T.C.
MİMAR SİNAN GÜZEL SANATLAR ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

MİNİMAL DOĞRUSAL KODLAR VE PERMÜTASYON OTOMORFİZMA GRUPLARI

YÜKSEK LİSANS TEZİ

Sevde Zehra BOYACIOĞLU

Matematik Ana Bilim Dalı

Matematik Yüksek Lisans Programı

Tez Danışmanı: Dr. Öğr. Ü. Fatma ALTUNBULAK AKSU

TEMMUZ 2024

T.C.
MİMAR SİNAN GÜZEL SANATLAR ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

MİNİMAL DOĞRUSAL KODLAR VE PERMÜTASYON OTOMORFİZMA GRUPLARI

YÜKSEK LİSANS TEZİ

Sevde Zehra BOYACIOĞLU

Matematik Ana Bilim Dalı

Matematik Yüksek Lisans Programı

Tez Danışmanı: Dr. Öğr. Ü. Fatma ALTUNBULAK AKSU

TEMMUZ 2024

Sevde Zehra BOYACIOĞLU tarafından hazırlanan MİNİMAL DOĞRUSAL KODLAR VE PERMÜTASYON OTOMORFİZMA GRUPLARI adlı bu tezin YÜKSEK LİSANS tezi olarak uygun olduğunu onaylarım.

Dr. Öğr. Üyesi Fatma ALTUNBULAK AKSU
Tez Danışmanı

Bu çalışma, jürimiz tarafından MATEMATİK Anabilim Dalında YÜKSEK LİSANS tezi olarak kabul edilmiştir.

Danışman : Dr. Öğr. Üyesi Fatma ALTUNBULAK AKSU _____

Üye : Doç. Dr. İpek TUVAY _____

Üye : Doç. Dr. İbrahim ÖZEN _____

Bu tez, Mimar Sinan Güzel Sanatlar Üniversitesi Lisansüstü Tez Yazım Klavuzuna uygun olarak yazılmıştır.

Mimar Sinan Güzel Sanatlar Üniversitesi Lisansüstü Tez Yazım Kılavuzuna uygun olarak hazırladığım bu tez çalışmasında;

- tez içindeki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi,
- görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel etik kurallarına uygun olarak sunduğumu,
- başkalarının eserlerinden yararlanılması durumunda ilgili eserlere bilimsel normlara uygun olarak atıfta bulunduğumu,
- atıfta bulunduğum eserlerin tümünü kaynak olarak gösterdiğimi,
- kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- ücret karşılığı başka kişilere yazdırmadığımı (dikte etme dışında), uygulamalarımı yaptırmadığımı,
- bu tezin herhangi bir bölümünü bu üniversite veya başka bir üniversitede başka bir tez çalışması olarak sunmadığımı

beyan ederim.

ÖNSÖZ

Hem bir matematikçi hem de bir kadın olarak örnek aldığım, bana olan güvenini her zaman hissettiren, çalışmamız boyunca bana yol gösteren ve değerli katkılarını esirgemeyen, yollarımız kesiştiği için kendimi şanslı hissettiğim, benim için bir danışmandan fazlası olan kıymetli hocam Dr. Öğr. Üyesi Fatma ALTUNBULAK AKSU'ya tüm kalbimle teşekkür ederim.

Tez jüri üyelerim olan Doç. Dr. İpek TUVAY ve Doç. Dr. İbrahim ÖZEN hocalarıma yaptıkları katkılardan dolayı çok teşekkür ederim.

Her zaman yanımda olan, bana inanan, destekleyen ve cesaretlendiren canım aileme ve sevdiklerime teşekkür ederim.

Bu tez TÜBİTAK 2211-Yurt İçi Lisansüstü Burs Programı kapsamında desteklenmiştir. Yüksek lisans öğrenimim boyunca bana verdiği maddi destekten dolayı TÜBİTAK'a teşekkür ederim.

MİNİMAL DOĞRUSAL KODLAR VE PERMÜTASYON OTOMORFİZMA GRUPLARI

ÖZET

Bu tezde, minimal doğrusal kodlar çalışılmıştır. Minimal kodların karakterizasyonu, iki farklı yöntemle incelenmiştir. Minimal doğrusal kodların parametreleri (uzunluk, boyut, ağırlık) arasındaki ilişkiler incelenmiş ve özel olarak bu kodların uzunlukları için sınır değerleri çalışılmıştır. Bazı düşük boyutlu özel minimal kodların uzunlukları için daha iyi alt sınır değerleri verilmiştir. Son olarak, minimal kodların permütasyon otomorfizma grupları incelenmiş, sabit noktası olmayan ve mertebesi üç olan permütasyon otomorfizmasına sahip üç boyutlu bir kodun minimal olması için gerekli ve yeterli koşullar sunulmuştur.

Anahtar Kelimeler : Doğrusal kod, minimal kod, kodun duali, kod ağırlığı, permütasyon otomorfizma grupları, sabit noktası olmayan permütasyon otomorfizma

MINIMAL LINEAR CODES AND PERMUTATION AUTOMORPHISM GROUPS

ABSTRACT

In this thesis, we study minimal linear codes. We examine two different characterizations of minimal linear codes. We also consider the relations between the parameters of minimal linear codes (length, dimension, weight) and in particular we study bounds for the length of minimal linear codes. We give better lower bounds for the length of some specific low dimensional minimal linear codes. Finally, we examine the permutation automorphism groups of minimal linear codes and we present the necessary and sufficient conditions for a three dimensional linear code which has a fixed point free permutation automorphism of order three to be a minimal code.

Key Words : Linear code, minimal code, dual of a code, weight of a code, permutation automorphism groups, fixed point free automorphism

İçindekiler

Bölüm 1

Giriş

Kodlama teorisi, günümüzün en önemli araçlarından biri olan verinin aktarılması için kullanılan kodların inşası, performans analizi ve hatasız bir şekilde iletilebilmesi gibi konular ile ilgilenen hem matematiğin hem bilgisayar biliminin çalışmalar yürüttüğü bir alandır. Kodlama teorisinin amacı, dış kaynakların (gürültü, teknik aksaklıklar vb.) etkisi altında, veriyi en etkin şekilde aktarmak ve saklamak için güvenilir yöntemler bulmaktır. Kodlama teorisi günümüz dijital dünyasında her zaman olduğundan daha önemli bir yere sahiptir. Bu yüzden farklı özelliklere sahip yeni kodlar inşa etmek, inşa edilen bu kodların karakterizasyonunu bulmak, parametreleri (boyut, uzunluk, ağırlık) için ilişkiler bulmak, sınır değerler vermek önemli problemlerdendir.

Bu tezde, kodlama teorisinde önemli yer edinen doğrusal kodlar çalışılmıştır ve doğrusal kodların önemli bir alt ailesi "minimal kodlar" incelenmiştir. Sonlu bir cisim üzerinde sonlu boyutlu bir vektör uzayının herhangi bir alt uzayına doğrusal kod denir. Doğrusal bir kodun elemanlarına kod sözcüğü denir. Bir kod sözcüğünün sıfırdan farklı koordinatlarının kümesine, kod sözcüğünün desteği denir. Bir kod sözcüğünün desteği sadece kendisinin bir skaler

katı olan kod sözcüğünün desteğini içeriyor ise ve diğer başka kod sözcüklerinin desteğini içermiyor ise, bu kod sözcüğüne minimal kod sözcüğü denir. Minimal kod sözcükleri, özellikle doğrusal bir kodun dualinin içindeki minimal kod sözcükleri oldukça yoğun çalışılan bir alandır. Bu kod sözcüklerinin önemini ilk vurgulayan çalışmalar, J.L. Massey tarafından 1993 ve 1995 yıllarında sunulmuştur. Bu çalışmalar için [15, 16] numaralı makalelere bakılabilir. Doğrusal bir kodun minimal kod sözcüklerini belirlemek, ikili doğrusal kodlar için bile, oldukça zor bir problemdir. [4] numaralı makalede, minimal kod sözcüklerinin, oldukça zor (NP-hard) olan tam kod çözme problemi(complete decoding problem) ile ilişkili olduğu belirtilmiştir. [4] numaralı makale ışığında, bütün kod sözcükleri minimal olan doğrusal kodlar düşünülmüştür. Eğer bir doğrusal kodun bütün kod sözcükleri minimal ise, bu doğrusal koda minimal kod denir. Minimal kodların bulunmasına dair ilk makale [9] numaralı makaledir. Minimal kodlar uygulama alanları sebebiyle de araştırmacıların yoğun ilgi duyduğu bir kod ailesidir. Uygulamaları için incelenebilecek makalelerden biri [6] numaralı makaledir. Minimal kodların inşası oldukça zor bir konudur. Minimal kodların inşası için farklı yöntemlerin gelişmesine sebep olan ve bir kodun minimal bir kod olması için yeterli sonuç, Ashikhmin ve Barg tarafından [3] numaralı makalede verilmiştir.

$\mathbb{F}_q$ eleman sayısı q olan sonlu bir cisim, $C \subseteq \mathbb{F}_q^n$ doğrusal bir kod olsun. $c \in C$ kod sözcüğü için ağırlık, sıfırdan farklı koordinatlarının sayısı olarak tanımlanır ve $wt(c)$ olarak gösterilir.

Teorem 1.1. [3] *$C \subseteq \mathbb{F}_q^n$ doğrusal bir kod ve*

$$w_{min} = min\{wt(c)|c \in C - \{0\}\}$$

$$w_{max} = max\{wt(c)|c \in C - \{0\}\}$$

olsun. Eğer $\frac{w_{max}}{w_{min}} < \frac{q}{q-1}$ ise, C minimaldir.

Bu teoremde gerekli bir koşul verilmemiştir. $q = 2$ için gerekli ve yeterli koşul [9] numaralı makalede sunulmuştur.

Teorem 1.2. [9] *$C \subset \mathbb{F}_2^n$ doğrusal bir kod olsun. C kodunun minimal olması için gerekli ve yeterli koşul sıfırdan ve birbirinden farklı her $a, b \in C$ kod sözcüğü ikilisi için $wt(a + b) \neq wt(b) - wt(a)$ eşitsizliğinin sağlanmasıdır.*

$q > 2$ için gerekli ve yeterli koşullar [10] numaralı makalede sunulmuştur. Teorem 1.1 ve Teorem 1.2 sonuçlarının her ikisi de bütün kod sözcüklerinin ağırlıklarının hesaplanmasını gerektirmektedir. Bu hesaplamalar, $\mathbb{F}_2$ üzerindeki kodlar (ikili kodlar) için bile oldukça zordur. Bu nedenle, minimal kodlar için daha etkin karakterizasyonlar bulunmak istenmektedir. Minimal kodların karakterizasyonu için [13] numaralı makalede farklı bir yöntem sunulmuştur. Bazı özel çoklu kümeler kullanılarak, farklı alt uzaylar inşa edilmiş ve bu alt uzaylar yardımıyla bir kodun minimal olması için gerekli ve yeterli koşullar sunulmuştur.

Minimal kodlar ile ilgili bir diğer problem, minimal kodların parametreleri arasında ilişkiler kurmak ve bu parametreler için sınır değerleri verebilmektir. [13] numaralı makalede minimal kodların uzunlukları için boyut ve cismin eleman sayısı cinsinden sınır değerler verilmiştir. [2] numaralı makalede uzunluk için daha iyi sınır değerleri sunulmuştur. [1] numaralı makalede de minimal bir kodun ağırlığı ve boyutu arasında ilişkiler verilmiştir.

İkili minimal kodlar için bile uzunluk değeri için daha iyi sınır değerleri verebilmek oldukça zordur. Bu tezde, minimal kodlar, sabit ağırlıklı ve sabit ağırlıklı olmayan minimal kodlar diye iki aileye ayrılarak düşünülmüş, sabit ağırlıklı olmayan ikili minimal kodlar için düşük boyutlarda uzunluk sınır değerleri verilmiştir ve aynı zamanda kodun ağırlığı için de alt sınır belirlenmiştir. Minimal kodların dualleri incelenmiş ve dual kodların minimalliği

ile ilgili koşullar verilmiştir. İki boyutlu minimal sabit ağırlıklı olmayan kendine dik bir kod için uzunluk alt sınırı belirlenmiştir.

S_n simetri grubu $\mathbb{F}_q^n$ vektör uzayı üzerinde koordinatları değiştiren bir etkiye sahiptir. Bu etkinin yardımıyla, $C \subseteq \mathbb{F}_q^n$ için $\{\sigma \in S_n \mid \sigma(C) = C\}$ kümesi düşünülebilir. Bu küme içindeki her eleman C'nin permütasyon otomorfizması adını alır. Dahası, bu küme fonksiyon bileşkesi altında bir gruptur ve C kodunun permütasyon otomorfizma grubu adını alır. [11] numaralı makalede, W. C. Huffman mertebesi tek asal olan bir permütasyon otomorfizması yardımıyla doğrusal bir kodun, iki özel alt kodun direkt toplamı olarak yazabileceğini göstermiştir. Bu tezde, [11] numaralı makalede çalışılmış bu iki özel alt kod, sabit noktası olmayan ve mertebesi üç olan bir permütasyon otomorfizması için düşünülmüş ve bu alt kodların minimal olduğu durumlarda ve düşük boyutlu olduğu durumlarda, uzunluk için alt sınırlar verilmiştir. Son olarak, bu alt kodlar minimal olduğu zaman, hangi koşullarda direkt toplamlarının minimal olduğu sorusu, üç boyutlu ikili kodlar için yanıtlanmıştır.

Tezin organizasyonu şu şekildedir. İkinci bölümde doğrusal kodlar ve minimal kodlar ile ilgili bazı temel tanımlar verilmiştir. [9] numaralı makalede ağırlığa bağlı olarak sunulmuş olan, ikili doğrusal kodların minimal olması için gerekli ve yeterli koşullar incelenmiştir. [13] numaralı makalede sunulmuş olan minimal kodların karakterizasyonu çalışılmıştır. [13] numaralı makalede verilmiş olan, parametreler arasındaki ilişkiler ve uzunluk için sınır değerleri incelenmiştir.

Üçüncü bölümde özel olarak iki ve üç boyutlu minimal doğrusal kodların parametreleri çalışılmıştır. Özel minimal kodların uzunluk değerleri için sınırlar verilmiştir. Minimal doğrusal kodların dualleri incelenmiştir ve dual kodların minimal olup olmadığı tartışılmıştır.

Dördüncü bölümde, minimal kodların permütasyon otomorfizma grupları incelenmiştir. Sabit noktası olmayan ve mertebesi üç olan otomorfizmaya sahip minimal kodlar için bazı özel alt kodlar çalışılmış ve bu alt kodların minimal olması durumunda ne zaman ana kodun minimal olacağı üç boyutlu kodlar için kanıtlanmıştır.

Bölüm 2

Minimal Kodlar

2.1 Temel Tanımlar

Bu kısımda, tez içerisinde kullandığımız temel tanımlara yer verilmiştir. Aksi belirtilmediği sürece, kodlama teorisindeki temel tanım ve sonuçlar için [14] ve [12] numaralı kaynaklar kullanılmıştır.

p asal bir sayı, $m \geq 1$ bir tamsayı, $q = p^m$ ve $\mathbb{F}_q$, eleman sayısı q olan bir cisim olsun.

Tanım. $n \geq k \geq 0$ birer tamsayı olmak üzere, $\mathbb{F}_q^n$ vektör uzayının, herhangi bir k-boyutlu alt uzayına, $\mathbb{F}_q$ üzerinde, uzunluğu n, boyutu k olan **doğrusal kod** denir.

Notasyon. $\mathbb{F}_q$ üzerinde n uzunluklu, k boyutlu bir C doğrusal kodu için, $[n, k]_q$ kodu ifadesi kullanılır.

Tanım. Eğer $q = 2$ ve C, $\mathbb{F}_q$ üzerinde doğrusal bir kod ise, C koduna ikili (binary) doğrusal kod denir.

Tanım. n uzunluklu doğrusal C kodunun elemanlarına **kod sözcüğü** denir ve herhangi bir kod sözcüğü $c \in C$, $c = c_1 c_2 \cdots c_n$ şeklinde gösterilir.

Tanım. C doğrusal bir kod ve $c \in C$ de bir kod sözcüğü olsun. c kod sözcüğünün sıfırdan farklı koordinat sayısına, **c kod sözcüğünün ağırlığı** denir ve **wt(c)** sembolü ile gösterilir.

Tanım. C doğrusal bir kod olsun. C kodunun minimum ağırlığı, içindeki sıfırdan farklı kod sözcüklerinin ağırlıklarının en küçüğü olarak tanımlanır ve

$$\mathbf{wt(C)} = \min\{wt(c)|c \in C - \{0\}\}$$

şeklinde gösterilir.

Tanım. Bir C kodunun içindeki sıfırdan farklı tüm kod sözcüklerinin ağırlıkları aynı ise, C koduna **sabit ağırlıklı** kod denir.

Örnek 1. $C = \{0000, 1100, 0101, 1001\}$ kodu için $wt(1100) = wt(0101) = wt(1001) = 2$ olur. C kodunun, sıfırdan farklı kod sözcükleri için sadece bir tane ağırlık değeri olduğu için C kodu sabit ağırlıklı bir koddur.

Tanım. C, $[n, k]_q$ kod olsun. $0 \leq i \leq n$ olmak üzere $A_i = |\{c \in C|wt(c) = i\}|$ şeklinde tanımlansın. Bu durumda $A(C) = (A_0, ..., A_n)$ dizisine C kodunun **ağırlık dağılımı** denir.

Örnek 2. $C = \{0000, 1000, 0110, 1110\}$, $[4, 2]_2$ kodudur. C kodu için, $wt(C) = 1$ olur. C kodunun, ağırlığı 0 olan bir tane, ağırlığı 1 olan bir tane, ağırlığı 2 olan bir tane, ağırlığı 3 olan bir tane kod sözcüğü vardır. Ağırlığı 4 olan kod sözcüğü yoktur. Dolayısıyla $A(C) = (1, 1, 1, 1, 0)$ olur.

Tanım. C, uzunluğu n olan doğrusal bir kod ve $c = c_1c_2 \cdots c_n \in C$ bir kod sözcüğü olsun. Bu durumda $\{1 \leq i \leq n : c_i \neq 0\}$ kümesine c **kod sözcüğünün desteği** denir ve bu küme suppt(c) sembolü ile gösterilir.

Not. Yukarıdaki tanımlara göre, $c \in C$ için $wt(c) = |\text{suppt}(c)|$ eşitliği açıktır.

Örnek 3. $\mathbb{F}_2 = \{0, 1\}$ olmak üzere

$$C = \{00000, 11010, 10101, 10010, 01111, 01000, 00111, 11101\}$$

uzunluğu 5, boyutu 3 olan ikili bir doğrusal koddur. $c = 11010$ kod sözcüğü için, $wt(c) = 3$ ve $\text{suppt}(c) = \{1, 2, 4\}$ olur.

Tanım. [7] C, doğrusal bir kod ve $a, b \in C$ kod sözcükleri olsun. Eğer $\text{suppt}(a) \subseteq \text{suppt}(b)$ ise **b kod sözcüğü, a kod sözcüğünü içerir** denir ve $a \preceq b$ ile gösterilir.

Tanım. [7] C doğrusal bir kod ve $c \in C$ olsun. Eğer c kod sözcüğü, $\alpha \in \mathbb{F}_q$ olmak üzere, sadece ve sadece αc şeklindeki kod sözcüklerini içeriyor ise, c kod sözcüğüne **minimal kod sözcüğü** denir.

$q = 2$ ise bu tanım aşağıdaki tanıma eşdeğer olur.

Tanım. C ikili doğrusal bir kod ve $c \in C$ olsun. Eğer c kod sözcüğünün desteği sıfırdan farklı herhangi bir kod sözcüğünün desteğini içermiyor ise, c kod sözcüğüne **minimal kod sözcüğü** denir.

Tanım. [7] C doğrusal bir kod olsun. C kodunun tüm kod sözcükleri minimal kod sözcüğü ise, C koduna **minimal kod** denir.

Bir boyutlu doğrusal kodlar, tanım gereği minimaldir. Bu nedenle bu kısımdan sonra minimal kod dediğimizde en az iki boyutlu kodlar anlaşılmalıdır.

Örnek 4. $C = \{0000, 10011, 10110, 00101\}$, $[5, 2]_2$ kodu için

$$\text{suppt}(10011) = \{1, 4, 5\},\ \text{suppt}(10110) = \{1, 3, 4\},\ \text{suppt}(00101) = \{3, 5\}$$

olur. Kod sözcüklerinin destekleri birbirini içermiyor, C minimal bir koddur.

Örnek 5. $C = \{0000, 11011, 11001, 00010\}$, $[5, 2]_2$ kodu için

$$\text{suppt}(11011) = \{1, 2, 4, 5\},\ \text{suppt}(11001) = \{1, 2, 5\},\ \text{suppt}(00010) = \{4\}$$

$\text{suppt}(c_4) \subset \text{suppt}(c_2)$ ya da $\text{suppt}(c_3) \subset \text{suppt}(c_2)$ olduğu için C minimal bir kod değildir.

2.2 İkili Minimal Kodların Karakterizasyonu

Bu bölümde, ikili doğrusal bir kodun minimal olması için gerekli ve yeterli koşullar çalışılmıştır. Özel olarak, 2-ağırlıklı ve 3-ağırlıklı ikili kodların hangi koşullarda minimal olacağı irdelenmiştir. Bu bölümdeki sonuçlar ve kanıtlar [7] numaralı makaleden çalışılmıştır. Kanıtlar detaylı bir şekilde yazılmıştır. İlgili tanımlar ve sonuçlar için örnekler verilmiştir.

Tanım. A ve B birer küme olsun.

$$A \triangle B = (A \setminus B) \cup (B \setminus A)$$

şeklinde tanımlanmış kümeye A ve B kümelerinin **simetrik farkı** denir.

Lemma 2.1. *$a, b \in \mathbb{F}_2^n$ elemanları için,*

$$wt(a + b) = wt(a) + wt(b) - 2|\text{supp}(a) \cap \text{supp}(b)|$$

eşitliği sağlanır.

Kanıt. Aşağıdaki eşitlikler istenilen ifadeyi verir.

$$\begin{aligned} wt(a+b) &= |(\text{supp}(a) \setminus \text{supp}(a) \cap \text{supp}(b)) \cup (\text{supp}(b) \setminus \text{supp}(a) \cap \text{supp}(b))| \\ &= |(\text{supp}(a) \setminus \text{supp}(a) \cap \text{supp}(b)| + |(\text{supp}(b) \setminus \text{supp}(a) \cap \text{supp}(b))| \\ &= wt(a) - |\text{supp}(a) \cap \text{supp}(b)| + wt(b) - |\text{supp}(a) \cap \text{supp}(b)| \\ &= wt(a) + wt(b) - 2|\text{supp}(a) \cap \text{supp}(b)| \end{aligned}$$

■

Lemma 2.2. *$a, b \in \mathbb{F}_2^n$ elemanları için, $a \preceq b$ olması için gerekli ve yeterli koşul*

$$wt(a+b) = wt(b) - wt(a)$$

eşitliğidir.

Kanıt. $\text{suppt}(a)$ ve $\text{suppt}(b)$ kümeleri için simetrik farklarını düşünelim.

$$\text{suppt}(a) \triangle \text{suppt}(b) = (\text{suppt}(a) \setminus \text{suppt}(b)) \cup (\text{suppt}(b) \setminus \text{suppt}(a))$$

Bu durumda

$$\text{suppt}(a+b) = \text{suppt}(a) \triangle \text{suppt}(b)$$

olduğu açıktır. Tanım sebebiyle

$$wt(a+b) = |\text{suppt}(a) \triangle \text{suppt}(b)|$$

elde edilir. $a \preceq b$ olduğunu kabul edelim. Tanım gereği $\text{suppt}(a) \subseteq \text{suppt}(b)$ sağlanır.

Bu durumda,

$$\begin{array}{rcl} wt(a+b) & = & |\text{suppt}(a) \triangle \text{suppt}(b)| \\ & = & |\text{suppt}(a) \setminus \text{suppt}(b) \quad \cup \quad (\text{suppt}(b) \setminus \text{suppt}(a)| \\ & = & |(\text{suppt}(b) \setminus \text{suppt}(a)| \\ & = & |(\text{suppt}(b)| - |\text{suppt}(a)| \\ & = & wt(b) - wt(a). \end{array}$$

eşitlikleri elde edilir.

Diyelim ki $wt(a+b) = wt(b) - wt(a)$ eşitliği sağlansın. Lemma 2.1 sebebiyle

$$wt(a) = |\text{supp}(a)| = |\text{suppt}(a) \cap \text{suppt}(b)|$$

eşitliği elde edilir. Dolayısıyla $\text{suppt}(a) \subseteq \text{suppt}(b)$ olur. Sonuç olarak $a \preceq b$ sağlanır.

■

Teorem 2.3. *$C \subset \mathbb{F}_2^n$ ikili doğrusal bir kod olsun. Aşağıdakiler birbirine denktir:*

(i) *Birbirinden ve sıfırdan farklı her $a, b \in C$ için $wt(a+b) \neq wt(b) - wt(a)$ eşitsizliği sağlanır.*

(ii) *C kodu minimaldir.*

Kanıt. Lemma 2.2 den kolayca elde edilir. ■

Tanım. C doğrusal bir kod olsun. Eğer sıfırdan farklı kod sözcükleri için sadece iki farklı ağırlık değeri var ise, C koduna 2-ağırlıklı kod denir.

Örnek 6. $C = \{0000, 1110, 0111, 1001\}$ kodu için $wt(1110) = wt(0111) = 3$ ve $wt(1001) = 2$ olur. C kodunun, sıfırdan farklı kod sözcükleri için iki ağırlık değeri olduğu için C kodu 2-ağırlıklı bir koddur. C kodu aynı zamanda minimal bir koddur.

Teorem 2.4. *C, n uzunluklu, 2-ağırlıklı bir kod olsun. Ağırlıklar w_1 ve w_2 olmak üzere $0 < w_1 < w_2 < n$ koşulu sağlansın. Bu durumda, aşağıdaki önermeler sağlanır.*

(1) Eğer $w_2 \neq 2w_1$ ise, C minimaldir.

(2) Eğer C minimal ve w_1 tek sayı ise, o zaman $w_2 \neq 2w_1$ olur.

Kanıt. a ve b ağırlıkları sırasıyla w_1 ve w_2 olan iki kod sözcüğü olsun.

(1) $0 < w_1 < w_2 < n$ olduğu için $a + b$, C kodunun sıfırdan farklı bir kod sözcüğü olur. $w_2 \neq 2w_1$ olduğunu kabul edelim. C kodu minimal olmasın. Bu durumda en az iki kod sözcüğü a ve b için $a \preceq b$ ifadesi sağlanır ve sonuç olarak

$$|\mathrm{suppt}(a) \cap \mathrm{suppt}(b)| = |\mathrm{suppt}(a)| = wt(a).$$

eşitliği elde edilir. Lemma 2.1 sebebiyle

$$wt(a+b) = wt(b) - wt(a) = w_2 - w_1$$

eşitliği bulunur. $w_1 \neq 0$ olduğundan $wt(a+b) \neq w_2$ olur. C kodu 2-ağırlıklı bir kod olduğu için, $wt(a+b) = w_1$ olur. Dolayısı ile $w_2 = 2w_1$ sonucuna ulaşılır. Fakat bu sonuç varsayımla çelişir.

(2) C kodu minimal ve w_1 tek sayı olsun. $w_2 = 2w_1$ olsun.
$\text{suppt}(a) \cap \text{suppt}(b) \subseteq \text{suppt}(a)$ olduğundan Lemma 2.1 sebebiyle,

$$wt(a+b) \geq wt(b) - wt(a)$$

eşitsizliği elde edilir. $w_2 = 2w_1$ olduğu için, $wt(a+b) \geq w_1$ olur. C kodu 2-ağırlıklı bir kod olduğu için, ya $wt(a+b) = w_1$ ya da $wt(a+b) = w_2$ olmalıdır. w_1 tek olduğu için ve

$$wt(a+b) \;=\; wt(a) \;+\; wt(b) \;-\; 2|\text{suppt}(a) \cap \text{suppt}(b)|$$

ifadeleri sağlandığı için, $wt(a+b) \neq w_2$ ifadesi elde edilir.

Bu durumda $wt(a+b) = w_1$ olur. Lemma 2.1 sebebiyle, $|\text{suppt}(a) \cap \text{suppt}(b)| = |\text{suppt}(a)|$ olur. Dolayısı ile $a \preceq b$ elde edilir. Bu durum, C kodunun minimal olması ile çelişir.

■

Tanım. C doğrusal bir kod olsun. Eğer C kodunun sıfırdan farklı kod sözcükleri için, 3 farklı ağırlık değeri var ise, C koduna 3-ağırlıklı doğrusal kod denir.

Örnek 7. $C = \{0000, 1011, 0100, 1111\}$ kodu 3-ağırlıklı bir koddur. Bu kod minimal değildir.

Teorem 2.5. *C, n uzunluklu, 3-ağırlıklı ikili doğrusal kod olsun. Ağırlıklar w_1, w_2 ve w_3 olmak üzere $0 < w_1 < w_2 < w_3 < n$ eşitsizliği sağlansın. Eğer*

$w_2 \neq 2w_1$, $w_3 \neq 2w_1$, $w_3 \neq 2w_2$ ve $w_3 \neq w_2 + w_1$ koşulları sağlanıyor ise, C minimaldir.

Kanıt. $w_2 \neq 2w_1$, $w_3 \neq 2w_1$, $w_3 \neq 2w_2$, $w_3 \neq w_2+w_1$ koşulları sağlansın ve C minimal olmasın. Bu durumda Teorem 2.3 sebebiyle, birbirinden ve sıfırdan farklı öyle a, b kod sözcükleri vardır ki

$$wt(a+b) + wt(a) = wt(b) \qquad (1)$$

eşitliği sağlanır. a ve b birbirinden farklı olduğu için $wt(a+b) \neq 0$ olmalıdır ve $wt(a) \neq wt(b)$ sağlanır. Ayrıca $wt(a) \neq 0$ ve $wt(b) \neq 0$ olduğu için, bu durumda $wt(a+b) < wt(b)$ ve $wt(a) < wt(b)$ eşitsizlikleri sağlanır. $wt(b)$ için üç durum söz konusudur.

1.durum: $wt(b) = w_1$

$0 < w_1 < w_2 < w_3 < n$ eşitsizliği ve (1) eşitliğinden bu durum mümkün değildir.

2.durum: $wt(b) = w_2$

Eğer $wt(b) = w_2$ ise $wt(a+b) = wt(a) = w_1$ olur. Böylece $w_2 = wt(b) = 2w_1$ olur ve kabulümüz ile çelişir.

3.durum: $wt(b) = w_3$

Eğer $wt(b) = w_3$ ise, iki durum söz konusudur. Eğer $wt(a+b) \neq wt(a)$ ise, bu durumda $w_3 = w_1 + w_2$ sağlanır. Eğer $wt(a+b) = wt(a)$ ise, ya $w_3 = 2w_1$ ya da $w_3 = 2w_2$ olur. Bunlar varsayımlar ile çelişir.

Sonuç olarak, $wt(a+b) \neq wt(b) - wt(a)$ olmalıdır. C minimaldir.

■

2.3 Minimal Kodların Karakterizasyonu

Bu bölümde hem ikili hem de ikili olmayan minimal kodların karakterizasyonu, Bölüm 2.2'deki yöntemlerden farklı olan yöntemlerle çalışılmıştır. Minimal kodların parametreleri (uzunluk, ağırlık, boyut) arasındaki ilişkiler çalışılmış, uzunluk için üst sınır ve alt sınır değerleri incelenmiştir.

Bu kısımdaki sonuçlar ve kanıtları [13] numaralı makaleden çalışılmıştır. Kanıtlar, detaylandırılarak irdelenmiş ve yazılmıştır. Sonuçlarla ve kanıtlardaki yöntemlerle ilgili örneklere yer verilmiştir.

Tanım. $n \geq 0$ olmak üzere $x = (x_1, x_2, \ldots, x_n)$, $y = (y_1, y_2, \ldots, y_n) \in \mathbb{F}_q^n$ olan iki tane vektör için **skaler çarpım** şu şekilde tanımlanır;

$$\langle x, y \rangle := x \cdot y^T = \sum_{i=1}^{n} x_i y_i = x_1 y_1 + \cdots + x_n y_n$$

Tanım. Herhangi bir doğrusal $S \subseteq \mathbb{F}_q^n$ kodu için

$$S^{\perp} := \{y \in \mathbb{F}_q^n \mid \langle x, y \rangle = 0, \forall x \in S\}$$

kümesine S kodunun **duali** denir. $S^{\perp}$ de doğrusal bir koddur.

Önerme 2.6. *$S \subseteq \mathbb{F}_q^n$ doğrusal kodu için aşağıdaki ifadeler sağlanır:*

1. $S = (S^{\perp})^{\perp}$

2. $\dim(S) + \dim(S^{\perp}) = n.$

Not. $\dim(S) + \dim(S^{\perp}) = n$ sağlandığı için eğer S, $[n, k]_q$ kodu ise $S^{\perp}$, $[n, n-k]_q$ kodu olur. Sonlu cisimler ile çalıştığımız için, $S \cap S^{\perp} = \{0\}$ olmayabilir. $S = \{0000, 1100, 0011, 1111\}$ kodu için $S^{\perp} = \{0000, 1100, 0011, 1111\}$ ve $S \cap S^{\perp} = S$ olur.

Not. S ve $S^{\perp}$ arasında 4 farklı durum olabilir,

- $S^{\perp} \subseteq S$
- $S = S^{\perp}$ bu durumda, S koduna **kendine dual kod** denir.
- $S \subseteq S^{\perp}$ bu durumda S koduna **kendine dik kod** denir.
- $S \cap S^{\perp} = \{0\}$ bu durumda S koduna LCD kod denir.

Örnek 8. $C = \{0000, 0011, 1100, 1111\}$, $[4, 2]_2$ kodu hem kendine dik kod, hem de kendi dual bir koddur.

Örnek 9. $C = \{000, 111\}$ için $C^{\perp} = \{000, 110, 011, 101\}$ kodudur. $C \cap C^{\perp} = \{000\}$ olduğu için C, LCD kodudur.

Gözlem. *Eğer C, uzunluğu n olan kendi dual bir kod ise, $dim(C) = dim(C^{\perp})$ eşitliği sağlanır. Yani $dim(C^{\perp}) = \frac{n}{2}$ olur. Bu durumda, eğer uzunluk çift değil ise, kodun kendi dual olma ihtimali yoktur.*

k ve n, $k \leq n$ eşitsizliğini sağlayan iki tane pozitif tamsayı olsun. $d_1, \ldots, d_n \in \mathbb{F}_q^k$ olmak üzere $D := \{d_1, \ldots, d_n\}$, bir çoklu küme (multiset) düşünelim. Ayrıca, D içindeki en büyük doğrusal bağımsız alt kümenin eleman sayısı yani $\text{rank}(D) = k$ olsun.

$x \in \mathbb{F}_q^k$ için $c(x) = (xd_1^T, \ldots, xd_n^T)$ olarak tanımlansın.

$$C(D) = \{c(x), x \in \mathbb{F}_q^k\}$$

şeklinde bir küme tanımlayalım. Burada her $i \in \{1, ..., n\}$ için d_i^T, d_i vektörünün transpozunu göstermektedir.

Lemma 2.7. *Eğer $\{e_1, \ldots, e_k\}$, $\mathbb{F}_q^k$ için baz ise $\{c(e_1), \ldots, c(e_k)\}$, $C(D)$ için bazdır.*

Kanıt. Öncelikle $c(e_1), \ldots, c(e_k)$ vektörlerinin doğrusal bağımsız olduğunu gösterelim. $i \in \{1, \ldots, k\}$ ve $j \in \{1, \ldots, k\}$ olsun.

$$c(e_i) = (e_i d_1^T, \ldots, e_i d_n^T), e_i \in \mathbb{F}_q^k$$

$c(e_i)$'nin bir skaler ile çarpımını şu şekilde yazabiliriz.

$$\alpha_j c(e_i) = (\alpha_j e_i d_1^T, \ldots, \alpha_j e_i d_n^T), e_i \in \mathbb{F}_q^k, \alpha_j \in \mathbb{F}_q$$

Eğer

$$\alpha_1 c(e_1) + \cdots + \alpha_k c(e_k) = (\alpha_1 e_1 d_1^T, \ldots, \alpha_1 e_1 d_n^T) + \cdots + (\alpha_k e_k d_1^T, \ldots, \alpha_k e_k d_n^T) = 0$$

ise

$$((\alpha_1 e_1 + \cdots + \alpha_k e_k) d_1^T, \ldots, (\alpha_1 e_1 + \cdots + \alpha_k e_k) d_n^T) = 0$$

olur. Bu durumda

$$(\alpha_1 e_1 + \cdots + \alpha_k e_k) = 0$$

olur. $\{e_1, \ldots, e_k\}$, $\mathbb{F}_q^k$ için baz olduğundan $\alpha_1 = \alpha_2 = \cdots = \alpha_k = 0$ olur. Sonuç olarak $c(e_1), \ldots, c(e_k)$ doğrusal bağımsızdır.

$x \in \mathbb{F}_q^k$ için öyle $\alpha_1, \ldots, \alpha_k$ vardır ki $x = \alpha_1 e_1 + \cdots + \alpha_k e_k$ sağlanır.

$$c(x) = (x d_1^T, \ldots, x d_n^T)$$

$$c(x) = ((\alpha_1 e_1 + \cdots + \alpha_k e_k) d_1^T, \ldots, (\alpha_1 e_1 + \cdots + \alpha_k e_k) d_n^T)$$

$$c(x) = (\alpha_1 e_1 d_1^T + \cdots + \alpha_k e_k d_1^T, \ldots, \alpha_1 e_1 d_n^T + \cdots + \alpha_k e_k d_n^T)$$

$$c(x) = ((\alpha_1 e_1 d_1^T, \ldots, \alpha_1 e_1 d_n^T) + \cdots + (\alpha_k e_k d_1^T, \ldots, \alpha_k e_k d_n^T))$$

$$c(x) = \alpha_1 c(e_1) + \cdots + \alpha_k c(e_k)$$

Sonuç olarak $c(x) \in C(D)$, $c(e_1), \ldots, c(e_k)$ vektörlerinin doğrusal bileşimi olarak yazılır. ■

Önerme 2.8. *$C(D), [n, k]_q$ doğrusal koddur.*

Kanıt. Öncelikle $C(D) \subseteq \mathbb{F}_q^n$ bir alt uzay olduğunu gösterelim.

$x = 0$ için $c(x) = 0$ olur. $0 \in C(D)$ olduğundan $C(D) \neq \emptyset$ olur.

$c(x), c(y) \in C(D)$ olsun.

Eğer $c(x) = \{(xd_1^T, \ldots, xd_n^T), x \in \mathbb{F}_q^k\}$, $c(y) = \{(yd_1^T, \ldots, yd_n^T), y \in \mathbb{F}_q^k\}$ ise

$$c(x) - c(y) = (xd_1^T - yd_1^T, \ldots, xd_n^T - yd_n^T)$$

$$c(x) - c(y) = ((x-y)d_1^T, \ldots, (x-y)d_n^T)$$

olur. $\mathbb{F}_q^k$ vektör uzayı ve $x, y \in \mathbb{F}_q^k$ olduğundan $x - y \in \mathbb{F}_q^k$ olur. O zaman $c(x) - c(y) \in C(D)$ elde ederiz.

$\alpha \in \mathbb{F}_q$, $c(x) \in C(D)$ alalım.

$$\alpha c(x) = (\alpha x d_1^T, \ldots, \alpha x d_n^T)$$

olur. $\mathbb{F}_q^k$ vektör uzayı ve $x \in \mathbb{F}_q^k$ olduğundan $\alpha x \in \mathbb{F}_q^k$ olur. Bu durumda, $\alpha c(x) \in C(D)$ elde ederiz. $C(D) \subseteq \mathbb{F}_q^n$ olduğundan $C(D)$'nin kod sözcüklerinin uzunluğu n olur. $C(D)$'nin k-boyutlu olduğu Lemma 2.7 sebebiyle açıktır.

■

$C(D)$ kodunu karakterize edebilmek için bazı alt uzay ve alt kümeler tanımlayalım. $C(D) = \{c(x), x \in \mathbb{F}_q^k\}$ ve $y \in \mathbb{F}_q^k$ için

$$H(y) := y^{\perp} = \{x \in \mathbb{F}_q^k \mid \langle x, y \rangle = 0\}$$

$$H(y, D) := D \cap H(y) = \{x \in D \mid \langle x, y \rangle = yx^T = 0\}$$

$$V(y, D) := \text{span}(H(y, D))$$

kümeleri tanımlansın.

Önerme 2.9. *Yukarıda tanımlanmış kümeler için*

$$H(y, D) \subseteq V(y, D) \subseteq H(y)$$

içermeleri sağlanır.

Kanıt. $H(y,D) \subseteq V(y,D)$ içermesi tanımları sebebiyle açıktır. $H(y,D) \subseteq H(y)$ olduğu tanımdan açıktır. $H(y,D)$ bir küme ve $H(y)$ bir vektör uzayı olduğu için $\text{span}(H(y,D)) \subseteq H(y)$ sağlanır. Dolayısıyla $V(y,D) \subseteq H(y)$ içermesi sağlanır.

■

Örnek 10. $k = 3$, $n = 5$ ve $q = 2$ olsun.

$\mathbb{F}_2^3 = \{000, 100, 010, 001, 110, 101, 011, 111\}$ olmak üzere

$$d_1 = 100,\ d_2 = 101,\ d_3 = 110,\ d_4 = d_1 + d_2 = 001,\ d_5 = d_2 + d_3 = 011$$

seçelim ve

$$D = \{d_1, d_2, d_3, d_4, d_5\} \subseteq \mathbb{F}_2^3$$

kümesini düşünelim. Bu durumda $\text{rank}(D) = k = 3$ olacağı açıktır.

$x = 000$ için $c(x) = 00000$	$x = 110$ için $c(x) = 11001$
$x = 100$ için $c(x) = 11100$	$x = 101$ için $c(x) = 11111$
$x = 010$ için $c(x) = 00101$	$x = 011$ için $c(x) = 01110$
$x = 001$ için $c(x) = 01011$	$x = 111$ için $c(x) = 10010$

olur. Bu durumda

$$C(D) = \{00000, 11100, 00101, 01011, 11001, 11111, 01110, 10010\}$$

uzunluğu 5, boyutu 3 olan ikili bir kod olur. $y = 011 \in \mathbb{F}_2^3$ için hesaplamaları yapalım.

$$H(y) = \{000, 100, 011, 111\}$$

$$H(y,D) = \{100, 011\}$$

$$V(y, D) = \{000, 100, 011, 111\}$$

kümeleri için,

$$H(y, D) \subseteq V(y, D) \subseteq H(y)$$

içermelerinin sağlandığı görülür.

Önerme 2.10. *$c(x) \preceq c(y)$ ifadesinin sağlanması için gerekli ve yeterli koşul $H(y, D) \subseteq H(x, D)$ içermesinin sağlanmasıdır.*

Kanıt. $D = \{d_1, \ldots d_k\}$ kümesi için, tanım gereği $c(x) = (xd_1^T, \ldots xd_k^T)$ ve $c(y) = (yd_1^T, \ldots yd_k^T)$ olarak yazılır. $c(x) \preceq c(y)$ olsun. Bu durumda $\text{suppt}(c(x)) \subseteq \text{suppt}(c(y))$ olur. $a \in H(y, D) = \{d \in D : yd^T = 0\}$ alalım. Bu durumda $ya^T = 0$ olur. Bu durumda $c(y)$ kod sözcüğünde ya^T nin bulunduğu koordinat sıfırdır. $\text{suppt}(c(x)) \subseteq \text{suppt}(c(y))$ olduğu için, $c(x)$ kod sözcüğünün de bu koordinatı sıfır olur. Dolayısıyla $xa^T = 0$ olur. Yani $a \in H(x, D)$ olur.

$H(y, D) \subseteq H(x, D)$ olsun. $i \in \text{suppt}(c(x))$ olsun. Bu durumda $xd_i^T \neq 0$ olur. Tanım gereği, $d_i \notin H(x, D)$ olur. Kabulümüz gereği, $d_i \notin H(y, D)$ elde edilir. Dolayısıyla $yd_i^T \neq 0$ sağlanır. Sonuç olarak $i \in \text{suppt}(c(y))$ olur.

■

Örnek 11. (örnek 10'nun devamı)

$x = 010$ için $c(x) = 00101$ olur. Bu durumda

$$H(x) = \{000, 100, 001, 101\}, \quad H(x, D) = \{100, 101\}$$

olarak elde edilir.

$y = 101$ için $c(y) = 10111$ olur.

$$H(y) = \{000, 101, 010, 111\}, \quad H(y, D) = \{101\}$$

kümeleri elde edilir. $c(x) \preceq c(y)$ olduğu açıktır. $H(y,D) \subseteq H(x,D)$ sağlandığını görebiliriz.

Teorem 2.11. *$y \in \mathbb{F}_q^k \setminus \{0\}$ olsun. Aşağıdaki koşullar birbirine denktir:*

1. *$c(y) \in C(D)$ minimal bir kod sözcüktür.*
2. *$\dim V(y,D) = k-1$.*
3. *$V(y,D) = H(y)$.*

Kanıt. $(1 \Rightarrow 3)$ $c(y) \in C(D)$ minimal kod sözcüğü olsun ve $V(y,D) \neq H(y)$ olduğunu kabul edelim. Önerme 2.9 sebebiyle, $V(y,D) \subset H(y)$ olur. Dolayısıyla $\dim(V(y,D)) < \dim(H(y)) = k-1$ olur. O zaman $\dim(V(y,D)) \leq k-2$.

$$\dim(V(y,D)) + \dim(V(y,D)^{\perp}) = k$$

eşitliğinden $\dim(V(y,D)^{\perp}) \geq 2$ elde edilir. Tanım gereği, $y \in V(y,D)^{\perp}$ olur. Bu durumda $x \in V(y,D)^{\perp}$ vardır ki x ve y doğrusal bağımsızdır. $d_i \in H(y,D) \subseteq V(y,D)$ alalım. $x \in V(y,D)^{\perp}$ olduğu için $xd_i^T = 0$ olur. Bu durumda tanım gereği $d_i \in H(x,D)$ olur. Yani $H(y,D) \subseteq H(x,D)$ olur. Teorem 2.10 sebebiyle $c(x) \preceq c(y)$ olur. Aynı zamanda x, y doğrusal bağımsız olduğu için, $c(x)$ ve $c(y)$ doğrusal bağımsız olur. Tanım gereği $c(y)$ minimal olamaz.

$(3 \Rightarrow 1)$ $V(y,D) = H(y)$ olsun ve $c(x) \preceq c(y)$ sağlansın. Önerme 2.10 sebebiyle $H(y,D) \subseteq H(x,D)$ içermesi sağlanır. Dolayısıyla $V(y,D) \subseteq V(x,D)$ olur. Dahası $H(y) = V(y,D) \subseteq V(x,D) \subseteq H(x)$ ifadesi sağlanır. Tanımları gereği $\dim(H(y)) = k-1 = \dim(H(x))$ olur . Dolayısıyla $H(x) = H(y)$ elde edilir. $H(x)$, x'in duali olduğu için ve altuzayın dualinin duali kendise eşit olduğundan $x \in H(x)^{\perp}$ olur. $H(y) = H(x)$ olduğundan $H(y)^{\perp} = H(x)^{\perp}$

sağlanır. Benzer şekilde $y \in H(y)^{\perp}$ olur, yani $H(y)^{\perp} = \text{span}(y)$ sağlanır. Sonuç olarak

$$\text{span}(x) = H(x)^{\perp} = H(y)^{\perp} = \text{span}(y)$$

elde edilir. Bu durumda, öyle $a \in \mathbb{F}_q - \{0\}$ vardır ki $x = ay$ yazılır. Daha açık yazmak gerekirse,

$$c(x) = (xd_1^T, \ldots, xd_n^T)$$

$$c(x) = (ayd_1^T, \ldots, ayd_n^T)$$

$$c(x) = a(yd_1^T, \ldots, yd_n^T)$$

Dolayısıyla

$$c(x) = ac(y)$$

elde ederiz. Bu da $c(y)$'nin minimal olduğunu gösterir.

$(2 \Rightarrow 3)$ $\dim(V(y, D)) = k - 1$ olduğunu kabul edelim. Önerme 2.9 sebebiyle $V(y, D) \subseteq H(y)$ içermesinin sağlandığını biliyoruz. Tanımı gereği $\dim(H(y)) = k - 1$ olduğu için, kabulümüz gereği $V(y, D) = H(y)$ olur.

$(3 \Rightarrow 2)$ $V(y, D) = H(y)$ olduğunu kabul edelim. $\dim(H(y)) = k - 1$ olduğu için $\dim V(y, D) = k - 1$ olur.

■

Teorem 2.12. *Aşağıdaki önermeler birbirine denktir:*

1. *$C(D)$ kodu minimaldir.*
2. *Herhangi bir $y \in \mathbb{F}_q^k \setminus \{0\}$ için $\dim V(y, D) = k - 1$.*
3. *Herhangi bir $y \in \mathbb{F}_q^k \setminus \{0\}$ için $V(y, D) = H(y)$.*

Kanıt. Teorem 2.11 sebebiyle açıktır. ■

Örnek 12. $k = 2$, $n = 3$ ve $q = 2$ olsun.

$\mathbb{F}_2^2 = \{00, 10, 01, 11\}$ vektör uzayını düşünelim.

$$d_1 = 10, d_2 = 01, d_3 = d_1 + d_2 = 11$$

elemanlarını seçelim ve $D = \{d_1, d_2, d_3\}$ kümesini düşünelim.

$x = 00$ için $c(x) = 000$ $\quad$ $x = 01$ için $c(x) = 011$

$x = 10$ için $c(x) = 101$ $\quad$ $x = 11$ için $c(x) = 110$

şeklinde hesaplanır.

$$C(D) = \{000, 011, 110, 101\}$$

$y \in \mathbb{F}_2^2$ için hesaplamaları yapalım.

$y = 10$ için $H(y) = \{00, 01\}$, $H(y, D) = \{01\}$, $V(y, D) = \{00, 01\}$

$y = 01$ için $H(y) = \{00, 10\}$, $H(y, D) = \{10\}$, $V(y, D) = \{00, 10\}$

$y = 11$ için $H(y) = \{00, 11\}$, $H(y, D) = \{11\}$, $V(y, D) = \{00, 11\}$

Teorem 2.12'in koşulları sağlanır ve $C(D)$ kodu minimaldir.

Örnek 13. Örnek 10'u düşünelim. $y = 101$ için

$$H(y) = \{000, 010, 101, 111\}$$

$$H(y, D) = \{101\}$$

$$V(y, D) = \{000, 101\}$$

$H(y) \neq V(y, D)$ olduğundan Teorem 2.12 koşulları sağlanmaz.

$$C(D) = \{0000, 11100, 00101, 01011, 11001, 11111, 01110, 10010\}$$

kodu minimal kod olmaz.

Teorem 2.12'de, $C(D)$ kodunun minimal olması ile ilgili gerekli ve yeterli koşullar sunulmuştur.

Aşağıdaki önerme herhangi bir doğrusal C kodu için D kümesi bulabileceğimizi ve $C = C(D)$ eşitliğini görebileceğimizi kanıtlamaktadır. Dolayısı ile Teorem 2.12, herhangi bir doğrusal kodun minimal olması için gerekli ve yeterli koşulları sunmuştur. Önerme 2.13 ve kanıtı, [13] makalesinde açık bir şekilde yazılmamıştır. Bütünlük için aşağıdaki haliyle yer verilmiştir.

Önerme 2.13. *C doğrusal bir kod olsun. Bu durumda öyle bir çoklu küme D vardır ki $C = C(D)$ olur.*

Kanıt. $C \subseteq \mathbb{F}_q^n$, k boyutlu doğrusal bir kod ve $\{c_1, c_2, ..., c_k\} \in C$, C için bir baz olsun. Her $i \in \{1, .., k\}$ için $c_i = (c_{i1}, ..., c_{in})$ şeklinde yazalım. Sonuç olarak

$$\begin{pmatrix} c_{11} & c_{12} & ...c_{1n} \\ c_{21} & c_{22} & ...c_{2n} \\ \vdots & \vdots & \vdots \\ c_{k1} & c_{k2} & ...c_{kn} \end{pmatrix}$$

matrisi C için üreteç matrisi olur.

Bu durumda her $i \in \{1, \ldots, n\}$ için $d_i = (c_{1i}, c_{2i}, \ldots, c_{ki})$ şeklinde seçelim, yani $D = \{d_1, \ldots, d_n\}$ kümesini üreteç matrisinin sütunlarının kümesi olarak seçelim. $c \in C$ alalım. Bu durumda öyle $a_1, \ldots, a_k \in \mathbb{F}_q^k$ skalerleri vardır ki $c = a_1c_1 + \cdots + a_kc_k$ şeklinde yazılır.

Yani

$$c = (a_1, \ldots, a_k) \begin{pmatrix} c_{11} & c_{12} & \ldots c_{1n} \\ c_{21} & c_{22} & \ldots c_{2n} \\ \vdots & \vdots & \vdots \\ c_{k1} & c_{k2} & \ldots c_{kn} \end{pmatrix}$$

şeklinde yazılır. Dolayısıyla $x = (a_1, \ldots, a_k) \in \mathbb{F}_q^k$ için $c = (xd_1^T, \ldots, xd_n^T)$ yazılmış olur. Yani $c = c(x) \in C(D)$ olur. Böylece $C \subseteq C(D)$ sağlanmış olur.

Öte taraftan D kümesinin tanımı gereği $c(x) = (xd_1^T, \ldots, xd_n^T) \in C$ sağlanır. Sonuç olarak $C = C(D)$ elde edilir. ■

Teorem 2.14. *$D_1 \subseteq D_2 \subseteq \mathbb{F}_q^k$, $\text{rank}(D_1) = \text{rank}\ (D_2) = k$ koşulunu sağlayan iki çoklu küme olsun. Eğer $C(D_1)$ minimal ise $C(D_2)$ de minimaldir.*

Kanıt. $y \in \mathbb{F}_q^k - \{0\}$ olsun. $D_1 \subseteq D_2$ olsun.

$$H(y, D_1) = H(y) \cap D_1 \subseteq H(y) \cap D_2 = H(y, D_2)$$

olacağı açıktır. Tanım gereği

$$V(y, D_1) = \text{span}H(y, D_1) \subseteq \text{span}H(y, D_2) = V(y, D_2) \subseteq H(y)$$

olur. $C(D_1)$ minimal olduğundan Teorem 2.12 sebebiyle $V(y, D_1) = H(y)$ olur. Dolayısıyla $V(y, D_2) = H(y)$ olur. Yine Teorem 2.12 sebebiyle $C(D_2)$ minimaldir. ■

Örnek 14.

$$D_1 = \{101, 111, 001, 011, 100, 110\}$$

$$C(D_1) = \{000000, 110011, 010101, 111100, 100110, 001111, 101001, 011010\}$$

$C(D_1)$ minimal koddur.

$$D_2 = \{101, 111, 001, 011, 100, 110, 001\}$$

$C(D_2) = \{0000000, 1100110, 0101010, 1111001, 1001100, 0011111, 1010011,$ $0110101\}$ $D_1 \subseteq D_2$ olduğundan ve $C(D_1)$ minimal olduğundan $C(D_2)$ de minimaldir.

Önerme 2.15. *Eğer $D = \mathbb{F}_q^k$ ise $C(D)$, $[q^k, k]_q$ minimal doğrusal koddur.*

Kanıt.

$$C(D) = \{(xd_1^T, \ldots, xd_n^T), x \in \mathbb{F}_q^k\}$$

olduğu için, $C(D)$'nin uzunluğu $|D| = |\mathbb{F}_q^k| = q^k$ kadar olur.

Ayrıca $D = \mathbb{F}_q^k$ olduğundan ve $H(y, D) = D \cap H(y)$ eşitliğinden $H(y, D) = H(y)$ olur. Önerme 2.9 sebebiyle $V(y, D) = H(y)$ eşitliği elde edilir. Teorem 2.12 sebebiyle $C(D)$ minimal olur. ■

Örnek 15.

$$D = \mathbb{F}_2^2 = \{00, 10, 01, 11\}$$

$$C(D) = \{0000, 0101, 0011, 0110\}$$

olur. $C(D)$, $[4, 2]_2$ minimal koddur.

2.3.1 Minimal kodların uzunlukları

Bu bölümde minimal kodların parametrelerine odaklanılmıştır. Minimal kodların olası uzunlukları için alt sınır ve üst sınır [13] ve [2] numaralı makalelerde verilmiştir. Bu kısımda [13] numaralı makaledeki sonuçlar detaylı bir şekilde incelenmiştir.

Şimdi minimal doğrusal kodların olası uzunluklarının kümesini tanımlayalım.

$N(k; q) := \{n \in N^+ | [n, k]_q$ parametrelerine sahip olan minimal doğrusal kod vardır.$\}$

Önerme 2.15 sebebiyle $D = \mathbb{F}_q^k$ iken $C(D)$, $[q^k, k]_q$ minimal bir kod olduğunu biliyoruz. O zaman $q^k \in N(k; q)$ olur, dolayısıyla $N(k; q) \neq \emptyset$ elde edilir.

$N(k; q)$ kümesinin minimumunu $n(k; q)$ ile göstereceğiz, yani

$$n(k; q) := \min N(k; q)$$

şeklinde yazacağız.

Önerme 2.16. *Herhangi bir pozitif tamsayı n için $[n,k]_q$ minimal doğrusal kodu olması için gerekli ve yeterli koşul $n \geq n(k;q)$ eşitsizliğinin sağlanmasıdır.*

Kanıt. n pozitif tamsayı için, $[n,k]_q$ lineer kodu minimal olsun. $n(k;q)$ tanımı gereği $n \geq n(k;q)$ eşitsizliği sağlanır.

$n \geq n(k;q)$ eşitsizliği sağlansın. $n(k,q)$'nun tanımından öyle D_1 kümesi vardır ki $|D_1| = n(k;q)$ ve $C(D_1)$ minimaldir. $D_2 \subseteq \mathbb{F}_q^k$, $|D_2| = n - n(k;q)$ koşulunu sağlayan başka bir çoklu küme ve $D = D_1 \cup D_2$ olsun. $|D| = |D_1| + |D_2| = n(k;q) + n - n(k;q) = n$. O zaman $D_1 \subseteq D$ olur. Ayrıca $\text{rank}(D_1) = \text{rank}(D)$ olur. Teorem 2.14 sebebiyle $C(D)$ minimal olur. ■

$\{e_1, e_2, \ldots, e_k\}$ kümesi $\mathbb{F}_q^k$ vektör uzayı için standart baz olsun. $D^{'}$ ve $D^{''}$ aşağıdaki gibi tanımlayalım:

$$D^{'} = \{e_1, e_2, \ldots, e_k\} \text{ ve } D^{''} = \{e_i + ae_j | 1 \leq i < j \leq k,\ a \in \mathbb{F}_q^*\}.$$

$D_0 := D^{'} \cup D^{''}$ tanımlayalım.

Örnek 16. $\mathbb{F}_q^k = \mathbb{F}_2^3$ için

$$D^{'} = \{100, 010, 001\},\ D^{''} = \{110, 011, 101\}$$

$$D_0 = \{100, 010, 001, 110, 101, 011\}.$$

Önerme 2.17. *$D^{'}$, $D^{''}$ ve D_0 tanımları yukarıdaki gibi olmak üzere $C(D_0)$, $[(q-1)\frac{k\cdot(k-1)}{2} + k, k]_q$ minimal doğrusal bir koddur.*

Kanıt. D_0 çoklu kümesinin eleman sayısı kodun uzunluğunu belirler. O zaman önce $|D_0|$'a karar verelim. $D_0 = D^{'} \cup D^{''}$ olduğundan $|D_0| = |D^{'}| + |D^{''}|$ olur. $D^{'}$ tanımından dolayı $|D^{'}| = k$ olur. Şimdi $|D^{''}|$'yi hesaplayalım. $\{e_1, e_2, \ldots, e_k\}$'dan yani k tane elemandan 2 tanesini seçeceğiz, kombinasyon

hesabı kullanalım. $C(k,2) = \frac{k\cdot(k-1)}{2}$ tane seçenek var. Katsayıyı yani a'yı $\mathbb{F}_q^*$'dan seçeceğiz. $\mathbb{F}_q^* = \mathbb{F}_q - \{0\}$ olduğundan $|\mathbb{F}_q^*| = q-1$ olur.O zaman $|D''| = (q-1)^{\frac{k\cdot(k-1)}{2}}$ olur. Sonuç olarak $|D_0| = (q-1)^{\frac{k\cdot(k-1)}{2}} + k$ elde ederiz.

Tanımlar düşünüldüğünde $\text{rank}(D_0) = \text{rank}(D')$ olur. D' kümesinin tanımı gereği $\text{rank}(D') = k$ olur. Böylece $\text{rank}(D_0) = k$ elde edilir. Önerme 2.15 sebebiyle $C(D)$, k-boyutludur. $y \in \mathbb{F}_q^k - \{0\}$ alalım. Tanımı gereği $\dim H(y) = k-1$ dir. D' kümesinin $\mathbb{F}_q^k$ için standart baz olması sebebiyle, $H(y)$ için baz D_0 kümesinin bir alt kümesi olacaktır. Dolayısıyla $\text{rank}(H(y,D)) = k-1$ olacaktır. Yani $\dim V(y,D) = k-1$ olur. Theorem 2.11 sebebiyle $C(D_0)$ minimaldir. ■

Önerme 2.18. *Eğer* $D = \{x \in \mathbb{F}_q^k - \{0\} \mid wt(x) \leq 2\}$ *ise* $C(D)$ *minimaldir.*

Kanıt. $D_0 = D' \cup D''$ ile tanımladığımız küme, D'nin alt kümesidir. Önerme 2.17 sebebiyle $C(D_0)$'ın minimal olduğunu biliyoruz. O zaman Önerme 2.14 sebebiyle $C(D)$ minimaldir. ■

Önerme 2.19. *D elemanları $\mathbb{F}_q^k - \{0\}$ kümesinden olan bir çoklu küme olsun. Eğer $C(D)$, $[n,k]_q$ minimal kod ise $n > q(k-1)$ sağlanır.*

Kanıt. Eğer $C(D)$, $[n,k]_q$ kod ise, $|D| = n$ dir.

$$X = X(D) := \{(y,d) \mid \langle y,d\rangle = 0, y \in \mathbb{F}_q^k, d \in D\}$$

kümesini düşünelim. Bu tanıma göre X'in eleman sayısını iki farklı şekilde hesaplayabiliriz. Bunlardan ilki

$$|X| = \sum_{(y,d)\in X} 1 = \sum_{d\in D} \sum_{y\in\mathbb{F}_q^k - \{0\}(y,d)\in X} 1 = \sum_{d\in D}(q^{k-1}-1) = n\cdot(q^{k-1}-1) \quad (1)$$

elde ederiz.

$$|X| = \sum_{(y,d)\in X} 1 = \sum_{y\in\mathbb{F}_q^k-\{0\}} \sum_{d\in D,(y,d)\in X} 1 = \sum_{y\in\mathbb{F}_q^k-\{0\}} |H(y,D)|$$

elde ederiz. $C(D)$ minimal olduğundan Önerme 2.12 sebebiyle $\dim(V(y,D)) = k-1$ ve $V(y,D) = \text{span}(H(y,D))$ olduğunu biliyoruz. $H(y,D)$ tanımından dolayı elaman sayısı için iki seçenek var; ya boyut kadar elemanı vardır ya da boyuttan daha fazla elemanı vardır ama boyut kadar doğrusal bağımsız elemanı vardır. O zaman $|H(y,D)| \geq k-1$.

$$|X| = \sum_{y\in\mathbb{F}_q^k-\{0\}} |H(y,D)| \geq \sum_{y\in\mathbb{F}_q^k} (k-1) = (q^k-1)(k-1)$$

O zaman

$$|X| \geq (q^k-1)(k-1) \quad (2)$$

elde ederiz. (1) ve (2)'den

$$n \cdot (q^{k-1}-1) \geq (q^k-1)(k-1)$$

$$\begin{array}{rcl} n & \geq & \frac{q^k-1}{q^{k-1}-1}(k-1) \\ & = & \frac{q^k-q+q-1}{q^{k-1}-1}(k-1) \\ & = & \frac{q(q^{k-1}-1)+q-1}{q^{k-1}-1}(k-1) \\ & = & \frac{q(q^{k-1}-1)(k-1)}{q^{k-1}-1} + \frac{q-1}{q^{k-1}-1}(k-1) \\ & \geq & q(k-1) \end{array}$$

■

Önerme 2.20. *$n(k;q)$ değeri için aşağıdaki eşitsizlikler sağlanır:*

$$q(k-1) < n(k;q) \leq (q-1)\frac{k\cdot(k-1)}{2} + k.$$

Kanıt. Önerme 2.17 ve Önerme 2.19 kullanılarak elde edilir. ■

Örnek 17. $k = 2$ için;

$$q(2-1) < n(2;q) \leq (q-1)\frac{2\cdot(2-1)}{2} + 2$$

$$q < n(2;q) \leq (q-1) + 2$$

$$n(2;q) = q + 1$$

Boyutu 2 olan kodlar için minimum uzunluk $q+1$'dir.

Örnek 18. $k = 3$ ve $q = 2$ için

$$2(3-1) < n(3,2) \leq (2-1)\frac{3(3-1)}{2} + 3$$

$$4 < n(3,2) \leq 6$$

0 zaman $n(3,2) \in \{5,6\}$ olabilir. Bir sonraki bölümde 3-boyutlu, 5 uzunluklu minimal kod olmadığını kanıtlayacağız. Bu kanıtı verebilmek için aşağıdaki teoreme ihtiyacımız olacak.

Teorem 2.21. [2, Teorem 4.3] *C, $[n,k]_q$ minimal bir kod, $k \geq 2$ ve $wt(C) = d$ olsun. Bu durumda $d \geq k + q - 2$ sağlanır.*

$q = 2$ için aynı sonucun elde edildiği başka bir teorem için [1] numaralı makalede Teorem 2.8' e bakılabilir.

Örnek 19. $k = 4$ ve $q = 2$ için

$$2(4-1) < n(4,2) \leq (2-1)\frac{4(4-1)}{2} + 4$$

$$6 < n(4,2) \leq 10$$

0 zaman $n(4,2) \in \{7,8,9,10\}$ olabilir.

Not. İkili minimal kodlar için $q = 2$ olduğundan $d \geq k$ sağlanır.

Bölüm 3

Düşük Boyutlu İkili Minimal Kodlar

Bu bölümde iki boyutlu ve üç boyutlu minimal kodlar için uzunluklar çalışılmıştır. Sonrasında minimal kodların dualleri çalışılarak, düşük boyutlu minimal kodların duallerinin minimal olduğu durumlar incelenmiştir.

3.1 İki Boyutlu İkili Minimal Kodlar

Bu bölümde iki boyutlu ikili minimal kodların özellikleri ve uzunlukları çalışılmıştır. İki boyutlu minimal kodlar, sabit ağırlıklı ve sabit ağırlıklı olmayan minimal kodlar olarak iki kod ailesi şeklinde düşünülmüştür. 3-ağırlıklı minimal bir kodun uzunluğu için alt sınır verilmiştir. Örnek 17'de açıklandığı üzere iki boyutlu kodlar için $n(2,2) = 3$'tür. Bu bilgi ışığında 3-ağırlıklı iki boyutlu minimal kodlar düşünülmüş ve uzunluk değeri için daha iyi bir alt sınır verilmiştir. Ayrıca bu kod ailesi için ağırlık için de alt sınır belirlenmiştir.

Önerme 3.1. *$C = \{0, c_1, c_2, c_3\}$ ikili bir kod olsun. Bu durumda, aşağıdakiler birbirine denktir:*

1) C kodu minimaldir.

2) Her $j,k \in \{1,2,3\}$ *için* $\text{suppt}(c_k) \cap \text{suppt}(c_j) \neq \emptyset$ *eşitsizliği sağlanır ve eğer* $j,k \in \{1,2,3\}$ *için* $wt(c_j) \leq wt(c_k)$ *oluyor ise* $|\text{suppt}(c_k) \cap \text{suppt}(c_j)| < wt(c_j)$ *eşitsizliği sağlanır.*

Kanıt. C minimal olsun ve her $j,k \in \{1,2,3\}$ için $\text{suppt}(c_k) \cap \text{suppt}(c_j) = \emptyset$ olsun. Bu durumda $\text{suppt}(c_k + c_j) = \text{suppt}(c_k) \cup \text{suppt}(c_j)$ olur. Dolayısıyla $\text{suppt}(c_j) \subseteq \text{suppt}(c_j + c_k)$ elde edilir. Bu da C kodunun minimal olması ile çelişir.

C minimal ve $wt(c_j) \leq wt(c_k)$ olsun. $|\text{suppt}(c_k) \cap \text{suppt}(c_j)| = wt(c_j)$ olduğunu kabul edelim. Bu durumda $\text{suppt}(c_j) \subset \text{suppt}(c_k)$ olur ve C minimal olmaz. Dolayısıyla $|\text{suppt}(c_k) \cap \text{suppt}(c_j)| < wt(c_j)$ sağlanır.

2)'deki koşulların sağlandığını kabul edelim. C kodunun minimal olmadığını kabul edelim. Bu durumda $i,k \in \{1,2,3\}$ vardır ve $\text{suppt}(c_i) \subseteq \text{suppt}(c_k)$ sağlanır. Bu durumda $\text{suppt}(c_i) \cap \text{suppt}(c_k) = \text{suppt}(c_i)$ olur. Dolayısıyla

$$|\text{suppt}(c_i) \cap \text{suppt}(c_k)| = wt(c_i)$$

elde edilir. Bu da kabulümüz ile çelişir. C minimaldir.

■

Önerme 3.2. *C, 2-boyutlu ikili doğrusal bir kod olsun. Eğer C sabit ağırlıklı ise, ağırlık tek sayı olamaz.*

Kanıt. C, 2-boyutlu ikili doğrusal kod olsun. Bu durumda $C = \{0, c_1, c_2, c_3\}$, $c_3 = c_1 + c_2$ olacak şekilde yazabiliriz. C kodunun ağırlığının tek olduğunu varsayalım. Lemma 2.1 yardımıyla

$$wt(c_3) = wt(c_1) + wt(c_2) - 2|\text{suppt}(c_1) \cap \text{suppt}(c_2)|$$

formülünü yazabiliriz. $wt(c_1)$ ve $wt(c_2)$ tek olduğu için, $wt(c_3)$ çift olur. C kodu sabit ağırlıklı olduğu için, bu bir çelişkidir. ■

Önerme 3.3. *C, 2-boyutlu, ağırlığı a olan sabit ağırlıklı ikili doğrusal bir kod olsun. Bu durumda her $v, u \in C$ için*

$$|\text{suppt}(v) \cap \text{suppt}(u)| = \frac{a}{2}$$

sağlanır.

Kanıt. $v, u \in C$ olsun. Bu durumda $C = \{0, u, v, u+v\}$ şeklinde yazabiliriz. Lemma 2.1 yardımıyla da $wt(u+v) = wt(u) + wt(v) - 2|\text{suppt}(u) \cap \text{suppt}(v)|$ eşitliğini yazabiliriz. C ağırlığı a olan sabit ağırlıklı bir kod olduğu için,

$$wt(u+v) = wt(u) = wt(v) = a$$

olur. Dolayısıyla $|\text{suppt}(u) \cap \text{suppt}(v)| = \frac{a}{2}$ elde ederiz.

■

Önerme 3.4. *C, 2-boyutlu, ağırlığı a olan sabit ağırlıklı ikili doğrusal bir kod olsun. Bu durumda C'nin uzunluğu en az $\frac{3}{2}a$ olmalıdır.*

Kanıt. $C = \{0, c_1, c_2, c_3\}$ şeklinde yazabiliriz. Önerme 3.3 sebebiyle

$$|\text{suppt}(c_1) \cap \text{suppt}(c_2)| = \frac{a}{2}$$

olur. $wt(c_1) = wt(c_2) = a$ olacağı için genellemeyi kaybetmeden

$$c_1 = \underbrace{111...1111}_{a \ tane}0000...$$

ve

$$c_2 = \underbrace{000..0}_{\frac{a}{2}\ tane}\underbrace{111...11}_{\frac{a}{2}\ tane}\underbrace{111..1}_{\frac{a}{2}\ tane}0000..$$

şeklinde yazabiliriz. Bu durumda

$$c_1 + c_2 = \underbrace{1111...111}_{\frac{a}{2}\ tane}\underbrace{000...000}_{\frac{a}{2}\ tane}\underbrace{1111...111}_{\frac{a}{2}\ tane}000...$$

olur. Dolayısıyla uzunluk en az $\frac{3a}{2}$ olmak zorundadır.

■

Önerme 3.5. *C, 2-boyutlu sabit ağırlıklı ikili doğrusal bir kod olsun. Bu durumda C minimaldir.*

Kanıt. C, 2-boyutlu ağırlığı a olan sabit ağırlıklı bir kod olsun. Bu durumda Önerme 3.3 yardımıyla, her $v, u \in C$ için

$$|\text{suppt}(u) \cap \text{suppt}(v)| = \frac{a}{2}$$

olur. Dolayısıyla $|\text{suppt}(u) \cap \text{suppt}(v)| < a = wt(u) = wt(v) = wt(u+v)$ olur. Bu durumda Önerme 3.1 yardımıyla C minimaldir.

■

Önerme 3.6. *C, uzunluğu $n > 1$ boyutu $k > 1$ olan bir kod olsun. Eğer C minimal bir kod ise ağırlığı 1 ve n olan kod sözcük içeremez.*

Kanıt. C minimal kod olsun. $v \in C$ elemanı ağırlığı bir olan bir eleman olsun. Genelliği bozmadan v'nin birinci koordinatının sıfırdan farklı olduğunu kabul edelim. $k > 1$ olduğu için C kodunun içinde v'den farklı bir w kod sözcüğü vardır. Eğer w kod sözcüğünün birinci koordinatı sıfırdan farklı olursa $\text{suppt}(v) \subset \text{suppt}(w)$ olur. Dolayısıyla C kodu minimal olamaz. Eğer w kod sözcüğünün birinci koordinatı sıfır olursa o zaman $v+w$ kod sözcüğünün birinci koordinatı sıfırdan farklı olur ve $\text{suppt}(v) \subset \text{suppt}(v+w)$ olur. Bu durumda da C minimal olamaz. Eğer u ağırlığı n olan bir kod sözcüğü ise, bu durumda sıfırdan farklı diğer elemanların desteği u kod sözğünün desteği içinde kalır. Bu durumda kod C minimal olamaz.

Sonuç olarak, C minimal kodu ağırlığı bir ve ağırlığı n olan kod sözcüğü içeremez.

■

Sonuç 3.7. *Eğer C uzunluğu $n > 1$ ve boyutu $k > 1$ olan minimal bir kod ise, C kodunun minimum ağırlığı en az iki olmalıdır.*

Önerme 3.8. *C, 2 boyutlu, 3 uzunluklu ikili bir kod olsun. Bu durumda aşağıdakiler birbirine denktir:*

1) C minimaldir.

2) C, ağırlığı 2 olan sabit ağırlıklı bir koddur.

Kanıt. C minimal olsun. Önerme 3.6 sebebiyle ağırlığı 1 ve 3 olan kod sözcük içeremez. O zaman C kodunun sıfırdan farklı elemanlarının ağırlığı 2 dir. Dolayısıyla sabit ağırlıklı bir koddur.
C, ağırlığı 2 olan sabit ağırlıklı kod olsun. Bu durumda

$$C = \{000, 110, 011, 101\}$$

olur. Minimal olduğu açıktır. ■

İki boyutlu ikili kodlarda bütün minimal kodların sabit ağırlıklı olduğu tek uzunluk 3 tür. Örneğin 2-boyutlu 4 uzunluklu kodlarda sabit ağırlıklı olmayan kodlar da minimal olabilmektedir.

Örnek 20. $C = \{0000, 1100, 0110, 1010\}$ sabit ağırlıklı minimal bir kod iken, $C = \{0000, 1100, 0111, 1011\}$ sabit ağırlıklı olmayan minimal bir koddur.

Bu nedenle bu kısımdan sonra minimal kodları, sabit ağırlıklı minimal kodlar ve sabit ağırlıklı olmayan minimal kodlar şeklinde iki aile olarak düşüneceğiz.

Önerme 3.9. *C, 2 boyutlu, 4 uzunluklu ve sabit ağırlıklı minimal bir kod olsun. Bu durumda C aşağıdakilerden biridir:*

1) $C = \{0000, 1100, 1010, 0110\}$,

2) $C = \{0000, 1100, 1001, 0101\}$,

3) $C = \{0000, 1010, 1001, 0011\}$.

Kanıt. C kodu sabit ağırlıklı olduğu için ve minimal olduğu için, Önerme 3.6 ve Önerme 3.2 sebebiyle, $wt(C) = 2$ dir. $\{x, y\}$, C için bir baz olsun. Bu durumda C minimal olduğu için, $|\text{suppt}(x) \cap \text{suppt}(y)| = 1$ olmalı ve $x + y = 1111$ olmamalıdır. Bu koşulu sağlayan ve farklı kodları üreten (x, y) ikilileri için olası bütün adaylar $\{(1100, 1010), (1100, 1001), (1010, 0011)\}$ olur. ■

Önerme 3.10. *C, 2 boyutlu, 4 uzunluklu ve sabit ağırlıklı olmayan ikili bir kod olsun. Eğer C minimal ise C, 2-ağırlıklı bir koddur.*

Kanıt. C minimal bir kod olsun. Önerme 3.6 sebebiyle C kodunun ağırlığı bir veya dört olamaz. Bu durumda $wt(C) \in \{2, 3\}$ olmalıdır. C sabit ağırlıklı olmadığı için, ağırlığı 2 ve ağırlığı 3 olan iki kod sözcüğü olmalıdır. Dolayısıyla C, 2-ağırlıklı bir koddur.

■

Not. Bu önermenin tersi doğru olmayacaktır. Örneğin,

$$C = \{0000, 1000, 1100, 0100\}$$

2 boyutlu 4 uzunluklu 2-ağırlıklı bir koddur ama minimal değildir.

Önerme 3.11. *C, 2 boyutlu, 4 uzunluklu sabit ağırlıklı olmayan ikili bir kod olsun. Bu durumda aşağıdakiler birbirine denktir:*

1) C minimaldir.

2) C için, ağırlık dağılımı, $A(C) = (1, 0, 1, 2, 0)$ olur.

Kanıt. $C = \{0, c_1, c_2, c_3\}$ minimal olsun. Önerme 3.10 sebebiyle, C 2-ağırlıklıdır. Dolayısıyla $A(C)$ için iki ihtimal vardır. $A(C) = (1, 0, 1, 2, 0)$ ya da

$A(C) = (1, 0, 2, 1, 0)$ olur. Diyelim $A(C) = (1, 0, 2, 1, 0)$ olsun ve $wt(c_1) = wt(c_2) = 2$ olsun. O zaman $|\text{suppt}(c_1) \cap \text{suppt}(c_2)| = 1$ olur. Lemma 2.1 sebebiyle $wt(c_3) = 2 + 2 - 2.1 = 2$ elde ederiz. Yani bu ağırlık dağılımı geçerli olamaz. Dolayısıyla $A(C) = (1, 0, 1, 2, 0)$ olur.

C için $A(C) = (1, 0, 1, 2, 0)$ olsun. Bu durumda $w_1 = 2, w_2 = 3$ olur. Teorem 2.4 sebebiyle C minimaldir. ■

Sonuç 3.12. *C, 2-boyutlu, 4 uzunluklu ikili minimal bir kod olsun. Bu durumda ya C ağırlığı 2 olan sabit ağırlıklı bir koddur ya da ağırlık dağılımı $A(C) = (1, 0, 1, 2, 0)$ olan bir koddur.*

Teorem 3.13. *C uzunluğu $n \geq 2$ olan iki boyutlu ikili minimal bir kod olsun. Eğer C, 3-ağırlıklı bir kod ise, bu durumda $n > 5$ ve C kodunun ağırlığı en az 3 olmalıdır.*

Kanıt. Önerme 3.8 ve Önerme 3.10 sebebiyle $n < 5$ olamaz. Dolayısıyla $n \geq 5$ olur. C minimal olduğu için Önerme 3.6 sebebiyle $wt(C) = 1$ olamaz. C kodunun ağırlığının 2 olduğunu kabul edelim. Bu durumda $v \in C$ ağırlığı iki olan eleman olsun. $w \in C$ da $wt(v) = 2 < wt(w)$ koşulunu sağlayan kod sözcüğü olsun. C minimal olduğu için, $|\text{suppt}(v) \cap \text{suppt}(w)| = 1$ olur.
Bu koşullarda,

$$wt(v+w) = wt(v)+wt(w)-2|\text{suppt}(v)\cap\text{suppt}(w)| = 2+wt(w)-2 = wt(w)$$

eşitliği elde edilir. C kodu 2-ağırlıklı olur. Bu da bir çelişkidir. Bu nedenle $wt(C) \geq 3$.

$n = 5$ ve $wt(C) = 3$ için, $v \in C$, $wt(v) = 3$ olan bir kod sözcüğü olsun. $w \in C$ de $wt(v) = 3 < wt(w)$ koşlunu sağlayan kod sözcüğü olsun. C minimal olduğu için, $|\text{suppt}(v) \cap \text{suppt}(w)| \in \{1, 2\}$ olur. Eğer $|\text{suppt}(v) \cap \text{suppt}(w)| = 1$ ise, $wt(v + w) = wt(v) + wt(w) - 2|\text{suppt}(v) \cap \text{suppt}(w)| = 3 + wt(w) - 2 =$

$wt(w)+1$. Önerme 3.6 sebebiyle $wt(w) < 5$ olmalıdır. Bu durumda tek seçenek $wt(w) = 4$ olur ve $wt(v+w) = wt(w)+1 = 5$ elde edilir. Bu da Önerme 3.6 ile çelişir. Eğer $|\text{suppt}(v) \cap \text{suppt}(w)| = 2$ ise, $wt(v+w) = wt(v)+wt(w)-2|\text{suppt}(v) \cap \text{suppt}| = 3+wt(w)-4 = wt(w)-1$ olur. $wt(v) = 3 < wt(w)$ ve Önerme 3.6 sebebiyle, $wt(w) = 4$ olur. Bu durumda $wt(v+w) = 3 = wt(v)$ elde edilir. C kodu 2-ağırlıklı olur. Bu da kabulümüzle çelişir. Bu nedenle $n > 5$ olmalıdır.

■

Örnek 21. Teorem 3.13'teki uzunluk ve ağırlık için alt sınırın sağlandığı örnek vardır. $C = \{00000, 111000, 001111, 110111\}$ uzunluğu 6 olan 3-ağırlıklı, ağırlığı 3 olan minimal bir koddur.

3.2 Üç Boyutlu İkili Minimal Kodlar

[13] numaralı makalede 3-boyutlu ikili minimal kodların uzunlukları için iki aday olduğu ortaya konmuştur. Daha açık yazmak gerekirse, üç boyutlu ikili minimal kodlar için olası en küçük uzunluk Örnek 18'de, $n(3,2) \in \{5,6\}$ olarak belirtilmiştir. [2] numaralı makalede geometrik yöntemler kullanarak $n(3,2) > 5$ olduğu elde edilmiştir. Bu kısımda [2] numaralı makaledeki yöntemlerden farklı bir yöntemle, Teorem 2.21 yardımıyla

$$n(3,2) = 6$$

olduğu kanıtlanmıştır.

Önerme 3.14. 3-*boyutlu,* 5 *uzunluklu ikili mimimal kod yoktur.*

Kanıt. C, $\{v_1, v_2, v_3\}$ kümesinin baz olduğu 3-boyutlu, 5 uzunluklu ikili minimal bir kod olsun. Teorem 2.21 sebebiyle $d = wt(C) \geq 3$ olacağı için

$i \in \{1,2,3\}$ olmak üzere $wt(v_i) \geq 3$ olur. Minimallikten dolayı kod sözcüklerin ağırlığının 5 olması mümkün değildir. Dolayısıyla dört durum söz konusu olur.

	$wt(v_1)$	$wt(v_2)$	$wt(v_3)$
1.durum	3	3	3
2.durum	3	3	4
3.durum	3	4	4
4.durum	4	4	4

1.durum $wt(v_1) = wt(v_2) = wt(v_3) = 3$ olsun. $i, j \in \{1,2,3\}$, $i \neq j$ olsun. Bu durumda, $|\text{suppt}(v_i) \cap \text{suppt}(v_j)| \in \{1,2\}$ olabilir. Bu sayı 2 olamaz. Çünkü olsaydı,

$$wt(v_i + v_j) = wt(v_i) + wt(v_j) - 2|\text{suppt}(v_i) \cap \text{suppt}(v_j)| = 3 + 3 - 2 \cdot 2 = 2$$

eşitliği sağlanırdı, fakat bu $wt(C) \geq 3$ olması ile çelişir.

Bu durumda $i \neq j \in \{1,2,3\}$ için $|\text{suppt}(v_i) \cap \text{suppt}(v_j)| = 1$ olmalıdır. Genelliği bozmadan v_1, v_2, v_3 vektörlerinin birinci koordinatlarını düşünelim. Eğer

$$v_1 = 1\overline{v_1}$$

$$v_2 = 1\overline{v_2}$$

$$v_3 = 1\overline{v_3}$$

ise, $\overline{v_1} + \overline{v_2} = 1111$ ve $\overline{v_1} + \overline{v_3} = 1111$ olur ve böylece $\overline{v_3} = \overline{v_2}$ elde ederiz. Bu durumda $v_2 = v_3$ olur, çelişki elde ederiz.

Eğer

$$v_1 = 1\overline{v_1}$$

$$v_2 = 1\overline{v_2}$$

$$v_3 = 0\overline{v_3}$$

ise, ya $|\text{suppt}(v_1) \cap \text{suppt}(v_3)| = 2$ ya da $|\text{suppt}(v_2) \cap \text{suppt}(v_3)| = 2$ olur. Bu durumda ya $wt(v_1 + v_3) = 2$ ya da $wt(v_2 + v_3) = 2$ olur. Her iki durumda $wt(C) \geq 3$ olması ile çelişir. Sonuç olarak 1.durum geçerli olamaz.

2.durum $wt(v_1) = wt(v_2) = 3$, $wt(v_3) = 4$ olsun. $|\text{suppt}(v_1) \cap \text{suppt}(v_2)| \in \{1, 2\}$ olabilir. Birinci durumdaki gibi $wt(v_1+v_2) = 2$ olacağı için $|\text{suppt}(v_1) \cap \text{suppt}(v_2)|$ değeri 2 olamaz. $|\text{suppt}(v_1) \cap \text{suppt}(v_2)| = 1$ olduğunu kabul edelim. $i \in \{1, 2\}$ olmak üzere $|\text{suppt}(v_i) \cap \text{suppt}(v_3)| \in \{2, 3\}$ olabilir. Eğer $|\text{suppt}(v_i) \cap \text{suppt}(v_3)| = 2$ olur ise, $wt(v_3) = 4$ olduğu için ya $v_3 = v_1 + v_2$ olur ya da $\text{suppt}(v_3)$, v_1, v_2 vektörlerinin birinin desteğini içerir. Dolayısıyla kodun minimal olması ile çelişir. Eğer en az bir $i \in \{1, 2\}$ için $|\text{suppt}(v_i) \cap \text{suppt}(v_3)| = 3$ ise, C minimal olamaz ve çelişki elde edilir. İkinci durum geçerli olamaz.

3.durum $wt(v_1) = 3$ ve $wt(v_2) = wt(v_3) = 4$ olsun. $|\text{suppt}(v_2) \cap \text{suppt}(v_3)| = 3$ olur.

$$|\text{suppt}(v_2)| + |\text{suppt}(v_3)| - 2|\text{suppt}(v_2) \cap \text{suppt}(v_3)| = 4 + 4 - 2 \cdot 3 = 2$$

elde ederiz. Bu durum $wt(C) \geq 3$ olması ile çelişir. Sonuç olarak 3.durum geçerli olamaz.

4.durum $wt(v_1) = wt(v_2) = wt(v_3) = 4$ olsun. $i, j \in \{1, 2, 3\}$ olmak üzere $i \neq j$ olsun. $|\text{suppt}(v_i) \cap \text{suppt}(v_j)| = 3$ olur.

$$|\text{suppt}(v_i)| + |\text{suppt}(v_j)| - 2|\text{suppt}(v_i) \cap \text{suppt}(v_j)| = 4 + 4 - 2 \cdot 3 = 2$$

elde ederiz. Aynı şekilde bu durum $wt(C) \geq 3$ olması ile çelişir. Sonuç olarak 4.durum da geçerli olamaz. Yani 3-boyutlu, 5 uzunluklu ikili minimal kod yoktur. ■

Sonuç 3.15. *Eğer C, n uzunluklu 3 boyutlu ikili minimal bir kod ise, $n \geq 6$ olur.*

3.3 Minimal Kodların Dualleri

Bu kısımda minimal kodların dualleri düşünülmüş ve düşük boyutlu minimal kodlar için hangi durumlarda dual kodların minimal olduğu incelenmiştir. 4 uzunluklu iki boyutlu kendi dual minimal kod olmadığı gösterilmiştir. İki boyutlu sabit ağırlıklı olmayan kendine dik minimal bir kodun uzunluğu için alt sınırın 8 olduğu kanıtlanmıştır. 8 uzunluklu sabit ağırlıklı olmayan kendine dik minimal bir kod için ağırlık dağılımı belirlenmiştir.

$\mathbb{F}_2$ üzerinde 1-boyutlu, 2 uzunluklu kodların hem kendileri hem de duallerinin minimal olduğu açıktır.

Örnek 22. $\mathbb{F}_2$ üzerinde 1-boyutlu, 3 uzunluklu kodlardan sadece ağırlığı 3 olan kod sözcüğün ürettiği kodun hem kendisi hem de duali minimaldir.

$$C = \{000, 111\}$$

$$C^{\perp} = \{000, 110, 011, 101\}$$

Gözlem. *1-boyutlu 4 uzunluklu kodların dualleri 3 boyutlu ve 4 uzunlukludur. Fakat 3-boyutlu kodlar için Önerme 3.14 ve Sonuç 3.15 sebebiyle minimum uzunluk 6 olduğundan 1-boyutlu 4 uzunluklu kodların dualleri minimal olamaz. Benzer durum 1-boyutlu 5 uzunluklu kodlar için de geçerlidir. Çünkü bu kodların dualleri 4-boyutlu, 5 uzunlukludur. Örnek 19 sebebiyle 4-boyutlu, 5 uzunluklu minimal kod yoktur.*

Önerme 3.16. $\mathbb{F}_2$ *üzerinde 2-boyutlu, 3 uzunluklu minimal kodun hem kendisi hem de duali minimaldir.*

Kanıt. Önerme 3.8 sebebiyle 2-boyutlu, 3 uzunluklu minimal kod

$$C = \{000, 110, 011, 101\}$$

olup, $C^{\perp} = \{000, 111\}$ olur. Yani hem kendisi hem de duali minimaldir. ■

Önerme 3.17. $\mathbb{F}_2$ *üzerinde* 2*-boyutlu,* 4 *uzunluklu, sabit ağırlıklı olmayan minimal kodların dualleri de minimaldir.*

Kanıt. C, 2-boyutlu, 4 uzunluklu, sabit ağırlıklı olmayan minimal bir kod olsun. Önerme 3.11 sebebiyle bu kodun ağırlık dağılımının $A(C) = (1, 0, 1, 2, 0)$ olduğunu biliyoruz. Şimdi C kodunun dualinin de minimal olduğunu göstereceğiz.

C 2-boyutlu, 4 uzunluklu olduğundan $C^\perp$ 2-boyutlu 4 uzunlukludur. Önerme 3.11 sebebiyle $A(C^\perp) = (1, 0, 1, 2, 0)$ olduğunu göstermemiz yeterli olacaktır.

$c \in C^\perp$ olsun. $wt(c) = 1$ olsun. Genellemeyi kaybetmeden $\text{suppt}(c) = \{1\}$ kabul edelim. Bu durumda $C = \{0, c_1, c_2, c_3\}$ için $1 \notin \text{suppt}(c_i)$ olmalıdır. Bu durumda $C = \{0, 0110, 0101, 0011\}$ olur. Yani sabit ağırlıklı olur. Çelişki elde ederiz. Dolayısıyla $C^\perp$ ağırlığı 1 olan kod sözcüğü içeremez.

$c \in C^\perp$ ve $wt(c) = 4$ olsun. $A(C) = (1, 0, 1, 2, 0)$ olduğu için, C içinde ağırlığı 3 olan bir eleman vardır. Bu eleman c_3 olsun. Bu durumda $\langle c, c_3 \rangle = 1$ olur. Yani $c \notin C^\perp$ olur. Çelişki elde ederiz.

Diyelim $x, y \in C^\perp$ ve $wt(x) = wt(y) = 2$ olsun. $c_2, c_3 \in C$, $wt(c_2) = wt(c_3) = 3$ elemanlar olsun. C minimal olduğu için $|\text{suppt}(c_2) \cap \text{suppt}(c_3)| = 2$ olur. Genellemeyi kaybetmeden $\text{suppt}(c_2) \cap \text{suppt}(c_3) = \{1, 2\}$ olduğunu kabul edelim. Bu durumda $\langle x, c_2 \rangle = \langle x, c_3 \rangle = \langle y, c_2 \rangle = \langle y, c_3 \rangle = 0$ olacağı için $x = y$ olmak zorundadır. Çelişki elde ederiz. Dolayısıyla ağırlığı 2 olan iki tane kod sözcüğü olamaz. Sonuç olarak $A(C^\perp) = (1, 0, 1, 2, 0)$ olur.

■

Örnek 23. Önerme 3.17 sabit ağırlıklı kodlar için doğru olmaz.

$$C = \{0000, 1100, 1010, 0110\}$$

2-boyutlu 4 uzunluklu sabit ağırlıklı minimal bir koddur.

$$C^{\perp} = \{0000, 0001, 1110, 1111\}$$

$C^{\perp}$, minimal değildir.

Önerme 3.18. *2-boyutlu, 4 uzunluklu hem minimal hem de kendine dual(self dual) olan kod yoktur.*

Kanıt. C, 2-boyutlu, 4 uzunluklu minimal bir kod olsun. $C = \{0, w_1, w_2, w_3\}$ ve kendi dual bir kod olsun. Bu durumda tanım gereği

$$\langle w_1, w_2 \rangle = 0,\ \langle w_2, w_3 \rangle = 0,\ \langle w_1, w_3 \rangle = 0$$

$$\langle w_1, w_1 \rangle = 0,\ \langle w_2, w_2 \rangle = 0,\ \langle w_3, w_3 \rangle = 0$$

sağlanır. Her $i \in \{1, 2, 3\}$ için $w_i \cdot w_i = 0$ sağlanması için $wt(w_i)$'nin çift sayı olması gerekir. O zaman kod sözcüklerin ağırlığı 2 yada 4 olabilir. C minimal olduğu için 4 olamaz.Bu durumda $wt(w_1) = wt(w_2) = wt(w_3) = 2$ olur. O zaman C sabit ağırlıklı bir kod olur. $i \neq j$ olmak üzere $i, j \in \{1, 2, 3\}$ için $|\text{suppt}(w_i) \cap \text{suppt}(w_j)| = 1$ olmalıdır. Bu durumda $\langle w_i, w_j \rangle = 1$ olur. Çelişki elde ederiz.

■

Sonuç 3.19. *2-boyutlu, 4 uzunluklu minimal kendine dik kod yoktur*

Örnek 24.

$$D = \{000000, 100111, 011011, 111100\}$$

Bu kod sabit ağırlıklı olup minimal bir koddur. Her kod sözcüğün ağırlığı çift olduğundan herbiri kendisine diktir. Herhangi iki kod sözcüğün desteklerinin kesişimi de iki elemanlıdır. Bu yüzden her kod sözcük birbirine diktir. Dolayısıyla bu kod kendine dik bir koddur.

Örnek 25.

$$C = \{0000, 1100, 1010, 0110\}$$

Bu kod sabit ağırlıklı olup minimal bir koddur. $\langle 1100, 1010\rangle = 1$ olduğu için kendine dik değildir. Yani sabit ağırlıklı her kod kendine dik değildir.

Önerme 3.20. 2-*boyutlu,* 6 *uzunluklu minimal sabit ağırlıklı olmayan kendine dik kod yoktur.*

Kanıt. C 2-boyutlu, 6 uzunluklu minimal sabit ağırlıklı olmayan kendine dik bir kod olsun ve $C = \{0, w_1, w_2, w_3\}$ şeklinde yazılsın. Bu durumda

$$\langle w_1, w_2\rangle = 0,\ \langle w_2, w_3\rangle = 0,\ \langle w_1, w_3\rangle = 0$$

$$\langle w_1, w_1\rangle = 0,\ \langle w_2, w_2\rangle = 0,\ \langle w_3, w_3\rangle = 0$$

sağlanır. Her $i \in \{1, 2, 3\}$ için $w_i \cdot w_i = 0$ sağlanması için $wt(w_i)$'nin çift sayı olması gerekir. O zaman kod sözcüklerin ağırlığı 2, 4 yada 6 olabilir. Ama minimallikten dolayı 6 olamaz. O zaman ağırlık dağılımı için iki ihtimal vardır.

i) $A(C) = (1, 0, 1, 0, 2, 0, 0)$

ii) $A(C) = (1, 0, 2, 0, 1, 0, 0)$

Diyelim ki $A(C) = (1, 0, 1, 0, 2, 0, 0)$ olsun. Genelliği bozmadan $wt(w_1) = 2$ olsun. Minimalliğin sağlanması için $|\text{suppt}(w_1) \cap \text{suppt}(w_2)| = 1$ olmalıdır. Bu durumda $\langle w_1, w_2\rangle = 1$ neden olur. Yani $C \nsubseteq C^{\perp}$ olur. $A(C) = (1, 0, 2, 0, 1, 0, 0)$ olsun. Genelliği bozmadan $wt(w_1) = wt(w_2) = 2$ olsun. Minimallikten dolayı $|\text{suppt}(w_1) \cap \text{suppt}(w_2)| = 1$ olmalıdır. Lemma 2.1'deki formül sebebiyle

$$wt(w_3) = wt(w_1) + wt(w_2) - 2|\text{suppt}(w_1) \cap \text{suppt}(w_2)|$$

Dolayısıyla $wt(w_3) = 2$ olur. Ama kabulümüze göre $wt(w_3) = 4$ olmalıydı. Sonuç olarak 2-boyutlu, 6 uzunluklu minimal, sabit ağırlıklı olmayan kendine dik bir kod yoktur. ■

Teorem 3.21. *C uzunluğu n olan ikili bir kod olsun. Eğer C iki boyutlu minimal sabit ağırlıklı olmayan kendine dik bir kod ise, $n \geq 8$ olur.*

Kanıt. $n \in \{2, 3\}$ olamayacağı açıktır. Sonuç 3.19 sebebiyle $n = 4$ ve Önerme 3.20 sebebiyle $n = 6$ olamaz. Dolayısıyla sadece iki durumu incelememiz yeterli olacaktır.

1. Durum: $n = 5$.

$C = \{0, c_1, c_2, c_3\}$ uzunluğu 5 olan iki boyutlu sabit ağırlıklı olmayan kendine dik bir kod olsun. Tanım gereği, her $i, j \in \{1, 2, 3\}$ için $\langle c_i, c_j \rangle = 0$ olacaktır. Dolayısıyla $wt(c_i)$ ve $|\text{suppt}(c_i) \cap \text{suppt}(c_j)|$ çift olmalıdır. C minimal olduğu için bu iki durum aynı anda sağlanamaz.Dolayısıyla $n = 5$ olamaz.

2. Durum: $n = 7$.

Birinci durumda olduğu gibi, $wt(c_i)$ ve $|\text{suppt}(c_i) \cap \text{suppt}(c_j)|$ çift olmalıdır. Bu durumda $wt(c_i) \in \{2, 4, 6\}$ olmalıdır. Ama herhangi bir i için $wt(c_i) = 2$ olamaz, aksi taktirde $i \neq j$ için $|\text{suppt}(c_i) \cap \text{suppt}(c_j)| = 2$ olur, bu durum C kodunun minimal olması ile çelişir. Dolayısıyla $wt(c_i) \in \{4, 6\}$ olabilir. Bu durumda ağırlık dağılımı için iki durum olabilir. Eğer $A(C) = (1, 0, 0, 0, 1, 0, 2, 0)$ ise genellemeyi kaybetmeden $wt(c_1) = 4$ ve $wt(c_2) = wt(c_3) = 6$ olur. Uzunluk 7 ve kod minimal olduğu için bu durumda

$$|\text{suppt}(c_1) \cap \text{suppt}(c_2)| = 3$$

olur. Bu da kodun kendine dik olması ile çelişir.

Eğer $A(C) = (1, 0, 0, 0, 2, 0, 1, 0)$ olur ise, genellemeyi kaybetmeden

$$wt(c_1) = 6, \quad wt(c_2) = wt(c_3) = 4$$

olur. Minimallik sebebiyle $|\text{suppt}(c_1) \cap \text{suppt}(c_2)| = 2$ olmalıdır. Lemma 2.1 sebebiyle, $wt(c_3) = wt(c_1)+wt(c_2)-2|\text{suppt}(c_1)\cap\text{suppt}(c_2)| = 6$ olur. Çelişki elde ederiz. Sonuç olarak, $n < 8$ uzunluklu, sabit ağırlıklı olmayan kendine dik minimal bir kod yoktur. ■

Teorem 3.21 de alt sınırda istenilen özelliklere sahip bir kod vardır.

Örnek 26. $C = \{0, 11110000, 00111111, 11001111\}$ kodu ağırlık dağılımı $A(C) = (1, 0, 0, 0, 1, 0, 2, 0, 0)$ olan kendine dik minimal bir koddur.

Önerme 3.22. *Eğer C uzunluğu sekiz olan sabit ağırlıklı olmayan kendine dik minimal 2-boyutlu ikili bir kod ise, $A(C) = (1, 0, 0, 0, 1, 0, 2, 0, 0)$ olur.*

Kanıt. C sabit ağırlıklı olmayan, kendine dik minimal bir kod olsun ve $A(C) = (1, 0, 0, 0, 1, 0, 2, 0, 0)$ olmasın. Bu durumda $A(C) = (1, 0, 0, 0, 2, 0, 1, 0, 0)$ olur. Genellemeyi kaybetmeden $wt(c_1) = wt(c_2) = 4$ ve $wt(c_3) = 6$ olsun. C minimal olduğu için $|\text{suppt}(c_1) \cap \text{suppt}(c_3)| = 2$ olacaktır. Lemma 2.1 sebebiyle, $wt(c_2) = 6$ olur. Çelişki elde ederiz.

■

Bölüm 4

Minimal Kodların Permütasyon Otomorfizma Grupları

Bu bölümde minimal kodların permütasyon otomorfizmaları incelenmiştir. Özel olarak sabit noktası olmayan mertebesi üç olan bir permütasyon otomorfizması kullanılarak, minimal bir kod için özel alt kodlar çalışılmıştır. Bu özel alt kodların minimal olduğu durumda, uzunluk için alt sınırlar verilmiştir. Son olarak, bu özel alt kodların direkt toplamının oluşturduğu kodun, üç boyutlu olduğu durumda ne zaman minimal olacağı kanıtlanmıştır.

4.1 Permütasyon Otomorfizma Grupları

Bu bölümdeki temel tanımlar ve kanıtlar için [8], [12] numaralı kaynaklar kullanılmıştır.

Tanım. X boş kümeden farklı bir küme olsun.

$$\mathrm{Sym}(X) = \{f : X \to X \mid f \text{ birebir, örten fonksiyon}\}$$

kümesi fonksiyonların bileşkesi işlemi altında bir grup olur. Bu gruba X üzerinde simetri grubu denir. $\mathrm{Sym}(X)$'in her alt grubuna **permütasyon grubu** adı verilir.

Eğer $X = \{1, 2, ..., n\}$ olur ise, Sym(X), S_n ile gösterilir ve X **üzerinde** n**'inci dereceden simetri grup** adını alır.

Tanım. G ve H iki grup olsun. Eğer $\varphi : G \to H$ fonksiyonu her $a, b \in G$ için

$$\varphi(ab) = \varphi(a)\varphi(b)$$

eşitliğini sağlıyor ise φ'ye **grup homomorfizması** denir. Eğer φ bire bir ve örten ise, **grup izomorfizması** denir. G grubundan kendisine yazılan grup izomorfizmasına **grup otomorfizması** denir.

Tanım. G bir grup, X boş kümeden farklı bir küme olsun. Eğer

$$G \text{ x } \text{X} \to \text{X}$$

$$(g, x) \to g \cdot x$$

fonksiyonu varsa ve aşağıdaki koşullar sağlanıyor ise, G**,** X **üzerinde etki eder** ya da X **bir** G**-kümesidir** denir.

1) $(e, x) \to e \cdot x = x$

2) her $g_1, g_2 \in G$, $x \in X$ için $g_1 \cdot (g_2 \cdot x) = (g_1 * g_2) \cdot x$

Örnek 27. $G = S_3 = \{id, (12), (23), (13), (123), (132)\}, X = \{1, 2, 3\}, \sigma \in S_3$

$$G \text{ x } \text{X} \to \text{X}$$

$$(\sigma, x) \to \sigma \cdot x = \sigma(x)$$

Bu bir grup etkisidir. Çünkü

1) $\sigma = \text{id}$, $\sigma \cdot x = \sigma(x) = \text{id}(x) = x$

2) $\sigma, \gamma \in S_3$, $\sigma \cdot (\gamma \cdot x) = \sigma \cdot \gamma(x) = \sigma \circ \gamma(x) = (\sigma \circ \gamma)(x) = (\sigma\gamma) \cdot (x)$ koşulları sağlanır.

X bir S_3-kümesidir.

$\beta = \{e_1, \ldots, e_n\}$, $\mathbb{F}_q^n$ vektör uzayının bazı olsun. $\sigma \in S_n$ bir permütasyon olsun. Her $i \in \{1, 2, \ldots n\}$ için

$$\sigma \cdot e_i = e_{\sigma(i)}$$

şeklinde bir etki tanımlayalım. Bu etkiyi, V nin bütün elemanlarına doğrusal olarak genişletelim. Yani $v = (v_1, \ldots, v_n) \in \mathbb{F}_q^n$ için $v = v_1e_1 + v_2e_2 + \cdots + v_ne_n$ olduğunda $\sigma \cdot v = v_1\sigma \cdot e_1 + v_2\sigma \cdot e_2 + \cdots + v_n\sigma \cdot e_n$ şeklinde genişletelim.

Örnek 28. $v = (v_1, v_2, v_3)$, $\beta = \{e_1, e_2, e_3\}$ ve $\sigma = (123)$ olsun.

$$\sigma \cdot v = v_1\sigma \cdot e_1 + v_2\sigma \cdot e_2 + v_3\sigma \cdot e_3$$

$$\sigma \cdot v = v_1e_2 + v_2e_3 + v_3e_1$$

olur. Sıralı baz $\{e_1, e_2, e_3\}$'e göre koordinatları yazarsak

$$\sigma \cdot v = (v_3, v_1, v_2)$$

olur. $\sigma^{-1} = (132)$ olduğundan, $v_3 = v_{\sigma^{-1}(1)}, v_1 = v_{\sigma^{-1}(2)}, v_2 = v_{\sigma^{-1}(3)}$ olur. Yani

$$\sigma \cdot v = \sigma \cdot (v_1, v_2, v_3) = (v_{\sigma^{-1}(1)}, v_{\sigma^{-1}(2)}, v_{\sigma^{-1}(3)})$$

olarak yazılır.

Bu örnekteki dönüşümü daha genel anlamda yazmak mümkündür.

$$v_i\sigma \cdot e_i = v_ie_{\sigma(i)}$$

eşitliğinde indisleri yeniden yazacak olursak

$$\sigma(i) = j \to \sigma^{-1}(j) = i$$

$$v_i\sigma \cdot e_i = v_ie_j = v_{\sigma^{-1}(j)}e_j$$

ifadesini elde ederiz.

Önerme 4.1. *S_n simetri grubu, $V = \mathbb{F}_q^n$ vektör uzayı olsun. $\sigma \in S_n, v \in V$ için, $\sigma \cdot v = (v_{\sigma^{-1}(1)}, v_{\sigma^{-1}(2)}, \ldots, v_{\sigma^{-1}(n)})$ etkisi bir grup etkisidir.*

Kanıt. $v = (v_1, ...v_n) \in V$ alalım. $\sigma = id$ için $\sigma \cdot v = (v_1, \ldots, v_n) = v$ olur. $\sigma, \gamma \in S_n$ alalım. Göstermemiz gereken $\sigma \cdot (\gamma \cdot v) = (\sigma\gamma) \cdot v$ eşitliğidir.

$$\gamma \cdot v = (v_{\gamma^{-1}(1)}, \ldots, v_{\gamma^{-1}(n)}) = (w_1, \ldots, w_n) \quad (1)$$

şeklinde yazalım. Bu durumda

$$\sigma \cdot (\gamma \cdot v) = \sigma(w_1, \ldots, w_n) = (w_{\sigma^{-1}(1)}, \ldots, w_{\sigma^{-1}(n)})$$

eşitliği elde edilir. (1) ifadesinden

$$w_1 = v_{\gamma^{-1}(1)},\ w_2 = v_{\gamma^{-1}(2)}, \ldots,\ w_n = v_{\gamma^{-1}(n)}$$

eşitliklerini düşünelim. Her $i \in \{1, 2, ..., n\}$ için $w_i = v_{\gamma^{-1}(i)}$ olur. $w_{\sigma^{-1}(i)}$ koordinatının nasıl hesaplandığını düşünelim. Genelliği bozmadan $w_{\sigma^{-1}(1)}$ için düşünelim. $\sigma^{-1}(1) = i$ olsun. $\sigma(i) = 1$ olur.

$$w_{\sigma^{-1}(1)} = w_i = v_{\gamma^{-1}(i)} = v_{\gamma^{-1}(\sigma^{-1}(1))} = v_{(\sigma\gamma)^{-1}(1)}$$

eşitliği elde edilmiş olur. Yani $w_{\sigma^{-1}(1)} = v_{(\sigma\gamma)^{-1}(1)}$ olur. Bunu herhangi bir j için yazarsak

$$w_{\sigma^{-1}(j)} = v_{(\sigma\gamma)^{-1}(j)}$$

eşitliği elde edilir. Yani

$$\sigma \cdot (\gamma \cdot v) = (v_{(\sigma\gamma)^{-1}(1)}, v_{(\sigma\gamma)^{-1}(2)}, \ldots, v_{(\sigma\gamma)^{-1}(n)} = (\sigma\gamma) \cdot v$$

eşitliği elde edilmiş olur.

■

Önerme 4.2. *$C \subseteq \mathbb{F}_q^n$ doğrusal kod olsun. S_n grubunun $\mathbb{F}_q^n$ üzerine etkisi düşünüldüğünde, bu etki altında C kodunun sabitleyicisi $\{\sigma \in S_n \mid \sigma \cdot C = C\}$ S_n grubunun bir alt grubudur.*

Kanıt. $id \in S_n$ için $id \cdot C = C$ olduğu açıktır. Dolayısıyla $id \in \{\sigma \in S_n \mid \sigma \cdot C = C\}$ sağlanır. $\sigma, \gamma \in \{\sigma \in S_n \mid \sigma \cdot C = C\}$ olsun. Eğer $\gamma \cdot C = C$ ise, $C = (\gamma^{-1}\gamma) \cdot C = \gamma^{-1}(\gamma \cdot C) = \gamma^{-1} \cdot C$ olur. Dolayısıyla her $\sigma\gamma^{-1} \cdot C = C$ sağlanır. Yani $\sigma\gamma^{-1} \in \{\sigma \in S_n \mid \sigma \cdot C = C\}$ olur. ■

Tanım. C doğrusal bir kod olsun.

$$\{\sigma \in S_n \mid \sigma \cdot C = C\} \leq S_n$$

alt grubuna C kodunun **permüstasyon otomorfizma grubu** denir ve $\mathrm{PAut}(C)$ ile gösterilir.

Önerme 4.3. *$C \subseteq \mathbb{F}_2^n$ bir boyutlu ikili doğrusal bir kod olsun ve v kod sözcüğü ile üretilsin. Eğer $wt(v) = t$ ise, bu durumda $\mathrm{PAut}(C) \cong S_t \times S_{n-t}$ olur.*

Kanıt. Genellemeyi kaybetmeden

$$v = \underbrace{111\ldots11}_{t \text{ tane}}00000\ldots00$$

şeklinde yazabiliriz. Bu durumda etki altında v kod sözcüğünün sabit kalması gerektiği için, birler kendi aralarında, sıfırlar da kendi aralarında yer değiştirebilirler. Dolayısıyla $\mathrm{PAut}(C) \cong S_t \times S_{n-t}$ elde edilir.

■

Örnek 29. $C = \{0000, 1110\}$ ise $\mathrm{PAut(C)} = \langle(12), (123)\rangle \cong S_3$ olur. Eğer $C = \{0000, 1100\}$ ise $\mathrm{PAut(C)} = \langle(12), (34)\rangle \cong C_2 \times C_2$ olur.

Bir boyutlu ikili doğrusal kodların tanım gereği minimal olduğunu biliyoruz. Bir boyutlu minimal kodlar için, Önerme 4.3 sebebiyle , uzunluk büyüdükçe, otomorfizma grubunun oldukça büyük olacağı açıktır. Önerme 4.3 sebebiyle, ağırlığı 1 ve 3 olan kod sözcüklerin ürettiği 1-boyutlu 4 uzunluklu minimal doğrusal kodların permütasyon otomorfizma grupları S_3'e, ağırlığı 4 olanınki S_4'e, ağırlığı 2 olanınki ise $C_2 \times C_2$'ye izomorfiktir.

Tanım. $C_1, C_2 \subseteq \mathbb{F}_q^n$ iki doğrusal kod olsun. $\sigma \in S_n$ olmak üzere $\sigma \cdot C_1 = C_2$ sağlanıyorsa C_1 ve C_2'ye **permütasyon denktir** denir.

Örnek 30. $C_1 = \{0000, 0011, 0110, 0101\}$ kodunu düşünelim. $\sigma \in S_4$ omak üzere $\sigma = (1432)$ olsun. $\sigma \cdot C_1 = \{0000, 0110, 1100, 1010\} = C_2$ olduğundan C_1 ve C_2 kodları permütasyon denk kodlardır.

Önerme 4.4. *Permütasyon denk kodların permütasyon otomorfizma grupları izomorfiktir.*

Kanıt. A ve B permütasyon denk olan uzunluğu n olan iki kod olsun. Bu durumda $\sigma \in S_n$ için $\sigma \cdot A = B$ sağlanır. PAut(A) ve PAut(B) sırası ile A ve B kodlarının permütasyon otomorfizma grupları olsun. Bu iki grup arasında bir fonksiyon tanımlayalım.

$$\phi : \mathrm{PAut(A)} \to \mathrm{PAut(B)}, \quad \phi(\sigma_\mathrm{A}) = \sigma\sigma_\mathrm{A}\sigma^{-1}$$

Tanım gereği $\sigma\sigma_A\sigma^{-1}$, PAut(B) içindedir. Her $\sigma_A, \gamma_A \in$ PAut(A) için,

$$\phi(\sigma_A\gamma_A) = \sigma\sigma_A\sigma^{-1}\sigma\gamma_A\sigma^{-1} = \phi(\sigma_A)\phi(\gamma_A)$$

eşitliği sağlanacağından, ϕ bir grup homomorfizmasıdır. $\beta_A, \gamma_A \in$ PAut(A) için, $\phi(\beta_A) = \phi(\gamma_A)$ olsun. Bu durumda

$$\sigma\beta_A\sigma^{-1} = \sigma\gamma_A\sigma^{-1}$$

$$\sigma^{-1}\sigma\beta_A\sigma^{-1}\sigma = \sigma^{-1}\sigma\gamma_A\sigma^{-1}\sigma$$

$$\beta_A = \gamma_A$$

elde edilir. Dolayısıyla ϕ birebirdir.

Aynı şekilde fonksiyon

$$\psi : \mathrm{PAut(B)} \to \mathrm{PAut(A)}, \quad \psi(\gamma_\mathrm{B}) = \sigma^{-1}\gamma_\mathrm{B}\sigma$$

tanımlayalım. Benzer şekilde ψ fonksiyonu birebir bir homomorfizma olur. Dahası $\psi\phi = id_{\mathrm{PAut}(A)}$ ve $\phi\psi = id_{\mathrm{PAut}(B)}$ eşitlikleri sağlanır.

Sonuç olarak

$$\mathrm{PAut}(A) \cong \mathrm{PAut}(B)$$

olur. ■

Örnek 31.

$$C_1 = \{0000, 1101, 0111, 1010\}$$

$$C_2 = \{0000, 1011, 0111, 1100\}$$

olsun. $\sigma = (23)$, $\sigma \cdot C_1 = C_2$ olduğundan C_1 ve C_2 denk kodlardır.

$$\mathrm{PAut}(C_1) = \{id, (13), (24), (13)(24)\} \cong C_2 \times C_2$$

$$\mathrm{PAut}(C_2) = \{id, (12), (34), (12)(34)\} \cong C_2 \times C_2$$

Yani kodlar denktir ve permütasyon otomorfizma grupları izomorfiktir.

Örnek 32.

$$C_1 = \{000, 101, 110, 011\}$$

$$C_2 = \{0000, 1001, 1100, 0101\}$$

olsun. C_1 ve C_2 denk kodlar değildir.

$$\mathrm{PAut}(C_1) = \{id, (12), (23), (13), (123), (132)\} \cong S_3$$

$$\mathrm{PAut}(C_2) = \{id, (14), (12), (24), (124), (142)\} \cong S_3$$

Fakat permütasyon otomorfizma grupları izomorfiktir. Dolayısıyla Önerme 4.4'ün tersi doğru değildir. Permüstayon otomorfizma grupları izomorfik olsa bile kodlar denk olmayabilir.

Teorem 4.5. *C, $\mathbb{F}_q$ üzerinde doğrusal bir kod olsun. O zaman*

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

olur.

Kanıt. Tanım gereği $a = a_1 \dots a_n \in C$ ve $b = b_1 \dots b_n \in C^{\perp}$ için

$$\langle a, b \rangle = \sum_{i=1}^{n} a_i b_i = 0$$

olduğunu biliyoruz. $\sigma \in \mathrm{PAut}(C)$ için $\sigma(a) \in C$ olacaktır. Bu durumda

$$\langle \sigma(a), \sigma(b) \rangle = \langle a_{\sigma^{-1}(1)} \dots a_{\sigma^{-1}(n)}, b_{\sigma^{-1}(1)} \dots b_{\sigma^{-1}(n)} \rangle = \sum_{i=1}^{n} a_i b_i = 0$$

sağlanır ve $\sigma(b) \in C^{\perp}$ olur. $\sigma \in \mathrm{PAut}(C^{\perp})$ olur. Dolayısıyla

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

elde ederiz.

Diğer taraftan C doğrusal olduğundan $(C^{\perp})^{\perp} = C$ olur. Böylece $\mathrm{PAut}(\mathrm{C}^{\perp}) \subset \mathrm{PAut}((\mathrm{C}^{\perp})^{\perp}) = \mathrm{PAut}(\mathrm{C})$ olur ve

$$\mathrm{PAut}(C^{\perp}) \subset \mathrm{PAut}(C)$$

sağlanır. Bu içermeleri düşündüğümüzde

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

eşitliği elde edilir.

■

Örnek 33. C, $[3,1]_2$ doğrusal kodunu düşünelim ve $\mathrm{PAut}(C)$ grubunu bulalım.

$$C = \{000, 100\}, \quad \mathrm{PAut}(C) = \langle (23) \rangle$$

O zaman $C^{\perp}$, $[3,2]_2$ formunda bir kod olur. Bu durumda

$$C^{\perp} = \{000, 010, 001, 011\}, \quad \mathrm{PAut}(C^{\perp}) = \langle (23) \rangle$$

elde ederiz. Yani $\mathrm{PAut}(C) = \mathrm{PAut}(C^{\perp})$ oldu.

4.2 İki Boyutlu İkili Minimal Doğrusal Kodların Permütasyon Otomorfizma Grupları

Bu kısımda, 2-boyutlu ikili minimal kodları inceleyeceğiz. Teorem 3.8 sebebiyle 2-boyutlu, 3-uzunluklu minimal kodun, sadece $C = \{000, 110, 011, 101\}$ olduğunu biliyoruz. $(12), (123) \in \mathrm{PAut(C)}$ olduğu açıktır. Yani

$$\langle (12), (123) \rangle \leq \mathrm{PAut(C)} \leq S_3$$

sağlanır. Dolayısıyla $\mathrm{PAut}(C) = S_3$ olur.

Önerme 4.6. *C, 2-boyutlu 4-uzunluklu sabit ağırlıklı minimal doğrusal kod ise,* $\mathrm{PAut}(C) \cong S_3$ *olur.*

Kanıt. Önerme 3.9 sebebiyle C kodunun ağırlığı ikidir. 2 boyutlu, 4 uzunluklu, ağırlığı iki olan doğrusal ikili bir kod, $C = \{0000, 1100, 0110, 1010\}$

koduna permütasyon denktir. Eğer C_1 ve C_2 permütasyon denk ise, Önerme 4.4 sebebiyle, $\mathrm{PAut}(C_1) \cong \mathrm{PAut}(C_2)$ olduğunu biliyoruz. Bu durumda C kodunun permütasyon otomorfizma grubunu hesaplamak yeterlidir. C kodunun, kod sözcüklerinin ilk üç koordinatı düşünüldüğünde, $(12), (123) \in \mathrm{PAut}(C)$ olduğu açıktır. Yani $\langle (12), (123) \rangle \leq \mathrm{PAut}(C)$ sağlanır. $(1234) \notin \mathrm{PAut}(C)$ olduğundan $\mathrm{PAut}(C) \neq S_4$ ve $\langle (12), (123) \rangle \not\leq A_4$ olacağından

$$\mathrm{PAut}(C) = \langle (12), (123) \rangle \cong S_3$$

olur.

■

Önerme 4.7. *C, 2-boyutlu 4-uzunluklu sabit ağırlıklı olmayan minimal doğrusal bir kod olsun. Bu durumda*

$$\mathrm{PAut}(C) \cong C_2 \times C_2$$

Kanıt. 2-boyutlu 4-uzunluklu sabit ağırlıklı olmayan minimal doğrusal bir kod olsun. Teorem 3.11 sebebiyle C, 2-boyutlu 4-uzunluklu sabit ağırlıklı olmayan minimal doğrusal bir kod için $A(C) = (1, 0, 1, 2, 0)$ dir. Bu koşula sahip bir kod $C = \{0000, 1011, 1101, 0110\}$ koduna permütasyon denktir. Bu durumda Önerme 4.4 sebebiyle sadece C kodunun permütasyon otomorfizma grubunu hesaplamak yeterlidir. Kod sözcüklerinin ağırlıkları düşünüldüğünde, 1011 kod sözcüğünü ya sabit tutan ya da 1101 kod sözcüğüne dönüştüren ve 0110 kod sözcüğünü sabit tutan permütasyonlar olmalıdır. Bunlar da $\mathrm{PAut(C)} = \langle (23), (14) \rangle$ olduğu görülmektedir. Dolayısıyla

$$\mathrm{PAut(C)} \cong C_2 \times C_2$$

olur.

■

4.3 İkili Minimal Kodların Permütasyon Otomorfizmalar ile İnşası

C, uzunluğu n olan doğrusal ikili bir kod olsun. $p \geq 3$ olan bir asal sayı ve $\sigma \in \mathrm{PAut}(C)$ mertebesi p olan bir permütasyon otomorfizma olsun. Bu durumda eşleniğe göre

$$\sigma = \underbrace{(1, \ldots, p)}_{\Omega_1}\underbrace{(p+1, \ldots, 2p)}_{\Omega_2}\ldots\underbrace{((c-1)p+1, \ldots, cp)}_{\Omega c}$$

şeklinde yazmak mümkündür.

Tanım. [11] Eğer $n = cp$ ise, yani σ herhangi bir sayıyı sabitlemiyor ise, bu durumda σ permütasyonunu **sabit noktası olmayan permütasyon** denir. $\Omega_i = \{(i-1)p+1, ..., ip\}$ kümesine de σ permütasyonunun i'ninci p-döngü kümesi denir.

Tanım. [11] σ ve Ω_i yukarıdaki gibi tanımlansın. $v = v_1...v_n \in \mathbb{F}_q^n$ vektörü için, $v|_{\Omega_i} = v_{(i-1)p+1}...v_{ip}$ bloğuna v vektörünün Ω_i kümesine indirgemesi denir.

Örnek 34. $\sigma = (123)(456)(789) \in S_9$ sabit noktası olmayan bir permütasyondur ve $\Omega_1 = \{1, 2, 3\}$, $\Omega_2 = \{4, 5, 6\}$, $\Omega_3 = \{7, 8, 9\}$ olur. $v = v_1 v_2 \ldots v_9 \in \mathbb{F}_2^9$ için, $v|_{\Omega_1} = v_1 v_2 v_3$, $v|_{\Omega_2} = v_4 v_5 v_6$, $v|_{\Omega_3} = v_7 v_8 v_9$ olur.

Tanım. [11] C doğrusal bir kod ve $\sigma \in \mathrm{PAut(C)}$ mertebesi $p \geq 3$ olan bir permütasyon olsun.

$$F_\sigma(C) = \{v \in C : \sigma \cdot v = v\},$$

$$E_\sigma(C) = \{v \in C : i = 1, \ldots, c \text{ için } wt(v|\Omega_i) \text{ çift}\}$$

Örnek 35. $C = \{000, 100, 010, 001, 110, 101, 011, 111\}$ kodu için $\sigma = (123)$ mertebesi 3 olan, sabit noktası olmayan bir permütasyon otomorfizmadır.

$\Omega_1 = \{1, 2, 3\}$ ve her $v \in C$ için $v|_{\Omega_1} = v$ olur. $E_\sigma(C) = \{000, 110, 011, 101\}$ ve $F_\sigma(C) = \{000, 111\}$ olur.

Tanım. C doğrusal bir kod ve $\sigma \in$ PAut(C) ve $W \subset C$ bir alt kod olsun. Eğer $\sigma \cdot W = \{\sigma \cdot w \mid w \in W\} \subseteq W$ içermesi sağlanıyor ise, W alt koduna σ-değişmez alt kod denir.

Önerme 4.8. [11] *C doğrusal bir kod ve $\sigma \in$ PAut(C) mertebesi $p \geq 3$ olan sabit noktası olmayan bir permütasyon olsun. Bu durumda $E_\sigma(C) \subseteq C$, σ-değişmez bir alt koddur.*

Kanıt. Eğer $E_\sigma(C) = \{0\}$ ise yapılacak birşey yoktur. Bu yüzden $E_\sigma(C) \neq \{0\}$ olduğunu kabul edelim. $v \in E_\sigma(C)$ olsun. Tanım gereği $wt(v|_{\Omega_i})$ çift olmalıdır. σ permütasyon olduğu için ağırlıkları değiştirmez yani $wt(\sigma \cdot v|_{\Omega_i})$ da çifttir. Bu nedenle $\sigma \cdot v \in E_\sigma(C)$ olur. $E_\sigma(C)$ σ-değişmezdir. Tanım gereği $0000...0000 \in E_\sigma(C)$ sağlanır. $v \neq w \in E_\sigma(C)$ alalım. $i \in \{1, .., c\}$ için eğer $\text{suppt}(w|_{\Omega_i}) = \text{suppt}(v|_{\Omega_i})$ ise $wt((v - w)|_{\Omega_i}) = 0$ olur. $\text{suppt}(w|_{\Omega_i}) \neq \text{suppt}(v|_{\Omega_i})$ ise, $wt((v - w)|_{\Omega_i})$ çift olur. Her iki durumda da $v - w \in E_\sigma(C)$ sağlanır. $\alpha \in \mathbb{F}_2$ ve $v \in E_\sigma(C)$ için, $wt(\alpha v|_{\Omega_i})$ çift olacağından $\alpha v \in E_\sigma(C)$ sağlanır. ■

Önerme 4.9. [11] *$F_\sigma(C)$, σ-değişmez bir alt koddur.*

Kanıt. Tanım gereği σ-değişmez olduğu açıktır. $000....00 \in F_\sigma(C)$ olduğu da açıktır. Şimdi $v, w \in F_\sigma(C)$ alalım. Bu durumda $\sigma v = v$ ve $\sigma w = w$ sağlanır.

$$\sigma(v - w) = \sigma(v) - \sigma(w) = v - w$$

olup $v - w \in F_\sigma(C)$ sağlanır. $\alpha \in \mathbb{F}_2$ ve $v \in F_\sigma(C)$ için, $\sigma \cdot (\alpha v) = \alpha v$ dir. Dolayısıyla $\alpha v \in E_\sigma(C)$ sağlanır. ■

Teorem 4.10. [11, Teorem 1] *Yukarıda verilen $F_\sigma(C)$ ve $E_\sigma(C)$ tanımlarıyla*

$$C = F_\sigma(C) \oplus E_\sigma(C)$$

olur.

Bu kısımdan sonraki kısımlar için, $\sigma = (123)(456)....(n-2\ n-1\ n) \in S_n$ olarak kabul edilecektir. Eğer C n-uzunluklu bir kod ise ve $\sigma \in \mathrm{PAut(C)}$ ise, bir $k \geq 1$ tamsayısı için $n = 3k$ olur.

Önerme 4.11. *C 2-boyutlu bir kod ve $\sigma \in \mathrm{PAut}(C)$ olsun. O zaman*

$$\dim(\mathrm{E}_\sigma(\mathrm{C})) \neq 1$$

olur.

Kanıt. Eğer $E_\sigma(C) = \{0\}$ ise, önermenin doğru olduğu açıktır. $E_\sigma(C) \neq \{0\}$ olsun ve $0 \neq c \in E_\sigma(C)$ alalım. Önerme 4.8 sebebiyle $E_\sigma(C)$ σ-değişmez olduğu için, $\sigma \cdot c \in E_\sigma(C)$ olur. σ sabit noktası olmayan bir permütasyon olduğu için, $\sigma \cdot c = c$ olamaz. Dolayısıyla $\{c, \sigma \cdot c\} \subseteq E_\sigma(C)$ olur. ■

Önerme 4.12. *C 2-boyutlu, 6 uzunluklu ikili minimal kod olsun. Eğer*

$$\sigma = (123)(456) \in \mathrm{PAut}(C)$$

ise $C \neq F_\sigma(C)$.

Kanıt. C 2-boyutlu, 6 uzunluklu minimal kod olsun ve $\sigma = (123)(456) \in \mathrm{PAut}(C)$ olsun. $c \in F_\sigma(C)$, $c = c_1c_2c_3c_4c_5c_6$ alalım. $F_\sigma(C)$ tanımı gereği $\sigma c = c$ olacağından

$$c = c_1c_2c_3c_4c_5c_6 = c_3c_1c_2c_6c_4c_5$$

$$c_1 = c_2 = c_3,\ c_6 = c_5 = c_4$$

elde ederiz. O zaman $F_\sigma(C)$'nin içindeki herhangi elemanın formu $x, y \in \{0,1\}$ olmak üzere $c = xxxyyy$ olur. Minimallikten dolayı $x \neq y$ olmalıdır. Şimdi $v \neq w$ olmak üzere $v, w \in F_\sigma(C) - \{0\}$ alalım. Bu durumda $v = 111000$, $w = 000111$ olur. $F_\sigma(C) = \{0, 111000, 000111, 111111\}$ olur. $F_\sigma(C)$ minimal olamaz. Yani $F_\sigma(C) \neq C$. ■

Sonuç 4.13. *C, 2-boyutlu, 6 uzunluklu ikili minimal kod olsun ve $\sigma = (123)(456) \in \mathrm{PAut}(C)$ olsun. Bu durumda $C = E_\sigma(C)$ olur.*

Kanıt. Önerme 4.12 sebebiyle $E_\sigma(C) = \{0\}$ olamaz. Önerme 4.11 sebebiyle $C = E_\sigma(C)$ olur.

■

Önerme 4.14. *C, 2 boyutlu n uzunluklu ikili doğrusal bir kod ve $\sigma \in \mathrm{PAut(C)}$ olsun. Eğer $C = F_\sigma(C)$ minimal ise, bu durumda $n \geq 9$ olur.*

Kanıt. $\sigma \in \mathrm{PAut(C)}$ mertebesi 3 olan sabit noktası olmayan bir permütasyon olduğu için bazı pozitif tamsayı k için $n = 3k$ şeklinde olur. $C = F_\sigma(C)$ ve minimal bir kod olsun ve $3k \leq 6$ olsun. $k = 1$ için $C = F_\sigma(C) = \{000, 111\}$ bir boyutlu bir kod olur. Çelişki elde ederiz. $k = 2$ için, $C = F_\sigma(C) = \{000000, 111000, 000111, 111111\}$ olur. Ama bu kod minimal değildir. Çelişki elde ederiz. ■

Örnek 36. $n = 9$ için $C = F_\sigma(C)$ koşulunu sağlayan ve minimal olan bir kod vardır. $C = \{000000000, 111000111, 000111111, 111111000\}$. Bu kod sabit ağırlıklı bir kod olduğundan minimaldir.

Önerme 4.15. *C ikili doğrusal bir kod ve $\sigma \in \mathrm{PAut(C)}$ olsun. Eğer $0 \neq v \in E_\sigma(C)$ ise bu durumda v ile σv doğrusal bağımsızdır ve $\sigma^2 v = v + \sigma v$ sağlanır.*

Kanıt. $0 \neq v \in E_\sigma(C)$ alalım. $E_\sigma(C)$ yapısını düşünürsek herhangi bir $i \in \{1, ..., c\}$ için $v|_{\Omega_i} \in \{000, 110, 011, 101\}$ olur. σ sabitlenmiş noktası olmayan bir permüstasyon olduğundan bir i için eğer $v|_{\Omega_i} \neq 0$ ise $\sigma v|_{\Omega_i} + v|_{\Omega_i} \neq 000$ olur. Dolayısıyla

$$v + \sigma v \neq 0$$

elde ederiz. Yani v ve σv doğrusal bağımsız olur. $v \neq 0$ olduğunda sıfırdan farklı bloklar vardır ve $v|_{\Omega_i} \neq 000$ ise $v|_{\Omega_i}, \sigma v|_{\Omega_i}, \sigma^2 v|_{\Omega_i} \in \{110, 011, 101\}$ olur. σ sabit noktası olmayan bir permütasyon olduğu için $v|_{\Omega_i}, \sigma v|_{\Omega_i}, \sigma^2 v|_{\Omega_i}$ bu üç blok birbirinden farklıdır ve $\{110, 011, 101\}$ kümesinde herhangi ikisinin toplamı üçüncü elemanı vermektedir. Dolayısıyla $\sigma^2 v|_{\Omega_i} = \sigma v|_{\Omega_i} + v|_{\Omega_i}$ sağlanır. Bu durum her i için sağlanacağından $\sigma^2 v = \sigma v + v$ olur. ■

Önerme 4.16. *Eğer C, 2- boyutlu n uzunluklu sabit ağırlıklı olmayan ikili minimal bir kod ise ve $\sigma \in$ PAut(C) ise, bu durumda $n \geq 12$ olur.*

Kanıt. C sabit ağırlıklı olmadığı için $C \neq E_\sigma(C)$ sağlanır. Önerme 4.11 ve Teorem 4.10 sebebiyle $C = F_\sigma(C)$ olmalıdır. $\sigma \in$ PAut(C) mertebesi 3 olan sabit noktası olmayan bir permütasyon olduğu için uzunluk üçün katıdır ve Önerme 4.14 sebebiyle , $n \geq 9$ olmalıdır. $C = F_\sigma(C)$ için 9 uzunlukta tek bir seçenek vardır. $C = \{000000000, 111000111, 000111111, 111111000\}$. Bu da sabit ağırlıklıdır. Dolayısıyla $n \geq 12$ olmalıdır. ■

Not: $n = 12$ için $C = F_\sigma(C)$ koşulunu sağlayan ve minimal olan, sabit ağırlıklı olmayan bir kod vardır. $C = \{0, 111000111000, 000111111111, 111111000111\}$ kod istenilen koşulları sağlar. Bu kod 2-ağırlıklıdır ve $w_1 = 6$, $w_2 = 9$'dur ve $w_2 \neq 2w_1$ sağlanır. Teorem 2.4 sebebiyle C minimaldir.

Önerme 4.17. *C, 2-boyutlu ikili doğrusal bir kod ve $\sigma \in$ PAut(C) olsun. Eğer $C = E_\sigma(C)$ ise bu durumda C sabit ağırlıklıdır.*

Kanıt. C, 2-boyutlu bir kod ve $\sigma \in \mathrm{PAut}(C)$ olsun. Diyelim $C = E_\sigma(C)$ olsun. $v \neq 0$ olmak üzere $v \in C$ alalım. $E_\sigma(C)$, σ-değişmez olduğundan ve Önerme 4.15 sebebiyle, $E_\sigma(C) = \{0, v, \sigma v, \sigma^2 v\}$ yazabiliriz.

$$wt(v) = wt(\sigma \cdot v) = wt(\sigma^2 \cdot v)$$

olduğu için, C sabit ağırlıklı olur. ■

Önerme 4.18. *C ikili doğrusal bir kod ve $\sigma \in \mathrm{PAut}(C)$ olsun. Eğer $E_\sigma(C)$ 2-boyutlu ise $E_\sigma(C)$ minimaldir.*

Kanıt. Önerme 4.17'den $E_\sigma(C)$ sabit ağırlıklıdır. Dolayısıyla $E_\sigma(C)$ minimaldir. ■

Önerme 4.19. *C, 2-boyutlu, 9 uzunluklu ikili minimal bir kod ve $\sigma \in \mathrm{PAut}(C)$ olsun. Bu durumda C, sabit ağırlıklıdır.*

Kanıt. C, 2 boyutlu olduğu için, ya $C = E_\sigma(C)$ ya da $C = F_\sigma(C)$ olur. Eğer $C = E_\sigma(C)$ ise, $E_\sigma(C)$ sabit ağırlıklı olacağı için, C sabit ağırlıklıdır. $C = F_\sigma(C) = \langle x, y \rangle$ olsun. C minimal olduğu için $wt(x), wt(y) \in \{3, 9\}$ olamaz. Dolayısıyla $wt(x) = wt(y) = 6$ olur. Bu durumda

$$x, y \in \{111111000, 111000111, 000111111\}$$

olur. Dolayısıyla $C = \{0, 111111000, 111000111, 000111111\}$ olur. C sabit ağırlıklıdır. ■

Sonuç 4.20. *C 2-boyutlu, $n = 3k$ uzunluklu ikili minimal bir kod, $\sigma \in \mathrm{PAut}(C)$ olsun.*

i) Eğer $k \leq 3$ ise C sabit ağırlıklıdır.

ii) Eğer $k > 3$ ve $C = E_\sigma(C)$ ise C sabit ağırlıklıdır.

C, $n = 3k$ uzunluklu ikili bir kod ve $\sigma \in \mathrm{PAut}(C)$ olmak üzere, $v \in F_\sigma(C)$ için $v = v|_{\Omega_1} \cdots v|_{\Omega_k}$ yazılır. Burada her $i \in \{1, ...k\}$ için $v|_{\Omega_i} \in \{000, 111\}$ olur.

$$\pi_j(v|_{\Omega_j}) = \begin{cases} 1 & v|_{\Omega_j=111} \text{ ise,} \\ 0 & v|_{\Omega_j=000} \text{ ise,} \end{cases}$$

olacak şekilde $\pi = \pi_1 \dots \pi_k : F_\sigma(C) \to \mathbb{F}_2^k$, $\pi(v) = \pi_1(v|_{\Omega_1}) \cdots \pi_k(v|_{\Omega_k})$ bir fonksiyon tanımlansın

Tanım. [5] C, uzunluğu $n = 3k$ olan doğrusal bir kod ve $\sigma \in \mathrm{PAut}(C)$ olsun. Yukarıdaki şekilde tanımlanmış $\pi : F_\sigma(C) \to \mathbb{F}_2^k$ fonksiyona projeksiyon fonksiyonu denir.

Örnek 37. $F_\sigma(C) = \{0, 111000111, 111111000, 000111111\}$ olsun. $k = 3$ olur ve $\pi : F_\sigma(C) \to \mathbb{F}_2^3$,

$$\pi(111000111) = 101,\ \pi(000111111) = 011,\ \pi(111111000) = 110$$

Önerme 4.21. *C, $n = 3k$ uzunluklu ve $\sigma \in \mathrm{PAut}(C)$ olsun.*

$$\pi \ : \ F_\sigma(C) \longrightarrow \mathbb{F}_2^k$$

projeksiyon fonksiyonu olsun. Bu durumda $F_\sigma(C)$'nin minimal olması için gerekli ve yeterli koşul $\pi(F_\sigma(C))$'nin minimal olmasıdır.

Kanıt. Tanım gereği $v \in F_\sigma(C)$ için $wt(v) = 3wt(\pi(v))$ dir. $v \neq w \in F_\sigma(C)$ için $wt(v + w) \neq wt(w) - wt(v)$ olması için gerekli ve yeterli koşul

$$wt(\pi(v + w) \neq wt(\pi(w)) - wt(\pi(v))$$

eşitliğidir. Sonuç Teorem 2.3 sebebiyle elde edilir. ■

Önerme 4.22. *C, n uzunluklu ve $\sigma \in \mathrm{PAut}(C)$ olsun. Eğer $F_\sigma(C)$ 2-boyutlu minimal bir kod ise, bu durumda $n \geq 9$ olur.*

Kanıt. 2-boyutta kodun minimal olması için uzunluk en az 3 olmalıydı. O zaman Önerme 4.21 sebebiyle 2-boyutlu $F_\sigma(C)$ minimal ise $n \geq 9$ olur. ■

Not. 2-boyutlu, 3 uzunluklu yalnızca bir tane minimal kod olduğundan $2-$boyutlu 9 uzunluklu sadece bir tane minimal $F_\sigma(C)$ vardır.

Önerme 4.23. *C, 3-boyutlu, n uzunluklu, minimal bir kod ve $\sigma \in \mathrm{PAut}(C)$ olsun. Eğer $C = F_\sigma(C)$ ise $n \geq 18$ olur.*

Kanıt. C 3-boyutlu, minimal ve $\sigma \in \mathrm{PAut}(C)$ olsun. 3-boyutta minimal kod için Önerme 2.20 sebebiyle uzunluk en az 6 olur. Önerme 4.21 sebebiyle $F_\sigma(C)$'nin uzunluğu en az 18 olur. ■

Örnek 38.

$$F_\sigma(C) = \langle 111111111000000000, 000111111111111000, 111111000000111111 \rangle$$

Bu kod, uzunluğu 18 olan 3-boyutlu 2-ağırlıklı minimal koddur.

Önerme 4.24. *C 3-boyutlu minimal bir kod ve $\sigma \in \mathrm{PAut}(C)$ olsun. Eğer $C = F_\sigma(C)$ sabit ağırlıklı ise, C en az 21 uzunlukludur.*

Kanıt. $C = F_\sigma(C) = \langle x, y, z \rangle$ sabit ağırlıklı bir kod olsun. Bu durumda $wt(x) = wt(y) = wt(z) = a$ olur. $a = 3$ olamaz, aksi takdirde $wt(x + y) = 6$ olur. Çelişki elde ederiz. $a = 6$ da olamaz. Çünkü olsaydı

$$|\mathrm{supp}(x) \cap \mathrm{supp}(y)| = 3$$

$$|\mathrm{supp}(x) \cap \mathrm{supp}(z)| = 3$$

$$|\mathrm{supp}(y) \cap \mathrm{supp}(z)| = 3$$

olurdu. Bu durumda ya

$$|\mathrm{supp}(x) \cap \mathrm{supp}(y) \cap \mathrm{supp}(z)| = 3$$

olmalıdır ya da

$$|\text{supp}(x) \cap \text{supp}(y) \cap \text{supp}(z)| = 0$$

olmalıdır. İkinci durum olursa $z = x + y$ elde edilir, birinci durum olursa $wt(x + y + z) = 12$ olur. Her iki koşulda da çelişki elde edilir. $a = 9$ da olamaz. Eğer olursa

$$|\text{supp}(x) \cap \text{supp}(y)| \in \{3, 6\}$$

olmalıdır.

$$|\text{supp}(x) \cap \text{supp}(y)| = 3$$

olduğunda $wt(x+y) = 9+9-2\times 3 = 12$ olur. Sabit ağırlıklı olmakla çelişir.

$$|\text{supp}(x) \cap \text{supp}(y)| = 6$$

olduğunda $wt(x + y) = 9 + 9 - 2 \times 6 = 6$ olur ve yine sabit ağırlıklı olmakla çelişir. Bu durumda $a \geq 12$ olmalıdır. $a = 12$ için Lemma 2.1 sebebiyle $|\text{supp}(x) \cap \text{supp}(y)| = 6$, $|\text{supp}(x) \cap \text{supp}(z)| = 6$ ve $|\text{supp}(y) \cap \text{supp}(z)| = 6$ olur. Olası en kısa uzunluk için

$$|\text{supp}(x) \cap \text{supp}(y) \cap \text{supp}(z)| = 3$$

olmalıdır.

Genellemeyi kaybetmeden, minimallik koşulları ve sabit ağırlık koşulları için

$$x = 111111111111000000000$$

$$y = 111111000000111111000$$

$$z = 111000111000111000111$$

seçildiği taktirde $C = \langle x, y, z \rangle$ sabit ağırlıklı bir kod olur. Dolayısıyla uzunluk en az 21 olmalıdır.

■

Not. C minimal ise $E_\sigma(C)$ ve $F_\sigma(C)$, C'nin alt kodları olduğu için minimaldir. Fakat $E_\sigma(C)$ ve $F_\sigma(C)$ minimal iken direkt toplamları olan C minimal olmayabilir.

Örnek 39.

$$v = 110110000$$

$$w = 011011000$$

$$z = 000000111$$

kod sözcükleri için

$$E_\sigma(C) = \langle v, w \rangle$$

$$F_\sigma(C) = \langle z \rangle$$

olsun. Burada $E_\sigma(C)$ ve $F_\sigma(C)$ minimaldir. $v + w + z = 101101111$ olduğu için ve $\text{suppt}(z) \subset \text{suppt}(v + w + z)$ olduğu için C minimal olmaz.

Sonraki kısımlarda $E_\sigma(C)$ ve $F_\sigma(C)$ minimal iken hangi durumda C'nin de minimal olduğunu tartışacağız.

Örnek 40.

$$E_\sigma(C) = \langle 110110110000, 011011011000 \rangle$$

$$F_\sigma(C) = \langle 111000111111 \rangle$$

olsun. Burada $E_\sigma(C), F_\sigma(C)$ minimaldir ve dahası

$C = \{0, 110110110000, 011011011000, 111000111111,$
$101101101000, 100011100111, 010110001111, 010101010111\}$ minimaldir. Bu örneği incelediğimizde iki boyutlu $\langle 110110110000, 111000111111 \rangle$ alt uzayının da minimal olduğunu görmekteyiz.

Bu örnek genellenebilir mi?

Teorem 4.25. *C, 3-boyutlu bir kod ve $\sigma \in \mathrm{PAut}(C)$ olsun. Dahası*

$$E_\sigma(C) = \langle v, \sigma v \rangle$$

ve

$$F_\sigma(C) = \langle w \rangle$$

olan minimal kodlar olsun. Aşağıdaki önermeler denktir:

i) C minimaldir.

ii) $< v, w >$ alt kodu minimaldir.

Kanıt. C kodu minimal ise $\langle v, w \rangle$ alt kodunun minimal olacağı açıktır.

$\langle v, w \rangle$ alt kodunun minimal olduğunu kabul edelim. Teorem 4.10 sebebiyle $C = F_\sigma(C) \oplus E_\sigma(C)$ olur. Bu durumda

$$C = \{0, v, \sigma \cdot v, \sigma^2 \cdot v, w, v + w, \sigma \cdot v + w, \sigma^2 \cdot v + w\}$$

olur. Uzunluğun $3k$ şeklinde olacağını biliyoruz. $[k] = \{1, 2, ..., k\}$ olsun. Böyle bir kodun yedi tane iki boyutlu alt kodu vardır. Bunlar

$$\langle v,\ \sigma \cdot v \rangle = \langle v,\ \sigma^2 \cdot v \rangle \ (1)$$

$$\langle v,\ w \rangle = \langle v,\ v + w \rangle \ (2)$$

$$\langle v,\ \sigma \cdot v + w \rangle = \langle v,\ \sigma^2 \cdot v + w \rangle \ (3)$$

$$\langle \sigma \cdot v,\ w \rangle = \langle \sigma \cdot v,\ \sigma \cdot v + w \rangle \ (4)$$

$$\langle \sigma \cdot v,\ v + w \rangle = \langle \sigma \cdot v,\ \sigma^2 \cdot v + w \rangle \ (5)$$

$$\langle \sigma^2 \cdot v,\ w \rangle = \langle \sigma^2 \cdot v,\ \sigma^2 \cdot v + w \rangle \ (6)$$

$$\langle \sigma^2 \cdot v,\ v + w \rangle = \langle \sigma^2 \cdot v,\ \sigma \cdot v + w \rangle \ (7)$$

alt kodlarıdır. C kodunun minimal olduğunu göstermek için bu yedi tane alt kodun minimal olduğunu göstermek yeterlidir. (1) nolu alt kodun minimal olduğu açıktır. (2) nolu alt kodun minimal olduğu verilmiştir. Diğerleri için iki durum vardır.

1.durum: Her $i \in [k]$ için $v|_{\Omega_i} \neq 000$ olsun. $\langle v, w \rangle$ minimal olduğu için, w için en az bir tane blok sıfır olmalıdır. Bir $i \in [k]$ için $w|\Omega_i = 000$ olsun. Bu durumda

$$(v + w)|_{\Omega_i} = v|_{\Omega_i}$$

olur. Aynı şekilde

$$(\sigma \cdot v + w)|_{\Omega_i} = \sigma \cdot v|_{\Omega_i}$$

$$(\sigma^2 \cdot v + w)|_{\Omega_i} = \sigma^2 \cdot v|_{\Omega_i}$$

olur. Bu durumda

$$\{\sigma \cdot v + w, \sigma \cdot v, w\}$$

elemanlarından hiç biri bir diğerini içeremez. Benzer şekilde

$$\{\sigma^2 \cdot v + w, \sigma^2 \cdot v, w\}$$

elemanlarından hiç biri bir diğerini içeremez.

Dolayısıyla $\langle \sigma \cdot v, w \rangle$ ve $\langle \sigma^2 \cdot v, w \rangle$ alt kodları da minimal olur. (4) ve (6) nolu kodlar minimaldir.

$v|_{\Omega_i} \neq \sigma \cdot v|_{\Omega_i} = (\sigma \cdot v + w)|_{\Omega_i}$ olduğu için, $\langle v, \sigma \cdot v + w \rangle = \langle v, \sigma^2 \cdot v + w \rangle$ minimaldir. (3) nolu kod minimaldir. Aynı şekilde

$$\sigma \cdot v|_{\Omega_i} \neq (v + w)|_{\Omega_i}$$

olur. Bu durumda (5) nolu kod minimaldir.

$$\sigma^2 \cdot v|_{\Omega_i} \neq (v + w)|_{\Omega_i}$$

olur. (7) nolu kod minimaldir.

2.durum: Bir $i \in [k]$ için $v|_{\Omega_i} = 000$ olsun. Eğer $w|_{\Omega_i} = 000$ ise, $\langle v, w \rangle$ kodu minimal olduğu için, öyle bir $j \in [k]$ vardır ki $v|_{\Omega_j} \neq 000$ ve $w|_{\Omega_j} = 000$ sağlanır. Bu durumda da birinci durumdaki aşamaları kontrol ederek, C kodunun minimalliğine karar verilir.

Eğer $w|_{\Omega_i} \neq 000$ ise, bu durumda

$$(v + w)|_{\Omega_i} = w|_{\Omega_i}$$

olur. Aynı şekilde

$$(\sigma \cdot v + w)|_{\Omega_i} = w|_{\Omega_i}$$

$$(\sigma^2 \cdot v + w)|_{\Omega_i} = w|_{\Omega_i}$$

olur. Bu durumda (3), (4) ve (6) nolu kodlar minimaldir.

$$\sigma^2 \cdot v|_{\Omega_i} \neq (v + w)|_{\Omega_i}$$

$$\sigma \cdot v|_{\Omega_i} \neq (v + w)|_{\Omega_i}$$

olduğu için, (5) ve (7) nolu kodlar minimaldir. Dolayısıyla C minimaldir.

■

Teorem 2.12 yardımıyla $E_\sigma(C)$, $F_\sigma(C)$ ve $E_\sigma(C) \oplus F_\sigma(C)$ formunda minimal kodlar inşa etmek istersek [13] makalesindeki D çoklu kümelerinden farklı çoklu kümeleri bulmamız gerekmektedir.

Örnek 41. Theorem 2.12 deki koşulları sağlayacak bir D çoklu kümesini seçelim.

$$D = \{1010, 1111, 0101, 1011, 1101, 0110, 1001, 1110, 0111, 0010, 0011, 0001\}$$

kümesi $\mathbb{F}_2^4$ uzayının bir alt kümesidir ve $\text{rank}(D) = 4$ tür.

$$C = C(D) = \langle 110110110000, 011011011000, 110101011110, 011110101011 \rangle$$

olur. C, 4-boyutlu $C = E_\sigma(C)$ olan bir koddur. Ayrıca 2-ağırlıklı bir kod olup bu ağırlıklar 6 ve 8'dir. Önerme 2.4'i kullanarak C kodunun minimal olduğunu söyleyebiliriz. $E_\sigma(C)$ kodunun inşası için bulduğumuz bu çoklu küme D [13] makalesinde kullanılmış D çoklu kümelerinden farklıdır.

Örnek 42.

$$k = 3 \; n = 9 \; q = 2$$

$$D = \{d_1, d_2, \ldots, d_9\}, \; \text{rank}(D) = 3$$

$$D = \{101, 111, 011, 100, 110, 010, 000, 000, 000\}$$

Bu D çoklu kümesi Önerme 2.18'de verilen D'den farklıdır. Şimdi bu D'yi kullanarak oluşturduğumuz $C(D)$ kodunu inceleyelim.

$$C(D) = F_\sigma(C) \oplus E_\sigma(C) = \langle 110110000, 011011000, 111000000 \rangle$$

Bu kod minimaldir.

Örnek 43. $D = \{111, 111, 111, 110, 110, 110, 101, 101, 101, 100, 100, 100, 011, 011, 011, 010, 010, 010, 001, 001, 001\}$ kümesi için $\text{rank}(D) = 3$ olur.

$$x = 111111111111000000000$$

$$y = 111111000000111111000$$

$$z = 111000111000111000111$$

olmak üzere

$$C(D) = F_\sigma(C) = \langle x, y, z \rangle$$

olur bu kod sabit ağırlıklıdır, dolayısıyla minimaldir.

Kaynakça

[1] Alfarano, G., Borello, M., Neri, A., Ravagnani, A., (2022), Three Combinatorial Perspectives on Minimal Codes. SIAM Journal on Discrete Mathematics, 36 (1), 461-489.

[2] Alfarano, G.N., Borello, M., Neri, A., (2022), A geometric characterization of minimal codes and their asymptotic performance, Adv. Math. Commun. 16(1), 115-133.

[3] Ashikhmin, A., Barg, A.: (1998), Minimal vectors in linear codes. IEEE Trans. Inform. Theory 44(5), 2010– 2017.

[4] Berlekamp, E.R., McEliece, R.J., van Tilborg, H.C.A., (1978), On the inherent intractability of certain coding problems. IEEE Trans. Inform. Theory 24(3), 384–386.

[5] Bouyuklieva, S. and Russeva, R., (2020), "Binary LCD Codes Having an Automorphism of Odd Prime Order," 2020 Algebraic and Combinatorial Coding Theory (ACCT), Albena, Bulgaria, 1-5.

[6] Chabanne, H., Cohen, G., Patey, A., (2013), Towards secure two-party computation from the wiretap channel. In: Information Security and Cryptology—ICISC 2013, pp. 34–46. Springer, Berlin.

[7] Ding, C., Heng, Z. and Zhou, Z., (2018), "Minimal Binary Linear Codes," in IEEE Transactions on Information Theory, vol. 64, no. 10, 6536-6545.

[8] Ding, C., Tang, C., (2021), Designs From Linear Codes, World Scientific Publishing Company.

[9] Ding, C., Yuan, J. (2003), Covering and secret sharing with linear codes. In: Calude, C.S., et al. (eds.) Discrete Mathematics and Theoretical Computer Science. Lecture Notes in Computer Science, vol. 2731, pp. 11–25. Springer, Berlin.

[10] Heng, Z., Ding, C., Zhou, Z., (2018), Minimal linear codes over finite fields. Finite Fields Appl. 54, 176–196

[11] Huffman, W. C., (1986), Decomposing and shortening codes using automorphisms, IEEE Trans. Inform. Theory, **32**, 833–836.

[12] Huffman, W.C., Pless, V., (2003), Fundamentals of Error Correcting Codes, Cambridge University Press.

[13] Lu, W., Wu, X. and Cao, X., (2021), The Parameters of Minimal Linear Codes,Finite Fields and Their Application, **71**, 176-196.

[14] MacWilliams, J., Sloane, N., 1977, The theory of Error Correcting Codes, Vol 16. Elsevier.

[15] Massey, J.L., (1993), Minimal codewords and secret sharing. In: Proceedings of the 6th Joint Swedish-Russian International Workshop on Information Theory, pp. 276–279.

[16] Massey, J.L., (1995), Some applications of coding theory in cryptography. In: Codes and Cyphers: Cryptography and Coding IV, pp. 33–47.