YILDIZ TEKNİK ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

DEVRESEL KODLARIN YAPISI VE DEĞİŞMELİ KODLAR

Esra YÖRÜK

F.B.E. Matematik Anabilim Dalında
hazırlanan

YÜKSEK LİSANS TEZİ

Tez Danışmanı : Prof.Dr. Erol BALKANAY

İSTANBUL , 1996

İÇİNDEKİLER

TEŞEKKÜR

Tez çalışmam süresince bana yön veren ve yardımlarını esirgemeyen değerli hocam Prof.Dr.Erol BALKANAY' a ve tezimin yazılmasını sağlayan değerli arkadaşım Arş.Gör. Çiğdem GENÇ' e teşekkürlerimi bir borç bilirim.

ÖZET

Kodlama teorisinin matematiksel yapısı, özellikle modern cebrin güzelliğini ve gücünü sergilemesi bakımından oldukça önemlidir.

Devresel kodlar, kodların önemli bir bölümünü teşkil etmektedir. Devresel kodları kurmak için $x^n - 1$ polinomunu çarpanlarına ayırmak gerekmektedir. Üreteç polinomunun ve üreteç idempotentinin devresel kodları kurmaktaki katkısı oldukça büyüktür.

Değişmeli kodlar, devresel kodların önemli bir uzantısı olarak düşünülmektedir. Burada ele alınan grup değişmeli olduğundan indirgenemez gösteriliş ile indirgenemez karakter arasında bir fark görülmemektedir.

ABSTRACT

Coding theory is of great mathematical interest, in particular, illustrating the power and the beauty of algebra.

Cyclic codes form an important class of codes. In order to construct cyclic codes, the polynomial $x^n - 1$ must be factored. The generator polynomial and the generating idempotent takes a big role to construct cyclic codes.

It is thought that abelian codes represent a significant extension of cyclic codes. In here, because of the considered group is abelian, no difference is seen between irreducible representation and irreducible character.

GİRİŞ

Kodlama teorisinin doğuşu, Shannon'un bir makalesiyle 1948 de ortaya çıkmıştır. O günden beri dijital bilgilerin ve haberleşmenin gürültülü bir kanalda güvenilir bir şekilde iletilebilmesi için bu bilgilerin kodlanması üzerine bir çok çalışma yapılmıştır.

Hata düzeltme kodları (Error-correcting codes) uzaydan resimlerin iletilmesinde, kayıt işlemlerinde, bilgilerin manyetik teypte kaydedilmesinde, bilgilerin depolanıp saklanmasında oldukça fazla kullanılmaktadır.

Kodlama teorisinin matematiksel yapısı da oldukça önemlidir. Modern cebrin güzelliğini ve gücünü sergilemektedir.

Devresel kodlarla ilgili ilk çalışma 1957 yılında Prange tarafından yapılmıştır. Devresel kodlar bir çok nedenden dolayı kodların önemli bir sınıfını oluşturmaktadır. Teorik olarak bakıldığında devresel kodlar zengin bir cebrik yapıya sahiptir. Devresel kodları kodlamak için devre kayıtları denen basit cihazlar kullanılmaktadır. Golay kodları, Hamming kodları ve BCH kodları gibi pek çok önemli kod devresel kodlar olarak gösterilmektedir. Bir devresel kod, sonlu bir cisim üzerinde bir devresel grubun grup cebrindeki bir ideal olarak düşünüldüğünde daha genel grup cebirlerindeki ideallerin yapısı olarak ele alınabilmektedir.

Değişmeli gruplar sınıfı, basit olmalarından dolayı ilgi odağı olan bir sınıftır. Böyle grupların yapısı iyi bilinse de değişmeli gruplar devresel grupların önemli bir uzantısını teşkil etmektedirler. 1970 yılında Camion değişmeli kodlarda devresel kodların dolaysız çarpımı ile elde edilemeyen ideallerin varolduğunu göstermiştir. Berman da 1967 yılında asimptotiksel olarak değişmeli kodların varlığını ispatlamıştır.

Bu çalışmanın amacı devresel kodların nasıl kurulduğunu ve değişmeli kodların devresel kodlarla ne şekilde bir ilişkisi olduğunu göstermektir.

Bu çalışma dört bölümden oluşmaktadır. İlk bölümde cebrik ön bilgiler, ikinci bölümde kodlarla ilgili ön bilgiler verilmiştir. Üçüncü bölümde devresel kodun tanımlanmasına, devresel kodların kurulmasında üreteç polinomunun önemine, dual

kodun üreteç polinomuna ve devresel kodların üreteç idempotentlerine yer verilmiştir. Son bölümde ise değişmeli kodlar ve bunların devresel kodlarla olan ilişkisi anlatılmaktadır.

BÖLÜM 1

1. CEBİRSEL ÖN BİLGİLER

Tanım 1.1: Bir R halkasındaki her I ideali uygun bir $a \in R$ için $I = (a)$ şeklindeyse R halkası bir esas ideal halkası adını alır.

Tanım 1.2: Birimli ve değişmeli R halkasının bir I ideali alınsın. $I \neq R$ ve R nin $I \subset J \subseteq R$ koşulunu sağlayan bir J ideali için $J = R$ oluyorsa I ya R nin maksimal ideali denir.

Tanım 1.3: Bir R halkasında bir M ideali tarafından kapsanan tek ideal sadece sıfır ise o zaman M ideali minimal ideal adını alır. Diğer bir deyişle birimli ve değişmeli R halkasının bir I ideali alınsın. $I \neq \{0\}$ ve R nin $\{0\} \subset J \subset I$ koşulunu sağlayan bir J ideali yoksa I' ya R nin minimal ideali denir.

Tanım 1.4: G bir sonlu grup ve K keyfi bir cisim olsun. KG grup cebri, sırasıyla

$$\sum_{g \in G} \alpha_g g + \sum_{g \in G} \beta_g g = \sum_{g \in G} (\alpha_g + \beta_g) g$$

olarak tanımlana bir toplama ve

$$\left(\sum_{g \in G} \alpha_g g \right) \left(\sum_{h \in G} \beta_h h \right) \sum_{g,h \in G} \alpha_g \beta_h gh = \sum_{f \in G} \nu_f f$$

olarak tanımlanan bir çarpma olmak üzere

$$KG = \left\{ \sum_{g \in G} \alpha_g g, \quad \alpha_g \in K \right\}$$

formal toplamların kümesidir.($\nu_f = \sum_{g \in G} \alpha_g \beta_{g^{-1} f}$)

Grup cebri, K üzerinde bir vektör uzayıdır. O zaman doğal olarak grup cebri birimli bir halka ve K üzerinde bir cebirdir. K üzerinde bir vektör uzayı olarak düşünülünce grup elemanları uygun bir baz oluşturur.

Tanım 1.5: R nin ideallerinin (içerme ile kısmi sıralı) her boş olmayan kümesi, bir minimal eleman içerirse minimum koşulu sağlanır.

Tanım 1.6: Minimum koşullu bir R halkası, $radR = \{0\}$ ise yarıbasit halka adını alır.

Tanım 1.7: $a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0, \quad a_i \in K$ (K bir cisim) polinomunda $a_n = 1$ ise polinom monik polinom adını alır.

Tanım 1.8: L bir cisim ve L nin bir alt kümesi K olsun. Eğer K kümesi L deki " + " ve "." işlemleri altında bir cisim ise L ye K nın bir cisim genişlemesi denir.

Tanım 1.9: Eğer bir $p(x) \in K[x]$ polinomu, sabit olmayan iki polinomun çarpımı olarak (K üzerinde) yazılamıyorsa $p(x)$ polinomuna indirgenemez polinom denir.

Tanım 1.10: Eğer $f(x)$ m. dereceden bir polinom ise o zaman $x^m f(x^{-1})$ şeklinde tanımlanan polinom $f(x)$ in karşıt (reciprocal) polinomu adını alır.

Eğer $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ ise bunun karşıt polinomu $a_0 x^n + a_1 x^{n-1} + \ldots + a_n$ şeklinde olur. Yani katsayıların sıralanması ters olur.

Tanım 1.11: Sonlu G grubunun bir gösterilişi

$$p : G \to GL(V) \qquad p(ab) = p(a)p(b) \qquad a, b \in G$$

olmak üzere bir grup homomorfizmidir. Burada $GL(V)$ genel lineer grup yani V nin terslenebilir izomorfizmlerinin veya lineer dönüşümlerinin çarpımsal grubudur. Yukarıdaki tanımdan

$$p(1) = I \quad , \quad p(a^{-1}) = (p(a))^{-1} \quad , \quad a \in G$$

dir.

Tanım 1.12: p, G nin V gösteriliş uzaylı bir gösterilişi olsun. Eğer V hiçbir esas değişmez V_1 alt uzayını (yani $V_1 \neq V$ ve $V_1 \neq \{0\}$) içermezse p bir indirgenemez gösteriliş adını alır. Her gösteriliş indirgenemez gösterilişlerin dolaysız bir toplamı olarak ifade edilebilir.

Tanım 1.13: Eğer $p(G)$ G nin bir gösterilişi ise G nin karakteri

$$\chi_p(g) = izp(g)$$

dir. Bir gösterilişin karakteri açıkça bir sınıf fonksiyonudur. Yani g_1 ve g_2 G nin aynı eşlenik sınıfında ise $\chi_p(g_1) = \chi_p(g_2)$ dir.

Tanım 1.14: Eğer $e(x), e^2(x) = e(x)$ olacak şekilde bir idempotent ise $GF(q)[x]/(x^n - 1)$ deki bir idealin $e(x)$ üreteci üreteç idempotenti adını alır.

Tanım 1.15: $0 \leq s < p^m - 1$ olmak üzere bir s gözönüne alınsın ve r, $p^{r+1}s \equiv s \pmod{(p^m - 1)}$ özelliğine sahip en küçük sayı olsun. s i içeren cyclotomic koseti $\{s, ps, p^2s, \ldots, p^r s\}$ i içerir. Burada her $p^i s \pmod{(p^m - 1)}$ e göre azaltılır. Eğer $OBEB(s, p^m - 1) = 1$ ise o zaman $r = m - 1$ dir, fakat $OBEB(s, p^m - 1) \neq 1$ ise o zaman r, s ile değişir. Cyclotomic kosetler, tamsayıları $\mod(p^m - 1)$ e göre ayırır, $\mod(p^m - 1)$ e göre her tamsayı kesinlikle bir cyclotomic kosetin içindedir.

BÖLÜM 2

2. KODLARLA İLGİLİ ÖN BİLGİLER

Tanım 2.1: C bir lineer kod ve bir kodsözcüğünün bir devresel düzeni de yine bir kodsözcüğü ise C kodu bir devresel kod adını alır. Bu durumda $a = (\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$, bir kodsözcüğü ise $(\alpha_{n-1}, \alpha_0, \alpha_1, \ldots, \alpha_{n-2})$ de bir kodsözcüğüdür.

Tanım 2.2: $(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ bir kodsözcüğü olmak üzere

$$a(x) = \sum_{i=0}^{n-1} \alpha_i x^i$$

ploinomuna C için kodsözcüğü polinomu denir.

$$a(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_{n-1} x^{n-1}$$

dir.

Tanım 2.3: $a(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_{n-1} x^{n-1}$ olmak üzere $xa(x) = \alpha_0 x + \alpha_1 x^2 + \ldots + \alpha_{n-1} x^n$ *olup* $x^n \equiv 1 \pmod{(x^n - 1)}$ olduğundan $xa(x) = \alpha_{n-1} + \alpha_0 x + \alpha_1 x^2 + \ldots + \alpha_{n-2} x^{n-1}$ olur. Buna a kodsözcüğünün devresel düzeni denir.

Tanım 2.4: $GF(q)[x]/(x^n - 1)$ de sıfırdan farklı bir devresel kod C olmak üzere C de;

1-) Derecesi en küçük tek bir monik polinom olan $g(x)$ varsa,

2-) $g(x)$, $C =< g(x) >$ i sağlıyorsa,

3-) $g(x)$, $x^n - 1$ in bir çarpanıysa bir üreteç polinomu adını alır.

Tanım 2.5: Eğer C bir lineer $[n, k]$ kod ise onun ağırlık numaralaması

$$W_c(z) = \sum_{i=0}^{n} A_i z^i = A_0 + A_1 z + A_2 z^2 + \ldots + A_n z^n$$

polinomu ile tanımlanır. Burada A_i , C deki i ağırlıklı kodsözcüklerinin sayısını gösterir.

Tanım 2.6: C bir kod ve $C^{\perp} = \{u \in V \mid u.w = 0 \quad , \forall w \in C\}$ olsun. Burada $u.w = 0$ dan u ve v birbirlerine ortogonaldir. C, k-boyutlu ise $C^{\perp}$, $n-k$ boyutludur. $C^{\perp}$ ye C nin dual kodu denir.

Tanım 2.7: Lineer bir $[n,k]$ kodun bir bazındaki vektörleri satırlara yazarak elde edilen bir kxn matris bu lineer kodun bir üreteç matrisi adını alır.

Tanım 2.8: Bir $[n,k]$ kod C olmak üzere $C^{\perp}$ (C nin duali)' ın bir H üreteç matrisi C nin parite-kontrol matrisi adını alır.

Tanım 2.9: Eğer $C \subset C^{\perp}$ ise o zaman C kodu self-ortogonal kod adını alır.

Tanım 2.10: $x^n - 1 = g(x)h(x)$ ve $g(x)$ bir C devresel kodunun üreteç polinomu ise o zaman $h(x)$ e C nin kontrol polinomu denir.

BÖLÜM 3

3. DEVRESEL KODLAR

3.1 Devresel Kodlar

Bir (n,k) kod C olmak üzere $x=(a_0,a_1,\ldots,a_{n-1})$ sözcüğü C nin bir kodsözcüğü olmak koşuluyla bunun ilk devresel düzeni $y=(a_{n-1},a_0,a_1,\ldots,a_{n-2})$ ise C devresel adını alır. Bu y nin ilk devresel düzeni olan $(a_{n-2},a_{n-1},a_0,a_1,\ldots,a_{n-3})$ ün ve x in diğer tüm devresel düzenlerinin de C de bulunduğu anlamına gelir.

Devresel kodlar gözönüne alındığında, bir $(a_0,a_1,\ldots,a_{n-1})$ vektörünü bir $a_0+a_1x+a_2x^2+\ldots+a_{n-1}x^{n-1}$ polinomuna karşılık getirmek yararlıdır. Bu durumda $(a_{n-1},a_0,a_1,\ldots,a_{n-2})$ sözcüğü, $a_{n-1}+a_0x+a_1x^2+\ldots+a_{n-2}x^{n-1}$ e karşılık gelir. Bu polinomun

$$(a_0+a_1x+a_2x^2+\ldots+a_{n-1}x^{n-1})x \pmod{(x^n-1)}$$

polinomuna eşit olduğu görülmektedir. $(x^n\equiv 1 \pmod{(x^n-1)})$

Devresel kodlar için, $\mathrm{mod}(x^n-1)$ e göre $GF(q)[x]$ deki polinomların eşlenik sınıflarını içeren $A_n=GF(q)[x]/(x^n-1)$ ile ilgilenilecektir. $GF(q)[x]$, x değişkenli $GF(q)$ üzerindeki bütün polinomların kümesidir. Aynı zamanda $GF(q)[x]$ bir esas ideal halkasıdır. $GF(q)[x]$ deki polinomların eşlenik sınıfları, derecesi n den küçük polinomlar olarak düşünülecektir. $GF(q)[x]/(x^n-1)$ de polinomlar $GF(q)[x]$ de olduğu gibi toplanır ve çıkarılır, ancak çarpma $\mathrm{mod}(x^n-1)$ e göre yapılır. $GF(q)[x]/(x^n-1)$ bölüm halkası ile çarpmada $\mathrm{mod}(x^n-1)$ e göre tanımlanmış derecesi n den küçük olan polinomların halkası arasında doğal bir izomorfizm vardır. Burada (x^n-1) ideali x^n-1 polinomuyla üretilmiştir.

Kesin olarak eğer $a(x)$ ve $b(x)$ gibi iki polinom varsa bunların $GF(q)[x]$ deki çarpımı bölme algoritmasından

$$a(x)b(x)=c(x)(x^n-1)+r(x)$$

şeklindedir. Burada $r(x)$ in derecesi x^n-1 in derecesinden azdır. $\mathrm{mod}(x^n-1)$ e göre çarpma ile $GF(q)[x]$ de derecesi n den az olan bütün polimonları A_n olarak düşünerek $r(x)$ e $a(x)$ ve $b(x)$ in çarpımları olarak bakılabilir. $GF(q)[x]$ ve

$GF(q)[x]/(x^n-1)$ in her ikiside ileride tanımlanacak olan cebrik yapının örnekleridir.

Birimli ve değişmeli bir $(R,+,.)$ halkası aşağıdaki özelliklere sahiptir.

(i) R, "+" ve "." işlemleri altında kapalıdır.

(ii) R, "+" işlemi altında değişmeli bir gruptur.

(iii) Her $a,b,c \in R$ için $a(bc)=(ab)c$ dir. Yani çarpmaya göre birleşme özelliği vardır.

(iv) Her $a,b \in R$ için $ab=ba$ dır. Yani çarpmaya göre değişme özelliği vardır.

(v) Her $a \in R$ için $a.1=1.a=a$ dır. Yani çarpmaya göre R nin birimi 1 dir.

(vi) Her $a,b,c \in R$ için $a(b+c)=ab+ac$ dir. Yani dağılma özelliği vardır.

Sıfırdan farklı bir eleman çarpımsal bir terse sahip olmak zorunda olmadığı gibi R de bir cisim olmak zorunda değildir. "+" ve "." ya göre tam sayılar birimli ve değişmeli bir halkadır.

Değişmeli bir R halkasında bir I ideali, aşağıdaki iki koşulu sağlayan R nin bir alt kümesidir.

(i) Eğer $a \in I$ ise o zaman her $b \in R$ için $ab \in I$ dır.

(ii) Eğer $a \in I$ ve $b \in I$ ise o zaman $a+b \in I$ ve $a-b \in I$ dır.

İkinci koşul I nın $(R,+)$ toplamsal grubunun bir alt grubu olduğu anlamına gelir.

V koordinatları 0' dan $n-1$ e kadar etiketlenen $GF(q)$ üzerinde bütün sıralı $n-$lilerin uzayı olsun ve bir $v=(a_0,a_1,...,a_{n-1})$ vektörü $A_n=GF(q)[x]/(x^n-1)$ deki bir $a_0+a_1x+a_2x^2+...+a_{n-1}x^{n-1}$ polimonuna karşılık gelsin. Aşağıdaki teorem bu eşlemeyi açıklamaktadır.

Teorem 3.1.1: A_n deki elemanların kümesi olan S ancak ve ancak A_n de bir ideal ise bir C devresel koduna karşılık gelir.

İspat:

S devresel bir koda karşılık gelen A_n deki elemanların bir kümesi olsun. O zaman eğer $a_1(x) \in S$ ve $a_2(x) \in S$ ise kod tanımından $a_1(x) \mp a_2(x) \in S$ dir. Devresel düzeni x ile çarpımına karşılık getirilirse $a(x) \in S$ ise o zaman $a(x)x \in S$ olur. Bunun gibi $(a(x)x)x = a(x)x^2$, $((a(x)x)x)x = a(x)x^3, \ldots \in S$ olur. $a(x) \in S$ ve $b(x) = b_0 + b_1x + b_2x^2 + \ldots + b_{n-1}x^{n-1}$ de A_n de bir polinom olmak üzere $a(x)b(x)$ gözönüne alınsın. Toplamdaki her eleman S de olduğundan

$$a(x)b(x) = b_0a(x) + b_1a(x)x + b_2a(x)x^2 + \ldots + b_{n-1}a(x)x^{n-1} \in S \quad olur.$$

Sonuç olarak S bir idealdir. Eğer S, A_n de bir ideal ise o zaman S deki polinomların, bir devresel kodun vektörlerine karşılık geldiği apaçık bellidir.

V tüm $Z_2 = \{0, 1\}$ nin sıralı 3-lülerinin uzayı olsun. Tüm ikili devresel kodlar, V ve A_3 belirtilsin.

Tablo 3.1

KOD	*V*	A_3
C_1	$(0,0,0)$	0
C_2	$(0,0,0)$	0
	$(1,1,1)$	$1+x+x^2$
C_3	$(0,0,0)$	0
	$(1,1,0)$	$1+x$
	$(0,1,1)$	$x+x^2$
	$(1,0,1)$	$1+x^2$
C_4	V nin tümü	A_3 ün tümü

Bundan böyle devresel bir kod denince ya devresel düzen altında kapalı bir kod yada A_n de bir ideal anlaşılacaktır.

3.2. Devresel Kodları Kurmak: Üreteç Polinomu

Tablo 3.1' deki C_3 e bakıldığında her vektörün $1+x$ polinomunun bir katı olduğu görülür. Koddaki vektörler $x+x^2=(1+x)x$ ve $1+x^2=(1+x)^2$ dir.

A_n deki bir I ideali, I nın her elemanı, $g(x)$ gibi sabit bir polinomun bir katı ise esas ideal adını alır. Eğer I bir esas ideal ise o zaman $I=\{c(x)g(x);\ c(x)\in A_n\}$ olur. Bu $I=<g(x)>$ ile gösterilir. $g(x)$ in I yı üreten tek polinom olmadığı göz önüne alınsın.

Aşağıdaki teoremler yardımıyla devresel kodların kuruluşu anlatılmış olacaktır.

Teorem 3.2.1: n uzunluklu bir C devresel kodu $A_n=GF(q)[x]/(x^n-1)$ de bir ideal ise $g(x)$, C de en küçük dereceli monik polinom olur. O zaman $g(x)$ tek bir şekilde belirlenir ve $C=<g(x)>$ olur.

İspat:

Burada A_n in bir esas ideal halkası olduğu ve bir idealin başka üreteçlere sahip olmasına rağmen en küçük dereceli monik üretecinin de tek olduğu gösterilmelidir.

Öncelikle A_n in bir esas ideal halkası olduğu gösterilsin. $g(x)$, C deki en küçük dereceli monik polinom ve $a(x)$ de C deki diğer polinom olsun. $GF(q)[x]$ teki bölme algoritmasından $a(x)=g(x)b(x)+r(x)$ olur. Burada $degr(x)<degg(x)$ tir. İdeal tanımından $r(x)\in C$ dir. Fakat bu, $r(x)$ özdeş olarak sıfır olmadıkça $g(x)$ in seçimiyle çelişir. Böylece $a(x)=g(x)b(x)$ olur. Buradan A_n bir esas ideal halkasıdır.

$g(x)$ ve $h(x)$ aynı dereceden iki monik polinom ise ve her ikisi de C nin elemanı ise o zaman $g(x)-h(x)$ polinomu derecesi $g(x)$ veya $h(x)$ in derecesinden küçük olan bir polinomdur. $g(x)$ en küçük dereceye sahip ise bu olamaz. Böylece $g(x)$, C deki en küçük dereceli tek monik polinomdur ve $C=<g(x)>$ tir.

Özet olarak $A_n=GF(q)[x]/(x^n-1)$ olmak üzere A_n, $GF(q)$ üzerinde bir cebirdir. Çünkü A_n, $GF(q)$ cismi üzerinde bir vektör uzayı olan bir halkadır. $GF(q)$ üzerinde n uzunluklu bir kodsözcüğü yine A_n in bir elemanı olarak belirtilir. A_n cebri birimli, değişmeli bir halka olduğundan ve her ideali tek bir üretece sahip

olduğundan bir esas ideal halkasıdır.

C_n n. mertebeden bir devresel grup olsun. $GF(q)C_n$ grup cebri, $GF(q)$ üzerinde bir vektör uzayı olan birimli bir halka ve $GF(q)$ üzerinde bir cebirdir. Dolayısıyla A_n cebri $GF(q)C_n$ grup cebrine izomorfiktir.

$x^n - 1$ polinomu devresel kodlar teorisinde bir anahtar rolü oynar. $(n, q) = 1$ olacak şekilde $x^n - 1$ in $GF(q)$ da 1 den büyük böleni yoktur.

Aşağıdaki teorem, kesin olarak bir devresel kodun bu $g(x)$ üretecinin nasıl bulunduğunu göstermek açısından önemlidir. Burada C, derecesi n den az olan $\text{mod}(x^n - 1)$ e göre $g(x)$ in katlarının eşlenik sınıflarının gösterilişlerini kapsayan ideal olarak düşünülür.

Teorem 3.2.2: Eğer C, A_n de bir ideal ise, C nin en küçük dereceli tek monik üreteci olan $g(x)$, $x^n - 1$ i böler ve tersine C deki bir $g(x)$ polinomu $x^n - 1$ i bölerse o zaman $g(x)$, $< g(x) >$ teki en küçük dereceye sahiptir.

İspat:

Öncelikle $g(x)$, C deki en küçük dereceli monik polinom olsun. $GF(q)[x]$ deki bölme algoritmasından $x^n - 1 = a(x)g(x) + r(x)$ olur. Burada $degr(x) < degg(x)$ tir. Böylece $r(x) = -a(x)g(x) \mod(x^n - 1)$ olur. Buradan da $r(x) \in < g(x) >$ olur. Bu, $r(x)$ özdeş olarak sıfır olmadıkça bir çelişkidir., Böylece $g(x)|x^n - 1$ dir.

Tersine, $g(x)$ in $x^n - 1$ i böldüğü ve $b(x) \in < g(x) >$ olduğu fakat $degb(x) < degg(x)$ olduğu düşünülsün. O zaman $GF(q)[x]$ de

$$b(x) = c(x)g(x) + (x^n - 1)d(x)$$

olur, çünkü $b(x) \in C$ dir. Bununla birlikte $g(x)$, $x^n - 1$ i böldüğünden $g(x)|b(x)$ dir. Bu bir çelişkidir.

Böylece bir devresel kod kurmak için $x^n - 1$ i çarpanlarına ayırmak gerekir. Bu çarpanlarına ayırmayı daha büyük n ler için yapmak zor olsa da yararlıdır. İkili devresel kodları gözönünde bulundururken, $x^n - 1$ farklı çarpanlara sahip olacağından n in tek sayı olduğu düşünülsün.

C deki en küçük dereceli monik polinom olan $g(x)$, C nin üreteç polinomu olarak adlandırılır. Önceki teoremlerden $C = < g(x) >$ olduğu ve $g(x)$ in $x^n - 1$ i

böldüğü bilinmektedir. $GF(q)$ üzerinde $x^n - 1$ çarpanlarına ayrılabilirse, $GF(q)$ üzerinde n uzunluklu tüm devresel kodlar kurulabilir.

Şimdi $x^n - 1$ in $i = 1, 2, ..., s$ olmak üzere $g_i(x)$ ler gibi çarpanları olsun. O zaman N_i, A_n in $g_i(x)$ ile üretilen bir maksimal idealidir. Çünkü

$$N_i =< g_i(x) > \neq GF(q)[x]/(x^n - 1)$$

dir. A_n in bir A idealindeki minimal dereceli $g(x)$ monik polinomu A nın bir üretecidir ve $x^n - 1$ i böler. O zaman $(x^n - 1)/g_i(x)$ ile üretilen minimal ideal de M_i dir. $i \neq j$ olmak üzere N_i ve N_j, A_n in birbirinden farklı maksimal idealleri olsun. $(n, q) = 1$ olduğundan $N_i.N_j = N_i \cap N_j$ dir. Dolayısıyla $g_i(x).g_j(x)$, $i \neq j$ ile üretilen ideal $N_i \cap N_j$ olur.

$\sigma_n : i \to iq \pmod{n}$ fonksiyonu gözönüne alınsın. Bu fonksiyon $\{0, 1, ..., n-1\}$ tamsayılarını, $i = 1, 2, ..., s$ olmak üzere, s_i kümelerine ayırır. $\{s_i, i = 1, 2, ..., s\}$ kümelerinin kümesi $\sum_q(n)$ ile gösterilsin. $|\sum_q(n)| = s$ olarak alınsın. Eğer α, $F(q)$ nun bir cisim genişlemesindeki birimin ilkel bir n. kökü ise

$$g_i(x) = \prod_{i \in s_i} (x - \alpha^j)$$

kabul edilebilir.

$C_n =< x >$, $x^n = 1$ olacak şekilde n. mertebeden çarpımsal devresel grup olsun. Bu durumda $GF(q)C_n$ grup cebri ile $GF(q)[x]/(x^n - 1)$ arasında bir izomorfizm vardır. Burada x değişkeni, her iki cebir için özdeşliği vurgulamak için kullanılır. $(n, q) = 1$ koşulu, $x^n - 1$ in birbirinden farklı köklere sahip olmasını, $GF(q)C_n$ grup cebrinde de yarıbasitliliği ve buradan da tek olan minimal ideallerin dolaysız bir toplamına ayrılmasını sağlar. Bu iki sonuç temel olarak aynıdır. Yarıbasit olmamanın sonucunu görmek için şunlar hatırlanmalıdır.

$GF(p)/(x^p - 1)$ cebri, $GF(p)C_p$ ye denk olsun. $GF(p)$ üzerinde $x^p - 1 = (x-1)^p$ dir. $GF(p)[x]/(x^p - 1)$ in herhangi bir ideali $(x^p - 1)$ in bir böleniyle üretilir. Bu ideallerin hepsine A_i denilsin. O zaman A_i ler $i = 0, 1, ..., p$ olmak üzere $(x-1)^i$ üreteç polinomlarına sahiptirler ve bunlar ideallerin tümünü oluştururlar. Bu idealler için

$$GF(p)[x]/(x^p - 1) = A_0 \supset A_1 \supset A_2 \supset ... \supset A_p$$

dir.

M_i ler, $GF(q)C_n$ in tek minimal idealleri olmak üzere

$$GF(q)C_n = M_1 \oplus M_2 \oplus ... \oplus M_s$$

olarak yazılabilir. Böylece $GF(q)C_n$ in her ideali, bu minimal ideallerin bir dolaysız toplamıdır. $h_i(x) = (x^n - 1)/g_i(x)$, M_i minimal idealinin üreteç polinomu olsun. İdempotent elemanı $e_i(x) \in M_i$ ile gösterilsin. $GF(q)C_n$ grup cebri birimli bir halka olduğundan $1 \in GF(q)C_n$ dir. Eğer $GF(q)C_n$ olduğu kabul edilirse

$$1 = e_1(x) + e_2(x) + ... + e_s(x) \tag{3.1}$$

olur. Bu eşitliğin her iki tarafı $e_i(x)$ ile çarpılırsa

$$e_i(x) = e_i(x)e_1(x) + e_i(x)e_2(x) + ... + e_i^2(x) + ... + e_i(x)e_s(x)$$

elde edilir.

Toplam dolaysız olduğundan

$$e_i(x)e_j(x) = \delta_{ij}e_i(x)$$

olmalıdır. Burada δ_{ij} Kronecker delta fonksiyonudur ve

$$\delta_{ij} = \begin{cases} 1 & , i = j \\ 0 & , i \neq j \end{cases}$$

dir.

Böylece $\{e_i(x)\}$ elemanlarının kümesi ortogonal idempotentlerinin bir kümesidir. M_i lerin minimal idealler olduğu bilinmektedir. Dolayısıyla

$$M_i = GF(q)C_n e_i(x)$$

yazılabilir. Burada $e_i(x)$, M_i nin birimidir ve M_i nin dışındaki herhangi bir elemanı yutar. Yani $f(x) = \sum f_i(x)$ ve $f_i(x) \in M_i$ ise $e_i(x)f(x) = f_i(x)$ dir. M_i ve M_j idealleri $GF(q)C_n$ devresel grup cebrinde sırasıyla $\frac{x^n-1}{g_i(x)}$ ve $\frac{x^n-1}{g_j(x)}$ ile üretilir. O halde $M_i \cup M_j = M_i \oplus M_j$,

$$\left(\frac{x^n-1}{g_i(x)}, \frac{x^n-1}{g_j(x)}\right) = \frac{x^n-1}{g_i(x)g_j(x)} \quad , \quad i \neq j$$

ile üretilir. $g_i(x)$ ile üretilen ideal $\bigoplus_{j=1,j\neq i}^{s} M_j = N_i$ dir. (3.1)' den N_i nin idempotenti

$$e_1(x) + e_2(x) + ... + e_{i-1}(x) + e_{i+1}(x) + ... + e_s(x) = 1 - e_i(x)$$

tir. Çünkü $GF(q)C_n = GF(q)C_n e_i(x) \oplus GF(q)C_n(1 - e_i(x))$ tir.

Özet olarak M_i, $h_i(x) = (x^n - 1)/g_i(x)$ üreteç polinomuna ve $e_i(x)$ idempotentine sahip iken, N_i de $g_i(x)$ üreteç polinomuna ve $1 - e_i(x)$ idempotentine sahiptir. Benzer şekilde eğer $\{i_1, ..., i_r\} \cup \{j_1, ..., j_{s-r}\} = \{1, 2, ..., s\}$ ise o zaman

$$g_{i_1}(x)...g_{i_r}(x) = (x^n - 1)/g_{j_1}(x)...g_{j_{s-r}}(x)$$

ile üretilen ideal $\bigoplus_{k=1}^{s-r} M_{jk}$ idealidir ve bu idealin idempotenti

$$1 - (e_{i_1}(x) + ... + e_{i_r}(x)) = e_{j_1}(x) + ... + e_{j_{s-r}}(x)$$

tir. $g(x)$, M de minimal dereceli tek monik polinom olsun. Eğer M in keyfi bir ideali $g(x)$ ile üretilirse o zaman $(n, q) = 1$ olacak şekilde, $h(x) = (x^n - 1)/g(x)$ tir. ve $g(x)$ ile aralarında asal olurlar. Böylece Öklid algoritmasına göre öyle $a(x)$ ve $b(x)$ polinomları vardır ki

$$a(x)g(x) + b(x)h(x) = 1 \tag{3.2}$$

dir. $e(x) = a(x)g(x) \in M$ olsun. (3.2) $e(x)$ ile çarpılsın.

$$a(x)g(x)e(x) + b(x)h(x)e(x) = e(x)$$

olur. (3.2) den $b(x)h(x) = 1 - a(x)g(x)$ tir. Buradan

$$a(x)g(x)e(x) + (1 - a(x)g(x))e(x) = e(x)$$

$$\Rightarrow \quad e^2(x) + e(x) - e^2(x) = e(x) = e^2(x) \quad \Rightarrow \quad e^2(x) = e(x)$$

olur. Dolayısıyla $e(x) = a(x)g(x) \in M$ bir idempotenttir. Bu idempotent tektir ve M i üretir. Ayrıca M üzerinde bir birimdir. $GF(q)C_n$ in her idempotenti belirli bir $e_i(x)$ lerin bir toplamıdır.

Ön Teorem 3.2.1: *Birimli ve değişmeli bir R halkasında M, R nin bir maksimal ideali ise R/M sonlu bir cisimdir.*

$i = 1, 2, ..., s$ olmak üzere M_i ler uygun büyüklükteki bütün sonlu cisimlerdir. $e(x)$, $GF(q)C_n$ in keyfi bir idempotenti olsun. Bu, $\sum_{i=1}^{s} a_i(x)$, $a_i(x) \in M_i$ şeklinde yazılabilir. $GF(q)C_n$ M_i lerin dolaysız bir toplamı olduğundan bu ayrılış tektir. $e(x)$ idempotent olduğundan

$$e^2(x) = \sum a_i^2(x) = \sum a_i(x)$$

olur. Bu $a_i(x) \in M_i$ nin de idempotent olduğunu gösterir. $e_i(x)$ idempotent ve M_i nin birimi olduğundan $a_i^2(x) = a_i(x) = a_i(x)e_i(x)$ olarak yazılabilir. Buradan $a_i(x)(a_i(x) - e_i(x)) = 0$ olur. Buradan da $a_i(x) = 0$ veya $a_i(x) - e_i(x) = 0$ olur. Bu işlem sonlu bir cisim içinde geçtiğinden istenen ispatlanmış olur. Böylece keyfi bir M ideali pek çok idempotente sahip olur, fakat bu idempotentlerin hepsi, $\alpha_i = 0, 1$ olmak üzere, $\sum \alpha_i e_i(x)$ şeklindedir. Eğer $M = M_{i_1} \oplus ... \oplus M_{i_r}$ ise o zaman M üzerinde bir birim görevi gören tek idempotenttir, yani üreteç idempotenti $e_{i_1}(x) + ... + e_{i_r}(x)$ tir.

M ve M' sırasıyla $e(x)$ ve $e'(x)$ üreteç idempotentine sahip, $GF(q)C_n$ in iki keyfi ideali olsun. O zaman $e(x)e'(x)$, $M \cap M'$ nün bir birimseli ve tek üreteç idempotentidir.

Örnek 2.1:

$i = 1, 2, 3, 4$ olmak üzere, M_i ler, $e_i(x)$ idempotentli, $GF(q)C_n$ in minimal idealleri olsun. $M = M_1 \oplus M_2 \oplus M_3$ ve $M' = M_2 \oplus M_3 \oplus M_4$ olsun.

M, $e(x) = e_1(x) + e_2(x) + e_3(x)$;

M' de, $e'(x) = e_2(x) + e_3(x) + e_4(x)$

idempotentine sahiptir. $M \cap M' = M_2 \oplus M_3$ tür ve $e_2(x) + e_3(x)$ idempotentine sahiptir. Basit bir hesapla aynı zamanda

$$e(x)e'(x) = (e_1(x) + e_2(x) + e_3(x))(e_2(x) + e_3(x) + e_4(x))$$

$$e_i(x)e_j(x) = \delta_{ij}e_i(x) \quad ve \quad \delta_{ij} = \begin{cases} 0 & , i \neq j \\ 1 & , i = j \end{cases}$$

den dolayı $e(x)e'(x) = e_2(x) + e_3(x)$ elde edilir.

$$n(M \cup M') = n(M) + n(M') - n(M \cap M')$$

olduğundan aynı notasyonu kullanarak $M \cup M'$, $e(x) + e'(x) - e(x)e'(x)$ idempotentine sahiptir ve bu $M \cup M'$ nün bir birimseli görevini görür. Aynı zamanda $M \cup M' = M_1 \oplus M_2 \oplus M_3 \oplus M_4$ tür. $M \cup M'$,

$$e_1(x) + e_2(x) + e_3(x) + e_4(x) = (e_1(x) + e_2(x) + e_3(x)) + (e_2(x) + e_3(x) + e_4(x)) - (e_2(x) + e_3(x))$$

idempotentine sahiptir. Bu da yapılan hesabı doğrular.

Genelde şüphesiz, eğer $M + M' = GF(q)C_n$ ve $M \cap M' = \{0\}$ ise o zaman $e'(x) = 1 - e(x)$ olur. Eğer $M \cap M' = \{0\}$ ise M in herhangi iki elemanı $f(x) \in M$ ve $f'(x) \in M'$ olacak şekilde $f(x)f'(x) = 0$ olur.

Teoerm 3.2.3: $degg(x) = n - k$ ise o zaman $C =< g(x) >$ in boyutu k dır. Eğer $g(x) = g_0 + g_1x + ... + g_{n-k}x^{n-k}$ ise o zaman C nin bir üreteç matrisi aşağıdaki gibidir.

$$\begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_{n-k} & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k-1} & g_{n-k} & 0 & \cdots & 0 \\ 0 & 0 & g_0 & \cdots & g_{n-k-2} & g_{n-k-1} & g_{n-k} & \cdots & 0 \\ \vdots & & & & & & & & \\ 0 & 0 & 0 & & . & . & . & & g_{n-k} \end{bmatrix}$$

İspat:

$g(x), g(x)x, g(x)x^2, ..., g(x)x^{k-1}$ vektörleri lineer bağımsızdır, aksi halde

$$a_0g(x) + a_1g(x)x + ... + a_{k-1}g(x)x^{k-1} = (a_0 + a_1x + ... + a_{k-1}x^{k-1})g(x) = 0$$

olacak şekilde $0 \leq i \leq k-1$ olmak üzere a_i cisim elemanlari var olacaktır. Fakat bu çarpım n den küçük dereceye sahiptir, böylece her $a_i = 0$ olmadıkça bu çarpım $\text{mod}(x^n - 1)$ e göre 0 olamaz. Bu vektörlerin C yi genişlettiğini görmek için C

deki herhangi bir $s(x)$, $c(x)g(x)$ şeklinde ifade edilebilir. Burada $derC(x) \leq k-1$ dir. Buradan

$$\begin{aligned} c(x)g(x) &= (c_0 + c_1x + ... + c_{k-1}x^{k-1})g(x) \\ &= c_0g(x) + c_1g(x)x + ... + c_{k-1}g(x)x^{k-1} \end{aligned}$$

elde edilir.

Buradan C nin bir üreteç matrisi, ilk satırı $g(x)$, ikinci satırı $g(x)x$, üçüncü satırı $g(x)x^2$,... , k. satırı $g(x)x^{k-1}$ olan bir matristir. Bu yukarıda verilen matristir.

Örnek olarak ikili devresel kodlar $n = 7$ için kurulabilir. İlk yapılacak olan $x^7 - 1$ i çarpanlarına ayırmaktır. O da

$$x^7 - 1 = (1+x)(1+x+x^3)(1+x^2+x^3)$$

tür. Bu çarpanlara ayrılış 7 uzunluklu tüm devresel kodları verir. Bunlardan sekizi $x^7 - 1$ in sekiz bölenine karşılık gelir. $g(x) = 1+x+x^3$ olmak üzere $C =< g(x) >$ olduğu gözönüne alınsın. O zaman C dört-boyutludur ve aşağıdaki üreteç matrisine sahiptir.

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

Bu devre kayıt kodu örneği olarak düşünülebilir. Fakat henüz devre kaydındaki bağlantıların bir açıklaması yoktur. Bunlar bir sonraki kısmın konusu olan dual kodun üreteç polinomunda verilecektir.

3.3 Dual Kodun Üreteç Polinomu, Üreteç İdempotenti:

$GF(q)$ üzerinde $x^n - 1$ i çarpanlarına ayırabilirsek o zaman $GF(q)$ üzerinde, n uzunluklu kaç tane devresel kodun bulunduğu bilinir. Daha ötesi, çarpanın derecesinden kodun boyutu bilinir. Aynı zamanda çarpan, kesin olarak bir üreteç matrisi verir. Çarpanlardan bir parite kontrol matrisi bulabilmek yararlı olacaktır. Bu hatta dual kodun üreteç polinomunu belirlemekle de yapılabilir. Devresel

kodun tanımından hemen görülmesine rağmen bu devresel bir kodun dualinin de devresel olduğunu gösterir.

$g(x)$, bir C devresel kodunun üreteç polinomu olsun. $g(x)$, x^n-1 i böldüğünden $x^n-1=g(x)h(x)$ dir. Eğer $degg(x)=n-k$ ise o zaman C, k boyutludur ve $degh(x)=k$ dır. $h(x)$, x^n-1 i böldüğünden, bir $C'^{\perp}$, $(n,n-k)$ devresel kodunun üreteç polinomudur. $C^{\perp}$, $n-k$ boyutlu olduğundan, $C^{\perp}$ nün üreteç polinomu $h(x)$ in terimleri cinsinden belirtilebilmektedir. Yani $C^{\perp}$ dual kodu $h^*(x)=x^k h(x^{-1})$ karşıt (reciprocal) polinomuyla üretilir. Eğer $C'^{\perp}$, $h(x)$ ile üretilen $(n,n-k)$ kod ise o zaman $C^{\perp}$ ve $C'^{\perp}$ denk kodlardır ve bunlara $GF(q)C_n$ de idealler gözüyle bakılır.

$$\eta: \quad C^{\perp} \to C'^{\perp}$$

$$x \to x^{-1}$$

fonksiyonu gözönüne alınsın. $GF(q)C_n$ deki çarpmanın terimleri ile $C'^{\perp}$ ideali C nin doğal bir dualidir. $a(x) \in C$ ve $b(x) \in C'^{\perp}$ ise $a(x)b(x)=0$ dır. Aşağıdaki teorem bu duruma açıklık kazandıracaktır.

Teorem 3.3.1: $a(x)=(a_0,a_1,...,a_{n-1})$ ve $b(x)=(b_0,b_1,...,b_{n-1})$ olsun. O zaman $GF(q)C_n$ de $a(x)b(x)=0$ olması için gyk $a(x)$ in $(b_{n-1},...,b_0)$ vektörüne ve bu vektörün her devresel düzenine ortogonal olmasıdır.

İspat:

İspatı kolaylaştırmak için $n=7$ hali ele alınacaktır. $a(x)=(a_0,a_1,...,a_6)$ $b(x)=(b_6,...,b_0)$ ve onun tüm düzenlerine ortogonal olması durumu aşağıdaki denklemlerle açıklanabilir.

$$a_0b_6+a_1b_5+...+a_6b_0=0$$

$$a_0b_0+a_1b_6+...+a_6b_1=0$$

$$\vdots$$

$$a_0b_5+a_1b_4+...+a_6b_6=0$$

Şimdi A_7 de $a(x)b(x)=(a_0+a_1x+...+a_6x^6)(b_0+b_1x+...+b_6x^6)$ hesaplansın. Burada çarpma işlemi $\bmod x^7-1$ e göredir. İspatın amaçları için x in kuvvetlerinin katsayıları $x^6,x^0=1,x,x^2,...,x^5$ sırasında yazılabilir.

O zaman

$$a(x)b(x) = (a_0b_6 + a_1b_5 + ... + a_6b_0)x^6 + (a_0b_0 + a_1b_6 + ... + a_6b_1) + ... \\ + (a_0b_5 + a_1b_4 + ... + a_6b_6)x^5$$

elde edilir. Bu katsayılar yukarıdaki çarpımlara eşit olduğundan teorem ispatlanmış olur.

$C^{\perp}$, daha alışılmış iç çarpıma göre, C nin doğal bir dualidir, eğer $e(x)$, C nin üreteç idempotenti ise o zaman $1 - e(x)$, $C'^{\perp}$ nin üreteç idempotentidir ve $e(x)(1 - e(x)) = 0$ dır. Çünkü

$$e(x)(1 - e(x)) = e(x) - e^2(x) = e(x) - e(x) = 0$$

dır.

Teorem 3.3.2: Eğer $g(x)h(x) = x^n - 1$ polinomu $GF(q)[x]$ te ise ve $g(x)$, bir C kodunun üreteç polinomu ise o zaman $h(x)$ in karşıt (reciprocal) polinomu $C^{\perp}$ nin üreteç polinomudur. Dahası, eğer $h(x) = h_0 + h_1x + ... + h_kx^k$ ise o zaman aşağıdaki matris C nin bir H parite kontrol matrisidir.

$$H = \begin{bmatrix} h_k & h_{k-1} & \dots & h_0 & 0 & 0 & \dots & 0 \\ 0 & h_k & \dots & h_1 & h_0 & 0 & \dots & 0 \\ \vdots & & \vdots & & & & & \\ 0 & 0 & h_k & . & . & . & & h_0 \end{bmatrix}$$

Buradan $C^{\perp}$ devreseldir.

İspat:

Son teoremde $a(x) = g(x)$ve $b(x) = h(x)$ olsun. O zaman $h(x)$ in karşıt polinomu

$$x^k h(x^{-1}) = h_0x^k + h_1x^{k-1} + ... + h_k = h_k + h_{k-1}x + ... + h_0x^k$$

olur. Bir önceki teorem, $g(x)$ in $h(x)$ in karşıt polinomuna ve onun tüm devresel düzenlerine ortogonal olduğunu gösterir. Teorem 3.2.3 te verildiği gibi G C nin

üreteç matrisi olsun. O zaman, G onun ilk r_1 satırını ve r_1 in ilk $k-1$ devresel düzenini kapsar. A, ilk k satırı G nin satırları olan ve $n-k$ satırı da r_1 in kalan devresel düzenlerinin yerine geçen nxn matris olsun. s_1, H nin ilk satırı ve B, s_1 ve onun devresel düzenlerinin tümünü içeren nxn matris olsun. O zaman r_1, B nin satırlarının tümüne ortogonaldir; çünkü $g(x)$, $h(x)$ in karşıt polinomuna ve onun düzenlerinin tümüne ortogonaldir. $l \equiv (j+i) \pmod{n}$ olmak üzere $(r_l, s_j) = (r_i, s_{l-1})$ olduğundan, A nın tüm satırları, B nin tüm satırlarına ortogonaldir. C nin boyutu k olduğundan ve H üreteç matrisli kodun boyutu $n-k$ olduğundan, H, C nin bir parite kontrol matrisi ve $C^{\perp}$ nün de bir üreteç matrisidir.

Bu oldukça önemlidir, çünkü $x^n - 1$ i çarpanlarına ayırdıktan sonra her C devresel kodu için, bir üreteç polinomu, aynı zamanda üreteci ve parite kontrol matrisleri belirlenebilir. Tekrar $GF(2)$ üzerindeki $x^7 - 1$ örneği ele alınsın.

$$x^7 - 1 = (1+x)(1+x+x^3)(1+x^2+x^3)$$

tür. Üreteç polinomu $1+x+x^3$ olan C devresel kodu için bir üreteç matrisi kurulmuştur. Şimdi C için bir parite kontrol matrisi bulunabilir. $h(x)$ kontrol polinomu, $h(x) = (1+x)(1+x^2+x^3) = 1+x+x^2+x^4$ tür. Bunun karşıt polinomu $x^4(1+x^{-1}+x^{-2}+x^{-4}) = 1+x^2+x^3+x^4$ tür. Buradan C için bir parite kontrol matrisi aşağıdaki gibidir.

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

Gerçekten C için, H nin bir parite kontrol matrisi olduğu kolaylıkla görülür. Aslında C deki devre kaydı için bağlantılar $1+x^2+x^3+x^4$ tarafından düzenlenir. Bir vektörün ilk dört bilgi konumları $v - v_0$, v_1, v_2 ve v_3, v nin 5. konumu olan v_4 mod2 ye göre $v_0 + v_2 + v_3$ ün toplamı olarak verilir. Bu, H nin ilk satırının, C ye ortogonal olduğu durumunu ifade eder. v nin 6. ve 7. basamakları benzer olarak H nin 2. ve 3. satırları kullanılarak hesaplanır. Bu yöntem bir devresel kod ürettiğinden ilk başlanan devre kaydının her yedi basamaktan sonra tekrar etmesi

gerektiğini göstermek zor değildir.

$$\eta_r : \quad GF(q)C_n \to GF(q)C_n$$
$$x^i \to \quad x^{ri} \qquad\qquad i = 1, 2, ..., n-1$$

fonksiyonu gözönüne alınsın. Bu fonksiyonun $(r, n) = 1$ ise bir cebir izomorfizmi olduğu gösterilebilir. Yani

1-) $\eta_r(x^{i_1} + x^{i_2}) = (x^{i_1} + x^{i_2})^r = (x^{ri_1} + x^{ri_2}) = \eta_r(x^{i_1}) + \eta_r(x^{i_2})$

2-) $\eta_r(x^{i_1}.x^{i_2}) = x^{(i_1+i_2)r} = x^{ri_1}.x^{ri_2} = \eta_r(x^{i_1}).\eta_r(x^{i_2})$

dir. Ayrıca η_r, $(1-1)$ dir. $\{\eta_r : (r, n) = 1\}$ fonksiyonları kümesi $\eta_{r_1}\eta_{r_2} = \eta_{r_1 r_2}$ iken bileşke işlemi altında otomorfizmaların bir grubunu oluşturur. Açıkça η_r gibi bir fonksiyon bir minimal ideali aynı boyuttaki başka bir minimal ideale görüntüler. Buna denk olarak η_r, bir $s_i \in \sum_q(n)$ kümesini bir s_j kümesine görüntüler. Burada $|s_i| = |s_j|$ dir. Benzer bir denklik, minimal ideallerin indirgenemez üreteç polinomlarının terimleri cinsinden kurulabilir. Eğer r birimselleri içeren s_i kümesi içinde ise, o zaman η_r, M_i nin bir otomorfizmidir. Burada M_i, s_i ye karşılık gelen minimal idealdir. Buradan, herhangi bir i için, $r = q^i(\text{mod}n)$ ve $r_1, r_2 \in s_j$ olduğundan $\eta_{r_1}(M_j) = \eta_{r_2}(M_j)$ olur.

Örnek:

$q = 3^2$ ve $n = 11$ olsun. $\sum_q(11)$ ' in devirleri,

$s_1 = \{0\}$

$s_2 = \{1, 9, 4, 3, 5\}$

$s_3 = \{2, 7, 8, 6, 10\}$ tür.

Şöyle ki mod11 e göre ve mertebesi 5 olduğundan

$s_1 = \{0.9^0, 0.9^1, ..., 0.9^4\} = \{0\}$

$s_2 = \{1.9^0, 1.9^1, 1.9^2, 1.9^3, 1.9^4\} = \{1, 9, 4, 3, 5\}$

$s_3 = \{2.9^0, 2.9^1, 2.9^2, 2.9^3, 2.9^4\} = \{2, 7, 8, 6, 10\}$ tür.

[redacted]

η_r otomorfizmalarının herhangi biri, cebrin birimini sabit tutar. η_r, keyfi bir M idealini M' ye görüntülesin. Eğer $e(x)$, M in üreteç idempotenti ise o zaman $\eta_r(e(x))$, M' nün üreteç idempotentidir. Genelde bir ideal bir çok idempotent

içerir. Fakat üreteç idempotenti, o ideal üzerinde bir birim görevi gören tek idempotenttir.

N_1, $GF(2)[x]/(x^n+1)$ de $\{1,2,2^2,...,2^{m-1}\}$ deviriyle ilgili olan

$$g_1(x) = \Pi_{i=0}^{m-1}(x-\alpha^{2^i})$$

polinomuyla üretilen maksimal ideal olsun. u ve v, n ile aralarında asal olan tamsayılar ve $u.v \equiv 1(\mathrm{mod}n)$ olsun. $\eta_u(N_1)$ in $\{v,2v,...,2^{m-1}v\}$ deviriyle ilgili olan maksimal ideal olduğu gösterilsin. Bu devirle ilgili olan indirgenemez polinom aynı zamanda $(v,n)=1$ iken n eksponentine sahiptir. $u.v \equiv 1$ iken

$$\eta_u(g_1(x)) = g_1(x^u) = \Pi_{i=0}^{m-1}(x^u-\alpha^{2^i}) = \Pi_{i=0}^{m-1}(x^u-\alpha^{2^i uv})$$

yazılabilir. $(x-\alpha^{2^i v})|(x^u-\alpha^{2^i uv})$ olduğundan $g_2(x)|\eta_u(g_1(x))$ tir. Burada $g_2(x)$, $\{v,2v,...,2^{m-1}v\}$ devresine karşılık gelir. Buradan $\eta_u(g_1(x))$, $g_2(x)$ ile üretilen N_2 maksimal ideali tarafından içerilir. η_u bir otomorfizm olduğundan $\eta_u(N_1)$ bir maksimal idealdir ve $\eta_u(N_1) = N_2$ olur. Buradan eğer M_1 ve M_2 sırasıyla $\{1,2,2^2,...,2^{m-1}\}$ ve $\{v,2v,...,2^{m-1}v\}$ devirleriyle ilgili minimal idealler ise o zaman $\eta_u(M_1) = M_2$ olur. Her durumda η_u, bir idempotenti bir idempotente görüntüler.

Yukarıda kullanılan devreler maksimum üslüdürler. M_1 ve M_2 aynı boyutlu $e = \frac{n}{r}$ üssüne sahip iki minimal ideal olsun. İlgili devirleri $\{a,2a,...,2^{l-1}a\}$ ve $\{b,2b,...,2^{l-1}b\}$ olsun. Bu devirler aynı uzunlukludur. $a = sb$ olmak üzere $(s,n)=1$ olacak şekilde bir s tamsayısı vardır. Yukarıdaki ispatla, $\eta_s(M_1) = M_2$ elde edilir. Böylece eğer M_1 ve M_2 aynı boyutlu ve aynı üslü ise o zaman $\eta_u(M_1) = M_2$ olacak şekilde bir η_u otomorfizması vardır.

Tersine, M_1 ve M_2 minimal idealler olsun ve $\eta_u(M_1) = M_2$ olacak şekilde bir η_u otomorfizması var olsun. M_1, $s_1 = \{a,2a,...,2^{l-1}a\}$ deviri ile, M_2 de $s_2 = \{b,2b,...,2^{l-1}b\}$ deviri ile ilgili olsun. M_1 ve M_2 nin aynı boyuta sahip olduğunu gösteren η_u bir izomorfizm olduğundan bu devirler aynı uzunluğa sahip olmalıdır. Yukarıdaki aynı yöntemi kullanarak, η_u fonksiyonunun bir kümeyi diğer bir kümeye görüntülediği gösterilebilir. $a = ub$ olarak kabul edilsin. s_1, e_1

üssüne, s_2 de e_2 üssüne sahip olsun. Buradan $\alpha^{ae_1} = 1 = (\alpha^{ub})^{e_1}$ elde edilir. Eğer $(u,v) = 1 \pmod{n}$ ise $va = b \pmod{n}$ ve $\alpha^{vae_1} = 1 = \alpha^{uvbe_1} = (\alpha^b)^{e_1}$ olur.Bu da e_2 nin e_1 i böldüğünü ve α^b mertebeli olduğunu gösterir. Benzer şekilde $e_1|e_2$ olduğu gösterilebilir ve buradan $e_1 = e_2$ olur. Dolayısıyla sonuç olarak eğer bir η_u otomorfizmi için $\eta_u(M_1) = M_2$ ise M_1 ve M_2 aynı üsse sahip olmalıdır.

Teorem 3.3.3: M_1 ve M_2, $GF(q)C_n$ in minimal idealleri olsun. O zaman ancak ve ancak $\eta_u(M_1) = M_2$ olmak üzere bir η_u otomorfizmi varsa, M_1 ve M_2 aynı boyuta ve aynı üsse sahiptir.

Eğer bu iki minimal ideal aynı ağırlık numaralamasına sahip ise izomorfiktirler.

Teorem 3.3.4: C_1 ve C_2, $g_1(x)$ ve $g_2(x)$ üreteç polinomlu devresel kodlar olsun. O zaman $C_1 \subseteq C_2$ olması için gyk $g_2(x)|g_1(x)$ olmasıdır.

İspat:

$C_1 \subseteq C_2$ olduğundan ancak ve ancak $g_2(x)|g_1(x)$ ise $< g_1(x) > \subseteq < g_2(x) >$ olur.

Teorem 3.3.5: $1+x$ üreteç polinomlu C devresel kodu, n uzunluklu bütün çift ağırlıklı vektörleri içeren $n-1$ boyutlu C kodudur. İkili bir $C = < g(x) >$ devresel kodu, ancak ve ancak $1+x$, $g(x)$ i bölerse sadece çift ağırlıklı vektörleri içerir.

İspat:

$1+x$ üreteç polinomlu C devresel kodunun boyutu $n-1$ dir. O zaman $(x^n-1) = (1+x)(1+x+...+x^{n-1})$ olduğundan ve $1+x+...+x^{n-1}$ kendinin karşıt polinomu olduğundan, $C^{\perp}$, $1+x+...+x^{n-1}$ üreteç polinomlu bir boyutlu uzaydır. Sıfır vektörünü ve bütün bir h vektörünü içeren kod olduğu kolaylıkla görülür. Açıkça, bir ikili vektör ancak ve ancak çift ağırlığa sahipse h ye ortogonaldir.

$g(x)$ üreteç polinomlu bir C' ikili devresel kodu ancak ve ancak $1+x$, $g(x)$ i bölerken $C' \subseteq C$ ise sadece çift ağırlıklı vektörleri içerir.

$1+x+x^3$ üreteç polinomlu, 7 uzunluklu ikili bir C koduyla ilgili son örnek gözönüne alındığında bu kodun tek ağırlıklı vektörleri içerdiği görülür. Bununla beraber $(1+x)(1+x+x^3) = 1+x^2+x^3+x^4$ üreteç polinomlu kod, sadece çift ağırlıklı vektörlere sahiptir ve C tarafından kapsanır.

Sonuç 3.3.1: $g(x)$ üreteç polinomlu bir ikili devresel kod, self-ortogonal ise o zaman $1+x$, $g(x)$ i bölmelidir.

İspat:

İkili bir self-ortogonal kodunda bütün ağırlıklar çifttir.

Aşağıdaki teorem, x^n-1 in çarpanlarına ayrılışının, bir devresel kodun self-ortogonal olup olmadığının gösterilmesinde oldukça yararlı olduğunu açıklar.

Teorem 3.3.6: $GF(q)$ üzerinde $x^n-1=g(x)h(x)$ olsun. $g(x)$ üreteç polinomlu bir C devresel kodu ancak ve ancak $h(x)$ in karşıt polinomu $g(x)$ i bölerse self-ortogonaldir.

İspat:

Bir C kodu ancak ve ancak $C^{\perp}$ nin üreteç polinomu $g(x)$ i bölerken $C \subseteq C^{\perp}$ ise self-ortogonaldir.

$(x^7+1)=(1+x)(1+x+x^3)(1+x^2+x^3)$ olduğundan $x^3h(x^{-1})=1+x+x^3$ iken $1+x^2+x^3+x^4$ ü bölen $1+x^2+x^3+x^4=(1+x)(1+x+x^3)$ üreteç polinomlu kod self-ortogonaldir.

Ön Teorem 3.3.1: İkili bir $f(x)$ polinomu, ancak ve $f(x)$ de sıfırdan farklı katsayılarla görünen x kuvvetlerinin S kümesi n için cyclotomic kalan sınıflarının birleşimi ise A_n de bir idempotenttir.

$n=7$ için cyclotomic kalan sınıfları hesaplanırsa

$C_0=\{0\}$

$C_1=\{1,2,4\}$

$C_3=\{3,6,5\}$

olur. Buradan tüm sekiz idempotent görülebilir. Kod ve kodun boyutu için üreteç polinomlu olarak aşağıdaki gibi sıralanabilir. İdempotentten sonra onun üreteç polinomuyla ilişkisi yazılabilir.

Tablo 2:

Üreteç Polinomu	Boyutu	Üreteç İdempotenti
$g_1(x) = (1+x+x^3)(1+x^2+x^3)$	1	$e_1(x) = g_1(x)$ $= 1+x+x^2+x^3+x^4+x^5+x^6$
$g_2(x) = (1+x)(1+x+x^3)$	3	$e_2(x) = x^3 g_2(x) = 1+x^3+x^5+x^6$
$g_3(x) = (1+x)(1+x^2+x^3)$	3	$e_3(x) = g_3(x) = 1+x+x^2+x^4$
$g_4(x) = 1+x$	6	$e_2(x)+e_3(x) = (x+x^3+x^5)g_4(x)$ $= x+x^2+x^3+x^4+x^5+x^6$
$g_5(x) = 1+x+x^3$	4	$e_1(x)+e_2(x) = xg_5(x) = x+x^2+x^4$
$g_6(x) = 1+x^2+x^3$	4	$e_1(x)+e_3(x) = x^3 g_6(x) = x^3+x^5+x^6$

7. idempotent ve kodu tüm uzaydır; 8. idempotent 0 dır ve kodu sadece sıfır vektörüdür. 7 uzunluklu her devresel kod bir üreteç idempotentidir. $e_1(x)$, $e_2(x)$ ve $e_3(x)$ belirli özel idempotentlerdir. Çünkü $1 = e_1(x)+e_2(x)+e_3(x)$, $i \neq j$ ise $e_i(x)e_j(x) = 0$ dır ve her diğer idempotent bu özel alanların bir toplamıdır. Görüldüğü gibi bunlar genel durumların belirli örnekleridir.

Şimdi $\hat{f}_i(x)$, $f_i(x)$ hariç bütün çarpanların çarpımı olmak üzere

$$x^n - 1 = (x-1)f_1(x)...f_k(x)$$

olsun.

Teorem 3.3.7: $f_i(x)$ ler indirgenemez olmak üzere, $x^n - 1 = (x-1)f_1(x)...f_k(x)$ olsun. O zaman bir C devresel kodu, ancak ve ancak $\hat{f}_i(x)$ veya $\widehat{(x-1)}$ gibi üreteç polinomuna sahipse bir minimal idealdir.

Teorem 3.3.8: Belirli bir n için, k tane cyclotomic kalan sınıfı olsun. O zaman 2^k tane ikili devresel kod vardır. Bundan başka n bir p asalı olsun ve $2^m \equiv 1(\mathrm{mod} p)$ olacak şekilde m en küçük tamsayı olsun. O zaman cyclotomic kalan sınıflarının $k-1$ tanesi m elemana sahiptir ve bir tanesi bir elemana sahiptir. f_i ler indirgenemez olmak üzere, $x^p - 1 = (x-1)f_1...f_{k-1}$ ise o zaman her f_i, m. dereceye sahiptir ve $< \widehat{x-1} >$ hariç, her minimal ideal m boyuta sahiptir.

İspat:

Eğer k tane cyclotomic kalan sınıfı varsa, o zaman 2^k tane idempotent hesaplanabilir ve herbiri bir devresel kod üretir. Eğer n bir p asalı ise, o zaman $\{0\}$ hariç her cyclotomic kalan sınıfı m elemana sahip olmalıdır.

$s2^i \equiv s2^j \,(\mathrm{mod}p)$ olduğundan $2^i \equiv 2^j \,(\mathrm{mod}p) \Rightarrow j-i \equiv m\,(\mathrm{mod}p) \Rightarrow j-i,\ m$ in bir katıdır. 2^k tane devresel kod olduğundan, x^p-1, k tane indirgenemez çarpana sahiptir ve bunlardan bir tanesi $x-1$ dir. Bundan başka her çarpan $< \hat{f}_i(x) >$ minimal idealinin boyutu olan $m.$ dereceye sahip olmalıdır.

Benzer bir teorem, $GF(q)$ üzerinde asal uzunluklu kodlar için sağlanır. Şöyle ki, devresel kodların boyutları ve sayıları cyclotomic kalan sınıflarının büyüklüklerinden ve sayılarından hesaplanabilir.

Eğer $e(x)$ idempotentiyle verilmiş bir devresel kod varsa şüphesiz, dual kodun idempotenti bilinmek istenir.

Teorem 3.3.9: $x^n-1 = g(x)h(x)$ olsun ve C, $g(x)$ üreteç polinomlu ve $e(x)$ üreteç idempotentli bir devresel kod olsun. O zaman $h(x)$ üreteç polinomlu kod $1-e(x)$ üreteç idempotentine sahiptir ve $C^\perp$, $1-e(x^{-1})$ üreteç idempotentine sahiptir.

İspat:

$g(x)$, C nin üreteç polinomu olduğuna göre, $h(x)$ in karşıt polinomu, $C^\perp$ nün üreteç polinomudur. Yani $h^*(x) = x^k h(x^{-1})$, $C^\perp$ in üreteç polinomudur. $1-e(x)$, $h(x)$ in üreteç idempotenti olduğuna göre $1-e(x^{-1})$ de $h^*(x)$ in üreteç idempotentidir. $e(x) \in C$ olduğuna göre ve A_n de $e(x)(1-e(x)) = 0$ olduğundan $1-e(x) \in C^\perp \Rightarrow 1-e(x^{-1}) \in C^\perp$ olur. $F[x]$ de $x^n-1 = g(x)h(x)$ ve $OBEB(g(x),h(x)) = 1$ olduğundan $F[x]$ de

$$1 = a(x)g(x) + b(x)h(x) \qquad (*)$$

olacak şekilde $a(x)$ ve $b(x)$ polinomları vardır. $1-e(x) = b(x)h(x)$ olduğuna göre $(*)$' ı $b(x)h(x)$ ile çarparsak A_n de

$$b(x)h(x) = a(x)g(x)b(x)h(x) + b^2(x)h^2(x) = b^2(x)h^2(x)$$

olur. $c(x) = d(x)h(x)$ olsun. (*) ı $c(x)$ ile çarparsak $F[x]$ de

$$c(x) = a(x)d(x)g(x)h(x) + b(x)c(x)h(x)$$

olur. Buradan A_n de $c(x) = b(x)c(x)h(x)$ olur. Böylece $c(x) = (1 - e(x))c(x)$ elde edilir. Bu da $1 - e(x)$ in $h(x)$ üreteç polinomlu kod için bir birim olduğunu gösterir. Dolayısıyla $1 - e(x^{-1})$ de $C^{\perp}$ için bir birim olur ve $C^{\perp}$ yi üretir.

BÖLÜM 4

4. DEĞİŞMELİ KODLAR

Devresel bir kodun sonlu bir cisim üzerinde bir devresel grubun grup cebrinde bir ideal olarak yorumlanabildiği bilinmektedir. İdealleri daha genel grup cebirlerinde ele almak doğal bir sonuçtur. Grup olarak değişmeli gruplar gözönüne alınabilir.

Öncelikle değişmeli (abelyen) kodları araştırabilmek için gerekli olan temel bilgiler verilmelidir. Cisim olarak binary cismi seçilecektir.

p_i ler birbirinden farklı olmaları gerekmeyen, asallar olmak üzere,

$$G = C_{p_1{}^{s_1}} \mathrm{x} C_{p_2{}^{s_2}} \mathrm{x} ... \mathrm{x} C_{p_k{}^{s_k}}$$

şeklinde devresel gruplar cinsinden, çarpanların sırasından vazgeçildiği takdirde, bir tek şekilde çarpanlara ayrılan n. mertebeden değişmeli grup G olsun. Burada $C_{p_i{}^{s_i}} =< a_i >$, a_i ile üretilen $p_i{}^{s_i}$ mertebeli devresel gruptur. Ayrıca keyfi bir sonlu grup için indirgenemez gösterilişlerin sayısı onun eşlenik sınıflarının sayısına eşit olduğu bilinmektedir. Boyutu 1 olan bütün gösterilişler indirgenemezdir. O halde birimin eşlenik sınıfını $C_1 = \{1\}$ olarak, her $g \in G$ için $p_1(g) = 1$ i birimin gösterilişi ve her G grubunun bir indirgenemez gösterilişi olarak almak uygundur. Değişmeli gruptaki her eleman, kendinin bir eşlenik sınıfının içindedir. n. mertebeden değişmeli grupta n tane eşlenik sınıf olduğundan, indirgenemez gösterilişlerin sayısı n olur. Bu gösterilişlerin hepsinin de, birimin n. kökünü içeren bir cisim üzerinde dereceleri birdir. Sözü edilen cismin karakteristiğinin n i bölmediği kabul edilmektedir.

Şimdi G, n. mertebeden keyfi bir grup olsun ve $\{\mathcal{X}_i, i = 1, ..., s\}$ kompleks sayılar kümesi üzerinde G nin indirgenemez karakterlerinin bir tam kümesi kabul edilsin. O zaman

$$(i) \quad \sum_{i=1}^{s} c_i \overline{\mathcal{X}}_j(C_i)\mathcal{X}_k(C_i) = n\delta_{jk} \qquad ; \qquad c_i = |C_i| \ , \ C_i = i. \text{ eşlenik sınıf}$$

$$(ii) \quad \sum_{i=1}^{s} \overline{\mathcal{X}}_i(C_j)\mathcal{X}_i(C_k) = \frac{n}{c_k}\delta_{jk}$$

ortogonallik bağıntılarına sahip olunur. Ayrıca G nin bir $\mathcal{X}$ karakteri ancak ve ancak $\sum_{i=1}^{s} c_i \overline{\mathcal{X}}(C_i)\mathcal{X}(C_i) = n$ ise indirgenemezdir.

G nin değişmeli olması halinde bir indirgenemez gösteriliş ile bir indirgenemez karakter arasında hiç bir fark yoktur. Özel olarak G nin $\mathcal{X}_i$ ve $\mathcal{X}_j$ indirgenemez gösterilişleri $\mathcal{X}_i\mathcal{X}_j$ gösterilişi ele alınsın. Bu $\mathcal{X}_i\mathcal{X}_j$ gösterilişi

$$(\mathcal{X}_i\mathcal{X}_j)(g) = \mathcal{X}_i(g)\mathcal{X}_j(g)$$

şeklinde tanımlanır. Grubun değişmeli ve boyutunun 1 olmasından dolayı bu bir gösteriliştir ve indirgenemezdir. Sonuç olarak indirgenemez bir karakter olur. Değişmeli bir grubun indirgenemez karakterleri, birimi esas (principal) karakter olan bir değişmeli grup oluşturur. Bu grup G^* ile gösterilsin. Yukarıda elde edilen sonuçlar grubun değişmeli olmaması halinde geçerli değildir.

G^* grubunun G grubuna izomorfik olduğu gösterilirse (ki öyledir), karakterleri tamsayılarla etiketlemek yerine grup elemanlarıyla etiketlemek mümkündür. Eğer G grubunun elemanlarının mertebelerinin en küçük ortak katı m ise o zaman indirgenemez bir karakter G den $GF(2)$ nin bir genişlemesi tarafından kapsanan birimin $m.$ kökleri içine bir homomorfizm olur. G nin dekompozisyonundaki devresel grupların üreteçleri üzerinde $\mathcal{X}_{a_i}$ karakteri ,

$$\mathcal{X}_{a_i}(a_i) = x_i \quad , \quad \mathcal{X}_{a_i}(a_j) = 1 \quad , \quad j \neq i$$

şeklinde tanımlansın. Burada x_i, birimin $p_i^{s_i}$ inci ilkel köküdür. Yukarıdaki indirgenemezlik kriteri uygulandığında bunun gerçekten G nin indirgenemez bir karakteri olduğu görülür. Sadece G^* çarpım grubu ile ilgili olunduğundan karakter denince indirgenemez karakter olduğu düşünülür. Daha açık bir anlatımla, G nin iki indirgenemez karakteri (gösterilişi) $\mathcal{X}_i$ ve $\mathcal{X}_j$ ise $\mathcal{X}_i+\mathcal{X}_j$, $\mathcal{X}_i \oplus \mathcal{X}_j$ dolaysız toplam gösterilişinin karakteri olur. Fakat bu tür karakterlerle ilgili olunmayacaktır.

G^* in keyfi bir elemanı $\mathcal{X}$ ve

$$\mathcal{X}(a_i) = \alpha_i \quad , \quad i = 1, ..., s$$

olsun. a_i nin mertebesi $p_i^{s_i}$ olduğundan

$$\mathcal{X}(a_i)^{p_i^{s_i}} = \mathcal{X}(a_i^{p_i^{s_i}}) = \mathcal{X}(1) = 1 = \alpha_i^{p_i^{s_i}}$$

olur ki buradan birimin $p_i^{s_i}$ inci kökünün α_i olduğu sonucu elde edilir. O zaman uygun bir k_i tamsayısı için

$$\mathcal{X}(a_i) = x_i^{k_i}$$

yazılabilir. Herhangi bir $g \in G$ için

$$g = a_1^{l_1} a_2^{l_2} ... a_s^{l_s}$$

olup

$$\mathcal{X}(g) = \prod_{i=1}^{s} \mathcal{X}(a_i^{l_i}) = \prod_{i=1}^{s} x_i^{k_i l_i} = \prod_{i=1}^{s} \mathcal{X}_{a_i}(a_i^{l_i})^{k_i}$$

yazılır. Buradan G^* daki keyfi bir karakterin $\mathcal{X}_{a_i}, i = 1, ..., s$ "temel" karakterlerinin bir çarpımı olarak yazılabildiği sonucu elde edilir. Buradan

$$f: \quad G \to G^*$$

$$g = a_1^{l_1} a_2^{l_2} ... a_s^{l_s} \to \mathcal{X}_{a_1}^{l_1} \mathcal{X}_{a_2}^{l_2} ... \mathcal{X}_{a_s}^{l_s} = \mathcal{X}_g$$

fonksiyonu akla gelir ki, grup değişmeli olduğundan dolayı G den G^* a bir homomorfizm olur. Tanımdan örtenlik ve 1-1 lik hemen görülmektedir. Şu halde G ile G^* izomorfiktirler. Sonuç olarak G^* ın elemanları G nin elemanları ile etiketlenebilir. Bu

$$\mathcal{X}_g \mathcal{X}_h = \mathcal{X}_{gh}$$

biçiminde yapılır.

Bir gruptaki karakterlerin ortogonalliği kavramı grubun değişmeli olması halinde

$$\sum_{\mathcal{X}_g \in G^*} \mathcal{X}_g(h) = \begin{cases} |G| = n & , \quad h = 1 \text{ ise} \\ 0 & , \quad \text{diğer halde} \end{cases}$$

ve

$$\sum_{h \in G} \mathcal{X}_g(h) = \begin{cases} |G| = n & , \quad g = 1 \text{ ise (yani } \mathcal{X}_1 \text{ esas karakter)} \\ 0 & , \quad \text{diğer halde} \end{cases}$$

haline dönüşür.

G nin elemanları $g_1 = 1, g_2, ..., g_n$ şeklinde sıralansın. O zaman (i, j) elemanı $\mathcal{X}_{g_j}(g_i)$ olan $\wedge$ karakter matrisi tanımlanabilir. Ortogonallik bağıntısından

$$\wedge \wedge^T = nI_n$$

sonucuna varılır ve buradan $\wedge$ singüler değildir.

İlerki çalışma için, bir grup karakteri kavramını cebirdeki bir karaktere aşağıdaki yolla genişletmek uygundur. $\mathcal{X} \in G^*$, G nin bir karakteri olsun, o zaman $\alpha \in GF(2)G$ ve $\alpha = \sum_G \alpha_g g$ olmak üzere $\mathcal{X}(\alpha)$,

$$\mathcal{X}(\alpha) = \mathcal{X}(\sum_G \alpha_g g) = \sum_G \alpha_g \mathcal{X}(g)$$

olarak tanımlanır. G değişmeli kabul edildiğinden, X' nin gerçekten $GF(2)G$ cebrinin bir gösterilişi olduğunu kontrol etmek kolay olur. Böylece

$$\mathcal{X}(\alpha\beta) = \mathcal{X}((\sum_G \alpha_g g)(\sum_G \beta_g g)) = \mathcal{X}(\sum_G \alpha_g g)\mathcal{X}(\sum_G \beta_g g) \quad , \quad \mathcal{X} \in G^*$$

ve özel olarak

$$\mathcal{X}(\alpha^2) = \mathcal{X}^2(\alpha) \quad , \quad \mathcal{X} \in G^* \quad , \quad \alpha \in GF(2)G$$

olur. $\mathcal{X}_{g_i}$, $\mathcal{X}_{g_j} \in G^*$ için

$$\mathcal{X}_{g_i}(g)\mathcal{X}_{g_i}(h) = \mathcal{X}_{g_i}(gh) \quad , \quad g, h \in G$$

ve

$$\mathcal{X}_{g_i}(g)\mathcal{X}_{g_j}(g) = \mathcal{X}_{g_i g_j}(g)$$

olduğu doğrudur. Genel olarak

$$\mathcal{X}_{g_i}(g)\mathcal{X}_{g_j}(h) = \mathcal{X}_{g_i g_j}(gh)$$

olduğu doğru değildir. Böylece farklı iki $\mathcal{X}_{g_i}$, $\mathcal{X}_{g_j} \in G^*$ karakterleri için genel olarak

$$\mathcal{X}_{g_i}(\sum_G \alpha_g g)\mathcal{X}_{g_j}(\sum_G \beta_g g) \neq \mathcal{X}_{g_i g_j}((\sum_G \alpha_g g)(\sum_G \beta_g g))$$

olur.

Değişmeli kodlar için gerekli olduğundan yarıbasit grup cebirleri hakkında bazı temel bilgiler verilmelidir. Cismin karakteri 2 kabul edildiğinden G nin mertebesi, aksi söylenmedikçe, tek sayı (n) kabul edilebilir.

Bu yarıbasit hal için grup cebri,

$$GF(2)G = \bigoplus_{i=1}^{r} M_i$$

şeklinde ifade edilebilir. Burada $i = 1, ..., r$ olmak üzere M_i ler birer (tek) minimal ideallerdir. Dahası

$$1 = e_1 + ... + e_r \quad , \quad e_i e_j = \delta_{ij} e_j$$

ve

$$M_i = GF(2)Ge_i$$

şeklinde karşılıklı olarak (ikişer ikişer) ortogonal e_i, $i = 1, ..., r$ idempotentleri mevcuttur.

Sözkonusu cebri elemanları $\alpha, \beta, ...$ ile gösterilsin.

$$\sigma_i = \sum_{g \in S_i} g \quad , \quad i = 1, ..., r'$$

elemanları $GF(2)G$ de idempotenttirler.

Ön Teorem 4.1: Eğer $\alpha = \sum_G \alpha_g g$ ise o zaman

$$\alpha_g = \frac{1}{n} \sum_{f \in G} \mathcal{X}_f(\alpha) \mathcal{X}_f(g^{-1})$$

olur. Tersine eğer

$$\alpha_g = \frac{1}{n} \sum_{h \in G} \beta_h \mathcal{X}_h(g^{-1})$$

ise o zaman $\mathcal{X}_h(\alpha) = \beta_h$ olur. Böylece h, G de bulunurken $\mathcal{X}_h(\alpha)$ değerlerinin kümesi tek bir α yı belirler.

İspat:

$\alpha = \sum_G \alpha_g g$ olsun ve

$$\begin{aligned} \sum_{h \in G} \mathcal{X}_h(\alpha) \mathcal{X}_h(g^{-1}) &= \sum_{h \in G} \left[\sum_{f \in G} \alpha_f \mathcal{X}_h(f) \right] \mathcal{X}_h(g^{-1}) \\ &= \sum_{f \in G} \alpha_f \left[\sum_{h \in G} \mathcal{X}_h(f) \mathcal{X}_h(g^{-1}) \right] \\ &= \sum_{f \in G} \alpha_f (n \delta_{fg}) = n \alpha_g \end{aligned}$$

toplamı ele alınsın. Tersine

$$\alpha_g = \frac{1}{n}\sum_{h\in G}\beta_h \mathcal{X}_h(g^{-1})$$

olduğu düşünülsün ve istenilen

$$\begin{aligned}\mathcal{X}_h(\alpha) = \sum_{g\in G}\alpha_g\mathcal{X}_h(g) &= \sum_{g\in G}\left[\frac{1}{n}\sum_{f\in G}\beta_f\mathcal{X}_f(g^{-1})\right]\mathcal{X}_h(g)\\ &= \frac{1}{n}\sum_{f\in G}\beta_f\sum_{g\in G}\mathcal{X}_f(g^{-1})\mathcal{X}_h(g)\\ &= \frac{1}{n}\sum_{f\in G}\beta_f\sum_{g\in G}\mathcal{X}_g(f^{-1})\mathcal{X}_g(h)\\ &= \frac{1}{n}\sum_{f\in G}\beta_f(n\delta_{fh}) = \beta_h\end{aligned}$$

ifadesi ele alınsın. Böylece eleman üzerindeki karakterlerin değerleri tek bir elemanı belirler.

Teorem 4.1: G,

$$G = \underbrace{C_{p^{s_1}}\mathrm{x}...\mathrm{x}C_{p^{s_1}}}_{s_1}\mathrm{x}C_{p^{s_2}}\mathrm{x}...\mathrm{x}C_{p^{s_{m-1}}}\mathrm{x}\underbrace{C_{p^{s_m}}\mathrm{x}...\mathrm{x}C_{p^{s_m}}}_{s_m}$$

biçiminde değişmeli bir p-grup olsun ve $KarGF(q) = p$ olmak üzere R, $GF(q)G$ grup cebrinin radikali olsun. O zaman R^j kodunun uzaklığı

$$1 \le j \le s_1(p^{s_1}-1) + ... + s_m(p^{s_m}-1)$$

olmak üzere

$$d(R^j) = \begin{cases} |G| & , \quad j = s_1(p^{s_1}-1) + ... + s_m(p^{s_m}-1) \text{ ise} \\ \mathrm{d(j)} & , \quad 1 \le j < s_1(p^{s_1}-1) + ... + s_m(p^{s_m}-1) \text{ ise} \end{cases}$$

formülüyle verilir.

Özel hal için $G = C_p^m$ iken, grup cebrindeki ideallerin uzaklıkları için verilen formüller bunun içinde kapsanır.

Bu teoremin diğer özel bir hali

$$G = C_p\mathrm{x}C_p\mathrm{x}...\mathrm{x}C_p \quad , \quad (s - defa)$$

iken görülür.

$$j = (p-1)k + r \quad , \quad 0 \leq r < p-1 \quad , \quad 0 \leq k \leq s \quad \text{iken}$$

$$d(R^j) = p^k(r+1) \quad , \quad 1 \leq j \leq (p-1)s$$

olur. $p = 2 = q$ iken bu formül

$$d(R^j) = 2^l \quad , \quad 1 \leq l \leq s$$

şeklini alır. Buradan bu kodların kolaylıkla Reed-Müller kodları olduğu görülür.

SONUÇLAR

Devresel kodların yapısında $x^n - 1$ polinomu bir anahtar işlevi görmektedir. Bu polinomun çarpanlarına uygun bir şekilde ayrılması sayesinde devresel kodlar kurulmaktadır. Ayrıca devresel bir kod bir ideal olarak ele alındığında, en küçük dereceli monik polinom bu idealin üreteci olmaktadır. Devresel kodun dualinin de devresel olduğu görülmektedir. Devresel kodların boyutları ve sayıları, cyclotomic kalan sınıflarının büyüklüklerinden ve sayılarından hesaplanabilmektedir.

Değişmeli kodlar, devresel kodlar bir ideal olarak ele alındığında, bu idealleri daha genel grup cebirlerinde ele almak amacıyla kullanılmaktadır. Cisim binary cisim seçildiğinden karakteristiği 2 dir. Buradan değişmeli kodların kolaylıkla Reed-Müller kodlara dönüşebileceği görülmektedir.

KAYNAKLAR

(1) Blake lan F. and Mullin Ronald C.,1975. The Mathematical Theory of Coding. Academic Press,Inc.,New york,204-244.

(2) Cameron P.J. and Van Lint J.H.,1975. Graph Teheory, Coding Theory and *Block Designs. London Mathematical Society* Lecture Note Series,19. Cambridge University Press.

(3) Cracknell Arthur P.,1968. Selected Readings in Physics "Applied Group Theory" Lecturer in Physics. University of Singapore. Pergamon Press Ltd.

(4) Hamermesh Morton, 1964. Group Theory and Its Application to Physical Problems. Argonne National Laboratory. Addison-Wesley Publishing Company.

(5) Hill Raymond, 1986. A First Course in Coding Theory. Oxford Applied Mathematics and Computing Science Series, Oxford University Press, New York:141-161.

(6) Pless Vera, 1989. Introduction to The Theory of Error-Correcting Codes. University of Hinois at Chicago Circle. A Wiley-Interscience Publication (Second Edition):67-83.

(7) Thomas AD and Wood GV, 1980. Group Tables. University Collage of Swansea Shiva Publishing Ltd.

(8) Van Lint J.H., 1971. Coding Theory. Lecture Notes in Mathematics Vol 201. A Collection of Informal Reports and Seminars. California Institute of Technology, Pasadena:42-59

ÖZGEÇMİŞ

Doğum Tarihi	: 29 Eylül 1971
Doğum Yeri	: Ankara
İlkokul	: 1977-1982 İstanbul Firuzköy İlkokulu
Ortaokul	: 1982-1986 T.E.D. Karabük Koleji Vakfı Özel Lisesi
Lise	: 1986-1989 İzmir Özel Fatih Lisesi
Lisans Eğitimi	: 1989-1994 İstanbul Üniversitesi Fen Edebiyat Fakültesi Matematik Bölümü
Yüksek Lisans	: 1994- Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü Matematik Programı
Görevi	: Özel İstanbul Ar-el Lisesinde Matematik Öğretmenliği yapıyor.