İSTANBUL KÜLTÜR ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

BCH KODLARI

YÜKSEK LİSANS TEZİ
Selda ÇALKAVUR
0309042008

Anabilim Dalı : Matematik Bilgisayar
Programı : Matematik Bilgisayar

Tez Danışmanı: Prof. Dr. Erol BALKANAY

ŞUBAT 2006

İÇİNDEKİLER

ÖNSÖZ

İstanbul Kültür Üniversitesi Fen Bilimleri Enstitüsü'ne bağlı Matematik Bilgisayar Ana Bilim Dalı, Matematik Bilgisayar Yüksek Lisans Programı'nın son aşaması olan bu tez çalışmasında, "BCH Kodları" ele alınmıştır.

Çalışmalarım esnasında, beni yalnız bırakmayan, değerli görüş ve fikirleri ile bu teze yön veren ve her türlü desteğini esirgemeyen saygıdeğer hocam Sayın Prof. Dr. Erol Balkanay'a katkılarından dolayı teşekkür etmeyi büyük bir borç bilir, saygılarımı sunarım.

Bugüne kadar bana hep destek olan başta babam Yusuf Çalkavur'a, bütün aileme ve görev yaptığım okul müdürüm Canan Ertekin'e de teşekkür ederim.

İstanbul, Şubat 2006 Selda ÇALKAVUR

ABSTRACT

This study which examines BCH codes consist of six chapters.

Chapter 1 develops those concepts from Abstract Algebra that are necessary to an uderstanding of BCH codes. Finite fields and structure of finite fields are introduced in this chapter.

Chapter 2 is devoted to presantation of polynomials over finite fields. Construction of irreducible polynomials are also given.

Chapter 3 contains an introduction to coding theory. In this chapter linear codes, generator matrix of a code, dual code and parity-check matrix are considered.

Hamming codes are introduced in chapter 4.

The properties of cylic codes, generator polynomial of cylic codes are presented in chapter 5.

Chapter 6 covers in detail BCH codes. Primitive element, primitive polynomial and minimal polynomiala are examined. A class of BCH codes for $t-$error correction is presented. Further, in this chapter the new developments of BCH codes and Goppa codes are presented.

Key Words: Finite fields, roots of unity and cyclotomic polynomials, order of polynomials, irreducible polynomials, linear codes, Hamming codes, cylic codes, generator polynomial, primitive element, primitive polynomial, minimal polynomials, designed distance, BCH codes, Reed-Solomon codes, Goppa codes.

ÖZET

BCH kodlarının ele alındığı bu çalışma, altı bölümden oluşmaktadır.

Bölüm 1'de BCH kodları için gerekli cebirsel bilgiler verilmiştir. Sonlu cisimler ve sonlu cisimlerin yapısı incelenmiştir.

Bölüm 2'de sonlu cisimler üzerinde polinomlardan söz edilmiş, indirgenemez polinomların kuruluşu ele alınmıştır.

Bölüm 3'te kodlar teorisine bir giriş yapılmıştır. Bu bölümde lineer kodlar, bir kodun üreteç matrisi, dual kod ve eşlik-denetim (parity-check) matrisi incelenmiştir.

Bölüm 4'te Hamming kodlarından söz edilmiştir.

Bölüm 5'te devresel kodların özelikleri, devresel kodların üreteç polinomu gösterilmiştir.

Bölüm 6'da BCH kodları detaylı bir şekilde incelenmiştir. Primitif eleman, primitif polinom ve minimal polinomlar anlatılmıştır. t – hata düzelten BCH kodlarının bir sınıfı ele alınmıştır. Ayrıca bu bölümde, BCH kodları hakkındaki son gelişmeler ve Goppa kodları anlatılmıştır.

Anahtar kelimeler: Sonlu cisimler, birimin kökleri ve cyclotomic polinomlar, polinomların mertebesi, indirgenemez polinomlar, lineer kodlar, Hamming kodları, devresel kodlar, üreteç polinomu, primitif eleman, primitif polinom, minimal polinomlar, tasarlanmış mesafe, BCH kodları, Reed-Solomon kodu, Goppa kodları.

SEMBOL LİSTESİ

BCH kodu : Bose-Chaudri-Hocquenghem kodları

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

C_{15} : 15 uzunluklu iki-hata düzelten BCH kodu

$E^{(n)}$: K cismi üzerinde birimin $n.$ köklerinin kümesi

F_q, $GF(q)$: Mertebesi $q = p^h$ (p asal, h pozitif tam sayı) olan Galois cismi

$(F_q)^n$: F_q nun elemanlarının sıralı $n-$lilerinin kümesi

$F_q[x]$: Katsayıları F_q da olan polinomlar halkası

F_q^* : F_q sonlu cisminin sıfırdan farklı elemanlarının çarpım grubu

F_{q^m} : $F_q[x]$ deki m dereceli indirgenemez f polinomunun F_q üzerinde parçalanış cismi

$F^m[x]$: $F[x]$ deki derecesi m den daha küçük olan tüm polinomların kümesi

$|F|$: F cisminin eleman sayısı

f_t : F_q üzerinde $\alpha^t \in F_{q^m}$ nin karakteristik polinomu

G^T : G üreteç matrisinin transpozesi

Ham$(r, 2)$: İkili (binary) Hamming kodu

$\mu(n)$: Moebious μ fonksiyonu

$N_q(d)$: $F_q[x]$ de derecesi d olan indirgenemez monik polinomların sayısı

$ord(f)$: f polinomunun mertebesi

RS kodu : Reed-Solomon kodu

$\Gamma(L, g)$: Goppa kodu

$[L : K]$: K cismi üzerinde L sonlu vektör uzayının derecesi

TABLO LİSTESİ

BÖLÜM 1

SONLU CİSİMLER

Bu bölüm, tezin asıl konusu olan BCH kodları için gerekli cebirsel bilgilerin özetlenmesine ayrılmıştır. Bu nedenle çoğu teorem, ispatsız olarak verilecektir.

Sonlu cisim, sonlu sayıda elemana sahip olan bir cisimdir. Bu eleman sayısı, cismin mertebesi olarak adlandırılır.

Sonlu cisimlerin mertebeleriyle ilgili, aşağıdaki önemli teoremi verelim.

Teorem 1.1. q mertebeli bir cismin var olması için gerek ve yeter koşul, q nun bir asal sayının kuvveti şeklinde olmasıdır. Yani; h pozitif bir tam sayı olmak üzere, $q = p^h$ biçiminde ifade edilir. ∎

q mertebeli bir cisim genellikle, q mertebeli bir GALOIS CİSMİ olarak adlandırılır ve "$GF(q)$" şeklinde gösterilir. (Kodlar üzerine çalışırken, ağırlıklı olarak "$GF(q)$" yerine "F_q" notasyonu kullanılmaktadır. Çalışmalarımızda "$GF(q)$" ve "F_q" aynı anlamda kullanılacaktır.

1.1. Cisim Genişlemeleri

F bir cisim olsun. F nin bir K alt kümesi, F deki işlemlere göre bir cisim ise F cismine, K nın bir cisim genişlemesi denir. K ya da, F nin bir alt cismi denmektedir. $K \neq F$ halinde K, bir öz alt cisim adını alır.

K, F_p (p asal) sonlu cisminin bir alt cismi ise bu durumda K, 0 ve 1 elemanlarını içermelidir.

Tanım 1.1.1. Öz alt cisimler içermeyen bir alt cisim, asal cisim adını alır.

Bu ifade; p mertebeli (p asal) herhangi bir cismin, bir asal cisim olduğunu gösterir. Q rasyonel sayılar cismi, asal cisme diğer bir örnektir.

Verilen bir F cisminin alt cisimlerinin boş olmayan topluluğunun bir kesişimi, yine F nin bir alt cismidir. F nin tüm alt cisimlerinin bir kesişimi ise, kesinlikle bir asal cisimdir.

Teorem 1.1.1. R, asal karakteristikli bir komütatif halka olsun. R nin karakteristiği p asal sayısı ise,

$$(a+b)^{p^n} = a^{p^n} + b^{p^n}$$

ve

$$(a-b)^{p^n} = a^{p^n} - b^{p^n} \qquad (a,\ b \in R \text{ ve } n \in \mathrm{N})$$

dir.

Teorem 1.1.2. Bir F cisminin asal alt cismi; F nin karakteristiği, p asalı veya sıfır olarak düşünülürse, F_p veya Q rasyonel sayılar cisminin ikisinden birine izomorfiktir.

Tanım 1.1.2. K, F cisminin bir alt cismi ve M, F nin herhangi bir alt kümesi olsun. Bu durumda $K(M)$; K ve M nin her ikisini de içeren, F nin tüm alt cisimlerinin kesişimi olan cisim olarak tanımlanır ve K nın elemanlarının eklenmesiyle elde edilen bir cisim genişlemesi adını alır.

Sonlu $M = \{\theta_1,...,\theta_n\}$ kümesi için $K(M)$ olarak, $K(M) = K(\theta_1,...,\theta_n)$ yazılır. M, bir tek $\theta \in F$ elemanını içeriyorsa bu durumda $L = K(\theta)$, K nın bir basit genişlemesi olarak ifade edilir ve θ, K üzerinde L nin tanımlayıcı bir elemanı adını

alır. $K(M)$ kesinlikle K ve M nin her ikisini de içeren F nin en küçük alt cismidir.

Tanım 1.1.3. K, F nin bir alt cismi ve $\theta \in F$ olsun. θ, K daki katsayılarla trivial olmayan bir polinom denklemini sağlıyorsa, yani

$$a_n \theta^n + a_{n-1}\theta^{n-1} + \ldots + a_1 \theta + a_0 = 0 \quad (a_i \in K)$$

(hepsi birden sıfır değil) ise bu durumda θ ya, K üzerinde cebirseldir denir.
L nin her elemanı K üzerinde cebirsel ise; K nın bir L genişlemesi, K üzerinde bir cebir veya K nın bir cebirsel genişlemesi olarak adlandırılır.

Tanım 1.1.4. $\theta \in F$, K üzerinde cebirsel ise bu durumda $J = \{f \in K[x] : f(\theta) = 0\}$ idealini üreten, bir tek şekilde belirli monik $g \in K[x]$ polinomuna, θ nın K üzerinde minimal polinomu adı verilir.

K üzerinde θ nın derecesi ile g nin derecesi anlaşılacaktır.

Tanım 1.1.5. L, K nın bir cisim genişlemesi olsun. L, K üzerinde bir sonlu vektör uzayı olarak düşünülürse L ye, K nın bir sonlu genişlemesi adı verilir. K üzerinde L vektör uzayının boyutu, K üzerinde L nin derecesi olarak adlandırılır ve $[L : K]$ ile gösterilir.

Teorem 1.1.3. L, K nın bir sonlu genişlemesi ve M, L nin bir sonlu genişlemesi ise bu durumda M, K nın bir sonlu genişlemesidir.

$$[M : K] = [M : L][L : K]$$

İspat. $[M : L] = m,$

$[L : K] = n,$

L üzerinde M nin bir tabanı $\{\alpha_1,\ldots,\alpha_m\}$ ve K üzerinde L nin bir tabanı $\{\beta_1,\ldots,\beta_n\}$ olsun. Bu durumda,

α , $\forall\ \alpha \in M$ için $\alpha = \gamma_1\ \alpha_1 + \ldots + \gamma_m\ \alpha_m$, $(\gamma_i \in L \quad 1 \le i \le m)$

şeklinde bir lineer kombinasyondur ve γ_i lerin her birini β_j taban elemanları cinsinden ifade edersek,

$$\alpha = \sum_{i=1}^{m} \gamma_i \alpha_i = \sum_{i=1}^{m} (\sum_{j=1}^{n} r_{ij} \beta_j) \alpha_i = \sum_{i=1}^{m} \sum_{j=1}^{n} r_{ij} \beta_j \alpha_i \ , \qquad (\mathrm{r}_{ij} \in K)$$

elde edilir.

mn tane $\beta_j \alpha_i$ $(1 \le i \le m\,,\ 1 \le j \le n)$ elemanlarının K üzerinde lineer bağımsız olduğu gösterilebilirse, ispat tamamlanmış olur. Bu amaçla,

$$\sum_{i=1}^{m} \sum_{j=1}^{n} s_{ij} \beta_j \alpha_i = 0\,, \quad (s_{ij} \in K)$$

olduğunu kabul edelim.

O zaman,

$$\sum_{i=1}^{m} (\sum_{j=1}^{n} s_{ij} \beta_j) \alpha_i = 0$$

dır ve L üzerinde α_i nin lineer bağımsızlığından,

$$\sum_{j=1}^{n} s_{ij} \beta_j = 0 \quad (1 \le i \le m)$$

sonucu elde edilir. Fakat β_j ler K üzerinde lineer bağımsız olduklarından, tüm s_{ij} ler "0" dır.

Teorem 1.1.4. K nın her sonlu genişlemesi, K üzerinde cebirseldir.

İspat. L, K nın bir sonlu genişlemesi ve $[L:K]=m$ olsun. $\theta \in L$ için, $1, \theta, \ldots, \theta^m$ gibi $m+1$ tane eleman, K üzerinde lineer bağımlı olmalıdır ve bu nedenle

$$a_0 + a_1\theta + \ldots + a_m\phi^m = 0, \ (a_i \in K)$$

dır.

Bu ifade, θ nın K üzerinde cebirsel olduğunu gösterir.

1.2. Sonlu Cisimlerin Yapısı

Yardımcı Teorem 1.2.1. F , q elemanlı bir K alt cismini içeren sonlu cisim olsun. Bu durumda $m=[F:K]$ olmak üzere,

$$|F| = q^m$$

dir. $|F|$ ile, F cisminin eleman sayısı gösterilmektedir.

İspat. F, K üzerinde bir vektör uzayı ve F sonludur. Bu nedenle F, K üzerinde sonlu bir vektör uzayı olarak düşünülebilir. $[F:K]=m$ ise F; $b_1, b_2, \ldots, b_m$ gibi m tane eleman içeren, K üzerinde bir tabana sahiptir. Bu nedenle F nin her elemanı bir tek şekilde,

$$a_1b_1 + a_2b_2 + \ldots + a_mb_m \quad (a_1, a_2, \ldots, a_m \in K)$$

olarak gösterilebilir. Her a_i katsayısı, q çeşit değer alabileceğinden F cismi, kesinlikle q^m elemanlıdır.

Teorem 1.2.1. F, bir sonlu cisim olsun. F nin karakteristiği p asalı ve onun asal alt cismi üzerinde F nin derecesi n olduğunda, F nin tam p^n elemanı vardır.

İspat. F sonlu ise, F nin karakteristiği bir p asalıdır. Buna göre teorem 1.1.2. gereğince, F nin asal alt cismi K, F_p ye izomorfiktir. Bu nedenle F nin eleman sayısı, p^n dir.

Yardımcı Teorem 1.2.2. F, q elemanlı bir sonlu cisim ise,

$\forall a \in F$ için $a^q = a$

dır.

İspat. $a^q = a$ özdeşliği, $a = 0$ için apaçık bellidir. Diğer yandan; F nin sıfırdan farklı elemanları, çarpma işlemi altında, mertebesi $q-1$ olan bir grup oluşturur.

Bu nedenle;

$a^{q-1} = 1 \qquad (\forall a \in F,\ a \neq 0)$

dir.

İspatlanması gereken de budur.

Yardımcı Teorem 1.2.3. F, q elemanlı bir sonlu cisim ve K, F nin bir alt cismi olsun. O zaman $K[x]$ deki $x^q - x$ polinomu, $F[x]$ de

$$x^q - x = \prod_{a \in F} (x - a)$$

şeklinde çarpanlarına ayrılır. Burada F, $x^q - x$ in K üzerinde bir parçalanış cismidir.

Teorem 1.2.2. (Sonlu Cisimlerin Varlığı ve Tekliği)

Her p asalı ve her pozitif n tam sayısı için, p^n elemanlı bir sonlu cisim vardır. $q = p^n$ elemanlı herhangi bir sonlu cisim, F_p üzerinde $x^q - x$ in parçalanış cismine izomorfiktir.

İspat. (Varlık)

$q = p^n$ olmak üzere $F_p[x]$ de $x^q - x$ ele alınsın ve F, onun F_p üzerindeki parçalanış cismi olsun. Bu polinom, F de q tane farklı köke sahiptir ve polinomun türevi $F_q[x]$ de,

$$qx^{q-1} - 1 = -1$$

dir.

Bu yüzden kök, $x^q - x$ ile ortak köke sahip olmaz.

$$S = \{a \in F : a^q - a = 0\}$$

olsun. Bu durumda S, F nin bir alt cismidir.

(i) S, 0 ve 1 i içerir.

(ii) $a, b \in S$ ve teorem 1.1.1. gereğince,

$$(a-b)^q = a^q - b^q = a - b$$

anlamına gelir ve buradan,

$$a - b \in S$$

elde edilir.

(iii) $a, b \in S$ ve $b \neq 0$ için;

$$(ab^{-1})^q = a^q b^{-q} = ab^{-1}$$

ve bu yüzden $ab^{-1} \in S$ tir. S, tüm $x^q - x$ in köklerini içerdiğinden, bu ifade S de parçalanmalıdır.

Bu nedenle $F = S$ ve S nin q tane elemanı vardır. Dolayısıyla F, q elemanlı bir sonlu cisimdir.

(Teklik)

F, $q = p^n$ elemanlı bir sonlu cisim olsun. Bu durumda teorem 1.2.1. gereğince, F nin karakteristiği p dir ve F, F_p gibi bir alt cisim içerir. Yardımcı teorem 1.2.3. gereğince F, F_p üzerindeki $x^q - x$ in bir parçalanış cismidir. Parçalanış cismi de tektir. (İzomorfikler aynı sayılmak koşuluyla.)

Teorem 1.2.3. (Alt Cisim Ölçütü)

F_q, $q = p^n$ elemanlı bir sonlu cisim olsun. F_q nun her alt cismi, n nin pozitif bir böleni m olmak üzere, p^m mertebelidir. Karşıt olarak n nin pozitif bir böleni m ise F_q nun p^m elemanlı bir tane alt cismi vardır.

İspat. F_q nun bir K alt cisminin mertebesi, uygun bir $m \le n$ pozitif tam sayısı için, p^m dir. Yardımcı teorem 1.2.1. den dolayı;

$q = p^n$, p^m nin bir kuvveti olmak durumundadır. $(p^n = (p^m)^t)$

Böylece,

$m \mid n$

bulunur.

Tersine; n nin pozitif bir böleni m ise,

$p^m - 1 \mid p^n - 1$

dir. Böylece, $F_p[x]$ de $x^{p^m-1} - 1$ polinomu, $x^{p^n-1} - 1$ polinomunu böler.

Sonuç olarak; $x^{p^m} - x$ polinomu, $x^{p^n} - x = x^q - x$ polinomunu böler.

F_q, F_p üzerindeki $x^{p^m} - x$ in bir parçalanış cismi gibi görülen bir alt cisim içermelidir ve teorem 1.2.2. nin ispatında, bir parçalanış cisminin mertebesinin p^m olduğu gösterilmişti. ∎

Teorem 1.2.3 ün ispatı; n nin pozitif bir böleni m olduğunda p^m mertebesinin, F_{p^n} nin bir tek alt cismine ait olduğunu gösterir. Bu alt cisim, F_{p^n} deki $x^{p^m} - x \in F_p[x]$ polinomunun köklerini kesinlikle içerir.

Tanım 1.2.1. Bir F_q sonlu cismi için, F_q nun sıfırdan farklı elemanlarının çarpım grubu, F_q^* ile gösterilir.

Teorem 1.2.4. Her F_q sonlu cismi için, F_q nun sıfırdan farklı elemanlarının çarpım grubu F_q^*, devreseldir.

Tanım 1.2.2. F_q^* devresel grubunun bir üreteci, F_q nun primitif bir elemanı olarak adlandırılır.

Teorem 1.2.5. F_q bir sonlu cisim ve F_r, bir sonlu cisim genişlemesi olsun. Bu durumda F_r, F_q nun basit bir cebirsel genişlemesidir ve F_r nin her primitif elemanı, F_q üzerinde F_r nin tanımlayıcı elemanı olarak işlev görür.

İspat. F_r nin bir primitif elemanı ξ olsun. $F_q(\xi) \subseteq F_r$ olduğu açıktır. Başka bir ifadeyle $F_q(\xi)$, ξ nin tüm kuvvetlerini ve sıfırı içerir. Bu nedenle $F_q(\xi)$, F_r nin tüm elemanlarını içerir. Dolayısıyla,

$$F_r = F_q(\xi)$$

dir.

Teorem 1.2.6. Her F_q sonlu cismi ve her pozitif n tam sayısı için $F_q[x]$ de, derecesi n olan indirgenemez bir polinom vardır.

İspat. F_r, F_q cisminin genişlemesi ve F_r nin mertebesi q^n olsun. Bu durumda,

$$[F_r : F_q] = n$$

dir. Teorem 1.2.5. gereğince,

$$\exists \xi \in F_r \text{ için } F_r = F_q(\xi)$$

dir. O halde, F_q üzerinde ξ nin minimal polinomu, $F_q[x]$ de n dereceli indirgenemez bir polinomdur.

Not. Her q asal sayısı ve her pozitif n tam sayısı için, F_q üzerinde n dereceli indirgenemez bir polinom vardır. Bu sonuç, her $n \geq 1$ tam sayısı için F_{q^n} cisminin varlığını gösterir.

Yardımcı Teorem 1.2.4. $f \in F_q[x]$, F_q üzerinde m dereceli indirgenemeyen bir polinom olsun. Bu durumda $f(x)$ in, $x^{q^n} - x$ i bölmesi için gerek ve yeter koşul, m nin n yi bölmesidir.

İspat. $f(x)$ in $x^{q^n} - x$ i böldüğünü kabul edelim. α, F_q üzerinde f nin parçalanış cismi içindeki bir kökü olsun.

Bu durumda,

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

dır ki,

$$\alpha \in F_{q^n}$$

dir.

$F_q(\alpha)$, F_{q^n} nin bir alt cismidir. Fakat,

$[F_q(\alpha) : F_q] = m$ ve $[F_{q^n} : F_q] = n$

idi. Bu da teorem 1.1.3. gereğince, m nin n yi böldüğünü gösterir.

Karşıt olarak m, n yi bölüyorsa teorem 1.2.3. gereğince, F_{q^n} nin F_{q^m} yi bir alt cisim olarak içerdiği anlaşılmaktadır.

F üzerinde f nin parçalanış cismi içindeki f nin bir kökü α ise,

$[F_q(\alpha) : F_q] = m$

ve

$F_q(\alpha) = F_{q^m}$

dir.

Sonuç olarak; $\alpha \in F_{q^n}$ ve böylece,

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

olur. Bu nedenle α, $x^{q^n} - x \in F_q[x]$ in bir köküdür.

Dolayısıyla $f(x)$, $x^{q^n} - x$ i böler.

Teorem 1.2.7. $F_q[x]$ de m dereceli indirgenemez bir polinom f ise, f nin F_{q^m} de bir α kökü vardır. Bundan başka, f nin tüm kökleri basit köktür ve F_q nun m tane farklı elemanı olan $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ ile verilirler.

İspat. F_q üzerinde f nin parçalanış cismi içinde f nin bir kökü α olsun.

Bu durumda,

$$[F_q(\alpha) : F_q] = m$$

dir. Böylece,

$$F_q(\alpha) = F_{q^m}$$

ve özel olarak,

$$\alpha \in F_{q^m}$$

dir.

$\beta \in F_{q^m}$, f nin bir kökü ise β^q nun da, f nin bir kökü olduğunu göstereceğiz.

$a_i \in F_q$ olacak şekilde,

$$f(x) = a_m x^m + ... + a_1 x + a_0, \quad (0 \le i \le m)$$

yazılsın. Bu durumda yardımcı teorem 1.2.2. ve teorem 1.1.2. gereğince;

$$f(\beta^q) = a_m \beta^{qm} + ... + a_1 \beta^q + a_0 = a_m{}^q \beta^{qm} + ... + a_1{}^q \beta^q + a_0{}^q$$

$$= (a_m \beta^m + ... + a_1 \beta + a_0)^q = f(\beta)^q = 0$$

dır.

Bundan dolayı; α, α^q, α^{q^2}, …, $\alpha^{q^{m-1}}$ elemanları, f nin kökleridir. Bu elemanların farklı olduğu gösterilmelidir.

Tersini kabul edelim. Yani, bu elemanlar farklı olmasın.

$\alpha^{q^j} = \alpha^{q^k}$ (bazı j ve k tam sayıları için) $(0 \le j < k \le m-1)$

kabul edelim. Bunun q^{m-k} kuvveti alınırsa,

$$\alpha^{q^{m-k+j}} = \alpha^{q^m} = \alpha$$

elde edilir.

Bu durumda $f(x)$, $x^{q^{m-k+j}} - x$ i böler. Yardımcı teorem 1.2.4. gereğince bu durum sadece m, $m-k+j$ yi bölerse mümkündür. Fakat,

$$0 < m-k+j < m$$

idi. Bu nedenle kabulümüz yanlıştır.

Sonuç 1.2.1. f, $F_q[x]$ de m dereceli indirgenemez bir polinom olsun. Bu durumda F_q üzerinde f nin parçalanış cismi, F_{q^m} ile verilir.

İspat. Teorem 1.2.7., F_{q^m} de f nin parçalandığını gösterir. Ayrıca F_{q^m} deki f nin bir α kökü için,

$$F_q(\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}) = F_q(\alpha) = F_{q^m}$$

dir.

Sonuç 1.2.2. $F_q[x]$ de dereceleri aynı olan herhangi iki indirgenemez polinom, izomorfik parçalanış cismine sahiptir.

Tanım 1.2.3. F_{q^m}, F_q nun bir genişlemesi ve $\alpha \in F_{q^m}$ olsun. Bu durumda $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ elemanlarına F_q ya göre α nın eşlenikleri denir.

$\alpha \in F_{q^m}$ nin eşleniklerinin farklı olması için gerek ve yeter koşul, α nın F_q üzerinde minimal polinomunun derecesinin m olmasıdır. Aksi halde; bu minimal polinomun derecesi d, m nin bir öz bölenidir ve bu durumda α nın eşlenikleri $\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}$ olup, her biri m/d kez tekrarlanır.

Teorem 1.2.8. F_q nun herhangi bir alt cismine göre $\alpha \in F_q^*$ nın eşlenikleri, F_q^* grubu içerisinde aynı dereceye sahiptir.

İspat. Teorem 1.2.4. gereğince F_q^*, bir devresel gruptur. F_q nun karakteristiğinin her kuvveti, F_q^* ın $q-1$ mertebesi ile aralarında asaldır.

Sonuç 1.2.3. Eğer α, F_q nun bir primitif elemanı ise F_q^* nın herhangi alt cismine göre tüm eşlenikleri de, primitif elemandır.

Örnek 1.2.1. $\alpha \in F_{16}$, $f(x) = x^4 + x + 1 \in F_2[x]$ in bir kökü olsun. O zaman α nın F_2 ye göre eşlenikleri,

$$\alpha,\ \alpha^2,\ \alpha^4 = \alpha + 1$$

ve

$$\alpha^8 = \alpha^2 + 1$$

olur.

Eşleniklerin her biri, F_{16} nın primitif elemanlarıdır.

α nın F_4 e göre eşlenikleri, α ve

$$\alpha^4 = \alpha + 1$$

dir.

1.3. Birimin Kökleri ve Cyclotomic Polinomlar

Tanım 1.3.1. n, pozitif bir tam sayı olsun. Bir K cismi üzerinde $x^n - 1$ in parçalanış cismi, K üzerinde "n. cyclotomic cisim" adını alır ve "$K^{(n)}$" ile gösterilir. $K^{(n)}$ de $x^n - 1$ in kökleri, K üzerinde "birimin n. kökleri" adını alır ve bu köklerin tamamının kümesi, "$E^{(n)}$" ile gösterilir.

Teorem 1.3.1. n, pozitif bir tam sayı ve K, p karakteristikli bir cisim olsun.

Bu durumda;

(i) p, n yi bölmezse bu durumda $E^{(n)}$, $K^{(n)}$ deki çarpmaya göre n mertebeli bir devresel gruptur.

(ii) p, n yi bölerse, pozitif m ve e tam sayıları ile

$$n = mp^e$$

yazılır ve m, p ile bölünemez. Bu durumda;

$$K^{(n)} = K^{(m)},\ E^{(n)} = E^{(m)}$$

ve

$K^{(n)}$ de $x^n - 1$ in kökleri, $E^{(m)}$ nin m tane elemanıdır. Bu elemanların her biri p^e ile çarpılarak elde edilir.

Tanım 1.3.2. K, p karakteristikli bir cisim ve n, p ile bölünemeyen pozitif bir tam sayı olsun. Bu durumda $E^{(n)}$ devresel grubunun bir üreteci, K üzerinde "birimin n. primitif kökü" adını alır.

Tanım 1.3.3. K, karakteristiği p olan bir cisim; n, p ile bölünemeyen pozitif bir tam sayı ve ξ, K üzerinde birimin n. primitif kökü olsun.

Bu durumda,

$$Q_n(x) = \prod_{s=1}^{n} (x - \xi^s), \qquad ((s,n)=1)$$

polinomu, K üzerinde "n. cyclotomic polinom" adını alır.

Teorem 1.3.2. K, karakteristiği p olan bir cisim ve n, p ile bölünemeyen pozitif bir tam sayı olsun. Bu durumda;

(i) $x^n - 1 = \prod_{d|n} Q_d(x)$,

(ii) Eğer K nın asal alt cismi rasyonel sayılar cismi ise $Q_n(x)$ in katsayıları, K nın asal alt cismine ve Z'e aittir.

Örnek 1.3.1. r bir asal sayı ve $k \in \mathrm{N}$ olsun. Bu durumda,

$$Q_{r^k}(x) = 1 + x^{r^{k-1}} + x^{2r^{k-1}} + \ldots + x^{(r-1)r^{k-1}}$$

dir.

Çünkü teorem 1.3.2. (i) gereğince,

$$Q_{r^k}(x) = \frac{x^{r^k} - 1}{Q_1(x)Q_r(x)\ldots Q_{r^{k-1}}(x)} = \frac{x^{r^k} - 1}{x^{r^{k-1}} - 1}$$

idi.

$k = 1$ için $Q_r(x) = 1 + x + x^2 + \ldots + x^{r-1}$

olur.

Teorem 1.3.3. $K^{(n)}$ cyclotomic cismi, K nın basit bir cebirsel genişlemesidir. Dahası,

(i) Eğer K, rasyonel sayılar cismi ise bu durumda Q_n cyclotomic polinomu, K üzerinde indirgenemezdir ve

$$[K^{(n)} : K] = \phi(n)$$

dir.

(ii) $(g,n) = 1$ iken $K = F_q$ ise bu durumda Q_n, $K[x]$ de her biri aynı d dereceli olan $\phi(n)/d$ tane monik indirgenemez çarpanlara ayrılır. $K^{(n)}$ cismi, K üzerinde herhangi böyle indirgenemez çarpanın parçalanış cismidir ve

$$[K^{(n)} : K] = d$$

dir. Burada d, $q^d \equiv 1 \mod n$ şeklindeki en küçük pozitif tam sayıdır.

Bu teoremi bir örnek üzerinde açıklayalım:

Örnek 1.3.2. $K = F_{11}$ ve $Q_{12}(x) = x^4 - x^2 + 1 \in F_{11}[x]$ olsun. Teorem 1.3.3. (ii) den dolayı $d = 2$ olur. $Q_{12}(x)$,

$$Q_{12}(x) = (x^2 + 5x + 1)(x^2 - 5x + 1)$$

şeklinde çarpanlarına ayrılır. Çarpanlarına ayrılan çarpanların her ikisi de $F_{11}[x]$ de indirgenemezdir. $K^{(12)}$ cyclotomic cismi, F_{121} e eşit olur.

Teorem 1.3.4. F_q sonlu cismi, kendi alt cisimlerinin herhangi biri üzerinde $(q-1)$ nci cyclotomic cisimdir.

Yardımcı teorem 1.3.1. d **,** pozitif n tam sayısının $(1 \le d \le n)$ bir böleni ise bu durumda $Q_n(x)$, $x^n - 1/x^d - 1$ ifadesini böler.

1.4. Sonlu Cisimlerin Elemanlarının Gösterilmesi

f , $F_p[x]$ de n dereceli indirgenemez bir polinom ise bu durumda teorem 1.2.7 ye göre f , F_q da bir α köküne sahiptir. Dolayısıyla,

$$F_q = F_p(\alpha)$$

dır. O halde; F_q nun her elemanı, F_p üzerinde derecesi n den daha küçük bir polinom olarak bir tek şekilde ifade edilir. F_q ya, $F_p[x]/(f)$ kalan sınıf halkası olarak bakılabilir.

Örnek 1.4.1. F_9 un elemanlarını bu yolla göstermek için F_9 a; F_3 ün, derecesi 2 olan, basit bir cebirsel genişlemesi olarak bakarız. Bu, F_3 üzerinde indirgenemez ve ikinci dereceden bir polinomun bir α kökünü eklemekle elde edilir.

$$f(x) = x^2 + 1 \in F_3[x]$$

diyelim.

Böylece,

$$f(\alpha) = \alpha^2 + 1 = 0 \in F_9$$

dır ve F_9 un 9 tane elemanı, $a_0 + a_1\alpha$ şeklinde verilir. (a_0 , $a_1 \in F_3$)

Ayrıntılı olarak,

$$F_9 = \{0, 1, 2, \alpha, 1+\alpha, 2+\alpha, 2\alpha, 1+2\alpha, 2+2\alpha\}$$

yazılabilir.

BÖLÜM 2

SONLU CİSİMLER ÜZERİNDE POLİNOMLAR

2.1. Polinomların Mertebesi ve Primitif Polinomlar

Yardımcı Teorem 2.1.1. $f \in F_q[x]$, $f(0) \neq 0$ olacak şekilde derecesi $m \geq 1$ olan bir polinom olsun. Bu durumda pozitif bir $e \leq q^m - 1$ tam sayısı vardır öyle ki $f(x)$, $x^e - 1$ i böler.

Bu teoremden yola çıkılarak aşağıdaki tanım verilir:

Tanım 2.1.1. $f \in F_q[x]$, sıfırdan farklı bir polinom olsun. $f(0) \neq 0$ ise bu durumda; $f(x)$ in böldüğü $x^e - 1$ için en küçük pozitif e tam sayısı, f nin mertebesi olarak adlandırılır ve

$$\text{ord}(f) = \text{ord}(f(x))$$

ile gösterilir.

$f(0) = 0$ ise bu durumda $f(x)$,

$$f(x) = x^h g(x) \quad (h \in \mathrm{N} \text{ ve } g \in F_q[x],\ g(0) \neq 0)$$

gösterimi ile bir tek şekilde ifade edilir. Böylece $\text{ord}(f)$, $\text{ord}(g)$ olarak tanımlanır.

f polinomunun mertebesi bazen f nin periyodu veya f nin kuvveti (exponenti) olarak da adlandırılır.

Not. n, pozitif bir tam sayı ve b tam sayısı n ile aralarında asal ise $b^k \equiv 1 \pmod{n}$ olduğunda, en küçük pozitif k tam sayısı, b nin (modül n) e göre çarpımsal mertebesi adını alır.

Teorem 2.1.1. $f \in F_q[x]$, $f(0) \neq 0$ olacak şekilde F_q üzerinde m dereceli indirgenemez bir polinom olsun. Bu durumda ord(f), $F_{q^m}^*$ çarpımsal grubundaki f nin herhangi bir kökünün mertebesine eşittir.

İspat. Sonuç 1.2.1 e göre F_{q^m}, F_q üzerinde f nin parçalanış cismidir. f nin kökleri teorem 1.2.8. gereğince, $F_{q^m}^*$ grubunda aynı mertebeye sahiptir. $\alpha \in F_{q^m}^*$, f nin herhangi bir kökü olsun. Bu durumda $\alpha^e = 1$ olması için gerek ve yeter koşul, $f(x)$ in $x^e - 1$ i bölmesidir.

Sonuç 2.1.1. $f \in F_q[x]$, F_q üzerinde m dereceli indirgenemez bir polinom ise bu durumda ord(f), $q^m - 1$ i böler.

İspat. $f(x) = cx$, $c \in F_q^*$ ise ord(f)=1 dir ve sonuç, aşikardır. Başka bir ifadeyle; teorem 2.1.1. gereğince $F_{q^m}^*$, $q^m - 1$ mertebeli bir gruptur.

Teorem 2.1.2. $F_q[x]$ de derecesi m ve mertebesi e olan, indirgenemez monik polinomların sayısı, $\phi(e)/m$ dir.
(Burada $e \geq 2$ ve q nun (modül e) ye göre çarpımsal mertebesi m dir.)

Yukarıda sözü edilen indirgenemez monik polinomların sayısı, eğer $m = e = 1$ ise ve diğer bütün durumlarda sıfır ise, 2 ye eşittir. $F_q[x]$ de mertebesi e olan indirgenemez bir polinomun derecesi; (modül e) ye göre, q nun çarpımsal mertebesine eşit olmalıdır.

İspat. f, $f(0) \neq 0$ olacak şekilde $F_q[x]$ de, indirgenemez bir polinom olsun. Teorem 2.1.1. e göre; $ord(f) = e$ olması için gerek ve yeter koşul, f nin tüm köklerinin, F_q üzerinde birimin $e.$ primitif kökü olmasıdır.

Başka bir ifadeyle; $ord(f) = e$ olması için gerek ve yeter koşul, f nin Q_e cyclotomic polinomunu bölmesidir. Teorem 1.3.3. (ii) gereğince, Q_e nin herhangi bir indirgenemez monik çarpanının derecesi, aynı m sayısıdır. m, $q^m \equiv 1 \pmod{e}$ olacak şekilde, en küçük pozitif tam sayıdır. Çarpanların sayısı da $\phi(e)/m$ dir.

$m = e = 1$ için indirgenemez monik polinom,

$$f(x) = x$$

dir.

Yardımcı Teorem 2.1.2. c, pozitif bir tam sayı olsun. Bu durumda; $f(0) \neq 0$ olacak şekilde bir $f \in F_q[x]$ polinomunun $x^c - 1$ i bölmesi için gerek ve yeter koşul, $ord(f)$ nin, c yi bölmesidir.

İspat. $e = ord(f)$, c yi bölerse; $f(x)$, $x^e - 1$ i böler ve $x^e - 1$, $x^c - 1$ i böler. Dolayısıyla $f(x)$, $x^c - 1$ i böler.

Tersine; $f(x)$, $x^c - 1$ i bölerse,

$c = me + r$ ($c \geq e$ idi.), ($m \in \mathrm{N}$ ve $0 \leq r < e$)

yazılabilir.

$$x^c - 1 = (x^{me} - 1)x^r + (x^r - 1)$$

idi.

Sadece $r = 0$ olduğunda $f(x)$, $x^r - 1$ i böler. Buradan; e nin, c yi böldüğü görülür.

Sonuç 2.1.2. e_1 ve e_2 pozitif tam sayılar ise bu durumda $F_q[x]$ de, $x^{e_1} - 1$ ve $x^{e_2} - 1$ in en büyük ortak böleni, $x^d - 1$ dir. Burada d, e_1 ve e_2 nin en büyük ortak bölenidir.

İspat. $f(x),\ x^{e_1}-1$ ve $x^{e_2}-1$ in en büyük ortak böleni olsun. $x^d-1,\ x^{e_i}-1$ in en büyük ortak böleni idi. $(i=1,\ 2,\ \ldots)$ Bu nedenle $x^d-1,\ f(x)$ i böler. Diğer taraftan $f(x),\ x^{e_i}-1$ in ortak bölenidir $(i=1,\ 2,\ \ldots)$ ve yardımcı teorem 2.1.2. ye göre $ord(f),\ e_1$ ve e_2 yi böler.

Sonuç olarak; $ord(f),\ d$ yi böler ve bu nedenle yardımcı teorem 2.1.2. gereğince $f(x),\ x^d-1$ i böler.

Böylece, $f(x)=x^d-1$ eşitliği elde edilir.

Teorem 2.1.3. $g\in F_q[x],\ g(0)\neq 0$ olacak şekilde F_q üzerinde indirgenemez bir polinom ve $f=g^b$ olsun. Burada $ord(g)=e$ ve b, pozitif bir tam sayıdır. t, $p^t\geq b$ olacak şekilde en küçük tam sayı olsun. (p, F_q sonlu cisminin karakteristiğidir.) Bu durumda,

$$ord(f)=ep^t$$

dir.

Teorem 2.1.4. $g_1,...,g_k$ polinomları, F_q üzerinde sıfırdan farklı polinomlar ve bu polinomlar, ikişer ikişer aralarında asal olsunlar. $f=g_1...g_k$ şeklinde bir polinom ise bu durumda $ord(f);\ ord(g_1),...,ord(g_k)$ nın en küçük ortak katına eşittir.

Örnek 2.1.1. $f(x)=x^{10}+x^9+x^3+x^2+1\in F_2[x]$ polinomunun mertebesini hesaplayalım.

F_2 üzerinde $f(x)$ polinomunun kanonik çarpanlarına ayrılışı,

$$f(x)=(x^2+x+1)^3(x^4+x+1)$$

biçimindedir.

Teorem 2.1.3. gereğince;

$$ord(x^2+x+1)=3 \text{ ve } ord((x^2+x+1)^3)=12$$

olarak hesaplanır. Ayrıca,

$$ord(x^4+x+1)=15$$

dir. Teorem 2.1.4. e göre $ord(f)$, 12 ve 15 in en küçük ortak katına eşittir. Dolayısıyla,

$$ord(f)=60$$

tır.

$ord(f)$, sonuç 2.1.1. de gösterildiği gibi, $2^{10}-1$ i bölemez.

Teorem 2.1.5. F_q, karakteristiği p olan sonlu cisim ve $f \in F_q[x]$, $f(0) \neq 0$ olacak şekilde pozitif dereceli bir polinom olsun. $f = af_1^{b_1} ... f_k^{b_k}$ ifadesi, $F_q[x]$ de, f nin kanonik çarpanlarına ayrılışıdır. ($a \in F_q$, $b_1,...,b_k \in N$ ve $f_1,..., f_k$, $F_q[x]$ de birbirinden farklı, indirgenemez monik polinomlardır.) Bu durumda,

$$ord(f)=ep^t$$

dir. (e; $ord(f_1),...,ord(f_k)$ nın en küçük ortak katı ve t, $p^t \geq \max(b_1,...,b_k)$ olacak şekilde, en küçük tam sayıdır.)

Tanım 2.1.2. $f(x)=a_nx^n+a_{n-1}x^{n-1}+...+a_1x+a_0 \in F_q[x]$, $(a_n \neq 0)$ olsun. Bu durumda, f polinomunun tersi olan f^* polinomu;

$$f^*(x)=x^n f(\frac{1}{x})=a_0x^n+a_1x^{n-1}+...+a_{n-1}x+a_n$$

şeklinde tanımlanır.

Teorem 2.1.6. f, $F_q[x]$ de sıfırdan farklı bir polinom ve f^*, f nin ters polinomu olsun.

Bu durumda,

$$ord(f) = ord(f^*)$$

dır.

Not. $f(-x)$ ve $f(x)$ in mertebeleri arasında gizli bir ilişki vardır. Karakteristiği 2 olan bir cisim için, $f(x) = f(-x)$ idi. Bu bilgi, karakteristiği tek sayı olan sonlu cisimlerin mertebelerinin bulunması için yeterlidir.

Tanım 2.1.3. Derecesi $m \geq 1$ olan bir $f \in F_q[x]$ polinomu, F_{q^m} nin bir primitif elemanının F_q üzerinde minimal polinomu ise, F_q üzerinde, primitif polinom adını alır. Bu nedenle, F_q üzerinde derecesi m olan bir primitif polinom, F_q üzerinde indirgenemez monik polinom olarak tanımlanabilir ve F_{q^m} nin çarpımsal grubunu üreten bir $\alpha \in F_{q^m}$ köküne sahiptir.

Teorem 2.1.7. Derecesi m olan bir $f \in F_q[x]$ polinomunun F_q üzerinde bir primitif polinom olması için gerek ve yeter koşul; $f(0) \neq 0$, f monik polinom ve $ord(f) = q^m - 1$ olmasıdır.

İspat. f, F_q üzerinde primitif polinom ise f, monik polinom ve

$$f(0) \neq 0$$

dır. f polinomu, F_q üzerinde indirgenemezdi. Teorem 2.1.1. e göre,

$$ord(f) = q^m - 1$$

dir. Gerçekten, f polinomunun bir kökü, F_{q^m} nin bir primitif elemanıdır.

Diğer taraftan;

$ord(f) = q^m - 1$

olması, $m \geq 1$ olmasını gerektirir.

f polinomunun F_q üzerinde indirgenemez olduğunu iddia ediyoruz. Şimdi, f polinomunun F_q üzerinde indirgenebilir olduğunu kabul edelim. Bu durumda f polinomu, indirgenemez bir polinomun kuvvetidir veya f polinomu, derecesi pozitif olan aralarında asal iki polinomun çarpımı şeklinde yazılabilir.

İlk durumda; F_q üzerinde indirgenemez $g \in F_q[x]$ ($g(0) \neq 0$) polinomu için

$f = g^b$ ve $b \geq 2$

idi. Bu durumda teorem 2.1.3. e göre $ord(f)$, F_q nun karakteristiği ile bölünebilir. Fakat $q^m - 1$ i bölmez. Bu bir çelişkidir. Şu halde birinci durum gerçekleşmez.

İkinci durumda,

$f = g_1 g_2$

idi. g_1, $g_2 \in F_q[x]$ aralarında asal monik polinomlarının dereceleri sırasıyla, pozitif m_1 ve m_2 sayılarıdır.

$e_i = ord(g_i)$, $(i = 1, 2)$ ise $ord(f) \leq e_1 e_2$

dir. (Teorem 2.1.4. e göre)

Ayrıca yardımcı teorem 2.1.1. gereğince,

$e_i \leq q^{m_i} - 1$, $(i = 1, 2)$

dir.

Bu nedenle,

$$ord(f) \le (q^{m_1}-1)(q^{m_2}-1) < q^{m_1+m_2}-1 = q^m - 1$$

dir. Bu ise, bir çelişkidir. f polinomunun F_q üzerinde indirgenebilir olduğunu kabul ederek çelişkiye düştük. Dolayısıyla f polinomu F_q üzerinde indirgenemezdir ve teorem 2.1.1. e göre, f polinomu F_q üzerinde bir primitif polinomdur.

Teorem 2.1.8. Derecesi $m \ge 1$ olan $f \in F_q[x]$ monik polinomunun, F_q üzerinde primitif polinom olması için gerek ve yeter koşul, $(-1)^m f(0)$ ifadesinin, F_q nun bir primitif elemanı olması ve F_q nun bazı elemanlarına $(\text{mod } f(x))$ e göre kongrüent olan, x^r deki en küçük pozitif r tam sayısının,

$$r = (q^m - 1)/(q-1)$$

olmasıdır.

F_q üzerinde f nin primitif olduğu durumda,

$$x^r \equiv (-1)^m f(0) \pmod{f(x)}$$

dir.

Örnek 2.1.2. $f(x) = x^4 + x^3 + x^2 + 2x + 2 \in F_3[x]$ polinomunu inceleyelim.

f, F_3 üzerinde indirgenemezdir. Teorem 2.1.5. e göre, kullanacağımız yöntemin taslağını oluşturabiliriz.

$$ord(f) = 80 = 3^4 - 1$$

dir.

Sonuç olarak, teorem 2.1.7. gereğince f, F_3 üzerinde primitif polinomdur. teorem 2.1.8. e göre ise,

$$x^{40} \equiv 2 \pmod{f(x)}$$

dir.

2.2. İndirgenemez Polinomlar

f, pozitif dereceli bir polinom ve f nin $F_q[x]$ de her çarpanlarına ayrılışı sabit bir polinom içeriyorsa, $f \in F_q[x]$ polinomu, F_q üzerinde indirgenemezdir.

Teorem 2.2.1. Herhangi bir $b \in F$ elemanının, $f \in F[x]$ in çok katlı bir kökü olması için gerek ve yeter koşul b nin, f polinomunun ve f polinomunun türevinin (f') bir kökü olmasıdır.

Teorem 2.2.2. $\forall n \in N$ ve her F_q sonlu cismi için, F_q üzerinde, dereceleri n yi bölen, bütün indirgenemez monik polinomların çarpımı, $x^{q^n} - x$ e eşittir.

İspat. Yardımcı teorem 1.2.4. e göre; $F_q[x]$ de, $g(x) = x^{q^n} - x$ polinomunun kanonik çarpanlarında ortaya çıkan, F_q üzerinde indirgenemez monik polinomlar, $g(x)$ in derecesi olan n yi bölerler.

$$g'(x) = -1$$

dir.

Teorem 2.2.1. e göre g polinomu, F_q üzerinde kendi parçalanış cismi içinde çok katlı köklere sahip değildir. Dolayısıyla, F_q üzerinde, dereceleri n yi bölen her bir indirgenemez monik polinom, $F_q[x]$ de, g nin kanonik çarpanları içinde tam bir kez ortaya çıkar.

Sonuç 2.2.1. $F_q[x]$ de derecesi d olan indirgenemez monik polinomların sayısı $\mathrm{N}_q(d)$ ise bu durumda,

$$q^n = \sum_{d|n} d\mathrm{N}_q(d) \quad (\text{Her } n \in N \text{ için}) \tag{2.2.1.}$$

dır. Burada toplam, n nin bütün pozitif bölenleri üzerinde alınır.

İspat. $g(x)$ polinomunun kanonik çarpanlarının toplam derecesi ile $g(x) = x^{q^n} - x$ polinomunun derecesi karşılaştırıldığında, teorem 2.2.2. den, (2.2.1.) özdeşliği elde edilir.

Tanım 2.2.1. Moebius μ fonksiyonu, N de tanımlı bir fonksiyondur.

$$\mu(n) = \begin{cases} 1, & n = 1 \text{ ise,} \\ (-1)^k, & n,\ k \text{ tane farklı asal sayının çarpımı ise,} \\ 0, & n, \text{ bir asal sayının karesi ile bölünebiliyorsa,} \end{cases}$$

$n \in N$ nin tüm pozitif d bölenleri üzerinde bir toplam belirtmek için, (2.2.1.) ifadesindeki gibi $\sum_{d|n}$ toplam sembolünü kullanırız. Benzer bir yaklaşımla çarpım sembolü olarak, $\prod_{d|n}$ sembolünü kullanırız.

Yardımcı Teorem 2.2.1. $n \in N$ için Moebius μ fonksiyonu,

$$\sum_{d|n} \mu(d) = \begin{cases} 1, n = 1 \\ 0, n > 1 \end{cases} \text{ise}$$

koşullarını sağlar.

İspat. $n > 1$ için, sadece n nin pozitif d bölenlerini hesaplayalım. $d = 1$ veya d, farklı asal sayıların bir çarpımı iken, $\mu(d) \neq 0$ dır. Bu nedenle; n nin farklı asal bölenleri $p_1, p_2, \ldots, p_k$ ise,

$$\sum_{d|n} \mu(d) = \mu(1) + \sum_{i=1}^{k} \mu(p_i) + \sum_{1 \le i_1 \le i_2 \le k} \mu(p_{i_1} p_{i_2}) + \ldots + \mu(p_1 p_2 \ldots p_k)$$

$$= 1 + \binom{k}{1}(-1) + \binom{k}{2}(-1)^2 + \ldots + \binom{k}{k}(-1)^k$$

$$= (1 + (-1))^k = 0$$

dır. Bu ifade, $n = 1$ durumunda apaçık bellidir.

Teorem 2.2.3. $F_q[x]$ de, derecesi n olan, indirgenemez monik polinomların sayısı $\mathrm{N}_q(n)$,

$$\mathrm{N}_q(n) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d}$$

eşitliği ile verilir.

(Burada "μ" ile Moebius Fonksiyonu ifade edilmektedir.)

Bu formül, her F_q sonlu cismi ve $\forall n \in N$ için, $F_q[x]$ de, derecesi n olan indirgenemez bir polinomun varlığını gösterir.

Örnek 2.2.1. $F_q[x]$ de derecesi 20 olan indirgenemez monik polinomların sayısı,

$$\mathrm{N}_q(20) = \frac{1}{20}(\mu(1)q^{20} + \mu(2)q^{10} + \mu(4)q^5 + \mu(5)q^4 + \mu(10)q^2 + \mu(20)q)$$

$$= \frac{1}{20}(q^{20} - q^{10} - q^4 + q^2)$$

dir.

Teorem 2.2.4. α; F_q nun F_{q^m} cisim genişlemesinin bir elemanı olsun. Kabul edelim ki, F_q üzerinde α nın derecesi d ve $g \in F_q[x]$, F_q üzerinde α nın minimal polinomu olsun. Bu durumda:

(i) g polinomu, F_q üzerinde indirgenemezdir ve g nin derecesi d, m yi böler.

(ii) Bir $f \in F_q[x]$ polinomunda $f(\alpha) = 0$ olması için gerek ve yeter koşul; g polinomunun, f polinomunu bölmesidir.

(iii) f, $f(\alpha) = 0$ olacak şekilde $F_q[x]$ de, indirgenemez monik polinom ise bu durumda, $f = g$ dir.

(iv) g, $x^q - x$ ve $x^{q^m} - x$ i böler.

(v) g polinomunun kökleri $\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}$ dir ve g, F_q üzerinde bu elemanların hepsinin minimal polinomudur.

(vi) $\alpha \neq 0$ ise bu durumda $ord(g)$, $F_{q^m}^*$ çarpımsal grubundaki α nın mertebesine eşittir.

(vii) g nin F_q üzerinde primitif polinom olması için gerek ve yeter koşul; α nın, $F_{q^m}^*$ deki mertebesinin $q^d - 1$ olmasıdır.

2.2.1. İndirgenemez Polinomların Kuruluşu

Bu bölümde öncelikle indirgenemez bir polinomun bilinmesiyle, yeni bir indirgenemez polinomun nasıl kurulacağı üzerinde durulacaktır.

Yardımcı Teorem 2.2.1.1. $s \geq 2$ ve $e \geq 2$ aralarında asal tam sayılar ve m, s nin (modül e) ye göre çarpımsal mertebesi olsun. $t \geq 2$, asal çarpanları e yi bölen fakat $(s^m - 1)/e$ sayısını bölmeyen bir tam sayı olsun.

$t \equiv 0 \pmod 4$ iken $s^m \equiv 1$ kabul edelim. Bu durumda; s nin (modül et) ye göre çarpımsal mertebesi, mt dir.

Teorem 2.2.1.1. $f_1(x),\ f_2(x), ...,\ f_N(x)$ polinomları, $F_q[x]$ de m dereceli, e mertebeli farklı indirgenemez monik polinomlar olsun ve $t \geq 2$, asal çarpanları e yi bölen fakat $q^m - 1/e$ yi bölmeyen bir tam sayı olsun. Üstelik, $t \equiv 0 \pmod 4$ iken $q^m \equiv 1 \pmod 4$ olduğunu kabul edelim. Bu durumda; $f_1(x^t),\ f_2(x^t), \ldots,\ f_N(x^t)$ polinomları, $F_q[x]$ de, derecesi mt ve mertebesi et olan, indirgenemez farklı polinomlardır.

Örnek 2.2.1.1. $F_2[x]$ de, derecesi 4 ve mertebesi 15 olan indirgenemez polinomlar,

$(x^4 + x + 1)$ ve $(x^4 + x^3 + 1)$

dir.

Bu durumda; $F_2[x]$ de, derecesi 12 ve mertebesi 45 olan indirgenemez polinomlar,

$(x^{12} + x^3 + 1)$ ve $(x^{12} + x^9 + 1)$

dir.

$F_2[x]$ de, derecesi 60 ve mertebesi 225 olan indirgenemez polinomlar,

$(x^{60} + x^{15} + 1)$ ve $(x^{60} + x^{45} + 1)$

dir.

$F_2[x]$ de, derecesi 100 ve mertebesi 375 olan indirgenemez polinomlar,

$(x^{100} + x^{25} + 1)$ ve $(x^{100} + x^{75} + 1)$

dir.

Teorem 2.2.1.2. $f_1(x),\ f_2(x), ...,\ f_N(x)$ polinomları, $F_q[x]$ de, tek m dereceli ve e mertebeli, farklı monik polinomlar olsun.

$q = 2^a u - 1,\ \ t = 2^b v \quad (a, b \geq 2)$

olsun.

Burada $u,\ v$ tek sayıdır ve t nin tüm asal çarpanları e yi bölsün, fakat $q^m - 1/e$ yi bölmesin.

$k,\ a$ ve b den daha küçük olan bir sayı olsun. Bu durumda; her $f_j(x^t)$ polinomu, $F_q[x]$ de, derecesi $mt2^{1-k}$ olan, $2^k - 1$ tane indirgenemez monik $g_{ij}(x)$ polinomlarının bir çarpımı şeklinde ifade edilir. $2^{k-1}\mathrm{N}$ tane $g_{ij}(x)$ polinomu, $F_q[x]$ de, derecesi $mt2^{1-k}$ ve mertebesi et olan, farklı indirgenemez monik polinomlardır.

Teorem 2.2.1.3. $f,\ F_q[x]$ de, m dereceli, indirgenemez monik bir polinom olsun. $\alpha \in F_{q^m}$, f polinomunun bir kökü ve $\forall t \in N$ için $f_t,\ F_q$ üzerinde $\alpha^t \in F_{q^m}$ nin karakteristik polinomu olsun. Bu durumda;

$$f_t(x^t) = (-1)^{m(t+1)} \prod_{j=1}^{t} f(w_j x)$$

tir.

Burada $w_1,...,w_t$ ler, F_q üzerinde birimin t. köküdür. (Katlılığa göre sayılan)

İspat. f nin tüm kökleri, $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_m$ olsun. Bu durumda; f_t nin, çarpmaya göre hesaplanan kökleri, $\alpha_1^t, \alpha_2^t, \ldots, \alpha_m^t$ olsun.

Bu nedenle;

$$f_t(x^t) = \prod_{i=1}^{m}(x^t - \alpha_i^t)$$

$$= \prod_{i=1}^{m}\prod_{j=1}^{t}(x - \alpha_i w_j)$$

$$= \prod_{i=1}^{m}\prod_{j=1}^{t} w_j(w_j^{-1}x - \alpha_i)$$

yazılır.

Özdeşlikteki katsayıların karşılaştırılması,

$$x^t - 1 = \prod_{j=1}^{t}(x - w_j)$$

olduğunu gösterir ki,

$$\prod_{j=1}^{t} w_j = (-1)^{t+1}$$

dir ve dolayısıyla,

$$f_t(x^t) = (-1)^{m(t+1)} \prod_{j=1}^{t} \prod_{i=1}^{m} (w_j^{-1} x - \alpha_i)$$

$$= (-1)^{m(t+1)} \prod_{j=1}^{t} f(w_j^{-1} x) = (-1)^{m(t+1)} \prod_{j=1}^{t} f(w_j x)$$

elde edilir.

$w_1^{-1},..., w_t^{-1}$ köklerinin hepsi, F_q üzerinde, birimin t. köküdür.

Örnek 2.2.1.2. $F_2[x]$ de, $f(x) = x^4 + x + 1$ indirgenemez polinomu gözönüne alınsın. f_3 karakteristik polinomu hesaplansın.

F_2 üzerinde birimin 3. kökleri 1, w, w^2 dir. Burada w, F_4 te $x^2 + x + 1$ in bir köküdür.

Bu durumda;

$$f_3(x^3) = (-1)^{16} f(x) f(wx) f(w^2 x)$$

$$= (x^4 + x + 1)(wx^4 + wx + 1)(w^2 x^4 + w^2 x + 1)$$

$$= x^{12} + x^9 + x^6 + x^3 + 1$$

dir.

Dolayısıyla,

$$f_3(x) = x^4 + x^3 + x^2 + x + 1$$

polinomu elde edilir. ∎

f_t karakteristik polinomunu hesaplayan bir başka metod, matris teorisi üzerine kurulmuştur.

$$f(x) = x^m - a_{m-1}x^{m-1} - \ldots - a_1 x - a_0$$

şeklinde bir polinom ve A, f polinomunun eşlik matrisi olsun. A, $m \times m$ tipinde bir matristir.

$$A = \begin{bmatrix} 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & \cdots & 0 & a_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & a_{m-1} \end{bmatrix}$$

Bu durumda f polinomu, lineer cebir anlamında, A nın karakteristik polinomudur. F_q üzerinde $m \times m$ tipindeki I birim matrisi ile

$$f(x) = \det(xI - A)$$

dır.

Her bir $t \in N$ için f_t, A^t nin (A nın t. kuvveti) karakteristik polinomudur. Bu nedenle, A nın kuvvetleri hesaplanarak, f_t polinomları bulunmuş olur.

Örnek 2.2.1.3. f_t karakteristik polinomları, $F_q[x]$ de indirgenemezdir.

Teorem 2.2.1.3. e göre; f_t nin $F_q[x]$ de indirgenemez olması için gerek ve yeter koşul, $k = m$ olmasıdır. $k = m$ olması için gerek ve yeter koşul; m nin, q nun (modül $d = e/(t,e)$) ye göre çarpımsal mertebesi olmasıdır.

Örneğin; $q = 2$, $m = 6$, $e = 63$ durumu incelensin.

q nun çarpımsal mertebesi; e nin bir böleninin modülüne göre, m nin bir böleni olmalıdır. m nin bölenleri, $k = 1,\ 2,\ 3$ tür.

O halde;

$q^k - 1 = 1, 3, 7$ ve $q^k \equiv 1 \pmod{d}$

dir. Bu durum, sadece $d = 1,\ 3,\ 7$ olduğunda gerçekleşir. Bu nedenle f_t,

$(t, 63)$=9, 21, 63

ise kesinlikle $F_2[x]$ de indirgenebilir.

$1 \le t \le 63$ koşulu ile t nin değerlerini hesaplamak yeterlidir.
$t = 9, 18, 21, 27, 36, 42, 45, 54, 63$ olduğunda f_t, $F_2[x]$ de indirgenemezdir. ∎

Pratikte; indirgenemez polinomlar, sık sık bir cisim genişlemesindeki elemanların minimal polinomları olarak karşımıza çıkarlar.

Yukarıda sözü edilen f polinomu, F_q üzerinde primitif polinom ise,

$e = q^m - 1$

dir. Bu durumda α nın kuvvetleri; F_{q^m} nin, sıfırdan farklı tüm elemanları arasında yer alır. Bu nedenle yukarıda sözü edilen metodlar; $F_{q^m}^*$ nin her bir elemanının, F_q üzerindeki minimal polinomunu hesaplamak için kullanılabilir.

Aşağıdaki metod ile minimal polinomlar ifade edilebilir:

θ, F_q üzerinde, F_{q^m} nin tanımlayıcı bir elemanı olsun. Dolayısıyla;
$\{1,\ \theta, \ldots, \theta^{m-1}\}$ kümesi, F_q üzerinde, F_{q^m} nin bir tabanıdır. F_q üzerinde $\beta \in F_{q^m}^*$ nın g minimal polinomunu bulmak için, tabanı oluşturan elemanlar cinsinden $\beta^0, \beta^1, \ldots, \beta^m$ kuvvetlerini yazalım.

$$\beta^{i-1} = \sum_{j=1}^{m} b_{ij}\theta^{j-1} \qquad (1 \le i \le m+1)$$

dir.

g polinomunu,

$$g(x) = c_m x^m + ... + c_1 x + c_0$$

şeklinde yazarız. g nin, $g(\beta) = 0$ olacak şekilde, en küçük pozitif dereceli, monik polinom olmasını istiyoruz.

$$g(\beta) = c_m \beta^m + ... + c_1 \beta + c_0 = 0$$

koşulu,

$$\sum_{i=1}^{m+1} c_{i-1} b_{ij} = 0 \qquad (1 \le j \le m) \qquad (2.2.1.1.)$$

lineer homojen denklemler sistemine götürür.

Burada $c_0, c_1, \ldots, c_m$ ler, bilinmeyenlerdir. B, sistemin katsayılar matrisi olsun. B; (i, j) elemanları b_{ij} olan, $(m+1)\,\mathrm{x}\,m$ tipinde bir matristir. r, B nin rankı olsun. Bu durumda; sistemin çözüm uzayının boyutu, $s = m+1-r$ dir. ($1 \le r \le m$ ve $1 \le s \le m$ idi.)

Eğer

$s = 1$ ise $c_m = 1$

ve eğer

$s > 1$ ise $c_m = c_{m-1} = ... = c_{m-s+2} = 0$ ve $c_{m-s+1} = 1$

dir.

Örnek 2.2.1.4. $F_2[x]$ de, $\theta \in F_{64}$ elemanı, $x^6 + x + 1$ indirgenemez polinomunun bir kökü olsun. $\beta = \theta^3 + \theta^4$ için,

$$\beta^0 = 1$$

$$\beta^1 = \theta^3 + \theta^4$$

$$\beta^2 = 1 + \theta + \theta^2 + \theta^3$$

$$\beta^3 = \theta + \theta^2 + \theta^3$$

$$\beta^4 = \theta + \theta^2 + \theta^4$$

$$\beta^5 = 1 + \theta^3 + \theta^4$$

$$\beta^6 = 1 + \theta + \theta^2 + \theta^4$$

olur. Bu durumda B matrisi,

$$B = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}$$

şeklinde oluşturulur. B matrisinin rankı, 3 tür.

Böylece,

$$s = m + 1 - r = 4$$

tür. Dolayısıyla,

$$c_6 = c_5 = c_4 = 0, \; c_3 = 1$$

olur.

Diğer katsayılar,

$$q^n = \sum_{d|n} d\mathrm{N}_q(d)$$

ifadesinden bulunur.

Buradan;

$$c_2 = 1,\ c_1 = 0,\ c_0 = 1$$

değerleri elde edilir.

Sonuç olarak; F_2 üzerinde β nın minimal polinomu,

$$g(x) = x^3 + x^2 + 1$$

dir. ■

Minimal polinomları bir başka şekilde tarif etmek için, teorem 2.2.4. (v) kullanılır.

F_q üzerinde, $\beta \in F_{q^m}$ elemanının g minimal polinomu bulunmak istenirse;

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

olacak şekilde en küçük d tam sayısı bulunana kadar $\beta, \beta^q, \beta^{q^2}, \ldots$ kuvvetleri hesaplanır. Bulunan d tam sayısı, g nin derecesidir. g polinomu,

$$g(x) = (x-\beta)(x-\beta^q)\ldots(x-\beta^{q^{d-1}})$$

biçiminde ifade edilir. $\beta, \beta^q, \ldots, \beta^{q^{d-1}}$ elemanları; F_q ya göre, β nın farklı eşlenikleridir. g ise, bu elemanların hepsinin F_q üzerinde minimal polinomudur.

Örnek 2.2.1.5. F_2 üzerinde, F_{16} nın tüm elemanlarının, minimal polinomlarını bulalım.

$\theta \in F_{16}$ elemanı, F_2 üzerinde $x^4 + x + 1$ primitif polinomunun bir kökü olsun. F_{16} nın sıfırdan farklı her elemanı, θ nın bir kuvveti şeklinde yazılabilir.

F_{16} için, indisler tablosu:

Tablo 2.2.1.1.

i	θ^i
0	1
1	θ
2	θ^2
3	θ^3
4	$1+\theta$
5	$\theta+\theta^2$
6	$\theta^2+\theta^3$
7	$1+\theta+\theta^3$
8	$1+\theta^2$
9	$\theta+\theta^3$
10	$1+\theta+\theta^2$
11	$\theta+\theta^2+\theta^3$
12	$1+\theta+\theta^2+\theta^3$
13	$1+\theta^2+\theta^3$
14	$1+\theta^3$

şeklindedir.

F_{16} üzerinde β elemanlarının minimal polinomları:

$\beta = 0$: $g_1(x) = x$

$\beta = 1$: $g_2(x) = x + 1$

$\beta = \theta$: F_2 ye göre, θ nın farklı eşlenikleri, θ, θ^2, θ^4, θ^8 dir ve minimal polinom,

$$g_3(x) = (x-\theta)(x-\theta^2)(x-\theta^4)(x-\theta^8)$$
$$= x^4 + x + 1$$

dir.

$\beta = \theta^3$: F_2 ye göre, θ nın farklı eşlenikleri, θ^3, θ^6, θ^{12}, $\theta^{24} = \theta^9$ dır ve minimal polinom,

$$g_4(x) = (x-\theta^3)(x-\theta^6)(x-\theta^9)(x-\theta^{12})$$
$$= x^4 + x^3 + x^2 + x + 1$$

dir.

$\beta = \theta^5$: $\beta^4 = \beta$ idi. F_2 ye göre, bu elemanın farklı eşlenikleri, θ^5, θ^{10} dur ve minimal polinom,

$$g_5(x) = (x-\theta^5)(x-\theta^{10})$$
$$= x^2 + x + 1$$

dir.

$\beta = \theta^7$: F_2 ye göre, θ^7 nin farklı eşlenikleri, θ^7, θ^{14}, $\theta^{28} = \theta^{13}$, $\theta^{56} = \theta^{11}$ dir ve minimal polinom,

$$g_6(x) = (x-\theta^7)(x-\theta^{11})(x-\theta^{13})(x-\theta^{14})$$
$$= x^4 + x^3 + 1$$

dir. ∎

Diğer önemli bir konu, primitif polinomların belirlenmesidir.

F_q üzerinde, m dereceli tüm primitif polinomların çarpımı, $e = q^m - 1$ olacak şekilde, Q_e cyclotomic polinomuna eşittir. Buradan, F_q üzerinde derecesi m olan tüm primitif polinomlar; Q_e cyclotomic polinomuna uygulanan, çarpanlara ayırma algoritmaları yardımıyla bulunabilir.

Bir başka yöntem, F_{q^m} nin bir primitif elemanının kurulmasına ve bunun F_q üzerinde minimal polinomunun yukarıda anlatılan yolla belirtilmesine dayanmaktadır.

F_{q^m} nin bir primitif elemanını bulmak için; $F_{q^m}^*$ grubundaki, mertebesi $q^m - 1$ olan bir elemandan başlanır ve çarpanlar, $q^m - 1 = h_1 ... h_k$ şeklindedir. Buradaki h_1 ,…, h_k pozitif tam sayıları, aralarında asaldır.

Her bir i $(1 \le i \le k)$ için, mertebesi h_i olan bir $\alpha_i \in F_{q^m}^*$ elemanı bulunabiliyorsa, bu durumda $\alpha_1 ... \alpha_k$ çarpımının mertebesi, $q^m - 1$ dir. Bu nedenle $\alpha_1 ... \alpha_k$ çarpımı, F_{q^m} nin bir primitif elemanıdır.

Örnek 2.2.1.6. F_3 üzerinde, derecesi 4 olan bir primitif polinom bulalım.

$3^4 - 1 = 16.5$

idi. İlk olarak; F_{81}^* grubunun, sırasıyla mertebesi 16 ve 5 olan iki tane elemanını yazalım.

Mertebesi 16 olan elemanlar,

$$Q_{16}(x) = x^8 + 1 \in F_3[x]$$

cyclotomic polinomunun kökleridir. 3 ün (modül 16) ya göre çarpımsal mertebesi, 4 tür.

($3^4 \equiv 1 \pmod{16}$)

Q_{16} polinomunun çarpanları; $F_3[x]$ de derecesi 4 olan, indirgenemez monik polinomlardır.

$$x^8 + 1 = (x^4 - 1)^2 - x^4$$

$$= (x^4 - 1 + x^2)(x^4 - 1 - x^2)$$

dir.

Dolayısıyla, $f(x) = x^4 - x^2 - 1$ polinomu, F_3 üzerinde indirgenemezdir. f nin bir kökü θ olmak üzere,

$$F_{81} = F(\theta)$$

dır.

Ayrıca θ; F_{81}^* grubunun, mertebesi 16 olan bir elemanıdır. Mertebesi 5 olan bir α elemanını bulmak için,

$$\alpha = a + b\theta + c\theta^2 + d\theta^3 \quad (a, b, c, d \in F_3)$$

yazarız ve

$$\alpha^{10} = 1$$

elde etmemiz gerektiğinden,

$$1 = \alpha^9\alpha = (a + b\theta^9 + c\theta^{18} + d\theta^{27})(a + b\theta + c\theta^2 + d\theta^3)$$

$$= (a - b\theta + c\theta^2 - d\theta^3)(a + b\theta + c\theta^2 + d\theta^3)$$

$$= (a + c\theta^2)^2 - (b\theta + d\theta^3)^2$$

$$= a^2 + (2ac - b^2)\theta^2 + (c^2 - 2bd)\theta^4 - d^2\theta^6$$

$$= a^2 + c^2 - d^2 + bd + (c^2 + d^2 - b^2 - ac + bd)\theta^2$$

yazılır.

Katsayıların karşılaştırılması ile,

$a^2 + c^2 - d^2 + bd = 1$, $\quad c^2 + d^2 - b^2 - ac + bd = 0$

elde edilir.

$a = d = 0$ olursa, $b^2 = c^2 = 1$

elde edilir.

$b = c = 1$ alalım. Bu durumda,

$\alpha = \theta + \theta^2$ nın mertebesinin 5 olduğu kolayca görülür.

Buradan, $\varsigma = \theta\alpha = \theta^2 + \theta^3$ nin mertebesi, 80 dir. Bu nedenle; ς, F_{81} cisminin, bir primitif elemanıdır.

F_3 üzerinde ς nin g minimal polinomu,

$$g(x) = (x - \varsigma)(x - \varsigma^3)(x - \varsigma^9)(x - \varsigma^{27})$$

$$= (x - \theta^2 - \theta^3)(x - 1 + \theta + \theta^2)(x - \theta^2 + \theta^3)(x - 1 - \theta + \theta^2)$$

$$= x^4 + x^3 + x^2 - x - 1$$

dir. Dolayısıyla; F_3 üzerinde, derecesi 4 olan bir primitif polinom bulmuş oluruz.

Not. F_q üzerinde, derecesi m olan, bir g primitif polinomu biliniyorsa; diğer primitif polinomlar, F_{q^m} de, g nin bir θ kökü ile hesaplanarak bulunabilir ve F_q üzerinde, tüm θ^t elemanlarının, minimal polinomu bulunur. Burada t, $\leq q^m - 1$ olan, tüm pozitif tam sayıları alır. t ile $q^m - 1$ aralarında asaldır.

BÖLÜM 3

LİNEER KODLAR

Lineer kodlar incelenirken F_q alfabesi, $GF(q)$ Galois cismi olarak alınır. (Burada q, bir asal sayının kuvveti şeklindedir.) $(F_q)^n$, F_q cismi üzerinde bir vektör uzayıdır.

$GF(q)$ üzerinde bir lineer kod, $(F_q)^n$ vektör uzayının bir alt uzayıdır. Bu durumda, $(F_q)^n$ vektör uzayının bir C alt kümesi ancak ve ancak

(i) $\forall u, v \in C$ için $u + v \in C$,

(ii) $\forall u \in C$, $r \in GF(q)$ için $ru \in C$

koşullarını gerçekliyorsa, lineer bir koddur.

Sonuç olarak; ikili (binary) bir kod, ancak ve ancak herhangi iki kodsözcüğünün toplamı yine bir kodsözcüğü ise lineerdir.

Tanım 3.1. C, $(F_q)^n$ vektör uzayının k-boyutlu bir alt uzayı ise, bu lineer C koduna, bir $[n, k]$-kod denir. Eğer C nin, d minimum uzaklığını da belirtmek gerekirse bu kod, bir $[n, k, d]$-kod olarak adlandırılır.

Tanım 3.2. Satırları, lineer bir $[n, k]$-kodun bir tabanını oluşturan $k \times n$ matrise, kodun bir üreteç matrisi denir.

Örnek 3.1.

$$C = \begin{cases} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{cases}$$

kodunu ele alalım.

C , üreteç matrisi

$$G = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}_{2x3}$$

olan, ikili bir [3, 2, 2]-koddur. ∎

G üreteç matrisi, lineer kodların denkliği kavramından yararlanılarak $G = [I_k \mid A]$ şekline dönüştürülebilir. $G = [I_k \mid A]$ şeklindeki üreteç matrisine, standard formdadır denir.

Örnek 3.2. Örnek 3.1 deki ikili bir [3, 2, 2]-kod olan C kodunun,

$$G = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

üreteç matrisinde satırların yerleri değiştirilerek, C kodu için standart formdaki,

$$[I_2 \mid A] = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

üreteç matrisi elde edilir.

Örnek 3.3. İkili bir [7, 4, 3]-kod olan C kodunun üreteç matrisini, standart forma dönüştürelim.

$$G=\begin{bmatrix}1&1&1&1&1&1&1\\1&0&0&0&1&0&1\\1&1&0&0&0&1&0\\0&1&1&0&0&0&1\end{bmatrix}\xrightarrow{r_2\to r_2-r_1}\begin{bmatrix}1&1&1&1&1&1&1\\0&1&1&1&0&1&0\\1&1&0&0&0&1&0\\0&1&1&0&0&0&1\end{bmatrix}\xrightarrow{r_3\to r_3-r_1}$$

$$\begin{bmatrix}1&1&1&1&1&1&1\\0&1&1&1&0&1&0\\0&0&1&1&1&0&1\\0&1&1&0&0&0&1\end{bmatrix}\xrightarrow{r_1\to r_1-r_2}\begin{bmatrix}1&0&0&0&1&0&1\\0&1&1&1&0&1&0\\0&0&1&1&1&0&1\\0&1&1&0&0&0&1\end{bmatrix}\xrightarrow{r_4\to r_4-r_2}$$

$$\begin{bmatrix}1&0&0&0&1&0&1\\0&1&1&1&0&1&0\\0&0&1&1&1&0&1\\0&0&0&1&0&1&1\end{bmatrix}\xrightarrow{r_2\to r_2-r_3}\begin{bmatrix}1&0&0&0&1&0&1\\0&1&0&0&1&1&1\\0&0&1&1&1&0&1\\0&0&0&1&0&1&1\end{bmatrix}\xrightarrow{r_3\to r_3-r_4}$$

$$\begin{bmatrix}1&0&0&0&1&0&1\\0&1&0&0&1&1&1\\0&0&1&0&1&1&0\\0&0&0&1&0&1&1\end{bmatrix}=[I_4\mid A]$$

3.1. Dual Kod ve Eşlik-Denetim (Parity-Check) Matrisi

$(F_q)^n$ de, $u=(u_1, u_2, \ldots, u_k)$ ve $v=(v_1, v_2, \ldots, v_k)$ vektörlerinin iç çarpımı, $u.v=u_1v_1+u_2v_2+\ldots+u_nv_n$ şeklinde tanımlanan skalerdir. Yani, $GF(q)$ nun bir elemanıdır.

Tanım 3.1.1. $u.v=0$ ise u ve v vektörlerine, ortogonaldir denir.

Tanım 3.1.2. C, lineer bir $[n, k]$-kod olmak üzere, C nin her bir kod sözcüğüne ortogonal olan $(F_q)^n$ in vektörlerinin kümesine, "C nin dual kodu" denir ve "$C^{\perp}$" ile gösterilir.

$$C^{\perp} = \{v \in (F_q)^n \mid v.u = 0, \ \forall u \in C\}$$

Yardımcı Teorem 3.1.1. C, üreteç matrisi G olan bir $[n, k]$-kod olsun. Bu durumda, $(F_q)^n$ in bir v vektörünün $C^{\perp}$ ne ait olması için gerek ve yeter koşul; v nin, G üreteç matrisinin her bir satırına ortogonal olmasıdır. Yani,

$$v \in C^{\perp} \Leftrightarrow v.G^T = 0$$

dır.

(Burada G^T ile G nin transpozesi belirtilmektedir.)

Teorem 3.1.1. C, $GF(q)$ üzerinde lineer bir $[n, k]$-kod olsun. Bu durumda C nin $C^{\perp}$ dual kodu, lineer bir $[n, n-k]$-koddur.

Örnek 3.1.1.

$$C = \begin{cases} 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{cases}$$ ise $C^{\perp}$ ni bulalım.

Bu durumda,

$$G = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

dir.

$$G^T = \begin{bmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{bmatrix}$$

olur.

$$v.G^T = (v_1, v_2, v_3, v_4)\begin{bmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{bmatrix} = 0 \Rightarrow \begin{cases} v_1 + v_2 = 0 \\ v_3 + v_4 = 0 \end{cases}$$

elde edilir. Dolayısıyla,

$$C^{\perp} = \{0000,\ 1100, 0011, 1111\}$$

olur.

Teorem 3.1.2. Herhangi bir $[n, k]$-kod C için,

$$(C^{\perp})^{\perp} = C$$

dir.

İspat. C deki her bir vektör, $C^{\perp}$ deki her vektöre ortogonal olduğundan,

$$C \subseteq (C^{\perp})^{\perp}$$

dir. Fakat,

$$\dim(C^{\perp})^{\perp} = n - (n - k) = k = \dim C$$

dir. Dolayısıyla,

$$(C^{\perp})^{\perp} = C$$

olur.

Tanım 3.1.3. C, bir $[n, k]$-kod olmak üzere, $C^{\perp}$ nin bir H üreteç matrisine, C nin bir eşlik-denetim (parity-check) matrisi denir.Bu durumda H, bir $(n-k)\,\mathrm{x}\,n$ matristir ve $G.H^T = 0$ eşitliğini gerçekler.

H, C nin bir eşlik-denetim matrisi ise,

$$C = \{x \in (F_q)^n \mid x.H^T = 0\}$$

dır.

Bu yolla lineer bir kod, bir eşlik-denetim matrisi ile tamamen belirlenebilir.

Teorem 3.1.3. C, bir $[n, k]$-kod olmak üzere, C nin standart formdaki üreteç matrisi $G = [I_k \mid A]$ ise, C için bir eşlik-denetim matrisi,

$$H = [-A^T \mid I_{n-k}]$$

dır.

İspat.

$$G = \begin{bmatrix} 1 & \cdots & 0 & a_{11} & \cdots & a_{1,n-k} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 1 & a_{k1} & \cdots & a_{k,n-k} \end{bmatrix}$$

olduğunu kabul edelim.

$$H = \begin{bmatrix} -a_{11} & \dots & -a_{k1} & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ -a_{1,n-k} & \cdots & -a_{k,n-k} & 0 & \cdots & 1 \end{bmatrix}$$

olsun.

Bu durumda H, bir eşlik-denetim matrisi için istenen boyuttadır ve H nin satırları lineer bağımsızdır. Böylece H nin her bir satırının, G nin her bir satırına ortogonal olduğunu göstermek yeterlidir.

G nin $i.$ satırı ile H nin $j.$ satırının iç çarpımı,

$$0 + \dots + 0 + (-a_{ij}) + 0 + \dots + 0 + a_{ij} + 0 + \dots + 0 = 0$$

dır.

Dolayısıyla ispat tamamlanmış olur.

Örnek 3.1.2. Örnek 3.3 ün standart formdaki üreteç matrisi,

$$[I_4 \mid A] = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

idi. Bu durumda $GF(2)$ de,

$$-A = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}_{4x3}$$

olur.

O halde,

$$-A^T = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix}_{3x4}$$

şeklinde bir matristir. Bu durumda eşlik-denetim matrisi,

$$H = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}_{3x7}$$

olur.

Tanım 3.1.4. Bir H eşlik-denetim matrisi için,

$$H = [B \mid I_{n-k}]$$

ise H ye, standart formda denir.

Eğer bir kod, standart formdaki bir $H = [B \mid I_{n-k}]$ eşlik-denetim matrisi ile belirlenirse, bu kod için bir üreteç matrisi,

$$G = [I_k \mid -B^T]$$

dir.

BÖLÜM 4

HAMMING KODLARI

Hamming kodları, lineer kodlardır ve herhangi $GF(q)$ sonlu cismi üzerinde tanımlanabilir. Bir Hamming kodu en uygun şekilde, eşlik-denetim (parity-check) matrisi ile belirtilir.

Tanım 4.1. r, pozitif bir tam sayı ve H; sütunları, $(F_q)^n$ in sıfırdan farklı vektörleri olan bir $r \times (2^r - 1)$ matris olsun. Eşlik-denetim matrisi H olan bir koda, "ikili (binary) Hamming kodu" denir ve "Ham$(r, 2)$" ile gösterilir.

Ham$(r, 2)$ için aşağıdaki özelikler hemen görülür:

(i) Ham$(r, 2)$ kodunun uzunluğu $n = 2^r - 1$, boyutu $k = n - r$ dir. Burada $r = n - k$, her bir kodsözcüğündeki kontrol sembollerinin sayısıdır.

(ii) H nin sütunları herhangi bir sırada alınabileceğinden, verilen r tam sayısı için Ham$(r, 2)$ kodu, denk kodlardan biridir.

(iii) İkili Hamming Ham$(r, 2)$ kodu, bir $[2^r - 1, 2^r - 1 - r, 3]$-koddur.

Örnek 4.1. $r = 3$ için Ham(3, 2) yi oluşturalım.

$(GF(2))^3$ nin birbirinden farklı ve sıfır olmayan vektörlerini sütunlara yazarak bir H matrisi oluşturalım.

$$H=\begin{bmatrix}0&0&0&1&1&1&1\\0&1&1&0&0&1&1\\1&0&1&0&1&0&1\end{bmatrix}_{3x7}\xrightarrow{r_1\to r_1+r_2}\begin{bmatrix}0&1&1&1&1&0&0\\0&1&1&0&0&1&1\\1&0&1&0&1&0&1\end{bmatrix}\xrightarrow{r_3\to r_1+r_3}$$

$$\begin{bmatrix}0&1&1&1&1&0&0\\0&1&1&0&0&1&1\\1&1&0&1&0&0&1\end{bmatrix}\xrightarrow{r_2\to r_2+r_3}\begin{bmatrix}0&1&1&1&1&0&0\\1&0&1&1&0&1&0\\1&1&0&1&0&0&1\end{bmatrix}$$

(H nin standart formdaki yazımı)

Buna göre;

$$-A^T=\begin{bmatrix}0&1&1&1\\1&0&1&1\\1&1&0&1\end{bmatrix}_{3x4},\qquad A=\begin{bmatrix}0&1&1\\1&0&1\\1&1&0\\1&1&1\end{bmatrix}_{4x3}$$

olur. Buradan,

$$G=[I_k\mid A]=[I_4\mid A]=\begin{bmatrix}1&0&0&0&0&1&1\\0&1&0&0&1&0&1\\0&0&1&0&1&1&0\\0&0&0&1&1&1&1\end{bmatrix}_{4x7}$$

matrisi elde edilir. Dolayısıyla Ham(3, 2), bir [7, 4, 3]-koda denktir.

Teorem 4.1. İkili Hamming kod Ham$(r, 2)$, $r \geq 2$ için;

(i) Bir $[2^r - 1,\ 2^r - 1 - r]$-koddur.

(ii) Minimum uzaklığı 3 tür. (Bu nedenle, tek hata düzeltir.)

(iii) Bir yetkin koddur.

Teorem 4.2. $GF(q)$ üzerinde eşlik-denetim matrisi H olan lineer bir kod, C olsun. C nin minimum mesafesinin (uzaklığının) d olması için gerek ve yeter koşul; H nin sütunlarından seçilen her $(d-1)$ tane sütununun lineer bağımsız, fakat lineer bağımlı d tane sütunun var olmasıdır.

4.1. Ham(r, q) nun Kuruluşu

Lineer bir $[n,\ n-r,\ 3]$-kod kurmaya çalışalım.

Burada $d = 3$ alınmıştır. Yani C nin, minimum mesafesi 3 olan bir kod olması için, H nin her sütun ikilisi, $(d - 1 = 3 - 1 = 2$ olduğundan) lineer bağımsız olmak zorundadır. O zaman H nin sütunları;

1) Sıfırdan farklı olmalı,

2) Biri, diğerinin skaler katı olmamalıdır.

$(F_q)^r$ nin sıfırdan farklı vektörleri arasından; biri, diğerinin skaler katı olmayanlar seçilmelidir. (Skaler dediğimiz, $GF(q)$ nun elemanlarıdır.)

$(F_q)^r = (GF(q))^r$ nin $q^r - 1$ tane sıfırdan farklı elemanı vardır. Bunlar içinde; biri diğerinin skaler katı olmayanların sayısı ise,

$$\frac{q^r - 1}{q - 1}$$

dir.

$\frac{q^r-1}{q-1}$ tane vektör, sütunlara yazılarak H matrisi oluşturulur.

Örnek 4.1.1. Ham(2,11) için;

$r=2,\ q=11$

dir.

$$\frac{q^r-1}{q-1}=\frac{11^2-1}{11-1}=\frac{120}{12}=12$$

tane, biri diğerinin skaler katı olmayan, sıfırdan farklı vektör vardır. Bunları sütunlara yazarak H matrisini oluşturalım.

$$H=\begin{bmatrix}0&1&1&1&1&1&1&1&1&1&1&1\\1&0&1&2&3&4&5&6&7&8&9&10\end{bmatrix}_{2x12}\xrightarrow{r_1\to r_1+r_2}$$

$$=\begin{bmatrix}1&1&2&3&4&5&6&7&8&9&10&0\\1&0&1&2&3&4&5&6&7&8&9&10\end{bmatrix}\xrightarrow{r_1\to(-1)r_1}$$

$$=\begin{bmatrix}10&10&9&8&7&6&5&4&3&2&1&0\\1&0&1&2&3&4&5&6&7&8&9&10\end{bmatrix}\xrightarrow{r_2\to(-1)r_2}$$

$$=\begin{bmatrix}10&10&9&8&7&6&5&4&3&2&1&0\\10&0&10&9&8&7&6&5&4&3&2&1\end{bmatrix}\xrightarrow{r_2\to r_2-2r_1}$$

$$=\begin{bmatrix}10&10&9&8&7&6&5&4&3&2&1&0\\1&2&3&4&5&6&7&8&9&10&0&1\end{bmatrix}$$

Buradan,

$$-A^T = \begin{bmatrix} 10 & 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{bmatrix},$$

$$-A = \begin{bmatrix} 10 & 1 \\ 10 & 2 \\ 9 & 3 \\ 8 & 4 \\ 7 & 5 \\ 6 & 6 \\ 5 & 7 \\ 4 & 8 \\ 3 & 9 \\ 2 & 10 \end{bmatrix}, \quad A = \begin{bmatrix} 1 & 10 \\ 1 & 9 \\ 2 & 8 \\ 3 & 7 \\ 4 & 6 \\ 5 & 5 \\ 6 & 4 \\ 7 & 3 \\ 8 & 2 \\ 9 & 1 \end{bmatrix}$$

matrisleri elde edilir.

O halde G üreteç matrisi,

$$G = \left[I_8 : \begin{matrix} 1 & 10 \\ 1 & 9 \\ 2 & 8 \\ 3 & 7 \\ 4 & 6 \\ 5 & 5 \\ 6 & 4 \\ 7 & 3 \\ 8 & 2 \\ 9 & 1 \end{matrix} \right]_{8x10}$$

şeklindedir.

BÖLÜM 5

DEVRESEL KODLAR

Devresel kodlar, kodların önemli bir sınıfıdır. Zengin bir cebir yapısı vardır. Ayrıca; ikili Hamming kodları, Golay kodları ve BCH kodları gibi birçok önemli koda denktir.

Tanım 5.1. Lineer bir C kodu,

$\forall(c_0, c_1, \ldots, c_{n-1}) \in C$ iken $(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C$

ise devreseldir.

Teorem 5.1. $(F_q)^n$ de, lineer bir C kodunun devresel olması için gerek ve yeter koşul; C nin, $F_q[x]/(x^n - 1)$ halkasında bir ideal olmasıdır.

İspat.

(i) C, $F_q[x]/(x^n - 1)$ de bir ideal ve $c(x) = c_0 + c_1 x + \ldots + c_{n-1}x^{n-1}$ polinomu, herhangi bir kodsözcüğü ise bu durumda $xc(x)$ polinomu da bir kodsözcüğüdür.

$(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C$

(x ile çarpma, bir devresel kaymaya karşılık gelir.)

(ii) Tersine; C devresel ise bu durumda, her $c(x)$ kodsözcüğü için,

$xc(x) \in C$

dir. Buradan, her i için,

$x^i c(x) \in C$

dir ve C, lineerdir.

Her $a(x)$ polinomu için,

$a(x)c(x) \in C$

dir.

Bu nedenle C, bir idealdir.

Tanım 5.2. Sıfırdan farklı bir C devresel kodunda; en küçük dereceli monik polinom, C nin üreteç polinomu olarak adlandırılır.

Örnek 5.1. F_2 üzerinde, ikili devresel kodların hepsini bulalım.

$x^3 - 1 = (x+1)(x^2 + x + 1)$

dir. ($x+1$ ve $x^2 + x + 1$ polinomları, F_2 üzerinde indirgenemediğinde)

Buna dayanarak, 3 uzunluklu ikili devresel kodların listesinin tamamı, aşağıda verilmiştir.

3 Uzunluklu İkili Devresel Kodlar

Tablo 5.1.

Üreteç Polinom	$F_2[x]/(x^3 - 1)$ deki Kod	$(GF(2))^3$ de Karşılık Gelen Kod
1	$F_2[x]/(x^3 - 1)$ in tamamı	$(GF(2))^3$ nin tamamı
$x+1$	$\{0,\ 1+x,\ x+x^2,\ 1+x^2\}$	{000, 110, 011, 101}
$x^2 + x + 1$	$\{0,\ 1+x+x^2\}$	{000, 111}
$x^3 - 1 = 0$	$\{0\}$	{000}

5.1. Üreteç Matris Ve Denetim Polinomu

$g(x)$, bir C devresel kodunun n uzunluklu üreteç polinomu olsun. $g(x)$ in derecesi $n-k$ ise bu durumda $g(x),\ xg(x), \ldots,\ x^{k-1}g(x)$ kodsözcükleri, C için bir taban oluştururlar. C, bir $[n, k]$-koddur.

Bu nedenle; $g(x) = g_0 + g_1 x + \ldots + g_{n-k} x^{n-k}$ ise bu durumda,

$$G = \begin{bmatrix} g_0 & g_1 & \cdots & g_{n-k} & 0 & 0 & \cdots & 0 \\ 0 & g_0 & \cdots & g_{n-k-1} & g_{n-k} & 0 & \cdots & 0 \\ 0 & 0 & \cdots & & & & \cdots & 0 \\ 0 & 0 & \cdots & & g_0 & g_1 & \cdots & g_{n-k} \end{bmatrix}$$

matrisi, C için bir üreteç matristir.

Bu ifade;

$$aG = (a_0 + a_1 x + \ldots + a_{k-1} x^{k-1}) g(x)$$

şeklinde bir $(a_0, a_1, \ldots, a_{k-1})$ dizisinin kodlanması anlamına gelmektedir.

Üreteç matrisin bir başka ifadesi;

$i \geq n-k$ için, $x^i = g(x) q_i(x) + r_i(x)$

ile bulunur.

Burada $r_i(x)$; derecesi, $(n-k)$ dan küçük olan bir polinomdur. $(x^i - r_i(x))$ polinomları, C nin kodsözcükleridir ve C nin, standart formdaki üreteç matrisini ortaya çıkaran kod için, bir taban oluşturur.

$(a_0, a_1, \ldots, a_{k-1})$ dizisi, aşağıdaki gibi kodlanır:

$(a_0 + a_1 x + ... + a_{k-1} x^{k-1}) x^{n-k}$ polinomu, $g(x)$ ile bölünür ve kalan, $(a_0 + a_1 x + ... + a_{k-1} x^{k-1}) x^{n-k}$ polinomundan çıkarılır. Buradan, bir kodsözcüğü elde edilir.

$g(x)$, $(x^n - 1)$ in bir böleni idi. Bu durumda; öyle bir $h(x) = h_0 + h_1 x + ... + h_k x^k$ polinomu vardır ki,

$$g(x)h(x) = x^n - 1 \in F_q[x]$$

dir.

$F_q[x]/(x^n - 1)$ halkasında $g(x)h(x) = 0$

idi.

Yani,

$$g_0 h_i + g_1 h_{i-1} + ... + g_{n-k} h_{i-n+k} = 0 \qquad (i = 0, 1, \ldots, n-1)$$

dır.

$$H = \begin{bmatrix} 0 & 0 & \cdots & 0 & h_k & \cdots & h_1 & h_0 \\ 0 & 0 & \cdots & h_k & \cdots & h_1 & h_0 & 0 \\ \vdots & & & & & & & \\ h_k & & \cdots & h_1 & h_0 & 0 & \cdots & 0 \end{bmatrix}$$

matrisi, C kodu için, bir eşlik-denetim matrisidir. $h(x)$ polinomu, C nin "denetim polinomu" olarak adlandırılır.

C kodu, $c(x)h(x) = 0$ şeklindeki $c(x)$ lerin tümünü içerir.

G üreteç matrisi ile H eşlik-denetim matrisi karşılaştırılırsa; üreteç matrisi $h(x)$ olan bir kodun, C kodunun dualine denk olduğu görülür. Bu kod, "C nin dual kodu" olarak adlandırılır.

Örnek 5.1.1. 4 uzunluklu üçlü devresel kodların tamamını bulalım ve bu devresel kodların her biri için bir üreteç matris yazalım.

$GF(3)$ üzerinde, $(x^4 - 1)$ in indirgenemez polinomları,

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

dir.

$F_3[x]$ de, $(x^4 - 1)$ in $2^3 = 8$ tane böleni vardır. Bunlar sadece, uzunluğu 4 olan üçlü devresel kodlardır. Bu kodlar, üreteç polinomları ve onlara karşılık gelen üreteç matrisler ile aşağıda belirtilmiştir.

2 boyutlu kodların minimum uzaklığı 3 tür. Bu yüzden, üçlü Hamming [4, 2, 3]-kodu, devresel değildir.

4 Uzunluklu Üçlü Devresel Kodların Üreteç Polinomları ve Üreteç Matrisleri

Tablo 5.1.1.

Üreteç Polinom	Üreteç Matris
1	$[I_4]$
$x-1$	$\begin{bmatrix} -1 & 1 & 0 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & -1 & 1 \end{bmatrix}$
$x+1$	$\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$
x^2+1	$\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$
$(x-1)(x+1)=x^2-1$	$\begin{bmatrix} -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{bmatrix}$
$(x-1)(x^2+1)=x^3-x^2+x-1$	$\begin{bmatrix} -1 & 1 & -1 & 1 \end{bmatrix}$
$(x+1)(x^2+1)=x^3+x^2+x+1$	$\begin{bmatrix} 1 & 1 & 1 & 1 \end{bmatrix}$
$x^4-1=0$	$\begin{bmatrix} 0 & 0 & 0 & 0 \end{bmatrix}$

Teorem 5.1.1. $n = (q^m - 1)/(q-1)$ ve β, F_{q^m} de birimin n. primitif kökü olsun.

Ayrıca,

$(m,\ q-1) = 1$

dir. Bu durumda;

$C = \{c(x) \mid c(\beta) = 0\}$

devresel kodu, F_q üzerinde $[n, n-m]$-Hamming koduna denktir.

İspat.

$n = (q-1)(q^{m-2} + 2q^{m-3} + ... + m - 1) + m$**,** $\qquad (n,\ q-1) = (m,\ q-1)$

dir. Buradan;

$\beta^{i(q-1)} \neq 1 \qquad (i = 1,\ 2,\ldots,\ n-1)$

dir. Dolayısıyla,

$\beta^i \notin F_q \qquad (i = 1,\ 2,\ldots,\ n-1)$

dır.

F_{q^m} de, 1, β, $\beta^2, \ldots, \beta^{n-1}$ vektörleri olarak gösterilen H matrisinin sütunları, F_q üzerinde ikişer ikişer lineer bağımsızdır.

Bu yüzden H matrisi, bir $[n, n-m]$-Hamming kodunun eşlik-denetim matrisidir.

Örnek 5.1.2. Birimin 9. primitif kökünü içeren F_2 cisminin en küçük cisim genişlemesi, F_{2^6} dır. α, bu cismin bir primitif elemanı ise bu durumda,

$\alpha^{63} = 1$ ve $\beta = \alpha^7$,

birimin 9. primitif köküdür.

β minimal polinomunun kökleri;

$$\beta,\ \beta^2,\ \beta^4,\ \beta^8,\ \ \beta^{16} = \beta^7,\ \ \beta^{14} = \beta^5$$

tir. Bu polinom,

$$(x^9 - 1)/(x^3 - 1) = x^6 + x^3 + 1$$

olmalıdır.

Bu nedenle,

$$(x^9 - 1) = (x - 1)(x^2 + x + 1)(x^6 + x^3 + 1) = f_1(x)\, f_2(x)\, f_3(x)$$

dir.

BÖLÜM 6

BCH KODLARI

Bu kısımda, $GF(2^m)$ Galois cisimlerinden faydalanarak, devresel kodların BCH kodları denen, özel bir sınıfı incelenecektir.

Öncelikle, sıkça kullanılacak olan bazı kavramlar açıklanmalıdır.

Tanım 6.1. (Primitif Eleman) $GF(q)$ cisminde, bir $a \neq 0$ elemanının mertebesi $q-1$ ise yani, $a^n = 1$ şeklindeki en küçük pozitif n tam sayısı $q-1$ ise a ya, bir "primitif eleman" denir. Bu tanımın alternatif bir şekli, tanım 1.2.2. de verilmiştir.

O zaman, $GF(q)$ nun sıfırdan farklı elemanları, a nın kuvvetleriyle elde edilir.

Örnek 6.1. $GF(7)$ de,

$$3^1 = 3$$

$$3^2 = 2$$

$$3^3 = 6$$

$$3^4 = 4$$

$$3^5 = 5$$

$$3^6 = 1$$

dir.

Yani,

$$3^{q-1} = 3^{7-1} = 3^6 = 1$$

olup, 3 bir primitif elemandır. ∎

$GF(2)$ üzerinde bir $p(x)$ polinomu ele alınsın. $p(x)$ in derecesi m olsun. Eğer $p(x)$ polinomu; $GF(2)$ üzerinde, derecesi m den küçük, sıfırdan büyük bir polinomla bölünemiyorsa; $p(x)$ e, $GF(2)$ de indirgenemez bir polinom denir.

Tanım 6.2. (Primitif Polinom) İndirgenemez bir $p(x)$ polinomu ele alınsın. $p(x)$ in derecesi m olsun. Eğer $p(x) \mid x^n + 1$ şeklindeki en küçük pozitif n tam sayısı $n = 2^m - 1$ ise $p(x)$ polinomuna, bir "primitif polinom" denir.

Daha genel bir anlatımla; $p(x) \in F_q[x]$, $\deg p(x) \geq 1$ olan bir $p(x)$ polinomu, F_{q^m} nin bir primitif elemanının F_q üzerindeki minimal polinomu ise $p(x)$ polinomuna, F_q üzerinde bir primitif polinomdur denir.

Örnek 6.2. $p(x) = x^4 + x + 1$ olsun.

$$p(x) \mid x^{15} + 1$$

dir.

Fakat $1 \leq n < 15$ için,

$$p(x) \nmid x^n + 1$$

dir.

Şu halde;

$n = 15 = 2^4 - 1$, $m = 4$ olup, $p(x) = x^4 + x + 1$ polinomu, primitiftir.

Örnek 6.3. $x^4 + x^3 + x^2 + x + 1$ polinomu, $GF(2)$ de indirgenemezdir. Fakat primitif değildir. Çünkü;

$m = 4$, $2^4 - 1 = 15$ ve 5<15 için,

$$x^4 + x^3 + x^2 + x + 1 \mid x^5 + 1$$

dir**.**

Örnek 6.4. $x^3 + x + 1$ polinomu, $GF(2)$ üzerinde indirgenemezdir. Bu nedenle $F_2[x]/(x^3 + x + 1)$, 8 mertebeli bir cisimdir. Üstelik x, bu cismin bir primitif elemanıdır.

$$F_2[x]/(x^3 + x + 1) = \{0,\ 1,\ x,\ x^2,\ x^3 = x + 1,\ x^4 = x^2 + x,\ x^5 = x^2 + x + 1,$$

$$x^6 = x^2 + 1\}$$

dir.

Not. Verilen bir m sayısı için, m dereceli primitif polinomların sayısı, birden fazla olabilir.

Tanım 6.3. Derecesi m den daha küçük olan $F[x]$ deki tüm polinomların kümesi, $F^{(m)}[x]$ olarak tanımlanır. F^m deki her bir sözcük, $F^{(m)}[x]$ deki bir polinoma karşılık gelir.

Örnek 6.5 $h(x) = 1 + x + x^4$ polinomu ele alınsın. $GF(2^2)$ de (1101)(0101) çarpımının sonucunu bulalım.

$$(1101)(0101) \leftrightarrow (1 + x + x^3)(x + x^3)$$

$$= x + x^2 + x^3 + x^6$$

$$x \equiv x + x^2 + x^3 + x^6 \quad \text{mod } (1 + x + x^4)$$

ifadesi elde edilir.

Bu nedenle,

$$(1101)(0101)=0100 \leftrightarrow x$$

bulunur.

Örnek 6.6. Çarpmanın tanımı ile $h(x) = 1 + x + x^3$ primitif polinomunu kullanarak, $GF(2^3)$ cismini kuralım.

Sözcük	$\leftrightarrow$	$x^i \bmod h(x)$
100		1
010		x
001		x^2
110		$x^3 \equiv 1 + x$
011		$x^4 \equiv x + x^2$
111		$x^5 \equiv 1 + x + x^2$
101		$x^6 \equiv 1 + x^2$

Tabloya göre;

$$(110)(001) \leftrightarrow (1 + x)x^2$$

$$\equiv x^3 x^2$$

$$\equiv x^5$$

$$\equiv 1 + x + x^2 \qquad (\mathrm{mod}\,(h(x))$$

olarak bulunur. Dolayısıyla;

(110)(001)=111

dir. ∎

Bir primitif polinom kullanarak $GF(2^m)$ cismini kurmak, primitif olmayan, indirgenemeyen bir polinom kullanmaktan daha kolaydır.

m dereceli bir primitif $h(x)$ polinomu verildiğinde; $(\mathrm{mod}\,(h(x))$ e göre x e karşılık gelen sözcük, $\alpha \in F^m$ ile gösterilsin. O zaman,

$$\alpha^i \leftrightarrow x^i \pmod{h(x)}$$

tir.

$$1 + x^n \pmod{h(x)}$$

ifadesi,

$$0 \equiv 1 + x^n \pmod{h(x)}$$

anlamına gelmektedir.

Bu nedenle,

$$h(x) \mid 1 + x^n$$

dir. Bizim bildiğimiz $h(x)$ polinomu,

$$n < 2^m - 1$$

için

$$h(x) \nmid 1 + x^n$$

dir ve $h(x)$ primitiftir.

Bu nedenle,

$$n < 2^m - 1$$

için

$$\alpha^n \neq 1$$

dir.

$$\alpha^j = \alpha^i \ \ (j \neq i) \Leftrightarrow \alpha^i = \alpha^{j-i}\alpha^i$$

dir ve bu ifade,

$$\alpha^{j-i} = 1$$

anlamına gelmektedir.

$$F^m / \{0\} = \{\alpha^i \mid i = 0,\ 1,\ldots,\ 2^n - 2\}$$

dir.

Not. F^m deki sıfırdan farklı her kodsözcüğü, α nın herhangi bir kuvveti ile gösterilebilir. Bu, cisimdeki çarpma işleminin bir özeliğidir.

Örnek 6.7. $p(x) = 1 + x + x^4$ polinomunu kullanarak, $GF(2^4)$ cismini kuralım.

$p(x) = 1 + x + x^4$ polinomunun, $GF(2)$ üzerinde primitif bir polinom olduğu bilinmektedir.

$$p(\alpha) = 1 + \alpha + \alpha^4 = 0$$

dır. Buradan, $\alpha^4 = 1 + \alpha$ eşitliği kullanılarak, $GF(2^4)$ cismi kurulabilir.

Örneğin;

$$\alpha^5 = \alpha\alpha^4 = \alpha(1+\alpha) = \alpha + \alpha^2$$

$$\alpha^6 = \alpha^2\alpha^4 = \alpha^2(1+\alpha) = \alpha^2 + \alpha^3$$

dır. İşlemlere bu şekilde devam edilirse, $p(x) = 1 + x + x^4$ ile üretilen $GF(2^4)$ ün elemanları, aşağıdaki tabloda verildiği gibi bulunur.

$p(x) = 1 + x + x^4$ ile Üretilen $GF(2^4)$ ün Elemanları

Tablo 6.1.

Sıralı 4-lü olarak	Polinom olarak	α nın kuvveti
0000	0	-
1000	1	$\alpha^0 = 1$
0100	α	α
0010	α^2	α^2
0001	α^3	α^3
1100	$1+\alpha$	α^4
0110	$\alpha+\alpha^2$	α^5
0011	$\alpha^2+\alpha^3$	α^6
1101	$1+\alpha+\alpha^3$	α^7
1010	$1+\alpha^2$	α^8
0101	$\alpha+\alpha^3$	α^9
1110	$1+\alpha+\alpha^2$	α^{10}
0111	$\alpha+\alpha^2+\alpha^3$	α^{11}
1111	$1+\alpha+\alpha^2+\alpha^3$	α^{12}
1011	$1+\alpha^2+\alpha^3$	α^{13}
1001	$1+\alpha^3$	α^{14}

BCH kodlarının kurulumunda minimal polinomlar, büyük önem taşımaktadır. Bu nedenle, minimal polinomları ayrıntılı olarak incelemek, yararlı olacaktır.

6.1. Minimal Polinomlar

$GF(2^m)$ nin sıfırdan farklı $2^m - 1$ elemanı, $x^{2^m-1} + 1$ in tüm köklerini oluşturur. $GF(2^m)$ nin 0 elemanı, x polinomunun kökü olduğundan, $GF(2^m)$ nin elemanları, $x^{2^m} + x$ polinomunun tüm köklerini oluşturur. Buna göre $GF(2^m)$ nin herhangi bir β elemanı, $x^{2^m} + x$ polinomunun bir kökü olduğundan; β, $GF(2)$ üzerinde, derecesi 2^m den küçük olan bir polinomun kökü olabilir.

$\phi(x)$, $GF(2)$ üzerinde $\phi(\beta) = 0$ şeklindeki en küçük dereceli polinom olsun. (Bunun, bir tek olduğu bellidir.) Bu $\phi(x)$ polinomuna, β nın "minimal polinomu" denmektedir.

Örneğin; $GF(2^m)$ nin 0 ının minimal polinomu x, 1 inin ise $x+1$ dir.

Minimal polinomun özeliklerine geçmeden önce, eşlenik kavramını inceleyelim.

Eğer β, $p(x)$ in bir kökü ise (β, $GF(2)$ nin genişlemesi), β^{2^l} nin de $p(x)$ in bir kökü olduğu bilinmektedir. Bu β^{2^l} elemanına, β nın bir eşleniği denmektedir. Böylece β nın tüm eşlenikleri, $GF(2^m)$ nin de elemanıdırlar ve aynı zamanda $p(x)$ in kökleridir.

Örnek 6.1.1. $p(x) = 1 + x^3 + x^4 + x^5 + x^6$ polinomunun bir kökü α^4 tür ve α^4, $GF(2^4)$ ün elemanıdır.

Bu, aşağıdaki yolla kolaylıkla gösterilebilir:

$$p(\alpha^4) = 1 + \alpha^{12} + \alpha^{16} + \alpha^{20} + \alpha^{24}$$

$$= 1 + \alpha^{12} + \alpha^{14}\alpha^2 + \alpha^{14}\alpha^6 + \alpha^{14}\alpha^{10}$$

$$= 1 + \alpha^{12} + (1+\alpha^3)\alpha^2 + (1+\alpha^3)\alpha^6 + (1+\alpha^3)\alpha^{10}$$

$$= 1 + \alpha^{12} + \alpha^2 + \alpha^5 + \alpha^6 + \alpha^9 + \alpha^{10} + \alpha^{13}$$

$$= 1 + 1 + \alpha + \alpha^2 + \alpha^3 + \alpha^2 + \alpha + \alpha^2 + \alpha^2 + \alpha^3 + \alpha + \alpha^3 + 1 + \alpha + \alpha^2 + 1 + \alpha^2 + \alpha^3$$

$$= 0$$

olur.

α^4 ün eşlenikleri;

$(\alpha^4)^2 = \alpha^8$,

$(\alpha^4)^{2^2} = \alpha^{16}$,

$(\alpha^4)^{2^3} = \alpha^{32} = \alpha^2$

dir.

$$\alpha^{32} = \alpha^{14}\alpha^{14}\alpha^{4}$$

$$= (1+\alpha^{3})(1+\alpha^{3})\alpha^{4}$$

$$= (1+\alpha^{3}+\alpha^{3}+\alpha^{6})\alpha^{4}$$

$$= (1+\alpha^{6})\alpha^{4}$$

$$= \alpha^{4}+\alpha^{10}$$

$$= 1+\alpha+1+\alpha+\alpha^{2}$$

$$= \alpha^{2}$$

dir.

Örnek 6.1.2. Örnek 6.7 de $p(x) = 1 + x + x^4$ polinomu kullanılarak, $GF(2^4)$ cismini kurmuştuk.

$$p(\alpha) = 1 + \alpha + \alpha^4 = 0$$

olduğundan α, α^3 ve α^5 in minimal polinomları sırasıyla,

$$\phi_1(x) = 1 + x + x^4$$

$$\phi_3(x) = 1 + x + x^2 + x^3 + x^4$$

$$\phi_5(x) = 1 + x + x^2$$

dir. Bunların nasıl elde edildiğini kısaca açıklayalım.

Biliyoruz ki, $GF(2^m)$ de bir β elemanının minimal polinomu $\phi(x)$ olduğunda, $\beta^{2^e} = \beta$ şeklindeki en küçük tam sayı e ise

$$\phi(x) = \prod_{i=0}^{e-1} (x + \beta^{2^i})$$

dir.

$\beta = \alpha^3$ alalım. β nın eşlenikleri,

$$\beta^2 = \alpha^6$$

$$\beta^{2^2} = \alpha^{12}$$

$$\beta^{2^3} = \alpha^{24} = \alpha^9$$

dır. $\beta = \alpha^3$ ün minimal polinomu,

$$\phi(x) = (x + \alpha^3)(x + \alpha^6)(x + \alpha^{12})(x + \alpha^9)$$

olur.

Gerekli çarpımlar yapılınca,

$$\phi(x) = x^4 + x^3 + x^2 + x + 1$$

polinomu elde edilir.

Teorem 6.1.1. $GF(2^m)$ nin bir elemanı, $\alpha \neq 0$ olsun. $\phi_\alpha(x)$, α nın minimal polinomu olsun. Bu durumda,

(i) $\phi_\alpha(x)$, F üzerinde indirgenemezdir.

(ii) $p(x)$, F üzerinde herhangi bir polinom ise $p(\alpha) = 0$ dır. O zaman $\phi_\alpha(x)$, $p(x)$ polinomunun bir çarpanıdır.

(iii) Minimal polinom tektir.

(iv) $\phi_\alpha(x)$ minimal polinomu, $1 + x^{2^m - 1}$ in bir çarpanıdır.

İspat.

(i) $\phi_\alpha(x) = g(x)h(x)$

ise

$$\phi_\alpha(\alpha) = 0$$

dır.

Bu da,

$$g(\alpha)h(\alpha) = 0$$

anlamına gelir.

Bu nedenle, ya

$$g(\alpha) = 0$$

dır ya da

$$h(\alpha) = 0$$

dır. Zira $\phi_\alpha(x),$ en küçük dereceli polinomdur öyle ki

$$\phi_\alpha(x) = 0$$

dır.

O zaman ya

$$g(x) = 1$$

dir ya da

$$h(x) = 1$$

dir.

Dolayısıyla $\phi_\alpha(x)$, F üzerinde indirgenemezdir.

(ii) Bölme algoritması ile;

$$r(x) = 0 \text{ veya } \deg r(x) < \deg \phi_\alpha(x)$$

olduğunda,

$$p(x) = \phi_\alpha(x)g(x) + r(x)$$

tir.

Şimdi $p(\alpha) = 0$ ise,

$$p(\alpha) = \phi_\alpha(\alpha)g(\alpha) + r(\alpha) = 0.g(\alpha) + r(\alpha) = r(\alpha)$$

dır.

$$r(\alpha) = 0$$

olduğunu biliyoruz.

$\phi_\alpha(x)$ in derecesinin minimalliğinden,

$$r(x) = 0$$

bulunur. Buradan,

$$p(x) = \phi_\alpha(x) g(x)$$

elde edilir.

O halde $\phi_\alpha(x)$, $p(x)$ polinomunun bir çarpanıdır.

(iii) Kabul edelim ki, $\phi_\alpha(x)$ ve $\phi'(x)$ gibi iki tane minimal polinom olsun. $\phi'(x)$, derecesi en küçük olan polinom ise,

$$\phi'(\alpha) = 0$$

dır. (ii) gereğince $\phi_\alpha(x)$, $\phi'(x)$ in bir çarpanıdır ve $\phi'(x)$, $\phi_\alpha(x)$ in bir çarpanıdır.

Buradan,

$$\phi_\alpha(x) = \phi'(x)$$

sonucu elde edilir.

Dolayısıyla minimal polinom, tektir.

(iv) β, $GF(2^m)$ nin bir primitif elemanı ve $\alpha = \beta^i$ olsun.

$$\alpha^{2^m-1} = (\beta^i)^{2^m-1} = (\beta^{2^m-1})^i = 1^i = 1$$

dir.

$$p(x) = 1 + x^{2^m-1} \Rightarrow p(\alpha) = 1 + \alpha^{2^m-1} = 1 + 1 = 0$$

dır.

Bu nedenle α , $1+x^{2^m-1}$ polinomunun bir köküdür ve (ii) gereğince $\phi_\alpha(x)$, $1+x^{2^m-1}$ in bir çarpanıdır.

Not. $GF(2)$ üzerinde $l \geq 0$ için

$$[p(x)]^{2^l} = p(x^{2^l})$$

dir.

(Burada $p(x)$ ile $GF(2)$ üzerinde bir polinom gösterilmektedir.)

Bunu görelim:

$$p(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$$

olsun.

$$p^2(x) = (a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n)^2$$

$$= [a_0 + (a_1 x + a_2 x^2 + \ldots + a_n x^n)]^2$$

$$= a_0^2 + \underbrace{2a_0(a_1 x + \ldots + a_n x^n)}_{0} + (a_1 x + a_2 x^2 + \ldots + a_n x^n)^2$$

$$= a_0^2 + (a_1 x + a_2 x^2 + \ldots + a_n x^n)^2$$

$$= a_0 + [a_1 x + (a_2 x^2 + \ldots + a_n x^n)]^2$$

$$= a_0 + (a_1 x)^2 + 2a_1 x(a_2 x^2 + \ldots + a_n x^n) + (a_2 x^2 + \ldots + a_n x^n)^2$$

$$= a_0 + a_1^2 x^2 + (a_2 x^2 + a_3 x^3 + \ldots + a_n x^n)^2$$

elde edilir. İşleme devam edilirse,

$$p^2(x) = a_0 + a_1 x^2 + a_2 (x^2)^2 + a_3 (x^2)^3 + ... + a_n (x^2)^n$$

bulunur. Tekrar tekrar kare alınarak,

$$[p(x)]^{2^l} = p(x^2)^l$$

olduğu görülür. $(GF(2)$ de$)$

$GF(2^m)$ deki tüm elemanlar için minimal polinomlar aranıyorsa, aşağıdaki yöntem kullanılabilir:

$$p(x)^2 = p(x^2)$$

olduğu göz önüne alınırsa,

$$(\sum_{i=0}^{n} a_i x^i)^2 = \sum_{i=0}^{n} a_i^2 (x^i)^2 = \sum_{i=0}^{n} a_i (x^2)^i$$

bulunur.

$((a+b)^2 = a^2 + b^2$ ve $a_i^2 = a_i$, $a_i \in [0, 1])$

Bu nedenle,

$$p(\alpha) = 0$$

ise

$$p(\alpha^2) = (p(\alpha))^2 = 0$$

dır ve α^2, $p(x)$ polinomunun bir köküdür.

Benzer olarak,

$$p(\alpha^4) = (p(\alpha^2))^2 = 0$$

ve $p(x)$ polinomunun bir kökü α ise α, α^2, α^4,..., α^{2^i},...de $p(x)$ polinomunun bir köküdür.

Teorem 6.1.2. $\phi_\alpha(x)$ minimal polinomu ile $GF(2^m)$ de bir eleman α olsun. Bu durumda $\{\alpha, \alpha^2, \alpha^4,..., \alpha^{2^{m-1}}\}$ kümesi, $\phi_\alpha(x)$ polinomunun tüm köklerinin kümesidir.

$\phi_\alpha(x)$ polinomunun derecesi,

$$|\{\alpha, \alpha^2,..., \alpha^{2^{m-1}}\}|$$

dir.

Örnek 6.1.3. $p(x) = 1 + x + x^4$ polinomu ile üretilen $GF(2^4)$ cismindeki tüm elemanların minimal polinomları aşağıdaki tabloda verilmiştir.

$p(x) = 1 + x + x^4$ Polinomu ile Üretilen $GF(2^4)$ Cismindeki Tüm Elemanların Minimal Polinomları

Tablo 6.1.1.

Eşlenik Kökler	Minimal Polinomlar
0	x
1	$1+x$
α, α^2, α^4, α^8	$1+x+x^4$
α^3, α^6, α^9, α^{12}	$1+x+x^2+x^3+x^4$
α^5, α^{10}	$1+x+x^2$
α^7, α^{11}, α^{13}, α^{14}	$1+x^3+x^4$

Örnek 6.1.4. $\alpha = \beta^5$, $\beta^5 \in GF(2^4)$ in minimal polinomu, $\phi_5(x)$ olsun. Zira,

$$\{\alpha, \alpha^2, \alpha^4, \alpha^8\} = \{\beta^5, \beta^{10}\}$$

dır.

$\phi_5(x)$ polinomunun kökleri β^5 ve β^{10} elemanlarıdır.

Dolayısıyla,

$$\deg(\phi_5(x)) = 2$$

dir.

Bu nedenle,

$$\phi_5(x) = a_0 + a_1 x + a_2 x^2$$

$$0 = a_0 1 + a_1 \beta^5 + a_2 \beta^{10}$$

$$= a_0(1000) + a_1(0110) + a_2(1110)$$

dır.

$$a_0 = a_1 = a_2 = 1$$

ve

$$\phi_5(x) = 1 + x + x^2$$

dir.

6.2. BCH Kodları

1960 yılında R. C. Bose ve D. K. Ray-Chaudri ile bunlardan bağımsız olarak 1959 yılında A. Hocquenghem tarafından bulunmuştur. Bu nedenle, Bose-Chaudri-Hocquenghem'in isimlerinin baş harfleriyle, yani BCH ile isimlendirilmiştir.

BCH kodları, devresel kodların önemli bir sınıfını oluşturmaktadır. Uygulama alanı oldukça geniştir.

Öncelikle, anlaşılması güçlük gösteren ve BCH kodlarının minimum mesafesi için oldukça önemli olan, "tasarlanmış mesafe" kavramı açıklanacaktır.

6.2.1. Tasarlanmış Mesafe

BCH kodlarının kuruluşunda önemli bir problem, kodun boyutu k ve minimum d mesafesinin belirtilmesindeki güçlüktür.

Tasarlanmış mesafe, gerçek d mesafesi hakkında verilen bir alt sınırdır. Bu alt sınırın, yani "tasarlanmış mesafenin" bilinmesi, oldukça yararlı olmaktadır. Örneğin, bir devresel kod verilmişse ve onun üreteç polinomunun $d-1$ elemanlı bir kök dizisine sahip olduğunu (ki bunlar, verilen bir kökün ardışık kuvvetlerinden oluşmuştur.) gösterebilirsek, o zaman kodun minimum mesafesi, en azından d dir. Bu sınır, sözkonusu kodun tipi göz önüne alınmaksızın, BCH sınırı olarak düşünülür.

Daha açık bir anlatımla; $t-$hata düzelten BCH kodunun minimum mesafesi, en az $2t+1$ dir. Bu, daha sonra bir teorem olarak ispatlanacaktır.

Buradaki $2t+1$ mesafesi, çoğunlukla $t-$hata düzelten BCH kodunun tasarlanmış mesafesi olarak adlandırılır. Bir BCH kodunun gerçek minimum mesafesi, tasarlanmış mesafeye eşit olur veya olmayabilir. Gerçek minimum mesafenin, tasarlanmış mesafeye eşit olduğu birçok durum var olmasına karşın;

gerçek minimum mesafenin, tasarlanmış mesafeden büyük olduğu durumlar da vardır.

Tanım 6.2.1.1. b, negatif olmayan bir tam sayı ve $\alpha \in F_{q^m}$, birimin n. primitif kökü olsun. Burada m, q nun (modül n) e göre çarpımsal mertebesidir. F_q üzerinde n uzunluklu ve d tasarlanmış mesafeli $(2 \le d \le n)$ olan bir BCH kodu, üreteç polinomun α^b, $\alpha^{b+1}, \ldots, \alpha^{b+d-2}$ kökleriyle tanımlı bir devresel koddur.

$b = 1$ ise BCH kodları, "Dar anlamda BCH kodları" olarak adlandırılan kodlara karşılık gelir.

$n = q^m - 1$ ise BCH kodları, "primitif" olarak adlandırılır.

$n = q - 1$ ise F_q üzerinde n uzunluklu bir BCH kodu, "Reed-Solomon Kodu" olarak bilinir.

Teorem 6.2.1.1. Tasarlanmış mesafesi d olan bir BCH kodunun minimum uzaklığı en az d dir.

İspat. BCH kodu,

$$H = \begin{bmatrix} 1 & \alpha^{b} & \alpha^{2b} & \cdots & \alpha^{(n-1)b} \\ 1 & \alpha^{b+1} & \alpha^{2(b+1)} & \cdots & \alpha^{(n-1)(b+1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{b+d-2} & \alpha^{2(b+d-2)} & \cdots & \alpha^{(n-1)(b+d-2)} \end{bmatrix}$$

matrisinin null (sıfır) uzayıdır.

Bu matrisin en az $(d-1)$ tane sütununun lineer bağımsız olduğu gösterilmelidir. H nin her $(d-1)$ tane farklı sütununun determinantı alınırsa bu durumda,

$$\begin{vmatrix} \alpha^{bi_1} & \alpha^{bi_2} & \cdots & \alpha^{bi_{d-1}} \\ \alpha^{(b+1)i_1} & \alpha^{(b+1)i_2} & \cdots & \alpha^{(b+1)i_{d-1}} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha^{(b+d-2)i_1} & \alpha^{(b+d-2)i_2} & \cdots & \alpha^{(b+d-2)i_{d-1}} \end{vmatrix} =$$

$$\alpha^{b(i_1+i_2+\ldots+i_{d-1})} \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \alpha^{i_1} & \alpha^{i_2} & \cdots & \alpha^{i_{d-1}} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha^{i_1(d-2)} & \alpha^{i_2(d-2)} & \cdots & \alpha^{i_{d-1}(d-2)} \end{vmatrix} =$$

$$\alpha^{b(i_1+i_2+\ldots+i_{d-1})} \prod_{1\le k<j\le d-1} (\alpha^{i_j} - \alpha^{i_k}) \neq 0$$

bulunur.

Buradan, kodun minimum uzaklığının an az d olduğu görülür.

6.2.2. BCH Kodunun Kuruluşu

Herhangi $m \geq 3$ ve $t < 2^{m-1}$ pozitif tam sayıları ele alınsın. Bu durumda,

Sözcük Uzunluğu : $n = 2^m - 1$

Eşlik-Denetim Sembolleri Sayısı : $n - k \leq mt$

Minimum Mesafe : $d_{\min} \geq 2t + 1$

parametrelerine sahip ikili (binary) BCH kodu mevcuttur. Bu kod, t veya daha az hatayı düzeltebilir. Bu nedenle, $t-$hata düzelten BCH kodu adını alır. Bu kodun üreteç polinomu, $GF(2^m)$ Galois cismindeki kökleri cinsinden belirlenir.

$GF(2^m)$ deki bir primitif eleman α olsun. $2^m - 1$ uzunluklu, t – hata düzelten BCH kodunun $g(x)$ üreteç polinomu, α, α^2, α^3,..., α^{2t} leri kök kabul eden, $GF(2)$ üzerindeki en küçük dereceli polinomdur. (yani $g(\alpha^i) = 0$, $1 \le i \le 2t$)

Katsayıları $GF(2)$ de bulunan bir $p(x)$ polinomu ele alınsa; α, $GF(2)$ nin bir cisim genişlemesinde bulunsa, herhangi $l \ge 0$ için α^{2^l} nin, $p(x)$ polinomunun bir kökü olduğu bilinmektedir.

Bu nedenle, $g(x)$ polinomunun köklerinin hepsi α, α^2,..., α^{2t} ve bunların eşlenikleridir. α^i nin minimal polinomu $\phi_i(x)$ olsun. O zaman $g(x)$ polinomu; $\phi_1(x)$, $\phi_2(x)$,..., $\phi_{2t}(x)$ polinomlarının en küçük ortak katı olur.

Yani,

$$g(x) = \text{ekok } \{\phi_1(x), \phi_2(x), \ldots, \phi_{2t}(x)\} \qquad (6.2.2.1.)$$

dir.

Eğer i bir çift sayı ise,

$$i = i' 2^l \qquad (6.2.2.2.)$$

şeklinde yazılabilir. Burada i' bir tek sayı ve $l \ge 1$ dir.

O zaman,

$$\alpha^i = (\alpha^{i'})^{2^l}$$

ifadesi, $\alpha^{i'}$ nün bir eşleniğidir. Böylece de α^i ve $\alpha^{i'}$ elemanları, aynı minimal polinoma sahiptir. Yani minimal polinomlar,

$$\phi_i(x) = \phi_{i'}(x)$$

tir.

Böylece,

$$\alpha,\ \alpha^2,\ \alpha^3,\ldots,\ \alpha^{2t} \qquad (6.2.2.3)$$

dizisinde α nın her bir çift kuvveti, dizide kendinden önce gelen tek kuvvetli elemanla aynı minimal polinoma sahiptir.

Böyle olunca, (6.2.2.1.) ile verilen 2^m-1 uzunluklu $t-$hata düzelten ikili (binary) BCH kodunun $g(x)$ üreteç polinomu,

$$g(x) = \text{ekok}\ \{\phi_1(x),\ \phi_3(x),\ldots,\ \phi_{2t-1}(x)\} \qquad (6.2.2.4.)$$

ifadesine indirgenir.

Herbir minimal polinomun derecesi m veya daha az olduğuna göre, $g(x)$ polinomunun derecesi en fazla mt ye eşit olabilir. Yani, $n-k$ olan eşlik-denetim sembollerinin sayısı en fazla mt olabilir. $n-k$ yı saymak için basit bir formül yoktur. Fakat, eğer t küçükse, kesinlikle $n-k=mt$ olur.

Yukarıdaki gibi tanımlanan BCH kodlarına, primitif (veya dar-anlamda) BCH kodları denmektedir. (6.2.2.4.) ten dolayı, 2^m-1 uzunluklu tek-hata düzelten BCH kodu,

$$g(x) = \phi_1(x)$$

ile üretilir.

$GF(2^m)$ nin primitif elemanı α olduğundan; $\phi_1(x)$ polinomu, derecesi m olan primitif bir polinomdur. O zaman 2^m-1 uzunluklu, tek-hata düzelten BCH kodu, bir Hamming kod adını alır.

Örnek 6.2.2.1. $q=2,\ n=15$ ve $d=4$ olsun. Bu durumda x^4+x+1 polinomu, $GF(2)$ üzerinde indirgenemezdir ve x^4+x+1 in kökleri, $GF(2^4)$ ün primitif

elemanlarıdır. Köklerden biri α ise bu durumda α^2 de bir köktür ve α^3, $(x^4 + x^3 + x^2 + x + 1)$ polinomunun bir köküdür. Bu nedenle $d = 4$ olacak şekilde dar anlamda bir BCH kodu,

$$g(x) = (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1)$$

ile üretilir. Üstelik $g(x)$ polinomu, $d = 5$ olacak şekilde bir BCH kodu için üreteçtir. α^2, $(x^4 + x + 1)$ in bir köküydü. Bu kodun boyutu,

$$15 - \deg(g(x)) = 7$$

dir.

Örnek 6.2.2.2. $n = 31,\ m = 5,\ q = 2,\ d = 8$ olsun. α, $GF(2^5)$ in bir primitif elemanı olsun. α nın minimal polinomu,

$$(x - \alpha)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8)(x - \alpha^{16})$$

dır.

Aynı yolla $\phi_3(x)$ polinomunu da buluruz. Fakat,

$$\phi_5(x) = (x - \alpha^5)(x - \alpha^{10})(x - \alpha^{20})(x - \alpha^9)(x - \alpha^{18}) = \phi_9(x)$$

tir.

$g(x);\ \phi_1(x),\ \phi_3(x),\ \phi_5(x),\ \phi_7(x)$ ve $\phi_9(x)$ polinomlarının, en küçük ortak katıdır. Buradan, tasarlanmış mesafesi 8 olan bir primitif BCH kodunun minimum uzaklığının, en az 11 olduğu görülür.

Örnek 6.2.2.3. Örnek 6.7 de $p(x) = 1 + x + x^4$ polinomu kullanılarak, $GF(2^4)$ cismi kurulmuştu. α, bu cismin bir primitif elemanı idi.

Bu polinom için, $n = 2^4 - 1 = 15$ uzunluklu iki-hata düzelten BCH kodu,

$$g(x) = \text{ekok } \{\phi_1(x),\ \phi_3(x)\}$$

polinomu ile üretilir.

Örnek 6.1.2 de α, α^3 ve α^5 elemanlarının minimal polinomları sırasıyla,

$$\phi_1(x) = 1 + x + x^4$$

$$\phi_3(x) = 1 + x + x^2 + x^3 + x^4$$

$$\phi_5(x) = 1 + x + x^2$$

idi. $\phi_1(x)$ ve $\phi_3(x)$, iki farklı indirgenemeyen polinom olduğundan,

$$g(x) = \phi_1(x)\phi_3(x)$$

$$= (1 + x + x^4)(1 + x + x^2 + x^3 + x^4)$$

$$= 1 + x^4 + x^6 + x^7 + x^8$$

olarak bulunur.

Sözkonusu kod, $d_{\min} \geq 5$ olan (15, 7)-parametreli devresel bir koddur. Üreteç polinomu, 5 ağırlıklı bir kod polinomu olduğundan, minimum mesafe kesinlikle 5 tir.

Üç-hata düzelten 15 uzunluklu BCH kodu ise,

$$g(x) = \text{ekok } \{\phi_1(x),\ \phi_3(x),\ \phi_5(x)\}$$
$$= 1 + x + x^2 + x^4 + x^5 + x^8 + x^{10}$$

polinomu ile üretilir.

Bu kod, (15, 5)-parametreli bir devresel koddur.

$d_{\min} \geq 7$

dir. Fakat üreteç polinom 7 ağırlıklı olduğundan, minimum mesafe kesinlikle 7 olarak bulunur.

Yardımcı Teorem 6.2.2.1. Aşağıdaki H matrisi; α, $GF(2^m)$ de bir primitif eleman ve üreteç polinom, $g(x) = \phi_1(x)\phi_3(x)$ olduğunda, $2^m - 1$ uzunluklu iki-hata düzelten BCH kodu için bir eşlik-denetim matrisidir.

$$H = \begin{bmatrix} \alpha^0 & \alpha^0 \\ \alpha^1 & \alpha^3 \\ \alpha^2 & \alpha^6 \\ \vdots & \vdots \\ \alpha^i & \alpha^{3i} \\ \vdots & \vdots \\ \alpha^{2^m-2} & \alpha^{3(2^m-2)} \end{bmatrix}$$

β^i, $GF(2^m)$ nin bir elemanıdır. β^i, m uzunluklu bir sözcüğü temsil eder. Bu yüzden H, bir $(2^m - 1)\,\mathrm{x}\,(2m)$ matristir. Üstelik,

$$\deg(\phi_1(x)) = m = \deg(\phi_3(x))$$

$$\deg(g(x)) = \deg(\phi_1(x)) + \deg(\phi_3(x))$$

$$= m + m$$

$$= 2m$$

dir ve bu nedenle kodun boyutu,

$$k = n - 2m = 2^m - 1 - 2m$$

dir.

Örnek 6.2.2.4. İki-hata düzelten BCH kodu C_{15} i kuralım.

Bunun için, $p(x) = 1 + x + x^4$ polinomu ile kurulan $GF(2^4)$ cismini kullanalım.

$$\begin{bmatrix} 1 & 1 \\ \alpha & \alpha^3 \\ \alpha^2 & \alpha^6 \\ \alpha^3 & \alpha^9 \\ \alpha^4 & \alpha^{12} \\ \alpha^5 & \alpha^1 \\ \alpha^6 & \alpha^3 \\ \alpha^7 & \alpha^6 \\ \alpha^8 & \alpha^9 \\ \alpha^9 & \alpha^{12} \\ \alpha^{10} & \alpha^1 \\ \alpha^{11} & \alpha^3 \\ \alpha^{12} & \alpha^6 \\ \alpha^{13} & \alpha^9 \\ \alpha^{14} & \alpha^{12} \end{bmatrix} \leftrightarrow \begin{bmatrix} 1000 & 1000 \\ 0100 & 0001 \\ 0010 & 0011 \\ 0001 & 0101 \\ 1100 & 1111 \\ 0110 & 1000 \\ 0011 & 0001 \\ 1101 & 0011 \\ 1010 & 0101 \\ 0101 & 1111 \\ 1110 & 1000 \\ 0111 & 0001 \\ 1111 & 0011 \\ 1011 & 0101 \\ 1001 & 1111 \end{bmatrix} = H$$

C_{15} in eşlik-denetim matrisi.

C_{15}, 15x8 eşlik-denetim matrisi H ve $g(x) = \phi_1(x)\phi_3(x)$ üreteç polinomu ile lineer bir kod olarak tanımlanır.

Teorem 6.2.2.1. Herhangi bir $m \geq 4$ tam sayısı için $k = 2^m - 2m - 1$ boyutlu, $n = 2^m - 1$ uzunluklu iki-hata düzelten bir BCH kodu ve $d = 5$ uzaklıklı $g(x) = \phi_1(x)\phi_3(x)$ üreteç polinomu vardır.

İspat. Uzaklığın 5 olduğunu ispat etmek için, iki-hatanın düzeltilebileceği gösterilmelidir. Bu nedenle uzaklık, en az 5 tir. Eşlik-denetim matrisinin tanımından,

$$n = 2^m - 1$$

dir. $\phi_1(x)$ ve $\phi_3(x)$ polinomlarının her birinin derecesinin m olduğu görülmektedir.

Dolayısıyla,

$$\deg(g(x)) = n - k = 2m$$

ve

$$k = 2^m - 2m - 1$$

dir.

Örnek 6.2.2.5. $\phi_1(x) = 1 + x + x^4$ polinomu, $\alpha \in F_{16}$ nın F_2 üzerinde minimal polinomu olsun. α^i $(0 \leq i \leq 14)$ kuvvetleri; 1, α, α^2, α^3 elemanlarının lineer kombinasyonları şeklinde gösterilsin. Buradan, (15, 11)-Hamming koduna denk bir kodun eşlik-denetim matrisi,

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$$= (1 \;\; \alpha \;\; \alpha^2 \;\; \alpha^3 \;\; \alpha^4 \;\; \alpha^5 \;\; \alpha^6 \;\; \alpha^7 \;\; \alpha^8 \;\; \alpha^9 \;\; \alpha^{10} \;\; \alpha^{11} \;\; \alpha^{12} \;\; \alpha^{13} \;\; \alpha^{14})$$

Bu kod, $GF(2)$ üzerinde tasarlanmış mesafesi $d = 3$ olan "dar anlamda BCH kodu" gibi görülebilir. (α^2, $\phi_1(x)$ in bir köküdür.) Kodun minimum uzaklığı 3 tür. Bundan dolayı bu kod, bir- hata düzeltebilir.

6.2.3. n=63 İçin Tüm BCH Kodlarının Oluşturulması

$p(x) = 1 + x + x^6$ primitif polinomu kullanılarak $GF(2^6)$ Galois cismi kolaylıkla kurulabilir.

- $p(\alpha) = 1 + \alpha + \alpha^6 = 0$ alınarak $GF(2^6)$ nın elemanlarını; α 'nın kuvveti olarak, polinom olarak, sıralı 6-lı olarak yazalım.

$p(x) = 1 + x + x^6$ Primitif Polinomu Kullanılarak Oluşturulan $GF(2^6)$ nın Elemanları

Tablo 6.2.3.1.

α nın Kuvveti	α Cinsinden Polinom Olarak	Sıralı 6-lı Olarak
0	0	(000000)
1	1	(100000)
α	α	(010000)
α^2	α^2	(001000)
α^3	α^3	(000100)
α^4	α^4	(000010)
α^5	α^5	(000001)
α^6	$1+\alpha$	(110000)
α^7	$\alpha+\alpha^2$	(011000)
α^8	$\alpha^2+\alpha^3$	(001100)
α^9	$\alpha^3+\alpha^4$	(000110)
α^{10}	$\alpha^4+\alpha^5$	(000011)
α^{11}	$1+\alpha+\alpha^5$	(110001)
α^{12}	$1+\alpha^2$	(101000)
α^{13}	$\alpha+\alpha^3$	(010100)
α^{14}	$\alpha^2+\alpha^4$	(001010)
α^{15}	$\alpha^3+\alpha^5$	(000101)
α^{16}	$1+\alpha+\alpha^4$	(110010)
α^{17}	$\alpha+\alpha^2+\alpha^5$	(011001)
α^{18}	$1+\alpha+\alpha^2+\alpha^3$	(111100)
α^{19}	$\alpha+\alpha^2+\alpha^3+\alpha^4$	(011110)
α^{20}	$\alpha^2+\alpha^3+\alpha^4+\alpha^5$	(001111)
α^{21}	$1+\alpha+\alpha^3+\alpha^4+\alpha^5$	(110111)
α^{22}	$1+\alpha^2+\alpha^4+\alpha^5$	(101011)

α^{23}	$1+\alpha^3+\alpha^5$	(100101)
α^{24}	$1+\alpha^4$	(100010)
α^{25}	$\alpha+\alpha^5$	(010001)
α^{26}	$1+\alpha+\alpha^2$	(111000)
α^{27}	$\alpha+\alpha^2+\alpha^3$	(011100)
α^{28}	$\alpha^2+\alpha^3+\alpha^4$	(001110)
α^{29}	$\alpha^3+\alpha^4+\alpha^5$	(000111)
α^{30}	$1+\alpha+\alpha^4+\alpha^5$	(110011)
α^{31}	$1+\alpha^2+\alpha^5$	(101001)
α^{32}	$1+\alpha^3$	(100100)
α^{33}	$\alpha+\alpha^4$	(010010)
α^{34}	$\alpha^2+\alpha^5$	(001001)
α^{35}	$1+\alpha+\alpha^3$	(110100)
α^{36}	$\alpha+\alpha^2+\alpha^4$	(011010)
α^{37}	$\alpha^2+\alpha^3+\alpha^5$	(001101)
α^{38}	$1+\alpha+\alpha^3+\alpha^4$	(110110)
α^{39}	$\alpha+\alpha^2+\alpha^4+\alpha^5$	(011011)
α^{40}	$1+\alpha+\alpha^2+\alpha^3+\alpha^5$	(111101)
α^{41}	$1+\alpha^2+\alpha^3+\alpha^4$	(101110)
α^{42}	$\alpha+\alpha^3+\alpha^4+\alpha^5$	(010111)
α^{43}	$1+\alpha+\alpha^2+\alpha^4+\alpha^5$	(111011)
α^{44}	$1+\alpha^2+\alpha^3+\alpha^5$	(101101)

(Bu tablonun devamı, ekler bölümünde verilmiştir.)

- $GF(2^6)$ daki elemanların minimal polinomları, aşağıdaki tabloda verildiği gibidir:

$GF(2^6)$ daki Elemanların Minimal Polinomları

Tablo 6.2.3.2.

Elemanlar	Minimal Polinomlar
$\alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}, \alpha^{32}$	$1+x+x^6$
$\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24}, \alpha^{48}, \alpha^{33}$	$1+x+x^2+x^4+x^6$
$\alpha^5, \alpha^{10}, \alpha^{20}, \alpha^{40}, \alpha^{17}, \alpha^{34}$	$1+x+x^2+x^5+x^6$
$\alpha^7, \alpha^{14}, \alpha^{28}, \alpha^{56}, \alpha^{49}, \alpha^{35}$	$1+x^3+x^6$
$\alpha^9, \alpha^{18}, \alpha^{36}$	$1+x^2+x^3$
$\alpha^{11}, \alpha^{22}, \alpha^{44}, \alpha^{25}, \alpha^{50}, \alpha^{37}$	$1+x^2+x^3+x^5+x^6$
$\alpha^{13}, \alpha^{26}, \alpha^{52}, \alpha^{41}, \alpha^{19}, \alpha^{38}$	$1+x+x^3+x^4+x^6$
$\alpha^{15}, \alpha^{30}, \alpha^{60}, \alpha^{57}, \alpha^{51}, \alpha^{39}$	$1+x^2+x^4+x^5+x^6$
α^{21}, α^{42}	$1+x+x^2$
$\alpha^{23}, \alpha^{46}, \alpha^{29}, \alpha^{58}, \alpha^{53}, \alpha^{43}$	$1+x+x^4+x^5+x^6$
$\alpha^{27}, \alpha^{54}, \alpha^{45}$	$1+x+x^3$
$\alpha^{31}, \alpha^{62}, \alpha^{61}, \alpha^{59}, \alpha^{55}, \alpha^{47}$	$1+x^5+x^6$

- O halde, n=63 uzunluklu tüm ikili primitif BCH kodlarının parametreleri ve üreteç polinomları, aşağıdaki gibi olur:

n=63 Uzunluklu Tüm İkili Primitif BCH Kodlarının Parametreleri ve Üreteç Polinomları

Tablo 6.2.3.3.

n	k	t	$g(x)$
63	57	1	$g_1(x) = 1 + x + x^6$
	51	2	$g_2(x) = (1 + x + x^6)(1 + x + x^2 + x^4 + x^6)$
	45	3	$g_3(x) = (1 + x + x^2 + x^5 + x^6)g_2(x)$
	39	4	$g_4(x) = (1 + x^3 + x^6)g_3(x)$
	36	5	$g_5(x) = (1 + x^2 + x^3)g_4(x)$
	30	6	$g_6(x) = (1 + x^2 + x^3 + x^5 + x^6)g_5(x)$
	24	7	$g_7(x) = (1 + x + x^3 + x^4 + x^6)g_6(x)$
	18	10	$g_{10}(x) = (1 + x^2 + x^4 + x^5 + x^6)g_7(x)$
	16	11	$g_{11}(x) = (1 + x + x^2)g_{10}(x)$
	10	13	$g_{13}(x) = (1 + x + x^4 + x^5 + x^6)g_{11}(x)$
	7	15	$g_{15}(x) = (1 + x + x^3)g_{13}(x)$

- $t-$hata düzelten, $n = 2^m - 1$ uzunluklu bir BCH kodunun tanımından da anlaşılacağı gibi, her kod polinomunun kökleri $\alpha, \alpha^2, \ldots, \alpha^{2t}$ ve bunların eşlenikleridir.

- Katsayıları $GF(2)$ den alınan,

$$v(x) = v_0 + v_1 x + \ldots + v_{n-1} x^{n-1}$$

polinomu ele alınsın.

Eğer $\nu(x)$ polinomu,

$$\alpha,\ \alpha^2,\ \ldots,\ \alpha^{2t}$$

yi kök kabul ederse, $\nu(x)$ polinomu, $\alpha,\ \alpha^2,\ \ldots,\ \alpha^{2t}$ nin $\phi_1(x), \phi_2(x), \ldots, \phi_{2t}(x)$ minimal polinomlarıyla bölünebilir. Çünkü, örneğin $\nu(x)$ polinomu, $\phi_1(x)$ ile bölünürse,

$$\nu(x) = \phi_1(x)q(x) + r(x), \qquad \deg r(x) < \deg \phi_1(x)$$

olur.

Denklemde α yerleştirilerek,

$$\nu(\alpha) = \phi_1(\alpha)q(\alpha) + r(\alpha)$$

elde edilir.

$$\nu(\alpha) = \phi_1(\alpha) = 0$$

olduğundan,

$$r(\alpha) = 0$$

elde edilir.

Eğer $r(x) \neq 0$ ise $\deg r(x) < \deg \phi_1(x)$ olmalıdır. Bu ise $\phi_1(x)$ in tanımına aykırıdır. Yani, $\phi_1(x)$ in minimal oluşuna aykırıdır. Dolayısıyla, $r(x) = 0$ olmak zorundadır.

Sonuç olarak,

$$\phi_1(x) \mid \nu(x)$$

bulunur. Diğerleri de benzer tarzda gösterilebilir.

$\phi_1(x) \mid \nu(x)$, $\phi_2(x) \mid \nu(x)$,…, ten $\phi_1(x)$,…, $\phi_{2t}(x)$ lerin en küçük ortak katı da $\nu(x)$ polinomunu böler.

$$g(x) = \text{ekok}\{\phi_1(x), \phi_2(x), \ldots, \phi_{2t}(x)\}$$

olup, $g(x)$ üreteç polinomu, $\nu(x)$ polinomunu böler. Böylece $\nu(x)$, bir kod polinomudur. Buradan yararlanılarak, $n = 2^m - 1$ uzunluklu, $t-$hata düzelten BCH kodu tanımlanabilir:

İkili bir

$$\nu = (\nu_0, \nu_1, \ldots, \nu_{n-1})$$

sıralı $n-$lisinin bir kodsözcüğü olması için gerek ve yeter koşul,

$$\nu(x) = \nu_0 + \nu_1 x + \ldots + \nu_{n-1} x^{n-1}$$

polinomunun

$$\alpha, \alpha^2, \ldots, \alpha^{2t}$$

leri, kök kabul etmesidir.

Bu tanım yardımıyla, kodun minimum mesafesi de kolaylıkla belirlenebilir:

- $n = 2^m - 1$ uzunluklu, $t-$hata düzelten bir BCH kodunun bir kod polinomu,

$$\nu(x) = \nu_0 + \nu_1 x + \ldots + \nu_{n-1} x^{n-1} \qquad (6.2.3.1.)$$

olsun. $1 \le i \le 2t$ için α^i elemanı $\nu(x)$ polinomunun bir kökü olduğundan,

$$\nu(\alpha^i) = \nu_0 + \nu_1 \alpha^i + \nu_2 \alpha^{2i} + \ldots + \nu_{n-1} \alpha^{(n-1)i} = 0 \qquad (6.2.3.2.)$$

olur. Bu eşitliği matrislerle ifade edersek;

$$(v_0, v_1, \ldots, v_{n-1}) \begin{bmatrix} 1 \\ \alpha^i \\ \alpha^{2i} \\ \vdots \\ \alpha^{(n-1)i} \end{bmatrix} = 0, \quad (1 \le i \le 2t) \qquad (6.2.3.3.)$$

(6.2.3.3.) ise, $(v_0, v_1, \ldots, v_{n-1})$ ile $(1, \alpha^i, \alpha^{2i}, \ldots, \alpha^{(n-1)i})$ vektörünün iç çarpımının sıfır olması demektir.

(6.2.3.3.) matris eşitliğinde $1 \le i \le 2t$ olduğunu hatırlayarak, $i = 1, 2, \ldots, 2t$ için,

$$(1, \alpha^i, \alpha^{2i}, \alpha^{3i}, \ldots, \alpha^{(n-1)i})$$

elemanını,

$$(\underbrace{1}_{(\alpha^i)^0}, (\alpha^i)^1, (\alpha^i)^2, (\alpha^i)^3, \ldots, (\alpha^i)^{n-1})$$

şeklinde düşünerek, $i = 1, 2, 3, \ldots, 2t$ satırlarını oluşturarak, aşağıdaki H matrisini yazalım:

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & (\alpha^2)^2 & (\alpha^2)^3 & \cdots & (\alpha^2)^{n-1} \\ 1 & \alpha^3 & (\alpha^3)^2 & (\alpha^3)^3 & \cdots & (\alpha^3)^{n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{2t} & (\alpha^{2t})^2 & (\alpha^{2t})^3 & \cdots & (\alpha^{2t})^{n-1} \end{bmatrix} \qquad (6.2.3.4.)$$

gibi $2t \times n$ matris elde edilir. Bu matriste $(\alpha^3)^2$ dendiğinde; 3. satır, 3. sütun elemanı anlaşılır. Yani $(\alpha^i)^j$ elemanı; $i.$ satır, $(j+1).$ sütun elemanıdır. O zaman (6.2.3.3.) eşitliğinden dolayı,

$$\nu = (\nu_0, \nu_1, \ldots, \nu_{n-1})$$

bir kodsözcüğü ise $t-$hata düzelten BCH kodunda,

$$\nu.H^T = 0 \qquad (6.2.3.5.)$$

olur.

Diğer yandan, eğer $\nu = (\nu_0, \nu_1, \ldots, \nu_{n-1})$ sıralı $n-$lisi, $\nu.H^T = 0$ koşulunu, yani koşul (6.2.3.5.)'i sağlarsa, (6.2.3.3.) ve (6.2.3.2.)'den dolayı, $1 \le i \le 2t$ için α^i ler, $\nu(x)$ polinomunun kökü olurlar. Böylece de ν, $t-$hata düzelten BCH kodunun bir kodsözcüğü olur. Böylece sözkonusu kod, H matrisinin null (sıfır) uzayıdır. Burada H, kodun eşlik-denetim matrisidir.

Eğer i ve j değerleri (pozitif tam sayılar) için α^j, α^i nin bir eşleniği ise,

$$\nu(\alpha^j) = 0 \Leftrightarrow \nu(\alpha^i) = 0$$

dır. Bunun anlamı; $\nu = (\nu_0, \nu_1, \ldots, \nu_{n-1})$ ile H nin $i.$ satırının iç çarpımı sıfır ise, ν ile H nin $j.$ sütununun iç çarpımının sıfır olması demektir.

Bu nedenle, H nin $j.$ satırı atılabilir. O zaman (6.2.3.4.) ile verilen H matrisi, aşağıdaki şekle indirgenmiş olur:

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \cdots & \alpha^{n-1} \\ 1 & \alpha^3 & (\alpha^3)^2 & (\alpha^3)^3 & \cdots & (\alpha^3)^{n-1} \\ 1 & \alpha^5 & (\alpha^5)^2 & (\alpha^5)^3 & \cdots & (\alpha^5)^{n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{2t-1} & (\alpha^{2t-1})^2 & (\alpha^{2t-1})^3 & \cdots & (\alpha^{2t-1})^{n-1} \end{bmatrix} \qquad (6.2.3.6.)$$

olur. Burada j ile, α^i nin eşleniği olan α^j deki j anlatılmaktadır. Ayrıca belirtilmeli ki; H deki elemanlar, $GF(2^m)$ nin elemanlarıdır. $GF(2^m)$ deki her eleman, $GF(2)$ deki elemanların sıralı $m-$lisi olarak yazılır ve sütunlara yerleştirilirse, kodun bir binary eşlik-denetim matrisi elde edilir.

Bunu aşağıdaki örnekle açıklayalım:

Örnek 6.2.3.1. $n = 2^4 - 1 = 15$ uzunluklu, çift-hata düzelten BCH kodu ele alınsın. Bu, bir (15, 7)-koddur. $GF(2^4)$ te primitif bir eleman α olsun. Eşlik-denetim matrisi,

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \cdots & \alpha^{14} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & \alpha^{15} & \alpha^{18} & \cdots & \alpha^{42} \end{bmatrix}$$

olur.

$\alpha^{15} = 1$ olduğu bilindiğine göre, sütunlardaki elemanların sıralı-dörtlüler halindeki gösterilişleri H de yazılırsa, kodun binary eşlik-denetim matrisi elde edilir.

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ . & . & . & . & . & . & . & . & . & . & . & . & . & . & . \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$(\alpha^{12} = \alpha^{27} = \alpha^{42})$ v.b. $\qquad (\mathrm{mod}\, n)$

6.2.4. İki-Hata Düzelten BCH Kodunu Çözmek

$g(x) = \phi_1(x)\phi_3(x)$ üreteç polinomlu iki-hata düzelten

$(2^m - 1,\ 2^m - 2m - 1,\ 5)$ - BCH kodu için eşlik-denetim matrisi H,

yardımcı teorem 6.2.2.1. deki gibi tanımlıdır.

w sözcüğünün alındığı kabul edilsin.

$$w \leftrightarrow w(x)$$

tir. O zaman w nin sendromu,

$$wH = [w(\alpha),\ w(\alpha^3)] = [S_1,\ S_3]$$

olur. S_1 ve S_3 sözcüklerinin her birinin uzunluğu m dir.

Gönderme sırasında hiç hata ortaya çıkmamışsa sendrom,

$$wH = 0$$

dır.

Gönderme sırasında bir-hata ortaya çıkmışsa o zaman hata polinomu,

$$e(x) = x^i$$

dir.

Bu nedenle,

$$wH = eH = [e(\alpha),\ e(\alpha^3)] = [\alpha^i,\ \alpha^{3i}] = [S_1,\ S_3]$$

dır. Buradan,

$$S_1^{\,3} = S_3$$

olur.

Gönderme sırasında i ve j konumlarında $(i \neq j)$ iki-hata ortaya çıkmışsa,

$$e(x) = x^i + x^j$$

ve

$$wH = eH = [e(\alpha),\ e(\alpha^3)] = [\alpha^i + \alpha^j,\ \alpha^{3i} + \alpha^{3j}] = [S_1,\ S_3]$$

dir.

$$\left.\begin{aligned} \alpha^i + \alpha^j &= S_1 \\ \alpha^{3i} + \alpha^{3j} &= S_3 \end{aligned}\right\}$$ denklemlerini çarpanlarına ayıralım.

$$(\alpha^i + \alpha^j)(\alpha^{2i} + \alpha^{i+j} + \alpha^{2j}) = \alpha^{3i} + \alpha^{3j}$$

ve

$$S_1{}^2 = (\alpha^i + \alpha^j)^2 = \alpha^{2i} + \alpha^{2j}$$

dir.

$$S_3 = \alpha^{3i} + \alpha^{3j}$$

$$= (\alpha^i + \alpha^j)(\alpha^{2i} + \alpha^{2j} + \alpha^{i+j})$$

$$= S_1(S_1{}^2 + \alpha^{i+j})$$

dir.

α^i ve α^j, kuadratik denklemin kökleridir.

$$x^2 + (\alpha^i + \alpha^j)x + \alpha^{i+j} = 0$$

ve

$$x^2 + S_1 x + (\frac{S_3}{S_1} + S_1^{\,2}) = 0$$

dır.

Bu denklem çözülerek, hataların yerleri bulunabilir. Denklemin sol tarafındaki polinom, "hata yerleştiren polinom" olarak adlandırılır.

6.2.5. BCH Kodları İçin Genel Kod Çözme Algoritması

BCH kodları için genel kod çözme algoritması aşağıdaki gibi tanımlanabilir:

Gönderilen Kod Polinomu : $w(x)$
Alınan Polinom : $v(x)$
Hata Polinomu : $e(x)$

olsun.

Dolayısıyla,

$$v(x) = w(x) + e(x)$$

tir.

İlk olarak v nin sendromunu bulalım.

$$S(v) = Hv^T = (S_b, S_{b+1}, \ldots, S_{b+d-2})^T$$

dir.

Burada

$$S_j = v(\alpha^j) = w(\alpha^j) + e(\alpha^j) \quad , \qquad (b \le j \le b+d-2)$$

dir.

$r \le t$ tane hata ortaya çıkıyorsa bu durumda,

$$e(x) = \sum_{i=1}^{r} c_i x^{a_i}$$

olur. $a_1,...,a_r$, $\{0, 1,\ldots, n-1\}$ in farklı elemanlarıdır.

$$\eta_i = \alpha^{a_i} \in F_{q^m}$$

elemanları, "hata yerleştirme sayıları" olarak adlandırılır.

$$c_i \in F_q^*$$

elemanları, "hata değerleri" adını alır.

Bu nedenle v nin sendromu için,

$$S_j = e(\alpha^j) = \sum_{i=1}^{r} c_i {\eta_i}^j \qquad (b \le j \le b+d-2)$$

ifadesi elde edilir.

Çünkü F_{q^m} de hesaplama kuralları,

$$S_j{}^q = \left(\sum_{i=1}^{r} c_i {\eta_i}^j \right)^q = \sum_{i=1}^{r} {c_i}^q {\eta_i}^{jq} = \sum_{i=1}^{r} c_i {\eta_i}^{jq} = S_{jq}$$

dır.

Bilinmeyen nicelikler; (η_i, c_i) çiftleri, $S(v)$ sendromunun S_j koordinatlarıdır. Bu bilinmeyenler, alınan v vektöründen hesaplanarak bulunabilir.

İkili durumda herhangi bir hata, yalnız η_i ile karakterize edilir. Bu durumda c_i lerin tümü 1 dir.

Kod çözme algoritmasının sonraki aşamasında,

$$\prod_{i=1}^{r}(\eta_i - x) = \sum_{i=0}^{r}(-1)^i \sigma_{r-i} x^i = \sigma_r - \sigma_{r-1}x + \ldots + (-1)^r \sigma_0 x^r$$

özdeş polinomu ile tanımlı σ_i katsayıları tanımlanır. Bu nedenle $\sigma_0 = 1$ ve $\sigma_1,\ldots,\sigma_r$, $\eta_1,\ldots,\eta_r$ de tanımlı temel simetrik polinomlardır. x in yerine η_i yazarak,

$$(-1)^r \sigma_r S_j + (-1)^{r-1}\sigma_{r-1}S_{j+1} + \ldots + (-1)\sigma_1 {\eta_i}^{r-1} + {\eta_i}^r = 0\,, \quad (i = 1,\ldots,r)$$

elde edilir.

Bu denklemi $c_i {\eta_i}^j$ ile çarpıp, sonra denklemleri toplayarak,

$$(-1)^r \sigma_r S_j + (-1)^{r-1}\sigma_{r-1}S_{j+1} + \ldots + (-1)\sigma_1 S_{j+r-1} + S_{j+r} = 0,$$

$$(i = 1,\ldots,r)\,,\ (J = b,\ b+1,\ \ldots,\ b+r-1)$$

sonucu elde edilir.

Yardımcı Teorem 6.2.5.1.

$$\sum_{i=1}^{r} c_i {\eta_i}^j = S_j\,, \qquad (j = b,\ b+1,\ldots,\ b+r-1)$$

denklemler sisteminde $\eta_{i,}$ $F_{q^m}^*$ nin farklı elemanları ise sistem çözülebilir. (c_i ler, bilinmeyenlerdir.)

İspat.

$$\begin{vmatrix} \eta_1^{\,b} & \eta_2^{\,b} & \cdots & \eta_r^{\,b} \\ \eta_1^{\,b+1} & \eta_2^{\,b+1} & \cdots & \eta_r^{\,b+1} \\ \vdots & \vdots & \vdots & \vdots \\ \eta_1^{\,b+r-1} & \eta_2^{\,b+r-1} & \cdots & \eta_r^{\,b+r-1} \end{vmatrix} = \eta_1^{\,b}\eta_2^{\,b}...\eta_r^{\,b} \prod_{1\le i<j\le r}(\eta_j - \eta_i) \neq 0$$

dır.

Yardımcı Teorem 6.2.5.2.

$$(-1)^r \sigma_r S_j + (-1)^{r-1}\sigma_{r-1}S_{j+1} + ... + (-1)\sigma_1 S_{j+r-1} + S_{j+r} = 0$$

$$(j = b,\, b+1,\, ...,\, b+r-1)$$

denklemler sisteminin çözülebilmesi için gerek ve yeter koşul, r tane hatanın ortaya çıkmasıdır. $(-1)^i \sigma_i,\ \ (i = 1,\, 2,\, \ldots,\, r)$ bilinmeyenlerdir.

İspat. Sistemin matrisi,

$$\begin{bmatrix} S_b & S_{b+1} & \cdots & S_{b+r-1} \\ S_{b+1} & S_{b+2} & \cdots & S_{b+r} \\ \vdots & \vdots & \vdots & \vdots \\ S_{b+r-1} & S_{b+r} & \cdots & S_{b+r-2} \end{bmatrix} = vDv^T$$

olarak ifade edilebilir.

Burada,

$$v = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \eta_1 & \eta_2 & \cdots & \eta_r \\ \vdots & \vdots & \vdots & \vdots \\ {\eta_1}^{r-1} & {\eta_2}^{r-1} & \cdots & {\eta_r}^{r-1} \end{bmatrix} \quad \text{ve} \quad D = \begin{bmatrix} c_1{\eta_1}^{b} & 0 & \cdots & 0 \\ 0 & c_2{\eta_2}^{b} & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & c_r{\eta_r}^{b} \end{bmatrix}$$

dir.

Verilen denklemler sisteminin matrisinin singüler olmaması için gerek ve yeter koşul, v ve D nin singüler olmamasıdır. v nin bir Vandermonde matrisi gibi singüler olmaması için gerek ve yeter koşul, η_i lerin $(i = 1,...,r)$ farklı olmasıdır. D nin singüler olmaması için gerek ve yeter koşul, η_i lerin tümünün ve c_i nin sıfırdan farklı olmasıdır. Her iki durumun sağlanması için gerek ve yeter koşul, r tane hatanın ortaya çıkmasıdır.

6.2.5.1. Hata Yerleştiren Polinom

Hata yerleştiren polinom,

$$S(x) = \prod_{i=1}^{r}(1 - \eta_i x) = \sum_{i=0}^{r}(-1)^i \sigma_i x^i$$

dir. Buradaki σ_i, yukarıda tarif edilmişti. $S(x)$ in kökleri ${\eta_1}^{-1}$, ${\eta_2}^{-1}$, …, ${\eta_r}^{-1}$ dir. Bu kökleri bulmak için, Chien'e atfedilen bir araştırma metodu kullanılabilir.

$\alpha = \alpha^{-(n-1)}$, $S(x)$ in bir kökü ise α^{n-1}, bir hata yerleştirme sayısıdır.

$$S(\alpha) = 0$$

dır.

Daha genel olarak α^{n-m}, $(m = 1, 2, \ldots, n)$ aynı yolla test edilir. İkili durumda hata yerleştiren polinomları tesbit etmek, hataları düzeltmek olarak da düşünülebilir.

$(-1)^{i\sigma_i}$ için τ_i yazarak, BCH kodunun kod çözme algoritması aşağıdaki gibi özetlenebilir:

Tasarlanmış mesafesi $d \geq 2t+1$ olan bir BCH kodu kullanarak gönderilen bir w kodsözcüğünde, en fazla t hata ortaya çıktığı kabul edilsin.

1. Adım: v alıcı sözcüğünün sendromu tanımlanır.

$$S(v) = (S_b,\ S_{b+1},\ \ldots,\ S_{b+d-2})^T, \qquad S_j = \sum_{i=1}^{r} c_i \eta_i{}^j, \qquad (b \leq j \leq b+d-2)$$

olsun.

2. Adım: $S_{j+r} + S_{j+r-1}\tau_1 + \ldots + S_j\tau_r = 0$, $(b \leq j \leq b+r-1)$ denklemler sisteminde $r \leq t$ olan maximum sayı tanımlanır. τ_i, singüler olmayan bir katsayı matrisine sahiptir. Bu nedenle bulunan r sayısı, ortaya çıkan hataların sayısıdır. Bu durumda hata yerleştiren polinom,

$$S(x) = \prod_{i=1}^{r}(1-\eta_i x) = \sum_{i=0}^{r}\tau_i x^i$$

dir. S_j den τ_i katsayıları bulunur.

3. Adım: $S(x)$ deki α nın kuvvetlerinin yerine konulması ile $S(x)=0$ denklemi çözülür. Buradan η_i hata düzeltme sayısı bulunur. (Chien Araştırması)

4. Adım: c_i hata değerlerini tanımlamak için ilk olarak, 1. adımın r tane denklemindeki η_i ifadesi tanımlanır. Bu durumda,

$$w(x) = v(x) - e(x)$$

ifadesinden, gönderilen w kodsözcüğü bulunur.

Örnek 6.2.5.1.1. Tasarlanmış mesafesi $d = 5$ olan bir BCH kodu hesaplansın. Bu kod, herhangi tek veya çift hatayı düzeltebilir.

$b = 1,\ n = 15,\ q = 2$

olsun. $\phi_i(x);\ \alpha \in F_{16}$ primitif eleman olduğunda, F_2 üzerinde α^i nin minimal polinomunu belirtiyorsa $\alpha,\ (x^4 + x + 1)$ in bir köküdür.

Bu durumda;

$\phi_1(x) = \phi_2(x) = \phi_4(x) = \phi_8(x) = 1 + x + x^4,$

$\phi_3(x) = \phi_6(x) = \phi_{12}(x) = \phi_9(x) = 1 + x + x^2 + x^3 + x^4$

olur.

Buradan BCH kodunun üreteç polinomu,

$g(x) = \phi_1(x)\phi_3(x) = 1 + x^4 + x^6 + x^7 + x^8$

olacaktır.

(15, 7)-kodu, eşlik-denetim polinomu ile

$h(x) = (x^{15} - 1) / g(x) = 1 + x^4 + x^6 + x^7$

dir. Vektörleri eşleyerek elde ettiğimiz $g(x),\ xg(x),\ x^2g(x),\ x^3g(x),\ x^4g(x),$ $x^5g(x),\ x^6g(x)$ polinomları, (15, 7)-BCH kodunun tabanı olarak düşünülebilir ve üreteç matrisi,

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

şeklindedir.

Şimdi, v alıcı vektörünün 100100110000100 şeklinde veya $v(x) = 1 + x^3 + x^6 + x^7 + x^{12}$ şeklinde bir polinom olduğunu kabul edelim. 1. adıma göre sendromu hesaplayalım. İşimizi kolaylaştırmak için,

$$S_j{}^q = \left(\sum_{i=1}^{r} c_i \eta_i^{\,j} \right)^q = \sum_{i=1}^{r} c_i{}^q \eta_i^{jq} = \sum_{i=1}^{r} c_i \eta_i^{jq} = S_{jq}$$

ifadesini kullanalım:

$$S_1 = e(\alpha) = v(\alpha) = 1,$$

$$S_2 = e(\alpha^2) = v(\alpha^2) = 1,$$

$$S_3 = e(\alpha^3) = v(\alpha^3) = \alpha^4,$$

$$S_4 = e(\alpha^4) = v(\alpha^4) = 1$$

olarak buluruz.

τ_i bilinmeyenlerinde (2. adım) lineer denklemler sisteminin en büyük ihtimali,

$$S_2\tau_1 + S_1\tau_2 = S_3$$

$$S_3\tau_1 + S_2\tau_2 = S_4$$

veya

$$\tau_1 + \tau_2 = \alpha^4$$

$$\alpha^4\tau_1 + \tau_2 = 1$$

dir.

Bu sistem, singüler olmayan bir katsayı matrisine sahiptir. Buradan 2 hata ortaya çıkmalıdır. Zira, $r = 2$ dir. Bu denklemler sistemini çözelim. $\tau_1 = 1$, $\tau_2 = \alpha$ olarak bulalım. $S(x)$ deki bu değerleri yerine yazıp, $\tau_0 = 1$ olduğunu hatırlarsak,

$$S(x) = 1 + x + \alpha x^2$$

elde ederiz.

F_{16} daki kökler gibi,

$$\eta_1^{-1} = \alpha^8,\ \eta_2^{-1} = \alpha^6$$

buluruz.

Bununla birlikte,

$$\eta_1 = \alpha^7,\ \eta_2 = \alpha^9$$

dur. Kodsözcüğünün hatalarının 8 ve 10 konumlarında ortaya çıkması gerektiğini biliyoruz. Alıcı polinomdaki bu hataları düzeltirsek,

$$w(x) = v(x) - e(x)$$

$$= (1 + x^3 + x^6 + x^7 + x^{12}) - (x^7 + x^9)$$

$$= 1 + x^3 + x^6 + x^9 + x^{12}$$

buluruz.

Buna karşılık gelen kodsözcüğü,

100100100100100

dır.

İlk baştaki mesaj, hata düzelten polinomla tekrar elde edilebilir. Gönderilen kod polinomu,

$$w(x) / g(x)$$

tir.

$$w(x) / g(x) = 1 + x^3 + x^4$$

tür. Ortaya çıkan bu sonuç, 1001100 mesaj sözcüğüne karşılık gelir.

6.3. Son Gelişmeler

Öncelikle minimum mesafe ve tasarlanmış mesafe hakkındaki özelikleri özetleyelim.

1) $n = 2^m - 1$ uzunluklu, tasarlanmış mesafesi $\delta = 2^l - 1$ olan primitif BCH kodunun minimum mesafesi δ olur.

2) Tasarlanmış mesafesi δ olan bir primitif BCH kodunun minimum d mesafesi için $d \leq 2\delta - 1$ dir.

3) İkili bir primitif BCH kodunun minimum ağırlığı bir tek sayıdır.

4) F_q üzerinde $n = q - 1$ uzunluklu primitif bir BCH kodu, bir Reed-Solomon Kodu (RS Kodu) adını alır. Bu kodun birçok önemli uygulaması vardır. Böyle bir kodun üreteci,

$$g(x) = \prod_{i=1}^{d-1} (x - \alpha^i)$$

şeklinde olup, α, F_q de primitiftir.

6.4. Goppa Kodları

BCH kodları yardımıyla tanımlanan bir koddur. Sözcük uzunluğu n, birimin n. bir primitif kökü β, tasarlanmış mesafesi d olan bir BCH kodunda bir

$(c_0, c_1, \ldots, c_{n-1})$

kodsözcüğü ele alınsın. O zaman tanım olarak,

$$\sum_{i=0}^{n-1} c_i (\beta^j)^i = 0 \quad (1 \leq j < d \text{ için})$$

dır.

Bu koşulu, diğer bir yolla yazmayı deneyelim:

$$\frac{z^n - 1}{z - \beta^{-i}} = \sum_{k=0}^{n-1} z^k (\beta^{-i})^{n-1-k} = \sum_{k=0}^{n-1} \beta^{i(k+1)} z^k$$

Buradan, uygun bir $p(z)$ polinomu için,

$$\sum_{i=0}^{n-1} \frac{c_i}{z - \beta^{-i}} = \frac{z^{d-1} p(z)}{z^n - 1}$$

yazılabilir.

Eğer $g(z)$ herhangi bir polinom ve $g(\gamma) \neq 0$ ise $\bmod g(z)$'e göre tek olan $\frac{1}{z-\gamma}$ tanımlanabilir. Burada,

$$(z-\gamma).\frac{1}{z-\gamma} \equiv 1 \pmod{g(z)},$$

yani

$$\frac{1}{z-\gamma} = \frac{-1}{g(\gamma)}.\left(\frac{g(z)-g(\gamma)}{z-\gamma}\right)$$

dır.

Bunlar yardımıyla Goppa kodu, aşağıdaki gibi tanımlanır.

Tanım 6.4.1. F_{q^m} üzerinde t dereceli ve monik $g(z)$ polinomu ele alınsın. $|L| = n$ ve $0 \leq i \leq n-1$ için $g(\gamma_i) \neq 0$ olacak şekilde,

$$L = \{\gamma_0, \gamma_1, \ldots, \gamma_{n-1}\} \subset F_{q^m}$$

kümesi belirlensin. Goppa polinomu $g(z)$ olan $\Gamma(L, g)$ Goppa kodu alfabesi, F_q alfabesi üzerinde

$$\sum_{i=0}^{n-1} \frac{c_i}{z-\gamma_i} \equiv 0 \pmod{g(z)}$$

olacak şekilde belirtilmektedir.

Eğer

$$g(z) = z^{d-1}, \quad L = \{\beta^{-i} \mid 0 \leq i \leq n-1\} \qquad (\beta:\ F_{q^m} \text{ de birimin primitif } n. \text{ kökü})$$

alınırsa $\Gamma(L, g)$ Goppa kodu, tasarlanmış mesafesi d olan dar anlamda BCH kodu olur. ∎

BCH kodları hakkında bazı yeni gelişmeler, aşağıdaki gibi özetlenebilir:

- Grassl M. ve Beth T. "Quantum BCH Codes, 1999" adıyla yaptıkları çalışmada klasik BCH kodları üzerine quantum hata-düzeltme kodlarının nasıl kurulduğunu göstermişlerdir.

- Robert W. Fitzgerald, "A Characterization of Primitive Polynomials Over Finite Fields" isimli çalışmasında, indirgenemez polinomlar arasında primitif polinomların yeni bir karakterizasyonunu vererek sonucu, maximal tasarlanmış mesafeli BCH kodlara uygulamıştır:

$m = 2^k - 1$ ve tasarlanmış mesafesi d olan bir BCH kod, $C \subset GF(2^k)$ olsun. O zaman,

(i) $\text{Boy}\, C = k + 1$

(ii) C nin gerçek minimum mesafesi δ dir.

(iii) $p(x)$, k dereceli bir primitif polinom olmak üzere, C nin denetim polinomu,

$$h(x) = (x-1)\,p(x)$$

dir.

Bunun sonucu olarak $\delta = 2^{k-1} - 1$ alınırsa $g(x)$ üreteç polinomunun ağırlığı $2^{k-1} - 1$ olur. Bu da, C nin minimal ağırlığıdır.

- Eric Ferard ise "Weight of Duals of BCH Codes and Exponential Sums" isimli makalesinde, uzunluğu $n = 2^m - 1$ olan ikili BCH kodlarında m nin tek sayı olma durumunda C nin dualinin mesafesi üzerindeki sınırı geliştirmiştir.

EKLER (*)

$p(x) = 1 + x + x^6$ Primitif Polinomu Kullanılarak $GF(2^6)$ nın Elemanları

Tablo A.1

α^{45}	$1+\alpha^3+\alpha^4$	(100110)
α^{46}	$\alpha+\alpha^4+\alpha^5$	(010011)
α^{47}	$1+\alpha+\alpha^2+\alpha^5$	(111001)
α^{48}	$1+\alpha^2+\alpha^3$	(101100)
α^{49}	$\alpha+\alpha^3+\alpha^4$	(010110)
α^{50}	$\alpha^2+\alpha^4+\alpha^5$	(001011)
α^{51}	$1+\alpha+\alpha^3+\alpha^5$	(110101)
α^{52}	$1+\alpha^2+\alpha^4$	(101010)
α^{53}	$\alpha+\alpha^3+\alpha^5$	(010101)
α^{54}	$1+\alpha+\alpha^2+\alpha^4$	(111010)
α^{55}	$\alpha+\alpha^2+\alpha^3+\alpha^5$	(011101)
α^{56}	$1+\alpha+\alpha^2+\alpha^3+\alpha^4$	(111110)
α^{57}	$\alpha+\alpha^2+\alpha^3+\alpha^4+\alpha^5$	(011111)
α^{58}	$1+\alpha+\alpha^2+\alpha^3+\alpha^4+\alpha^5$	(111111)
α^{59}	$1+\alpha^2+\alpha^3+\alpha^4+\alpha^5$	(101111)
α^{60}	$1+\alpha^3+\alpha^4+\alpha^5$	(100111)
α^{61}	$1+\alpha^4+\alpha^5$	(100011)
α^{62}	$1+\alpha^5$	(100001)

$$\alpha^{63} = 1$$

(*) Bu tabloların belirlenmesinde, büyük ölçüde Costello, D.J. and JR' nin (Shu Lin University of Hawaii, Texas A&M University Prentice-Hall, Inc. Englewood Cliffs, New Jersey.) adlı kitabından yararlanılmıştır.

KAYNAKLAR

A) Kitap ve Kitap Bölümleri için gösterim

Blake, L.F. and Müllin, R.C., 1975. The Mathematical Theory Of Coding, New York-San Francisco, London.

Costello, D.J. and JR., 1983. Error Control Coding, Fundamentals And Applications, Shu Lin University of Hawaii, Texas A&M University, Prentice-Hall, Inc. Englewood Cliffs, New Jersey.

Ferard, E., 2003. Weight Of Duals Of BCH Codes And Exponential Sums, Finite Fields And Their Applications 9, pp. 1-19.

Fitzgerald, R.W., 2003. A Characterization Of Primitive Polynomials Over Finite Fields, Finite Fields And Its Applications 9, pp. 117-121.

Grassl, M. And Beth, T., 1999. Quantum BCH Codes, pp. 207-212, arxiv:quant-ph/9910060v1.

Hankerson ve diğ. (1991). Coding Theory And Cryptography, Auburn University, New York.

Hill, R., 1986. A First Course In Coding Theory, Oxford University, Oxford.

Lidl, R. and Niederreiter, H., 1997. Finite Fields, Vol. 1, Vol. 2, Cambridge University, Cambridge.

Niederreiter, H., 2002. Coding Theory And Cryptology, pp. 259-283, Singapore University, Singapore.

Shparlinski, I. E., 1999. Finite Fields, Theory And Computation, pp. 255-265, Kluwer Academic Publishers.

Stepanov, S. A., 1999. Codes On Algebraic Curves, Kluwer Academic/Plenum Publishers, New York.

Sweeney, P., 1991. Error Control Coding An Introduction Department Of Electronic And Electrical Engineering, University Of Surrey, New York.

Van Lint, J. H., 1999. Introduction to Coding Theory, Springer-Verlag, Berlin.

B) Tezler için gösterim

Zengin, S., 2003. Z_4 Üzerinde Kodlar, Yüksek Lisans Tezi, İ.K.Ü. Fen Bilimleri Enstitüsü, İstanbul.

ÖZGEÇMİŞ

Adı-Soyadı : Selda Çalkavur

Doğum Tarihi : 07.11.1978

Doğum Yeri : Erzincan

İlkokul : 1984-1987, Hürriyet İlkokulu (Kütahya)
1987-1989, Azot İlkokulu (Kütahya)

Ortaokul : 1989-1992, Kütahya Lisesi (Kütahya)

Lise : 1992-1993, Kütahya Lisesi (Kütahya)
1993-1995, Atatürk Lisesi (Van)

Lisans : 1996-2000, Dumlupınar Üniversitesi Fen-Edebiyat Fakültesi Matematik Bölümü

Yüksek Lisans : 2004-2006, İstanbul Kültür Üniversitesi Fen-Bilimleri Enstitüsü Matematik-Bilgisayar Anabilim Dalı

Çalıştığı Kurum : 2000-(Devam ediyor.) İHKİB Yenibosna Hazır Giyim Meslek Lisesi

Görevi : Matematik Öğretmeni