T.C.
NECMETTİN ERBAKAN
ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

SONLU CİSİMLER ÜZERİNDEKİ DÜŞÜK AĞIRLIKLI MİNİMAL DOĞRUSAL KODLARIN TASARIMI

Mustafa Ali ÇATALKAYA

YÜKSEK LİSANS TEZİ

Matematik Anabilim Dalı

Eylül - 2024

KONYA

TEZ KABUL VE ONAYI

Mustafa Ali ÇATALKAYA tarafından hazırlanan " *SONLU CİSİMLER ÜZERİNDEKİ DÜŞÜK AĞIRLIKLI MİNİMAL DOĞRUSAL KODLARIN TASARIMI*" adlı tez çalışması 27/09/2024 tarihinde aşağıdaki jüri tarafından oy birliği / oy çokluğu ile Necmettin Erbakan Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalı'nda YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Jüri Üyeleri **İmza**

Başkan

Prof. Dr. Nihat AKGÜNEŞ _____

Danışman

Doç. Dr. Ahmet SINAK _____

Üye

Doç. Dr. Elif Segah ÖZTAŞ _____

Fen Bilimleri Enstitüsü Yönetim Kurulu'nun ..../ .../20.. gün ve ..... sayılı kararıyla onaylanmıştır.

Prof. Dr. Havvanur UÇBEYİAY

FBE Müdürü

TEZ BİLDİRİMİ

Bu tezdeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edildiğini ve tez yazım kurallarına uygun olarak hazırlanan bu çalışmada bana ait olmayan her türlü ifade ve bilginin kaynağına eksiksiz atıf yapıldığını bildiririm.

DECLARATION PAGE

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Mustafa Ali ÇATALKAYA

Tarih: 27/09/2024

ÖZET

YÜKSEK LİSANS TEZİ

SONLU CİSİMLER ÜZERİNDEKİ DÜŞÜK AĞIRLIKLI MİNİMAL DOĞRUSAL KODLARIN TASARIMI

Mustafa Ali ÇATALKAYA

Necmettin Erbakan Üniversitesi Fen Bilimleri Enstitüsü

Matematik Anabilim Dalı

Danışman: Doç. Dr. Ahmet SINAK

2024, 52 Sayfa

Jüri

Doç. Dr. Ahmet SINAK

Prof. Dr. Nihat AKGÜNEŞ

Doç. Dr. Elif Segah ÖZTAŞ

Kodlama teorisinde doğrusal kodlar, şifreleme sistemleri, depolama sistemleri, dijital iletişim gibi birçok alanda büyük öneme sahiptir. Özellikle, düşük ağırlıklı minimal doğrusal kodlar, sır paylaşım şemaları gibi gizlilik gerektiren sistemler için güvenli iletişim ve depolama sağlar. Bu tez çalışmasında, tek karakteristikli sonlu cisimler üzerinde düşük ağırlıklı minimal doğrusal kodların inşası çalışılmıştır. İlk olarak, literatürde bilinen inşa yönteminde D_{01} ve D_{SQ} tanım kümelerini kullanarak üç ağırlıklı ve iki ağırlıklı yeni doğrusal kod aileleri elde ettik. Daha sonra, doğrusal kodlar için yeni bir inşa yöntemi önerdik ve bu yöntemle D_0 tanım kümesine dayanan dört ağırlıklı yeni doğrusal kod ailesi elde ettik. Elde ettiğimiz yeni kodların Hamming ağırlıklarını ve ağırlık dağılımlarını hesapladık. Daha sonra, bu elde ettiğimiz yeni kodların minimal kod olduğunu gözlemledik. Böylece, elde edilen minimal kodların dual kodlarının Hamming mesafesini hesaplayarak iyi erişim yapılarına sahip sır paylaşım şemalarının tasarımında kullanılabileceğini gözlemledik ve bu sır paylaşım şemalarının erişim yapılarını verdik.

Anahtar Kelimeler: Doğrusal kodlar, Kodlama teorisi, Kriptografi, Sonlu cisimler

ABSTRACT

MS THESIS

THE CONSTRUCTION OF FEW-WEIGHT MINIMAL LINEAR CODES OVER FINITE FIELDS

Mustafa Ali ÇATALKAYA

THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCE OF NECMETTİN ERBAKAN UNIVERSITY

THE DEGREE OF MASTER OF SCIENCE / MATHEMATICS

Advisor: Assoc. Prof. Dr. Ahmet SINAK

2024, 52 Pages

Jury

Assoc. Prof. Dr. Ahmet SINAK

Prof. Dr. Nihat AKGÜNEŞ

Assoc. Prof. Dr. Elif Segah ÖZTAŞ

Linear codes in coding theory are of great importance in various fields such as cryptographic systems, storage systems, and digital communication. In particular, few-weight minimal linear codes provide secure communication and storage for systems requiring privacy such as secret sharing schemes. This thesis studies the construction of few-weight minimal linear codes over the odd characteristic finite fields. We first construct new families of linear codes with three-weights and two-weights by using new defining sets D_{01} and D_{SQ}, respectively, in the known construction method. Moreover, we introduce a new construction method for linear codes and obtain a new family of four-weight linear codes based on the defining set D_0. We calculate the Hamming weights and weight distributions of the obtained codes. Then, we observe that these obtained codes are minimal. Thus, by calculating the Hamming distance of their dual codes, we demonstrate that they can be used to design secret-sharing schemes with good access structures. We provide the access structures of these secret sharing schemes.

Keywords: Linear Codes, Coding Theory, Cryptography, Finite Fields

ÖNSÖZ

Yüksek lisans eğitimim ve tez sürecinin tüm aşamalarında beni destekleyen, bilgisi, sabrı ve tecrübeleriyle bana rehberlik eden çok kıymetli danışman hocam Doç. Dr. Ahmet SINAK'a en içten teşekkürlerimi sunarım.

Tüm eğitim hayatım boyunca daima yanımda olan sevgisini ve desteğini hiç esirgemeyen rahmetli babam Salih ÇATALKAYA'ya teşekkürlerimi sunarım.

Tezim boyunca daima yanımda olan, beni motive edip destekleyen sevgili eşime, anneme ve ablama teşekkür ederim.

Çalışmam, TÜBİTAK BİDEB 2211-Yurt İçi Lisansüstü Burs Programı kapsamında desteklenmiştir. Desteklerinden dolayı TÜBİTAK Bilim İnsanı Destek Programları Başkanlığı'na (BİDEB) teşekkürlerimi sunarım.

Mustafa Ali ÇATALKAYA

KONYA-2024

İÇİNDEKİLER

ÇİZELGELER LİSTESİ

Çizelge **Sayfa**

SİMGELER VE KISALTMALAR

Simge	Açıklama
$\mathbb{N}$	Doğal sayılar kümesi
$\mathbb{Z}$	Tam sayılar kümesi
$\mathbb{Q}$	Rasyonel sayılar kümesi
$\mathbb{C}$	Karmaşık sayılar kümesi
p	Bir asal sayı
q	Bir asal sayının kuvveti
t	Pozitif bir tam sayı
$\mathbb{F}_p$	p elemanlı bir cisim
$\mathbb{F}_{q^n}$	q^n elemanlı bir cisim
$\mathbb{F}_q^n$	$\mathbb{F}_q$ üzerinde n boyutlu bir vektör uzayı
$\mathrm{Tr}_{q^t}^{q^n}$	$\mathbb{F}_{q^n}$'den $\mathbb{F}_{q^t}$'e tanımlı iz fonksiyonu
$[n, k, d]$	Uzunluğu n, boyutu k, Hamming mesafesi d olan doğrusal kodun parametreleri
C	Doğrusal kod
$C^\perp$	C kodunun dual kodu
ϵ_p	İlkel p'ninci birim kök (Primitive p-th root of unity)
$''.''$	Skaler çarpım
$(\frac{a}{p})$	$a \in \mathbb{F}_p$ için Legendre sembolü
η_t	$\mathbb{F}_{p^t}$ üzerindeki kare karakter (quadratic character)

1. GİRİŞ

Günümüzde haberleşme, güvenlik ve benzeri durumlar için veri iletimi büyük bir önem taşımaktadır. Örneğin, uydular binlerce kilometre uzaklıktan veri aktarımı yapmakta ve bu verilerin bozulmadan, güvenilir bir şekilde iletilmesi gerekmektedir. Bu ihtiyaç, Kodlama Teorisi ile karşılanmaktadır. Kodlama teorisinin temelleri, 1940'lı yıllarda Claude Shannon'un "A Mathematical Theory of Communication" (Shannon, 1948) adlı çalışması ile atılmıştır.

Shannon'ın çalışması, uygun bir kodlamanın var olduğunu gösterse de bu kodlamanın nasıl oluşturulacağına dair net bir yol sunmamaktadır; yani çalışması yapısal (constructive) bir kanıt içermemektedir. Bu eksiklik, uygun kodlamanın nasıl geliştirilebileceğine yönelik çeşitli araştırmaları teşvik etmiş ve kodlama teorisinin ilerlemesine öncülük etmiştir. Bu alandaki ilk somut adımlardan biri, Richard W. Hamming'in hata düzeltme kodları (error-correcting codes) üzerine gerçekleştirdiği çalışmaların detaylarını yayımlamasıyla atılmıştır. Daha sonraki yıllarda kodlama teorisi hızla gelişmiş ve genişlemiştir.

Kodlama teorisi, gürültüye sahip kanallar üzerinden veri iletilirken ortaya çıkabilecek bozulmaların tespit edilmesi ve düzeltilmesiyle ilgilenir. Bu alan, bilgiyi daha okunabilir hale getirmeyi amaçlarken, veriyi daha zor anlaşılır hale getiren şifreleme (kriptografi) alanından farklıdır. Burada "ileti" ve "kanal" terimleri en geniş anlamlarıyla kullanılır. İletiler yalnızca konuşma ya da yazı değil, aynı zamanda ses, resim, müzik, video gibi farklı yapılar da olabilir. Verinin iletilmesi, bir noktadan diğerine aktarım (haberleşme) anlamına gelebileceği gibi, gelecekte kullanılmak üzere saklanması anlamına da gelebilir. Bu bağlamda kanal, uzay, atmosfer, telefon teli gibi fiziksel bir ortam olabileceği gibi, veri saklama sürecinde zamanı veya veriyi sakladığımız fiziksel ortamlara (örneğin, bir CD yüzeyi) da işaret edebilir.

Örneklerdeki kanalların hiçbirinin veri iletimi açısından mükemmel olmadığına dikkat edilmelidir. Örneğin, uzayda ve atmosferde oluşan manyetik alanlar radyo dalgalarını bozabilir; kötü hava koşulları telefon tellerindeki sinyalleri etkileyebilir; bir CD üzerindeki çizikler veya lekeler de depolanan veriyi bozabilir. Bu tür olumsuzluklarla karşılaşma olasılığı olan kanallara gürültülü kanal denir. Gürültüden dolayı veri iletiminde oluşabilecek hataların tespit edilmesi ve düzeltilmesi ise kodlama

teorisinin temel amaçlarından birisidir.

Doğrusal kodlar, doğrusal vektör uzayları oldukları için, üzerlerindeki cebirsel yapı sayesinde doğrusal olmayan kodlara kıyasla daha kolay tanımlanır ve daha pratik bir şekilde kullanılır. Bu nedenle doğrusal kodlar, graf teorisi, veri depolama sistemleri, iletişim, tüketici elektroniği, tasarım teorisi ve kriptografi gibi çeşitli alanlarda geniş uygulama alanlarına sahiptir. Özellikle, düşük ağırlığa sahip doğrusal kodlar, pratik kullanımda birçok sistemde kullanım alanı bulmaktadır.

Düşük ağırlıklı doğrusal kodların inşası için çeşitli yöntemler mevcut olup, bu yaklaşımlardan biri sonlu cisimler üzerinde tanımlı bazı özel fonksiyonların kullanılmasına dayanır (Carlet vd., 2005; Ding, 2016; Ding ve Ding, 2015; Mesnager, 2017; Schoenmakers, 1999; Tang vd., 2016). Fonksiyonlardan doğrusal kodlar oluşturmak, son zamanlarda literatürde kapsamlı bir şekilde çalışılan bir araştırma konusudur. Bu alanda önemli ilerlemeler kaydedilmiş olsa da, hâlâ aktif bir araştırma konusu olarak çalışılmaktadır. Literatürde bulunan birçok doğrusal kod, kuadratik fonksiyonlar (Ding, 2015, 2016; Ding ve Ding, 2015; Zhou vd., 2016), zayıf düzenli bükük fonksiyonlar (Ding, 2015, 2016; Mesnager, 2017; Tang vd., 2016; Wu vd., 2020), neredeyse mükemmel doğrusal olmayan fonksiyonlar (Carlet vd., 2005; Li vd., 2014) ve zayıf düzenli plato fonksiyonlar (Sınak, 2022; Mesnager vd., 2019a; Sınak, 2017; Mesnager vd., 2019b; Mesnager ve Sınak, 2020; Sınak, 2021a,b; Mesnager ve Sınak, 2020) gibi kriptografik fonksiyonlardan elde edilmiştir. Literatürde, fonksiyonlardan doğrusal kodlar elde etmek için kullanılan *birinci* inşa yöntemi ve *ikinci* inşa yöntemi olarak adlandırılan iki temel inşa yöntemi vardır. Literatürde, hem *birinci* inşa yöntemi (Carlet vd., 2005; Ding, 2016; Mesnager, 2017; Mesnager vd., 2019b) hem de *ikinci* inşa yöntemi (Ding, 2016; Ding ve Ding, 2015; Mesnager ve Sınak, 2020; Sınak, 2021a) kullanılarak birçok iyi parametreye sahip düşük ağırlıklı doğrusal kodlar üretilmiştir.

Doğrusal kodlar, modern kriptografik sistemlerin temel bileşenlerinden birisidir. Hata düzeltme, veri bütünlüğü, güvenli anahtar paylaşımı ve çeşitli saldırılara karşı koruma sağlayarak dijital dünyada kritik bilgilerin güvence altına alınmasında önemli bir rol oynar. Özellikle, düşük ağırıklı doğrusal kodlar, güvenli iletişim, sır paylaşım şemaları (Anderson vd., 1998; Carlet vd., 2005; Ding ve Ding, 2015; Yuan ve Ding, 2006), kimlik doğrulama kodları (Ding ve Wang, 2005) ve güvenli iki taraflı hesaplama (Schoenmakers, 1999) gibi alanlarda önemli uygulamalara sahiptir.

Sır paylaşım şemaları 1979'da Blakley (Blakley vd., 1979) ve Shamir (Shamir,

1979) tarafından önerilmiştir. Gerçek dünya uygulamalarının çeşitliliği nedeniyle birçok araştırmacı tarafından geniş çapta incelenmiştir. Sır paylaşım şemaları oluşturmak için çeşitli yöntemler vardır; bunlardan biri kodlama teorisindeki doğrusal kodlara dayanmaktadır. Aslında Shamir'in sır paylaşım şeması ile Reed-Solomon kodları arasındaki bağlantı 1981'de McEliece ve Sarwate (McEliece ve Sarwate, 1981) tarafından verilmiş ve o zamandan beri doğrusal kodlardan sır paylaşım şemalarının oluşturulması birçok araştırmacı tarafından kapsamlı bir şekilde incelenmiştir (Carlet vd., 2005; Ding ve Yuan, 2003; Ding ve Ding, 2015).

1.1. Motivasyon Ve Tezin Önemi

Kodlama teorisi, bilginin hataya dayanıklı bir biçimde aktarımını ve depolanmasını sağlamak için matematiksel yapıların geliştirilmesini amaçlayan önemli bir araştırma alanıdır. Günümüzde özellikle kriptografi, veri güvenliği ve dijital iletişim gibi alanlarda kodlama teorisi, güvenilir ve verimli sistemlerin oluşturulmasında kritik bir rol oynamaktadır. Bu bağlamda, doğrusal kodlar ve onların minimal kod özellikleri, hem teorik açıdan hem de birçok alanda kullanılabilmesi nedeniyle uygulama açısından büyük bir ilgi görmektedir.

Literatürde düşük ağırlıklı doğrusal kodlar oluşturmak için çeşitli yöntemler vardır, bunlardan birisi de sonlu cisimler üzerindeki bazı özel fonksiyonlardan doğrusal kod inşasıdır. Son zamanlarda, Zhu ve ark. (Zhu ve Liao, 2023), sonlu cisimler üzerinde iz fonksiyonları kullanarak iki ağırlıklı doğrusal kodların yeni ailelerini inşa etmişlerdir. Ayrıca, Cheng ve ark. (Cheng vd., 2022) yeni bir inşa yöntemi üzerinde iz fonksiyonları kullanarak iki ağırlıklı yeni kod aileleri elde etmişlerdir. Bu tez çalışmasında, kodlama teorisine katkıda bulunmak amacıyla, literatürde yer alan (Zhu ve Liao, 2023) ve (Cheng vd., 2022) çalışmaları temel alınarak düşük ağırlıklı yeni doğrusal kod aileleri üretilmiştir. Elde edilen bu kodların minimal kodlar olduğu gözlemlenmiş ve bu kodların dual kodlarının Hamming mesafeleri Pless güç momentleri kullanılarak MAGMA cebirsel programlama yazılımı (Bosma vd., 1997) yardımıyla hesaplanmıştır. Hesaplamalar sonucunda dual kodların Hamming mesafelerinin 2 olduğu görülmüştür. Son olarak, üretilen kodların dual kodlarına dayalı sır paylaşım şemalarının erişim yapıları da verilmiştir.

Bu tezin temel amacı, gerçek dünyada uygulama alanlarına sahip olabilecek

sonlu cisimler üzerinde düşük ağırlıklı minimal doğrusal kodlar üretmektir. Ayrıca, bu tezde elde edilen kodların dual kodlarına dayalı sır paylaşım şemalarının erişim yapılarının tasarımı hedef alınmıştır. Bu sayede, doğrusal kodlar ve sır paylaşım şemaları konularında pratik ve teorik fayda sağlayacak yeni yaklaşımlar geliştirilmiştir. Bu tez çalışması, hem kriptografi alanında hemde kodlama teorisi alanında literatüre katkı sağlamaktadır.

1.2. Organizasyon

Bu tez aşağıdaki gibi organize edilmiştir. Bölüm 2'de sonlu cisimler, kodlama teorisi ve kod inşası ile ilgili gerekli tanımları veriyoruz. Bölüm 3'te (Zhu ve Liao, 2023) makalesini ayrıntılı çalıştık ve sonuçlarını sunduk. Bölüm 4'te (Zhu ve Liao, 2023) çalışmasındaki kod inşa yönteminde D_λ, D_{01} ve D_{SQ} tanım kümeleri kullanılarak düşük ağırlıklı yeni kod aileleri elde ediyoruz ve oluşturulan kodların ağırlık dağılımlarını hesaplıyoruz. Bölüm 5'te (Zhu ve Liao, 2023) ve (Cheng vd., 2022) çalışmalarındaki inşa yöntemlerini sentezleyerek yeni bir inşa yöntemi tasarlıyoruz ve bu tasarımda D_0 kümesini kullanarak yeni bir doğrusal kod ailesi elde ediyoruz. Ayrıca ağırlık dağılımını da hesaplıyoruz. Bölüm 6'da, bu tezde elde edilen kodların minimal kodlar olduğunu gösteriyoruz. Dual kodların Hamming mesafesini, MAGMA programı (Bosma vd., 1997) yardımıyla hesaplıyoruz ve minimal kodların dual kodlarındaki sır paylaşım şemalarının erişim yapılarını veriyoruz. Son olarak, Bölüm 7'de tezde verilen sonuçlar özetlenmiş ve önerilerle tez tamamlanmıştır.

2. TEMEL TANIMLAR

Bu bölümde sonlu cisim teorisi, kriptografi ve kodlama teorisindeki temel notasyonları veriyoruz ve gerekli bazı tanımları/sonuçları hatırlatıyoruz. Temel teori ve kavramlar hakkında daha fazla bilgi için okuyucunun sonlu cisim teorisi için (Lidl ve Niederreiter, 1997; Mullen ve Panario, 2013), kriptografi için (Budaghyan, 2015; Carlet, 2010a,b; Mesnager, 2016) ve kodlama teorisi için (Huffman ve Pless, 2010) çalışmasını incelemesi önerilir.

2.1. Sonlu Cisim Teorisi

p bir asal sayı olsun. $\mathbb{Z}_p := \mathbb{Z}/_{\langle p \rangle}$ cismi Galois cismi olarak adlandırılır ve genellikle $\mathbb{F}_p$ ile gösterilir. p bir asal sayı ve n bir pozitif tamsayı olmak üzere, $\mathbb{F}_p$ üzerinde derecesi n olan indirgenemez bir polinom ile p^n elemanlı sonlu bir cisim genişlemesi oluşturulabilir. $g(x) \in \mathbb{F}_p[x]$ derecesi n olan indirgenemez bir polinom olmak üzere kalan sınıf halkası

$$\mathbb{F}_p[x]/_{\langle g(x) \rangle} = \{a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} : 0 \leq i \leq n-1 \text{ için } a_i \in \mathbb{F}_p\} \qquad (2.1)$$

p^n elemanlı sonlu bir cisim oluşturur. p^n elemanlı bu sonlu cisim izomorfizma altına tektir ve $\mathbb{F}_{p^n}$ ile gösterilir. ζ üreteci için $\mathbb{F}_{p^n}^\star = \langle \zeta \rangle$ kümesi çarpma işlemi ile birlikte $p^n - 1$ elemanlı çarpımsal bir devirli gruptur. $\mathbb{F}_p$ cismi ise $\mathbb{F}_{p^n}$ cisminin içerdiği asal cisimdir.

$\alpha \in \mathbb{F}_{p^n}$ elemanı indirgenemez $g(x)$ polinomunun kökü olsun. $B = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\} \subseteq \mathbb{F}_{p^n}$ kümesini baz olarak kabul eden $\mathbb{F}_p$ üzerindeki n boyutlu vektör uzayı

$$\mathbb{F}_p^n = \langle B \rangle = \{a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} : 0 \leq i \leq n-1 \text{ için } a_i \in \mathbb{F}_p\} \quad (2.2)$$

şeklinde tanımlanır. Her $a \in \mathbb{F}_{p^n}$ elemanı, $a = (a_0, a_1, ..., a_{n-1}) \in \mathbb{F}_p^n$ vektörü olarak görülebilir; burada $0 \leq i \leq n-1$, $a_i \in \mathbb{F}_p$'dir. Bu tanımlama, denklem (2.1)'de tanımlanan $\mathbb{F}_{p^n}$ cisim genişlemesine ile denklem (2.2)'deki $\mathbb{F}_p^n$ vektör uzayı arasında bir izomorfizm verir. $\mathbb{F}_p$ üzerinde $\mathbb{F}_p^n$ vektör uzayının boyutu, $dim(\mathbb{F}_p^n) = n$, B kümesinin eleman sayısıdır. $\mathbb{F}_p^n$ vektör uzayının eleman sayısı $\#\mathbb{F}_p^n = p^{dim(\mathbb{F}_p^n)} = p^n$ ile gösterilir.

Şimdi iz fonksiyonunun tanımını verelim.

Tanım 2.1 *$k \mid n$ olmak üzere n ve k iki pozitif tamsayı olsun. $\mathbb{F}_p^n$ sonlu cisminden alt cisim $\mathbb{F}_{p^k}$'ya göreceli iz fonksiyonu $\mathrm{Tr}_{p^k}^{p^n}$ şu şekilde tanımlanır:*

$$\mathrm{Tr}_{p^k}^{p^n}(x) = \sum_{i=0}^{\frac{n}{k}-1} x^{p^{ki}} = x + x^{p^k} + \cdots + x^{p^{n-k}}.$$

Her $x \in \mathbb{F}_{p^n}$ için $\mathbb{F}_p$ üzerindeki mutlak iz fonksiyonu $\mathrm{Tr}_p^{p^n}(x) = x + x^p + \cdots + x^{p^{n-1}}$ ile tanımlanır. Bu tezde, mutlak iz fonksiyonu kısaca Tr ile ifade edilecektir.

Önerme 2.1 . *İz fonksiyonu aşağıdaki önemli özelliklere sahiptir:*

- *Örten fonksiyondur.*
- *Doğrusal fonksiyondur: Tüm $x, y \in \mathbb{F}_{p^n}$ ve $a, b \in \mathbb{F}_p$ için $\mathrm{Tr}_p^{p^n}(ax + by) = a\mathrm{Tr}_p^{p^n}(x) + b\mathrm{Tr}_p^{p^n}(y)$.*
- *Bir cisim genişlemesi zincirinde geçişme özelliğini sağlar, yani $x \in \mathbb{F}_{p^n}$ için $\mathrm{Tr}_p^{p^n}(x) = \mathrm{Tr}_p^{p^k}\left(\mathrm{Tr}_{p^k}^{p^n}(x)\right)$.*
- *Her $x \in \mathbb{F}_{p^n}$ için $\mathrm{Tr}_p^{p^n}(x^p) = \mathrm{Tr}_p^{p^n}(x)$.*

Aşağıda Legendre sembolünü tanımlayalım.

Legendre Sembolü: a pozitif bir tam sayı, p ise tek asal sayı olsun. Aşağıdaki ikinci dereceden kongrüansı göz önünde bulunduralım:

$$x^2 \equiv a \pmod{p}. \tag{2.3}$$

Eğer (2.3)'deki kongrüans denklemi $\mathbb{F}_p^\star$ üzerinde bir çözüme sahipse, yani $\sqrt{a} \in \mathbb{F}_p^\star$ olacak şekilde bir çözüm varsa, a sayısına $\mod p$'de ikinci dereceden kalan denir. Eğer böyle bir çözüm yok, yani $\sqrt{a} \notin \mathbb{F}_p^\star$ ise, $a \mod p$'de ikinci dereceden kalan yoktur denir. *Legendre sembolü* şu şekilde tanımlanır:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{eğer } p|a, \\ 1 & \text{eğer } a,\ p \text{ modülünde kuadratik rezidü (tam kare) ise,} \\ -1 & \text{eğer } a,\ p \text{ modülünde kuadratik rezidü değil ise.} \end{cases}$$

Lemma 2.1 *Legendre sembolü aşağıdaki kongrüansı sağlar:*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}. \tag{2.4}$$

İspat p, a'yı böldüğünde her iki tarafın da $0 \mod p$ olduğu açıktır. p'nin a'yı bölmediğini varsayalım. ζ, $\mathbb{F}_p$ cisminin bir üreteci olsun. Bazı i'ler için tüm ikinci dereceden kalanların ζ^{2i} formunda olduğuna dikkat ediniz. $i \in \mathbb{N}$ için $a \equiv \zeta^{2i} \pmod p$ ise o zaman

$a^{\frac{p-1}{2}} \equiv \zeta^{2i(\frac{p-1}{2})} \equiv \zeta^{i(p-1)} \equiv (\zeta^{p-1})^i \equiv 1 \pmod p$. Bu (2.4)'ün geçerli olduğunu gösterir. $i \in \mathbb{N}$ için ikinci dereceden olmayan bir $a \equiv \zeta^{2i+1} \pmod p$ kalanı için şunu elde ederiz:

$$a^{\frac{p-1}{2}} \equiv \zeta^{(2i+1)\frac{p-1}{2}} \equiv \zeta^{i(p-1)}\zeta^{\frac{p-1}{2}} \equiv \zeta^{\frac{p-1}{2}} \equiv -1 \pmod p.$$

Bu, (2.4)'ün bu durumda da geçerli olduğunu göstermektedir. Kanıt tamamlandı.

Legendre sembolü, pozitif a, b tamsayıları ve tek asal sayılar p, q için aşağıdaki özellikleri sağlar:

- Legendre sembolü çarpımsal özelliğe sahiptir: $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. Lemma 2.1'e göre,

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \pmod p = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \pmod p \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

- Eğer $p \nmid a$ ise $\left(\frac{a^2}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{p}\right) = 1$ ve $\left(\frac{1}{p}\right) = 1$ olur.
- Eğer $a \equiv b \pmod p$ ise $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$'dir.
- $$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod p = \begin{cases} 1 & \iff p \equiv 1 \pmod 4, \\ -1 & \iff p \equiv 3 \pmod 4. \end{cases}$$

Bu tezde, p tek bir asal sayı olmak üzere $a \in \mathbb{F}_p^\star$ için $\left(\frac{a}{p}\right)$ ifadesi Legendre sembolünü ifade eder.

2.2. Kodlama Teorisinde Doğrusal Kodlar

Kodlama teorisindeki en önemli kod sınıfı doğrusal kodlardır. Doğrusal kodlar, çeşitli pratik uygulama alanlarına sahip oldukları için literatürde ayrıntılı olarak çalışılmaktadır. Kodlama teorisi hakkında daha fazla bilgi edinmek için okuyucu (Huffman ve Pless, 2010) kitabını inceleyebilir.

Doğrusal Kodlar: p bir asal sayı ve n, k pozitif tam sayılar olsun. $\mathbb{F}_p$ cismi üzerinde uzunluğu n, boyutu k olan C doğrusal kodu, n-boyutlu $\mathbb{F}_p^n$ vektör uzayının k boyutlu bir doğrusal alt uzayıdır ve $[n,k]_p$ şeklinde gösterilir. Ayrıca, minimum Hamming mesafesi d olan C kodu $[n,k,d]_p$ ile gösterilir. d ile ifade edilen minimum Hamming mesafesi, C kodunun hata düzeltme kapasitesini tespit eder. Doğrusal kodun elemanlarına (vektör uzayının vektörlerine) *kod sözcükleri (codewords)* denir. Kodun minimum Hamming mesafesi, sıfırdan farklı kod sözcüklerinin minimum Hamming ağırlığıdır. $\mathbf{a} = (a_0, \ldots, a_{n-1}) \in \mathbb{F}_p^n$ kod sözcüğünün Hamming ağırlığı

$$\mathrm{supp}(\mathbf{a}) := \{0 \leq i \leq n-1 : a_i \neq 0\}$$

kümesinin eleman sayısıdır, ve $wt(\mathbf{a}) = \#\mathrm{supp}(\mathbf{a})$ ile gösterilir.

A_w, C kodunun Hamming ağırlığı w olan kod sözcüklerinin sayısını göstersin. O halde, $(1, A_1, \ldots, A_n)$ vektörüne C kodunun *ağırlık dağılımı* ve $1 + A_1 y + \cdots + A_n y^n$ polinomuna C kodunun *ağırlık sayıcı* denir. Ağırlık dağılımındaki sıfırdan farklı A_w sayısı t ise C koduna *t-ağırlıklı kod* denir. Doğrusal kodların ağırlık dağılımı oldukça dikkat çekmektedir. Hata tespiti ve düzeltme olasılığını tahmin etmek için önemli bilgiler içerdiğinden kodlama teorisinde yaygın olarak çalışılmaktadır. Ayrıca bir $\mathbf{c}$ kod sözcüğünün tam ağırlık sayıcı monomiyaldir:

$$w(\mathbf{c}) = w_0^{t_0} w_1^{t_1} \ldots w_{p-1}^{t_{p-1}}$$

$w_0, w_1, \ldots, w_{p-1}$ değişkenlerinde, t_i $(0 \leq i \leq p-1)$, $\mathbf{c}$ kod sözcüğünün i değerine eşit bileşenlerinin sayısını belirtir. C kodunun tam ağırlık sayıcı şu şekilde tanımlanır:

$$W(C) = \sum_{\mathbf{c} \in C} w(\mathbf{c})$$

Doğrusal bir C kodunun *dual kodu*, $\mathbb{F}_p$ cismi üzerinde

$$C^{\perp} = \{\mathbf{b} \in \mathbb{F}_p^n : \mathbf{b} \cdot \mathbf{a} = 0 \text{ her } \mathbf{a} \in C\},$$

şeklinde tanımlanan n uzunluklu ve $(n-k)$ boyutlu bir alt uzaydır. Burada " $\cdot$ ", $\mathbb{F}_p^n$ vektör uzayı üzerinde bir iç çarpımdır. $C^{\perp}$ dual kodu $[n, n-k, d^{\perp}]_p$ parametreleri ile gösterilir. Burada $d^{\perp}$, $C^{\perp}$ dual kodunun minimum Hamming mesafesini belirtir.

Herhangi bir doğrusal kod doğrusal alt uzay olduğu için bir baza sahiptir. Doğrusal bir kodun kod sözcüklerinden herhangi biri, baz vektörlerinin doğrusal bir kombinasyonu olarak yazılabilir. Doğrusal bir C kodunun G *üreteç matrisi*, satırları C

kodu için bir baz oluşturan $k \times n$ boyutlu bir matrisdir. Diğer bir ifadeyle, G üreteç matrisi, satır vektörleri C doğrusal alt uzayını oluşturan bir matristir. $C^{\perp}$ dual kodunun bir *üreteç matrisi* H, satırları $C^{\perp}$ dual kodunun bazını oluşturan $(n-k) \times n$ boyutlu bir matrisdir, yani H matrisinin satır vektörleri $C^{\perp}$ dual kodunu oluşturur.

2.3. Yardımcı Sonuçlar

Bu bölümde, ilerleyen bölümlerde kullanacağımız gerekli sonuçları veriyoruz. t pozitif tam sayı ve p tek asal sayı olmak üzere $q = p^t$ olsun. q elemanlı sonlu cisim $\mathbb{F}_q$ (denk olarak, $\mathbb{F}_{p^t}$) ile gösterilir. Bu tezde, $\mathbb{F}_{p^t}$ cisminden $\mathbb{F}_p$ cismine tanımlı mutlak iz fonksiyonu Tr ile gösterilmektedir.

$\mathbb{F}_{p^t}$ cisminin toplamsal karakteri χ, $\mathbb{F}_{p^t}$ cisminden $U = \{u : |u| = 1, u \in \mathbb{C}\}$ çarpım grubuna bir fonksiyondur. Bu fonksiyon $x, y \in \mathbb{F}_{p^t}$ için $\chi(x+y) = \chi(x)\chi(y)$ olacak şekilde tanımlanır. Her $b \in \mathbb{F}_{p^t}$ için $x \in \mathbb{F}_{p^t}$ olmak üzere

$$\chi_b(x) = \epsilon_p^{\mathrm{Tr}(bx)}$$

fonksiyonu $\mathbb{F}_{p^t}$ cisminin toplamsal karakteri olarak adlandırılır. Burada $\epsilon_p = e^{\frac{2\pi\sqrt{-1}}{p}}$, kompleks sayılar cisminin ilkel p'ninci birim köküdür. $b = 0$ olduğunda, $x \in \mathbb{F}_{p^t}$ için $\chi_0(x) = 1$'dir. $\chi := \chi_1$ karakteri $\mathbb{F}_{p^t}$'nin kanonik toplamsal karakteri olarak adlandırılır ve $\mathbb{F}_{p^t}$'nin her toplamsal karakteri $\chi_b(x) = \chi(bx)$ olarak yazılabilir. Toplamsal karakterler için ortogonallik özelliği aşağıda verilmektedir.

$$\sum_{x \in \mathbb{F}_{p^t}} \epsilon_p^{\mathrm{Tr}(bx)} = \begin{cases} p^t, & b = 0; \\ 0, & b \neq 0. \end{cases}$$

$\mathbb{F}_{p^t}$ üzerindeki kuadratik karakter (quadratic character) η_t şu şekilde tanımlanır: $\eta_t(0) = 0$, $\eta_t(a) = 1$ eğer a elemanı $\mathbb{F}_{p^t}^{\star}$'da tam kare ise, ve $\eta_t(a) = -1$ eğer a elemanı $\mathbb{F}_{p^t}^{\star}$'da tam kare değil ise. Özel olarak, $t = 1$ için $\mathbb{F}_p^{\star}$ üzerindeki kuadratik karakter η_1 ile gösterilir. Dolayısıyla, $\left(\frac{a}{p}\right)$ Legendre değeri $\eta_1(a)$ kuadratik karakteri ile tanımlanabilir. Bu tezde, $p^* = \left(\frac{-1}{p}\right) p = \eta_1(-1)p$ şeklinde ifade edilmiştir.

$\mathbb{F}_{p^t}$ üzerindeki kuadratik Gauss toplamı ise şu şekilde tanımlanır:

$$G_t = \sum_{c \in \mathbb{F}_{p^t}^{\star}} \eta_t(c)\chi(c) = \sum_{c \in \mathbb{F}_{p^t}} \eta_t(c)\chi(c).$$

Şimdi, kuadratik karakterler ve kuadratik Gauss toplamları için bazı özellikler aşağıda verilmiştir.

Lemma 2.2 *(Lidl ve Niederreiter, 1997)* $\sum_{a\in\mathbb{F}_p} \epsilon_p^{ab} = \begin{cases} p, & \text{eğer } b = 0; \\ 0, & \text{eğer } b \in \mathbb{F}_p^\star. \end{cases}$

Lemma 2.3 *(Ding ve Ding, 2015, Lemma 7).* $x \in \mathbb{F}_p^\star$ *için;*

$$\eta_t(x) = \begin{cases} 1, & 2|t; \\ \eta_1(x), & \text{diğer durumlarda.} \end{cases}$$

Lemma 2.4 *(Lidl ve Niederreiter, 1997, Teorem 5.15).* $\mathbb{F}_{p^t}$ *üzerindeki Gauss toplamları* G_t *için;*

$$G_t = (-1)^{t-1}(\sqrt{-1})^{\frac{(p-1)^2 t}{4}} p^{\frac{t}{2}}.$$

Lemma 2.5 *(Lidl ve Niederreiter, 1997, Teorem 5.33).* $a_2 \neq 0$ *olmak üzere* $f(x) = a_2x^2 + a_1x + a_0 \in \mathbb{F}_{p^t}[x]$ *polinomu için*

$$\sum_{c\in\mathbb{F}_{p^t}} \chi(f(c)) = G_t\eta_t(a_2)\chi(a_0 - a_1^2(4a_2)^{-1}).$$

Lemma 2.6 *(Lidl ve Niederreiter, 1997, Teorem 5.33)*

$$\sum_{x\in\mathbb{F}_{p^t}} \epsilon_p^{\mathrm{Tr}(ax^2+bx)} = G(\eta_t)\eta_t(a)\epsilon_p^{-\mathrm{Tr}(\frac{b^2}{4a})}.$$

Aşağıda, Pless güç momentlerini (The Pless Power Moment-PPM) verelim.

Lemma 2.7 *(Huffman ve Pless, 2010, Page 260)* C *doğrusal kodu* $\mathbb{F}_p$ *üzerinde bir* $[n, k, d]$ *kodu olsun.* C *ve* $C^\perp$ *kodlarının ağırlık dağılımları sırasıyla* $(1, A_1, \ldots, A_n)$ *ve* $(1, A_1^\perp, \ldots, A_n^\perp)$ *ile gösterilsin. İlk dört Pless güç momentleri şu şekilde verilir:*

$$\begin{aligned}
\sum_{i=0}^{n} A_i &= p^k, \\
\sum_{i=0}^{n} iA_i &= p^{k-1}\left(pn - n - A_1^\perp\right), \\
\sum_{i=0}^{n} i^2A_i &= p^{k-2}\left((p-1)n(pn-n+1) - (2pn - p - 2n + 2)A_1^\perp + 2A_2^\perp\right), \\
\sum_{i=0}^{n} i^3A_i &= p^{k-3}[(p-1)n(p^2n^2 - 2pn^2 + 3pn - p + n^2 - 3n + 2) \\
&\quad -(3p^2n^2 - 3p^2n - 6pn^2 + 12pn + p^2 - 6p + 3n^2 - 9n + 6)A_1^\perp \\
&\quad +6(pn - p - n + 2)A_2^\perp - 6A_3^\perp].
\end{aligned}$$

Pless güç momentleri, doğrusal kodların ve dual kodlarının parametrelerini hesaplamak için kullanılabilir.

2.4. Doğrusal Kodların Sır Paylaşım Şemalarında Uygulanması

Bu bölümde öncelikle sır paylaşım şemasını tanımlayıp ardından doğrusal kodların sır paylaşım şemalarında uygulamasını vereceğiz.

2.4.1. Sır Paylaşım Şemaları

Bir sır paylaşım şeması şunlardan oluşur:

- bir dağıtıcı D ve $(n-1)$ katılımcıdan oluşan bir grup $\mathcal{P} = \{P_1, P_2, \ldots, P_{n-1}\}$;
- bir sır uzayı S;
- $(n-1)$ tane paylaşım uzayı $S_1, S_2, \ldots, S_{n-1}$;
- bir paylaşım hesaplama prosedürü; ve
- bir sır kurtarma prosedürü.

Dağıtıcı D, S'den bir gizli (sır) s seçer ve her katılımcı P_i için S_i'ye ait olan bir s_i payını (paylaşım hesaplama prosedürüyle) hesaplar ve ardından payı P_i'ye verir; burada $1 \leq i \leq n-1$. Katılımcıların uygun bir alt kümesi, sır kurtarma prosedürü ile kendi pay değerlerinden sır s'i kurtarabilirler. s sırrını kurtarabilecek bir grup katılımcıyı kapsayan herhangi bir küme s sır değerini kurtarabilir. Paylaşım hesaplama prosedürü ve sır s yalnızca D tarafından bilinirken, sır kurtarma prosedürü $\mathcal{P}$'deki tüm katılımcılar tarafından bilinmektedir.

Tanım 2.2 *Pay değerlerini kullanarak gizli değeri (sır değerini) kurtarabilen katılımcılardan oluşan gruba erişim kümesi adı verilir. Tüm erişim kümelerinin oluşturduğu kümeye, sır paylaşım şemasının erişim yapısı adı verilir. Daha az katılımcıya sahip uygun alt kümelerinden herhangi biri gizli değeri kurtaramazsa bu erişim kümesine minimal erişim kümesi adı verilir.*

Not 2.1 *Herhangi bir erişim kümesinin herhangi bir üst kümesi aynı zamanda bir erişim kümesi ise bu sır paylaşım şeması monoton erişim yapısına sahiptir. Böyle bir sır paylaşım şemasında erişim yapısı, minimal erişim kümeleriyle tamamen karakterize edilir.*

Sır paylaşım şemaları oluşturmak için çeşitli yöntemler vardır. Bunlardan biri, aşağıdaki alt bölümde açıklanacak olan kodlama teorisindeki doğrusal kodlara dayanmaktadır.

2.4.2. Doğrusal Kodlardan Sır Paylaşım Şemalarının Oluşturulması

Shamir'in sır paylaşım şeması ile Reed-Solomon kodları arasındaki bağlantı 1981'de (McEliece ve Sarwate, 1981) verildi ve o zamandan beri doğrusal kodlardan sır paylaşım şemalarının oluşturulması yaygın olarak çalışılmaktadır.

Doğrusal kodlardan elde edilen sır paylaşım şemalarında aşağıdaki iki temel problem akla gelir:

- Doğrusal koda dayalı sır paylaşım şemasının erişim yapısı nasıl bulunabilir?
- Bilgi oranını en aza indirerek, sır paylaşım şemasının iyi bir erişim yapısına sahip olması için doğrusal bir kod nasıl oluşturulabilir?

İlk soru doğrusal kodların kapsama problemine eşdeğerdir. İkinci soru ise birinci sorunun çözümlerine bağlıdır ve daha genel bir problemdir.

Sır paylaşım şemalarının oluşturulmasında doğrusal kodları kullanmanın birkaç yolu vardır. 1993 yılında Massey (Massey, 1993, 1995) doğrusal hata düzeltme kodlarını kullanarak aşağıdaki sır paylaşım şemalarının yapısını tanıttı. Doğrusal bir $[n, k, d]_p$ C kodu verildiğinde, onun $k \times n$ boyutlu G üreteç matrisi, $G = [\mathbf{g}_0, \mathbf{g}_1, \ldots, \mathbf{g}_{n-1}]$ ile gösterilir. C koduna dayalı sır paylaşım şemasında s, $\mathbb{F}_p$ cisminin bir elemanıdır. s sır değerine göre payları hesaplamak için, D dağıtıcısı, iki vektörün iç çarpımı $s = \mathbf{u}\mathbf{g}_0$ olacak şekilde rastgele bir $\mathbf{u} = (u_0, u_1, \ldots, u_{k-1}) \in \mathbb{F}_p^k$ vektörünü seçer. $\mathbf{u} \in \mathbb{F}_p^k$ gibi p^{k-1} tane vektörlerin mevcut olduğuna dikkat edelim. Dağıtıcı D karşılık gelen kod sözcüğünü şu şekilde hesaplar:

$$\mathbf{l} = (l_0, l_1, \ldots, l_{n-1}) = \mathbf{u}G = (\mathbf{u}\mathbf{g}_0, \mathbf{u}\mathbf{g}_1, \ldots, \mathbf{u}\mathbf{g}_{n-1}).$$

Daha sonra, dağıtıcı D her $1 \leq i \leq n-1$ için l_i değerini P_i katılımcısına pay olarak atar, ve böylece katılımcıların pay değerleri oluşturulmuş ve dağıtılmış olur. Şimdi, sır kurtarma prosedürünü açıklayalım. s sır değerinin $l_0 = \mathbf{u}\mathbf{g}_0$ olduğuna dikkat edelim. $\{l_{i_1}, l_{i_2}, \ldots, l_{i_m}\}$ pay değerlerinin kümesinden s sır değeri elde edilebilir ancak ve ancak $\mathbf{g}_0$ değeri $\mathbf{g}_{i_1}, \mathbf{g}_{i_2}, \ldots, \mathbf{g}_{i_m}$ değerlerinin doğrusal bir birleşimidir.

Lemma 2.8 *(Massey, 1993) Sır paylaşım şemasında, sır (gizli bilgi) s, ancak ve ancak aşağıdaki formda bir kod sözcüğü $C^{\perp}$ dual kodunda mevcutsa belirlenebilir:*

$$(1, 0, \ldots, 0, c_{i_1}, 0, \ldots, 0, c_{i_m}, 0, \ldots, 0), \tag{2.5}$$

burada $c_{i_j} \neq 0$ olacak şekilde en az bir j için, $1 \leq i_2 < \cdots < i_m \leq n-1$ ve $1 \leq m \leq n-1$ şartlarını sağlar.

İspat Eğer $C^{\perp}$ dual kodunda (2.5) formunda bir kod sözcüğü varsa, bu durumda $\mathbf{g}_0$ değeri $\mathbf{g}_{i_1}, \mathbf{g}_{i_2}, \ldots, \mathbf{g}_{i_m}$ elemanlarının doğrusal kombinasyonu olarak yazılabilir, yani:

$$\mathbf{g}_0 = \sum_{j=1}^{m} x_j \mathbf{g}_{i_j},$$

burada x_j değerleri uygun katsayılardır. Bu durumda, sır s aşağıdaki şekilde hesaplanabilir:

$$s = \sum_{j=1}^{m} x_j l_{i_j}.$$

Not 2.2 *Lemma 2.8'un ışığında, C kodu üzerine kurulu sır paylaşım şemasının minimal erişim kümeleri ile $C^{\perp}$ dual kodunda ilk koordinatı 1 olan minimal kod sözcükleri arasında bire bir ilişki vardır. Bu kod sözcüklerinde sıfırdan farklı olan diğer koordinatlar, minimal erişim kümelerinde yer alan katılımcılara karşılık gelir.*

Not 2.2'ye göre, C kodu üzerine kurulmuş sır paylaşım şemasının erişim yapısını bulmak için, ilk koordinatı 1 olan tüm minimal kod sözcüklerini, yani $C^{\perp}$ dual kodun tüm minimal kod sözcükleri kümesinin bir alt kümesini bulmak yeterlidir. Hemen hemen her durumda, $C^{\perp}$ dual kodunun tüm minimal kod sözcüklerinin kümesini bulmamız gerektiğine dikkat ediniz.

Doğrusal koda dayalı sır paylaşım şemasının erişim yapısı genel olarak karmaşık olmakla birlikte bazı durumlarda kolaylıkla bulunabilmektedir. Aşağıdaki teorem (Carlet vd., 2005; Ding ve Yuan, 2003; Yuan ve Ding, 2006), doğrusal bir koda dayalı sır paylaşım şemasının erişim yapısını verir.

Teorem 2.1 *C kodu, üreteç matrisi $G = [\mathbf{g}_0, \mathbf{g}_1, \ldots, \mathbf{g}_{n-1}]$ olan $\mathbb{F}_p$ cismi üzerinde doğrusal bir $[n, k, d]_p$ kodu olsun. $C^{\perp}$ dual kodunun minimal Hamming mesafesi $d^{\perp}$ ile gösterilsin. Eğer C kodunun sıfırdan farklı tüm kod sözcükleri minimal ise, o zaman $C^{\perp}$ dual kodunu temel alan sır paylaşım şemasında katılımcı sayısı $(n-1)$ tanedir ve p^{k-1} tane minimal erişim kümesi mevcuttur.*

- $d^{\perp} = 2$ *ise erişim yapısı aşağıdaki gibi verilir:*
  - *Eğer* $\mathbf{g}_i$, $1 \leq i \leq n-1$, $\mathbf{g}_0$*'ın katı ise,* P_i *tüm minimal erişim kümelerinde vardır. Bu şekildeki* P_i *katılımcısına diktatöryal katılımcı denir.*
  - *Eğer* $\mathbf{g}_i$, $1 \leq i \leq n-1$, $\mathbf{g}_0$*'ın katı değilse, o zaman* P_i, p^{k-1} *tane minimal erişim kümelerinin* $(p-1)p^{k-2}$ *tanesinde yer alır.*
- *Eğer* $d^{\perp} \geq 3$ *ise, herhangi bir sabit* $1 \leq l \leq \min\{k-1, d^{\perp}-2\}$ *için, her* l *katılımcı kümesi* p^{k-1} *tane minimal erişim kümelerinin* $(p-1)^l p^{k-(l+1)}$ *tanesinde yer alır.*

C kodunun minimum Hamming mesafesi d, herhangi bir minimal erişim kümesinin boyutu için alt sınır $(d-1)$'i verirken, $C^{\perp}$ dual kodunun minimum Hamming mesafesi $d^{\perp}$, sır paylaşım şemasının demokrasi boyutunu gösterir. Ancak aralarında $d + d^{\perp} \leq n + 2$ bağıntısı vardır. Burada eşitlik sağlanır ancak ve ancak C kodu MDS koddur.

Not 2.3 *C koduna dayalı sır paylaşım şemasında katılımcıların payları C kodunun G üreteç matrisi'nin seçimine bağlıdır. Ancak G seçimi sır paylaşım şemalarının erişim yapılarını etkilemez. Bu nedenle G matrisinden bahsetmeden şemaya, C koduna dayalı sır paylaşım şeması diyebiliriz.*

3. İKİ AĞIRLIKLI PROJEKTİF DOĞRUSAL KODLARIN İNŞASI

Bu bölümde, tez çalışmamızın odaklandığı (Zhu ve Liao, 2023) çalışması incelenmiştir ve bu çalışmadaki sonuçları verilmiştir.

2007 yılında, Ding ve Niederreiter (Ding ve Niederreiter, 2007) çalışmasında D tanım kümesinden iz fonksiyonu aracılığıyla doğrusal kod tanımladılar. $D = \{d_1, d_2, \ldots, d_n\} \subseteq \mathbb{F}_{p^t}^\star$ tanım kümesi ve $\mathrm{Tr} : \mathbb{F}_{p^t} \to \mathbb{F}_p$ iz fonksiyonu olmak üzere bir p-li doğrusal kod şu şekilde tanımlanmıştır:

$$C_D = \{\mathbf{c}(x) = (\mathrm{Tr}(xd_1), \mathrm{Tr}(xd_2), \ldots, \mathrm{Tr}(xd_n)) \mid x \in \mathbb{F}_{p^t}\}.$$

Daha sonra bu tanımdan yola çıkarak, Li ve arkadaşları (Li vd., 2017) aşağıdaki doğrusal kodu tanımladılar: Tanım kümesi $D \subseteq \mathbb{F}_{p^t}^2$ olmak üzere

$$C_D = \left\{\mathbf{c}_{(a,b)} = (\mathrm{Tr}(ax + by))_{(x,y)\in D} \mid (a, b) \in \mathbb{F}_{p^t} \times \mathbb{F}_{p^t}\right\}.$$

Son olarak, Zhu ve Liao (Zhu ve Liao, 2023) çalışmasında d bir pozitif tam sayı olmak üzere $D \subseteq \mathbb{F}_{p^t}^2$ için, C_D doğrusal kodunu şu şekilde tanımlamışlardır:

$$C_D = \left\{(\mathrm{Tr}(ayx^d + bx))_{(x,y)\in D} \mid (a, b) \in \mathbb{F}_{p^t} \times \mathbb{F}_{p^t}\right\}. \tag{3.1}$$

$\lambda \in \mathbb{F}_p$ olmak üzere

$$D^\star = \left\{(x, y) \in \mathbb{F}_{p^t}^\star \times \mathbb{F}_{p^t}^\star \mid \mathrm{Tr}(yx^{d+1}) = 0\right\}, \tag{3.2}$$

$$D_\lambda = \left\{(x, y) \in \mathbb{F}_{p^t}^\star \times \mathbb{F}_{p^t} \mid \mathrm{Tr}(yx^{d+1}) = \lambda\right\} \tag{3.3}$$

tanım kümeleri ele alınmıştır. Böylece, $C_{D^\star}$ ve C_{D_λ} kodları inşa edilmiştir. Bu kodların parametreleri ve tam ağırlık sayaçları karakter toplamları kullanılarak hesaplanmıştır.

Bölüm 3.1'de kod inşası için gerekli olan lemmalar verilmiştir, ve Bölüm 3.2'de iki-ağırlıklı doğrusal kodlar inşa edilmiştir ve parametreleri hesaplanmıştır.

3.1. Yardımcı Sonuçlar

Yukarıda tanımlanan tanım kümeleri D_λ ve $D^\star$ olmak üzere $\tilde{D} \in \{D_\lambda, D^\star\}$ olsun. $C_{\tilde{D}}$ kodunun uzunluğu tanım gereğince $\tilde{D}$ tanım kümesinin eleman sayısına eşittir. Herhangi bir $(a, b) \in \mathbb{F}_{p^t}^2$ için $C_{\tilde{D}}$ kodunda $\mathbf{c}_{(a,b)} = (\mathrm{Tr}(ayx^d + bx))_{(x,y)\in\tilde{D}}$ kod sözcüğünün Hamming ağırlığı ise

$$wt(\mathbf{c}_{(a,b)}) = \#\tilde{D} - \#\left\{(x, y) \in \tilde{D} \mid \mathrm{Tr}(ayx^d + bx) = 0\right\}$$

şeklinde hesaplanabilir. Dolayısıyla, Hamming ağırlıkları bulmak için aşağıdaki kümeleri tanımlayabiliriz:

$$\begin{aligned} N_{\lambda,\lambda_1}(a,b) &= \left\{(x,y) \in \mathbb{F}_{p^t}^\star \times \mathbb{F}_{p^t} \mid \mathrm{Tr}(x^{d+1}y) = \lambda \text{ ve } \mathrm{Tr}(ax^d y + bx) = \lambda_1\right\}, \\ N_{\lambda_1}^\star(a,b) &= \left\{(x,y) \in \mathbb{F}_{p^t}^\star \times \mathbb{F}_{p^t}^\star \mid \mathrm{Tr}(x^{d+1}y) = 0 \text{ ve } \mathrm{Tr}(ax^d y + bx) = \lambda_1\right\}. \end{aligned}$$

$C_{\tilde{D}}$ kodundaki kod sözcüklerinin uzunluğunu ve Hamming ağırlığını belirlemek için $\lambda, \lambda_1 \in \mathbb{F}_p$ olmak üzere $D^\star, D_\lambda, N_{\lambda,\lambda_1}(a,b), N_{\lambda_1}^\star(a,b)$ kümelerinin eleman sayılarının hesaplanması yeterlidir.

Aşağıdaki lemmada D_λ ve $D^\star$ tanım kümelerinin eleman sayıları hesaplanmıştır.

Lemma 3.1 *$\lambda \in \mathbb{F}_p$ için*

$$\#D_\lambda = p^{2t-1} - p^{t-1}, \tag{3.4}$$

$$\#D^\star = p^{2t-1} - p^t - p^{t-1} + 1. \tag{3.5}$$

İspat Gauss toplamının özelliklerini kullanarak

$$\begin{aligned} \#D_\lambda &= \sum_{x\in\mathbb{F}_{p^t}^\star} \sum_{y\in\mathbb{F}_{p^t}} (p^{-1} \sum_{z_1\in\mathbb{F}_p} \epsilon_p^{z_1(\mathrm{Tr}(x^{d+1}y)-\lambda)}) \\ &= p^{-1} \sum_{x\in\mathbb{F}_{p^t}^\star} \sum_{y\in\mathbb{F}_{p^t}} (\sum_{z_1\in\mathbb{F}_p^\star} \epsilon_p^{z_1(\mathrm{Tr}(yx^{d+1})-\lambda)} + 1) \\ &= p^{t-1}(p^t-1) + p^{-1} \sum_{z_1\in\mathbb{F}_p^\star} \epsilon_p^{-z_1\lambda} \sum_{x\in\mathbb{F}_{p^t}^\star} \sum_{y\in\mathbb{F}_{p^t}} \epsilon_p^{\mathrm{Tr}(z_1x^{d+1}y)} \\ &= p^{2t-1} - p^{t-1} \end{aligned}$$

elde edilir. Dolayısıyla, $\#D^\star = \#D_0 - (p^t - 1) = p^{2t-1} - p^t - p^{t-1} + 1$ elde edilir.

$\#N_{\lambda,\lambda_1}(a,b)$ ve $\#N_{\lambda_1}^\star(a,b)$ değerleri sırasıyla Lemma 3.2 ve 3.3'de hesaplanmıştır.

Lemma 3.2 *d herhangi bir pozitif tamsayı ve $\lambda, \lambda_1 \in \mathbb{F}_p$, $(a,b) \in \mathbb{F}_{p^t} \times \mathbb{F}_{p^t} \setminus \{(0,0)\}$ olmak üzere*

$$\#N_{\lambda,\lambda_1}(a,b) = \left\{(x,y) \in \mathbb{F}_{p^t}^\star \times \mathbb{F}_{p^t} \mid \mathrm{Tr}(x^{d+1}y) = \lambda \textit{ ve } \mathrm{Tr}(ax^d y + bx) = \lambda_1\right\}$$

olsun. O halde aşağıdaki durumlar geçerlidir.

Durum 1: $\lambda = \lambda_1 = 0$*,*

$$\#N_{0,\lambda_1}(a,b) = \begin{cases} p^{2t-2} - p^{t-1}, & \textit{eğer } a = 0 \textit{ ve } b \neq 0, \textit{ veya } \mathrm{Tr}(ab) \neq 0; \\ p^{2t-2} + (p-2)p^{t-1}, & \textit{eğer } a \neq 0 \textit{ ve } \mathrm{Tr}(ab) = 0. \end{cases} \tag{3.6}$$

Durum 2: $\lambda = 0$ *ve* $\lambda_1 \neq 0$

$$\#N_{0,\lambda_1}(a,b) = \begin{cases} p^{2t-2}, & \text{eğer } a = 0 \text{ ve } b \neq 0, \text{ veya } a \neq 0 \text{ ve } \mathrm{Tr}(ab) \neq 0; \\ p^{2t-2} - p^{t-1}, & \text{eğer } a \neq 0 \text{ ve } \mathrm{Tr}(ab) = 0. \end{cases} \tag{3.7}$$

Durum 3: $\lambda \neq 0$ *ve* $\lambda_1 = 0$

$$\#N_{0,\lambda_1}(ab) = \begin{cases} p^{2t-2} - p^{t-1}, & \text{eğer } a = 0 \text{ ve } b \neq 0, \text{ veya } a \neq 0 \\ & \text{ve } \mathrm{Tr}(ab) = 0; \\ p^{2t-2} + \eta_1(-\lambda \mathrm{Tr}(ab))p^{t-1}, & \text{eğer } \mathrm{Tr}(ab) \neq 0. \end{cases} \tag{3.8}$$

Durum 4: $\lambda \neq 0$ *ve* $\lambda_1 \neq 0$,

$$\#N_{0,\lambda_1}(a,b) = \begin{cases} p^{2t-2}, & \text{eğer } a = 0 \text{ ve } b \neq 0, \text{ veya } a \neq 0 \\ & \text{ve } \mathrm{Tr}(ab) = 0; \\ p^{2t-2} + \eta_1(\lambda_1^2 - 4\lambda \mathrm{Tr}(ab))p^{t-1}, & \text{eğer } a \neq 0 \text{ ve } \mathrm{Tr}(ab) \neq 0. \end{cases} \tag{3.9}$$

İspat $N_{\lambda,\lambda_1}(a,b)$ kümesinin tanımından

$$\begin{aligned} \#N_{\lambda,\lambda_1}(a,b) &= \sum_{x \in \mathbb{F}_{p^t}^\star} \sum_{y \in \mathbb{F}_{p^t}} \left(p^{-1} \sum_{z_1 \in \mathbb{F}_p} \epsilon_p^{z_1(\mathrm{Tr}(x^{d+1}y) - \lambda)} \right) \left(p^{-1} \sum_{z_2 \in \mathbb{F}_p} \epsilon_p^{z_2(\mathrm{Tr}(ayx^d + bx) - \lambda_1)} \right) \\ &= p^{-2} \sum_{x \in \mathbb{F}_{p^t}^\star} \sum_{y \in \mathbb{F}_{p^t}} \Big(\sum_{z_1 \in \mathbb{F}_p^\star} \epsilon_p^{z_1(\mathrm{Tr}(yx^{d+1}) - \lambda)} + 1 \Big) \Big(\sum_{z_2 \in \mathbb{F}_p^\star} \epsilon_p^{z_2(\mathrm{Tr}(ax^d y + bx) - \lambda_1)} + 1 \Big) \\ &= p^{t-2}(p^t - 1) + p^{-2} \sum_{z_2 \in \mathbb{F}_p^\star} \epsilon_p^{-z_2\lambda_1} \sum_{x \in \mathbb{F}_{p^t}^\star} \sum_{y \in \mathbb{F}_{p^t}} \epsilon_p^{\mathrm{Tr}(z_2(ayx^d + bx))} \\ &+ p^{-2} \sum_{z_1 \in \mathbb{F}_p^\star} \sum_{z_2 \in \mathbb{F}_p^\star} \epsilon_p^{-(z_1\lambda + z_2\lambda_1)} \sum_{x \in \mathbb{F}_{p^t}^\star} \epsilon_p^{\mathrm{Tr}(z_2 bx)} \sum_{y \in \mathbb{F}_{p^t}} \epsilon_p^{\mathrm{Tr}((z_1 x + z_2 a)x^d y)} \\ &= p^{t-2}(p^t - 1) + \Omega_1 + \Omega_2. \end{aligned}$$

$\Omega_1 + \Omega_2$ toplamı aşağıda iki durumda hesaplanmaktadır.

Durum 1: $a = 0$ ve $b \neq 0$ için;

$$\begin{aligned} \Omega_1 + \Omega_2 &= p^{-2} \sum_{z_2 \in \mathbb{F}_p^\star} \epsilon_p^{-z_2\lambda_1} \sum_{x \in \mathbb{F}_{p^t}^\star} \sum_{y \in \mathbb{F}_{p^t}} \epsilon_p^{\mathrm{Tr}(z_2 bx)} \\ &+ p^{-2} \sum_{z_1 \in \mathbb{F}_p^\star} \sum_{z_2 \in \mathbb{F}_p^\star} \epsilon_p^{-(z_1\lambda + z_2\lambda_1)} \sum_{x \in \mathbb{F}_{p^t}^\star} \epsilon_p^{\mathrm{Tr}(z_2 bx)} \sum_{y \in \mathbb{F}_{p^t}} \epsilon_p^{\mathrm{Tr}(z_1 x^{d+1} y)} \\ &= -p^{t-2} \sum_{z_2 \in \mathbb{F}_p^\star} \epsilon_p^{-(z_2\lambda_1)} = \begin{cases} -p^{t-2}(p-1), & \lambda_1 = 0; \\ p^{t-2}, & \lambda_1 \neq 0. \end{cases} \end{aligned}$$

Durum 2: $a \neq 0$ durumunda kolayca $\Omega_1 = 0$ olduğu görülebir. Ω_2 değeri aşağıdaki gibi hesaplanabilir.

$$\begin{aligned}
\Omega_2 &= p^{-2} \sum_{z_1 \in \mathbb{F}_p^\star} \sum_{z_2 \in \mathbb{F}_p^\star} \epsilon_p^{-(z_1\lambda + z_2\lambda_1)} \sum_{x \in \mathbb{F}_{p^t}^\star} \epsilon_p^{\mathrm{Tr}(z_2 bx)} \sum_{y \in \mathbb{F}_{p^t}} \epsilon_p^{\mathrm{Tr}((z_1 x + z_2 a)x^d y)} \\
&= p^{-2} \sum_{z_1 \in \mathbb{F}_p^\star} \sum_{z_2 \in \mathbb{F}_p^\star} \epsilon_p^{-(z_1\lambda + z_2\lambda_1)} \sum_{z_1 x + z_2 a = 0} \epsilon_p^{\mathrm{Tr}(z_2 bx)} \sum_{y \in \mathbb{F}_{p^t}} \epsilon_p^{\mathrm{Tr}((z_1 x + z_2 a)x^d y)} \\
&= p^{t-2} \sum_{z_1 \in \mathbb{F}_p^\star} \sum_{z_2 \in \mathbb{F}_p^\star} \epsilon_p^{-(z_1\lambda + z_2\lambda_1)} \epsilon_p^{-z_1^{-1} z_2^2 \mathrm{Tr}(ab)}
\end{aligned}$$

Eğer $\mathrm{Tr}(ab) = 0$ ise;

$$\Omega_2 = p^{t-2} \sum_{z_1 \in \mathbb{F}_p^\star} \sum_{z_2 \in \mathbb{F}_p^\star} \epsilon_p^{-(z_1\lambda + z_2\lambda_1)} = \begin{cases} (p-1)^2 p^{t-2}, & \text{eğer } \lambda = \lambda_1 = 0; \\ -p^{t-2}(p-1), & \text{eğer } \lambda = 0 \text{ ve } \lambda_1 \neq 0, \\ & \text{veya } \lambda \neq 0 \text{ ve } \lambda_1 = 0; \\ p^{t-2}, & \text{eğer } \lambda, \lambda_1 \neq 0. \end{cases}$$

Eğer $\mathrm{Tr}(ab) \neq 0$ ise Ω_2 aşağıdaki gibi elde edilir.

$$\begin{aligned}
\Omega_2 &= p^{t-2} \sum_{z_1 \in \mathbb{F}_p^\star} \sum_{z_2 \in \mathbb{F}_p^\star} \epsilon_p^{-(z_1\lambda + z_2\lambda_1)} \epsilon_p^{-z_1^{-1} z_2^2 \mathrm{Tr}(ab)} \\
&= p^{t-2} \sum_{z_1 \in \mathbb{F}_p^\star} \epsilon_p^{-z_1\lambda} \sum_{z_2 \in \mathbb{F}_p^\star} \epsilon_p^{(-z_1^{-1}\mathrm{Tr}(ab) z_2^2 - \lambda_1 z_2)} \\
&= p^{t-2} \sum_{z_1 \in \mathbb{F}_p^\star} \epsilon_p^{-\lambda z_1} \left(\epsilon_p^{(\lambda_1^2 (4\mathrm{Tr}(ab))^{-1} z_1)} \eta_1(-\mathrm{Tr}(ab) z_1^{-1}) G_1 - 1 \right) \\
&= p^{t-2} G_1 \sum_{z_1 \in \mathbb{F}_p^\star} \left(\epsilon^{((4\mathrm{Tr}(ab))^{-1}\lambda_1^2 - \lambda) z_1} \eta_1(-(4\mathrm{Tr}(ab))^{-1} z_1) \right) - p^{t-2} \sum_{z_1 \in \mathbb{F}_p^\star} \epsilon_p^{-\lambda z_1} \\
&= \begin{cases} -p^{t-2}(p-1), & \text{eğer } \lambda = \lambda_1 = 0; \\ (\eta_1(-1) G_1^2 - (p-1)) p^{t-2}, & \text{eğer } \lambda = 0 \text{ ve } \lambda_1 \neq 0; \\ p^{t-2}, & \text{eğer } \lambda \neq 0 \text{ ve } 4\lambda \mathrm{Tr}(ab) - \lambda_1^2 = 0; \\ (\eta_1(4\lambda \mathrm{Tr}(ab) - \lambda_1^2) G_1^2 + 1) p^{t-2}, & \text{eğer } \lambda \neq 0 \text{ ve } 4\lambda \mathrm{Tr}(ab) - \lambda_1^2 \neq 0. \end{cases}
\end{aligned}$$

Yukarıdaki hesaplama işleminde Lemma 2.5 kullanılmıştır. Elde edilen Ω_1 ve Ω_2 değerleri yerlerine yazıldığı zaman istenilen $N_{\lambda,\lambda_1}(a,b)$ değerleri elde dilir. Böylece ispat tamamlanmıştır.

Lemma 3.3 *Herhangi bir d tamsayısı için $\lambda_1 \in \mathbb{F}_p$, $(a,b) \in \mathbb{F}_{p^t} \times \mathbb{F}_{p^t} \setminus \{(0,0)\}$ olmak üzere*

$$N_{\lambda_1}^\star(a,b) = \left\{ (x,y) \in \mathbb{F}_{p^t}^\star \times \mathbb{F}_{p^t}^\star \mid \mathrm{Tr}(x^{d+1}y) = 0 \textit{ ve } \mathrm{Tr}(ax^d y + bx) = \lambda_1 \right\}$$

olsun. Bu durumda aşağıdaki sonuçlar geçerlidir.

Durum 1: $\lambda_1 = 0$ *için,*

$$\#N^{\star}_{\lambda_1}(a,b) = \begin{cases} p^{2t-2} - 2p^{t-1} + 1, & \text{eğer } a = 0 \text{ ve } b \neq 0, \text{ veya } \mathrm{Tr}(ab) \neq 0, \\ & \text{veya } a \neq 0 \text{ ve } b = 0; \\ p^{2t-2} + (p-3)p^{t-1} + 1, & \text{eğer } a \neq 0, b \neq 0 \text{ ve } \mathrm{Tr}(ab) = 0. \end{cases} \tag{3.10}$$

Durum 2: $\lambda_1 \neq 0$ *için,*

$$\#N^{\star}_{\lambda_1}(a,b) = \begin{cases} p^{2t-2} - p^{t-1}, & \text{eğer } a = 0 \text{ ve } b \neq 0, \text{ veya } a \neq 0, \\ & \text{ve } \mathrm{Tr}(ab) \neq 0 \text{ veya } a \neq 0 \text{ ve } b = 0; \\ p^{2t-2} - 2p^{t-1}, & \text{eğer } a \neq 0, b \neq 0 \text{ ve } \mathrm{Tr}(ab) = 0. \end{cases} \tag{3.11}$$

İspat $N_{0,\lambda_1}(a,b)$ ve $N^{\star}_{\lambda_1}(a,b)$'in tanımlarından aşağıdakiler elde edilmektedir:

$$\begin{aligned} \#N^{\star}_{\lambda_1}(a,b) &= \#N_{0,\lambda_1}(a,b) - \#\left\{(x,y) \in \mathbb{F}^{\star}_{p^t} \times \{0\} \mid \mathrm{Tr}(bx) = \lambda_1\right\} \\ &= \#N_{0,\lambda_1}(a,b) - \begin{cases} p^t - 1, & \text{eğer } b = \lambda_1 = 0; \\ p^{t-1} - 1, & \text{eğer } b \neq 0 \text{ ve } \lambda_1 = 0; \\ 0, & \text{eğer } b = 0 \text{ ve } \lambda_1 \neq 0; \\ p^{t-1}, & \text{eğer } b \neq 0 \text{ ve } \lambda_1 \neq 0. \end{cases} \end{aligned} \tag{3.12}$$

Denklem (3.12) ifadesi göz önüne alındığında Lemma 3.2'deki denklem (3.6) ve (3.7)'den sırasıyla durum (3.10) ve (3.11) elde edilebilir. Böylece ispat tamamlanır.

İz fonksiyonu dengeli bir fonksiyon olduğu için aşağıdaki lemma kolayca ifade edilebilir.

Lemma 3.4 $l \in \mathbb{F}_p$ *için* $A(l) = \left\{(a,b) \in \mathbb{F}^{\star}_{p^t} \times \mathbb{F}_{p^t} \mid \mathrm{Tr}(ab) = l\right\}$ *olsun. Bu durumda*

$$\#A(l) = p^{t-1}(p^t - 1).$$

3.2. Doğrusal Kodlar

Bu bölümde, doğrusal kodlar inşa edilmekte ve kodların parametreleri verilmektedir.

Teorem 3.1 *Herhangi bir* $t \geq 2$ *tam sayısı için,* D_0 *kümesi ve* C_{D_0} *kodu sırasıyla (3.3) ve (3.1'de verilmiştir. O zaman* C_{D_0} *kodu, Çizelge 3.1'deki ağırlık dağılımına sahip bir*

$[p^{2t-1}-p^{t-1}, 2t, (p-1)(p^{t-1}-1)p^{t-1}]$ *doğrusal koddur ve tam ağırlık sayıcı şöyle ifade edilmiştir:*

$$W(C_{D_0}) = \quad w_0^{p^{2t-1}-p^{t-1}} + (p^t - p^{t-1} + 1)(p^t - 1)w_0^{p^{2t-2}-p^{t-1}} \prod_{i\in\mathbb{F}_p^\star} w_i^{p^{2t-2}}$$
$$+p^{t-1}(p^t-1)w_0^{p^{2t-2}+(p-2)p^{t-1}} \textstyle\prod_{i\in\mathbb{F}_p^\star} w_i^{p^{2t-2}-p^{t-1}}.$$

Çizelge 3.1. Teorem 3.1'deki C_{D_0} kodunun parametreleri

Hamming Ağırlığı ω	*Frekansı* A_ω
0	1
$(p-1)p^{2t-2}$	$(p^t-1)(p^t-p^{t-1}+1)$
$(p-1)(p^{t-1}-1)p^{t-1}$	$(p^t-1)p^{t-1}$

İspat C_{D_0} kodunun tanımından dolayı uzunluğu $n = \#D_0 = p^{2t-1} - p^{t-1}$ ve Hamming ağırlığı

$$wt(\mathbf{c}_{(a,b)}) = n - \#N_{0,0}(a,b)$$

şeklindedir. $\lambda \in \mathbb{F}_p$ ve $a, b \in \mathbb{F}_{p^t}$ için Lemma 3.2'den aşağıdaki iki durum vardır.

Durum 1: $a = 0$ ve $b \neq 0$ veya $\mathrm{Tr}(ab) \neq 0$

$$\#N_{0,\lambda_1}(ab) = \begin{cases} p^{2t-2} - p^{t-1}, & \lambda_1 = 0; \\ p^{2t-2}, & \lambda_1 \neq 0. \end{cases}$$

Dolayısıyla, $\lambda_1 = 0$ durumunda kod sözcüğünün ağırlığı $w_1 = n - \#N_{0,0}(a,b) = (p-1)p^{2t-2}$ olur ve bu kod sözcüğünün frekansı Lemma 3.4'den

$$A_{w_1} = (p^t - 1) + \sum_{l\in\mathbb{F}_p^\star} \#A(l) = (p^t - p^{t-1} + 1)(p^t - 1)$$

şeklinde elde edilmiştir.

Durum 2: $a \neq 0$ ve $\mathrm{Tr}(ab) = 0$ için,

$$\#N_{0,\lambda_1}(ab) = \begin{cases} p^{2t-2} + (p-2)p^{t-1}, & \lambda_1 = 0; \\ p^{2t-2} - p^{t-1}, & \lambda_1 \neq 0. \end{cases}$$

Dolayısıyla, $\lambda_1 = 0$ durumunda kod sözcüğünün ağırlığı

$$wt(\mathbf{c}_{(a,b)}) = n - \#N_{0,0}(a,b) = (p-1)(p^{t-1}-1)p^{t-1}$$

olur ve bu kod sözcüğünün frekansı Lemma 3.4'den $A_{w_2} = \#A(0) = p^{t-1}(p^t-1)$ elde edilir. Böylece, Teorem 3.1 'in ispatı tamamlanmış olur.

Teorem 3.2 *Herhangi bir $t \geq 2$ tam sayısı için $D^\star$ kümesi ve $C_{D^\star}$ kodu sırasıyla (3.2) ve (3.1)'de verilmiştir. O zaman $C_{D^\star}$ kodu, Çizelge 3.2'deki ağırlık dağılımına sahip $[p^{2t-1}-p^t-p^{t-1}+1, 2t, (p-1)(p^{t-1}-2)p^{t-1}]$ parametreli bir doğrusal koddur ve tam ağırlık sayıcı şöyle ifade edilmiştir:*

$$\begin{aligned} W(C_{D^\star}) = \; & w_0^{p^{2t-1}-p^t-p^{t-1}+1} \\ & +(p^t-p^{t-1}+2)(p^t-1)w_0^{p^{2t-2}-2p^{t-1}+1}\prod_{i\in\mathbb{F}_p^\star} w_i^{(p^{t-1}-1)p^{t-1}} \\ & +(p^{t-1}-1)(p^t-1)w_0^{p^{2t-2}+(p-3)p^{t-1}+1}\prod_{i\in\mathbb{F}_p^\star} w_i^{(p^{t-1}-2)p^{t-1}}. \end{aligned}$$

Çizelge 3.2. Teorem 3.2'deki $C_{D^\star}$ kodunun parametreleri

Hamming Ağırlığı ω	*Frekansı* A_ω
0	1
$(p-1)(p^{t-1}-1)p^{t-1}$	$(p^t-1)(p^t-p^{t-1}+2)$
$(p-1)(p^{t-1}-2)p^{t-1}$	$(p^t-1)(p^{t-1}-1)$

İspat Denklem (3.5) ve Lemma 3.3 göz önüne alınarak Teorem 3.1 için yapılan ispata benzer şekilde ispat tamamlanır.

Teorem 3.3 *Herhangi bir $t \geq 2$ tam sayısı ve $\lambda \in \mathbb{F}_p^\star$ için D_λ kümesi ve C_{D_λ} kodu sırasıyla (3.3) ve (3.1)'de verilmiştir. O zaman C_{D_λ} kodu, Çizelge 3.3'teki ağırlık dağılımına sahip $[p^{2t-1}-p^{t-1}, 2t, (p^t-p^{t-1}-2)p^{t-1}]$ parametreli bir doğrusal koddur ve tam ağırlık sayıcı şöyle ifade edilmiştir:*

$$\begin{aligned} W(C_{D_\lambda}) = \; & w_0^{p^{2t-1}-p^{t-1}} + (p^{t-1}+1)(p^t-1)w_0^{p^{2t-2}-p^{t-1}}\prod_{i\in\mathbb{F}_p^\star} w_i^{p^{2t-2}} \\ & +\tfrac{P-1}{2}p^{t-1}(p^t-1)\sum_{j\in\mathbb{F}_p^\star}\prod_{i\in\mathbb{F}_p} w_i^{p^{2t-2}+\eta_1(i^2-4\lambda j)p^{t-1}} \\ & +\tfrac{P-1}{2}p^{t-1}(p^t-1)\sum_{j\in\mathbb{F}_p^\star}\prod_{i\in\mathbb{F}_p} w_i^{p^{2t-2}+\eta_1(i^2-4\lambda j)p^{t-1}}. \end{aligned}$$

Çizelge 3.3. Teorem 3.3'deki C_{D_λ} kodunun parametreleri

Hamming Ağırlığı ω	*Frekansı* A_ω
0	1
$(p-1)p^{2t-2}$	$(p^t-1)(\frac{p+1}{2}p^{t-1}+1)$
$p^{t-1}(p^t-p^{t-1}-2)$	$p^{t-1}(p^t-1)\frac{p-1}{2}$

İspat Denklem (3.4)'den $\lambda \in \mathbb{F}_p^\star$ için C_{D_λ} kodunun uzunluğu

$$n = \#D_\lambda = p^{2t-1} - p^{t-1}$$

ve Hamming ağırlığı $wt(\mathbf{c}_{(a,b)}) = n - \#N_{\lambda,0}(a,b)$ şeklindedir. Lemma 3.2'ye göre $\lambda_1 \in \mathbb{F}_p$ ve $a, b \in \mathbb{F}_{p^t}$ için aşağıdaki iki durum vardır.

Durum 1: $a = 0$ ve $b \neq 0$, veya $a \neq 0$ ve $\mathrm{Tr}(ab) = 0$ için (3.8)-(3.9)'dan aşağıdaki durum geçerlidir.

$$\#N_{\lambda,\lambda_1}(a,b) = \begin{cases} p^{2t-2} - p^{t-1}, & \lambda_1 = 0; \\ p^{2t-2}, & \text{diğer durumlarda.} \end{cases}$$

Dolayısıyla, bu durumda C_{D_λ} kodunun kod sözcüğünün ağırlığı

$$wt(\mathbf{c}_{(a,b)}) = n - \#N_{\lambda,0}(a,b) = (p-1)p^{2t-2}, \tag{3.13}$$

ve frekansı ise

$$A_w = (p^t - 1) + \#A(0) = (p^{t-1} + 1)(p^t - 1). \tag{3.14}$$

Durum 2: $\mathrm{Tr}(ab) \neq 0$ ise (3.8) ve (3.9)'dan şu sonuca varılmaktadır:

$$\#N_{\lambda,\lambda_1}(a,b) = p^{2t-2} + \eta_1(\lambda_1^2 - 4\lambda \mathrm{Tr}(ab))p^{t-1}.$$

Eğer $\eta_1(-\mathrm{Tr}(ab)\lambda) = -1$ ise $\#N_{\lambda,0}(a,b) = p^{2t-2} - p^{t-1}$, ve böylece Hamming ağırlığı

$$wt(\mathbf{c}_{(a,b)}) = n - \#N_{\lambda,0}(a,b) = (p-1)p^{2t-2}, \tag{3.15}$$

ve frekansı

$$A_w = \sum_{\eta_1(\lambda l)=1} \#A(l) = \sum_{\eta_1(l)=\eta_1(\lambda)} \#A(l) = \frac{p-1}{2} p^{t-1}(p^t - 1) \tag{3.16}$$

şeklinde elde edilir. Eğer $\eta_1(-\lambda \mathrm{Tr}(ab)) = 1$ ise $\#N_{\lambda,0}(ab) = p^{2t-2} + p^{t-1}$ ve böylece

$$wt(\mathbf{c}_{(a,b)}) = n - \#N_{\lambda,0}(0,0) = (p^t - p^{t-1} - 2)p^{t-1}$$

ve frekansı

$$A_w = \sum_{\eta_1(\lambda l)=-1} \#A(l) = \sum_{\eta_1(l)=-\eta_1(\lambda)} \#A(l) = \frac{p-1}{2} p^{t-1}(p^t - 1)$$

şeklinde hesaplanmıştır. Şimdi, (3.13)-(3.14) ve (3.15)-(3.16)'den Hamming ağırlığı $w = (p-1)p^{2t-2}$ olan kod sözcüklerinin sayısı

$$A_w = (p^{t-1} + 1)(p^t - 1) + \frac{p-1}{2} p^{t-1}(p^t - 1) = \left(\frac{p+1}{2} p^{t-1} + 1 \right)(p^t - 1)$$

şeklinde elde edilir. Böylece, ispat tamamlanmıştır.

4. DÜŞÜK AĞIRLIKLI DOĞRUSAL KODLARIN YENİ AİLELERİ

Bu bölümde, (Zhu ve Liao, 2023) çalışmasında önerilen doğrusal kod inşa yönteminde yeni tanım kümeleri kullanılarak yeni doğrusal kod aileleri inşa edilmiştir. Kod inşa yönteminde yeni tanım kümeleri kullanılarak yeni parametrelere sahip kodlar elde edilmiştir. Elde edilen kodların uzunlukları, Hamming ağırlıkları ve ağırlık dağılımları hesaplanmıştır. Yeni kodun yapısı tanımlanarak; kodun uzunluğu, Hamming ağırlığı ve ağırlık dağılımı parametrelerinin doğrulukları kanıtlanmıştır.

4.1. D_λ Kümesi Üzerinde Tanımlanan İki Ağırlıklı Doğrusal Kodun İnşası

d herhangi bir pozitif tamsayı ve $\lambda \in \mathbb{F}_p$ olmak üzere

$$D_\lambda = \left\{(x,y) \in \mathbb{F}_q \times \mathbb{F}_q \mid \mathrm{Tr}(yx^{d+1}) = \lambda\right\} \tag{4.1}$$

kümesini alalım. $\lambda \in \mathbb{F}_p^\star$ durumunda tanımdan dolayı $(0,0) \notin D_\lambda$ olduğu açıktır. Bu tanım kümesi üzerinde

$$C_{D_\lambda} = \left\{\mathbf{c}_{(a,b)} = \mathrm{Tr}(ayx^d + bx)_{(x,y)\in D_\lambda} \mid (a,b) \in \mathbb{F}_{p^t} \times \mathbb{F}_{p^t}\right\} \tag{4.2}$$

kodunu tanımlayalım. Tanım gereği bu kodun uzunluğu tanım kümesinin eleman sayısına eşittir. Tanımdan dolayı $\mathbf{c}_{(0,0)}$ kod sözcüğünün Hamming ağırlığı 0'dır. Her $(a,b) \in \mathbb{F}_q \times \mathbb{F}_q \setminus \{(0,0)\}$ için $\mathbf{c}_{(a,b)}$ kod sözcüğünün Hamming ağırlığını bulmayı amaçlıyoruz. C_{D_λ} kodunun Hamming ağırlığını hesaplamak için $\lambda \in \mathbb{F}_p$ ve $(a,b) \in \mathbb{F}_q \times \mathbb{F}_q \setminus \{(0,0)\}$ olmak üzere

$$\begin{aligned} N_\lambda(a,b) &= \left\{(x,y) \in \mathbb{F}_q \times \mathbb{F}_q \mid (x,y) \in D_\lambda \text{ ve } \mathrm{Tr}(ax^d y + bx) = 0\right\} \\ &= \left\{(x,y) \in \mathbb{F}_q \times \mathbb{F}_q \mid \mathrm{Tr}(x^{d+1}y) = \lambda \text{ ve } \mathrm{Tr}(ax^d y + bx) = 0\right\} \end{aligned} \tag{4.3}$$

kümesini tanımlayalım. C_{D_λ} kodunun her kod sözcüğünün Hamming ağırlığı $wt(\mathbf{c}_{(a,b)}) = \#D_\lambda - \#N_\lambda(a,b)$ şeklinde hesaplanabilir.

Öncelikle aşağıdaki lemmada tanım kümesinin eleman sayısını bulalım.

Lemma 4.1 *Denklem (4.1)'de verilen D_λ kümesinin eleman sayısı*

$$\#D_\lambda = \begin{cases} p^{2t-1} + (p-1)p^{t-1}, & \text{eğer } \lambda = 0; \\ p^{2t-1} - p^{t-1}, & \text{eğer } \lambda \neq 0. \end{cases}$$

İspat Kümenin tanımından

$$\begin{aligned}
\#D_\lambda &= \sum_{x\in\mathbb{F}_q}\sum_{y\in\mathbb{F}_q}\left(p^{-1}\sum_{z_1\in\mathbb{F}_p}\epsilon^{z_1(\mathrm{Tr}(yx^{d+1})-\lambda)}\right)\\
&= \tfrac{1}{p}\sum_{x\in\mathbb{F}_q}\sum_{y\in\mathbb{F}_q}\left(\sum_{z_1\in\mathbb{F}_p^\star}\epsilon_p^{z_1(\mathrm{Tr}(yx^{d+1})-\lambda)}+1\right)\\
&= p^{2t-1}+\tfrac{1}{p}\sum_{z_1\in\mathbb{F}_p^\star}\epsilon_p^{-\lambda z_1}\sigma_{z_1}\left(\sum_{x\in\mathbb{F}_q}\sum_{y\in\mathbb{F}_q}\epsilon_p^{Tr(yx^{d+1})}\right)\\
&= p^{2t-1}+\tfrac{1}{p}\sum_{z_1\in\mathbb{F}_p^\star}\epsilon_p^{-\lambda z_1}\sigma_{z_1}\left(\sum_{x\in\mathbb{F}_q^\star}\sum_{y\in\mathbb{F}_q}\epsilon_p^{Tr(yx^{d+1})}+1\right)\\
&= p^{2t-1}+\tfrac{1}{p}\sum_{z_1\in\mathbb{F}_p^\star}\epsilon_p^{-\lambda z_1}\sigma_{z_1}\left(p^t+\sum_{x\in\mathbb{F}_q^\star}\sum_{y\in\mathbb{F}_q}\epsilon_p^{Tr(yx^{d+1})}\right)\\
&= p^{2t-1}+p^{t-1}\sum_{z_1\in\mathbb{F}_p^\star}\epsilon_p^{-\lambda z_1}.
\end{aligned}$$

İstenen sonuçlar Lemma 2.2'den dolayı elde edilir. Böylece, ispat tamamlanmış olur.

Aşağıdaki lemmada denklem (4.3)'de verilen kümenin eleman sayısını bulalım.

Lemma 4.2 *$\lambda\in\mathbb{F}_p$ ve $(a,b)\in\mathbb{F}_q\times\mathbb{F}_q\setminus\{(0,0)\}$ olmak üzere denklem (4.3)'de verilen $N_\lambda(a,b)$ kümesinin eleman sayısı $\lambda=0$ için*

$$\#N_0(a,b)=\begin{cases}
p^{2t-2}+(p-1)p^{t-1}, & \text{eğer } a=0\wedge b\neq 0,\\
 & \text{veya } a\neq 0\wedge b\in\mathbb{F}_q\wedge \mathrm{Tr}(ab)\neq 0;\\
p^{2t-2}+2(p-1)p^{t-1}, & \text{eğer } a\neq 0\wedge b\in\mathbb{F}_q\wedge \mathrm{Tr}(ab)=0,
\end{cases}$$

$\lambda\neq 0$ için

$$\#N_\lambda(a,b)=\begin{cases}
p^{2t-2}-p^{t-1}, & \text{eğer } a=0\wedge b\neq 0,\\
 & \text{veya } a\neq 0 \text{ ve } b\in\mathbb{F}_q \text{ ve } \mathrm{Tr}(ab)=0,\\
 & \text{veya } a\neq 0\wedge b\in\mathbb{F}_q\wedge \mathrm{Tr}(ab)\neq 0\wedge -4\lambda\mathrm{Tr}(ab)\in NSQ;\\
p^{2t-2}+p^{t-1}, & \text{eğer } a\neq 0\wedge b\in\mathbb{F}_q\wedge \mathrm{Tr}(ab)\neq 0\wedge -4\lambda\mathrm{Tr}(ab)\in SQ.
\end{cases}$$

İspat $N_\lambda(a,b)$ kümesinin tanımından

$$\begin{aligned}
\#N_\lambda(a,b) &= \sum_{x\in\mathbb{F}_q}\sum_{y\in\mathbb{F}_q}\left(p^{-1}\sum_{z_1\in\mathbb{F}_p}\epsilon_p^{z_1(\mathrm{Tr}(x^{d+1}y)-\lambda)}\right)\left(p^{-1}\sum_{z_2\in\mathbb{F}_p}\epsilon_p^{z_2(\mathrm{Tr}(ayx^d+bx))}\right)\\
&= p^{-2}\sum_{z_1,z_2\in\mathbb{F}_p}\left(\sum_{x,y\in\mathbb{F}_q}\epsilon_p^{z_1(\mathrm{Tr}(yx^{d+1})-\lambda)+z_2(\mathrm{Tr}(ax^dy+bx))}\right)\\
&= p^{2t-2}+p^{-2}\sum_{z_1\in\mathbb{F}_p^\star}\left(\sum_{x,y\in\mathbb{F}_q}\epsilon_p^{z_1(\mathrm{Tr}(yx^{d+1})-\lambda)+z_2(\mathrm{Tr}(ax^dy+bx))}\right)\\
&+p^{-2}\sum_{z_2\in\mathbb{F}_p^\star}\left(\sum_{x,y\in\mathbb{F}_q}\epsilon_p^{z_1(\mathrm{Tr}(yx^{d+1})-\lambda)+z_2(\mathrm{Tr}(ax^dy+bx))}\right)\\
&+p^{-2}\sum_{z_1,z_2\in\mathbb{F}_p^\star}\left(\sum_{x,y\in\mathbb{F}_q}\epsilon_p^{z_1(\mathrm{Tr}(yx^{d+1})-\lambda)+z_2(\mathrm{Tr}(ax^dy+bx))}\right)\\
&= p^{2t-2}+\tfrac{1}{p^2}\left(\Omega_0+\Omega_1+\Omega_2\right).
\end{aligned}$$

elde edilir. Burada,

$$\begin{aligned}
\Omega_0 &= \sum_{z_1\in\mathbb{F}_p^\star}\left(\sum_{x,y\in\mathbb{F}_q}\epsilon_p^{z_1(\mathrm{Tr}(yx^{d+1})-\lambda)}\right)\\
\Omega_1 &= \sum_{z_2\in\mathbb{F}_p^\star}\left(\sum_{x,y\in\mathbb{F}_q}\epsilon_p^{z_2(\mathrm{Tr}(ax^dy+bx))}\right)\\
\Omega_2 &= \sum_{z_1,z_2\in\mathbb{F}_p^\star}\left(\sum_{x,y\in\mathbb{F}_q}\epsilon_p^{z_1(\mathrm{Tr}(yx^{d+1})-\lambda)+z_2(\mathrm{Tr}(ax^dy+bx))}\right).
\end{aligned}$$

Şimdi, $(a,b)\in\mathbb{F}_q\times\mathbb{F}_q\setminus\{(0,0)\}$ için Ω_0, Ω_1, Ω_2 değerlerini a, b ve λ'nın farklı durumlarına göre hesaplayalım.

Durum 1: Ω_0'ı hesaplayalım.

$$\begin{aligned}
\Omega_0 &= \sum_{z_1\in\mathbb{F}_p^\star}\epsilon_p^{-\lambda z_1}\left(\sum_{x,y\in\mathbb{F}_q}\epsilon_p^{z_1\mathrm{Tr}(yx^{d+1})}\right)\\
&= \sum_{z_1\in\mathbb{F}_p^\star}\epsilon_p^{-\lambda z_1}\left(\sum_{x\in\mathbb{F}_q^\star}\sum_{y\in\mathbb{F}_q}\epsilon_p^{\mathrm{Tr}(z_1yx^{d+1})}+p^t\right)\\
&= p^t\sum_{z_1\in\mathbb{F}_p^\star}\epsilon_p^{-\lambda z_1} = \begin{cases}(p-1)p^t, & \text{eğer } \lambda=0;\\ -p^t, & \text{eğer } \lambda\neq 0.\end{cases}
\end{aligned}$$

Ω_1'i iki durum için hesaplayalım.

Durum 1: $a=0$ ve $b\neq 0$ için

$$\Omega_1 = \sum_{z_2\in\mathbb{F}_p^\star}\left(\sum_{x,y\in\mathbb{F}_q}\epsilon_p^{z_2(\mathrm{Tr}(bx))}\right) = \sum_{z_2\in\mathbb{F}_p^\star}\sum_{y\in\mathbb{F}_q}\left(\sum_{x\in\mathbb{F}_q}\epsilon_p^{\mathrm{Tr}(z_2bx)}\right) = 0.$$

Durum 2: $a \neq 0$ ve $b \in \mathbb{F}_q$ için

$$\begin{aligned}
\Omega_1 &= \sum_{z_2 \in \mathbb{F}_p^\star} \left(\sum_{x,y \in \mathbb{F}_q} \epsilon_p^{z_2(\mathrm{Tr}(ax^d y + bx))} \right) \\
&= \sum_{z_2 \in \mathbb{F}_p^\star} \left(\sum_{x \in \mathbb{F}_q^\star} \sum_{y \in \mathbb{F}_q} \epsilon_p^{z_2 \mathrm{Tr}(ax^d y + bx)} + p^t \right) \\
&= (p-1)p^t + \sum_{z_2 \in \mathbb{F}_p^\star} \left(\sum_{x \in \mathbb{F}_q^\star} \sum_{y \in \mathbb{F}_q} \epsilon_p^{z_2 \mathrm{Tr}(ax^d y + bx)} \right) \\
&= (p-1)p^t + \sum_{z_2 \in \mathbb{F}_p^\star} \sum_{x \in \mathbb{F}_q^\star} \epsilon_p^{\mathrm{Tr}(z_2 bx)} \left(\sum_{y \in \mathbb{F}_q} \epsilon_p^{\mathrm{Tr}(z_2 a x^d y)} \right) \\
&= (p-1)p^t.
\end{aligned}$$

Şimdi, Ω_2'yi hesaplayalım.

$$\begin{aligned}
\Omega_2 &= \sum_{z_1, z_2 \in \mathbb{F}_p^\star} \left(\sum_{x,y \in \mathbb{F}_q} \epsilon_p^{z_1(\mathrm{Tr}(yx^{d+1}) - \lambda) + z_2(\mathrm{Tr}(ayx^d + bx))} \right) \\
&= \sum_{z_1, z_2 \in \mathbb{F}_p^\star} \epsilon_p^{-\lambda z_1} \left(\sum_{x,y \in \mathbb{F}_q} \epsilon_p^{\mathrm{Tr}(z_1 yx^{d+1}) + \mathrm{Tr}(z_2 ayx^d + z_2 bx)} \right) \\
&= \sum_{z_1, z_2 \in \mathbb{F}_p^\star} \epsilon_p^{-\lambda z_1} \sum_{x \in \mathbb{F}_q} \epsilon_p^{\mathrm{Tr}(z_2 bx)} \left(\sum_{y \in \mathbb{F}_q} \epsilon_p^{\mathrm{Tr}(z_1 yx^{d+1} + z_2 ayx^d)} \right) \\
&= p^t \sum_{z_1, z_2 \in \mathbb{F}_p^\star} \epsilon_p^{-\lambda z_1} + \sum_{z_1, z_2 \in \mathbb{F}_p^\star} \epsilon_p^{-\lambda z_1} \sum_{x \in \mathbb{F}_q^\star} \epsilon_p^{\mathrm{Tr}(z_2 bx)} \left(\sum_{y \in \mathbb{F}_q} \epsilon_p^{\mathrm{Tr}(z_1 yx^{d+1} + z_2 ayx^d)} \right).
\end{aligned}$$

Durum 1: $a = 0$ ve $b \neq 0$ için

$$\begin{aligned}
\Omega_2 &= p^t \sum_{z_2 \in \mathbb{F}_p^\star} \sum_{z_1 \in \mathbb{F}_p^\star} \epsilon_p^{-\lambda z_1} + \sum_{z_1 \in \mathbb{F}_p^\star} \epsilon_p^{-\lambda z_1} \sum_{z_2 \in \mathbb{F}_p^\star} \sum_{x \in \mathbb{F}_q^\star} \epsilon_p^{\mathrm{Tr}(z_2 bx)} \left(\sum_{y \in \mathbb{F}_q} \epsilon_p^{\mathrm{Tr}(z_1 yx^{d+1})} \right) \\
&= \begin{cases} (p-1)^2 p^t, & \text{eğer } \lambda = 0; \\ -(p-1)p^t, & \text{eğer } \lambda \neq 0. \end{cases}
\end{aligned}$$

Durum 2: $a \neq 0$ ve $b \in \mathbb{F}_q$ için

$$\begin{aligned}
\Omega_2 &= p^t \sum_{z_1, z_2 \in \mathbb{F}_p^\star} \epsilon_p^{-\lambda z_1} + \sum_{z_1, z_2 \in \mathbb{F}_p^\star} \epsilon_p^{-\lambda z_1} \sum_{x \in \mathbb{F}_q^\star} \epsilon_p^{\mathrm{Tr}(z_2 bx)} \left(\sum_{y \in \mathbb{F}_q} \epsilon_p^{\mathrm{Tr}((z_1 x + z_2 a) yx^d)} \right) \\
&= p^t \sum_{z_1, z_2 \in \mathbb{F}_p^\star} \epsilon_p^{-\lambda z_1} + \sum_{z_1, z_2 \in \mathbb{F}_p^\star} \epsilon_p^{-\lambda z_1} \sum_{z_1 x + z_2 a = 0} \epsilon_p^{\mathrm{Tr}(z_2 bx)} p^t \\
&= p^t \sum_{z_1, z_2 \in \mathbb{F}_p^\star} \epsilon_p^{-\lambda z_1} + p^t \sum_{z_1, z_2 \in \mathbb{F}_p^\star} \epsilon_p^{-\lambda z_1} \epsilon_p^{-z_1^{-1} z_2^2 \mathrm{Tr}(ab)}
\end{aligned}$$

$\mathrm{Tr}(ab) = 0$ ise,

$$\Omega_2 \;= 2p^t \sum_{z_1 \in \mathbb{F}_p^\star} \epsilon_p^{-\lambda z_1} = \begin{cases} 2(p-1)^2 p^t, & \text{eğer } \lambda = 0; \\ -2(p-1)p^t, & \text{eğer } \lambda \neq 0. \end{cases}$$

$\mathrm{Tr}(ab) \neq 0$ ise,

$$\begin{aligned}
\Omega_2 &= p^t \sum_{z_1,z_2 \in \mathbb{F}_p^\star} \epsilon_p^{-\lambda z_1} + p^t \sum_{z_1,z_2 \in \mathbb{F}_p^\star} \epsilon_p^{-\lambda z_1} \epsilon_p^{-z_1^{-1} z_2^2 \mathrm{Tr}(ab)} \\
&= p^t \sum_{z_1,z_2 \in \mathbb{F}_p^\star} \epsilon_p^{-\lambda z_1} + p^t \sum_{z_1 \in \mathbb{F}_p^\star} \epsilon_p^{-\lambda z_1} \sum_{z_2 \in \mathbb{F}_p^\star} \epsilon_p^{-z_1^{-1}\mathrm{Tr}(ab) z_2^2} \\
&= p^t \sum_{z_1,z_2 \in \mathbb{F}_p^\star} \epsilon_p^{-\lambda z_1} + p^t \sum_{z_1 \in \mathbb{F}_p^\star} \epsilon_p^{-\lambda z_1} \left(\eta_1(-\mathrm{Tr}(ab) z_1^{-1}) G_1 - 1 \right) \\
&= p^t \sum_{z_1,z_2 \in \mathbb{F}_p^\star} \epsilon_p^{-\lambda z_1} - p^t \sum_{z_1 \in \mathbb{F}_p^\star} \epsilon_p^{-\lambda z_1} + p^t G_1 \eta_1(-1) \sum_{z_1 \in \mathbb{F}_p^\star} \eta_1 \left(\frac{z_1}{4\mathrm{Tr}(ab)} \right) \epsilon_p^{-\lambda z_1} \\
&= p^t \sum_{z_1,z_2 \in \mathbb{F}_p^\star} \epsilon_p^{-\lambda z_1} - p^t \sum_{z_1 \in \mathbb{F}_p^\star} \epsilon_p^{-\lambda z_1} + p^t G_1 \eta_1(-1) \sum_{z_1 \in \mathbb{F}_p^\star} \eta_1 \left(\frac{z_1}{4\mathrm{Tr}(ab)} \right) \epsilon_p^{\frac{z_1}{4\mathrm{Tr}(ab)}(-4\lambda \mathrm{Tr}(ab))} \\
&= \begin{cases} (p-1)^2 p^t - (p-1)p^t, & \text{eğer } \lambda = 0; \\ -(p-1)p^t + p^t + p^t \eta_1(-1)\eta_1(k) G_1^2, & \text{eğer } \lambda \neq 0 \text{ ve } -4\lambda \mathrm{Tr}(ab) \in SQ; \\ -(p-1)p^t + p^t + p^t \eta_1(-1)\eta_1(k) G_1^2, & \text{eğer } \lambda \neq 0 \text{ ve } -4\lambda \mathrm{Tr}(ab) \in NSQ, \end{cases} \\
&= \begin{cases} (p-2)(p-1)p^t, & \text{eğer } \lambda = 0; \\ 2p^t, & \text{eğer } \lambda \neq 0 \text{ ve } -4\lambda \mathrm{Tr}(ab) \in SQ; \\ 2(1-p)p^t, & \text{eğer } \lambda \neq 0 \text{ ve } -4\lambda \mathrm{Tr}(ab) \in NSQ. \end{cases}
\end{aligned}$$

Elde edilen değerler $\#N_\lambda(a,b) = p^{2t-2} + \frac{1}{p^2}(\Omega_0 + \Omega_1 + \Omega_2)$ denkleminde yerine yazılarak istenilen sonuçlar elde edilir. Böylece lemmanın ispatı tamamlanmıştır.

İz fonksiyonu dengeli olduğu için aşağıdaki sonuç açıkça verilebilir. Bu sonuç kodun ağırlık dağılımını hesaplamak için kullanılacaktır.

Lemma 4.3 *$l \in \mathbb{F}_p$ için*

$$A(l) = \left\{ (a,b) \in \mathbb{F}_{p^t}^\star \times \mathbb{F}_{p^t} \mid \mathrm{Tr}(ab) = l \right\}$$

olsun. Bu durumda $\#A(l) = p^{t-1}(p^t - 1)$ olur.

Elde ettiğimiz kodunun parametrelerini aşağıdaki teoremde verelim.

Teorem 4.1 *$t \geq 2$ bir tam sayı olsun. $\lambda \in \mathbb{F}_p^\star$ için denklem (4.1)'deki D_λ tanım kümesi ve denklem (4.2)'deki C_{D_λ} kodu verilsin. Bu durumda, C_{D_λ} kodu $\mathbb{F}_p$ cismi üzerinde $[p^{2t-1} - p^{t-1}, 2t, (p^t - p^{t-1} - 2)p^{t-1}]$ parametrelerine sahip iki-ağırlıklı bir koddur ve Hamming ağırlığı Çizelge 4.1'de verilmiştir.*

Çizelge 4.1. Teorem 4.1'deki C_{D_λ} kodunun parametreleri

Hamming Ağırlığı ω	*Frekansı* A_ω
0	1
$(p-1)p^{2t-2}$	$(\frac{1}{2}(p+1)p^{t-1}+1)(p^t-1)$
$(p^t-p^{t-1}-2)p^{t-1}$	$\frac{1}{2}(p-1)p^{t-1}(p^t-1)$

İspat C_{D_λ} kodunun tanımından dolayı uzunluğu

$$n = \#D_\lambda = p^{2t-1} - p^{t-1}.$$

$\lambda \in \mathbb{F}_p^\star$ ve $a, b \in \mathbb{F}_{p^t}$ için Lemma 4.2'den aşağıdaki iki durum vardır.

- $a = 0 \wedge b \neq 0,$ veya $a \neq 0 \wedge b \in \mathbb{F}_q \wedge \mathrm{Tr}(ab) = 0$ veya $a \neq 0 \wedge b \in \mathbb{F}_q \wedge \mathrm{Tr}(ab) \neq 0 \wedge -4\lambda\mathrm{Tr}(ab) \in NSQ$ durumlarında $\#N_\lambda(a,b) = p^{2t-2} - p^{t-1}$.
- $a \neq 0 \wedge b \in \mathbb{F}_q \wedge \mathrm{Tr}(ab) \neq 0 \wedge -4\lambda\mathrm{Tr}(ab) \in SQ$ durumlarında $\#N_\lambda(a,b) = p^{2t-2} + p^{t-1}$.

Bu durumlar göz önüne alınarak her kod sözcüğünün Hamming ağırlığı $wt(\mathbf{c}_{(a,b)}) = n - \#N_\lambda(a,b)$ şeklinde hesaplanarak

- $w_1 = p^{2t-1} - p^{2t-2}$ eğer $a = 0 \wedge b \neq 0$ veya $a \neq 0 \wedge b \in \mathbb{F}_q \wedge \mathrm{Tr}(ab) = 0$ veya $a \neq 0 \wedge b \in \mathbb{F}_q \wedge \mathrm{Tr}(ab) \neq 0 \wedge -4\lambda\mathrm{Tr}(ab) \in NSQ$,
- $w_2 = p^{2t-1} - p^{2t-2} - 2p^{t-1}$ eğer $a \neq 0 \wedge b \in \mathbb{F}_q \wedge \mathrm{Tr}(ab) \neq 0 \wedge -4\lambda\mathrm{Tr}(ab) \in SQ$

elde edilir. Yukarıdaki durumlar ve Lemma 4.3 göz önüne alınarak w_1 ve w_2 ağırlıklarının frekansları

$$\begin{aligned} A_{w_1} &= p^{t-1} + \#A(0) + \sum_{\eta_1(-4\lambda l)=1} \#A(l) \\ &= (p^{t-1}+1)(p^t-1) + \tfrac{p-1}{2}p^{t-1}(p^t-1) \\ &= (\tfrac{1}{2}(p+1)p^{t-1}+1)(p^t-1), \\ A_{w_2} &= \sum_{\eta_1(-4\lambda l)=-1} \#A(l) = \frac{1}{2}(p-1)p^{t-1}(p^t-1) \end{aligned}$$

şeklinde elde edilir. Böylece teoremin ispatı tamamlanmış olur.

Not 4.1 *$\lambda \in \mathbb{F}_p^\star$ için denklem (4.1)'deki D_λ tanım kümesi üzerinde tanımlanan denklem (4.2)'deki C_{D_λ} kodu (Zhu ve Liao, 2023) çalışmasında Teorem 4.3'de verilen kodla aynı koddur. $\lambda \in \mathbb{F}_p^\star$ durumunda, D_λ kümesinin tanımında $(0, y)$ elemanlarını kümeye dahil etmemizin C_{D_λ} kodunu etkilemediğini gözlemledik.*

Örnek 4.1 *$p = 5$ ve $t = 2$ için denklem (4.1)-(4.2) kullanılarak MAGMA programı (Bosma vd., 1997) ile $\mathbb{F}_p$ cismi üzerinde $C_{D_\lambda} = [120, 4, 90]$ kodunun ağırlık polinomu $1 + 240z^{90} + 384z^{100}$ şeklinde elde edilmiştir. C_{D_λ} kodu iki-ağırlıklı projektif minimal koddur. Bu kodun dual kodu $C_{D_\lambda}^{\perp} = [120, 116, 2]$ şeklindedir. Bu sonuç Teorem 4.1 ile uyumludur.*

Not 4.2 *Bu bölümde, $\lambda = 0$ için denklem (4.1)'deki D_0 tanım kümesi üzerinde tanımlanan denklem (4.2)'deki C_{D_0} kümesi vektör uzayı oluşturmadığı için bir kod değildir. D_0 kümesindeki $(0, y)$ elemanları için her kod sözcüğünün karşılık gelen bileşeni sıfırdır. Dolayısıyla, C_{D_0} kümesini üreten kod sözcükleri lineer bağımlıdır. Diğer bir ifadeyle, C_{D_0} kümesinin üreteç matrisi sıfır sütunlarına sahiptir ve matrisin rankı k dan azdır.*

4.2. D_{01} Kümesi Üzerinde Tanımlanan Üç Ağırlıklı Doğrusal Kodun İnşası

d herhangi bir pozitif tamsayı olmak üzere

$$D_{01} = \left\{(x, y) \in \mathbb{F}_q^\star \times \mathbb{F}_q \mid \mathrm{Tr}(yx^{d+1}) \in \{0, 1\}\right\} \tag{4.4}$$

kümesi verilsin. Tanımdan dolayı $(0, 0) \notin D_{01}$'dır. Bu küme üzerinde

$$C_{D_{01}} = \left\{\mathbf{c}_{(a,b)} = \mathrm{Tr}(ayx^d + bx)_{(x,y)\in D_{01}} \mid (a, b) \in \mathbb{F}_{p^t} \times \mathbb{F}_{p^t}\right\} \tag{4.5}$$

kodunu tanımlayalım. Tanım gereği bu kodun uzunluğu tanım kümesinin eleman sayısına eşittir. Tanımdan dolayı $\mathbf{c}_{(0,0)}$ kod sözcüğünün Hamming ağırlığı 0'dır. Her $(a, b) \in \mathbb{F}_q \times \mathbb{F}_q \setminus \{(0, 0)\}$ için $\mathbf{c}_{(a,b)}$ kod sözcüğünün Hamming ağırlığını bulmayı amaçlıyoruz.

Öncelikle aşağıdaki lemmada tanım kümesinin eleman sayısını (kodun uzunluğunu) verelim. Bu sonuç Lemma 3.1'den kolaylıkla elde edilebilir.

Lemma 4.4 *Denklem (4.4)'de verilen D_{01} kümesinin eleman sayısı $\#D_{01} = 2p^{2t-1} - 2p^{t-1}$.*

$C_{D_{01}}$ kodunun Hamming ağırlığını hesaplamak için $(a, b) \in \mathbb{F}_q \times \mathbb{F}_q \setminus \{(0, 0)\}$ olmak üzere

$$N_{01}(a, b) = \left\{(x, y) \in \mathbb{F}_q^\star \times \mathbb{F}_q \mid \mathrm{Tr}(x^{d+1}y) \in \{0, 1\} \text{ ve } \mathrm{Tr}(ax^d y + bx) = 0\right\} \tag{4.6}$$

kümesini tanımlayalım. Lemma 3.2'den bu kümenin eleman sayısını hesaplayan aşağıdaki lemmayı verebiliriz.

Lemma 4.5 $(a,b) \in \mathbb{F}_q \times \mathbb{F}_q \setminus \{(0,0)\}$ *olmak üzere denklem (4.6)'da verilen* $N_{01}(a,b)$ *kümesinin eleman sayısı* $\#N_{01}(a,b)$

$$= \begin{cases} 2p^{2t-2} - 2p^{t-1}, & \text{eğer } a = 0 \wedge b \neq 0, \text{ veya} \\ & a \neq 0 \wedge b \in \mathbb{F}_q \wedge \mathrm{Tr}(ab) \neq 0 \wedge -\lambda \mathrm{Tr}(ab) \in NSQ; \\ 2p^{2t-2} - 3p^{t-1} + p^t, & \text{eğer } a \neq 0 \wedge b \in \mathbb{F}_q \wedge \mathrm{Tr}(ab) = 0; \\ 2p^{2t-2}, & \text{eğer } a \neq 0 \wedge b \in \mathbb{F}_q \wedge \mathrm{Tr}(ab) \neq 0 \wedge -\lambda \mathrm{Tr}(ab) \in SQ. \end{cases}$$

Aşağıdaki teoremde kodun parametrelerini veriyoruz.

Teorem 4.2 $t \geq 2$ *bir tam sayı olsun. Denklem (4.4)'deki* D_{01} *tanım kümesi ve denklem (4.5)'deki* $C_{D_{01}}$ *kodu verilsin. Bu durumda* $C_{D_{01}}$ *kodu* $\mathbb{F}_p$ *cismi üzerinde* $[2p^{2t-1} - 2p^{t-1}, 2t, p^{t-1}(2p^t - 2p^{t-1} - p + 1)]$ *parametrelerine sahip üç-ağırlıklı bir koddur ve Hamming ağırlığı Çizelge 4.2'de verilmiştir.*

Çizelge 4.2. Teorem 4.2'deki $C_{D_{01}}$ kodunun parametreleri

Hamming Ağırlığı ω	Frekansı A_ω
0	1
$(p-1)2p^{2t-2}$	$(\frac{1}{2}(p-1)p^{t-1}+1)(p^t-1)$
$p^{t-1}(2p^t - 2p^{t-1} - p + 1)$	$(p^t-1)p^{t-1}$
$2p^{t-1}(p^t - p^{t-1} - 1)$	$\frac{1}{2}(p-1)p^{t-1}(p^t-1)$

İspat $C_{D_{01}}$ kodunun tanımından dolayı uzunluğu

$$n = \#D_{01} = 2p^{2t-1} - 2p^{t-1}.$$

Her $a, b \in \mathbb{F}_{p^t}$ için Lemma 4.5'den aşağıdaki üç durum vardır.

- Durum 1: $a = 0 \wedge b \neq 0,$ veya $a \neq 0 \wedge b \in \mathbb{F}_q \wedge \mathrm{Tr}(ab) \neq 0 \wedge -\lambda \mathrm{Tr}(ab) \in NSQ$ için $\#N_{01}(a,b) = 2p^{2t-2} - 2p^{t-1}$.
- Durum 2: $a \neq 0 \wedge b \in \mathbb{F}_q \wedge \mathrm{Tr}(ab) = 0$ için $\#N_{01}(a,b) = 2p^{2t-2} - 3p^{t-1} + p^t$.
- Durum 3: $a \neq 0 \wedge b \in \mathbb{F}_q \wedge \mathrm{Tr}(ab) \neq 0 \wedge -\lambda \mathrm{Tr}(ab) \in SQ$ için $\#N_{01}(a,b) = 2p^{2t-2}$.

Bu durumlar göz önüne alınarak Hamming ağırlıklar $wt(\mathbf{c}_{(a,b)}) = n - \#N_{01}(a,b)$ şeklinde hesaplanarak

- $w_1 = 2p^{2t-1} - 2p^{2t-2}$ eğer $a = 0 \wedge b \neq 0,$ veya $a \neq 0 \wedge b \in \mathbb{F}_q \wedge \mathrm{Tr}(ab) \neq 0 \wedge -\lambda \mathrm{Tr}(ab) \in NSQ$,

- $w_2 = 2p^{2t-1} - 2p^{2t-2} + p^{t-1} - p^t$ eğer $a \neq 0 \wedge b \in \mathbb{F}_q \wedge \mathrm{Tr}(ab) = 0$,
- $w_3 = 2p^{2t-1} - 2p^{2t-2} - 2p^{t-1}$ eğer $a \neq 0 \wedge b \in \mathbb{F}_q \wedge \mathrm{Tr}(ab) \neq 0 \wedge -\lambda \mathrm{Tr}(ab) \in SQ$

elde edilir. Yukarıdaki durumlar ve Lemma 4.3 göz önüne alınarak w_1, w_2 ve w_3 ağırlıklarının frekansları

$$\begin{aligned} A_{w_1} &= (p^t - 1) + \sum_{\eta_1(-\lambda l)=1} \#A(l) = (p^t - 1)(\frac{1}{2}(p-1)p^{t-1} + 1), \\ A_{w_2} &= \#A(0) = (p^t - 1)p^{t-1}, \\ A_{w_3} &= \sum_{\eta_1(-\lambda l)=-1} \#A(l) = \frac{1}{2}(p-1)p^{t-1}(p^t - 1) \end{aligned}$$

şeklinde elde edilir. Böylece teoremin ispatı tamamlanır.

Örnek 4.2 *$p = 3$ ve $t = 3$ için denklem (4.4)-(4.5) kullanılarak MAGMA programı (Bosma vd., 1997) ile $\mathbb{F}_p$ cismi üzerinde $C_{D_{01}} = [468, 6, 306]$ kodunun ağırlık polinomu $1 + 468z^{306} + 260z^{324}$ olarak elde edilmiştir. $C_{D_{01}}$ kodu 3 ağırlıklı minimal koddur. Bu kodun dual kodu $C_{D_{01}}^{\perp} = [468, 462, 2]$'dir. Bu sonuç Teorem 4.2 ile uyumludur.*

4.3. D_{SQ} Kümesi Üzerinde Tanımlanan İki Ağırlıklı Doğrusal Kodun İnşası

d herhangi bir pozitif tamsayı olmak üzere

$$D_{SQ} = \left\{(x, y) \in \mathbb{F}_q \times \mathbb{F}_q \mid \mathrm{Tr}(yx^{d+1}) \in SQ\right\} \tag{4.7}$$

tanım kümesi verilsin. Tanımdan dolayı $(0, 0) \notin D_{SQ}$'dır. Bu küme üzerinde

$$C_{D_{SQ}} = \left\{\mathbf{c}_{(a,b)} = \mathrm{Tr}(ayx^d + bx)_{(x,y)\in D_{SQ}} \mid (a, b) \in \mathbb{F}_{p^t} \times \mathbb{F}_{p^t}\right\} \tag{4.8}$$

kodunu tanımlayalım. Tanım gereği bu kodun uzunluğu tanım kümesinin eleman sayısına eşittir. Tanımdan dolayı $\mathbf{c}_{(0,0)}$ kod sözcüğünün Hamming ağırlığı 0'dır. Her $(a, b) \in \mathbb{F}_q \times \mathbb{F}_q \setminus \{(0, 0)\}$ için $\mathbf{c}_{(a,b)}$ kod sözcüğünün Hamming ağırlığını bulmayı amaçlıyoruz.

Öncelikle aşağıdaki lemmada tanım kümesinin eleman sayısını bulalım. Bu sonuç, Lemma 4.1'den kolaylıkla verilebilir.

Lemma 4.6 *Denklem 4.7'de verilen D_{SQ} tanım kümesinin eleman sayısı $\#D_{SQ} = \frac{p-1}{2}(p^{2t-1} - p^{t-1})$'dir.*

$C_{D_{SQ}}$kodunun Hamming ağırlığını hesaplamak için $(a,b) \in \mathbb{F}_q \times \mathbb{F}_q \setminus \{(0,0)\}$ olmak üzere

$$N_{SQ}(a,b) \ = \{(x,y) \in \mathbb{F}_q \times \mathbb{F}_q \mid \mathrm{Tr}(x^{d+1}y) \in SQ \text{ ve } \mathrm{Tr}(ax^d y + bx) = 0\} \quad (4.9)$$

kümesini tanımlayalım. Aşağıdaki lemmada bu kümenin eleman sayısını bulalım. Bu sonuç, Lemma 4.2'den kolaylıkla verilebilir.

Lemma 4.7 *$(a,b) \in \mathbb{F}_q \times \mathbb{F}_q \setminus \{(0,0)\}$ olmak üzere denklem (4.9)'de verilen $N_{SQ}(a,b)$ kümesinin eleman sayısı $\#N_{SQ}(a,b)$*

$$= \begin{cases} \frac{p-1}{2}(p^{2t-2} - p^{t-1}), & \text{eğer } a = 0 \wedge b \neq 0, \\ & \text{veya } a \neq 0 \text{ ve } b \in \mathbb{F}_q \text{ ve } \mathrm{Tr}(ab) = 0, \\ & \text{veya } a \neq 0 \wedge b \in \mathbb{F}_q \wedge \mathrm{Tr}(ab) \neq 0 \wedge -4\lambda\mathrm{Tr}(ab) \in NSQ; \\ \frac{p-1}{2}(p^{2t-2} + p^{t-1}), & \text{eğer } a \neq 0 \wedge b \in \mathbb{F}_q \wedge \mathrm{Tr}(ab) \neq 0 \wedge -4\lambda\mathrm{Tr}(ab) \in SQ. \end{cases}$$

Aşağıdaki teoremde kodun parametrelerini veriyoruz.

Teorem 4.3 *$t \geq 2$ bir tam sayı olsun. $\lambda \in SQ$ için denklem (4.7)'deki D_{SQ} tanım kümesi ve denklem (4.8)'deki $C_{D_{SQ}}$ kodu verilsin. Bu durumda $C_{D_{SQ}}$ kodu $\mathbb{F}_p$ cismi üzerinde $[\frac{p-1}{2}(p^{2t-1} - p^{t-1}), 2t, \frac{p-1}{2}(p^t - p^{t-1} - 2)p^{t-1}]$ parametrelerine sahip iki-ağırlıklı bir koddur ve Hamming ağırlığı Çizelge 4.3'de verilmiştir.*

Çizelge 4.3. Teorem 4.3'deki $C_{D_{SQ}}$ kodunun parametreleri

Hamming Ağırlığı ω	*Frekansı* A_ω
0	1
$\frac{p-1}{2}(p-1)p^{2t-2}$	$(\frac{1}{2}(p+1)p^{t-1}+1)(p^t-1)$
$\frac{p-1}{2}(p^t - p^{t-1} - 2)p^{t-1}$	$\frac{1}{2}(p-1)p^{t-1}(p^t-1)$

İspat C_{D_λ} kodunun tanımından dolayı uzunluğu şöyledir:

$$n = \#D_{SQ} = \frac{p-1}{2}(p^{2t-1} - p^{t-1})$$

ve her kod sözcüğünün Hamming ağırlığı

$$wt(\mathbf{c}_{(a,b)}) = n - \#N_{SQ}(a,b)$$

şeklindedir. $\lambda \in SQ$ ve $a,b \in \mathbb{F}_{p^t}$ için Lemma 4.7'den aşağıdaki iki durum vardır.

- Durum 1: $a = 0 \wedge b \neq 0,$ veya $a \neq 0 \wedge b \in \mathbb{F}_q \wedge \mathrm{Tr}(ab) = 0$ veya $a \neq 0 \wedge b \in \mathbb{F}_q \wedge \mathrm{Tr}(ab) \neq 0 \wedge -4\lambda\mathrm{Tr}(ab) \in NSQ$ durumlarında $\#N_{SQ}(a,b) = \frac{p-1}{2}(p^{2t-2} - p^{t-1})$.

- Durum 2: $a \neq 0 \wedge b \in \mathbb{F}_q \wedge \mathrm{Tr}(ab) \neq 0 \wedge -4\lambda\mathrm{Tr}(ab) \in SQ$ durumlarında $\#N_{SQ}(a,b) = \frac{p-1}{2}(p^{2t-2} + p^{t-1})$.

Dolayısıyla bu durumlar göz önüne alınarak her kod sözcüğünün ağırlığı $wt(\mathbf{c}_{(a,b)}) = n - \#N_{SQ}(a,b)$ şeklinde hesaplanarak Hamming ağırlıklar

- $w_1 = \frac{p-1}{2}(p^{2t-1} - p^{2t-2})$ eğer $a = 0 \wedge b \neq 0$ veya $a \neq 0 \wedge b \in \mathbb{F}_q \wedge \mathrm{Tr}(ab) = 0$ veya $a \neq 0 \wedge b \in \mathbb{F}_q \wedge \mathrm{Tr}(ab) \neq 0 \wedge -4\lambda\mathrm{Tr}(ab) \in NSQ$,
- $w_2 = \frac{p-1}{2}(p^{2t-1} - p^{2t-2} - 2p^{t-1})$ eğer $a \neq 0 \wedge b \in \mathbb{F}_q \wedge \mathrm{Tr}(ab) \neq 0 \wedge -4\lambda\mathrm{Tr}(ab) \in SQ$

elde edilir. Yukarıdaki durumlar ve Lemma 3.4 göz önüne alınarak w_1 ve w_2 ağırlıklarının frekansları

$$\begin{aligned} A_{w_1} &= p^{t-1} + \#A(0) + \sum_{\eta_1(-4\lambda l)=1} \#A(l) \\ &= (p^{t-1}+1)(p^t-1) + \tfrac{p-1}{2}p^{t-1}(p^t-1) \\ &= (\tfrac{1}{2}(p+1)p^{t-1}+1)(p^t-1), \\ A_{w_2} &= \sum_{\eta_1(-4\lambda l)=-1} \#A(l) = \frac{1}{2}(p-1)p^{t-1}(p^t-1) \end{aligned}$$

şeklinde elde edilir. Böylece teoremin ispatı tamamlanır.

Örnek 4.3 *$p = 5$ ve $t = 3$ için denklem (4.7)-(4.8) kullanılarak MAGMA programı (Bosma vd., 1997) ile $\mathbb{F}_p$ cismi üzerinde $C_{D_{SQ}} = [6200, 6, 4900]$ kodunun ağırlık polinomu $1 + 6200z^{4900} + 9424z^{5000}$ olarak elde edilmiştir. $C_{D_{SQ}}$ kodu iki-ağırlıklı projektif minimal koddur. Bu kodun dual kodu $C_{D_{SQ}}^{\perp} = [6200, 6194, 2]$ şeklindedir. Bu sonuç Teorem 4.3 ile uyumludur.*

5. DOĞRUSAL KODLAR İÇİN YENİ İNŞA YÖNTEMİ

Bu bölümde, (Zhu ve Liao, 2023) çalışmasındaki inşa yöntemi ile (Cheng vd., 2022) çalışmasındaki inşa yöntemi sentezlenerek yeni bir inşa yöntemi önerilmektedir. Önerilen yeni yöntem ile dört ağırlıklı yeni bir doğrusal kod ailesi elde edilmiştir. Çalışmada, düşük ağırlıklı doğrusal kodlar için kullanılan teknikler temel alınmıştır. Burada farklı elemanlar ve tanım kümesi seçilerek kod parametreleri üzerinde yeni sonuçlar elde edilmiştir. Özellikle, kodların inşa yönteminde tanım kümesi üzerinde yapılan değişiklikler ve yeni eleman seçimleri, elde edilen doğrusal kodun uzunluğunu, Hamming ağırlığını ve ağırlık dağılımını etkilemektedir.

(Cheng vd., 2022) çalışmasında D_2 tanım kümesi aşağıdaki gibi tanımlanmıştır,

$$D_2 = \{(x, y, z) \in \mathbb{F}_q^3 \setminus \{(0, 0, 0)\} : f(x) + g(y) + h(z) = 0\},$$

ve bu küme üzerinde aşağıdaki doğrusal kod

$$C_{D_2} = \{\mathrm{Tr}(ax + by + cz)_{(x,y,z)\in D_2} : a, b, c \in \mathbb{F}_q\}$$

tanımlanmıştır. Biz de bu çalışmadan esinlenerek (Zhu ve Liao, 2023) çalışmasındaki kod inşasına yeni bir terim ekleyerek yeni bir kod inşa yöntemi önerdik. Bu iki çalışmada verilen inşa yöntemlerinden yola çıkarak bu bölümde aşağıdaki inşa yöntemi tanımlanmıştır.

d herhangi bir pozitif tam sayı olmak üzere

$$D_0 = \left\{(x, y, z) \in \mathbb{F}_{p^t}^\star \times \mathbb{F}_{p^t} \times \mathbb{F}_{p^t} : \mathrm{Tr}(yx^{d+1}) + \mathrm{Tr}(z) = 0\right\} \tag{5.1}$$

kümesi verilsin. D_0 kümesinin tanımından dolayı $(0, 0, 0) \notin D_0$'dır. Bu küme üzerinde

$$C_{D_0} = \left\{\mathrm{Tr}(ayx^d + bx + cz)_{(x,y,z)\in D_0} \ : \ (a, b, c) \in \mathbb{F}_q^3\right\} \tag{5.2}$$

kodunu tanımlayalım. Tanım gereği bu kodun uzunluğu tanım kümesinin eleman sayısına eşittir. Tanımdan dolayı $\mathbf{c}_{(0,0,0)}$ kod sözcüğünün Hamming ağırlığı 0'dır. Her $(a, b, c) \in \mathbb{F}_q \times \mathbb{F}_q \times \mathbb{F}_q \setminus \{(0, 0, 0)\}$ için $\mathbf{c}_{(a,b,c)}$ kod sözcüğünün Hamming ağırlığını bulmak için aşağıdaki $N_0(a, b, c)$ kümesini tanımlayalım:

$$\begin{aligned}&\left\{(x, y, z) \in \mathbb{F}_{p^t}^\star \times \mathbb{F}_{p^t} \times \mathbb{F}_{p^t} \mid (x, y, z) \in D_0 \text{ ve } \mathrm{Tr}(ayx^d + bx + cz) = 0\right\} = \\ &\left\{(x, y, z) \in \mathbb{F}_{p^t}^\star \times \mathbb{F}_{p^t} \times \mathbb{F}_{p^t} \mid \mathrm{Tr}(yx^{d+1} + z) = 0 \text{ ve } \mathrm{Tr}(ayx^d + bx + cz) = 0\right\}.\end{aligned} \tag{5.3}$$

Aşağıdaki bölümde, kodun uzunluğunu ve koddaki kod sözcüklerinin Hamming ağırlıklarını bulmak için gerekli olan hesaplamalar yapılmaktadır.

5.1. Doğrusal Kod İnşası için Yardımcı Sonuçlar

Aşağıdaki lemmada tanım kümesinin eleman sayısı hesaplanmaktadır.

Lemma 5.1 *Denklem (5.1)'de verilen D_0 kümesinin eleman sayısı $n = \#D_0 = p^{3t-1} - p^{2t-1}$'dir.*

İspat Kümenin tanımından

$$\begin{aligned}
\#D_0 &= \sum_{x\in\mathbb{F}_{p^t}^\star}\sum_{y\in\mathbb{F}_{p^t}}\sum_{z\in\mathbb{F}_{p^t}}(p^{-1}\sum_{s_1\in\mathbb{F}_p}\epsilon_p^{s_1(\mathrm{Tr}(yx^{d+1})+\mathrm{Tr}(z))}) \\
&= \tfrac{1}{p}\sum_{x\in\mathbb{F}_{p^t}^\star}\sum_{y,z\in\mathbb{F}_{p^t}}\left(\sum_{s_1\in\mathbb{F}_p^\star}\epsilon_p^{s_1(\mathrm{Tr}(yx^{d+1})+\mathrm{Tr}(z))}+1\right) \\
&= p^{2t-1}(p^t-1)+\tfrac{1}{p}\sum_{s_1\in\mathbb{F}_p^\star}\sigma_{s_1}\left(\sum_{x\in\mathbb{F}_{p^t}^\star}\sum_{y\in\mathbb{F}_{p^t}}\epsilon_p^{\mathrm{Tr}(yx^{d+1})}\sum_{z\in\mathbb{F}_{p^t}}\epsilon_p^{\mathrm{Tr}(z)}\right) \\
&= p^{3t-1}-p^{2t-1}.
\end{aligned}$$

İspat böylece tamamlanmış olur.

Her $(a,b,c)\in\mathbb{F}_q\times\mathbb{F}_q\times\mathbb{F}_q\setminus\{(0,0,0)\}$ için C_{D_0} kodundaki kod sözcüklerinin Hamming ağırlıklarını hesaplamak için denklem (5.3)'te verilen $N_0(a,b,c)$ kümesinin eleman sayısını bulalım.

Lemma 5.2 *$(a,b,c)\in\mathbb{F}_q\times\mathbb{F}_q\times\mathbb{F}_q\setminus\{(0,0,0)\}$ olmak üzere denklem 5.3'te verilen $N_0(a,b,c)$ kümesinin eleman sayısı*

$$\#N_0(a,b,c)=\begin{cases}
p^{2t-2}(p^t-1) & \text{eğer } a=0,b=0,c\neq 0 \text{ veya } a=0,b\neq 0,c\neq 0 \\
 & \text{veya } a\neq 0,b=0,c=0 \text{ veya } a\neq 0,b\neq 0,c=0; \\
p^{2t-2}(p^t-p) & \text{eğer } a=0,b\neq 0,c=0; \\
p^{2t-2}(p^t+p-2) & \text{eğer } a\neq 0,b=0,c\neq 0 \text{ veya} \\
 & a\neq 0,b\neq 0,c\neq 0 \text{ ve } \mathrm{Tr}(\tfrac{ab}{c})=0; \\
p^{2t-2}(p^t-2) & \text{eğer } a\neq 0,\ b\neq 0,\ c\neq 0 \text{ ve } \mathrm{Tr}(\tfrac{ab}{c})\neq 0.
\end{cases}$$

İspat $N_0(a,b,c)$ kümesinin tanımından

$$\begin{aligned}
\#N_0(a,b,c) &= \sum_{x\in\mathbb{F}_{p^t}^\star}\sum_{y,z\in\mathbb{F}_{p^t}}(p^{-1}\sum_{s_1\in\mathbb{F}_p}\epsilon_p^{s_1(\mathrm{Tr}(yx^{d+1})+\mathrm{Tr}(z))})(p^{-1}\sum_{s_2\in\mathbb{F}_p}\epsilon_p^{s_2\mathrm{Tr}(ayx^d+bx+cz)}) \\
&= p^{-2}\sum_{x\in\mathbb{F}_{p^t}^\star}\sum_{y,z\in\mathbb{F}_{p^t}}(\sum_{s_1\in\mathbb{F}_p^\star}\epsilon_p^{s_1(\mathrm{Tr}(yx^{d+1})+\mathrm{Tr}(z))}+1)(\sum_{s_2\in\mathbb{F}_p^\star}\epsilon_p^{s_2\mathrm{Tr}(ayx^d+bx+cz)}+1) \\
&= p^{-2}\sum_{x\in\mathbb{F}_{p^t}^\star}\sum_{y,z\in\mathbb{F}_{p^t}}(1+\sum_{s_1\in\mathbb{F}_p^\star}\epsilon_p^{s_1(\mathrm{Tr}(yx^{d+1})+\mathrm{Tr}(z))}+\sum_{s_2\in\mathbb{F}_p^\star}\epsilon_p^{s_2\mathrm{Tr}(ayx^d+bx+cz)} \\
&+\sum_{s_1\in\mathbb{F}_p^\star}\sum_{s_2\in\mathbb{F}_p^\star}\epsilon_p^{s_1\mathrm{Tr}(yx^{d+1})+s_1\mathrm{Tr}(z)+s_2\mathrm{Tr}(ayx^d+bx+cz)}) \\
&= p^{2t-2}(p^t-1)+p^{-2}\sum_{s_1\in\mathbb{F}_p^\star}\sum_{x\in\mathbb{F}_{p^t}^\star}\sum_{y\in\mathbb{F}_{p^t}}\epsilon_p^{s_1\mathrm{Tr}(yx^{d+1})}\sum_{z\in\mathbb{F}_{p^t}}\epsilon_p^{s_1\mathrm{Tr}(z)} \\
&+p^{-2}\sum_{s_2\in\mathbb{F}_p^\star}\sum_{x\in\mathbb{F}_{p^t}^\star}\epsilon_p^{s_2\mathrm{Tr}(bx)}\sum_{y\in\mathbb{F}_{p^t}}\epsilon_p^{s_2\mathrm{Tr}(ayx^d)}\sum_{z\in\mathbb{F}_{p^t}}\epsilon_p^{s_2\mathrm{Tr}(cz)} \\
&+p^{-2}\sum_{s_1\in\mathbb{F}_p^\star}\sum_{s_2\in\mathbb{F}_p^\star}\sum_{x\in\mathbb{F}_{p^t}^\star}\epsilon_p^{s_2\mathrm{Tr}(bx)}\sum_{y\in\mathbb{F}_{p^t}}\epsilon_p^{\mathrm{Tr}(yx^d(s_1x+s_2a))}\sum_{z\in\mathbb{F}_{p^t}}\epsilon_p^{\mathrm{Tr}(z)(s_1+s_2c)} \\
&= p^{3t-2}-p^{2t-2}+\Delta_1(a,b,c)+\Delta_2(a,b,c)
\end{aligned}$$

elde edilir. Burada,

$$\Delta_1(a,b,c)=p^{-2}\sum_{s_2\in\mathbb{F}_p^\star}\sum_{x\in\mathbb{F}_{p^t}^\star}\epsilon_p^{s_2\mathrm{Tr}(bx)}\sum_{y\in\mathbb{F}_{p^t}}\epsilon_p^{s_2\mathrm{Tr}(ayx^d)}\sum_{z\in\mathbb{F}_{p^t}}\epsilon_p^{s_2\mathrm{Tr}(cz)},$$

$$\Delta_2(a,b,c)=p^{-2}\sum_{s_1\in\mathbb{F}_p^\star}\sum_{s_2\in\mathbb{F}_p^\star}\sum_{x\in\mathbb{F}_{p^t}^\star}\epsilon_p^{s_2\mathrm{Tr}(bx)}\sum_{y\in\mathbb{F}_{p^t}}\epsilon_p^{\mathrm{Tr}(yx^d(s_1x+s_2a))}\sum_{z\in\mathbb{F}_{p^t}}\epsilon_p^{\mathrm{Tr}(z)(s_1+s_2c)}.$$

$(a,b,c)\in\mathbb{F}_q\times\mathbb{F}_q\times\mathbb{F}_q\setminus\{(0,0,0)\}$ olmak üzere (a,b,c) üçlüsünün 7 farklı durumu için bu değerleri hesaplayarak istenilen sonuçları elde edeceğiz.

İlk olarak, $a=0,\ b\neq 0,\ c=0$ durumunda

$$\begin{aligned}
\Delta_1(0,b,0) &= p^{-2}\sum_{s_2\in\mathbb{F}_p^\star}\sum_{x\in\mathbb{F}_{p^t}^\star}\epsilon_p^{s_2\mathrm{Tr}(bx)}\sum_{y\in\mathbb{F}_{p^t}}\epsilon_p^{s_2\mathrm{Tr}(ayx^d)}\sum_{z\in\mathbb{F}_{p^t}}\epsilon_p^{s_2\mathrm{Tr}(cz)} \\
&= p^{-2}\sum_{s_2\in\mathbb{F}_p^\star}\sum_{x\in\mathbb{F}_{p^t}^\star}\epsilon_p^{s_2\mathrm{Tr}(bx)}\sum_{y\in\mathbb{F}_{p^t}}\epsilon_p^0\sum_{z\in\mathbb{F}_{p^t}}\epsilon_p^0 \\
&= p^{2t-2}\sum_{s_2\in\mathbb{F}_p^\star}\sum_{x\in\mathbb{F}_{p^t}^\star}\epsilon_p^{s_2\mathrm{Tr}(bx)} \\
&= p^{2t-2}(1-p)=p^{2t-2}-p^{2t-1}
\end{aligned}$$

elde edilir. Diğer tüm durumlarda, Tr dengeli bir fonksiyon olduğu için $\Delta_1(a,b,c)=0$ elde edilir. Şimdi, $\Delta_2(a,b,c)$ değerini 7 farklı durum için hesaplayalım.

Durum 1: $a \neq 0, b = 0, c = 0$ olsun.

$$\begin{aligned}
\Delta_2(a,0,0) &= p^{-2} \sum_{s_1 \in \mathbb{F}_p^\star} \sum_{s_2 \in \mathbb{F}_p^\star} \sum_{x \in \mathbb{F}_{p^t}^\star} \epsilon_p^{s_2 \mathrm{Tr}(bx)} \sum_{y \in \mathbb{F}_{p^t}} \epsilon_p^{\mathrm{Tr}(yx^d(s_1 x + s_2 a))} \sum_{z \in \mathbb{F}_{p^t}} \epsilon_p^{\mathrm{Tr}(z(s_1 + s_2 c))} \\
&= p^{-2} \sum_{s_1 \in \mathbb{F}_p^\star} \sum_{s_2 \in \mathbb{F}_p^\star} \sum_{x \in \mathbb{F}_{p^t}^\star} \epsilon_p^{s_2 \mathrm{Tr}(0x)} \sum_{y \in \mathbb{F}_{p^t}} \epsilon_p^{\mathrm{Tr}(yx^d(s_1 x + s_2 a))} \sum_{z \in \mathbb{F}_{p^t}} \epsilon_p^{\mathrm{Tr}(z(s_1 + 0))} \\
&= p^{-2} \sum_{s_1 \in \mathbb{F}_p^\star} \sum_{s_2 \in \mathbb{F}_p^\star} \sum_{x \in \mathbb{F}_{p^t}^\star} \epsilon_p^{0} \sum_{y \in \mathbb{F}_{p^t}} \epsilon_p^{\mathrm{Tr}(yx^d(s_1 x + s_2 a))} \sum_{z \in \mathbb{F}_{p^t}} \epsilon_p^{\mathrm{Tr}(s_1 z)} \\
&= 0.
\end{aligned}$$

Durum 2: $a = 0,\ b \neq 0,\ c = 0$ olsun.

$$\begin{aligned}
\Delta_2(0,b,0) &= p^{-2} \sum_{s_1 \in \mathbb{F}_p^\star} \sum_{s_2 \in \mathbb{F}_p^\star} \sum_{x \in \mathbb{F}_{p^t}^\star} \epsilon_p^{s_2 \mathrm{Tr}(bx)} \sum_{y \in \mathbb{F}_{p^t}} \epsilon_p^{\mathrm{Tr}(yx^d(s_1 x + s_2 a))} \sum_{z \in \mathbb{F}_{p^t}} \epsilon_p^{\mathrm{Tr}(z(s_1 + s_2 c))} \\
&= p^{-2} \sum_{s_1 \in \mathbb{F}_p^\star} \sum_{s_2 \in \mathbb{F}_p^\star} \sum_{x \in \mathbb{F}_{p^t}^\star} \epsilon_p^{s_2 \mathrm{Tr}(bx)} \sum_{y \in \mathbb{F}_{p^t}} \epsilon_p^{\mathrm{Tr}(yx^d(s_1 x + 0))} \sum_{z \in \mathbb{F}_{p^t}} \epsilon_p^{\mathrm{Tr}(z(s_1 + 0))} \\
&= p^{-2} \sum_{s_1 \in \mathbb{F}_p^\star} \sum_{s_2 \in \mathbb{F}_p^\star} \sum_{x \in \mathbb{F}_{p^t}^\star} \epsilon_p^{s_2 \mathrm{Tr}(bx)} \sum_{y \in \mathbb{F}_{p^t}} \epsilon_p^{s_1 \mathrm{Tr}(yx^{d+1})} \sum_{z \in \mathbb{F}_{p^t}} \epsilon_p^{\mathrm{Tr}(s_1 z)} \\
&= 0.
\end{aligned}$$

Durum 3: $a = 0,\ b = 0,\ c \neq 0$ olsun.

$$\begin{aligned}
\Delta_2(0,0,c) &= p^{-2} \sum_{s_1 \in \mathbb{F}_p^\star} \sum_{s_2 \in \mathbb{F}_p^\star} \sum_{x \in \mathbb{F}_{p^t}^\star} \epsilon_p^{s_2 \mathrm{Tr}(bx)} \sum_{y \in \mathbb{F}_{p^t}} \epsilon_p^{\mathrm{Tr}(yx^d(s_1 x + s_2 a))} \sum_{z \in \mathbb{F}_{p^t}} \epsilon_p^{\mathrm{Tr}(z(s_1 + s_2 c))} \\
&= p^{-2} \sum_{s_1 \in \mathbb{F}_p^\star} \sum_{s_2 \in \mathbb{F}_p^\star} \sum_{x \in \mathbb{F}_{p^t}^\star} \epsilon_p^{s_2 \mathrm{Tr}(0)} \sum_{y \in \mathbb{F}_{p^t}} \epsilon_p^{\mathrm{Tr}(yx^d(s_1 x + 0))} \sum_{z \in \mathbb{F}_{p^t}} \epsilon_p^{\mathrm{Tr}(z(s_1 + s_2 c))} \\
&= p^{-2} \sum_{s_1 \in \mathbb{F}_p^\star} \sum_{s_2 \in \mathbb{F}_p^\star} \sum_{x \in \mathbb{F}_{p^t}^\star} \epsilon_p^{0} \sum_{y \in \mathbb{F}_{p^t}} \epsilon_p^{s_1 \mathrm{Tr}(yx^{d+1})} \sum_{z \in \mathbb{F}_{p^t}} \epsilon_p^{\mathrm{Tr}(z(s_1 + s_2 c))} \\
&= 0.
\end{aligned}$$

Durum 4: $a \neq 0,\ b \neq 0,\ c = 0$ olsun.

$$\begin{aligned}
\Delta_2(a,b,0) &= p^{-2} \sum_{s_1 \in \mathbb{F}_p^\star} \sum_{s_2 \in \mathbb{F}_p^\star} \sum_{x \in \mathbb{F}_{p^t}^\star} \epsilon_p^{s_2 \mathrm{Tr}(bx)} \sum_{y \in \mathbb{F}_{p^t}} \epsilon_p^{\mathrm{Tr}(yx^d(s_1 x + s_2 a))} \sum_{z \in \mathbb{F}_{p^t}} \epsilon_p^{\mathrm{Tr}(z(s_1 + s_2 c))} \\
&= p^{-2} \sum_{s_1 \in \mathbb{F}_p^\star} \sum_{s_2 \in \mathbb{F}_p^\star} \sum_{x \in \mathbb{F}_{p^t}^\star} \epsilon_p^{s_2 \mathrm{Tr}(bx)} \sum_{y \in \mathbb{F}_{p^t}} \epsilon_p^{\mathrm{Tr}(yx^d(s_1 x + s_2 a))} \sum_{z \in \mathbb{F}_{p^t}} \epsilon_p^{\mathrm{Tr}(z(s_1 + 0))} \\
&= p^{-2} \sum_{s_1 \in \mathbb{F}_p^\star} \sum_{s_2 \in \mathbb{F}_p^\star} \sum_{x \in \mathbb{F}_{p^t}^\star} \epsilon_p^{s_2 \mathrm{Tr}(bx)} \sum_{y \in \mathbb{F}_{p^t}} \epsilon_p^{\mathrm{Tr}(yx^d(s_1 x + s_2 a))} \sum_{z \in \mathbb{F}_{p^t}} \epsilon_p^{\mathrm{Tr}(s_1 z)} \\
&= 0.
\end{aligned}$$

Durum 5: $a = 0,\ b \neq 0,\ c \neq 0$ olsun.

$$\begin{aligned}
\Delta_2(0,b,c) &= p^{-2} \sum_{s_1\in\mathbb{F}_p^\star} \sum_{s_2\in\mathbb{F}_p^\star} \sum_{x\in\mathbb{F}_{p^t}^\star} \epsilon_p^{s_2\mathrm{Tr}(bx)} \sum_{y\in\mathbb{F}_{p^t}} \epsilon_p^{\mathrm{Tr}(yx^d(s_1x+s_2a))} \sum_{z\in\mathbb{F}_{p^t}} \epsilon_p^{\mathrm{Tr}(z(s_1+s_2c))} \\
&= p^{-2} \sum_{s_1\in\mathbb{F}_p^\star} \sum_{s_2\in\mathbb{F}_p^\star} \sum_{x\in\mathbb{F}_{p^t}^\star} \epsilon_p^{s_2\mathrm{Tr}(bx)} \sum_{y\in\mathbb{F}_{p^t}} \epsilon_p^{\mathrm{Tr}(yx^d(s_1x+0))} \sum_{z\in\mathbb{F}_{p^t}} \epsilon_p^{\mathrm{Tr}(z(s_1+s_2c))} \\
&= p^{-2} \sum_{s_1\in\mathbb{F}_p^\star} \sum_{s_2\in\mathbb{F}_p^\star} \sum_{x\in\mathbb{F}_{p^t}^\star} \epsilon_p^{s_2\mathrm{Tr}(bx)} \sum_{y\in\mathbb{F}_{p^t}} \epsilon_p^{s_1\mathrm{Tr}(yx^{d+1})} \sum_{z\in\mathbb{F}_{p^t}} \epsilon_p^{\mathrm{Tr}(z(s_1+s_2c))} \\
&= 0.
\end{aligned}$$

Durum 6: $a \neq 0,\ b = 0,\ c \neq 0$ olsun.

$$\begin{aligned}
\Delta_2(a,0,c) &= p^{-2}. \sum_{s_1\in\mathbb{F}_p^\star} \sum_{s_2\in\mathbb{F}_p^\star} \sum_{x\in\mathbb{F}_{p^t}^\star} \epsilon_p^{s_2\mathrm{Tr}(bx)} \sum_{y\in\mathbb{F}_{p^t}} \epsilon_p^{\mathrm{Tr}(yx^d(s_1x+s_2a))} \sum_{z\in\mathbb{F}_{p^t}} \epsilon_p^{\mathrm{Tr}(z(s_1+s_2c))} \\
&= p^{-2}. \sum_{s_1\in\mathbb{F}_p^\star} \sum_{s_2\in\mathbb{F}_p^\star} \sum_{x\in\mathbb{F}_{p^t}^\star} \epsilon_p^{s_2\mathrm{Tr}(0)} \sum_{y\in\mathbb{F}_{p^t}} \epsilon_p^{\mathrm{Tr}(yx^d(s_1x+s_2a))} \sum_{z\in\mathbb{F}_{p^t}} \epsilon_p^{\mathrm{Tr}(z(s_1+s_2c)} \\
&= p^{-2} \sum_{s_2\in\mathbb{F}_p^\star} \sum_{s_1=-s_2c} \sum_{x=\frac{a}{c}} \epsilon_p^0 \sum_{y\in\mathbb{F}_{p^t}} \epsilon_p^0 \sum_{z\in\mathbb{F}_{p^t}} \epsilon_p^0 \\
&= p^{2t-2} \sum_{s_2\in\mathbb{F}_p^\star} \sum_{s_1=-s_2c} \sum_{x=\frac{a}{c}} 1 \\
&= p^{2t-2} \sum_{s_2\in\mathbb{F}_p^\star} 1 \\
&= p^{2t-1} - p^{2t-2}.
\end{aligned}$$

Yukarıdaki denklemde ikinci adımda $(s_1x + s_2a) \neq 0$ veya $(s_1 + s_2c) \neq 0$ durumlarında Tr fonksiyonu dengeli olduğu için toplam sıfır olur, bu yüzden sadece $(s_1x + s_2a) = 0$ ve $(s_1 + s_2c) = 0$ yani, $x = -\frac{s_2}{s_1}a$ ve $s_1 = -s_2c$ durumlarını ele alıyoruz. Son eşitlik Lemma 2.2'den açıktır.

Durum 7: $a \neq 0,\ b \neq 0,\ c \neq 0$ olsun.

$$\begin{aligned}
\Delta_2(a,b,c) &= p^{-2} \sum_{s_1\in\mathbb{F}_p^\star} \sum_{s_2\in\mathbb{F}_p^\star} \sum_{x\in\mathbb{F}_{p^t}^\star} \epsilon_p^{s_2\mathrm{Tr}(bx)} \sum_{y\in\mathbb{F}_{p^t}} \epsilon_p^{\mathrm{Tr}(yx^d(s_1x+s_2a))} \sum_{z\in\mathbb{F}_{p^t}} \epsilon_p^{\mathrm{Tr}(z(s_1+s_2c))} \\
&= p^{-2} \sum_{s_2\in\mathbb{F}_p^\star} \sum_{s_1=-s_2c} \sum_{x\in\mathbb{F}_{p^t}^\star} \epsilon_p^{s_2\mathrm{Tr}(bx)} \sum_{y\in\mathbb{F}_{p^t}} \epsilon_p^{\mathrm{Tr}(0)} \sum_{z\in\mathbb{F}_{p^t}} \epsilon_p^{\mathrm{Tr}(0)} \\
&= p^{-2} \sum_{s_2\in\mathbb{F}_p^\star} \sum_{s_1=-s_2c} \sum_{x=\frac{a}{c}} \epsilon_p^{s_2\mathrm{Tr}(\frac{ab}{c})} \sum_{y\in\mathbb{F}_{p^t}} \epsilon_p^0 \sum_{z\in\mathbb{F}_{p^t}} \epsilon_p^0 \\
&= p^{2t-2} \sum_{s_2\in\mathbb{F}_p^\star} \sum_{s_1=-s_2c} \sum_{x=\frac{a}{c}} \epsilon_p^{s_2\mathrm{Tr}(\frac{ab}{c})} \\
&= p^{2t-2} \sum_{s_2\in\mathbb{F}_p^\star} \epsilon_p^{s_2\mathrm{Tr}(\frac{ab}{c})} \\
&= \begin{cases} p^{2t-1} - p^{2t-2} & \text{eğer } \mathrm{Tr}(\frac{ab}{c}) = 0; \\ -p^{2t-2} & \text{eğer } \mathrm{Tr}(\frac{ab}{c}) \neq 0. \end{cases}
\end{aligned}$$

Yukarıdaki denklemde birinci adımda $(s_1x+s_2a) \neq 0$ veya $(s_1+s_2c) \neq 0$ durumlarında Tr fonksiyonu dengeli olduğu için toplam sıfır olur, bu yüzden sadece $(s_1x + s_2a) = 0$ ve $(s_1 + s_2c) = 0$ yani, $x = -\frac{s_2}{s_1}a$ ve $s_1 = -s_2c$ durumlarını ele alıyoruz. Son eşitlik Lemma 2.2'den açıktır. Elde edilen $\Delta_1(a, b, c)$ ve $\Delta_2(a, b, c)$ değerleri

$$\#N_0(a, b, c) = p^{3t-2} - p^{2t-2} + \Delta_1(a, b, c) + \Delta_2(a, b, c)$$

denkleminde yerlerine yazılarak istenen sonuçlar elde edilir. Böylece lemmanın ispatı tamamlanır.

İz fonksiyonu dengeli olduğu için aşağıdaki sonuç kolaylıkla gözlemlenebilir. Bu sonuç kodun frekansını hesaplamak için bize yardımcı olacaktır.

Lemma 5.3 *$l \in \mathbb{F}_p$ için*

$$B(l) = \left\{(a, b, c) \in \mathbb{F}_{p^t}^\star \times \mathbb{F}_{p^t}^\star \times \mathbb{F}_{p^t}^\star \mid \mathrm{Tr}\left(\frac{ab}{c}\right) = l\right\}$$

olsun. Bu durumda

$$\#B(l) = \begin{cases} (p^t - 1)^2(p^{t-1} - 1), & l = 0; \\ (p^t - 1)^2 p^{t-1}(p - 1), & l \neq 0. \end{cases}$$

5.2. D_0 Kümesi Üzerinde Tanımlanan Dört Ağırlıklı Doğrusal Kodun İnşası

Bu bölümde, C_{D_0} kodunun parametreleri verilmiştir.

Teorem 5.1 *$t \geq 2$ bir tam sayı olsun. Denklem 5.1'deki D_0 tanım kümesi ve denklem 5.2'deki C_{D_0} kodu verilsin. Bu durumda, C_{D_0} kodu $\mathbb{F}_p$ cismi üzerinde $[p^{2t-1}(p^t - 1), 3t, (p - 1)(p^{3t-2} - 2p^{2t-2})]$ parametrelerine sahip dört-ağırlıklı bir koddur ve kodun ağırlıklı dağılımı Çizelge 5.1'de verilmiştir.*

Çizelge 5.1. Teorem 5.1'deki C_{D_0} kodunun parametreleri

Hamming Ağırlığı ω	*Frekansı* A_ω
0	1
$(p-1)(p^t-1)p^{2t-2}$	$2p^{2t} - 2p^t$
$(p-1)p^{3t-2}$	$p^t - 1$
$(p-1)(p^{3t-2} - 2p^{2t-2})$	$(p^t-1)^2p^{t-1}$
$(p-1)p^{3t-2} - (p-2)p^{2t-2}$	$(p^t-1)^2p^{t-1}(p-1)$

İspat C_{D_0} kodunun tanımından dolayı uzunluğu

$$n = \#D_0 = p^{3t-1} - p^{2t-1}$$

ve her kod sözcüğünün Hamming ağırlığı

$$wt(\mathbf{c}_{(a,b,c)}) = n - \#N_0(a,b,c)$$

şeklindedir. $a, b, c \in \mathbb{F}_{p^t}$ olmak üzere Lemma 5.2'den aşağıdaki dört durum vardır.

- Durum 1: $a = 0, b = 0, c \neq 0$ veya $a = 0, b \neq 0, c \neq 0$ veya $a \neq 0, b = 0, c = 0$ veya $a \neq 0, b \neq 0, c = 0$ için $\#N_0(a,b,c) = p^{2t-2}(p^t - 1)$.
- Durum 2: $a = 0$, $b \neq 0$ ve $c = 0$ için $\#N_0(a,b,c) = p^{2t-2}(p^t - p)$.
- Durum 3: $a \neq 0$, $b = 0$ ve $c \neq 0$ veya $a \neq 0, b \neq 0, c \neq 0$ ve $\mathrm{Tr}(\frac{ab}{c}) = 0$ için $\#N_0(a,b,c) = p^{2t-2}(p^t + p - 2)$.
- Durum 4: $a \neq 0,\ b \neq 0,\ c \neq 0$ ve $\mathrm{Tr}(\frac{ab}{c}) \neq 0$ için $\#N_0(a,b,c) = p^{2t-2}(p^t - 2)$.

Dolayısıyla bu durumlar göz önüne alınarak her kod sözcüğünün Hamming ağırlığı $wt(\mathbf{c}_{(a,b,c)}) = n - \#N_0(a,b,c)$ şeklinde hesaplanarak

- $w_1 = (p-1)(p^t - 1)p^{2t-2}$ eğer $a = 0, b = 0, c \neq 0$ veya $a = 0, b \neq 0, c \neq 0$ veya $a \neq 0, b = 0, c = 0$ veya $a \neq 0, b \neq 0, c = 0$,
- $w_2 = (p-1)p^{3t-2}$ eğer $a = 0, b \neq 0, c = 0$,
- $w_3 = (p-1)(p^{3t-2} - 2p^{2t-2})$ eğer $a \neq 0, b = 0, c \neq 0$ veya $a \neq 0, b \neq 0, c \neq 0$ ve $\mathrm{Tr}(\frac{ab}{c}) = 0$,
- $w_4 = (p-1)p^{3t-2} - (p-2)p^{2t-2}$ eğer $a \neq 0,\ b \neq 0,\ c \neq 0$ ve $\mathrm{Tr}(\frac{ab}{c}) \neq 0$

elde edilir. Yukarıdaki durumlar göz önüne alınarak w_1 ve w_2 ağırlıklarının frekansları

$$\begin{aligned} A_{w_1} &= (p^t - 1) + (p^t - 1)^2 + (p^t - 1) + (p^t - 1) = 2p^{2t} - 2p^t, \\ A_{w_2} &= p^t - 1 \end{aligned}$$

olarak kolaylıkla belirlenebilir. Ayrıca, Lemma 5.3 göz önüne alınarak w_3 ve w_4 ağırlıklarının frekansları

$$\begin{aligned} A_{w_3} &= (p^t - 1)^2 + \#B(0) = (p^t - 1)^2 + (p^t - 1)^2(p^{t-1} - 1) = p^{t-1}(p^t - 1)^2, \\ A_{w_4} &= \sum_{l \in \mathbb{F}_p^\star} \#B(l) = (p^t - 1)(p^t - 1)p^{t-1}(p-1) = (p^t - 1)^2 p^{t-1}(p-1) \end{aligned}$$

şeklinde elde edilir. Böylece teoremin ispatı tamamlanmış olur.

Örnek 5.1 $p = 5$ *ve* $t = 2$ *için denklem (5.1)-(5.2) kullanılarak MAGMA programı (Bosma vd., 1997) ile* $\mathbb{F}_p$ *cismi üzerinde* $C_{D_0} = [3000, 6, 2300]$ *kodunun ağırlık polinomu* $1 + 2880z^{2300} + 1200z^{2400} + 11520z^{2425} + 24z^{2500}$ *olarak elde edilmiştir.* C_{D_0} *kodu dört-ağırlıklı minimal koddur. Bu kodun dual kodu* $C_{D_0}^{\perp} = [3000, 2994, 2]$ *şeklindedir. Bu sonuç Teorem 5.1 ile uyumludur.*

6. MINIMAL KODLARDAN SIR PAYLAŞIM ŞEMALARININ TASARIMI

Bu bölümde, önceki bölümlerde (Bölüm 4 ve Bölüm 5) elde edilen doğrusal kodların minimal kodlar olduklarını gözlemliyoruz. Daha sonra elde edilen kodların dual kodlarının minimum mesafe $d^{\perp}$ değerlerini buluyoruz ve bu kodlardan oluşturulan sır paylaşım şemalarının tasarımlarını veriyoruz.

Öncelikle doğrusal kodların kapsama problemini hatırlayalım.

Doğrusal Kodların Kapsama Problemi: C, $\mathbb{F}_p$ cismi üzerinde doğrusal bir $[n, k, d]_p$ kodu olsun. Eğer $\mathrm{supp}(\mathbf{b}) \subset \mathrm{supp}(\mathbf{a})$ ise, $\mathbf{a}$ kod sözcüğünün $\mathbf{b}$ kod sözcüğünü kapsadığını söyleriz. Eğer doğrusal bir C kodunun sıfır olmayan kod sözcüğü $\mathbf{a}$, C kodunun sıfırdan farklı herhangi bir kod sözcüğünü kapsamıyorsa, o zaman $\mathbf{a}$ kod sözcüğüne C kodunun minimal kod sözcüğü denir.

Tanım 6.1 *Doğrusal bir C kodunun kapsama problemi, C kodunun tüm minimal kod sözcüklerini bulmayı amaçlar.*

Kapsama problemi genel doğrusal kodlar için son derece zordur, ancak bazı özel doğrusal kodlar için kolaydır.

Doğrusal bir C kodunun kod sözcüklerinin Hamming ağırlıkları birbirine çok yakın olduğunda, C kodunun sıfırdan farklı tüm kod sözcükleri minimaldir. Dolayısıyla, C kodu minimal koddur. Verilen bir doğrusal kodun minimal kod olması için yeter koşul olan bu sonucu aşağıdaki lemmada ifade edelim.

Lemma 6.1 *(Ashikhmin ve Barg, 1998; Ashikhmin vd., 1995) C, $\mathbb{F}_p$ cismi üzerinde doğrusal bir kod olsun. O halde, C kodunun sıfırdan farklı tüm kod sözcükleri minimaldir, eğer*

$$\frac{w_{\min}}{w_{\max}} > \frac{p-1}{p},$$

burada $w_{\min}$ ve $w_{\max}$ sırasıyla C kodunun sıfırdan farklı minimum ve maksimum ağırlıklarını belirtir.

Bu tezde elde edilen doğrusal kodlar Lemma 6.1'de verilen yeter koşula göre neredeyse tüm durumlar için minimal koddur. Aşağıdaki önermelerde, elde edilen kodların minimal kodlar olduğu gösterilmiştir.

Önerme 6.1 *Teorem 4.1'de verilen* $C_{D_\lambda} = [p^{2t-1} - p^{t-1}, 2t, (p^t - p^{t-1} - 2)p^{t-1}]$ *doğrusal kodu minimal koddur.*

İspat Çizelge 4.1'den $w_{min} = (p^t - p^{t-1} - 2)p^{t-1}$ ve $w_{max} = (p-1)p^{2t-2}$ olduğunu biliyoruz. $t \geq 2$ olduğu durumda;

$$\frac{w_{min}}{w_{max}} = \frac{(p^t - p^{t-1} - 2)p^{t-1}}{(p-1)p^{2t-2}} = 1 - \frac{2}{p^t - p^{t-1}} > \frac{p-1}{p}$$

eşitsizliğini elde ederiz. Lemma 6.1'e göre $t \geq 2$ için C_{D_λ} kodunun sıfırdan farklı tüm kod sözcükleri minimaldir. Böylece, C_{D_λ} minimal koddur.

Önerme 6.2 *Teorem 4.2'de verilen* $C_{D_{01}} = [2p^{2t-1} - 2p^{t-1}, 2t, p^{t-1}(2p^t - 2p^{t-1} - p + 1)]$ *doğrusal kodu minimal koddur.*

İspat Çizelge 4.2'den $w_{min} = p^{t-1}(2p^t - 2p^{t-1} - p + 1)$ ve $w_{max} = (p-1)2p^{2t-2}$ olduğunu biliyoruz. $t \geq 2$ olduğu durumda;

$$\frac{w_{min}}{w_{max}} = \frac{p^{t-1}(2p^t - 2p^{t-1} - p + 1)}{(p-1)2p^{2t-2}} = 1 - \frac{1}{2p^{t-1}} > \frac{p-1}{p}$$

eşitsizliğini elde ederiz. Lemma 6.1'e göre $t \geq 2$ için $C_{D_{01}}$ kodunun sıfırdan farklı tüm kod sözcükleri minimaldir. Böylece, $C_{D_{01}}$ minimal koddur.

Önerme 6.3 *Teorem 4.3'de verilen* $C_{D_{SQ}} = [2p^{2t-1} - 2p^{t-1}, 2t, p^{t-1}(2p^t - 2p^{t-1} - p + 1)]$ *doğrusal kodu minimal koddur.*

İspat Çizelge 4.3'den $w_{min} = \frac{(p-1)^2}{2}(p^{2t-2} - 2p^{t-1})$ ve $w_{max} = \frac{(p-1)^2}{2}p^{2t-2}$ olduğunu biliyoruz. $t > 2$ olduğu durumda;

$$\frac{w_{min}}{w_{max}} = \frac{\frac{(p-1)^2}{2}(p^{2t-2} - 2p^{t-1})}{\frac{(p-1)^2}{2}p^{2t-2}} = 1 - \frac{2}{p^{t-1}} > \frac{p-1}{p}$$

eşitsizliğini elde ederiz. Lemma 6.1'e göre $t > 2$ için $C_{D_{SQ}}$ kodunun sıfırdan farklı tüm kod sözcükleri minimaldir. Böylece, $C_{D_{SQ}}$ minimal koddur.

Önerme 6.4 *Teorem 5.1'de verilen* $C_{D_0} = [p^{2t-1}(p^t - 1), 3t, (p-1)(p^{3t-2} - 2p^{2t-2})]$ *doğrusal kodu minimal koddur.*

İspat Çizelge 5.1'den $w_{min} = (p-1)(p^{3t-2} - 2p^{2t-2})$ ve $w_{max} = (p-1)p^{3t-2}$ olduğunu biliyoruz. $t \geq 2$ olduğu durumda;

$$\frac{w_{min}}{w_{max}} = \frac{(p-1)(p^{3t-2} - 2p^{2t-2})}{(p-1)p^{3t-2}} = 1 - \frac{2}{p^t} > \frac{p-1}{p}$$

eşitsizliğini elde ederiz. Lemma 6.1'e göre $t \geq 2$ için C_{D_0} kodunun sıfırdan farklı tüm kod sözcükleri minimaldir. Böylece, C_{D_0} minimal koddur.

Yukarıda verilen Önerme 6.1, Önerme 6.2, Önerme 6.3 ve Önerme 6.4'de elde etiğimiz C_{D_λ}, $C_{D_{01}}$, $C_{D_{SQ}}$ ve C_{D_0} kodlarının minimal kodlar oldukları gösterilmiştir. Dolayısıyla, bu kodların dual kodları üzerinde tasarlanan sır paylaşım şemaları iyi erişim yapılarına sahiptir.

Aşağıdaki sonuçlarda, elde edilen minimal kodların dual kodlarının minimum Hamming mesafe değerleri verilmiştir.

Sonuç 6.1 *Teorem 4.1'de verilen C_{D_λ} kodu için dual Hamming mesafesi $d^\perp = 2$'dir. Böylece, dual kod $C_{D_\lambda}^\perp = [p^{2t-1} - p^{t-1}, p^{2t-1} - p^{t-1} - 2t, 2]$ parametreli bir doğrusal koddur.*

İspat C_{D_λ} kodunun parametreleri kullanılarak Pless güç momentinin ikinci denkleminden $A_1^\perp = 0$ ve üçüncü denkleminden $A_2^\perp > 0$ olduğu kolayca görülebilir. Dolayısıyla, $d^\perp = 2$'dir.

Sonuç 6.2 *Teorem 4.2'de verilen $C_{D_{01}}$ kodu için dual Hamming mesafesi $d^\perp = 2$'dir. Böylece, dual kod $C_{D_{01}}^\perp = [2p^{2t-1} - 2p^{t-1}, 2(p^{2t-1} - p^{t-1} - t), 2]$ parametreli bir doğrusal koddur.*

İspat $C_{D_{01}}$ kodunun parametreleri kullanılarak Pless güç momentinin ikinci denkleminden $A_1^\perp = 0$ ve üçüncü denkleminden $A_2^\perp > 0$ olduğu kolayca görülebilir. Dolayısıyla, $d^\perp = 2$'dir.

Sonuç 6.3 *Teorem 4.3'de verilen $C_{D_{SQ}}$ kodu için dual Hamming mesafesi $d^\perp = 2$'dir. Böylece, dual kod $C_{D_{SQ}}^\perp = [\frac{(p-1)}{2}(p^{2t-1} - p^{t-1}), \frac{(p-1)}{2}(p^{2t-1} - p^{t-1}) - 2t, 2]$ parametreli bir doğrusal koddur.*

İspat $C_{D_{SQ}}$ kodunun parametreleri kullanılarak Pless güç momentinin ikinci denkleminden $A_1^\perp = 0$ ve üçüncü denkleminden $A_2^\perp > 0$ olduğu kolayca görülebilir. Dolayısıyla, $d^\perp = 2$'dir.

Sonuç 6.4 *Teorem 5.1'de verilen C_{D_λ} kodu için dual Hamming mesafesi $d^\perp = 2$'dir. Böylece, dual kod $C_{D_0}^\perp = [p^{2t-1}(p^t - 1), p^{2t-1}(p^t - 1) - 3t, 2]$ parametreli bir doğrusal koddur.*

İspat C_{D_0} kodunun parametreleri kullanılarak Pless güç momentinin ikinci denkleminden $A_1^\perp = 0$ ve üçüncü denkleminden $A_2^\perp > 0$ olduğu kolayca görülebilir. Dolayısıyla, $d^\perp = 2$'dir.

Bu tezde elde edilen minimal kodların dual kodlarının minimum Hamming mesafe değerlerinin 2 olduğu gözlemlenmiştir. Örnek 4.1, Örnek 4.2, Örnek 4.3 ve Örnek 5.1'de verilen kodlar minimaldir ve bu kodların dual kodlarının minimum Hamming mesafeleri ikidir.

Aşağıdaki önermeye göre her bir minimal kodun dual kodlarından elde edilen sır paylaşım şemalarının erişim yapılarını tanımlayabiliriz. $C^{\perp}$ koduna dayalı bir sır paylaşım şemasındaki minimal erişim kümeleri ile C kodunun minimal kod sözcükleri arasında birebir bir ilişki vardır (Carlet vd., 2005; Massey, 1993).

Aşağıdaki önerme, minimal bir doğrusal kodun dual koduna dayalı bir sır paylaşım şemasının erişim yapısını açıklar.

Önerme 6.5 *(Ding ve Yuan, 2003; Yuan ve Ding, 2006)* C, $\mathbb{F}_p$ *cismi üzerinde* $[n, k, d]_p$ *parametreli bir minimal doğrusal kod olsun ve bu kodun üreteç matrisi* $G = [\mathbf{g}_0, \mathbf{g}_1, \ldots, \mathbf{g}_{n-1}]$ *olsun.* $C^{\perp}$ *dual kodundan elde edilen sır paylaşım şemasının katılımcı sayısı* $(n-1)$ *olup, minimal erişim kümelerinin sayısı* p^{k-1}*'dir.*

- $d^{\perp} = 2$ *durumunda:* $\mathbf{g}_i$, $1 \leq i \leq n-1$, $\mathbf{g}_0$*'ın bir katıysa,* P_i *katılımcısı tüm minimal erişim kümelerinde yer alır; değilse* $(p-1)p^{k-2}$ *tane minimal erişim kümesinde yer alır.*

- $d^{\perp} \geq 3$ *durumunda: sabit bir* $1 \leq l \leq \min\{k-1, d^{\perp}-2\}$ *için, her* l *katılımcı grubu,* $(p-1)^l p^{k-(l+1)}$ *tane minimal erişim kümesinde bulunur.*

Bu durumda, $d^{\perp} = 2$ ise bazı P_i'ler tüm minimal erişim kümelerinde yer almak zorundadır ve bu tür bir P_i, diktatör katılımcı olarak adlandırılır. Eğer $d^{\perp} \geq 3$ ise, her bir P_i aynı role sahiptir, çünkü P_i, $1 \leq i \leq n-1$ için aynı sayıda minimal erişim kümesine dahil olur. Bu tür sır paylaşım şeması demokratik olarak adlandırılır. Her iki durumda da sır paylaşım şemasının iyi bir erişim yapısı vardır.

Dolayısıyla, elde edilen kodların dual kodlarına dayalı sır paylaşım şemaları, Önerme 6.5'da açıklanan iyi erişim yapılarına sahiptir. Önerme 6.5'a göre, bu kodların dual kodlarına dayanan sır paylaşım şemalarının erişim yapıları tanımlanabilir. Böyle bir sır paylaşım şeması, katılımcılar grubunun tamamında bir diktatöre sahiptir. Örnek olarak, aşağıdaki sır paylaşım şemalarını açıklıyoruz.

Sonuç 6.5 $t \geq 2$ *olmak üzere Teorem 4.1'de verilen* $[p^{2t-1}-p^{t-1}, 2t, (p^t-p^{t-1}-2)p^{t-1}]_p$ *parametreli* C_λ *minimal kodunun üreteç matrisi* $G = [g_0, g_1, \ldots, g_{n-1}]$ *olsun. O zaman*

$d^{\perp} = 2$ olan $C_{\lambda}^{\perp}$ dual koduna dayanan sır paylaşım şemasında, katılımcı sayısı $p^{2t-1} - p^{t-1} - 1$ ve minimal erişim kümelerinin sayısı p^{2t-1}'dir. Ayrıca eğer g_i, $i \neq 0$, g_0'ın bir katı ise, P_i tüm minimal erişim kümelerinde yer almalıdır; aksi takdirde P_i katılımcısı, $(p-1)p^{2t-2}$ tane minimal erişim kümesinde yer almalıdır.

Sonuç 6.6 *$t \geq 2$ olmak üzere Teorem 4.2'de verilen*

$$[2p^{2t-1} - 2p^{t-1}, 2t, (2p^t - 2p^{t-1} - p + 1)p^{t-1}]_p$$

parametreli $C_{D_{01}}$ minimal kodunun üreteç matrisi $G = [g_0, g_1, \ldots, g_{n-1}]$ olsun. O zaman, $d^{\perp} = 2$ olan $C_{D_{01}}^{\perp}$ dual koduna dayanan sır paylaşım şemasında, katılımcı sayısı $2p^{2t-1} - 2p^{t-1} - 1$ ve minimal erişim kümelerinin sayısı p^{2t-1}'dir. Ayrıca eğer g_i, $i \neq 0$, g_0'ın bir katı ise, P_i tüm minimal erişim kümelerinde yer almalıdır; aksi takdirde P_i katılımcısı, $(p-1)p^{2t-2}$ tane minimal erişim kümesinde yer almalıdır.

Sonuç 6.7 *$t > 2$ olmak üzere Teorem 4.3'de verilen*

$$[\frac{p-1}{2}(p^{2t-1} - p^{t-1}), 2t, \frac{p-1}{2}(p^t - p^{t-1} - 2)p^{t-1}]_p$$

parametreli $C_{D_{SQ}}$ minimal kodunun üreteç matrisi $G = [g_0, g_1, \ldots, g_{n-1}]$ olsun. O zaman, $d^{\perp} = 2$ olan $C_{D_{SQ}}^{\perp}$ dual koduna dayanan sır paylaşım şemasında, katılımcı sayısı $\frac{p-1}{2}(p^{2t-1} - p^{t-1}) - 1$ ve minimal erişim kümelerinin sayısı p^{2t-1}'dir. Ayrıca eğer g_i, $i \neq 0$, g_0'ın bir katı ise, P_i tüm minimal erişim kümelerinde yer almalıdır; aksi takdirde P_i katılımcısı, $(p-1)p^{2t-2}$ tane minimal erişim kümesinde yer almalıdır.

Sonuç 6.8 *$t \geq 2$ için Teorem 5.1'de verilen $[p^{2t-1}(p^{t-1}), 3t, (p-1)(p^{3t-2} - 2p^{2t-2})]_p$ parametreli C_{D_0} minimal kodunun üreteç matrisi $G = [g_0, g_1, \ldots, g_{n-1}]$ olsun. O zaman, $d^{\perp} = 2$ olan $C_{D_0}^{p}erp$ dual koduna dayanan sır paylaşım şemasında, katılımcı sayısı $p^{2t-1}(p^{t-1}) - 1$ ve minimal erişim kümelerinin sayısı p^{3t-1}'dir. Ayrıca eğer g_i, $i \neq 0$, g_0'ın bir katı ise, P_i tüm minimal erişim kümelerinde yer almalıdır; aksi takdirde P_i katılımcısı, $(p-1)p^{3t-2}$ tane minimal erişim kümesinde yer almalıdır.*

7. SONUÇ VE ÖNERİLER

7.1. Sonuçlar

Bu tez çalışmasında, literatürde mevcut olan (Zhu ve Liao, 2023) ve (Cheng vd., 2022) çalışmaları incelenerek düşük ağırlıklı yeni minimal doğrusal kod aileleri elde edilmiştir. İlk olarak, (Zhu ve Liao, 2023) çalışmasında önerilen doğrusal kod inşa yönteminde yeni tanım kümeleri D_λ, D_{01} ve D_{SQ} kullanılarak yeni doğrusal kodlar elde edilmiştir. Daha sonra, (Cheng vd., 2022) çalışmasındaki doğrusal kod inşa yöntemi ile (Zhu ve Liao, 2023) çalışmasındaki inşa yöntemi birleştirilerek yeni bir inşa yöntemi geliştirilmiş ve bu inşa yönteminde D_0 kümesi kullanılarak dört ağırlıklı yeni doğrusal C_{D_0} kodu elde edilmiştir. Elde edilen kodların, parametreleri, Hamming ağırlıkları ve ağırlık dağılımları hesaplanmıştır. Ayrıca, elde edilen tüm kodların minimal kodlar oldukları gözlemlenmiştir. Ek olarak, elde edilen kodların dual kodlarının minimum Hamming mesafelerinin 2 olduğu gözlemlenmiştir. Son olarak, elde edilen minimal kodların dual kodlarından tasarlanan sır paylaşım şemalarının minimal erişim yapıları verilmiştir.

Tezde elde edilen sonuçlar aşağıda listelenmiştir.

- Bölüm 4'te (Zhu ve Liao, 2023) çalışmasında önerilen inşa yöntemiyle
  - Teorem 4.1'de iki ağırlıklı C_{D_λ} doğrusal kod ailesi üretilmiştir,
  - Teorem 4.2'de yeni üç ağırlıklı $C_{D_{01}}$ doğrusal kod ailesi üretilmiştir,
  - Teorem 4.3'de yeni iki ağırlıklı $C_{D_{SQ}}$ doğrusal kod ailesi üretilmiştir.
- Bölüm 5'te yeni inşa yöntemi önerilerek Teorem 5.1'de yeni dört ağırlıklı C_{D_0} doğrusal kod ailesi üretilmiştir.
- Bölüm 6'da Teorem 4.1, 4.2, 4.3 ve 5.1'da elde edilen kodların minimal kodlar oldukları gösterilmiştir ve bu kodların dual kodlarının Hamming mesafelerinin 2 olduğu gözlemlenmiştir. Böylece, bu tezde elde edilen minimal kodların dual kodlarından tasarlanan sır paylaşım şemalarının erişim yapıları verilmiştir.

Sonuç olarak, bu tezde farklı kümeler ve yeni yöntem kullanılarak yeni minimal doğrusal kodlar elde edilmiştir ve bu kodların sır paylaşım şemalarındaki uygulaması sunulmuştur.

7.2. Öneriler

Bu çalışmanın sonuçları, kodlama teorisinde düşük ağırlıklı minimal doğrusal kodların tasarımına ve bu kodların sır paylaşım şemaları üzerindeki uygulamalarına katkı sağlamaktadır. Dolayısıyla, bu tez çalışması hem kodlama teorisi hem de kriptografi alanlarına katkı sağlamaktadır.

İleriki çalışmalar, bu kodların farklı sınıflarının daha geniş uygulama alanlarını keşfetmeye ve yeni kombinatorik yapıların oluşturulmasına odaklanabilir. Ayrıca, bu doğrusal kodların performansını ve verimliliğini artırmak için daha ileri algoritmik tekniklerin geliştirilmesi araştırma alanını zenginleştirecektir. Bu doğrusal kodları daha geniş bir güvenlik ve iletişim teknolojileri yelpazesinde kullanılarak yeni yapısal keşifler yapılabilir.

KAYNAKLAR

Anderson, R., Ding, C., Helleseth, T., ve Klove, T. (1998). How to build robust shared control systems. *Designs, Codes and Cryptography*, 15(2):111–124.

Ashikhmin, A. ve Barg, A. (1998). Minimal vectors in linear codes. *IEEE Transactions on Information Theory*, 44(5):2010–2017.

Ashikhmin, A., Barg, A., Cohen, G., ve Huguet, L. (1995). Variations on minimal codewords in linear codes. *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, s. 96–105.

Blakley, G. R. ve others (1979). Safeguarding cryptographic keys. In *Proceedings of the national computer conference*, volume 48, s. 313–317.

Bosma, W., Cannon, J., ve Playoust, C. (1997). The magma algebra system i: The user language. *Journal of Symbolic Computation*, 24(3-4):235–265.

Budaghyan, L. (2015). *Construction and Analysis of Cryptographic Functions*. Springer.

Carlet, C. (2010a). Boolean functions for cryptography and error correcting codes. *Boolean models and methods in mathematics, computer science, and engineering*, 2:257–397.

Carlet, C. (2010b). Vectorial boolean functions for cryptography. *Boolean models and methods in mathematics, computer science, and engineering*, 134:398–469.

Carlet, C., Ding, C., ve Yuan, J. (2005). Linear codes from perfect nonlinear mappings and their secret sharing schemes. *IEEE Transactions on Information Theory*, 51(6):2089–2102.

Cheng, X., Cao, X., ve Qian, L. (2022). Constructing few-weight linear codes and strongly regular graphs. *Discrete Mathematics*, 345(12):113101.

Ding, C. (2015). Linear codes from some 2-designs. *IEEE Transactions on information*

theory, 61(6):3265–3275.

Ding, C. (2016). A construction of binary linear codes from boolean functions. *Discrete mathematics*, 339(9):2288–2303.

Ding, C. ve Niederreiter, H. (2007). Cyclotomic linear codes of order 3. *IEEE Transactions on information theory*, 53(6):2274–2277.

Ding, C. ve Wang, X. (2005). A coding theory construction of new systematic authentication codes. *Theoretical computer science*, 330(1):81–99.

Ding, C. ve Yuan, J. (2003). Covering and secret sharing with linear codes. *DMTCS*, 2731:11–25.

Ding, K. ve Ding, C. (2015). A class of two-weight and three-weight codes and their applications in secret sharing. *IEEE Transactions on Information Theory*, 61(11):5835–5842.

Huffman, W. C. ve Pless, V. (2010). *Fundamentals of error-correcting codes*. Cambridge university press.

Li, C., Li, N., Helleseth, T., ve Ding, C. (2014). The weight distributions of several classes of cyclic codes from apn monomials. *IEEE transactions on information theory*, 60(8):4710–4721.

Li, C., Yue, Q., ve Fu, F.-W. (2017). A construction of several classes of two-weight and three-weight linear codes. *Applicable Algebra in Engineering, Communication and Computing*, 28:11–30.

Lidl, R. ve Niederreiter, H. (1997). *Finite fields*. Number 20. Cambridge university press.

Massey, J. L. (1993). Minimal codewords and secret sharing. In *Proceedings of the 6th joint Swedish-Russian international workshop on information theory*, s. 276–279.

Massey, J. L. (1995). Some applications of coding theory in cryptography. *Codes and*

Ciphers: Cryptography and Coding IV, s. 33–47.

McEliece, R. J. ve Sarwate, D. V. (1981). On sharing secrets and reed-solomon codes. *Communications of the ACM*, 24(9):583–584.

Mesnager, S. (2016). *Bent functions*. Springer.

Mesnager, S. (2017). Linear codes with few weights from weakly regular bent functions based on a generic construction. *Cryptography and Communications*, 9(1):71–84.

Mesnager, S. ve Sınak, A. (2020). Infinite classes of six-weight linear codes derived from weakly regular plateaued functions. In *2020 International Conference on Information Security and Cryptology (ISCTURKEY)*, s. 93–100. IEEE.

Mesnager, S. ve Sınak, A. (2020). Several classes of minimal linear codes with few weights from weakly regular plateaued functions. *IEEE Transactions on Information Theory*, 66(4):2296–2310.

Mesnager, S., Sınak, A., ve Yayla, O. (2019a). Minimal linear codes with few weights and their secret sharing. *International Journal of Information Security Science*, 8(4):77–87.

Mesnager, S., Özbudak, F., ve Sınak, A. (2019b). Linear codes from weakly regular plateaued functions and their secret sharing schemes. *Design Codes and Cryptograph*, s. 463–480.

Mullen, G. L. ve Panario, D. (2013). *Handbook of finite fields*. CRC Press.

Schoenmakers, B. (1999). A simple publicly verifiable secret sharing scheme and its application to electronic voting. In *Annual International Cryptology Conference*, s. 148–164. Springer.

Shamir, A. (1979). How to share a secret. *Communications of the ACM*, 22(11):612–613.

Shannon, C. E. (1948). A mathematical theory of communication. *The Bell system*

technical journal, 27(3):379–423.

Sınak, A. (2021a). Minimal linear codes from weakly regular plateaued balanced functions. *Discrete Mathematics*, 344(3):112215.

Sınak, A. (2021b). Minimal linear codes with six-weights based on weakly regular plateaued balanced functions. *International Journal of Information Security Science*, 10(3):86–98.

Sınak, A. (2017). Contributions on plateaued (vectorial) functions for symmetric cryptography and coding theory.

Sınak, A. (2022). Construction of minimal linear codes with few weights from weakly regular plateaued functions. *Turkish Journal of Mathematics*, 46(3):953–972.

Tang, C., Li, N., Qi, Y., Zhou, Z., ve Helleseth, T. (2016). Linear codes with two or three weights from weakly regular bent functions. *IEEE Transactions on Information Theory*, 62(3):1166–1176.

Wu, Y., Li, N., ve Zeng, X. (2020). Linear codes with few weights from cyclotomic classes and weakly regular bent functions. *Designs, Codes and Cryptography*, 88:1255–1272.

Yuan, J. ve Ding, C. (2006). Secret sharing schemes from three classes of linear codes. *IEEE Transactions on Information Theory*, 52(1):206–212.

Zhou, Z., Li, N., Fan, C., ve Helleseth, T. (2016). Linear codes with two or three weights from quadratic bent functions. *Designs, Codes and Cryptography*, 81(2):283–295.

Zhu, C. ve Liao, Q. (2023). Two new classes of projective two-weight linear codes. *Finite Fields and Their Applications*, 88:102186.