FEN BİLİMLERİ ENSTİTÜLERİ
ORTAK YÜKSEK LİSANS PROGRAMI

YÜKSEK LİSANS TEZİ

Ömer ÖZKAN

BAZI OPTİMAL YARI BURMALI KODLAR

MATEMATİK ANABİLİM DALI

OSMANİYE – 2019

FEN BİLİMLERİ ENSTİTÜSÜ
ORTAK YÜKSEK LİSANS PROGRAMI

BAZI OPTİMAL YARI BURMALI KODLAR

Ömer ÖZKAN

MATEMATİK
ANABİLİM DALI

OSMANİYE
AĞUSTOS-2019

TEZ ONAYI

BAZI OPTİMAL YARI BURMALI KODLAR

Ömer ÖZKAN tarafından Dr. Öğr. Üyesi Basri ÇALIŞKAN danışmanlığında, Osmaniye Korkut Ata Üniversitesi Fen Bilimleri Enstitüsü **Matematik** Anabilim Dalı'nda hazırlanan bu çalışma, aşağıda imzaları bulunan jüri üyeleri tarafından oy birliği/~~çokluğu~~ ile **Yüksek Lisans Tezi** olarak kabul edilmiştir.

Danışman: Dr. Öğr. Üyesi Basri ÇALIŞKAN .....
Matematik Anabilim Dalı, OKÜ

Üye: Dr. Öğr. Üyesi Mehmet ÇİTİL .....
Matematik Anabilim Dalı, KSÜ

Üye: Dr. Öğr. Üyesi Zehra VELİOĞLU .....
Matematik Anabilim Dalı, HRÜ

Yukarıdaki jüri kararı Osmaniye Korkut Ata Üniversitesi Fen Bilimleri Enstitüsü Yönetim Kurulu'nun ...../...../..... tarih ve ...../..... sayılı kararı ile onaylanmıştır.

Doç. Dr. Coşkun ÖZALP .....
Enstitü Müdürü, **Fen Bilimleri Enstitüsü**

Bu Çalışma OKÜ Bilimsel Araştırma Projeleri Birimi Tarafından Desteklenmiştir.

Proje No: OKÜBAP-2019-PT3-006

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, bu çalışma sonucunda elde edilmeyen her türlü bilgi ve ifade için ilgili kaynağa eksiksiz atıf yapıldığını ve bu tezin Osmaniye Korkut Ata Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına uygun olarak hazırlandığını bildiririm.

Ömer ÖZKAN

ÖZET

BAZI OPTİMAL YARI BURMALI KODLAR

Ömer ÖZKAN
Yüksek Lisans, Matematik Anabilim Dalı
Danışman :Dr. Öğr. Üyesi Basri ÇALIŞKAN

Ağustos 2019, 51 sayfa

Bu tezde öncelikle yarı devirli kodların bir genellemesi olan yarı burmalı kodların yapısal özellikleri derlenerek, F_3 ve F_5 sonlu cisimleri üzerindeki bazı yeni yarı burmalı kodlar verilmiştir.

Bunlara ilave olarak, 2-üreteçli iki ağırlıklı yarı burmalı kodların bir ailesinin yeni bir açık inşası derlenmiştir. Bu metot ile elde edilmiş bazı yeni uzunluk optimal ikili yarı devirli ve iyi üçlü yarı devirli kodlar sunulmuştur.

Son olarak, serbest $\mathbb{Z}_2\mathbb{Z}_4\mathbb{Z}_8$-toplamsal kod tanımı yapılmış ve bu kodların sayısını veren bir formül elde edilmiştir.

Anahtar Kelimeler: Lineer kod, devirli kod, yarı devirli kod, yarı burmalı kod, optimal kod

ABSTRACT

SOME OPTIMAL QUASI TWISTED CODES

Ömer ÖZKAN
M.Sc., Department of Mathematics
Supervisor :Assist. Prof. Dr. Basri ÇALIŞKAN

August 2019, 51 pages

In this thesis, firstly it is compiled quasi-twisted codes, which are generalizations of quasi-cyclic codes. Then their structural properties are compiled and given some new codes over the finite fields F_3 and F_5.

In addition, a new explicit construction of a family of 2-generator quasi-twisted two-weight codes is compiled. It is presented some new distance-optimal binary quasi-cyclic codes and some good ternary quasi-cyclic codes obtained by the construction.

Finally, it is defined free $\mathbb{Z}_2\mathbb{Z}_4\mathbb{Z}_8$-additive codes and obtained a formula for the number of these codes.

Key Words: Linear code, cyclic code, quasi cyclic code, quasi twisted code, optimal code

Canım Aileme

TEŞEKKÜR

Yüksek Lisans tez konumun belirlenerek tez çalışmamın yürütülmesini üstlenen, çalışmalarım süresince değerli bilgi ve tecrübelerini katkılarını esirgemeyen danışman hocam Sayın Dr. Öğr. Üyesi Basri ÇALIŞKAN'a teşekkürlerimi sunarım.

Ayrıca manevi desteği ile daima yanımda duran değerli aileme ve çalışmama katkılarından dolayı OKÜ Matematik Bölümü'nün diğer akademik ve idari personellerine teşekkür ederim.

İÇİNDEKİLER

ŞEKİLLER DİZİNİ

SİMGELER VE KISALTMALAR

$\langle a \rangle$	a ile üretilen küme
$A_q(n,d)$	n uzunluklu d uzaklığa sahip kodların maksimum sayısı
BCH	BCH sınırı
$F < K$	K cismi F cisminin genişlemesi
$\|G\|$	G kümesinin eleman sayısı
G/H	G bölüm grubu
$H \times K$	H ile K'nın iç direkt çarpımı
$[K : F]$	F cisminin bir sonlu genişlemesi olan K cismi
$N_{(k_1,k_2,\ldots,k_m)}$	R halkası üzerinde $(k_1,k_2,\ldots,k_m)-$tipinde kodların sayısı
$R[x]$	Katsayıları R'den alınan polinomlar halkası
$\mathbb{Z}$	Tam sayılar kümesi
$\mathbb{Z}_n$	Modülo n'e göre tam sayılar halkası
$[n,k,d]_q$	F_q üzerinde uzunluğu n, boyutu k, uzaklığı d olan bir lineer kod
$\begin{bmatrix} n \\ k \end{bmatrix}$	Gauss binom katsayısı
$\binom{n}{k}$	Binom katsayısı

Alt İndisler

q	q elemanlı sonlu cisim
i	Ağırlığı i olan kodsöz
n	n. kuvvet

Üst İndisler

-1	Elemanın tersi
$*$	İlgili kümenin sıfırdan farklı elemanlarının kümesi

1. GİRİŞ

Teknoloji çağı olan günümüzde haberleşme araçlarının çok fazla önemi vardır. Günümüz teknolojisindeki yeni haberleşme araçlarının büyük bir kısmının çok eski bir geçmişi yoktur. 1870'de telefonun hayatımıza girmesiyle beraber iletişim teknolojisi her geçen gün gelişmiş ve bugünkü halini almıştır. İletişim araçlarının yaygınlaşması, daha kaliteli ve güvenli iletişim ihtiyacını ortaya çıkarmış ve bu ihtiyaca *bilgi ve kodlama teorisi* denilen bilim dalı çözüm aramaya başlamıştır.

Kod, matematik alanında istatistik biliminde, bilgisayar alanında şifreleme konusunda, haberleşme alanında, haberleşme karmaşıklığını en düşük seviyeye indirmek ve kaynakların etkin biçimde temsil edilmesini sağlamak için kullanılmaktadır.

Kodlama, iletişim alanında kaynakların, kanalların, alıcıların bilgi karakteristiklerini incelemek, bilginin iletimini optimize etmek ve iletimin güvenilirliğinin düzeltilmesini sağlamak amacıyla kullanılmaktadır.

Bilgi ve kodlama teorisi ile ilgili ilk çalışmalar 1940'lı yıllarda Hamming, Shannon ve Golay tarafından yapılmıştır. Ancak kodlama teorisi için başlangıç noktası olarak kabul edilen ve bu teorinin temellerinin atıldığı çalışma 1948 yılında Shannon tarafından yayımlanan"*A mathematical theory of communication*" adlı makaledir [1]. Shannon bu makale ile bilgi aktarımının gerçekleştiği bir kanal için kanal kapasitesi denilen bir sayı tanımlamış ve bu kanal kapasitesinin altındaki bir oran için güvenilir bilgi iletişiminin gerçekleştirilebileceğini ispatlamıştır. Shannon'un verdiği bu sonuçlar, bilginin gönderilmeden önce, kanalda değişime uğrayacak bilginin özel bir doğruluk değeriyle dekodlanmasını sağlayacak şekilde, kodlanabilmesini garanti altına almıştır. Bu sonuçlar günümüzde cep telefonlarında, CD'lerde ve bilgi depolama aygıtlarında kullanılmaktadır. Bu konu cebirdeki matematik kavramları kullanılarak geliştirilmiş ve *Cebirsel Kodlama Teorisi* adını almıştır. Golay, Hamming kodlarının gelişimine yardımcı olacak çalışmalar yapmıştır. Aynı zamanda Golay kodlarını ortaya çıkarmıştır [2].

Richard Hamming tarafından verilen ve Hamming kodları olarak bilinen hata düzeltme

kodları en önemli kodlama sistemlerinden birini teşkil eder. Hamming kodları hatayı bulan ve düzelten kodlardır [3].

Gilbert, [4] de, Varshamov, [5] de verilen herhangi uzunlukta ve minimum mesafeli kodların alt sınırları ile ilgili teorilerini öne sürmüşlerdir bunlar Gilbert-Varshamov sınırları olarak da bilinir. Daha sonra lineer kodların önemli bir sınıfı olan devirli kodlar bulunmuştur.

Slepian tarafından lineer kodlar için çözümleme tablosu verilmiştir [6].

Birbirlerinden bağımsız olarak R.C. Bose, D.K. Ray-Chaudhuri ve A. Hocquenhgem tarafından hata düzeltmede, kodlama ve kod çözmede etkin bir özelliğe sahip olan devirli kodların önemli bir ailesi teşkil eden BCH kodları keşfedilmiştir. BCH kodları Hamming kodlarının genelleştirilmesidir. Daha sonraları çoklu kanallar ve çoklu alıcılar için Space-Time kodları geliştirilmiştir [7].

Irving Reed ve Gus Solomon, hata düzeltme kodlarında yeni bir sınıf olan ve günümüzde kompakt disk çalarlardan uzun mesafeli iletişim araçlarına kadar değişik alanlarda kullanılan Reed-Solomon kodlarını keşfetmişlerdir [8].

Nordstrom ve Robinson, Nordstrom-Robinson kodu olarak bilinen nonlineer kodların en iyi temsilcilerinden olan 16 uzunluklu 256 kodsözlü bir kod keşfetmişlerdir [9].

V.D. Goppa, cebirsel geometri kullanarak günümüzde kendi adıyla bilinen Goppa kodlarını keşfetmiştir [10].

Kodlama teorisiyle ilgili cisimler üzerinde yapılan çalışmalar çoğunlukta olsa da 1990'lı yıllarda kodlama teorisiyle ilgili çalışmalar halkalar üzerine aktarılmaya başlanmıştır.

1994 yılında Hammons ve arkadaşları $\mathbb{Z}_4$ halkası üzerinde bir çalışma yaptılar ve bu çalışma sonlu halkalar üzerindeki kodların araştırılması için bir başlangıç oldu [11]. Daha sonra bazı özel halkalar üzerindeki kodlar da çalışılmaya başlanmıştır.

2010 yılında $\mathbb{Z}_2 \times \mathbb{Z}_4$ toplamsal kodlar tanımlanmış ve bu kodların yapısı incelenmiştir.

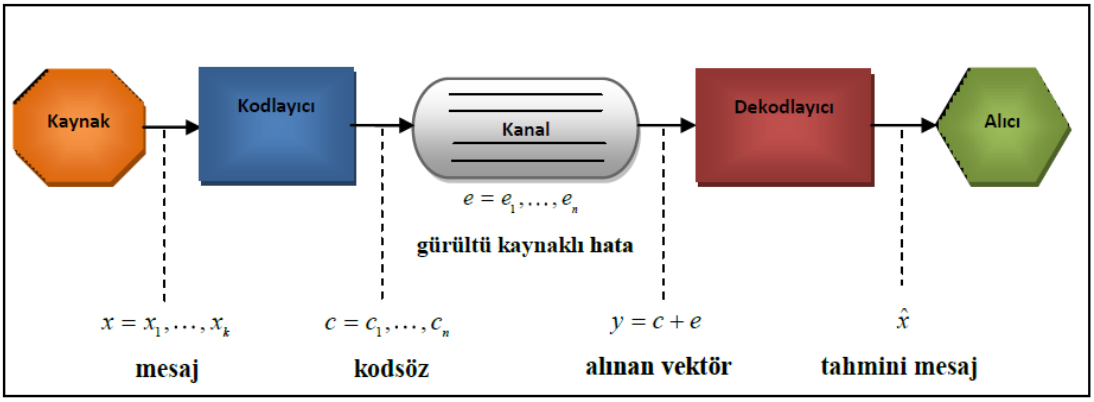
Bu kodlar bünyelerinde hem ikili hem de dörtlü kodları barındırdıklarından kodlama teorisinin ilginç ve araştırmaya açık bir alanı haline gelmiştir.

Kodlama teorisi içinde iletişim için en yaygın olarak kullanılan kodlar ikili kodlardır. n uzunluğunda ikili bir söz $\mathbb{Z}_2$'in bir alt kümesidir. Lineer kodlar, cebirsel yapıları ve lineer olmayan kodlara göre kodlama ve dekodlama işleminin daha kolay yapılabilmesi açısından kodlama teorisinde en çok kullanılan kodlardır.

Kodlama teorisi, bilginin bir kaynaktan diğerine verimli ve doğru bir şekilde aktarılmasını sağlayacak metotları belirleyen çalışma alanıdır. Bilgilerin iletildiği fiziksel ortam *kanal* olarak adlandırılır. Telefon hatları ve atmosfer birer kanal örnekleridir. Bilgiler iletilirken meydana gelebilecek hatalar kaçınılmazdır. Bilgi kanala girdiği anda farklı nedenlerden dolayı, mesela telefon hatlarındaki kablonun küçük bir yerinde kırık olması, bozulmaya ya da kanal kirliliğine maruz kalabilir. Bu yüzden gönderilen bilginin kanalda maruz kaldığı kirlilikten dolayı oluşan hatayı belirlemek ve hatta mümkünse bu hatayı düzeltmek için sistematik bir yöntem kullanılması akıllıca olacaktır. Kodlama teorisinin asıl amacı da budur. Bilgi gönderilmeden önce kodlama denilen ve bilginin sayılara dönüştürüldüğü ve bu dönüşüme cebirsel bir yapı giydirildiği bir yöntemle değiştirilir ve kanaldan çıktıktan sonra da dekodlama denilen bir yöntemle sayılar tekrar bilgi haline dönüştürülür. Genel olarak zor olan kodlama değil dekodlama işlemidir. Çünkü çoğu zaman, bilginin iletimi esnasında arzu edilmeyen durumlarla karşılaşılabilir. Bu durumlar iletilen bilginin bozulmasına neden olabilir ve bu bozukluklar *gürültü* olarak adlandırılır. Kodlama teorisi, bilgi iletimi esnasında kanaldaki gürültü nedeniyle meydana gelen hataları tespit etme ve bu hataları düzeltme problemi üzerinde çalışır. Kodlama teorisinin temel olarak beş amacı vardır. Bunlar,

- Bilginin hızlı kodlanması
- Kodlanmış mesajların kolay taşınması
- Alınan mesajların hızlı dekodlanması
- Kanalda oluşan hataların düzeltilmesi
- Birim zamanda maksimum bilgi transferi.

Bilgi transfer şeması genel olarak aşağıdaki gibi verilir.



Şekil 1.1 Gauss İletişim Şeması

İletişimde amaç, kaynaktan gönderilen mesajı doğruluğu yüksek bir olasılıkla iletmektir. Mesajı göndermek için alfabe olarak adlandırılan sonlu kümeler kullanılır. Bu küme genellikle sonlu bir halka veya cisim olarak alınır. İletilecek mesaj, oluşabilecek hatalardan korunmak üzere şifrelenir. Şifrelenen mesaj, kodun elemanları olan kodsözlerdir. Kodsözler kanala gönderilir. Bazı terimleri değişmiş yani hata olmuş olabilir. Dekoder hata olup olmadığını kontrol eder, hata varsa düzeltir ve orijinal mesaj elde edilip alıcıya gönderilir.

Kod teorinin en temel problemi, n uznunluklu k tane kodsözden oluşan ve minimum uzaklığı d olan bir lineer $[n,k,d]$ kod için n nin en küçük değerini veya d nin en büyük değerini bulmaktır.

Verhoeff [12] çalışmasında, ikili kodlar için bu parametrelerle ilgili geniş bir tablo vermiştir. q ve k verildiğinde d nin yeterince büyük değerleri için Griesmer sınırı [13], n nin minmum değerinin bulunması için bir alt sınır belirler.

1981 yılında, Tilborg, $q = 2$ ve $k \leq 7$ ve d nin tüm değerleri için n yi hesaplamıştır [14].

1990 yılında Ytrehus and Helleseth, $k = 8$ için bazı çalışmalar yapmışlardır [15].

Son yıllarda önemli sayıda optimal kodlar yarı devirli kodlardan oluşmaktadır. Yarı devirli kodların cebirsel yapıları lineer kodlarla kıyaslandığında çok daha basittir. Ayrıca

yarı devirli kodlar devirli kodların önemli bir sınıfının doğal bir genellemesi olduklarından bir çok araştırmacı yarı devirli kodlar üzerine araştırmalar yapmaktadır. Yarı burmalı kodlar, yarı devirli kodların bir genellemesi olduğu için daha fazla iyi ve optimal kodların yarı burmalı olması süpriz olmayacaktır.

Bu tezin ikinci bölümünde, kodlama teorisi ile ilgili temel tanım ve teoremler verilmiştir.

Tezin üçüncü bölümünde, yarı devirli kodların bir genellemesi olan yarı burmalı kodların yapısal özellikleri ele alınmış ve F_3 ve F_5 sonlu cisimleri üzerindeki en iyi bilinen lineer kodların minimum uzaklıklarının daha iyileri olan elde edilmiş yeni yarı burmalı kodlar tasnif edilmiştir. Yarı burmalı kodlar için minimum uzaklık üzerinde bir BCH tipi sınır verilmiştir ve bir yarı burmalı kodun bir yarı devirli koda denk olabilmesi için gerek koşul verilmiştir.

Tezin dördüncü bölümünde, 2-üreteçli iki ağırlıklı yarı burmalı kodların açık bir inşası verilmiştir. Ayrıca bu ailede Griesmer sınırına ulaşan kodlar ve dolayısıyla uzunluk optimal olan kodlar verilmiştir. Bazı yeni uzunluk optimal ikili yarı devirli ve iyi üçlü yarı devirli kodlar bu inşa ile elde edilmiştir.

Tezin beşinci bölümünde, serbest $\mathbb{Z}_2\mathbb{Z}_4\mathbb{Z}_8$-toplamsal kod tanımı yapılmış ve bu kodların sayısını veren bir formül elde edilmiştir.

Tezin son bölümünde ise, bu alanla ilgili bazı açık problemler ve sonuçlardan bahsedilmiştir.

2. TEMEL TANIMLAR ve TEOREMLER

Bu bölümde kodlama teorisi ile ilgili temel tanım ve teoremler verilmiştir. Bu konularla ilgili daha fazla bilgiye [27], [17] ve [18] nolu kaynaklardan ulaşılabilir.

2.1 Cebirsel Tanımlar

Tanım 2.1 G boş olmayan bir küme ve $\cdot$ G üzerinde ikili işlem (çarpma) olsun. Eğer $(G,\cdot)$ ikilisi aşağıdaki koşulları sağlıyorsa, bu ikiliye bir *grup* denir: Her $a,\ b,\ c \in F$ için;

- Kapalılık : $a \cdot b \in G$
- Birleşme özelliği : $(a+b)+c = a+(b+c)$ ve $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ dır.
- Birim eleman : $a.e = e.a = a$ olacak şekilde bir tek $e \in G$ vardır.
- Ters eleman :$a \cdot a^{-1} = a^{-1} \cdot a = 1$ olacak şekilde bir tek $a^{-1} \in G$ vardır.

İlave olarak,

- Değişme özelliği : $a \cdot b = b \cdot a$ oluyorsa G ye *abelyen* veya *değişmeli grup* denir.

Tanım 2.2 Bir R kümesi, $+$ ve $\cdot$ ile gösterelien, sırasıyla toplama ve çarpma ikili işlemleri ile aşağıdaki koşulları sağlıyorsa, $(R,+,\cdot)$ e bir *halka* denir:

- $(R,+)$ bir abelyen gruptur.
- Her $a,\ b,\ c \in R$ için; $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ dır.
- Her $a,\ b,\ c \in R$ için; $a \cdot (b+c) = a \cdot b + a \cdot c$ ve $(a+b)c = ac+bc$. İlave olarak,
- Her $a,\ b,\ c \in R$ için; $a \cdot b = b \cdot a$ oluyorsa, *değişmeli halka* denir.

Tanım 2.3 $(R,+,\cdot)$ bir halka ve $\emptyset \neq I \subseteq R$ olmak üzere eğer;

- Her $a,\ b \in I$ için; $a-b \in I$

- Her $a \in I$ ve $r \in R$ için; $ra \in I$ ve $ar \in I$ oluyorsa, I ya R nin bir *ideali* denir.

Not 2.4 $R/I = \{a+I \,|\, a \in R\}$ olmak üzere $(R/I,+,\cdot)$ bir halkadır. Ayrıca, R değişmeli ise, R/I değişmeli, R birimli ise R/I de birimlidir.

Tanım 2.5 $(R,+,\cdot)$ halkası için $R \setminus \{0\}$ bir abelyen grup oluyorsa buna bir *cisim* denir ve F ile gösterilir. $a \cdot b$ yerine kısaca ab ve $F \setminus \{0\}$ yerine de kısaca F^* yazılır.

2.1.1 Polinom Halkaları

Tanım 2.6 F bir cisim olsun.

$$F[x] = \left\{ \sum_{i=0}^{n} a_i x^i : a_i \in F,\ n \geq 0 \right\} \tag{2.1}$$

kümesine bilinen toplama ve çarpma işlemleriyle F üzerindeki *polinom halkası* denir. $p(x) = \sum_{i=0}^{n} a_i x^i$ polinomu için $a_n = 1$ ise o zaman $p(x)$ polinomuna bir *monik polinom* denir. Pozitif dereceli bir $p(x) \in F[x]$ polinomu için $p(x) = f(x)g(x)$ olacak sekilde dereceleri $p(x)$'in derecesinden küçük sabit olmayan $f(x),\ g(x) \in F[x]$ polinomları bulunabiliyor ise $p(x)$ polinomuna F üzerinde *indirgenebilir polinom* adı verilir. (Aksi halde $p(x)$ polinomuna F üzerinde *indirgenemez polinom* denir.)

2.1.2 Sonlu Cisimler

Bu bölümde katsayıları sonlu bir cisimden alınmış polinomların yapıları, sonlu bir cismin elemanının minimal polinomunun nasıl bulunacağı ve $x^n - 1$ polinomunun nasıl parçalanacağı incelenecektir.

Tanım 2.7 $(V,+)$ bir abelyen grup, F bir cisim ve $F \times V \to V$ dönüşümü aşağıdaki gibi tanımlansın;

- Her $a \in V$ için; $1a = a$

- Her $\alpha,\ \beta \in F$ ve $a \in V$ için; $\alpha(\beta a) = (\alpha\beta)a$
- Her $\alpha \in F$ ve $a,\ b \in V$ için; $\alpha(a+b) = \alpha a + \alpha b$
- Her $\alpha,\ \beta \in F$ ve $a \in V$ için; $(\alpha+\beta)a = \alpha a + \beta a$

Bu durumda, $(V,+,\cdot,F)$ ye F üzerinde bir *vektör uzayı* denir.

Tanım 2.8 K ve F birer cisim olsun. Eğer $F \subseteq K$ ise K cismine F cisminin bir *genişlemesidir* denir ve $F < K$ ile gösterilir. Aynı zamanda K, F üzerinde bir vektör uzayıdır. K nın F üzerinde boyutu sonlu ise bu boyut $[K : F]$ ile gösterilir ve K ya F nin bir *sonlu genişlemesidir* denir.

Teorem 2.9 (*Kronecker*) F bir cisim ve $f(x)$ sabit olmayan bir polinom olsun $(f(x) \in F[x])$. Buna göre F nin $\alpha \in K$ ve $f(\alpha) = 0$ olacak şekilde bir K cisim genişlemesi vardır.

Yukarıdaki teorem katsayıları cisimden alınmış bir polinomun kökünü içeren daha büyük bir cismin varlığını göstermektedir.

Teorem 2.10 F sonlu bir cisim ise F nin karakteristiği bir asal sayıdır. Eğer F nin karakteristiği p ise n pozitif bir tamsayısı olmak üzere F nin p^n tane elemanı vardır.

Bir sonlu cisme aynı zamanda *Galois cismi* denir ve $q = p^n$ elemanlı bir Galois cismi $GF(p^n)$ veya F_q ile gösterilir.

2.1.3 Sonlu Cisimlerin Karakterizasyonu

Cisim tanımından, F^* çarpma işlemine göre bir gruptur. $|F| = q$ ise $|F^*| = q-1$ dir. Ayrıca F^* bir grup olduğundan,

$$\alpha \in F^* \Rightarrow \alpha^{q-1} = 1$$

ya da

$$\alpha \in F \Rightarrow \alpha^q = \alpha.$$

Diğer bir değişle $\alpha \in F$ cisminin her elemanı $f_q(x) = x^q - x$ polinomunun bir köküdür. Bu polinomun en fazla q tane kökü vardır. Aynı zamanda F cismi $f_q(x) = x^q - x$ *polinomunun parçalanış cismidir*.

Teorem 2.11 $|F| = q$ ise F cismi $f_q(x) = x^q - x$ polinomunun köklerinden oluşur ve aynı zamanda bu polinomun *parçalanış cismidir*.

2.1.4 Sonlu Cismin Çarpımsal Yapısı

Tanım 2.12 F cisminin sıfırdan farklı elemanlarının kümesi F^* devirli grubunu doğuran herhangi bir elemanına F_q nun bir *ilkel elemanı* denir.

Tanım 2.13 Bir $\alpha \in F_q^*$ için $\alpha^k = 1$ olacak şekildeki en küçük k pozitif tamsayısına α nın mertebesi denir ve $m(\alpha)$ ile gösterilir.

Önerme 2.14
1. F_q cisminin sıfırdan farklı bir elemanının ilkel olması için gerek ve yeter koşul bu elemanın mertebesinin $q-1$ olmasıdır.
2. Her sonlu cisim en az bir ilkel eleman içerir.

2.1.5 Sonlu Bir Cismin Elemanlarının Temsili

Sonlu bir cismi temsil etmede iki yol kullanılır. Bunlardan birincisinde $p(x)$ indirgenemez polinom olmak üzere $F[x]/p(x)$ bölüm halkası kullanılır. Bu toplama işleminde kolaylık sağlar. İkincisi ise F_q^* ın devirli grup olması nedeniyle, F_q nun tüm elemanlarını bir ilkel elemanın kuvveti şeklinde ifade edilmesidir. Bu yöntem ise çarpmada kolaylık sağlar. $p(x)$, $F_q[x]$ üzerinde bir indirgenemeyen polinom olduğunda

$$K = F_q[x]/\langle p(x)\rangle$$

bölüm halkası bir cisimdir. K nın $F_q[x]$ üzerindeki derecesi d olup, $K = F_{q^d}$ dir. F_{q^d} cismi çarpma ve toplama işleminin modülo $p(x)$ e göre yapıldığı polinomlar kümesi ile temsil edilebilir.

$$F_{q^d} = \frac{F_q[x]}{\langle p(x)\rangle} = \{r(x) + \langle p(x)\rangle \mid der(r(x)) < d\}.$$

α, $p(x)$ polinomunun parçalanış cismindeki bir kökü ise, F_{q^d} yi derecesi d den küçük olan ve çarpma ile toplama işlemleri modülo $p(\alpha)$ ile yapılan α değişkenli polinomlar olarak alınabilir. Bunun sebebi ise, $F(\alpha)$ cismi ile $F_{q^d} = \frac{F[x]}{\langle p(x) \rangle}$ cisminin izomorfik olmasıdır.

2.1.6 Minimal Polinomlar

Tanım 2.15 $\alpha \in F_{q^m}$ olsun. $P(\alpha) = 0$ olacak şekildeki en küçük dereceli bir monik $P(x) \in F_q[x]$ polinomuna α elemanının $F_q[x]$ üzerinde bir *minimal polinomu* denir.

Teorem 2.16

1. $\alpha \in F_{q^m}$ elemanının F_q üzerinde $P(x)$ gibi bir minimal polinomu varsa, $f(\alpha) = 0$ olacak şekildeki her $f(x) \in F_q[x]$ için $P(x) \mid f(x)$ dir.
2. F_{q^m}'in her elemanının F_q üzerinde bir minimal polinomu vardır ve tektir. Bu polinom ayrıca F_q üzerinde indirgenemezdir.
3. Eğer bir $M(x) \in F_q[x]$ monik indirgenemez polinomunun bir kökü $\alpha \in F_{q^m}$ ise bu durumda $M(x)$ polinomu α'nın F_q üzerindeki minimal polinomudur.

Bir $\alpha \in F_{q^m}$ ilkel elemanının minimal polinomunu biliniyorsa bu takdirde herhangi bir i için α^i elemanının da minimal polinomunu bulunabilir.

Tanım 2.17 n ile q aralarında asal olsun.

$$cl_i = \left\{ \left(i \cdot q^j \pmod{n} \right) \mid j = 0, 1, 2, \ldots \right\}$$

ile tanımlanan kümeye q nun n modülüne göre i yi içeren dairesel koseti (cyclo- tomic coset) adıverilir. Eğer $C_{i_1}, \ldots, C_{i_t}$ kümeleri birbirinden farklı ve

$$\bigcup_{j=1}^{t} cl_{i_j} = \mathbb{Z}_n$$

ise $\{i_1, \ldots, i_t\}$ kümesine q nun n modülüne göre dairesel kosetlerinin bir *tam temsilci kümesi* denir.

Teorem 2.18 $\alpha \in F_{q^m}$ bir ilkel eleman ve C_i, q nun $q^m - 1$ modülüne göre i yi içeren dairesel koseti olsun. Buna göre α^i elemanının F_q üzerindeki minimal polinomu

$$M^i(x) = \prod_{j \in cl_i} (x - \alpha^j)$$

polinomudur.

Örnek 2.19 α, $x^2 + x + 2 \in F_3[x]$ polinomunun bir kökü olsun. Buna göre α ve α^3 elemanlarının minimal polinomları $x^2 + x + 2$ polinomudur. α^2 elemanının minimal polinomu ise $x^2 + 1$ olarak bulunur. 3 ün mod 8 e göre dairesel kosetleri $cl_1 = \{1,3\} = cl_3$, $cl_2 = \{2,6\} = cl_6$, $cl_4 = \{4\}$ ve $cl_5 = \{5,7\} = cl_7$ olarak bulunur. Buna göre α^2 elemanının F_3 üzerindeki minimal polinomu

$$M^2(x) = (x - \alpha^2)(x - \alpha^6) = x^2 - (\alpha^2 + \alpha^6)x + 1$$

olur. Burada

$$\begin{aligned} \alpha^2 + \alpha^6 &= (2\alpha + 1) + (2\alpha + 1)^3 \\ &= 2\alpha + 1 + 2\alpha^3 + 1 \\ &= 2\alpha + 2 + \alpha^2 + 2\alpha \\ &= \alpha^2 + \alpha + 2 \\ &= 0. \end{aligned}$$

olacacağınndan $M^2(x) = x^2 + 1$ elde edilir. Benzer şekilde α^5 elemanının minimal polinomunun $x^2 + 2x + 2$ olduğunu görülebilir.

2.2 Lineer Kodlar

Tanım 2.20 $F = \{\lambda_1, \lambda_2, \cdots, \lambda_n\}$ ayrık n tane elemandan oluşan sonlu bir küme olsun. F_q ya bir *alfabe* denir. F_q^n ise F_q kümesinden alınan n-lileri temsil etsin, bu durumda F_q^n kümesinin elemanlarına kısaca *sözler* denir. F_q^n nin herhangi bir C alt kümesine *q-lu blok kodu* denir. C nin sözlerine *kodsöz* denir. Eğer $C \subseteq F_q^n$ nin M tane elemanı varsa, C ye n uzunluğunda, M kodsözler (vektörler) elemanlı bir *kod* denir ve C ye kısaca bir $[n, M]$-kodu denir.

Genelikle $F_q = \mathbb{Z}_q = \{0,1,2,\cdots,q-1\}$ olarak alınır. Özel olarak $F_2 = \mathbb{Z}_2 = \{0,1\}$ alınırsa 0 ve 1 lerin oluşturduğu kodsözlerden oluşan bir kümeye de *ikili (binary) kod* denir.

Örnek 2.21 $C = \{00000, 11111\}$ kümesi bir kod, 00000 ve 11111 ifadeleri birer kodsözdur.

Örnek 2.22 10 haneli cep telefon numaraları 10 uzunluklu 10-lu bir koddur.

Not 2.23 p bir asalsayı ve h da bir pozitif tam sayı olmak üzere, eğer $q = p^h$ oluyorsa F_q bir sonlu cisim olarak alınır.

Gösterim 2.24 Bir C kodu, n uzunluklu M tane kodsözlerden oluşuyorsa bu kod satırları kodsözler olan $M \times n$ şeklinde bir matris gibi yazılır.

Örnek 2.25 Uzunluğu 3 olan ikili tekrarlama kodu,

$$\begin{pmatrix} 000 \\ 111 \end{pmatrix}$$

yani (2×3) matris şeklinde gösterilir.

Tanım 2.26 $x, y \in F_q^n$ olsun. x ve y vektörlerin *Hamming uzaklığı*, x ve y nin farklı bileşenlerinin sayısı olarak tanımlanır ve $d(x,y)$ ile gösterilir. Eğer $x = (x_1, x_2, \ldots, x_n)$ ve $y = (y_1, y_2, \ldots, x_n)$ ise,

$$d(x,y) = |\{i | x_i \neq y_i\}|$$

olarak tanımlanır. Bir C kodunun *minimum uzaklığı* $d(C)$ ile gösterilir ve ayrık kodsözlerın arasındaki uzaklıkların en küçüğü olarak tanımlanır,

$$d(C) = min\{d(x,y) | x, y \in C, x \neq y\}.$$

n uzunluğunda M elemana sahip ve minimum uzaklığı d olan bir kod kısaca $[n, M, d]$-kodu olarak gösterilir.

Örnek 2.27 F_2^5 de $d(00111, 11001) = 4$, F_3^4 de $d(0122, 1220) = 3$ tür.

Tanım 2.28 Hamming uzaklığı F_q^n de bir uzaklık fonksiyonu olarak tanımlanır ve aşağıdaki özellikleri sağlar; her $x, y, z \in F_q^n$ ise,

1. $d(x,y) \geq 0$ ve $d(x,y) = 0 \Leftrightarrow x = y$ (Pozitif tanımlı),

2. $d(x,y) = d(y,x)$ (Simetri),

3. $d(x,y) = d(x,z) + (z,y)$ (Üçgen eşitsizliği).

$\left(F_q^n, d\right)$ bir *metrik uzaydır*.

$V(n,q) = F_q^n$, uzunlukları n olan vektörlerden oluşan n boyutlu bir vektör uzayı olsun.

Tanım 2.29 $V(n,q)$ vektör uzayının bir alt uzayına *lineer kod* denir. Eğer C nin boyutu k ise C ye $[n,k]$-kod denir ya da C nin minimum uzaklığı d ise C ye $[n,k,d]$-kodu denir.

Not 2.30
1. Bir q lu $[n,k,d]$-kodu aynı zamanda q-lu (n,q^k,d)-kodudur ama her (n,q^k,d)-kodu bir $[n,k,d]$-kodu olmayabilir.

2. **0** vektörü lineer kodun elemanıdır.

Teorem 2.31 C bir $[n,k,d]$-kodu olsun. $d = 2t+1$ ya da $d = 2t+2$ olacak şekilde bir $t \in \mathbb{Z}^+$ vardır. C koduna t hata düzelten bir kod denir. Ayrıca, $d \geq s+1$ ise C koduna $s \in \mathbb{Z}^+$ hatayı tespit eden bir kod denir.

Tanım 2.32 $x \in V(n,q)$ olsun x vektörunun *(Hamming) ağırlığı* $w(x)$ ile gösterilir ve x in sıfırdan farklı bileşenlerinin sayısı olarak tanımlanır. Bir C kodunun minimum ağırlığı $w(C)$, o kodun sıfırdan farklı vektörlerin ağırlıklarının en küçüğüdür.

Lineer kodların önemli bir özelliği ise $d(C) = w(C)$ olmasıdır. Yani lineer bir kodun minimum uzaklığı minimum ağırlığa eşittir. Genel olarak, M tane kodsözden oluşan bir genel kod için minimum uzaklığı bulmak için

$$\binom{M}{2} = \frac{1}{2}M(M-1) \tag{2.2}$$

tane Hamming uzaklığının hesap edilmesi gerekmektedir. Ancak kod bir lineer kod ise sadece $M-1$ tane sıfırdan farklı kodsözun ağırlığının bulunması gereklidir.

n uzunluğundaki bir kodun bütün önemli bilgileri (parametrelerini) taşıyan kodun ağırlık sayacı olarak tanımlanan n. dereceden homojen polinom aşağıdaki gibi tanımlanır.

Tanım 2.33 C, n uzunluğunda bir kod olsun. C kodunda ağırlığı i olan kodsözlerin sayısı A_i olsun. $A_i = |\{c|w(c) = i,\ c \in C\}|$.

$$W_C(x,y) = \sum_{c \in C} x^{n-w(c)} y^{w(c)} = \sum_{i=1}^{n} A_i x^{n-i} y^i \tag{2.3}$$

polinomuna C kodun *Hamming ağırlık sayacı* denir.

Ağırlık sayacında y nin en küçük pozitif kuvveti kodun minimum uzaklığını, homojenlik derecesi kodun uzunluğunu ve katsayılarının toplamı kodsözlerin sayısını vermektedir.

2.2.1 Lineer Kodun Üreteç Matrisi

Lineer kodlar bir alt vektör uzayı olduklarından bazları (tabanlar) vasıtasıyla temsil edilebilir. Baz vektörlerini, bir matrisin satırları olarak göstermekle bir vektör uzayı temsil edilmiş olur.

Tanım 2.34 C bir $[n,k]$-kod olsun. k tane satırı bu lineer kodun bir bazı olan $k \times n$ şeklindeki G matrisine lineer kodun *üreteç matrisi* denir. Eğer G matrisi C nin üreteç matrisi ise C nin kodsözleri, G nin satırlarının lineer kombinasyonundan oluşur. Yani,

$$C = \{xG \mid x \in V(k,q)\}.$$

Örnek 2.35 $C_2 = \{000, 011, 101, 110\}$, $[3,2,2]$ kodun üreteç matrisi

$$G = \begin{bmatrix} 011 \\ 101 \end{bmatrix}$$

dir.

Teorem 2.36 C, bir $[n,k]$-kod, G de $[n,k]$ kodunun bir üreteç matrisi olsun. I_k, $k \times k$ birim matris, A da $k \times (n-k)$ tipinde bir matris olmak üzere bazı elemanter satır ve sütün işlemeleri ile G matrisi

$$G_S = [I_k \,|A]$$

şeklinde *standart forma* dönüştürülebilir.

Örnek 2.37 F_3 üzerinde $[6,3]$ kodunun üreteç matrisi,

$$G = \begin{bmatrix} 000111 \\ 011112 \\ 102211 \end{bmatrix}$$

olup, standart formu

$$G_S = \left[\begin{array}{c|c} 100 & 011 \\ 010 & 112 \\ 001 & 211 \end{array}\right]$$

dır.

Tanım 2.38 p bir asal sayı ve m bir pozitif tamsayı olmak üzere, F_q, $q = p^m$ tane elemana sahip sonlu bir cisim ve C, F_q üzerinde n uzunluklu bir lineer kod olsun. $\lambda \in F_q \setminus \{0\}$ ve l bir tamsayı olmak üzere, eğer her $(c_0, c_1, \ldots, c_{n-1}) \in C$ kodsözü için $(\lambda c_{n-l}, \lambda c_{n-l+1} \ldots, \lambda c_{n-1}, c_0, c_1, \ldots, c_{n-l-1}) \in C$ oluyorsa, C ye bir (λ, l) *yarı burmalı (quasi twisted) kod* denir. Eğer, $\lambda = l = 1$ ise, C ye bir *devirli (cyclic) kod*, $l = 1$ ise, C ye bir λ *sabit devirli (consta cyclic) kod* ve $\lambda = 1$ ise, C ye bir l *yarı devirli (quasi cyclic) kod* denir.

2.2.2 Lineer Kodlar İçin Bazı Sınırlar

Bu bölümde uzunluğu ve mininmum uzaklığı verilen kodlar için mümkün olan maksimum sayıdaki kodsözlerin sayısı için bazı sınırlardan bahsedilecektir.

Tanım 2.39 $(n, M, d)_q$, n uzunluklu, M tane kodsözden oluşan ve minimum uzaklığı d olan F_q üzerinde bir kod olmak üzere,

$$A_q(n,d) = mak\left\{M \mid (n,M,d)_q \text{ bir kod}\right\}$$

olsun. Eğer $|C| = A_q(n,d)$ oluyorsa, C koduna bir *optimal kod* denir.

2.2.3 Küre Paket (Hamming) Sınırı

Herhangi bir $u \in F_q^n$ vektörü ve herhangi bir $r \geq 0$ tam sayısı için, u merkezli yarıçapı r olan bir küre

$$S(u,r) = \left\{ v \in F_q^n \mid d(u,v) \leq r \right\}$$

şeklinde gösterilir.

Lemma 2.40 F_q^n de yarıcapı r olan bir küre $(0 \leq r \leq n)$

$$\binom{n}{0} + \binom{n}{1}(q-1) + \binom{n}{2}(q-2)^2 + \cdots + \binom{n}{r}(q-1)^r$$

tane vektör verir.

Teorem 2.41 Bir $(n, M, 2t+1)_q$ kodu

$$M\left\{ \binom{n}{0} + \binom{n}{1}(q-1) + \cdots + \binom{n}{t}(q-1)^t \right\} \leq q^n$$

eşitliğini sağlar.

Tanım 2.42 Eğer bir kod, küre-paket sınırına ulaşıyorsa bu koda *mükemmel (perfect) kod* denir.

Örnek 2.43 1. Uzunluğu n olan tekrarlama kodu, n tek olmak üzere;

$$C = \begin{cases} 000\cdots0 \\ 111\cdots1 \end{cases}$$

$(n,2,n)-$kodu bir mükemmel koddur.

2. F_q^n tüm kodsözlerinden oluşan kod bir mükemmel koddur.

2.2.4 Griesmer Sınırı

J.H. Griesmer [13] deki çalışmasında k boyutlu minimum uzaklığı d olan bir $[k,d]_q$-lineer kod için kodsöz uzunluğu n nin minimum uzunluğu için bir alt sınır belirlemiştir.

Tanım 2.44 $N(k,d)$, bir $[k,d]$-lineer kod için minimum kodsöz uzunluğu olsun. Bu durumda

$$N(k,d) \geq \sum_{i=0}^{k-1} \left\lfloor \frac{d+2^i-1}{2^i} \right\rfloor \tag{2.4}$$

şeklinde tanımlanır. Burada, $\left\lfloor \frac{d+2^i-1}{2^i} \right\rfloor$ değeri, $\left(\frac{d+2^i-1}{2^i}\right)$ değerine eşit ya da daha küçük olan en büyük tamsayısı göstermektedir ve ayrıca $N(1,d) = d$ dir.

Örnek 2.45

$$\begin{aligned} N(5,7) &\geq \left\lfloor \frac{7+2^0-1}{2^0} \right\rfloor + \left\lfloor \frac{7+2^1-1}{2^1} \right\rfloor + \left\lfloor \frac{7+2^2-1}{2^2} \right\rfloor + \left\lfloor \frac{7+2^3-1}{2^3} \right\rfloor + \left\lfloor \frac{7+2^4-1}{2^4} \right\rfloor \\ &\geq 7+4+2+1+1 \\ &\geq 15. \end{aligned}$$

2.2.5 BCH Sınırı

Lineer kodlarda kodun minimum uzaklığının hesaplanmasında tek tek hesap yapılmadığı sürece herhangi bir bilgiye ulaşmak çok zor ya da imkansızdır. Ancak aşağıdaki teorem, devirli bir kodun üreteç polinomunun sıfırlarını inceleyerek minimum uzaklığın büyüklüğü hakında bir alt sınır elde etmeye olanak tanımaktadır.

Teorem 2.46 w, F_q üzerinde birimin n. bir kökü olsun. C bir devirli kod olmak üzere, bu kodun üreteç polinomu $g(x)$, F_q üzerinde en küçük dereceli monik polinom olsun. $b \geq 0$ olmak üzere, ardışık $\delta - 1$ sayıdaki

$$w, w^{b+1}, \ldots, w^{b+\delta-2}$$

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

İspat: İspat için [18] e bakınız.

3. 1-ÜRETEÇLİ YARI BURMALI KODLARIN YAPISI

3.1 Sabit Devirli Kodlar

Bu bölümde [19] daki makaleden yararlanılmıştır.

Sabit devirli kodlar, devirli kodlarınkine benzer cebirsel özeliklere sahiptir [20, 21, 22]. Örneğin; sabit devirli kodlar, üreteç polinomlarının kökleri aracılığıyla belirlenebilirler. Devirli kodlar için $x^n - 1$'in çarpanlara ayrılması çok önemlidir. Benzer şekilde $x^n - a$'nın F_q üzerinde çarpanlarına ayrılması da sabit devirli kodlar için çok önemlidir. Bu kısımda öncelikle sabit devirli kodların devirli kodlara denk olduğu gösterilmiştir.

Tanım 3.1 [17] C_1 ve C_2, F_q üzerinde n uzunluklu kodlar olsunlar. Eğer F_q nun $\pi_0, \pi_1, \ldots, \pi_{n-1}$ şeklinde n tane permütasyonu varsa ve

$$(c_0, c_1, \ldots, c_{n-1}) \in C_1 \text{ iken } \sigma(\pi_0(c_0), \ldots, \pi_{n-1}(c_{n-1})) \in C_2$$

olacak şekilde n kordinat pozisyonlarının bir σ permütasyonu bulunuyorsa C_1 ve C_2 ye *denk kodlar* denir. Eğer tüm π_i ler birim permütasyonlarsa C_1 ve C_2 ye *permütasyon denk*, eğer her bir π_i sıfırdan farklı bir skalerin çarpımı ise C_1 ve C_2 ye *monomial denk* denir.

Teorem 3.2 C, F_q üzerinde n uzunluklu ve $g(x) \mid x^n - a$ polinomu tarafından üretilen bir sabit devirli kod olsun. δ, $a \in F_q$ nun n. kökü olmak üzere, $K = F_q[\delta]$ (F_q ve δ yı içeren en küçük cisim) üzerinde aynı polinom tarafından üretilen sabit devirli kod C_δ, K üzerinde aynı uzunluktaki bir devirli koda denktir.

İspat: $i : F_q \hookrightarrow K$ içerme dönüşümü ile F_q cismi F_q nun bir cisim genişlemesi olan $K = F_q[\delta]$ nın içine gömülebilir. C nin görüntüsü $i(C)$, $\frac{K[x]}{\langle x^n - a \rangle}$ da bir ideal olmak zorunda değildir, fakat $g(x) \in \frac{K[x]}{\langle x^n - a \rangle}$ tarafından üretilen C_δ ideali tarafından içerilir. Herhangi bir $p(x) \in K[x]$ polinomu için, $\overline{p(x)}, p(x)$ in $\frac{K[x]}{\langle x^n - a \rangle}$ de mod$(x^n - 1)$ e göre kalan sınıfı olmak üzere

$$\psi : K[x] \longrightarrow \frac{K[x]}{\langle x^n - a \rangle}$$

dönüşümü, $\psi(p(x)) = \overline{p(x\delta)}$ olarak tanımlanırsa, ψ bir halka homomorfizmi olup, herhangi bir $\overline{p(x)} \in \frac{K[x]}{\langle x^n-1\rangle}$ için $p\left(x\delta^{-1}\right) \in K[x]$ olduğundan ψ örtendir. Bu yüzden

$$\left|\frac{K[x]}{Ker\psi}\right| = \left|\frac{K[x]}{\langle x^n-1\rangle}\right|$$

dir. $\psi(x^n-a) = \overline{(\delta x)^n - a} = \overline{a(x^n-1)} = \overline{0}$ olduğundan, x^n-a bu homomorfizmin çekirdeği $(Ker(\psi))$ nın içindedir. Ama $Ker(\psi)$ bir idealidir, dolaysıyla

$$\langle x^n-a\rangle \subseteq Ker(\psi)$$

dir. Bu yüzünden

$$\left|\frac{K[x]}{Ker\psi}\right| \leq \left|\frac{K[x]}{\langle x^n-a\rangle}\right|$$

dir. Ayrıca

$$\left|\frac{K[x]}{\langle x^n-1\rangle}\right| = \left|\frac{K[x]}{\langle x^n-a\rangle}\right|$$

dır. Bunun için aşağıdaki eşitsizlik elde edilir

$$\left|\frac{K[x]}{\langle x^n-1\rangle}\right| = \left|\frac{K[x]}{Ker\psi}\right| \leq \left|\frac{K[x]}{\langle x^n-a\rangle}\right| = \left|\frac{K[x]}{\langle x^n-1\rangle}\right|$$

Bu da

$$\left|\frac{K[x]}{Ker\psi}\right| = \left|\frac{K[x]}{\langle x^n-1\rangle}\right|.$$

olmasını gerektirir. $\langle x^n-a\rangle \subseteq Ker\psi$ olması ile birlikte $Ker\psi = \langle x^n-a\rangle$ sonucu elde edilir. Sonuç olarak $\frac{K[x]}{\langle x^n-a\rangle}$ ile $\frac{K[x]}{\langle x^n-1\rangle}$ halkaları izomorfiktir. Dolaysıyla, verilen ψ ile bu halkaların idealleri bire bir karşılık gelir. Bu ise Tanım 3.1 de K nın $\pi_i(\alpha) = \delta^i\alpha, \alpha \in K$ permütasyonların ve δ birim permütasyonu ile verilen denklik ile verilir ve bu bir monomial denkliktir (aynı ağırlık sayacına ve minmum uzaklığa sahiptirler).

Not 3.3 Sonuç olarak bölüm halkaları arasında aşağıdaki gibi bir bağıntı vardır,

$$\frac{F_q[x]}{\langle x^n-a\rangle} \hookrightarrow \frac{K[x]}{\langle x^n-a\rangle} \cong \frac{K[x]}{\langle x^n-1\rangle}$$

Not 3.4 Teorem 3.2 deki C kodu gerçekte C_δ nın F_q ya kısıtlanışı olan alt cismi-alt kodudur.

Sonuç 3.5 F_q, a nın bir $n.$ kökü δ yı içerdiğinde, F_q üzerindeki n uzunluklu bir sabit devirli kod, F_q üzerinde n uzunluklu bir devirli koda denktir.

Aşağıdaki lemma bir $a \in F_q$ nın F_q da ne zaman bir $n.$ köke sahip olabileceğini söylemektedir.

Lemma 3.6 α, F_q cisminin bir ilkel elemanı olmak üzere $a = \alpha^i$ olsun. Bu durumda $x^n = a$ denkleminin F_q da bir çözümünün olabilmesi için gerek ve yeter koşul n ile $q-1$ in en büyük ortak böleni $(n, q-1)$ olmak üzere $(n, q-1) \,|i$ olmasıdır [23].

3.2 $x^n - a$ nın Çarpanları ve Bir BCH Sınırı

Bu bölümle ilgili daha detaylı bilgiye [20] den ulaşılabilir.

$a \in F_q^*$ elemanı, $n.$ kökü F_q da olmayan bir eleman olsun. $x^n - a$ nın katlı köke sahip olmaması için $(n, q) = 1$ olduğu kabul edilir. $\delta^n = a$ ve ζ birimin $n.$ ilkel olmak üzere $x^n - a$ nın kökleri $\delta, \delta\zeta, \delta\zeta^2, \ldots, \delta\zeta^{n-2}$ ve $\delta\zeta^{n-1}$ dir. Bu durumda $m = ord_n(q)$ (q nun mod n ye göre çarpımsal mertebesi) olmak üzere ζ, F_{q^m} dedir. $\delta^n = a$ olduğunda $r = \frac{q-1}{(i,q-1)}$, a nın F_q^* çarpımsal gurubundaki derecesi, $a = \zeta^i$ ve ζ, F_q nun bir ilkel elemanı olmak üzere $\delta^{nr} = a^r = 1$ elde edilir. Dolaysıyla δ, birimin $nr.$ köküdür. Bu yüzden, $s = ord_{nr}(q)$ olmak üzere $\delta \in F_{q^s}$ dir. Buradan $q^s - 1 \equiv 0 \,(\mathrm{mod}\, nr)$ olup $q^s - 1 \equiv 0 \,(\mathrm{mod}\, n)$ elde edilir. Bu ise $\frac{m}{s}$ olmasını gerektirir. Sonuç olarak $F_{q^m} \subseteq F_{q^s}$ olur. Dolaysıyla F_{q^s} cismi hem ζ hem de δ yı içeren ve w, F_{q^s} nin bir ilkel elemanı (bu yüzden birimin bir $(q^s - q)$ köküdür) ve en az bir t tamsayısı için $q^s - q = ntr$ olmak üzere $\delta = w^t$ ve $\zeta = w^{rt}$ alınabilir. Dolaysıyla $\alpha = \delta^r$ ve $x^n - a$ aşağıdaki gibi çarpanlara sahiptir;

$$x^n - a = \prod_{i=0}^{n-1} \left(x - \delta\zeta^i\right) = \prod_{i=0}^{n-1} \left(x - w^{t(1+ir)}\right) = \prod_{i=0}^{n-1} \left(x - \delta^{1+ir}\right) \tag{3.1}$$

$x^n - a$ nın her indirgenemez çarpanı nr (n modülo olmak zorunda değil) modülüne göre bir devresel kosetine karşılık gelir. Her indirgenemez çarpanın derecesi, modulo nr ye göre devresel kosetin eleman sayısına eşittir. $x^n - a$ nın tüm kökleri, birimin $n.$ kökleri olduğundan,

$$(x^n - a) \mid (x^{nr} - 1)$$

ve

$$\left(x^{nr-1} - 1\right) \mid \left(x^{n(q-1)} - 1\right) \mid \left(x^{q^s-1} - 1\right).$$

Örnek 3.7 $q = 5$, $n = 6$ ve $x^6 - 3$ polinomu ele alınsın. (F_5 üzerinde $a = 3$ olan, 6 uzunluklu sabit devirli kodlar) F_5 in bir ilkel elemanı 2 olup, 3, F_5 de $3 = 2^3$ dir. 3 ün F_5 deki derecesi 4 ve $(n, q-1) = (6,4) = 2 \nmid 3$ olduğundan F_5 de 3 ün 6. kökü yoktur. Yukarıdakilere göre

$$x^6 - 3 = \prod_{i=0}^{5} \left(x - \delta^{4i+1}\right) = \left(x^2 + 3x + 3\right)\left(x^2 + 3x + 3\right)\left(x^2 + 3\right)$$

dır. δ birimin $6.4 = 24$. ilkel köküdür. δ nın kuvvetleri (F_5 üzerindeki indirgenemez çarpanların sayısı kadar) bunlar modülo 24 e göre üç tane devresel kosetin birleşimi olup, bu devresel kosetler,

$$cl_1 = \{1,5\},\ cl_9 = \{9,21\},\ cl_{13} = \{13,17\}$$

dir. Diğer taraftan $x^{24} - 1$ ve $x^6 - 1$ F_5 üzerinde aşağıdaki gibi çarpanlara ayrılır:

$$\begin{aligned} x^{24} - 1 \;=\; & \left(x^2 + 3x + 3\right)\left(x^2 + 2x + 3\right)\left(x^2 + 3\right)\left(x^2 + 4x + 1\right)\left(x^2 + x + 2\right) \\ & \left(x^2 + 2x + 4\right)\left(x^2 + x + 1\right)\left(x^2 + 4x + 2\right)\left(x^2 + 3x + 4\right)\left(x^2 + 2\right) \\ & (x+3)(x+4)(x+2)(x+1), \end{aligned}$$

ve

$$x^6 - 1 = \left(x^2 + 4x + 1\right)\left(x^2 + x + 1\right)(x+1)(x+4).$$

$x^6 - 1$ modülo 24 e göre $x^6 - 3$ kosetlerinin 1 ötelemesi ile elde edilen aşağıdaki devresel kosetlere karşılık gelir

$$cl_0 = \{0\},\ cl_4 = \{4,20\},\ cl_8 = \{8,16\} \text{ ve } cl_{12} = \{12\}.$$

Teorem 3.8 [21](Sabit Devirli Kodlar İçin BCH Sınırı) C, F_q üzerinde n uzunluklu bir sabit devirli kod, ζ birimin nt. ilkel kökü ve δ a nın nt. kökü olmak üzere $g(x)$ üreteç polinomu kökleri arasındaki $\left\{\delta\zeta^i | 1 \le i \le d-1\right\}$ elemanlarına sahip olsun. Bu durumda C nin minimum uzaklığı $\ge d$ dir.

İspat: Teorem 3.2 deki gösterimler ve tanımlamalar kabul edilsin. Bu durumda

$$\left\{\delta\zeta, \delta\zeta^2, \ldots, \delta\zeta^{d-1}\right\} = \left\{\delta^{r+1}, \delta^{2r+1}, \ldots, \delta^{(d-1)r+1}\right\}$$

dir. Bu kümenin elemanları $g(x)|x^n - a$ polinomunun kökleri arasında olmak üzere, üreteç polinomu $g(x)$ olan n uzunluklu K üzerindeki C_δ sabit devirli kod dikkate alınsın. K üzerinde $g(\delta x)|x^n - 1$ ile üretilen $\psi(C_\delta)$ devirli kodu, $\zeta, \zeta^2, \ldots, \zeta^{d-1}$ elemanlarına sahip olup, bu elemanlar $g(\delta x)$ in kökleri arasında yer almaktadır. Bilinen BCH sınırından dolayı $\psi(C_\delta)$ nın minimum uzaklığı $\geq d$ dir. C_δ ve $\psi(C_\delta)$ denk kodlar olduğu için $d(C_\delta) \geq d$ dir. Son olarak, C, C_δ nın alt-cisim alt-kodu olduğundan minimum uzaklığı $\geq d$ dir.

Örnek 3.9 Teorem 3.2 deki gösterimler kabul edilsin. $q = 3$ ve $n = 28$ olsun ve $a = 2$ olan ve $n = 28$ uzunluklu F_3 üzerindeki sabit devirli kodlar dikkate alınsın. $(n, q-1) \nmid i$ koşulu, F_3 üzerinde sadece çift uzunlukların dikkate alınmasının yeterli olabilmesini gerektirir (devirli kodlara denk olmayan sabit devirli kodlar elde etmek için).

$r = 2$ olduğu bulunur ve bunun için

$$(x^{28} - 2)|(x^{56} - 1)$$

dır. $x^{28} - 2$ nin F_3 üzerindeki çarpanları;

$$\begin{aligned} x^{28} - 2 &= \prod_{i=0}^{27}(x - \delta\zeta^i) = \prod_{i=0}^{27}(x - \delta^{2i+1}) \\ &= \left(x^6 + 2x^4 + x^3 + x^2 + 2\right)\left(x^6 + 2x^5 + x^3 + 2x + 2\right)\left(x^2 + x + 2\right) \\ &\quad \left(x^6 + x^5 + x + 2\right)\left(x^6 + 2x^4 + 2x^3 + x^2 + 2\right)\left(x^2 + 2x + 2\right) \end{aligned}$$

şeklindedir. δ, F_3 üzerinde birimin 56. ilkel kökü ve $\zeta = \delta^2$ F_3 üzerinde birimin 28. ilkel köküdür. δ nın bu çarpımlardaki üstleri modülo 56 ya göre tam olarak tek olan sayılardır ve bunlar aşağıdaki devresel kosetlere ayrılır;

$$\{1,3,9,19,25,27\}, \{5,13,15,23,37,45\}, \{7,21\},$$

$$\{11,17,33,41,43,51\}, \{35,49\} \text{ve} \{29,31,37,47,53,55\}$$

dir.

$g(x)$ polinomu, kökleri arasından $\delta^i,\ i = 5, 11, 29$ ve 35 i içeren en küçük dereceli bir polinom olsun. Bu durumda;

$$\begin{aligned} g(x) &= x^{20} + 2x^{19} + x^{17} + 2x^{16} + 2x^{13} + 2x^{12} + 2x^{11} + x^{10} \\ & \quad x^9 + 2x^8 + x^7 + 2x^4 + 2x^3 + x + 1 \end{aligned}$$

dir ve $\delta\zeta^i,\ 14 \leq i \leq 27$ elemanları $g(x)$ in arasındadır. Bu yüzden sabit devirli kodlar için BCH sınırı, 28 uzunluklu $g(x)$ ile üretilen sabit devirli kodun minimum uzaklığı en az 15 (ve boyutu 8) dir. Bu ζ boyutlu 28 uzunluklu F_3 üzerinde bir optimal lineer koddur [24].

3.3 1-Üreteçli Yarı Burmalı Kodların Yapısı

Bu bölümde 1-üreteçli yarı burmalı kodlar ele alınmıştır. 1-üreteçli yarı devirli kodlar ve onların yapısal özelikleri [25] ve [26] de ele alınmıştır. Son yıllarda ise, Gröbner bazı kullanılarak r-üreteçli yarı devirli kodların yapısı çalışılmıştır [27].

$$G_0 = \begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_{m-1} \\ ag_{m-1} & g_0 & g_1 & \cdots & g_{m-2} \\ ag_{m-2} & ag_{m-1} & g_0 & \cdots & g_{m-3} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ ag_1 & ag_2 & ag_1 & \cdots & ag_0 \end{bmatrix}_{m \times m}$$

matrisi m mertebeli burmalı (twistulant) matris olsun. [28] de yarı devirli kodların sütünlarının uygun permütasyonların aracılığıyla devresel bloklara dönüştürüldüğü gösterildi ($a = 1$ olan burmalı matris). Benzer bir ispat yarı burmalı kodlar için yapılabilir.

C, F_q üzerinde bir yarı burmalı kod olsun. $c_1, c_2, \ldots, c_r$, C nin üreteç matrisinin satırları olsun. Uygun tüm l yarı burmalı kaydırmalar alınarak C için yeni bir üreteç matrisi yazılsın. Böylece C nin bir $rm \times n$ tipinde bir üreteç matrisi oluşturulur. Daha sonra üreteç matrisinin $C_1, C_2, \ldots, C_n$ sütünlarının sıralanmasıyla aşağdaki forma dönüşür;

$$C_1, C_{l+1}, \ldots, C_{(m-1)(l+1)}, C_2, C_{2+l}, \ldots, C_{(m-1)(l+2)}, C_{2l}, \ldots, C_{ml}.$$

Bu durumda elde edilen matris burmalı matrislerin bloklarıdır. Dolaysıyla bir r-üreteçli üreteç matrisleri ve 1-üreteçli yarı burmalı kodların üreteç matrisleri aşağıdaki gibi kabul edilebilir:

$$\begin{bmatrix} G_{11} & G_{12} & \cdots & G_{1l} \\ G_{21} & G_{22} & \cdots & G_{2l} \\ \vdots & \vdots & & \vdots \\ G_{r1} & G_{r2} & \cdots & G_{rl} \end{bmatrix}_{rm \times n} \tag{3.2}$$

ve

$$\begin{bmatrix} G_1 & G_2 & \ldots & G_l \end{bmatrix}_{m \times n}$$

Burada, her G_{ij} (ya da G_k) G_0 daki formda olan bir yarı devirli kodlardaki duruma benzer olarak $n = ml$ uzunluklu F_q üzerindeki bir $l-$yarı burmalı kod, $\left(F_q[x] / \langle x^m - a \rangle\right)^l$ nin bir $F_q[x] / \langle x^m - a \rangle$ alt modülü olarak görülür.

Bu durumda, r-üreteçli bir yarı burmalı kod, $\left(F_q[x] / \langle x^n - a \rangle\right)^l$ nin r tane elemanı tarafından gerilir.

$1 \leq i \leq l$ olsun. Sabit bir i için $n = ml$ uzunluklu bir $l-$yarı burmalı kod üzerine i izdüşüm dönüşümü aşağıdaki gibi olsun.

$$\Pi_i : F_q^n \longmapsto F_q^m$$

$$(c_0, c_1, \ldots, c_{ml-1}) \longrightarrow \left(c_{(i-1)m}, c_{(1+(1-l)m)}, \ldots, c_{m-1+(i-1)m}\right)$$

her i için $\Pi_i(C)$ bir sabit devirli koddur.

Teorem 3.10 *C, F_q üzerinde $n = ml$ uzunluklu 1-üreteçli bir yarı burmalı kod olsun. Bu durumda; her $1 \leq i \leq l$ için $g_i(x) \mid (x^m - a)$ ve $\left(f_i(x), \frac{(x^m-a)}{g_i(x)}\right) = 1$ olmak üzere C nin bir $\mathbf{g(x)} \in \left(F[x] / \langle x^m - a \rangle\right)^l$ üreteçi aşağıdaki formdadır:*

$$\mathbf{g(x)} = \left(f_1(x) g_1(x), f_2(x) g_2(x), \ldots, f_l(x) g_l(x)\right).$$

İspat: Her i için $\Pi_i(C)$ bir sabit devirli kod olduğundan istenilen elde edilir.

Teorem 3.11 C, $n = ml$ uzunluklu 1-üreteçli bir yarı burmalı kod olsun. Her $1 \leq i \leq l$ için $g(x) \mid (x^m - a)$, $g(x)$, $f_i(x) \in F[x] / \langle x^m - a \rangle$ ve $(f_i(x), h(x)) = 1$, $h(x) = \frac{x^m - a}{g(x)}$ olmak üzere C nin üreteçi

$$\mathbf{g(x)} = (f_1(x) g(x), f_2(x) g(x), \ldots, f_l(x) g(x))$$

formunda olsun. Bu durumda, bazı s, d $(d > 0)$ tamsayıları için $\{\delta \zeta^i | s \leq i \leq s + (d-1)\}$ kümesinin elemanları $g(x)$ in kökleri arasında ve C nin boyutu $n - deg(g(x))$ olmak üzere

$$l(d+1) \leq d(C)$$

dir.

İspat: Her $1 \leq i \leq l$ için $\Pi_i(C)$ nin $f_i(x) g(x)$ tarafından üretilen bir sabit devirli kod olduğu dikkate alınsın. $p(x) f_i(x) g(x) = 0$ olabilmesi için gerek ve yeter koşul $(p(x) \neq 0$ ise$)$ $h(x) \mid (p(x) f_i(x))$ olması gerektiğinden, bileşenlerden birinin sıfır olabilmesi için gerek ve yeter koşul diğerlerinin de sıfır olmasıdır. Bu da $(f_i(x), h(x)) = 1$ olduğundan $h(x) \mid p(x)$ olması gerektirir. Dolaysıyla her j için $p(x) f_j(x) g(x) = 0$ dır. Bu yüzden , $\mathbf{c} \in C$ de sıfırdan farklı bir kodsöz ise her i için $\Pi_i(\mathbf{c}) \neq 0$ dır. $\langle f_i(x) g(x) \rangle = \langle g(x) \rangle$ olduğundan $\Pi_i(C)$ üreteç polinomu $g(x)$ olan bir sabit devirli koddur ve sıfırdan farklı her kodsözünün ağırlığı $> d$ (BCH sınırı) dır. Dolaysıyla C de sıfırdan farklı bir kodsözün ağırlığı $\geq l(d+1)$ dir. Dahası, devirli kodlardaki duruma benzer olarak $\mathbf{g(x)}, x\mathbf{g(x)}, \ldots, x^{n-(deg(x)-1)}\mathbf{g(x)}$ elemanlarının C kod için bir baz oluşturduğu gösterilebilir. Eğer

$$\sum_{i=0}^{deg(g(x)-1)} a_i x^i g(x) = \mathbf{0},$$

, $a_i \in F_q$ bağıntısı varsa (m-boyutlu vektörler); aynı bağıntı;

$$\sum_{i=0}^{deg(g(x)-1)} a_i x^i \mathbf{g(x)} = \mathbf{0},$$

F_q^n da sağlanır. Ayrıca ,eğer

$$\sum_i b_i x^i g(x) \neq \mathbf{0},$$

ise

$$\sum_i b_i x^i \mathbf{g(x)} = \mathbf{0}$$

dır.

Teorem 3.12 α, F_q nun bir ilkel elemanı olmak üzere $a = \alpha^i$ olsun. Eğer $(m, q-1)\,|i$ ise, F_q üzerindeki $n = ml$ uzunluklu bir yarı burmalı kod, F_q üzerindeki n uzunluklu bir sabit devirli koda denktir.

İspat: C, (3.1) deki gibi verilen G üreteç matrisine sahip olan bir yarı burmalı kod olsun. G nin m sütünlarının $1 \leq j \leq l$ için her bir düşey j bloklarına Teorem 3.2 nin ispatındaki π_i, $1 \leq i \leq m$ permütasyonları uygulansın. Bu durumda elde edilen kod bir sabit devirli koda denk olur.

3.4 Yeni Kodlar ve Üreteç Matrisleri

Bu bölümde Teorem 3.2 üzerine dayalı olan bir metod ile bazı yeni optimal 1-üreteçli yarı burmalı kodlar elde edilmiştir.Bu kodların üreteçleri aşağıdaki formdadır.

$$(g(x), f_2(x)\,g(x), \ldots, f_l(x)\,g(x))$$

Metodun iyi uygulanabilmesi için uygun kodların devresel kosetleri dikate alındı ve üreteç polinomlarının kökleri arasındaki ζ ların ardışık kosetlerinin en uzun dizisine sahip olacak şekilde oluşturuldu. $g(x)$ belirlendikten sonra (blok uzunluğu m olacak şekilde kodun boyutu belirlenmiş olur) $f_i(x)$ üzerinde araştırılmış (bilgisayar yardımıyla). En çok kullanılan durumlar $l = 2$ ya da $l = 3$ dır. $l = 2$ iken, sadece $deg(f(x)) < m - deg(g(x))$ araştırılmış. Bu durumda araştırma m uzunluklu bloklara sahip yarı burmalı kodları üzerinde etraflıca yapılmış. Metodu göstermek için aşağıdaki detaylı örnek çalışılmıştır.

Örnek 3.13 $q = 3, m = 40$ *ve* $q = 2$ olmak üzere F_3 üzerinde 40 uzunluklu sabit devirli kod ele alınsın. mod 3 e göre 2'nin derecesi 2 dir ve $x^{40} - 2$, F_3 üzerinde;

$$x^{40} - 2 = \prod_{i=0}^{39} \left(x - \delta^{2i+1}\right)$$

olarak çarpanlarına ayrılır.

δ kuvvetleri (1'in 80. ilkel kökü) aşağıdaki gibi mod 80 e göre kosetleri bir parçalanışı olan mod 80 e göre tek tamsayılarıdır. $\{1,3,9,27\}$, $\{5,15,45,5\}$, $\{7,21,29,63\}$, $\{11,19,33,57\}$, $\{13,31,37,39\}$ $\{17,51,59,73\}$, $\{23,47,61,69\}$, $\{25,35,65,75\}$, $\{41,43,49,69\}$ ve $\{53,71,77,79\}$.

$h(x) = 1,7$ *ve* 25 kosetlerinin içeren polinom ve

$$\begin{aligned} g(x) &= \frac{x^{40}-2}{h(x)} = x^{28}+2x^{27}+2x^{25}+x^{24}+2x^{23}+x^{21}+2x^{20}+x^{19}+x^{18} \\ &\quad +2x^{17}+2x^{15}+x^{14}+x^{13}+2x^{11}+x^{8}+2x^{7}+2x^{5}+x^{3}+x^{2}+2 \end{aligned}$$

olsun. Bu durumda $deg(g(x)) = 28$ dir ve kökler arasında $18 \leq i \leq 30$, $\delta\zeta^i$ leri içerir. Bu yüzden $g(x)$ tarafından üretilen 40 uzunluklu sabit devirli kodun boyutu 12 dir ve minimum uzaklığı ≥ 14 tür ve (g, gf_1, gf_2) formundaki $\left(f_i, \frac{x^{40}-2}{g}\right) = 1$, $i = 1,2,3,\ldots$ olan bir yarı burmalı kod 120 uzunluklu ve boyutu 12 olup minimum uzaklığı en az 42 dir.

$f_1 = 2x^{10}+x^9+x^8+x^6+2x^4+x^3+2x^2+x+1$ ve $f_2 = x^{11}+x^9+x^6+x^2+2x$ olsun. Bu üreteçlere sahip olan yarı burmalı kodun minimum uzaklığı 66 ve bunun F_3 üzerinde parametreleri $[120,12,63]$ olarak bilinen lineer kodun minimum uzaklığından 3 daha büyük olduğu elde edilmiştir. Bu kodun ağırlık sayacı

$$0^{1}66^{4480}69^{14000}72^{36080}75^{75008}78^{116160}81^{11040}84^{49840}90^{19552}93^{4480}96^{560}99^{80}$$

dır.

3.5 Üreteçler ve Ağırlık Sayaçları

Bu bölümde yeni kodların üreteç matrisleri ve ağırlık sayaçları verilmiştir. 1-üreteçli yarı burmalı kodların bir üreteç matrisi yalnızca ilk satırı ile belirlendiğinden (ve sabit a), sadece blokları bir virgül ile ayrılmış ilk satır verilmiştir. Aşağıda verilen ilk 15 kod üçlü yarı burmalı kod olup sadece 14. kod için $a = 1$ olup bir yarı devirli kod ve diğerleri için $a = 2$ dir. Son üç kod ise F_5 üzerinde $a = 4$ olan yarı burmalı kodlardır.

1. $[120, 12, 66]_3$ kodu;

$$(201102221002011202112102120210000000000$$
$$222112010212020201011201120011220200220$$
$$012201001122010012200210112202200112121 1).$$

2. $[160, 12, 90]_3$ kodu;

$$(201102221002011202112102120210000000000$$
$$002011021112221102110112001010100201001 0$$
$$020112101201222220201202022200112101012 0$$
$$121222101102001212000112222002112212202 2).$$

Bu kodun ağırlık sayacı;

$$0^{1}90^{3472}93^{8080}96^{22160}99^{46400}102^{73440}105^{102320}108^{107280}$$
$$111^{84080}114^{49040}117^{24720}120^{7408}123^{2160}126^{800}129^{80}.$$

3. $[164, 8, 102]_3$ kodu;

$$(100112121211002110220122101222111122202122121121101122012,$$
$$012200211111112001000000 0,000011102101212000101020111211 02$$
$$220212012222120102020001111011021200001122222021211 2.)$$

Bu kodun ağırlık sayacı;

$$0^{1}102^{1312}108^{656}111^{1312}114^{1312}120^{328}128^{328}.$$

4. $[164, 10, 96]_3$, 5. $[56, 12, 27]_3$, 6. $[56, 16, 21]_3$, 7. $[68, 16, 30]_3$, 8. $[182, 12, 105]_3$

9. $[182, 14, 99]_3$, 10. $[82, 17, 36]_3$, 11. $[70, 17, 29]_3$, 12. $[148, 18, 71]_3$, 13. $[52, 13, 23]_3$

14. $[52, 10, 26]_3$, 15. $[84, 9, 54]_5$, 16. $[78, 10, 48]_5$, 17. $[42, 12, 21]_5$.

4. 2- ÜRETEÇLİ YARI BURMALI KODLARIN BİR AÇIK İNŞASI

Bu bölümde, Chen'in [29] deki çalışmadan yaralanılarak, 2-üreteçli iki ağırlıklı yarı burmalı kodların bir ailesinin açık bir inşaası sunulmuş ve bu aileye ait bir çok kod parametrelerinin iyi ve optimal oldukları gösterilmiştir.

Tanım 4.1 Bir lineer kodun dual kodunun minimum uzaklığı en az üç ise bu koda *projektif* denir ve eğer bir kod sıfırdan farklı iki ağırlığa sahip ise bu koda *iki ağırlıklı kod* denir. w_1 ve w_2, $w_1 \neq w_2$ olacak şekilde iki ağırlıklı kodun sıfırdan farklı ağırlıkları olsun. Bir projektif $q-$lu lineer iki ağırlıklı kod $[n,k;w_1,w_2]_q$ ile gösterilir.

Herhangi bir $t>1$ tamsayısı ve asalın kuvveti olan q için bir $\lambda-$sabit devirli simpleks $[(q^t-1)/(q-1),t,q^t-1]_q$ kodu inşa edilebilir. $g(x)$, $\lambda-$sabit devirli simpleks kodun bir üreteç polinomu olsun. $a_1,a_2,\ldots,a_{q-1}$ F_q nun $q-1$ adet sıfırdan farklı elemanları olsun ve $m=(q^t-1)/(q-1)$ olsun. $\lambda-$sabit devirli sabit simpleks $[(q^t-1)/(q-1),t,q^t-1]_q$ kodunun herhangi bir kodsözü, $i=1,2,\ldots,q-1$ ve $j=1,2,\ldots,m-1$ olmak üzere modülo $x^m-\lambda$ hesaplamasına göre $g_{i,j}(x)=a_i x^j g(x)$ polinomu ile ifade edilebilir. G_t, $g(x)$ polinomu tarafından tanımlanan burmalı matris ve $G_{i,j}$, $g_{i,j}(x)$ tarafından tanımlanan burmalı matrisi olsun. Bu durumda q^t-1 tane burmalı matrisi elde edilmiş olur. $B_1,B_2,\ldots,B_{q-1}$ ler, q^t-1 tane $\left\{G_{i,j}|i=1,2,\ldots,q-1 \text{ ve } j=0,1,2,\ldots,m-1\right\}$ şeklinde yukarıdaki tanımlanan burmalı matrislerinden elde edilen $p-1$ adet farklı burmalı matrisi olmak üzere 2-üreteçli yarı burmalı kod için bir üreteç matrisi;

$$G=\begin{bmatrix} G_t & G_t & \ldots & G_t \\ 0 & B_1 & \ldots & B_{p-1} \end{bmatrix}=\begin{bmatrix} G_1 \\ G_2 \end{bmatrix} \tag{4.1}$$

şeklinde olup, G_1 ve G_2 , G burmalı matrisinin birinci ve ikinci satırlarıdır.

Teorem 4.2 Herhangi bir $t>1$ tamsayısı ve asalın kuvveti olan q için $m=\frac{q^t-1}{q-1}$ ve $p=2,3,\ldots,q^t$ olmak üzere (4.1) de verilen üreteç matrisi 2-üreteçli yarı burmalı iki ağırlıklı bir $\left[pm,2t,(p-1)q^{t-1},pq^{t-1}\right]$ kodunu tanımlar.

İspat: Bir $\lambda-$sabit devirli simpleks $\left[(q^t-1)/(q-1), t, q^{t-1}\right]_q$ kodu eşit uzunluklu bir koddur. Bu kodun q^t-1 tane sıfırdan farklı kodsözü $q-1$ tane kodsözü grubuna parçalanabilir ve her grup $m=\frac{(q^t-1)}{q-1}$ tane kodsözüne sahiptir ve bu kodsözleri $\lambda-$sabit devirlidir. $m(x)$, $g_{i,j}=a_i x^j g(x)$ tanımlayıcı polinomu tarafından kodlanmış bir mesaj polinomu, $b_1(x)$ ve $b_2(x)$, B_1 ve B_2 ayrık burmalı matrisilere karşılık gelen iki polinom olsun. Bu durumda $b_1(x)$ ve $b_2(x)$ tarafından $m(x)b_1(x)$ ve $m(x)b_2(x)$ olarak $x^m-\lambda$ modül çarpmasına göre hesaplanarak kodlanan kodsözleri farklı olacaktır. C_1, G_1 tarafından tanımlanan kodun bir alt kodu, C_2 de G_2 tarafından tanımlanan kodun bir alt kodu olsun. Dolaysıyla C_1, $\left[m, t, q^{t-1}\right]_q$ sabit devirli simpleks kodun kodsözlerin p kez tekrarları olan kodsözlerinden oluşur. Bu yüzden C_1, uzaklığı pq^{t-1} olan bir eşit uzaklıklı koddur. Benzer şekilde C_2 nin sözleri m tane sıfırı takip eden $(p-1)$ tane $\left[m, t, q^{t-1}\right]_q$ sabit devirli simpleks kodun farklı kodsözlerinden oluştuğu için C_2 de $(p-1)q^{t-1}$ esit uzunluklu bir koddur. Simpleks kodun eşit uzunluklu olma özeliği ve (4.1) deki üreteç matrisine dayanarak C_1 ve C_2 deki sıfırdan farklı kodsözlerinin toplamı, C_1 ve C_2 deki kodsözlerinin $\left[m, t, q^{t-1}\right]_q$ sabit devirli simpleks koddan aynı kodsözüne sahip olup olmadığına bağlı olarak $(p-1)q^{t-1}$ ya da pq^{t-1} ağırlıklarına sahiptir. Bunun için (4.1) tarafından tanımlanan herhangi bir 2-üreteçli yarı burmalı kod $w_1=(p-1)q^{t-1}$ ya da $w_2=pq^{t-1}$ ağırlığa sahiptir.

Sonuç 4.3 $q=2$ olsun. Herhangi bir $t>1$ tamsayısı için $p=2,3,\ldots,2^t$ olmak üzere (4.1) deki üreteç matrisi 2-üreteçli yarı devirli iki ağırlıklı $\left[p(2^t-1), 2t; (p-1)2^{t-1}, p2^{t-1}\right]$ kodu tanımlar.

Eğer t ve $q-1$ aralarında asal ise $\left[(q^t-1)/(q-1), t, q^{t-1}\right]_q$ kodu devirli bir koddur ve dolaysıyla aşağıdaki sonuç elde edilir.

Sonuç 4.4 $t>1$ herhangi bir pozitif tam sayı ve q asalın bir kuvveti olsun. Eğer t ve $q-1$ aralarında asal ise $m=(q^t-1)/(q-1)$ ve $q=2,3,4,\ldots,q^t$ olmak üzere (4.1) deki üreteç matrisi 2-üreteçli yarı devirli iki ağırlıklı

$$\left[pm, 2t; (p-1)q^{t-1}\right]_q$$

kodunu tanımlar.

Örnek 4.5 $q=2$ ve $t=3$ olsun. Bu durumda

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

dir. Dolaysıyla ikili $[7,3,4]$ devirli simpleks kodu $g(x)=x^4+x^2+x+1$ ile tanımlanır. G_3, $g(x)$ tarafından tanımlanan bir devresel matris ve $G_{1,j}$, $j=0,1,2,\ldots,6$ olmak üzere $G_{1,j}=x^j g(x)$ polinomları tarafından tanımlanan devresel matrisler olsun. Bu durumda aşağıda verilen üreteç matrisi bir ikili 2-üreteçli yarı devirli iki ağırlıklı $[56,6;28,32]$ kodu tanımlanır.

$$G=\begin{bmatrix} G_3 & G_3 & G_3 & G_3 & G_3 & G_3 & G_3 & G_3 \\ 0 & G_{10} & G_{11} & G_{12} & G_{13} & G_{14} & G_{15} & G_{16} \end{bmatrix}$$

Eğer yukarıdaki üreteç matrisinin içindeki matrislerin p sütunları alınırsa $1<p\leq 8$ için diğer $[14,6;4,8]$, $[21,6;8,12]$, $[28,6;12,16]$, $[35,6;16,20]$, $[42,6;20,24]$, $[49,6;24,28]$ 2-üreteçli yarı devirli iki ağırlıklı kodlar elde edilir.

Örnek 4.6 $q=3$ ve $t=3$ olsun. Bu durumda $m=13$ ve $q-1=2$ dir. 3 ve 2 aralarında asal olduğundan bir devirli simpleks $[13,3,9]_3$ kodu elde edilir. $g(x)=x^{10}-x^9+x^8-x^6-x^5+x^4+x^3+x^2+1$ polinomunu $[13,3,9]_3$ kodunu tanımlar. Dolaysıyla $p=2,3,\ldots,27$ olmak üzere 2-üreteçli yarı devirli iki ağırlıklı $[13p,6;9(p-1),9p]_3$ kod serisi elde edilir.

Örnek 4.7 $q=3$ ve $t=2$ olsun. Bu durumda $m=4$, $q-1=2$ ve $\lambda=2$ dir. t ve $q-1$ aralarında asal olmadığından 2-sabit devirli $[4,2,3]_3$ kodu elde edilir. F_3 üzerinde 2. dereceden bir ilkel polinom $h(x)=x^2-x-1$ dir. Dolaysıyla 2-sabit devirli koduna karşılık gelen üreteç polinomu

$$g(x)=\left(x^4-2\right)/h(x)=x^2+x-1$$

dir. $a_1=1$, $a_2=2$ olsun. G_2, $g(x)$ tarafından tanımlanan burmalı matris ve G_{ij}, $i=1,2$ ve $j=1,2,3$ için $a_i x^j g(x)$ tarafından tanımlanmış burmalı matrisi olsun. Teorem 4.2 den $p=2,3,\ldots,9$ için 2-üreteçli yarı burmalı iki ağırlıklı $[4p,4;3,3p]_3$ kod serisi inşa edilir.

4.1 İyi ve Optimal Kodlar

$[n,k,d]_q$ bir doğrusal kod olmak üzere eğer bu kodun minimum uzaklığı daha fazla iyileştirilemiyorsa, yani $[n,k,d+1]_q$ şeklinde başka bir kod bulunmuyorsa bu koda *uzaklık-optimal* ya da *d-optimal kod* denir. [30] da verilen n, k ve q için bilinen en iyi kodların online tablosu bulunmaktadır. Bu tabloda bir kodun minimum uzaklığı üzerine sınırlar verilmiştir. Bazı parametereler için sınırlar tam değer iken diğerleri için alt ve üst sınırlar verilmiştir. Sınıra ulaşan bir koda d-optimal kod denir. Minimum uzaklık için verilen sınırlar için alt sınıra ulaşan bir koda *iyi kod* denir, yani bu durumda daha büyük uzunlukta başka kod bulunmamaktadır. Yukarıdaki gibi inşa edilen 2-üreteçli yarı devirli ve yarı burmalı iki ağırlıklı kodların çoğu iyi kodlardır ve d-optimaldır.

Örnek 4.8 2-üreteçli yarı devirli iki ağırlıklı $[7p,6;4(p-1),4p]$ $2 \leq p \leq 8$ ve $[15p,8;8(p-1),8p]$ $9 < p \leq 16$ kodları d-optimaldır. 2-üreteçli yarı burmalı iki ağırlıklı $[4p,4;3(p-1),3p]_3$ $2 < p \leq 9$ kodu, 2-üreteçli yarı devirli $[5p,4;4(p-1),4p]_4$ $6 < p \leq 25$ kodları d-optimaldır. Bu kodlar arasındaki $[195,8,96]$,$[210,8,104]$ ve $[240,8,120]$ kodlar yarı devirli olarak daha önce bilinmiyordu [31]. İyi kodlar için bilgisayar yardımıyla, Gulliver ve Bhargava 1-üreteçli yarı devirli $[36,4,23]_3$ kodu inşa ettiler [32].

Ama yukarıda tanımlanan metod ile $q=3$, $t=2$ ve $p=9$ için $d-$optimal 2-üreteçli yarı burmalı $[36,4,24]_3$ kodu elde edilir. $q=3$, $t=3$ ve $p=16$ ve $p=17$ ile 2-üreteçli yarı devirli iki ağırlıklı $[208,6,135;144]_3$ ve $[221,6,135;153]_3$ kodu elde edilir ve bunlar [30] daki uzunluklar üzerindeki alt sınıra ulaşırlar.

4.2 Uzunluk-Optimal Kodlar

$[n,k,d]_q$ bir lineer kod olsun. Eğer bir kodun uzunluğu azaltılamıyorsa yani $[n-1,k,d]_q$ şeklinde bir kod bulunmuyorsa bu koda uzunluk-optimal ya da n-optimal kod denir. [22] de bir $[n,k,d]_q$ kodu için blok uzunluğu kuralı, $\lceil x \rceil$, x'e eşit veya büyük

en küçük tamsayıyı göstermek üzere Griesmer sınırı olarak verildi,

$$n \geq \sum_{j=0}^{k-1} \left\lceil \frac{d}{q^j} \right\rceil .$$

$p = q^t$ olsun. Bu durumda $2t$ boyutlu simpleks kod 2-üreteçli yarı burmalı bir kod şeklinde inşa edilebilir.

Teorem 4.9 q bir asal sayının herhangi bir kuvveti ve $t > 1$ için $p = q^t$ ve $m = (q^t - 1)/(q-1)$ olsun. Aşağıdaki üreteç matrisi 2-üreteçli yarı burmalı simpleks $\left[(q^t-1)/(p-1) = (p+1)m, 2t, q^{2t-1}\right]_q$ kodunu tanımlar.

$$G = \begin{bmatrix} G_t & G_t & G_t & \dots & G_t & 0 \\ 0 & B_1 & B_2 & \dots & B_{p-1} & G_t \end{bmatrix} \tag{4.2}$$

İspat: Bu teoremin ispatı Teorem 4.2 dekine benzer bir yöntem ile yapılabilir.

Aşağıdaki teorem genel olarak kodların nasıl iyi kod olduklarını söyler.

$t > 1$, $j = 1,2,\dots,t$ ve $i = 1,2,\dots,q^{t-1}$ tamsayıları için gap adında bir fonksiyon aşağıdaki gibi tanımlanır;

$$gap(i,t,q) = \sum_{j=1}^{t} \left\lceil \frac{i}{q^{j-1}} \right\rceil - t$$

Teorem 4.10 q bir asalın kuvveti ve $t > 1$ tamsayısı için i, r ve q, $i = 1,2,\dots,q^t - 1$, $r = 1,2,\dots,q$ ve $p = q^t - iq + r + 1$ olacak şekilde tamsayılar olsun. (4.1) ve (4.2) de verilen üreteç matrisleri ile üretilen 2-üreteçli yarı burmalı $\left[p(q^t-1)/(q-1), 2t, (p-1)q^{t-1}\right]_q$ kodu $gap(i,t,q)$ ile verilen bir gap ile Griesmer sınırına ulaşır.

İspat: Griesmer sınırı ile, boyutu $k = 2t$ olan n uzunluklu ve minimum uzaklığı $d = (p-1)q^{t-1}$ olan bir kod aşağıdaki eşitsizlikleri sağlar;

$$\begin{aligned} n &\geq \sum_{j=0}^{k-1} \left\lceil \frac{d}{q^j} \right\rceil = \sum_{j=0}^{2t-1} \left\lceil \frac{(p-1)q^{t-1}}{q^j} \right\rceil \\ n &\geq \sum_{j=0}^{t-1} \left\lceil \frac{(p-1)q^{t-1}}{q^j} \right\rceil + \sum_{j=t}^{2t-1} \left\lceil \frac{(p-1)q^{t-1}}{q^j} \right\rceil \end{aligned}$$

$$n \geq (p-1)\left(q^{t-1}+q^{t-2}+\ldots+1\right)+\sum_{j=1}^{t}\left\lceil\frac{(p-1)}{q^j}\right\rceil$$

$$n \geq (p-1)\left(\frac{q^{t-1}}{q-1}\right)+\sum_{j=1}^{t}\left\lceil\frac{(q^t-iq+r)}{q^j}\right\rceil.$$

$$\sum_{j=1}^{t}\left\lceil\frac{(q^t-iq+r)}{q^j}\right\rceil=\sum_{j=1}^{t}q^{t-j}-\sum_{j=1}^{t}\left\lceil\frac{i}{q^{j-1}}\right\rceil-1$$

olduğundan $n \geq (p-1)(q^t-1)/(q-1)+(q^t-1)/(q-1)-gap(i,t,q)$ ya da $n \geq p(q^t-1)/(q-1)-gap(i,t,q)$.

Dolaysıyla kod tanımlanan fonksiyon ile Griesmer sınırına ulaşır. Eğer $i=1$ ise $gap(1,t,q)=0$ dır. Dolaysıyla aşağıdaki sonuç elde edilir.

Sonuç 4.11 q bir asalın kuvveti ve $t>1$ için r ve p, $r=1,2,\ldots,q$ ve $p=q^t-q+r+1$ olacak şekilde tamsayılar olsun. $\left[p(q^t-1)/(q-1),2t,(p-1)q^{t-1}\right]_q$ şeklinde inşa edilen kod Griesmer sınırına ulaşılır ve uzunluk optimaldır.

$t=q=3$ için bir örnek olarak Çizelge 4.1, $p=17,18,\ldots,28$ için elde edilen kodlar için hesaplanmıştır. Çizelge 4.1 den, p artıkça kodun daha iyi olduğu anlaşımaktadır. Çizelge 4.1 deki gb uzunluk üzerindeki Griesmer sınırını göstermektedir. Ama 2-üreteçli yarı burmalı iki ağırlıklı bir kod ailesinde p nin maksimum değeri q^t dir ve $p=q^t+1$ olduğundan bir 2-üreteçli yarı burmalı simpleks kodu elde edilir.

Çizelge 4.1 Örnek Kodlar Çizelgesi

p	d	n	gb	gap	i	R	q
17	144	221	217	4	4	1	3
18	153	234	230	4	4	2	3
19	162	247	243	4	4	3	3
20	171	260	258	2	3	1	3
21	180	273	271	2	3	2	3
22	189	286	284	2	3	3	3
23	198	299	298	1	2	1	3
24	207	312	311	1	2	2	3
25	216	325	324	1	2	3	3
26	225	338	338	0	1	1	3
27	234	351	351	0	1	2	3
28	243	364	364	0	1	3	3

5. SERBEST $\mathbb{Z}_2\mathbb{Z}_4\mathbb{Z}_8$-TOPLAMSAL KODLARI SAYMA

Lineer kodları kombinatorik açıdan incelemek, yani lineer kodların alt lineer kodlarının sayılarını bulmak oldukça önemli bir problemdir. Bu problem, cisimler üzerinde lineer kodlar için tamamıyla çözülmüştür ve kodların sayısı Gauss binom katsayıları ile gösterilmektedir. Öte yandan, halkalar üzerinde kodların sayıları ile ilgili de çok çeşitli çalışmalar ([33], [34], [35], [36]) yapılmıştır. Bu bölümde, serbest $\mathbb{Z}_2\mathbb{Z}_4\mathbb{Z}_8$-toplamsal kod tanımı yapılmış ve bu kodların sayısını veren bir formül elde edilmiştir.

1973 yılında [37] de Delsarte toplamsal kodları ilk defa birleşim şemalarını esas alarak tanımlamıştır. Genel olarak toplamsal kod, ötelenmiş birleşim şemasındaki değişmeli grubun bir alt grubu olarak tanımlanır. Daha sonra ise 1997 yılında ötelenme ile değişmeyen propelineer kodlar tanımlanmış ve bu ikili kodların $\mathbb{Q}_8$ sekiz elemanlı değişmeli olmayan quaterniyon grubu göstermek üzere, $\mathbb{Z}_2^{\alpha}\mathbb{Z}_4^{\beta}\mathbb{Q}_8^{\sigma}$ in alt gruplarına izomorf oldukları ispatlanmıştır [38].

Birleşim şemasının Hamming şeması olduğu durumda, yani değişmeli grubun mertebesinin 2^n olduğu durumda, toplamsal kodlar değişmeli ötelenme ile değişmeyen propelineer kodlarla çakışırlar. Böylece, bu tip değişmeli gruplar, $\alpha+2\beta=n$ olmak üzere, sadece $\mathbb{Z}_2^{\alpha}\times\mathbb{Z}_4^{\beta}$ formunda olacaktır [38]. Buradan, ikili Hamming şemasındaki toplamsal kodlar yalnızca $\mathbb{Z}_2^{\alpha}\times\mathbb{Z}_4^{\beta}$ nın C alt grupları olarak incelenir.

α ve β birer pozitif tamsayı olmak üzere $\mathbb{Z}_2^{\alpha}\times\mathbb{Z}_4^{\beta}$ nın bir C alt grubuna $\mathbb{Z}_2\mathbb{Z}_4$-toplamsal kod denir. $\mathbb{Z}_2\mathbb{Z}_4$-toplamsal kodların cebirsel yapısı 2010 yılında Borges ve arkadaşları tarafından [39] de incelenmiş ve bu makalede $\mathbb{Z}_2\mathbb{Z}_4$-toplamsal kodların standart haldeki üreteç ve kontrol matrisleri belirlenmiştir. Bu çalışmayla beraber $\mathbb{Z}_2\mathbb{Z}_4$-toplamsal kodlar birçok matematikçinin ilgisini çekmiş ve bugüne kadar bu konuyla ilgili olarak çeşitli çalışmalar yapılmıştır ([40], [41], [42]). 2017 yılında, Aydoğdu ve Gürsoy [43] de, $\mathbb{Z}_2\mathbb{Z}_4\mathbb{Z}_8$-toplamsal devirli kodları litaratüre kazandırdılar. Bu kodlar $\mathbb{Z}_2\mathbb{Z}_4$-toplamsal kodların bir genellemesi olarak görülebilir. 2019 da [44] de Çalışkan ve Balıkçı herhangi bir tipteki $\mathbb{Z}_2\mathbb{Z}_4\mathbb{Z}_8$-toplamsal kodların sayısı için bir

formül verdiler.

Tanım 5.1 [17] $q \neq 1$, k ve n pozitif tamsayılar olsun. q-lu Gauss katsayıları $\begin{bmatrix} n \\ k \end{bmatrix}_q$ olarak gösterilir ve

$$\begin{bmatrix} n \\ 0 \end{bmatrix}_q = 1$$

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)},\ k = 1,2,\ldots$$

olarak tanımlanır.

Teorem 5.2 [17] F_q cismi üzerinde $[n,k]$-lineer kodların sayısı $\begin{bmatrix} n \\ k \end{bmatrix}_q$ Gauss katsayısı ile verilir.

Örnek 5.3 Uzunluğu 3, boyutu 1 olan üçlü lineer kodların sayısı 13 dür. Yani parametreleri $[3,1]$ olan $\mathbb{Z}_3$ cismi üzerindeki lineer kodların sayısı,

$$\begin{bmatrix} 3 \\ 1 \end{bmatrix}_3 = \frac{3^3-1}{3-1} = 13.$$

Bu lineer kodların üreteç matrisleri $x, y \in \mathbb{Z}_3$ olmak üzere aşağıdaki gibidir,

$$[1\ x\ y],\ [0\ 1\ x],\ [0\ 0\ 1].$$

Dougherty ve Saltürk [45] de sonlu zincir halkaları üzerindeki kodların sayısını veren formülü elde ettiler.

Teorem 5.4 [46] $\mathbb{Z}_4$ bir sonlu zincir halkası olarak alınsın. A ve C, $\mathbb{Z}_2$ üzerinde matrisler, B, $\mathbb{Z}_2$ üzerinde matris olmak üzere $\mathbb{Z}_4$ üzerindeki bir lineer kod aşağıdaki üreteç matrisi ile verilen bir lineer koda permütasyon denktir,

$$\begin{pmatrix} I_{k_0} & A & B \\ 0 & 2I_{k_1} & 2C \end{pmatrix}.$$

Sonuç 5.5 [45] $\mathbb{Z}_4$ üzerinde (k_0,k_1) tipindeki ayrık lineer kodların sayısı

$$\frac{2^{nk_0}\prod_{i=0}^{k_0-1}(2^n-2^i)\prod_{j=0}^{k_1-1}(2^n-2^{k_0+j})}{2^{k_0^2+2k_0k_1}\prod_{t=0}^{k_0-1}(2^{k_0}-2^t)\prod_{l=0}^{k_1-1}(2^{k_0}-2^l)}$$

dır.

Örnek 5.6 $\mathbb{Z}_4$ üzerinde 4 uzunluklu $(1,3)$ tipindeki ayrık lineer kodların sayısı,

$$\frac{2^4(2^4-1)(2^4-2)(2^4-2^2)(2^4-2^3)}{2^7(2^1-1)(2^3-1)(2^3-2)(2^3-2^2)} = 15$$

dir. Bu lineer kodların üreteç matrisleri $x,y,z \in \mathbb{Z}_2$ olmak üzere aşağıdaki gibidir,

$$\begin{pmatrix} 1 & x & y & z \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 1 & x & y \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 1 & x \\ 0 & 0 & 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Yine Dougherty ve Saltürk [47] de hem $(\alpha,\beta;\gamma,\delta,\kappa)$ tipindeki ayrık $\mathbb{Z}_2\mathbb{Z}_4$-toplamsal kodların hemde serbest $\mathbb{Z}_2\mathbb{Z}_4$-toplamsal kodların sayısını veren formülleri elde ettiler.

Teorem 5.7 [47] $(\alpha,\beta;\gamma,\delta,\kappa)$ tipindeki ayrık $\mathbb{Z}_2\mathbb{Z}_4$-toplamsal kodların sayısı,

$$2^{(\alpha+\beta-\gamma-\delta)\delta+(\beta-\delta-\gamma+\kappa)\kappa} \begin{bmatrix} \beta \\ \delta \end{bmatrix}_2 \begin{bmatrix} \alpha \\ \kappa \end{bmatrix}_2 \begin{bmatrix} \beta-\delta \\ \gamma-\kappa \end{bmatrix}_2$$

dir.

Örnek 5.8 $(2,2;2,0,1)$ tipindeki ayrık $\mathbb{Z}_2\mathbb{Z}_4$-toplamsal kodların sayısı,

$$\frac{2^2(2^2-1)(2^2-1)}{(2^2-2)(2-1)} = 18$$

olup, bu kodların üreteç matrisleri aşağıdaki gibidir,

$$\left(\begin{array}{cc|cc} 1 & x & y & 0 \\ 0 & 0 & y & 2 \end{array}\right), \left(\begin{array}{cc|cc} 0 & 1 & y & 0 \\ 0 & 0 & y & 2 \end{array}\right), \left(\begin{array}{cc|cc} 1 & x & 0 & 0 \\ 0 & 0 & 2 & 0 \end{array}\right),$$

$$\left(\begin{array}{cc|cc} x & 1 & 0 & 2 \\ 0 & 0 & 2 & 0 \end{array}\right), \left(\begin{array}{cc|cc} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \end{array}\right), \left(\begin{array}{cc|cc} 1 & 0 & 0 & 2 \\ 0 & 0 & 2 & 0 \end{array}\right).$$

s tane vektör tarafından üretilen bir $\mathbb{Z}_2\mathbb{Z}_4$-toplamsal kodun tipi $(\alpha,\beta;0,s,\kappa)$ dır.

Teorem 5.9 [47] $\mathbb{Z}_2^{\alpha} \times \mathbb{Z}_4^{\beta}$ da, s tane vektör tarafından üretilen serbest $\mathbb{Z}_2\mathbb{Z}_4$-toplamsal kodların sayısı,

$$2^{s(\beta+\alpha-s)} \begin{bmatrix} \beta \\ s \end{bmatrix}_2$$

dir.

Örnek 5.10 $\alpha = 1$ ve $\beta = 2$ olmak üzere $s = 1$ vektör tarafından üretilen serbest $\mathbb{Z}_2\mathbb{Z}_4$-toplamsal kodların sayısı,

$$2^{1(2+1-1)} \begin{bmatrix} 2 \\ 1 \end{bmatrix}_2 = 12$$

olup, bu kodların üreteç matrisleri aşağıdaki gibidir,

$$\left(\begin{array}{c|cc} 1 & 0 & 1 \end{array}\right), \left(\begin{array}{c|cc} 1 & 1 & 1 \end{array}\right), \left(\begin{array}{c|cc} 1 & 2 & 1 \end{array}\right), \left(\begin{array}{c|cc} 1 & 3 & 1 \end{array}\right),$$
$$\left(\begin{array}{c|cc} 1 & 1 & 0 \end{array}\right), \left(\begin{array}{c|cc} 1 & 1 & 2 \end{array}\right), \left(\begin{array}{c|cc} 0 & 0 & 1 \end{array}\right), \left(\begin{array}{c|cc} 01 & 1 & 1 \end{array}\right),$$
$$\left(\begin{array}{c|cc} 0 & 2 & 1 \end{array}\right), \left(\begin{array}{c|cc} 0 & 3 & 1 \end{array}\right), \left(\begin{array}{c|cc} 0 & 1 & 0 \end{array}\right), \left(\begin{array}{c|cc} 0 & 1 & 2 \end{array}\right).$$

[48] de Aydogdu ve Şiap ayrık $\mathbb{Z}_2\mathbb{Z}_8$-toplamsal kodların sayısı için bir formül elde ettiler. S_1 ve S_2, $\mathbb{Z}_2$ üzerinde matrisler, A_{01}, A_{02}, A_{03}, A_{12} ve A_{13}, $\mathbb{Z}_4$ üzerinde matrisler, A_{23}, $\mathbb{Z}_8$ üzerinde matris, T_{03}, $\mathbb{Z}_2$ üzerinde matris, I_{k_0}, I_{k_1}, I_{k_2} ve I_{k_4} birim matrisler olmak üzere $\mathbb{Z}_2^{\alpha} \times \mathbb{Z}_8^{\beta}$ da $(\alpha, \beta; k_0, k_1, k_2, k_3)$ tipindeki bir toplamsal kodun standart üreteç matrisi aşağıdaki gibidir,

$$\left(\begin{array}{cc|cc|cc} I_{k_0} & \overline{A}_{01} & \mathbf{0} & \mathbf{0} & \mathbf{0} & 4T_{03} \\ \mathbf{0} & S_1 & I_{k_1} & A_{01} & A_{02} & A_{03} \\ \mathbf{0} & S_2 & \mathbf{0} & 2I_{k_2} & 2A_{12} & 2A_{13} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & 4I_{k_3} & A_{23} \end{array}\right).$$

Teorem 5.11 [48] $(\alpha, \beta; k_0, k_1, k_2, k_3)$ tipinde ayrık $\mathbb{Z}_2\mathbb{Z}_8$-toplamsal kodların sayısı, $\delta = k_0(\beta - l) + k_1(\alpha - k_0 + 2(\beta - l) + k_3) + k_2((\beta - l) + (\alpha - k_0))$ ve $l = k_1 + k_2 + k_3$ olmak üzere

$$N_{2\times 8} = 2^{\delta} \begin{bmatrix} \alpha \\ k_0 \end{bmatrix}_2 \begin{bmatrix} \beta \\ k_1, k_2, k_3 \end{bmatrix}_2$$

dır.

Örnek 5.12 C, $(2,2;1,1,1,0)$ tipinde bir $\mathbb{Z}_2\mathbb{Z}_8$-toplamsal kod olmak üzere, bu tipteki ayrık kodların sayısı, $\delta = 1(2-2) + 1(2-1+2(2-2)+0) + 1((2-2)+(2-1)) = 2$ olmak üzere,

$$N_{2\times 8}(2,2;1,1,1,0) = 2^2 \begin{bmatrix} 2 \\ 1 \end{bmatrix}_2 \begin{bmatrix} 2 \\ 1,1,0 \end{bmatrix}_2 = 36$$

dır. Bu kodların üreteç matrisleri $x,y,z,t \in \mathbb{Z}_2$ olmak üzere aşağıdaki gibidir,

$$\begin{pmatrix} 1 & x & 0 & 0 \\ 0 & y & 1 & t \\ 0 & z & 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & x & 0 & 0 \\ 0 & y & 0 & 1 \\ 0 & z & 2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 0 \\ x & 0 & 1 & y \\ z & 0 & 0 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 0 \\ x & 0 & 0 & 1 \\ y & 0 & 2 & 0 \end{pmatrix}.$$

Tanım 5.13 $\mathbb{Z}_2$, $\mathbb{Z}_4$ ve $\mathbb{Z}_8$ sırasıyla modülo 2, 4 ve 8 e göre tamsayı halkaları olsunlar. Bu durumda, $\mathbb{Z}_2^{\alpha} \times \mathbb{Z}_4^{\beta} \times \mathbb{Z}_8^{\theta}$ nin bir alt grubu C ye bir $\mathbb{Z}_2\mathbb{Z}_4\mathbb{Z}_8$-toplamsal kod denir. C, $\mathbb{Z}_2^{\alpha} \times \mathbb{Z}_4^{\beta} \times \mathbb{Z}_8^{\theta}$ nin

$$\mathbb{Z}_2^{k_0} \times \mathbb{Z}_2^{2k_1} \times \mathbb{Z}_2^{k_2} \times \mathbb{Z}_2^{3k_3} \times \mathbb{Z}_2^{2k_4} \times \mathbb{Z}_2^{k_5}$$

şeklindeki bir alt grubuna izomorfik olup, C ye $(k_0,k_1,k_2,k_3,k_4,k_5)$ tipinde bir $\mathbb{Z}_2\mathbb{Z}_4\mathbb{Z}_8$-toplamsal kod denir [43].

[44] de Çalışkan ve Balıkçı $\mathbb{Z}_2\mathbb{Z}_4$ ve $\mathbb{Z}_2\mathbb{Z}_8$-toplamsal kodlar için elde edilmiş olan bu formüllerin bir genellemesini yaparak $\mathbb{Z}_2^{\alpha}\mathbb{Z}_4^{\beta}\mathbb{Z}_8^{\theta}$ da $(\alpha,\beta,\theta;k_0,k_1,k_2,k_3,k_4,k_5)$ tipindeki ayrık $\mathbb{Z}_2\mathbb{Z}_4\mathbb{Z}_8$-toplamsal kodların sayısı için bir formül elde ettiler.

C, $(\alpha,\beta,\theta;k_0,k_1,k_2,k_3,k_4,k_5)$ tipinde bir $\mathbb{Z}_2\mathbb{Z}_4\mathbb{Z}_8$-toplamsal kodunun standart üreteç matrisi, $\overline{A}_{01}$, $\overline{S}_1$, $\overline{S}_2$, $\overline{S}_3$, $\mathbb{Z}_2$ üzerinde matrisler, B_{02}, B_{12}, S_{02} ve S_{12}, $\mathbb{Z}_4$ üzerinde matrisler, T_4, T_5 ve A_{i3} $0 \le i \le 2$ için $\mathbb{Z}_8$ üzerinde matrisler, B_{01}, S_{01} ve T_1 matrislerinin tüm bileşenleri $\{0,1\} \subseteq \mathbb{Z}_4$ den, benzer şekilde A_{01} ve T_2, $\mathbb{Z}_4$ üzerinde matrisler olup tüm bileşenleri $\{0,1\}$ den, T_3, A_{12} ve A_{02} $\mathbb{Z}_8$ üzerinde matrisler ama tüm bileşenleri $\{0,1,2,3\}$ kümesinin elemanlarından olmak üzere C, $2^{k_0}2^{2k_1}2^{k_2}2^{3k_3}2^{2k_4}2^{k_5}$ tane kodsöze sahiptir ve aşağıdaki gibi bir standart üreteç matrise permütasyon denktir [43],

$$\left(\begin{array}{cc|ccc|ccc|c} I_{k_0} & \overline{A}_{01} & 0 & 0 & 2T_1 & 0 & 0 & 0 & 4T_2 \\ 0 & \overline{S}_1 & I_{k_1} & B_{01} & B_{02} & 0 & 0 & 2T_3 & 2T_4 \\ 0 & 0 & 0 & 2I_{k_2} & 2B_{12} & 0 & 0 & 0 & 4T_5 \\ 0 & \overline{S}_2 & 0 & S_{01} & S_{02} & I_{k_3} & A_{01} & A_{02} & A_{03} \\ 0 & \overline{S}_3 & 0 & 0 & 2S_{12} & 0 & 2I_{k_4} & 2A_{12} & 2A_{13} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4I_{k_5} & 4A_{23} \end{array}\right).$$

Teorem 5.14 [44] C, $(\alpha,\beta,\theta;k_0,k_1,k_2,k_3,k_4,k_5)$ tipinde $\mathbb{Z}_2\mathbb{Z}_4\mathbb{Z}_8$-toplamsal kod olsun. $s=k_1+k_2$ ve $t=k_3+k_4+k_5$ ve

$$\begin{aligned}\delta &= k_0[(\beta-s)+(\theta-t)]\\ &\quad +k_1[(\alpha-k_0)+(\beta-s)+2(\theta-t)+k_5]\\ &\quad +k_2[(\theta-t)-2k_3-k_4]\\ &\quad +k_3[(\alpha-k_0)+2(\beta-s)+2(\theta-t)+k_2+k_5]\\ &\quad +k_4[(\alpha-k_0)+2(\beta-s)+(\theta-t)+k_2]\end{aligned}$$

olmak üzere bu kodların sayısı,

$$N_{2\times4\times8}=2^{\delta}\begin{bmatrix}\alpha\\ k_0\end{bmatrix}_2\begin{bmatrix}\beta\\ k_1,k_2\end{bmatrix}_2\begin{bmatrix}\theta\\ k_3,k_4,k_5\end{bmatrix}_2$$

dır.

Örnek 5.15 C, $(2,1,1,1,1,0,1,0,0)$ tipinde bir $\mathbb{Z}_2\mathbb{Z}_4\mathbb{Z}_8$-toplamsal kod olsun. Bu ayrık kodların sayısı, $\alpha=2$, $\beta=\theta=1$, $k_0=k_1=k_3=1$ and $k_2=k_4=k_5=0$, $\delta=2$ olmak üzere,

$$N_{2\times4\times8}=2^2\begin{bmatrix}2\\ 1\end{bmatrix}_2\begin{bmatrix}1\\ 1,0\end{bmatrix}_2\begin{bmatrix}1\\ 1,0,0\end{bmatrix}_2=12$$

olup, bu kodların üreteç matrisleri x, y ve z 0 ya da 1 olmak üzere aşağıdaki gibidir,

$$\begin{pmatrix}1&x&0&0\\ 0&y&1&0\\ 0&z&0&1\end{pmatrix},\ \begin{pmatrix}0&1&0&0\\ y&0&1&0\\ z&0&0&1\end{pmatrix}.$$

Tanım 5.16 [49] $v_1,v_2,\ldots,v_k\in\mathbb{Z}_8$ olmak üzere, eğer $\sum_{i=1}^{k}\alpha_i v_i=0$ iken her i için $\alpha_i=0$ oluyorsa vektör kümesine *lineer bağımsız* denir. Eğer $\sum_{i=1}^{k}\alpha_i v_i=0$ iken her i için $\alpha_i=\{0,2,4\}$ oluyorsa vektör kümesine *modüler bağımsız* denir.

$\mathbb{Z}_8$ üzerindeki kodlar için modüler bağımsız üreteç kümesi en küçük üreteç kümesidir. Böylece standart formda verilen üreteç matrisindeki satırlar modüler bağımsızdırlar [50].

Tanım 5.17 [51] Bir R halkası üzerinde herhangi bir kod, s adet lineer bağımsız vektör ile üretiliyorsa bu koda *serbest (free) kod* denir.

Tanım 5.18 Herhangi bir $\mathbb{Z}_2\mathbb{Z}_4\mathbb{Z}_8$-toplamsal C kodu için, eğer her 2 mertebeli $u \in C$ ve 4 mertebeli $v \in C$ vektörleri için $u = w_1 + w_1 + w_1 + w_1$ and $v = w_2 + w_2$ olacak şekilde $w_1,\ w_2 \in C$ vektörleri bulunabiliyorsa C koduna bir serbest kod denir.

$(\alpha, \beta, \theta; k_0, k_1, k_2, k_3, k_4, k_5)$ tipinde bir $\mathbb{Z}_2\mathbb{Z}_4\mathbb{Z}_8$-toplamsal kodunun standart matrisi, $\overline{S}_2$, $\mathbb{Z}_2$ üzerinde bir matris, S_{02}, $\mathbb{Z}_4$ üzerinde bir matris, A_{03}, $\mathbb{Z}_8$ üzerinde matrisler, A_{01}, $\mathbb{Z}_4$ üzerinde bir matris olup tüm bileşenleri $\{0,1\}$ den, A_{02}, $\mathbb{Z}_8$ üzerinde matrisler ama tüm bileşenleri $\{0,1,2,3\}$ kümesinin elemanlarından olmak üzere $\mathbb{Z}_2\mathbb{Z}_4\mathbb{Z}_8$-toplamsal kodun standart üreteç matrisinden herhangi bir serbest $\mathbb{Z}_2\mathbb{Z}_4\mathbb{Z}_8$-toplamsal kod için üreteç matrisi aşağıdaki gibi elde edilir

$$\left(\begin{array}{c|c|cc} \overline{S}_2 & S_{02} & I_{k_3} & A_{03} \end{array} \right).$$

Lemma 5.19 C herhangi bir $\mathbb{Z}_2\mathbb{Z}_4\mathbb{Z}_8$-toplamsal kod ve $i = 1, 2, \ldots, k$ için $v_i = (v_{i_X}, v_{i_Y}, v_{i_Z}) \in \mathbb{Z}_2^{\alpha} \times \mathbb{Z}_4^{\beta} \times \mathbb{Z}_8^{\theta}$ olsun. $v_1, v_2, \ldots, v_k \in C$ vektörlerinin bir serbest kod üretebilmesi için gerek yeter koşul $v_{1_Z}, v_{2_Z}, \ldots, v_{k_Z}$ vektörlerinin bir serbest $\mathbb{Z}_8$ kodunu üretmesidir.

İspat: Kabul edelim ki c, 8 mertebeli bir $\mathbb{Z}_2\mathbb{Z}_4\mathbb{Z}_8$ vektör olsun. Bu durumda $c+c+c+c \neq 0$ dır ve c_X bir ikili kod olduğundan $c_X + c_X + c_X + c_X = 0$ ve $c_Y + c_Y + c_Y + c_Y = 0$ dır. Dolayısıyla $4c_Z \neq 0$ ve $\mathbb{Z}_8$ kısmı 8 mertebelidir. Buradan, bir $\mathbb{Z}_2\mathbb{Z}_4\mathbb{Z}_8$ vektörün 8 mertebeli olabilmesi için gerek yeter koşulun onun $\mathbb{Z}_8$ kısmının 8 mertebeli olması gerektiği elde edilir.

Şimdi sırasıyla $\mathbb{Z}_2\mathbb{Z}_4\mathbb{Z}_8$-toplamsal kodun 8 mertebeli bir vektörün katı olmayan 2 mertebeli ve 4 mertebeli vektörler içermediğini yani $\mathbb{Z}_2\mathbb{Z}_4\mathbb{Z}_8$-toplamsal kodun bir serbest kod olduğunu gösterelim.

$w_1, w_2, \ldots, w_k$ vektörleri bir serbest $\mathbb{Z}_8$ kodunu üreten sekizli lineer bağımsız vektörler olsun. Eğer bir w vektörü bu kodda 2 mertebeli vektör ise, $\alpha_i \in \mathbb{Z}_8$ için $w = \alpha_1 w_1 + \alpha_2 w_2 + \cdots + \alpha_k w_k$ olduğu elde edilir. w, 2 mertebeli bir vektör olduğundan, $2w =$

$2(\alpha_1 w_1 + \alpha_2 w_2 + \cdots + \alpha_k w_k) = 0$ dır. Bu ise vektörlerin lineer bağımsız olmalarından dolayı her bir α_i nin ya 0 ya da 4 olmasını gerektirir. $\alpha_i' = \frac{\alpha_i}{4}$ olsun. Bu durumda $\alpha_1' w_1 + \alpha_2' w_2 + \cdots + \alpha_k' w_k$ vektörü 8 mertebeli bir koddur. Bu da, lineer bağımsız vektörler tarafından üretilen bir serbest $\mathbb{Z}_8$ kodda 2 mertebeli her vektörün 8 mertebeli bir vektörün herhangi katı olması gerektiğni ispatlar.

Benzer şekilde, eğer bir w' vektörü bu kodda 4 mertebeli vektör ise, $\beta_i \in \mathbb{Z}_8$ için $w' = \beta_1 w_1 + \beta_2 w_2 + \cdots + \beta_k w_k$ olduğu elde edilir. w', 4 mertebeli bir vektör olduğundan, $4w' = 4(\beta_1 w_1 + \beta_2 w_2, \cdots + \beta_k w_k) = 0$ dır. Bu ise vektörlerin lineer bağımsız olmalarından dolayı her bir β_i nin ya 0 ya da 2 olmasını gerektirir. $\beta_i' = \frac{\beta_i}{2}$ olsun. Bu durumda $\beta_1' w_1 + \beta_2' w_2 + \cdots + \beta_k' w_k$ vektörü 8 mertebeli bir koddur. Bu da, lineer bağımsız vektörler tarafından üretilen bir serbest $\mathbb{Z}_8$ kodda 4 mertebeli her vektörün 8 mertebeli bir vektörün herhangi bir katı olması gerektiğini ispatlar.

s vektör tarafından üretilen bir serbest $\mathbb{Z}_2\mathbb{Z}_4\mathbb{Z}_8$-toplamsal kod $(\alpha, \beta, \theta; 0, 0, 0, s, 0, 0)$ tipindedir.

Lemma 5.20 $\mathbb{Z}_2^{\alpha} \times \mathbb{Z}_4^{\beta} \times \mathbb{Z}_8^{\theta}$ de serbest bir $\mathbb{Z}_2\mathbb{Z}_4\mathbb{Z}_8$-toplamsal kodu üreten s vektörünü seçmenin yollarının sayısı

$$N_s = \prod_{i=0}^{s-1} \left(8^{\theta} - 4^{\theta} 2^i\right) 2^{\alpha+2\beta}$$

dır.

İspat: [51] deki Lemma 2.3 ü $\mathbb{Z}_8$ e uygulandığında s tane lineer bağımsız vektörlerini seçmenin yollarının sayısı

$$\left(8^{\theta} - 4^{\theta}\right)\left(8^{\theta} - 2\left(4^{\theta}\right)\right)\left(8^{\theta} - 2^2\left(4^{\theta}\right)\right) \cdots \left(8^{\theta} - \left(2^{s-1}\right) 4^{\theta}\right).$$

dır.

Diğer taraftan, bu durumda bir vektörün her bir seçimi eşlik eden ikili ve dörtlü vektörlerin seçimini verir. Yani Lemma 5.19 dan dolayı, v_{1_X} ve v_{1_Y} lerin ne oldukları önemsizdir. Dolaysıyla, bir serbest kodu üreten s vektörlerinin seçim yollarının sayısı

$$\left(8^{\theta} - 4^{\theta}\right) 2^{\alpha} 4^{\beta} \left(8^{\theta} - 2\left(4^{\theta}\right) 2^{\alpha} 4^{\beta}\right) \left(8^{\theta} - 2^2\left(4^{\theta}\right)\right) 2^{\alpha} 4^{\beta} \cdots \left(8^{\theta} - \left(2^{s-1}\right) 4^{\theta}\right) 2^{\alpha} 4^{\beta}$$

dır.

Lemma 5.21 $\mathbb{Z}_2^{\alpha} \times \mathbb{Z}_4^{\beta} \times \mathbb{Z}_8^{\theta}$ de s vektör tarafından üretilen bir serbest $\mathbb{Z}_2\mathbb{Z}_4\mathbb{Z}_8$-toplamsal kodun bir en küçük üreteç kümesini bulmanın yollarının sayısı

$$D_s = 2^{2s^2} \prod_{i=0}^{s-1} \left(2^s - 2^i\right)$$

dır.

İspat: Buradaki sayma işlemi Lemma 5.20 dekine benzer olup, ikili ve dörtlü kısımlar için serbest seçimler dikkate alınmayacağından, s vektör tarafından üretilen bir serbest $\mathbb{Z}_2\mathbb{Z}_4\mathbb{Z}_8$-toplamsal kodun bir en küçük üreteç kümesini bulmanın yollarının sayısı

$$\left(8^s - 4^s\right)\left(8^s - 2\left(4^s\right)\right)\left(8^s - 2^2\left(4^s\right)\right)\cdots\left(8^s - \left(2^{s-1}\right)4^s\right)$$

olarak elde edilir.

Teorem 5.22 $\mathbb{Z}_2^{\alpha} \times \mathbb{Z}_4^{\beta} \times \mathbb{Z}_8^{\theta}$ de s vektör tarafından üretilen serbest $\mathbb{Z}_2\mathbb{Z}_4\mathbb{Z}_8$-toplamsal kodların sayısı

$$2^{s[\alpha+2\beta+2(\theta-s)]} \begin{bmatrix} \theta \\ s \end{bmatrix}_2$$

dır.

İspat: Pay kısmı Lemma 5.20 den ve payda kısmı Lemma 5.21 den gelmek üzere,

$$\begin{aligned} & \frac{\left(8^{\theta} - 4^{\theta}\right)\left(8^{\theta} - 2\left(4^{\theta}\right)\right)\left(8^{\theta} - 2^2\left(4^{\theta}\right)\right)\cdots\left(8^{\theta} - \left(2^{s-1}\right)4^{\theta}\right)2^{s\alpha}4^{s\beta}}{\left(8^s - 4^s\right)\left(8^s - 2\left(4^s\right)\right)\left(8^s - 2^2\left(4^s\right)\right)\cdots\left(8^s - \left(2^{s-1}\right)4^s\right)} \\ = & \frac{\left(4^{\theta}\right)^s 2^{s\alpha}4^{s\beta}}{\left(4^s\right)^s}\left[\frac{\left(2^{\theta}-1\right)\left(2^{\theta}-2\right)\left(2^{\theta}-2^2\right)\cdots\left(2^{\theta}-2^{s-1}\right)}{\left(2^s-1\right)\left(2^s-2\right)\left(2^s-2^2\right)\cdots\left(2^s-2^{s-1}\right)}\right] \\ = & 2^{s[\alpha+2\beta+2(\theta-s)]}\begin{bmatrix} \theta \\ s \end{bmatrix}_2 \end{aligned}$$

bulunur.

Örnek 5.23 C, $(2,1,1,0,0,0,1,0,0)$ tipinde bir serbest $\mathbb{Z}_2\mathbb{Z}_4\mathbb{Z}_8$-toplamsal kod olsun. Bu kodların sayısı,

$$2^{1[2+2\cdot 1+2(1-1)]}\begin{bmatrix}1\\1\end{bmatrix}_2 = 16$$

dir. Bu kodların üreteç matrisleri $x,\ y \in \mathbb{Z}_2$ ve $z \in \mathbb{Z}_4$ olmak üzere aşağıdaki gibidir,

$$\left(\begin{array}{cc|c|c} x & y & z & 1 \end{array}\right).$$

6. SONUÇLAR VE ÖNERİLER

Bu çalışmada, [19] deki makalede sunulmuş olan 1-üreteçli yarı burmalı kodların cebirsel yapıları araştırılarak, F_3 ve F_5 cisimleri üzerinde tanımlı bazı yeni elde edilmiş optimal kodlar tasnif edilmiştir.

Ayrıca [29] deki makalede verilmiş olan 2-üreteçli yarı burmalı kodların açık bir inşaası metodu ile edilmiş olan yeni optimal kodların bir sınıfı çalışılmıştır.

Son kısımda ise serbest $\mathbb{Z}_2\mathbb{Z}_4\mathbb{Z}_8$-toplamsal kod tanımı yapılmış ve bu kodların sayısını veren bir formül elde edilmiştir.

İlerleyen araştırmalar için, bir $\mathbb{Z}_2^{\alpha}\mathbb{Z}_4^{\beta}\mathbb{Z}_8^{\theta}$ uzayında kendine dual kodlar ile ilgili çalışmalar yapılabilir [43]. Ayrılamayan $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_4$ devirli kodların duallerinin yapıları ile ilgili araştırmalar yapılabilir ve bu iki kod grubu için tek ağırlıklı olabilmeleri için gerek ve yeter koşullar incelenebilir [52].

KAYNAKLAR

[1] Shannon, C.E., A mathematical theory of communication, The Bell System Technical Journal, 27, 379-423, 1948.

[2] Golay, M.J.E., Notes on digital coding, Proceedings of The Institute of Electrical and Electronics Engineers, 37, 657, 1949.

[3] Hamming, R.W., Error detecting and error-correcting codes, The Bell System Technical Journal, 29, 147-60, 1950.

[4] Gilbert, E.N., A comparision of signalling alphabets, The Bell System Technical Journal, 31, 504- 22, 1952.

[5] Varshamov, R.R., Estimate of the number of signals in error-correcting codes, Doklady Akademii Nauk SSSR, 117, 739-41, 1957.

[6] Slepian, D., Some further theory of group codes, The Bell System Technical Journal, 39, 1219-52, 1960.

[7] Bose, R.C., Ray-Chaudhuri, D.K., On a class of error-correcting binary group codes, Information and Control, 3, 68-79, 1960.

[8] Reed, I.S., Solomon, G., Polynomial Codes Over Certain Finite Fields, SIAM Journal of Applied Mathematics, 8, 300-304, 1960.

[9] Nordstrom, A.W., Robinson, J.P., An optimum nonlinear code, Information and Control, 11, 613-16, 1967.

[10] Goppa, V.D., A new class of linear error-correcting codes. Problems of information Transmission, 6(3), 207-12, 1970.

[11] Hammons, A.R., Kumar, P.V., Calderbank, A.R., Sloane, N.J., Sole, P., The $\mathbb{Z}_4$ linearity of Kerdock, Preparata, Goethals and related codes, The Institute of Electrical and Electronics Engineers Transactions on Information Theory, 40, 301–319, 1994.

[12] Verhoeff, T., An updated table of minimum-distance bounds for binary linear codes, The Institute of Electrical and Electronics Engineers Transactions on Information Theory, 33, 665-680, 1987.

[13] Griesmer, J.H., A bound for error-correcting codes, International Business Machines Journal of Research and Development, 4, 532-542, 1960.

[14] Van Tilborg, H.C.A., The smallest length of binary 7-dimensional linear codes with prescribed minimum distance, Discrete Mathematics, 33, 197-207, 1981.

[15] Ytrehus, O., Helleseth, T., There is no binary [25, 8, 10]-code, The Institute of Electrical and Electronics Engineers Transactions on Information Theory, 36, 695-696, 1990.

[16] Külhan, N., Genelleştirilmiş Parçalı Devirli Kodlar ve Cebirsel Yapıları, Sakarya Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, 94, 2003.

[17] MacWilliams, F.J., Sloane, N.J.A., The Theory Of Error Correcting Codes, North Holland, New York 1977.

[18] Roman, S., Coding and Information Theory, Springer-Verlag, New York 1992.

[19] Aydın, N., Siap, I ve Chaudhuri, D.K.R., The Structure of 1-Generator Quasi-Twisted Codes and New Linear Codes, Designs, Codes and Cryptography, 24, 313–326, 2001.

[20] Jensen, J.M., Cyclic concatenated codes with constacyclic outer codes, The Institute of Electrical and Electronics Engineers Transactions on Information Theory, Vol. 38(3), 950-959, 1992.

[21] Krishna A., Sarwate, D.V., Pseudocyclic maximum-distance-separable codes, The Institute of Electrical and Electronics Engineers Transactions on Information Theory, 36(4), 880–884, 1990.

[22] Berlekamp, E.R., Algebraic Coding Theory, Revised 1984.

[23] Roman, S., Field Theory, Springer-Verlag, New York 1995.

[24] Brouwer, A.E., Linear code bound (server), Eindhoven University of Technology, The Netherlands, Erişim adresi : http://www.win.tue.nl/math/dw/personalpages/aeb/voorlincod.html.

[25] Séguin, G.E., Drolet, G., The theory of 1-generator quasi-cyclic codes, Manuscript, Department of Electrical and Computer Engineering, Royal Military College of Canada, Kingston, Ontario, 1990.

[26] Conan J., Seguin, G.E., Structural properties and enumeration of quasi-cyclic codes, Applied Algebra in Engineering Communication and Computing, 4(1), 25-39, 1993.

[27] Lally, K., Fitzpatrick, P., Construction and classification of quasi-cyclic codes, WCC 99, Workshop on Coding and Cryptography Paris, France, 11–14, 1999.

[28] Thomas K., Polynomial approach to quasi-cyclic codes, Bulletin of the Calcutta Mathematical Society, 69,51-59, 1977.

[29] Chen, Z., An Explicit Construction of 2–Generator Quasi-Twisted Codes, The Institute of Electrical and Electronics Engineers Transactions on Information Theory, 54(12), 5770-5773, 2008.

[30] Grassl, M., Bounds on the Minimum Distance of Linear Codes [Online], The Institute of Electrical and Electronics Engineers Transactions on Information Theory, 40, 301-319, 1994. Erişim adresi: http://www.codetables.de, Erişim tarihi: 12.02.2019.

[31] Chen, E.Z., Web Database of Binary QC Codes [Online]. Erişim adresi: http://moodle.tec.hkr.se/ chen/research/codes/searchqc2.htm, Erişim tarihi: 14.03.2019.

[32] Gulliver, T.A., Bhargava, V.K., Some best rate $1/p$ and rate $(p-1)/p$ systematic quasi-cyclic codes over $GF(3)$ and $GF(4)$, The Institute of Electrical and Electronics Engineers Transactions on Information Theory, 38(4), 1369-1374, 1992.

[33] Delsarte, S., Fonctions de Möbius Sur les Groups Abeliens Finis, Annals of Mathematics, 49(3), 600-609, 1948.

[34] Djubjuk, P.E., On the number of subgroups of a finite abelian group, Izvestiya Rossiiskoi Akademii Nauk Seriya Matematicheskaya, 12, 351-378, 1948.

[35] Yeh, Y., On Prime Power Abelian Groups. Bulletin of the American Mathematical Society, 54, 323-327, 1948.

[36] Bhowmik, G., Evaluation of the divisor function of matrices, Acta Arithmetica 74, 155-159, 1996.

[37] Delsarte, P., An algebraic approach to the association schemes of coding theory. Philips Research Report, Supplement, 10, 1973.

[38] Pujol, J., Rifa, J., Translation Invarriant Propelinear Codes, The Institute of Electrical and Electronics Engineers Transactions on Information Theory, 43, 590-598, 1997.

[39] Borges, J., Fernández-Córdoba, C., Pujol, J., Rifá, J., and Villanueva, M.: $\mathbb{Z}_2\mathbb{Z}_4$-linear codes: generator matrices and duality, Desings Codes Cryptography, 54(2), 167-179, 2010.

[40] Bilal, M., Borges, J., Dougherty, S.T., Fernández-Córdoba, C., Maximum distance separable codes over $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_4$, Designs, Codes and Cryptography, 61, 31-40, 2011.

[41] Bilal, M., Borges, J., Dougherty, S.T., Fernández-Córdoba, C., Optimal codes over $\mathbb{Z}_2 \times \mathbb{Z}_4$, VII Jornadas de Matemática Discreta y Algorítmica Castro Urdiales, Cantabria, 7–9 de julio de 2010.

[42] Fernández-Córdoba, C., Pujol, J., Villanueva, M., $\mathbb{Z}_2\mathbb{Z}_4$-linear codes:rank and kernel, Designs, Codes and Cryptography, 56, 43-59, 2010.

[43] Aydoğdu, İ., Gürsoy, F., $\mathbb{Z}_2\mathbb{Z}_4\mathbb{Z}_8$-Cyclic Codes. Journal of Applied Mathematics and Computing, 60(1-2), 327-341, 2019.

[44] Çalışkan B., Balıkçı K., Counting $\mathbb{Z}_2\mathbb{Z}_4\mathbb{Z}_8$-additive codes, European Journal of Pure and Applied Mathematics, 12(2), 668-679, 2019.

[45] Dougherty, S.T., Saltürk, E., Counting Codes Over Rings, Desings, Codes and Cryptography, 67(3), 293-402,2013.

[46] Wan, Z.X., Quaternary Codes, World Scientific, 1997.

[47] Dougherty, S.T., Saltürk, E., Counting $\mathbb{Z}_2\mathbb{Z}_4$-Additive Codes. Noncommutative Rings and Their Applications, Contemporary Mathematics, 634, 137-147, 2015.

[48] Aydogdu, I., Siap, I., Counting The Generator Matrices of $\mathbb{Z}_2\mathbb{Z}_8$-Codes. Mathematical Sciences And Applications E-Notes, 1(2), 143-149, 2013.

[49] Dougherty, S.T., Fernández-Córdoba, C., Codes over $\mathbb{Z}_{2^k}$, gray map and self-dual codes, Advances in Mathematics of Communications, 5, 571-588, 2011.

[50] Park, Y.H., Modular independence and generator matrices for codes over m, Designs, Codes and Cryptography, 50, 147-162, 2009.

[51] Saltürk, E., Bulanık Alt Grupların ve Kodların Sayısı ile Bazı Uygulamaları, Yıldız Teknik Üniversitesi, Fen Bilimleri Enstitüsü, Doktora Tezi, 115, 2013.

[52] Wu, T., Gao, J., Gao, Y., Fu, F.W., $\mathbb{Z}_2\mathbb{Z}_2\mathbb{Z}_4$-Cyclic Codes, Advances in Mathematics of Communications, 12(4), 641-657, 2018.

ÖZGEÇMİŞ

1. **Adı Soyadı** **:** Ömer ÖZKAN
2. **Doğum Tarihi** **:**10.09.1995
3. **Ünvanı** **:** Matematik Öğretmeni
4. **Öğrenim Durumu :**

Derece	**Alan**	**Üniversite**	**Yıl**
Lisans	Matematik	Karadeniz Teknik Üniversitesi	2017

5. **İş Tecrübesi:**

Görev Ünvanı	**Görev Yeri**	**Yıl**
Matematik Öğretmeni	Özel Artı Bilim Eğitim Kursu, Osmaniye	2018

6. **Yayınlar:**

- Özkan, Ö., Çalışkan, B., Serbest $\mathbb{Z}_2\mathbb{Z}_4\mathbb{Z}_8$-toplamsal kodları sayma, 32. Ulusal Matematik Sempozyumu, , Ondokuz Mayıs Üniversitesi, Samsun-Türkiye, 31 Ağustos-2 Eylül 2019.
- Çalışkan, B., Özkan, Ö., Serbest $\mathbb{Z}_2\mathbb{Z}_4\mathbb{Z}_8$-toplamsal kodları sayma, Erzincan University Journal of Science and Technology, (Gönderildi).

OSMANİYE KORKUT ATA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
YÜKSEK LİSANS/DOKTORA TEZ ÇALIŞMASI ORİJİNALLİK RAPORU

OSMANİYE KORKUT ATA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
MATEMATİK ANABİLİM DALI BAŞKANLIĞI'NA

Tarih: 03/09/2019

Tez Başlığı / Konusu: **BAZI OPTİMAL YARI BURMALI KODLAR**

Yukarıda başlığı/konusu belirlenen tez çalışmamın a) Kapak sayfası, b) Özet ve Abstract, c) Giriş, d) Ana bölümler ve e) Sonuç, f) Kaynakça kısımlarından oluşan toplam 51 sayfalık kısmına ilişkin, 03/09/2019 tarihinde şahsım/tez danışmanım tarafından Turnitin adlı intihal tespit programından aşağıda belirtilen filtreleme tiplerinden biri uygulanarak alınmış olan orijinallik raporuna göre, tezimin benzerlik oranı **% 16** 'dır.

Filtreleme Tip 1 (maksimum %30) ☑	**Filtreleme Tip 2 (maksimum %10)** ☐
1- Kabul/Onay ve Bildirim sayfaları hariç, 2- Kaynakça hariç, 3- Alıntılar dahil, 4- 5 kelimeden daha az örtüşme içeren metin kısımları hariç.	1- Kabul/Onay ve Bildirim sayfaları hariç, 2- Kaynakça hariç, 3- Alıntılar hariç, 4- 5 Kelimeden daha az örtüşme içeren metin kısımları hariç.

Osmaniye Korkut Ata Üniversitesi Fen Bilimleri Enstitüsü Tez Çalışması Orjinallik Raporu Alınması ve Kullanılması Uygulama Esasları'nı inceledim ve bu Uygulama Esasları'nda belirtilen azami benzerlik oranlarına göre tez çalışmamın herhangi bir intihal içermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Gereğini saygılarımla arz ederim.

03.09.2019
Tarih ve İmza

Adı Soyadı: Ömer ÖZKAN
Öğrenci No: 1711109108
Anabilim Dalı: Matematik
Programı: Matematik
Statüsü: ☑ Y.Lisans ☐ Doktora

DANIŞMAN ONAYI

UYGUNDUR.

Dr. Öğr. Üyesi Bahar AKKAYA
(Unvan, Ad Soyad, İmza)

RAPORU DÜZENLEYEN

Arş.Gör.Esra Zeynep ŞENSOY
(Unvan, Ad Soyad, İmza)