = s_1$ hatayı düzeltmeye yol gösterir. $p \equiv 5 \mod 12$ için Gauss'un Tersinir Kanunu'na göre -3 p nin ikinci dereceden bir kalanı değildir. Bundan dolayı $z_{3,4} \notin G_\pi$ olur. Böylece teoreme göre 1 ve 2 hata arasındaki hatalar ayırt edilebilir.

Örnek 2.3.2: $p=13, \pi=3+2i$ olsun. $\beta=1+i$ bir ilkel kök olduğundan, kontrol matris;

$$H=\begin{pmatrix}\beta^0, & \beta^1, & \beta^2, & \cdots & \beta^{n-1}\\ \beta^0, & \beta^5, & \beta^{10}, & \cdots & \beta^{(n-1).5}\end{pmatrix}$$

$$H=\begin{pmatrix}1 & 1+i & 2i\\ 1 & 2 & -1+i\end{pmatrix}$$

olur. Burada 4n+1=13 olduğundan n=3 tür. c=(i 1 –i) bir kodsözdür. Bu kodsöz kanalda 2. bileşeninde bir hataya uğrayarak r=(i 0 –i) olsun. Bu durumda sendrom;

$$S=H.r^{tr}=\begin{pmatrix}1 & 1+i & 2i\\ 1 & 2 & -1+i\end{pmatrix}.\begin{pmatrix}i\\ 0\\ -i\end{pmatrix}=\begin{pmatrix}2+i\\ 1+2i\end{pmatrix}$$

$$=\begin{pmatrix}-1-i\\ -2\end{pmatrix}=\begin{pmatrix}s_1\\ s_5\end{pmatrix}\bmod(3+2i)$$

olarak hesaplanır. Buradan

$$s_1^5=(-1-i)^5=4+4i\equiv -2=s_5\neq 0 \bmod(3+2i)$$

olduğu görülür. Yani burada 1 hata oluşmuştur. Bu hatanın

$$z=s_1=-1-i\equiv\alpha^7 \bmod(3+2i)$$

ve

$$7\equiv 1 \bmod(3+2i)$$

olduğundan gelen sözün 2. bileşeninde meydana gelmiştir ve bu hatanın değeri de

$$s_1.\alpha^{-l} = \frac{-1-i}{1+i} = -1$$

dir. Böylece hata c=r-e olduğundan c=(i 0 –i)-(0 -1 0)=(i 1 –i) olarak düzeltilir.

Şimdi r=(1 0 –i) olacak biçimde gelen sözde iki hata meydana gelsin. Bu durumda sendrom;

$$\text{S}=\begin{pmatrix} -2i \\ -1-i \end{pmatrix}=\begin{pmatrix} s_1 \\ s_5 \end{pmatrix}$$

olarak hesaplanır. Burada $s_5 \neq s_1^5$ dir. Yani iki hata olmuştur. Bu hatayı hesaplamak için

$$z_{1,2} = \frac{s_1}{2}\left(1 \mp \sqrt{-1-2.\sqrt{\frac{s_1^5+4s_5}{5s_1^5}}}\right)$$

kullanılırsa, $z_{1,2} = 1 \pm \sqrt{3} \notin G_\pi$ veya $z_{1,2} = 1 \pm \sqrt{5} \notin G_\pi$ olur. Teorem 2.3.1 de de gösterildiği gibi $p = 13 \equiv 1 \bmod 12$ olduğundan (1) deki kontrol matrisi ancak 1 hata düzeltebilir.

Örnek 2.3.2: $p = 29 \equiv 5 \bmod 12$, $\pi = 5+2i$ ve $\beta = 2$ alalım. $\beta^n = i$ olduğundan 2, bir ilkel köktür. İki hata düzelten Mannheim kodun kontrol matrisi;

$$H = \begin{pmatrix} 1 & 2 & -1-2i & 1+3i & -1-i & -2-2i & 1-2i \\ 1 & -2-2i & -3+i & -2 & -1+2i & -1+i & -1-2i \end{pmatrix}$$

olur. Bu kodun üreteç polinomu ise

$$g(x) = (x-\beta).(x-\beta^5)$$

$$=(x-2).(x+2+2i)$$

$$=x^2+2ix+1-2i \mod(5+2i)$$

dir. $c=(1-2i \quad 2i \quad 1 \quad 0 \quad 0 \quad 0 \quad 0)$ kodsözünün 4. ve 6. bileşenlerinde bir hata yapılsın ve gelen söz $r=(1-2i \quad 2i \quad 1 \quad 1 \quad 0 \quad 1 \quad 0)$ olsun. Bu durumda sendrom;

$$S=\begin{pmatrix}-1+i\\-3+i\end{pmatrix}=\begin{pmatrix}s_1\\s_5\end{pmatrix}$$

olarak hesaplanır. $s_5 \neq s_1^5 \neq 0$ olduğundan iki hata olmuştur. Bu hataların yerleri:

$$z^2-s_1z+\varepsilon=0$$

eşitliğinde önce ε değeri hesaplanır.

$$\varepsilon^2-s_1^2.\varepsilon+\frac{s_1^5-s_5}{5s_1}=0$$

olduğundan

$$\varepsilon^2-(-2i).\varepsilon+\frac{4-4i+3-i}{-5+5i}=0$$

yazılır ve buradan da $\varepsilon=2i$ olur. Bu değer $z^2-s_1z+\varepsilon=0$ eşitliğinde yerine yazılırsa;

$$z^2-(-1+i)z+2i=0$$

olur. $2i\equiv\beta^8=\beta^3.\beta^5$ ve $\beta^3+\beta^5\equiv-1+i$ olduğundan gelen sözün 4. ve 6. bileşenlerinde hata oluştuğu anlaşılır. Bu bileşenlerdeki hata,

4. bileşen için $\beta^3.\frac{1}{\beta^3}=1$

6. bileşen için $\beta^5.\frac{1}{\beta^5}=1$

dir. Böylece kodlanmış söz;

$$c=r-e=(1-2i \quad 2i \quad 1 \quad 1 \quad 0 \quad 1 \quad 0)-(0 \quad 0 \quad 0 \quad 1 \quad 0 \quad 1 \quad 0)$$
$$=(1-2i \quad 2i \quad 1 \quad 0 \quad 0 \quad 0 \quad 0)$$

olur. Eğer $r=(1-2i \quad 2i \quad 1 \quad i \quad 0 \quad 1 \quad 0)$ olsaydı o zaman sendrom;

$$S=\begin{pmatrix} i \\ -1+i \end{pmatrix}=\begin{pmatrix} s_1 \\ s_5 \end{pmatrix}$$

ve ε ise

$$\varepsilon^2+\varepsilon+\frac{i+1+i}{5i}=0 \Rightarrow 5\varepsilon^2+5\varepsilon++2-i=0 \Rightarrow \varepsilon=-2$$

olarak hesaplanır. Bu durumda hata yerini tespit eden polinom ve kökleri;

$$z^2-iz-2=0$$
$$(z-\beta^{10})(z-\beta^4)=0$$

olur. $10\equiv 3 \bmod 7$ olduğundan hata 4. ve 5. bileşenlerde oluşmuştur. Bu hataların değerleri ise

4. bileşen için $\beta^{10}\frac{1}{\beta^3}=\frac{-3+i}{1+3i}=i$,

6. bileşen için $\beta^5\frac{1}{\beta^5}=1$

dir. Böylece kodlanmış söz

$$c = r - e = (1-2i \quad 2i \quad 1 \quad i \quad 0 \quad 1 \quad 0) - (0 \quad 0 \quad 0 \quad i \quad 0 \quad 1 \quad 0)$$
$$= (1-2i \quad 2i \quad 1 \quad i \quad 0 \quad 1 \quad 0)$$

olur.

2.4. Ağırlık Sayaçları

Tanım 2.4.1: C bir sonlu F cismi üzerinde [n,k,d] bir lineer kod ve $C^{\perp}$ bu kodun dual kodu olsun. C de ağırlığı i olan kodsöz z^{a_i} ile gösterilir ve eğer ağırlığı i olan kodsözlerin sayısı a_i ise bu durumda;

$$A(z) = \sum_{i=o}^{n} a_i . z^i$$

polinomuna C kodunun (Mannheim metriğine göre) ağırlık sayacı denir.

Mannheim metriği ile oluşturulan bir kod ailesinin ağırlık sayaçları aşağıdaki örnekte açıklanmıştır.

Örnek 2.3.3: p=17, r=1, $\alpha = 1 + i$ ve üreteç polinomu $g(x) = (x - \alpha)(x - \alpha^5)$ olur. Bu polinom [4,2,4] kodunu oluşturur. g(x) ile üretilen ailenin ağırlık sayacı şöyle olur:

$$\begin{aligned} g(x) &= x^2 - x(\alpha^5 + \alpha) + \alpha^6 \\ &= x^2 - 2ix - 2 \\ &= -2 - 2ix + x^2 \end{aligned}$$

olduğundan üreteç matris

$$G = \begin{pmatrix} -2 & -2i & 1 & 0 \\ 0 & -2 & -2i & 1 \end{pmatrix}$$

dir. Bu üreteç matrisi ile toplam 17.17=289 tane kodsöz elde edilir. Bu kodsözlerden c=(-2,-2i,1,0) kodsözünün ağırlığı;

w(c)=|-2|+|-2|+1+0=5

olur. Kodsözlerin ağılıkları hesaplandığında bu kodun ağırlık sayacı şöyle olur:

$A(z) = 1 + 16z^4 + 16z^5 + 32z^6 + 64z^7 + 80z^8 + 64z^9 + 16z^{11}$.

BÖLÜM 3. BAZI SONLU HALKALAR ÜZERİNDE MANNHEİM METRİĞİ İLE LİNEER KODLAR

3.1. Lineer Kodlar

Tanım 3.1.1: F_q^* devirli grubunu üreten F_q daki bir elemana F_q nun pirimitif (ilkel) elemanı denir.

Önerme 3.1.1: [9] R bir halka ve R^*, R nin birimsel elemanlarından oluşan bir küme olsun. Bu durumda;

i. $\phi(n) = \left|(Z / Z_n)^*\right|$,

ii. Eğer n=2, 4 ya da p^r (p asal tek sayı) ise $(Z / Z_n)^*$ bir devirli grup,

iii. Eğer $(Z / Z_n)^*$ bir devirli grup ise $(Z / Z_n)^*$ ın $\phi(\phi(n))$ tane üreteci,

olur.

Tanım 3.1.2: [11] p bir asal tamsayı olmak üzere; $1, g, ..., g^{p-2}$ indirgenmiş tam temsilciler sistemi olacak şekilde bir $g \in \mathbb{Z}$ varsa g ye modulo p bir primitif (ilkel) kök denir. g nin modulo p ilkel kök olması için gerek ve yeter koşul

$$g^k \equiv 1 (\text{mod } p)$$

olacak şekilde en küçük pozitif k sayısının p -1 olmasıdır.

Önerme 3.1.2: [1] G bir grup, $a \in G$ ve $o(a) = n$ olsun.

$$a^m = e$$

olması için gerek ve yeter şart $n \mid m$ olmasıdır.

Önerme 3.1.3: [10] p >2 olmak üzere g tamsayısı p modülüne göre bir primitif kök ise $g^{\phi(p)/2} \equiv -1 \bmod p$ dir.

Teorem 3.1.1: [12] Eğer a ve b aralarında asal tamsayılar ise $\mathbb{Z}[i]/\langle a+bi \rangle \cong \mathbb{Z}_{a^2+b^2}$ olur.

Teorem 3.1.2: [13] $a,b,p \in \mathbb{Z}$ olmak üzere $p = a^2 + b^2$ olması için gerek ve yeter şart $p \equiv 1$ mod4 olmasıdır.

Sonuç 3.1.1: $\pi_1 = a+bi$, $p_1 = a^2+b^2$ ve $\pi_2 = c+di$, $p_2 = c^2+d^2$ olacak biçimde $p_1 = 4n_1+1$ ve $p_2 = 4n_2+1$ $(n_1, n_2 \in \mathbb{Z})$ olsun. $\pi = \pi_1.\pi_2$ alınırsa $m = p_1.p_2$ olur ve $m = 4n+1$ olacak şekilde $n \in \mathbb{Z}$ vardır.

İspat: $\pi_1 = a+bi$ ve $\pi_2 = c+di$ ise $\pi = \pi_1.\pi_2 = (ac-bd)+(ad+bc)i$ olur. Böylece,

$$\begin{aligned} m &= (ac-bd)^2 + (ad+bc)^2 \\ &= a^2c^2 - 2acbd + b^2d^2 + a^2d^2 + 2acbd + b^2c^2 \\ &= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2 \\ &= a^2(c^2+d^2) + b^2(d^2+c^2) \\ &= (a^2+b^2)(c^2+d^2) \\ &= (4n_1+1)(4n_2+1) \\ &= 16n_1n_2 + 4n_1 + 4n_2 + 1 \\ &= 4\underbrace{(4n_1n_2 + n_1 + n_2)}_{\in\mathbb{Z}} + 1 \\ &= 4n+1 \end{aligned}$$

elde edilir.

Önerme 3.1.4: π, G de bir asal olsun. p, $p>2$ ve $\pi = a+bi$ olmak üzere $p = a^2+b^2 = 4n+1$ olacak şekilde bir asal tamsayı olsun. g, $G^*_{\pi^2}$ ın bir üreteci ise

$$g^{\phi(p^2)/4} \equiv i \,(\bmod \pi^2) \quad (\text{ya da } g^{\phi(p^2)/4} \equiv -i \,(\bmod \pi^2))$$

olur.

İspat: Teorem 3.1.1 e göre $\mathbb{Z}_{p^2} \cong G_{\pi^2}$ olur. g, $G^*_{\pi^2}$ ın bir üreteci ise g Gauss tamsayısı G_{π^2} de π^2 modülüne göre $g, g^2, ..., g^{\phi(p^2)}$ Gauss tamsayıları bir indirgenmiş kalanlar sistemi oluşturur. Dolayısı ile $g^k \equiv i \bmod \pi^2$ ($g^k \equiv -i \bmod \pi^2$) olacak biçimde $1 \le k \le \phi(p^2)$ indisi vardır. Buradan $g^{4k} \equiv 1 \bmod \pi^2$ yazılabilir. Önerme 3.1.2 ye göre $\phi(p^2) \mid 4k$ olmalıdır. $4 \le 4k \le 4\phi(p^2)$ olduğundan $\phi(p^2) = k, \phi(p^2) = 2k$ veya $\phi(p^2) = 4k$ olmalıdır. Eğer $\phi(p^2) = k$ ise $i \equiv 1 \bmod \pi^2$ ($-i \equiv 1 \bmod \pi^2$) olur. Yani $\pi^2 \mid i-1$ (ya da $\pi^2 \mid -i-1$) dir. $\mp i - 1$ bir asal Gauss tamsayısı ve $|\pi^2|^2 > 2$ (burada $|\ |$ bir karmaşık sayının modülünü göstermektedir) olduğundan $\phi(p^2) = k$ olamaz. $\phi(p^2) = 2k$ olsun. Bu durumda $1 \equiv -1 \bmod \pi^2$ olur. Yani $\pi^2 \mid 2$ dır. Ancak $|\pi^2|^2 > 2$ olduğundan $\phi(p^2) = 2k$ olamaz. Bu durumda $\phi(p^2) = 4k$ dır.

Önerme 3.1.5: π, G de bir asal olsun. p, $p > 2$ ve $\pi = a + bi$ olmak üzere $p = a^2 + b^2 = 4n + 1$ olacak şekilde bir asal tamsayı olsun. Eğer g, $G^*_{\pi^2}$ ın bir üreteci ve

$$g^{\phi(p^2)/4} \equiv i \bmod \pi^2$$

ise –g de bir üreteçtir ve

$$(-g)^{\phi(p^2)/4} \equiv -i \bmod \pi^2$$

olur.

İspat: $\phi(p^2) = p.(p-1) = (4n+1).(4n+1-1) = 4n(4n+1)$ olur ve n bir tek tamsayı olduğundan

$$(-g)^{\phi(p^2)/4} \equiv -i \bmod \pi^2 \Rightarrow (-1)^{n(4n+1)}.(g)^{n(4n+1)} \equiv -i \bmod \pi^2$$

olur.

Önerme 3.1.6: G Gauss tamsayıları üzerinde p, $p>2$ ve $\pi = a+bi$ olmak üzere $p = a^2+b^2 = 4n+1$ $(a,b,n \in \mathbb{Z})$ olacak şekilde $\mathbb{Z}$ de bir asal tamsayı ise G_{π^2} halkasında daima devirli kodlar yazılabilir. Bu kod bir free G_{π^2} -modül olur.

İspat: $\mathbb{Z}_{p^2} \cong G_{\pi^2}$ olduğunda $G^*_{\pi^2}$ ı üreten bir g$\in$ G_{π^2} vardır. $g^{\phi(p^2)/4} \equiv i \bmod \pi^2$ ise Önerme 3.1.4 den $(-g)^{\phi(p^2)/4} \equiv -i \bmod \pi^2$ olur. Bu durumda;

$$x^{\phi(p^2)/4} - i = (x-g).Q(x) \pmod{\pi^2} \quad (x = g \text{ için})$$

ve

$$x^{\phi(p^2)/4} + i = (x+g).R(x) \pmod{\pi^2} \quad (x = -g \text{ için})$$

şeklinde parçalanır. Ayrıca

$$(x^{\phi(p^2)/4} - i).\ (x^{\phi(p^2)/4} + i) = (x^{\phi(p^2)/2} + 1)$$

olacağından,

$$(x^{\phi(p^2)/2} + 1) = (x-g).(x+g).A(x) \pmod{\pi^2}$$

şeklinde de parçalanabilir. Üstelik buradan üreteç polinomu olarak monik polinomlar seçileceğinden, üreteç matrisinde bir satırın tamamındaki bileşenleri sıfır bölenlerden oluşmaz. Dolayısıyla bu kod bir free G_{π^2} -modül olur.

Önerme 3.1.7: $\pi_k, (k = 1,2,...,m)$ Gauss tamsayılarındaki asallar olsun. $p_k, p_k > 2 (k = 1,2,...,m)$ ve $\pi_k = a_k + ib_k$ olmak üzere $p_k = a_k^2 + b_k^2 = 4n_k + 1$

şeklindeki asallar olsun. Eğer $g, G^*_{\pi^k}$ ın bir üreteci ise $g^{\phi(p^k)/4} \equiv i \pmod{\pi^k}$ (ya da $g^{\phi(p^k)/4} \equiv -i \pmod{\pi^k}$ olur.

İspat: Önerme 3.1.4 den ispat kolayca görülür.
Bu önerme ile devirli kodun uzunluğunu artırma hedeflenmiştir.

Örnek 3.1.1: $\pi_1 = 3+2i$ ve $\pi_2 = 4+i$ seçilirse $p_1 = 13 = 4n_1 + 1$ ve $p_2 = 17 = 4n_2 + 1$ olur. Böylece $\pi = \pi_1.\pi_2 = 10+11i$ ve $m = p_1.p_2 = 13.17 = 10^2 + 11^2 = 221 = 4n+1$ olur.

$\pi_1 = a+bi$, $p_1 = a^2 + b^2$ ve $\pi_2 = c+di$, $p_2 = c^2 + d^2$ alınırsa $\pi = \pi_1.\pi_2$ ve $m = p_1.p_2$ olur. m tek sayı olmak üzere G_π bir halka olur ve (2) deki fonksiyon altında $\mathbb{Z}_p$ ye izomorftur.

Örnek 3.1.2: $\pi_1 = 2+i$ ve $\pi_2 = 3+2i$ olsun. Bu durumda $\pi = 4+7i$ olur ve $G_{4+7i} \cong \mathbb{Z}_{65}$ dir. G_{4+7i} nin elemanları Tablo 3.1.1 de gösterilmiştir. Şekil 3.1.1 de ise G_{4+7i} nin elemanlarının analitik düzlem üzerindeki dağılımı görülmektedir.

Örnek 3.1.3: G_{4+7i} halkası üzerinde üreteç matrisi

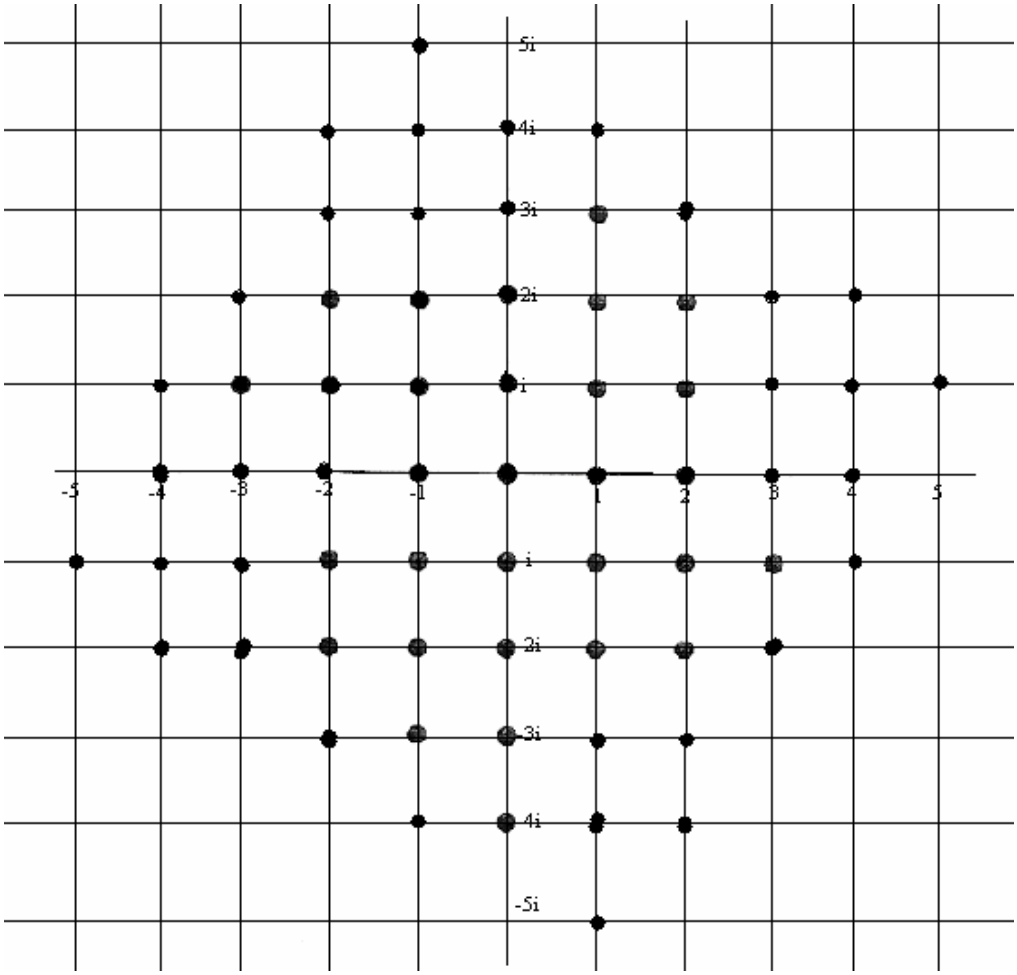
$$G = \begin{pmatrix} 1 & 0 & 1 & i \\ 0 & 1 & -i & -i \end{pmatrix}$$

olan bir lineer kod yazılır. Kontrol matrisi G=($I_k \mid A$) ise $C^\perp$=H=(-$A^T \mid I_{n-k}$) olduğundan şu şekilde yazılır:

$$H = \begin{pmatrix} -1 & i & 1 & 0 \\ -i & i & 0 & 1 \end{pmatrix}$$

Tablo 3.1.1 G_{4+7i} nin elemanları

$\mathbb{Z}_{65}$	G_{4+7i}		$\mathbb{Z}_{65}$	G_{4+7i}		$\mathbb{Z}_{65}$	G_{4+7i}		$\mathbb{Z}_{65}$	G_{4+7i}
0	0		16	-2+ i		32	3-2i		48	1-i
1	1		17	-1+ i		33	-3+2i		49	2-i
2	2		18	İ		34	-2+2i		50	3-i
3	3		19	1+ i		35	-1+2i		51	4-i
4	4		20	2+ i		36	2i		52	-2+3i
5	-2+4 i		21	3+ i		37	1+2i		53	-1+3i
6	-1+4 i		22	4+i		38	2+2i		54	3i
7	4 i		23	5+ i		39	3+2i		55	1+3i
8	1+4 i		24	-1+5i		40	4+2i		56	2+3i
9	-2-3 i		25	-4-2i		41	1-5i		57	-1-4i
10	-1-3 i		26	-3-2i		42	-5-i		58	-4i
11	-3 i		27	-2-2i		43	-4-i		59	1-4i
12	1-3 i		28	-1-2i		44	-3-i		60	2-4i
13	2-3 i		29	-2i		45	-2-i		61	-4
14	-4+ i		30	1-2i		46	-1-i		62	-3
15	-3+ i		31	2-2i		47	-i		63	-2



Şekil 3.1.1 G_{4+7i} nin elemanlarının kompleks düzlemdeki yerleri

3.2. Bazı Sonlu Halkalar Üzerinde Mannheim Metriği İle Devirli Kodlar

$\mathbb{Z}_n$ nin (çarpma işlemine göre) tersinir elemanlarını oluşturduğu küme $\mathbb{Z}_n^*$ ile gösterilir. Eğer $k \geq 1$ ve $k \mid n$ ise

$$\mathbb{Z}_n^*(k) = \left\{ x \in \mathbb{Z}_n^* : x \equiv 1 \bmod k \right\}$$

kümesi $\mathbb{Z}_n^*$ ın bir altgrubudur. [14]

Teorem 3.2.1: [14] s ve t aralarında asal doğal sayılar ise,

i. $\mathbb{Z}_{st}^*(s) \cong \mathbb{Z}_t^*, \mathbb{Z}_{st}^*(t) \cong \mathbb{Z}_s^*$

ii. $\mathbb{Z}_{st}^* \cong \mathbb{Z}_{st}^*(s) \times \mathbb{Z}_{st}^*(t) \cong \mathbb{Z}_s^* \oplus \mathbb{Z}_t^*$

dir.

Önerme 3.2.1: p_1, p_2 birer asal tek tamsayı, $p_1 \neq p_2$ olmak üzere, $\pi_1 = a + bi$, $\pi_2 = c + di$, $p_1 = a^2 + b^2 = 4n_1 + 1$ ve $p_2 = c^2 + d^2 = 4n_2 + 1$ $(a, b, c, d, n_1, n_2 \in \mathbb{Z})$ olacak şekilde π_1, π_2 Gauss tamsayısı olsun. Bu durumda $e^{\phi(p_2)} \equiv 1 (\bmod \pi_1 . \pi_2)$ ve $f^{\phi(p_1)} \equiv 1 (\bmod \pi_1 . \pi_2)$ olacak şekilde bir $e, f \in G_{\pi_1 . \pi_2}^*$ vardır

İspat: p_1, p_2 asal olduklarından aralarında da asal olurlar ve bu durumda π_1 ile π_2 de asal ve aralarında asaldır. Teorem 3.2.1 i. de özel olarak $s = a^2 + b^2 = 4n_1 + 1$ ve $t = c^2 + d^2 = 4n_2 + 1$ şeklinde seçilebilir. Bu durumda (2) fonksiyonu vasıtası ile $\mathbb{Z}_s \cong G_{\pi_1}$, $\mathbb{Z}_t \cong G_{\pi_2}$ ve Teorem 3.1.1 den $\mathbb{Z}_{s.t}(\pi_1) \cong G_{\pi_1 . \pi_2}$ olur. Bununla birlikte,

$$G_{\pi_1 . \pi_2}^*(\pi_1) \cong \mathbb{Z}_{s.t}^*(s) \cong \mathbb{Z}_t^* \cong G_{\pi_2}^* \text{ ve } G_{\pi_1 . \pi_2}^*(\pi_2) \cong \mathbb{Z}_{s.t}^*(t) \cong \mathbb{Z}_s^* \cong G_{\pi_1}^*$$

olur. π_2 bir asal Gauss tamsayı olduğundan $G_{\pi_2}^*$ bir devirli gruptur. Bu devirli grubun bir üreteci vardır. $G_{\pi_1 . \pi_2}^*(\pi_1) \cong G_{\pi_2}^*$ ve $G_{\pi_2}^*$ ın bir üreteci olduğundan $G_{\pi_1 . \pi_2}^*(\pi_1)$ in de bir üreteci vardır. Bu üretece e diyelim. Bu durumda $e^{\phi(p_2)} \equiv 1 \bmod \pi_1 . \pi_2$ olur. Aynı yolla $G_{\pi_1 . \pi_2}^*(\pi_2) \cong G_{\pi_1}^*$ ve $G_{\pi_1}^*$ ın bir üreteci olduğundan $f^{\phi(p_1)} \equiv 1 \bmod \pi_1 . \pi_2$ olacak şekilde $f \in G_{\pi_1 . \pi_2}^*(\pi_2)$ vardır.

Not 3.2.1: Gauss tamsayıları kullanılarak yukarıdaki şartlar altında elde edilen bazı sonlu halkalar üzerinde kodlama yapılacağından burada $k=\pi_1$ (veya $k=\pi_2$) ve $n=\pi_1.\pi_2$ olarak alınacağında daima $k|n$ dir. Ayrıca (2) deki fonksiyon 1-1, örten bir homomorfizma olduğundan (fonksiyon tanım kümesindeki sıfır bölenleri değer kümesindeki sıfır bölenlere karşılık getirmektedir), $G^*_{\pi_1.\pi_2}(\pi_1)\cong\mathbb{Z}^*_{s.t}(s)$, $\mathbb{Z}^*_t\cong G^*_{\pi_2}$ ve $G^*_{\pi_1.\pi_2}(\pi_2)\cong\mathbb{Z}^*_{s.t}(t)$, $\mathbb{Z}^*_s\cong G^*_{\pi_1}$ olur.

Örnek 3.2.1: $53\in\mathbb{Z}^*_{5.13}(13)$ $f:\mathbb{Z}^*_{5.13}(13)\to\mathbb{Z}^*_5$, $f(x)=\min\{x-5t:\ t\in\mathbb{Z},\ x-5t\geq 0\}$ fonksiyonu altında görüntüsü 3 tür. 3, $\mathbb{Z}^*_5$ ın bir üretecidir. 53 sayısının (2) deki fonksiyon altındaki görüntüsü ise $-1+3i\in G_{4+7i}$ ve $4+7i=(2+i).(3+2i)$ dir.

Bu durumda $(-1+3i)^{\phi(5)}\equiv 1\bmod(4+7i)$ olmalıdır. Gerçekten de $(-1+3i)^4\equiv 8-4i\equiv 1\bmod(4+7i)$ dir.

Önerme 3.2.2: p_1, p_2 birer asal tek tamsayı, $p_1\neq p_2$ olmak üzere, $\pi_1=a+bi$, $\pi_2=c+di$, $p_1=a^2+b^2=4n_1+1$ ve $p_2=c^2+d^2=4n_2+1$ $(n_1,n_2\in\mathbb{Z})$ olacak şekilde π_1,π_2 Gauss tamsayısı olsun. Bu durumda $G_{\pi_1.\pi_2}$ halkası üzerinde daima $\phi(p_1)$ ve $\phi(p_2)$ uzunluğunda devirli kod yazılır. Bu devirli kodun üreteç polinomu 1. dereceden bir monik polinomdur.

İspat: Önerme 3.2.1 e göre $e^{\phi(p_2)}\equiv 1(\bmod\pi_1.\pi_2)$ olduğundan;

$$x^{\phi(p_2)}-1=(x-e).D(x)\ \ (\bmod\pi_1\pi_2)$$

şeklinde çarpanlarına ayrılabilir. Buradan $g(x)=x-e$ olarak alınan üreteç polinomu, monik polinom olduğundan bir satırının tüm bileşenleri sıfır bölen olmayan üreteç matrisini üretir.

Önerme 3.2.3: $p_k,(k=1,2,...,m)$ asal tek tamsayılar $p_1\neq p_2\neq\cdots\neq p_m$ olmak üzere $\pi_k=a_k+ib_k$ $(k=1,2,...,m)$ ve $p_k=a_k^2+b_k^2=4n_k+1\,(a_k,b_k\in\mathbb{Z}\ k=1,2,...,m)$ olacak şekilde π_k lar asal Gauss tamsayıları olsun. Bu durumda

$e_k^{\phi(p_k)} \equiv 1 \,(\mathrm{mod}\, \pi_1.\pi_2...\pi_m)\ (k = 1,2,...,m)$ olacak şekilde $e_k \in G^*_{\pi_1.\pi_2...\pi_m}\ \ (k = 1,2,...,m)$ elemanları vardır.

İspat: Önerme 3.2.1 den ispat kolayca görülür.
Bu önerme ile farklı uzunluklara sahip devirli kod yazabilmek hedeflenmiştir.

Örnek 3.2.2: p_1=5, p_2=13 olsun. Bu durumda $(3+i)^{\phi(p_1)} = (3+i)^4 \equiv 1(\mathrm{mod}\, 4+7i)$ olduğundan $x^4 - 1 = (x-3-i).[x^3 + (3+i)x^2 + (4-i)x + 2 - 2i]\ \ \mathrm{mod}(4+7i)$ şeklinde parçalanabilir. Burada $g(x) = x - 3 - i$ ve $h(x) = [x^3 + (3+i)x^2 + (4-i)x + 2 - 2i]$ olarak seçilirse kontrol ve üreteç matrisleri;

$$H = \begin{pmatrix} 1 & 3+i & 4-i & 2-2i \end{pmatrix}$$

ve

$$G = \begin{pmatrix} -3-i & 1 & 0 & 0 \\ 0 & -3-i & 1 & 0 \\ 0 & 0 & -3-i & 1 \end{pmatrix}$$

olarak elde edilir. Bu kod ailesinin 65.65.65=274625 tane kodsözü vardır. Toplam vektör sayısı ise $65^4 = 17.850.625$ dir.

$r(x) = \begin{pmatrix} -3-i & 1 & i & 0 \end{pmatrix}$ gelen vektör olsun. Bu durumda sendrom;

$$\frac{r(x)}{g(x)} = \frac{ix^2 + x - 3 - i}{x - 3 - i} = (x - 3 - i)(ix + 3i) + (1 + 4i)$$

olur. $1 + 4i \equiv x^2.i$ olduğundan $r(x)$;

$$c(x) = r(x) - ix^2 = x - 3 - i$$

şeklinde kodlanır. Böylece

$$c(x) = \begin{pmatrix} -3-i & 1 & 0 & 0 \end{pmatrix}$$

olur. Tablo 3.2.1 de sınıf lideri ve sendromu gösterilmiştir.

Tablo 3.2.1 Sınıf Lideri ve Sendromu

0	0
1	1 (ilgilileri)
x	3+i (ilgilileri)
x^2	4-i (ilgilileri)
x^3	2-2i (ilgilileri)

3.3. Bazı Halkalar Üzerinde Mannheim Metriği İle i-Devirli Kodlar

π, G de bir asal olsun. p, $p>2$ ve $\pi=a+bi$ olmak üzere $p=a^2+b^2=4n+1$ olacak şekilde bir asal tamsayı olsun. Önerme 3.1.4 e göre g, $G^*_{\pi^2}$ ın bir üreteci ise

$$g^{\phi(p^2)/4} \equiv i \bmod \pi^2$$

şeklinde yazılır. Bu durumda,

$$x^{\phi(p^2)/4} - i = (x-g).Q(x) \ (\bmod \pi^2)$$

biçiminde parçalanır. Bu şekilde parçalanarak elde edilen devirli kodlara i devirli kodlar denir.

Örnek 3.3.1: $p=5$ olsun. Bu durumda,

$$\mathbb{Z}_{25} \equiv G_{3+4i} \text{ ve } (-2)^{\phi(p^2)/4} = (-2)^5 \equiv i \,(\bmod 3+4i)$$

olur. Buradan,

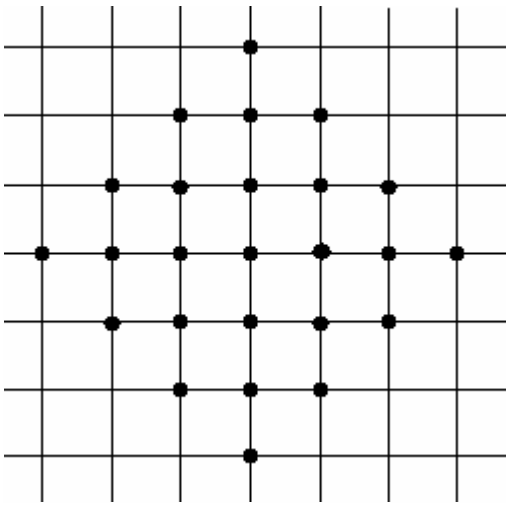
$$x^5 - i = (x+2)(x^4 - 2x^3 + 3ix^2 + (-1+i)x + (-2+i))$$

şeklinde parçalanır. Tablo 3.3.1 de G_{3+4i} nin elemanları ve şekil 3.3.1 de de G_{3+4i} nin elemanlarının düzlemdeki dağılımı gösterilmiştir. $g(x)=x+2$ alınırsa 5 uzunluğunda ki devirli kodun üreteç matrisi aşağıdaki gibidir.

$$G = \begin{pmatrix} 2 & 1 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 2 & 1 \end{pmatrix}$$

Tablo 3.3.1 G_{3+4i} halkasının elemanları

$\mathbb{Z}_{25}$	G_{3+4i}		$\mathbb{Z}_{25}$	G_{3+4i}		$\mathbb{Z}_{25}$	G_{3+4i}		$\mathbb{Z}_{25}$	G_{3+4i}
0	0		7	-i		14	-2i		21	-3i
1	1		8	1-i		15	1-2i		22	-3
2	2		9	2-i		16	-2+i		23	-2
3	3		10	-1+2i		17	-1+i		24	-1
4	3i		11	2i		18	İ		25	0
5	-2-i		12	1+2i		19	1+i		26	1
6	-1-i		13	-1-2i		20	2+i		27	2



Şekil 3.3.1 G_{3+4i} halkasının elemanlarının düzlem üzerindeki dağılımı

3.4. Bazı Halkalar Üzerinde Mannheim Metriği İle Nega-i Devirli Kodlar

π, G de bir asal olsun. p, $p>2$ ve $\pi=a+bi$ olmak üzere $p=a^2+b^2=4n+1$ olacak şekilde bir asal tamsayı olsun. Önerme 3.1.4 e göre g, $G^*_{\pi^2}$ bir üreteci ise

$$g^{\phi(p^2)/4} \equiv -i \bmod \pi^2$$

yazılır. Bu durumda,

$$x^{\phi(p^2)/4}+i=(x-g).R(x) \ (\bmod \pi^2)$$

biçiminde parçalanır. Bu şekilde parçalanarak elde edilen devirli kodlara nega-i devirli kodlar denir.

Örnek 3.4.1: p=5 olsun. Bu durumda x^5+i polinomunun G_{3+4i} halkası üzerinde parçalanışı;

$$x^5+i=(x-2)(x^4+2x^3+3ix^2+(1-i)x+(-2+i)$$

şeklindedir. Tablo 3.3.1 de G_{3+4i} nin elemanları ve şekil 3.3.1 de de G_{3+4i} nin elemanlarının düzlemdeki dağılımı gösterilmiştir. Burada $g(x)=(x-2)$ ve $h(x)=x^4+2x^3+3ix^2+(1-i)x-2+i$ olarak seçilirse kontrol ve üreteç matrisleri;

$$H=\begin{pmatrix}1 & 2 & 3i & 1-i & -2+i\end{pmatrix}$$

ve

$$G=\begin{pmatrix}-2 & 1 & 0 & 0 & 0\\ 0 & -2 & 1 & 0 & 0\\ 0 & 0 & -2 & 1 & 0\\ 0 & 0 & 0 & -2 & 1\end{pmatrix}$$

olur. Tablo 3.4.1 de sınıf lideri ve sendromu gösterilmiştir.

Tablo 3.4.1 Sınıf Lideri ve Sendromu

0	0
1	1 (ve ilgilileri)
x	2 (ve ilgilileri)
x^2	3i (ve ilgilileri)
x^3	1-i (ve ilgilileri)
x^4	-2+i (ve ilgilileri)

$r(x) = \begin{pmatrix} -2 & 1 & 0 & i & 0 \end{pmatrix}$ olsun. Bu durumda sendrom;

$$\frac{r(x)}{g(x)} = (x-2)(ix^2 + 2ix - 2) + (1+i)$$

olarak hesaplanır. $1+i \equiv x^3.i \bmod(3+4i)$ olduğundan $r(x)$ i;

$$c(x) = r(x) - ix^3 = x - 2 \bmod(3+4i)$$

şeklinde dekodlanır. $r(x) = \begin{pmatrix} -2 & 1 & 1 & 2 & 0 \end{pmatrix}$ olsun. Bu durumda sendrom;

$$S = \frac{r(x)}{g(x)} = (x-2)(2x^2 - (2+i)x + 2i) + (2+i)$$

olarak hesaplanır. Ancak $2+i$ kalanı sendromlarda yoktur yani gelen sözde en az iki hata vardır.

3.5. Halka Üzerinde Mannheim Metriği İle Nega-Devirli Kodlar

π, G de bir asal olsun. p, $p>2$ ve $\pi=a+bi$ olmak üzere $p=a^2+b^2=4n+1$ olacak şekilde bir asal tamsayı olsun. Önerme 3.1.4 e göre

$$g_1^{\phi(p^2)/4} \equiv i \bmod \pi^2 \text{ ve } g_2^{\phi(p^2)/4} \equiv -i \bmod \pi^2$$

olacak biçimde $g_1, g_2 \in G^*_{\pi^2}$ vardır. Bu durumda;

$$x^{\phi(p^2)/2}+1=(x-g_1)(x-g_2).B(x)$$

şeklinde parçalanır. Bu şekilde parçalanarak elde edilen devirli kodlara nega-devirli kodlar denir.

Örnek 3.5.1: G_{3+4i} halkası üzerinde $2^5+i \equiv 0 \bmod(3+4i)$ ve $(1-i)^5-i \equiv 0 \bmod(3+4i)$ olduğundan $(x-2).(x-1+i) \mid x^{10}+1$ dir. Yani

$$x^{10}+1=[x^2+(1-2i)x+(-2+i)].[x^8-(1-2i)x^7-(-2+i)x^6-(2+i)x^5-(1+i)x^4 \\ -(2+i)x^3+3ix^2+(-1+2i)x+2i]$$

olur. $g(x)=x^2+(1-2i)x+(-2+i)$ alınırsa üreteç matrisi;

$$G=\begin{pmatrix} -2+i & 1-2i & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -2+i & 1-2i & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -2+i & 1-2i & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -2+i & 1-2i & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -2+i & 1-2i & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -2+i & 1-2i & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -2+i & 1-2i & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -2+i & 1-2i & 1 \end{pmatrix}$$

ve kontrol (parity check) matrisi;

$$H = \begin{pmatrix} 1 & -(1-2i) & -(-2+i) & -(2+i) & -(1+i) & -(2+i) & 3i & -1+i & 2i & 0 \\ 0 & 1 & -(1-2i) & -(-2+i) & -(2+i) & -(1+i) & -(2+i) & 3i & -1+i & 2i \end{pmatrix}$$

olur. Gelen 1 hatalı vektör $r(x) = \begin{pmatrix} -2+i & 1-2i & 1 & i & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$ olsun. Bu durumda sendrom;

$$\frac{ix^3 + x^2 + (1-2i)x + (-2+i)}{x^2 + (1-2i)x + (-2+i)} = [ix - (1+i)].[x^2 + (1-2i)x + (-2+i)] + (1+2i)x + (2+i)$$

ve buradan $S = (1+2i)x + (2+i)$ olarak hesaplanır. $S = (1+2i)x + (2+i) \equiv ix^3$ olduğundan gelen hatalı vektör;

$$c(x) = r(x) - ix^3 = x^2 + (1-2i)x + (-2+i)$$

şeklinde dekodlanır.

BÖLÜM 4. SONUÇLAR VE ÖNERİLER

Manhheim Metriği kullanılarak Gauss tamsayılar halkası üzerinde lineer kodların yapısı incelendi ve bazı sonlu halkalar üzerinde lineer ve devirli kodlar verildi.

Bununla birlikte aynı metrik kullanılarak sonlu halkalar üzerinde BCH kod yazılıp yazılamayacağı araştırılabilir. Ayrıca $G/\langle a+bw\rangle$ ($a,b\in\mathbb{Z}$, $w=cis\frac{\pi}{4}=\frac{\sqrt{2}+i\sqrt{2}}{2}$) halkası üzerinde birimin 8. dereceden kökü olarak $cis\frac{\pi}{4}=\frac{\sqrt{2}+i\sqrt{2}}{2}$ kullanılarak dizayn mesafesi $8n+1$ olan BCH kod yazılıp yazılamayacağı araştırılabilir.

KAYNAKLAR

[1] ÇALLIALP F., "Soyut Cebir", Sakarya Ünv. Yay. No:16, Sakarya, 1995.

[2] ROMAN S., "Coding and Information Theory, Graduate Text in Mathematics, Springer Verlag, 1992.

[3] MACWILLIAMS F.J. and SLOANE N.J., The Theory of Error Correcting Codes, North Holland Pub. Co., 1977.

[4] HUBER K., "Codes Over Gaussian Integers" IEEE Trans. Inform.Theory, vol. 40, pp. 207-216, jan. 1994.

[5] HUBER K., "Codes Over Eisenstein-Jacobi Integers," AMS, Contemp. Math., vol.158, pp. 165-179, 1994.

[6] HUBER K., "The MacWilliams theorem for two-dimensional modulo metric" AAECC Springer Verlag, vol.8, pp.41-48, 1997.

[7] NETO T.P. da N., "Lattice Constellations and Codes From Quadratic NumB. Fields" IEEE Trans. Inf.Theory, vol.47, pp.1514-1527, May 2001.

[8] FAN Y. and GAO Y., "Codes Over Algebraic Integer Rings of Cyclotomic Fields" IEEE Trans. Inform. Theory, vol. 50, No. 1 jan. 2004.

[9] McDONALDS B.R., "Finite Rings With Identity", Marcel Dekkar, New York, 1974.

[10] ADLER A. and COURY J.E., "The Theory of Number" The University of British Colombia, Jones and Bartlett Publishers.Inc., 1995.

[11] ÇALLIALP F., "Sayılar Teorisi" Marmara Üniversitesi, İstanbul, 1999.

[12] DRESDEN G. and DYMACEK W.M., "Finding Factors of Factor Rings Over The Gaussian Integers" The Mathematical Association of America, Monthly Aug-Sep. 2005.

[13] ZIVEN I., ZUCKERMAN H.S. and MONTGOMERY H.L., "An Introduction to The Number Theory" John Wiley & Sons, İnc., 1991.

[14] KARAKAŞ H.İ.,"Soyut Cebire Giriş"M.V.ODTÜ Ankara,1998.

ÖZGEÇMİŞ

Murat Güzeltepe, 10.04.1981 de Erzurum' da doğdu. İlk, orta ve lise eğitimini Erzurum'da tamamladı. 1995 yılında Erzurum Lisesi'nden mezun oldu. 1996 yılında başladığı Atatürk Üniversitesi Fen Edebiyat Fakültesi Matematik Bölümü'nü 2000 yılında bitirdi. 2000-2007 yılları arasında Milli Eğitim Bakanlığı'na bağlı çeşitli okullarda matematik öğretmenliği yaptı. 19 Aralık 2006 da Sakatya Üniversitesi Fen Edebiyat Fakültesi Matematik Bölümü'nde araştırma görevlisi olarak göreve başladı. Halen Sakarya Üniversitesi Fen Edebiyat Fakültesi Matematik Bölümü'nde araştırma görevlisi olarak görev yapmaktadır.