

TÜRKİYE CUMHURİYETİ
YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

SABİT DEVİRLİ KODLARDAN MAKSİMUM UZAKLIĞA
AYRIŞABİLEN KUANTUM KODLARIN İNŞASI

Mustafa SARI

DOKTORA TEZİ
Matematik Anabilim Dalı
Matematik Programı

Danışman
Doç. Dr. Emre KOLOTOĞLU

Temmuz, 2019

TÜRKİYE CUMHURİYETİ
YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

SABİT DEVİRLİ KODLARDAN MAKSİMUM UZAKLIĞA AYRIŞABİLEN
KUANTUM KODLARIN İNŞASI

Mustafa SARI tarafından hazırlanan tez çalışması 12.07.2019 tarihinde aşağıdaki jüri tarafından Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalı Matematik Programı **DOKTORA TEZİ** olarak kabul edilmiştir.

Doç. Dr. Emre KOLOTOĞLU
Yıldız Teknik Üniversitesi
Danışman

Jüri Üyeleri

Doç. Dr. Emre KOLOTOĞLU, Danışman
Yıldız Teknik Üniversitesi

Prof. Dr. Mehmet ÖZEN, Üye
Sakarya Üniversitesi

Doç. Dr. Murat ALAN, Üye
Yıldız Teknik Üniversitesi

Doç. Dr. Fatih DEMİRKALE, Üye
Yıldız Teknik Üniversitesi

Doç. Dr. Esra ŞENGELİN SEVİM, Üye
İstanbul Bilgi Üniversitesi

Danışmanım Doç. Dr. Emre KOLOTOĞLU sorumluluğunda tarafımca hazırlanan Sabit Devirli Kodlardan Maksimum Uzaklığa Ayrışabilen Kuantum Kodların İnşası başlıklı çalışmada veri toplama ve veri kullanımında gerekli yasal izinleri aldığımı, diğer kaynaklardan aldığım bilgileri ana metin ve referanslarda eksiksiz gösterdiğimi, araştırma verilerine ve sonuçlarına ilişkin çarpıtma ve/veya sahtecilik yapmadığımı, çalışmam süresince bilimsel araştırma ve etik ilkelerine uygun davrandığımı beyan ederim. Beyanımın aksinin ispatı halinde her türlü yasal sonucu kabul ederim.

Mustafa SARI

İmza



Bu tez çalışması, TÜBİTAK BİDEB 2211 Yurt İçi Doktora Burs Programı ile desteklenmiştir.

TEŞEKKÜR

Değerli bilimsel katkılarından ve özverili desteklerinden dolayı tez danışmanım Sayın Doç. Dr. Emre KOLOTOĞU'na teşekkürlerimi sunarım. Yapıcı desteklerinden dolayı tez izleme komitesi üyeleri Sayın Prof. Dr. Mehmet ÖZEN ve Sayın Doç. Dr. Murat ALAN hocalarıma ve tez jüri komitesi üyeleri Sayın Doç. Dr. Fatih DEMİRKALE ve Sayın Doç. Dr. Esra Şengelen SEVİM hocalarıma teşekkür ederim.

Doktora tez sürecinde yardımını hiçbir zaman esirgemeyen Arş. Gör. Dr. Mehmet Emin KÖROĞLU'na teşekkür ederim.

Sadece doktora tez çalışması boyunca değil hayatım boyunca maddi ve manevi desteklerini devamlı hissettiğim aileme can-ı gönülden teşekkür ederim.

Mustafa SARI

İÇİNDEKİLER

SİMGE LİSTESİ	viii
KISALTMA LİSTESİ	x
TABLO LİSTESİ	xi
ÖZET	xii
ABSTRACT	xiv
1 Giriş	1
1.1 Literatür Özeti	1
1.2 Tezin Amacı	3
1.3 Hipotez	3
2 Temel Bilgiler	4
2.1 Lineer Kodlar	5
2.2 Sabit Devirli Kodlar	7
2.3 Kuantum Kodlar	8
2.3.1 Kuantum Bitler ve Kuantum Hatalar	9
2.3.2 Stabilizer Kuantum Kodlar	11
2.3.3 Dolaşık Destekli Kuantum Kodlar	14
3 Geliştirilmiş Minimum Uzaklıklı Kuantum Kodlar	16
3.1 Kuantum MDS Kodların Bir Sınıfının İnşası	16
3.2 İyileştirilmiş Parametrelere Sahip Kuantum Kodlar	19
4 $\frac{q^2+1}{13}$ ve $\frac{q^2+1}{17}$ Uzunluklu Kuantum MDS Kodlar	21
4.1 $\frac{q^2+1}{13}$ Uzunluklu Kuantum MDS Kodlar	21
4.2 $\frac{q^2+1}{17}$ Uzunluklu Kuantum MDS Kodlar	24
5 Dolaşık Destekli Kuantum MDS Kodların İnşası	27
5.1 $q^2 + 1$ Uzunluklu Dolaşık Destekli Kuantum MDS Kodlar	27
5.2 $\frac{q^2-1}{4}$ Uzunluklu Dolaşık Destekli Kuantum MDS Kodlar	32

5.3 Kıyaslama	37
6 Sonuç ve Öneriler	38
Referanslar	39
Tezden Üretilmiş Yayınlar	42



SİMGE LİSTESİ

$\mathbb{F}_q$	q elemanlı sonlu cisim
$\mathbb{F}_{q^2}$	q^2 elemanlı sonlu cisim
$\mathbb{F}_q^n$	Bileşenleri $\mathbb{F}_q$ cisminden olan n -li vektörlerin kümesi
$\times$	Kartezyen çarpım
$[n, k]_q$	$\mathbb{F}_q$ üzerinde n uzunluğunda k boyutlu bir lineer kod
$[n, k, d]_q$	$\mathbb{F}_q$ üzerinde n uzunluğunda k boyutlu d minimum uzaklığına sahip bir lineer kod
$w_h(x)$	x vektörünün Hamming ağırlığı
$\langle x, y \rangle$	x ile y vektörlerinin Öklid iç çarpımı
$\langle x, y \rangle_h$	x ile y vektörlerinin Hermit iç çarpımı
$C^\perp$	C kodun Öklid iç çarpımına göre dual kodu
$C^{\perp_h}$	C kodun Hermit iç çarpımına göre dual kodu
$\mathbb{F}_q^\times$	$\mathbb{F}_q \setminus \{0\}$
$ \cdot\rangle$	Sütun vektör
$\mathbb{C}^q$	q boyutlu kompleks vektör uzayı
$\mathbb{C}^{q^n}$	q^n boyutlu kompleks vektör uzayı
$\otimes$	Tensör çarpım
$\lfloor x \rfloor$	x 'ten küçük en büyük tamsayı
$((n, M))_q$	$\mathbb{C}^{q^n}$ kompleks vektör uzayının M boyutlu alt vektör uzayı
$((n, M, d))_q$	$\mathbb{C}^{q^n}$ kompleks vektör uzayının d minimum uzaklıklı M boyutlu alt vektör uzayı
$\llbracket n, k, d \rrbracket_q$	$\mathbb{F}_q$ üzerinde n uzunluğunda k boyutlu d minimum uzaklığına sahip bir kuantum kod
$\llbracket n, k, d; c \rrbracket_q$	$\mathbb{F}_q$ üzerinde c dolaşık haldeki kuantum durumunu kullanarak k kubiti n kubite kodlayan d minimum uzaklıklı bir kuantum kod

G_n	n kubit üzerinde hata grubu
$Z(G_n)$	G_n grubunun merkezi
$SZ(G_n)$	S ve $Z(G_n)$ ile üretilen grup
$C_{G_n}(S)$	S alt grubunun G_n grubundaki merkezleyeni
$\langle x, y \rangle_s$	x ile y vektörlerinin iz-simplektik iç çarpımı
$swt(x)$	x vektörünün simplektik ağırlığı
$\langle x, y \rangle_a$	x ile y vektörlerinin iz-alternatif iç çarpımı
$C^{\perp_s}$	C kodun iz-simplektik iç çarpımına göre dual kodu
$C^{\perp_a}$	C kodun iz-alternatif iç çarpımına göre dual kodu
$C_{q,n}(i)$	$\text{mod } n$ 'ye göre i yi içeren q -devirsel koset
$C_{q^2,n}(i)$	$\text{mod } n$ 'ye göre i yi içeren q^2 -devirsel koset
$H^\dagger$	H matrisinin eşlenik transpozesi
$o_{rn}(q^2)$	q^2 'nin $\text{mod } rn$ 'ye göre çarpımsal mertebesi

KISALTMA LİSTESİ

BCH	Bose, Chaudhri ve Hocquenghem
bkz	Bakınız
CSS	Calderbank, Shor ve Steane
IEEE	The Institute of Electrical and Electronics Engineers
MDS	Maksimum Uzaklığa Ayırışabilen

TABLO LİSTESİ

Tablo 3.1	[41]'de elde edilen kuantum kodlar ile bir kıyaslama	20
Tablo 3.2	[41]'deki inşa ile elde edilemeyen kuantum kodların bazıları	20
Tablo 4.1	Teorem 4.4 ile elde edilen bazı kuantum MDS kodların parametreleri	24
Tablo 4.2	Teorem 4.7 ile elde edilen bazı kuantum MDS kodların parametreleri	26
Tablo 5.1	Teorem 5.3 ile elde edilen bazı dolaşık destekli kuantum MDS kodların parametreleri	29
Tablo 5.2	Teorem 5.4 ile elde edilen bazı dolaşık destekli kuantum MDS kodların parametreleri	32
Tablo 5.3	Teorem 5.7 ile elde edilen bazı dolaşık destekli kuantum MDS kodların parametreleri	34
Tablo 5.4	Teorem 5.9 ile elde edilen bazı dolaşık destekli kuantum MDS kodların parametreleri	36
Tablo 5.5	[13]'te elde edilen kuantum MDS kodlar ile Bölüm 5.2'de elde edilen dolaşık destekli kuantum MDS kodların bir kıyaslaması	37
Tablo 5.6	[24]'te ve Bölüm 5.2'de elde edilen dolaşık destekli kuantum MDS kodların bir kıyaslaması	37

Sabit Devirli Kodlardan Maksimum Uzaklığa Ayrışabilen Kuantum Kodların İnşası

Mustafa SARI

Matematik Anabilim Dalı
Doktora Tezi

Danışman: Doç. Dr. Emre KOLOTOĞLU

Kuantum mekaniğinin klasik mekaniğe teorik olarak üstünlüğü kuantum hesaplama ve iletişim üzerine çalışmaları yoğunlaştırmıştır. Fakat bu durum iyi kuantum hata düzelten kodların inşası problemini ortaya çıkarmıştır. Bu tez çalışmasında lineer kodların bir sınıfı olan sabit devirli kodlardan iyi parametrelere sahip kuantum kodlar elde edilmiştir.

Bölüm 1’de literatür özeti, tezin amacı ve hipoteze yer verilmiştir.

Bölüm 2’de sonraki bölümlerde ihtiyaç duyulan lineer kodlar, sabit devirli kodlar ve kuantum kodlar hakkında temel tanım ve sonuçlar verilmiştir.

Bölüm 3’te literatürde var olan kuantum kodların parametreleri iyileştirilmiş ve maksimum uzaklığa ayrışabilen kuantum kodların bir sınıfı için farklı bir inşası verilmiştir.

Bölüm 4’te q tek asal kuvveti olmak üzere sabit devirli kodlardan $\frac{q^2+1}{13}$ ve $\frac{q^2+1}{17}$ uzunluklu maksimum uzaklığa ayrışabilen kuantum kodlar elde edilmiştir.

Bölüm 5’te $q \equiv 3 \pmod{4}$ olmak üzere $q^2 + 1$ ve $\frac{q^2-1}{4}$ uzunluklu maksimum uzaklığa ayrışabilen dolanıklık destekli kuantum kodlar elde edilmiştir. Ayrıca, elde edilen $\frac{q^2-1}{4}$ uzunluklu maksimum uzaklığa ayrışabilen dolaşık destekli kuantum kodların literatürde var olanlardan daha iyi parametrelere sahip olduğu gösterilmiştir.

Bölüm 6’da sonuç ve önerilere yer verilmiştir.

Anahtar Kelimeler: Sabit devirli kod, tanımlayıcı küme, kuantum MDS kod, dolaşık destekli kuantum MDS kod



The Construction of Quantum Maximum Distance Separable Codes from Constacyclic Codes

Mustafa SARI

Department of Mathematics

Doctor of Philosophy Thesis

Advisor: Assoc. Prof. Dr. Emre KOLOTOĞLU

Theoretical superiorities of quantum mechanics to classical mechanics have increased the studies on quantum computation and communication. However, this has led to the problem of construction of efficient quantum error correcting codes. In this thesis, efficient quantum codes from constacyclic codes which are a class of linear codes are constructed.

In Section 1, the literature summary, the purpose of the thesis and the hypothesis are given.

In Section 2, fundamental definitions and results about linear codes, constacyclic codes and quantum codes that are needed in the following sections are given.

In Section 3, the parameters of quantum codes existing in the literature are improved and a different construction for a class of maximum distance separable quantum codes is presented.

In Section 4, maximum distance separable quantum codes of length $\frac{q^2+1}{13}$ and $\frac{q^2+1}{17}$, for odd prime power q , from constacyclic codes are constructed.

In Section 5, for odd prime power q satisfying $q \equiv 3 \pmod{4}$, entanglement assisted maximum distance separable quantum codes of length $q^2 + 1$ ve $\frac{q^2-1}{4}$ are obtained. Moreover, it is proved that entanglement assisted maximum distance separable quantum codes of length $\frac{q^2-1}{4}$ which are constructed in this section have better parameters than the ones existing in the literature.

In Section 6, the findings in this thesis and some recommendations for future studies are given.

Keywords: Constacyclic code, defining set, quantum MDS code, entanglement-assisted quantum MDS code



1.1 Literatür Özeti

İlk kuantum hata düzelten kod P. W. Shor tarafından bulunmuştur [1]. Calderbank ve arkadaşlarının dört elemanlı sonlu cisim ($\mathbb{F}_4$) üzerindeki toplamsal (additive) kodlardan ikili (binary) kuantum kod elde eden makalesinin [2] ardından kuantum hata düzelten kodlar üzerine çalışmalar giderek yoğunlaşmıştır. Bu çalışmaya göre ikili kuantum hata düzelten kod bulma problemi $\mathbb{F}_4$ üzerinde belli bir iç çarpıma göre dualini içeren toplamsal kod bulmaya dönüştürülmüştür. Andrew M. Steane, [2] çalışmasında verilen kuantum kod inşasını geliştirmiş ve yeni ikili kuantum kodlar elde etmiştir [3]. Daniel Gottesman bir kuantum kodu ikili kubitler üzerindeki Pauli matris grubunun değişmeli bir altgrubunun sabit bıraktığı kompleks vektör uzayı olarak tanımlamış ve bu alt grubun cebirsel yapısından yararlanarak kuantum hataları sınıflandırmıştır [4]. Alexei Ashikhmin ve Emanuel Knill, ikili olmayan kuantum kodları tanımlamış ve bu kuantum kodların nasıl elde edileceğini göstermişlerdir [5]. Avanti Ketkar ve arkadaşları, $\mathbb{F}_q$ üzerinde Pauli matrislerini tanımlamış ve ikili olmayan kuantum kod bulma işini önce $\mathbb{F}_q$ üzerinde iz-simplektik (trace-symplectic) iç çarpımına göre dualini içeren toplamsal kod bulmaya sonra da $\mathbb{F}_{q^2}$ üzerinde iz-alternatif (trace-alternating) iç çarpımına göre dualini içeren toplamsal kod bulmaya dönüştürmüştür [6]. Ayrıca, $\mathbb{F}_{q^2}$ üzerindeki lineer kodların Hermit iç çarpımına göre duali ile iz-alternatif (trace-alternating) iç çarpımına göre dualininin aynı olduğu gösterilmiştir [6]. Bu ise $\mathbb{F}_{q^2}$ üzerindeki lineer kod ailelerinin Hermit iç çarpımına göre dualini (Hermityen dualini) içerme koşullarının çalışılmasını gerektirmiştir. Salah Aly ve arkadaşları, $\mathbb{F}_{q^2}$ üzerindeki BCH kodların Hermityen duallerini içerme şartlarını araştırmış ve bu kodlardan elde edilen kuantum kodların parametrelerini belirlemiştir [7].

Lineer kodlar için verilen Singleton sınırı kuantum kodlar için de belirlenmiştir. Kuantum Singleton sınırını sağlayan bir kuantum koda maksimum uzaklığa ayrışabilen (MDS) kuantum kod denir [6]. $\mathbb{F}_{q^2}$ üzerindeki lineer kodların Hermityen dualinden kuantum MDS kodların inşası üzerine yoğun bir şekilde çalışılmaktadır

[8–21]. Lingfei Jin ve arkadaşları, genelleştirilmiş Reed-Solomon (GRS) kodların Hermityen duallerini içirme durumlarını incelemiş ve kuantum MDS kodların bazı sınıflarını elde etmiştir [8]. La Guardia, $q = 2^t$ olmak üzere $\mathbb{F}_{q^2}$ üzerindeki devirli kodlardan $[[q^2 + 1, q^2 - 2d + 3, d]]_q$, $3 \leq d \leq q + 1$ parametrelerine sahip kuantum MDS kodları inşa etmiştir [9]. Xiaoshan Kai ve Shixin Zhu, $\mathbb{F}_{q^2}$ üzerindeki nega-devirli kodların tanımlayıcı kümelerinden yararlanarak $q \equiv 1 \pmod{4}$ denliğini sağlayan tek asal kuvveti q için $[[q^2 + 1, q^2 - 2d + 3, d]]_q$, $2 \leq d(\text{çift}) \leq q + 1$ ve $[[\frac{(q^2 + 1)}{2}, \frac{(q^2 + 1)}{2} - 2d + 2, d]]_q$, $3 \leq d \leq q$ kuantum MDS kodlarını elde etmiştir [10]. Xiaoshan Kai ve arkadaşları, sabit devirli kodlardan Hermityen inşası ile kuantum MDS kodların bazı sınıflarının parametrelerini ortaya koymuştur [11]. Lingfei Jin ve Chaoping Xing, GRS kodlardan Hermityen inşası ile minimum uzaklığı en az $q/2 + 1$ olan kuantum MDS kodları elde etmiştir [12]. Weijun Fang ve Fang-Wei Fu, kuantum MDS kodların iki yeni ailesini inşa etmiştir [20].

Kuantum kodların önemli sınıflarından bir tanesi dolaşık destekli (entanglement assisted) kuantum kodlardır. İlk olarak Todd Brun ve arkadaşları tarafından sunulan bu kuantum kod ailesi, gönderici ile alıcı arasında önceden paylaşılan belli sayıdaki (c sayısı) dolaşık haldeki kuantum durumunu kullanarak daha fazla kuantum hata düzeltmeyi amaçlar [22]. Dolaşık destekli kuantum kodlar için de Singleton sınırı belirlenmiştir [22]. Bu sınırı sağlayan dolaşık destekli yeni kuantum kodların (kuantum MDS kod) inşası ayrı bir problemdir [23–29]. Lineer kodlardan dolaşık destekli kuantum kodlar elde edilmesinde dualini içirme şartı aranmadığından bu durum tüm lineer kodların bir kuantum koda dönüştürülebilmesine imkan tanımıştır [22]. Fakat lineer kodlardan elde edilen dolaşık destekli kuantum kodlar için c sayısını belirlemek kolay değildir. Bir $[n, k, d]_q$ lineer koddan $c = \text{rank}(HH^\dagger)$ olmak üzere $[[n, 2k - n + c, d; c]]_q$ parametrelerine sahip dolaşık destekli kuantum kodun inşası gösterilmiştir [30]. Rui-Hu Liu ve arkadaşları, devirli kodların tanımlayıcı kümeleri için bir ayrışım tanımlayarak c sayısını belirlemiş ve bazı dolaşık destekli kuantum kodlar elde etmiştir [31]. Jianzhang Chen ve arkadaşları devirli kodlar tanımlayıcı kümeleri için verilen ayrışım tanımını nega-devirli kodların tanımlayıcı kümelerine taşımış ve minimum uzaklıkları en az $q + 1$ olan dolaşık destekli kuantum MDS kodların yeni sınıflarını inşa etmiştir. Yang Liu ve arkadaşları, bu tanımlayıcı kümeleri için vermiş ve minimum uzaklığı en az $q + 1$ olan $\frac{q^2 - 1}{r}$, $r = 3, 4, 5, 6, 7$ uzunluklu dolaşık destekli kuantum MDS kodların inşasını vermiştir [23].

1.2 Tezin Amacı

Bu tezde, sonlu cisimler üzerindeki sabit devirli kodların tanımlayıcı kümeleri üzerine çalışarak literatürde var olan kuantum kodların parametreleri iyileştirilecek, kuantum MDS kodların bir sınıfı için yeni bir inşa verilecek ve yeni dolaşık destekli kuantum MDS kodlar elde edilecektir.

1.3 Hipotez

Sabit devirli kodların zengin cebirsel yapıya sahip olmaları bu kod ailesi ile dualleri arasındaki ilişkinin belirlenmesini kolaylaştırdığı gibi kuantum MDS kodların ve dolaşık destekli kuantum MDS kodların inşasına da imkan tanımaktadır.



2 Temel Bilgiler

Bu bölümde sonlu cisimler üzerinde tanımlı lineer kodlar, sabit devirli kodlar, kuantum kodlar ve dolaşık destekli kuantum kodlar hakkında temel bilgiler verilecektir. Aksi belirtilmediği sürece $\mathbb{F}_q$, q elemanlı sonlu bir cisim ve $\mathbb{F}_q^n$, bileşenleri $\mathbb{F}_q$ sonlu cisminden olan n -li vektörlerin kümesidir.

Dijital ortamda bilgi birimi 0 ve 1 bitleridir. Bilgi ise bitlerin bir dizisinden oluşur. Bilginin iletilmesi esnasında bit veya bitlerde meydana gelen değişikliğe hata denir. İletişim kanalında bilginin iletilmesi sırasında oluşabilecek hataları farkedene ve düzelten yapıların inşası iletişim teorisinde önemli bir problemdir [32]. Bu problemin çözümü için geliştirilen matematiksel yapılara kod denir. Genel olarak kod tanımı aşağıdaki gibidir.

$A = \{a_1, a_2, \dots, a_q\}$, q elemanlı bir küme ve $A^n = \underbrace{A \times \dots \times A}_{n \text{ defa}}$ olsun. A üzerinde n uzunluğunda bir kod, A^n kümesinin boştan farklı bir alt kümesidir. A 'ya kod alfabesi, A^n kümesinin bir elemanına A üzerinde n uzunluğunda bir söz ve kodun elemanlarına da kodsözler denir [33].

C. E. Shannon (bkz. [32]) tarafından ortaya konulan yukarıdaki problemin ilk sistematik çözümü R. W. Hamming tarafından verilmiştir [34]. R. W. Hamming tarafından tanımlanan Hamming kod, bir $x_1x_2x_3x_4$ dizisini

$$x_1 + x_3 + x_5 + x_7 \equiv 0 \pmod{2}$$

$$x_2 + x_3 + x_6 + x_7 \equiv 0 \pmod{2}$$

$$x_4 + x_5 + x_6 + x_7 \equiv 0 \pmod{2}$$

denklem sistemini sağlayan x_5 , x_6 ve x_7 bitlerinin sona eklenmesiyle $x_1x_2x_3x_4x_5x_6x_7$ şeklinde kodlayan yapıdır. Yukarıdaki denklem sisteminin çözüm kümesi, $\mathbb{F}_2^7$ vektör uzayının bir alt vektör uzayını oluşturduğundan genel olarak $\mathbb{F}_q^n$ vektör uzayının bir alt vektör uzayının kod olarak görülmesini sağlamış ve lineer kodların tanımını ortaya çıkarmıştır.

2.1 Lineer Kodlar

Bu alt başlık altında lineer kodlar hakkında detaylı bilgiler verilecektir.

Tanım 2.1. [35] $\mathbb{F}_q$ üzerinde n uzunluğunda bir toplamsal kod $\mathbb{F}_q^n$ vektör uzayının toplamaya göre kapalı bir alt kümesidir.

Tanım 2.2. [33] $\mathbb{F}_q$ üzerinde n uzunluğunda k boyutlu bir lineer kod $\mathbb{F}_q^n$ vektör uzayının k boyutlu bir alt vektör uzayıdır ve $[n, k]_q$ ile gösterilir. Kodun elemanlarına kodsözler denir.

Tanım 2.3. [33] Bir $x = (x_1, x_2, \dots, x_n) \in \mathbb{F}_q^n$ vektörünün Hamming ağırlığı x vektörünün sıfırdan farklı bileşenlerinin sayısıdır ve $w_h(x)$ ile gösterilir:

$$w_h(x) = |\{i : x_i \neq 0, 1 \leq i \leq n\}|. \quad (2.1)$$

Tanım 2.4. [33] $x = (x_1, x_2, \dots, x_n) \in \mathbb{F}_q^n$ ve $y = (y_1, y_2, \dots, y_n) \in \mathbb{F}_q^n$ vektörleri arasındaki Hamming uzaklığı farklı bileşenlerinin sayısıdır ve $d_h(x, y)$ ile gösterilir:

$$d_h(x, y) = |\{i : x_i \neq y_i, 1 \leq i \leq n\}| = w_h(x - y). \quad (2.2)$$

Tanım 2.5. [33] $C, \mathbb{F}_q$ üzerinde n uzunluğunda bir kod olmak üzere C kodunun minimum (Hamming) uzaklığı C kodundaki farklı kodsözlerin arasındaki en küçük Hamming uzaklığıdır. Bu uzaklık d ile gösterilirse

$$d = \min \{d_h(x, y) : x, y \in C, x \neq y\} \quad (2.3)$$

olur.

Bundan sonra aksi belirtilmedikçe bir kodun minimum uzaklığı ile o kodun minimum Hamming uzaklığı kastedilecektir.

Bir kodun hata farketme ve düzeltme kapasitesi o kodun minimum uzaklığı ile yakından ilişkilidir.

Teorem 2.1. [33] $C, \mathbb{F}_q$ üzerinde minimum uzaklığı d olan bir kod olsun. Bu durumda aşağıdakiler sağlanır:

1. C, t hata farkedilen bir koddur ancak ve ancak $d \geq t + 1$.
2. C, t hata düzeltilen bir koddur ancak ve ancak $d \geq 2t + 1$.

Tanım 2.6. [33] $\mathbb{F}_q$ üzerinde n uzunluğunda k boyutlu d minimum (Hamming) uzaklığına sahip bir lineer kod $[n, k, d]_q$ notasyonu ile gösterilir. Burada n, k ve d sayılarına C kodunun parametreleri denir.

Tanım 2.7 (Lineer Kodlar İçin Singleton Sınırı). [33] $[n, k, d]_q$ parametrelerine sahip bir C kodunun minimum uzaklığı için $d \leq n - k + 1$ sınırı vardır ve bu sınıra Singleton sınırı denir. Eğer $d = n - k + 1$ ise C koduna maksimum uzaklığa ayrışabilen (MDS) kod denir.

$x = (x_1, x_2, \dots, x_n) \in \mathbb{F}_q^n$ ve $y = (y_1, y_2, \dots, y_n) \in \mathbb{F}_q^n$ vektörlerinin Öklid iç çarpımı $\langle x, y \rangle$ ile gösterilir ve

$$\langle x, y \rangle = x_1 y_1 + x_2 y_2 + \dots + x_n y_n \quad (2.4)$$

şeklinde tanımlanır.

Tanım 2.8. [33] C , $\mathbb{F}_q$ üzerinde n uzunluğunda bir kod olsun. C kodunun Öklid iç çarpımına göre duali $C^\perp$ ile gösterilir ve

$$C^\perp = \{y \in \mathbb{F}_q^n : \langle x, y \rangle = 0, \forall x \in C\} \quad (2.5)$$

olarak tanımlanır.

C , bir $[n, k]_q$ parametrelili lineer kod ise $C^\perp$, $[n, n - k]_q$ parametrelili lineer koddur.

$\mathbb{F}_{q^2}$, q^2 elemanlı sonlu cisim olmak üzere $x = (x_1, x_2, \dots, x_n) \in \mathbb{F}_{q^2}^n$ ve $y = (y_1, y_2, \dots, y_n) \in \mathbb{F}_{q^2}^n$ vektörlerinin Hermityen iç çarpımı

$$\langle x, y \rangle_h = x_1 y_1^q + x_2 y_2^q + \dots + x_n y_n^q \quad (2.6)$$

şeklindedir.

Tanım 2.9. C , $\mathbb{F}_{q^2}$ üzerinde n uzunluğunda bir kod olsun. C kodunun Hermit iç çarpımına göre duali (Hermityen duali) $C^{\perp_h}$ ile gösterilir ve

$$C^{\perp_h} = \{y \in \mathbb{F}_{q^2}^n : \langle x, y \rangle_h = 0, \forall x \in C\} \quad (2.7)$$

şeklinde tanımlanır.

Tanım 2.10. [33] C , $\mathbb{F}_q$ üzerinde bir lineer kod olsun.

1. C kodun baz vektörlerini satır kabul eden matrise C kodun üreteç matrisi denir.
2. $C^\perp$ kodun baz vektörlerini satır kabul eden matrise C kodun kontrol matrisi denir.

Örnek 2.1. $C = \{00000, 11100, 00111, 11011\} \leq \mathbb{F}_2^5$ lineer kodu, $[5, 2, 3]$ parametrelerine sahip ve 1-hata düzelten bir koddur. $C^\perp =$

$\{00000, 10101, 01101, 11000, 00011, 10110, 01110, 11011\}$ lineer kodu ise $[5, 3, 2]$ parametrelili, 2-hata farkedebilen bir lineer koddur. C kodun üreteç ve kontrol matrisleri sırasıyla

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

ve

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

şeklindedir.

2.2 Sabit Devirli Kodlar

Lineer kodların önemli bir sınıfı, zengin cebirsel yapısından dolayı sabit devirli kodlardır. Bundan sonra aksi söylenmedikçe $\mathbb{F}_q^\times = \mathbb{F}_q \setminus \{0\}$, $\alpha \in \mathbb{F}_q^\times$ ve r , α 'nın çarpımsal mertebesidir.

Tanım 2.11. [35] C , $\mathbb{F}_q$ üzerinde n uzunluğunda bir lineer kod olsun. Eğer her $c = (c_0, c_1, \dots, c_{n-1}) \in C$ kodsözü için $(\alpha c_{n-1}, c_0, \dots, c_{n-2}) \in C$ oluyorsa C koduna $\mathbb{F}_q$ üzerinde n uzunluğunda bir α -sabit devirli kod denir. Özel olarak $\alpha = 1$ ise C koduna devirli kod, $\alpha = -1$ ise C koduna nega-devirli kod denir.

C , $\mathbb{F}_q$ üzerinde n uzunluğunda bir α -sabit devirli kod olsun. $\varphi : \mathbb{F}_q^n \rightarrow \frac{\mathbb{F}_q[x]}{\langle x^n - \alpha \rangle}$, $\varphi((c_0, c_1, \dots, c_{n-1})) = c_0 + c_1x + \dots + c_{n-1}x^{n-1}$ dönüşümü bir $\mathbb{F}_q$ vektör uzayı izomorfizmasıdır ve C kodunun φ altındaki görüntüsü $\varphi(C)$, $\frac{\mathbb{F}_q[x]}{\langle x^n - \alpha \rangle}$ bölüm halkasında bir idealdir.

Teorem 2.2. [35] $\mathbb{F}_q$ üzerinde n uzunluğunda α -sabit devirli kodlar ile $\frac{\mathbb{F}_q[x]}{\langle x^n - \alpha \rangle}$ bölüm halkasındaki idealler arasında birebir bir ilişki vardır. Dahası $x^n - \alpha$ 'yı bölen bir $g(x)$ polinomu için $\varphi(C)$, $g(x)$ polinomu tarafından üretilen bir idealdir.

Teorem 2.2, $\mathbb{F}_q$ üzerinde n uzunluğunda bir α -sabit devirli kodun $\frac{\mathbb{F}_q[x]}{\langle x^n - \alpha \rangle}$ bölüm halkasında bir ideal olarak görülmesini sağlar. $\frac{\mathbb{F}_q[x]}{\langle x^n - \alpha \rangle}$ halkasının idealleri $x^n - \alpha$ 'nın bölenleri tarafından üretilen idealler olduğundan $x^n - \alpha$ 'nın $\mathbb{F}_q$ üzerindeki indirgenemz çarpanları önemlidir.

$(n, q) = 1$ olsun. Bu durumda $\mathbb{F}_q$ 'nin bir cisim genişlemesinde $\gamma^n = \alpha$ olacak şekilde birimin rn ninci ilkel kökü vardır ve $x^n - \alpha$ 'nın $\mathbb{F}_q$ üzerindeki tüm kökleri $\gamma, \gamma^{1+r}, \dots, \gamma^{1+(n-1)r}$ şeklindedir. $O_{r,n} = \{1, 1+r, \dots, 1+r(n-1)\}$ olsun. $0 \leq j \leq n-1$ olmak üzere $\text{mod } rn$ 'ye göre $1+rj$ 'yi içeren q^2 -devirsel koset $C_{1+rj} =$

$\{(1+rj)q^{2i} \pmod{rn} : i \in \mathbb{N}\}$ kümesidir. Bu durumda $O_{r,n}$ bazı q^2 -devirsel kosetlerin birleşimidir.

Teorem 2.3. [35] Her $0 \leq j \leq n-1$ için $\pi_j(x) = \prod_{i \in C_{1+rj}} (x - \gamma^i)$ polinomu katsayıları $\mathbb{F}_q$ cisminden olan $\mathbb{F}_q$ üzerinde indirgenemez bir polinomdur. Dahası $x^n - \alpha$, bazı $0 \leq j \leq n-1$ tamsayıları için $\pi_j(x)$ polinomlarının çarpımıdır.

$\mathbb{F}_q$ üzerinde n uzunluğunda bir α -sabit devirli $C = \langle g(x) \rangle$ kodunun tanımlayıcı kümesi $Z = \{1+rj : g(\gamma^{1+rj}) = 0, 1+rj \in O_{r,n}\}$ olarak tanımlanır. Sonlu cisimler üzerindeki sabit devirli kodların minimum uzaklıklarına dair bir alt sınır belirlenmiştir.

Teorem 2.4 (Sabit devirli kodlar için BCH sınırı). [36, 37] $(n, q) = 1$ olsun. $\alpha, \mathbb{F}_q$ 'nin çarpımsal mertebesi r olan sıfırdan farklı bir elemanı ve $\gamma, \mathbb{F}_q$ 'nin bir genişlemesinde $\gamma^n = \alpha$ eşitliğini sağlayan birimin rn ninci ilkel kökü olsun. $C, \mathbb{F}_q$ üzerinde n uzunluğunda tanımlayıcı kümesi Z olan bir α -sabit devirli kod olmak üzere eğer bir μ tamsayısı için $\{1+rj, \mu \leq j \leq \mu+d-2\} \subseteq Z$ ise C kodun minimum uzaklığı en az d kadardır.

$\mathbb{F}_{q^2}$ üzerinde bir α -sabit devirli kodun Hermityen duali $\mathbb{F}_{q^2}$ üzerinde bir α^{-q} -sabit devirli koddur. Aşağıda $\mathbb{F}_{q^2}$ üzerinde bir α -sabit devirli kodun Hermityen dualini içermesi şartı verilmiştir.

Lemma 2.5. [11] $(n, q) = 1$ ve $C, \mathbb{F}_{q^2}$ üzerinde tanımlayıcı kümesi Z olan bir sabit devirli kod olsun. Bu durumda, $C^{\perp_h} \subseteq C$ ancak ve ancak $Z \cap -qZ = \emptyset$ olmasıdır.

Örnek 2.2. $C, \mathbb{F}_9$ üzerinde 11 uzunluğunda bir $\alpha = 2$ -sabit devirli kod olsun. Bu durumda $r = 2$ olur ve $\mathbb{F}_9$ üzerinde $\gamma^{11} = 2$ olacak şekilde birimin 22 nci ilkel kökü γ vardır. $1+2j$ 'yi içeren $\text{mod } 22$ 'ye göre tüm 9-devirsel kosetler aşağıdaki gibidir:

$$\begin{aligned} C_1 &= \{1, 3, 5, 9, 15\}, \\ C_7 &= \{7, 13, 17, 19, 21\}, \\ C_{11} &= \{11\}. \end{aligned}$$

Burada $-3C_1 = C_7$ olduğu görülür. C , tanımlayıcı kümesi $Z = C_1$ olan bir 2-sabit devirli kod olsun. C_1 devirsel koseti aralarındaki fark 2 olacak şekilde 3 ardışık eleman içerdiğinden C kodun minimum uzaklığı BCH sınırından en az 4'tür. Aynı zamanda $-3C_1 \cap C_1 = C_7 \cap C_1 = \emptyset$ şartı sağlandığından Lemma 2.5'e göre $C^{\perp_h} \subseteq C$ olur.

2.3 Kuantum Kodlar

Klasik mekaniğin kurallarına göre çalışan bilgisayarlar yerine günümüzde kuantum mekaniğinin kurallarına göre çalışan bilgisayarlar düşünülmektedir. Bu durum

kuantum bilginin iletilmesi sırasında meydana gelebilecek kuantum hataları düzeltebilen yapıların inşa edilmesi problemini ortaya çıkarmıştır. Bu yapılara kuantum kodlar denir. Kuantum kodların inşasından önce kuantum bilginin temel birimi olan kuantum bitlerin (kubitlerin) bilinmesi gerekir.

2.3.1 Kuantum Bitler ve Kuantum Hatalar

Klasik hesaplamanın ve klasik bilginin temel birimi bitler iken kuantum hesaplamanın ve kuantum bilginin temel birimi ise kubitlerdir [38]. q bir asalın kuvveti olmak üzere bir kubit, q boyutlu kompleks vektör uzayındaki bir vektör ile temsil edilir. $\mathbb{C}^q$, q boyutlu kompleks vektör uzayı ve $|\cdot\rangle$ notasyonu bir sütun vektörünü temsil etmek üzere bir kubit

$$|x\rangle = (a_i)_{q \times 1}, \quad a_i \in \mathbb{C}$$

olarak yazılır.

Bir $|x\rangle \in \mathbb{C}^q$ kubitinin kendisinden farklı bir $|y\rangle \in \mathbb{C}^q$ kubitine dönüşmesine kuantum hata denir. Dolayısıyla, bir kubit üzerinde meydana gelen bir kuantum hata, $\mathbb{C}^q$ vektör uzayı üzerinde bir lineer dönüşüm olarak düşünülebilir. $\mathbb{C}^q$ vektör uzayı üzerindeki lineer dönüşümlerin kümesi, $\mathbb{C}^q$ üzerinde ayrıca bir vektör uzayı (kuantum hata uzayı) belirttiğinden bu vektör uzayı için bir taban oluşturulabilir. $\{|x\rangle \in \mathbb{C}^q : x \in \mathbb{F}_q\}$ kümesi $\mathbb{C}^q$ vektör uzayının ortonormal bir tabanı olsun. ω , birimin p ninci ilkel kökü ve $iz : \mathbb{F}_q \rightarrow \mathbb{F}_p$, $iz(x) = \sum_{i=0}^{m-1} x^{p^i}$, $q = p^m$ olsun. Her $a, b \in \mathbb{F}_q$ için X_a ve Z_b lineer dönüşümleri

$$X_a |x\rangle = |x + a\rangle, \quad (2.8)$$

$$Z_b |x\rangle = \omega^{iz(bx)} |x\rangle \quad (2.9)$$

şeklinde tanımlanansın. Bu durumda $\{X_a Z_b : a, b \in \mathbb{F}_q\}$ kümesi bir kubit üzerindeki kuantum hata uzayı için bir tabandır [6].

Örnek 2.3. $q = 2$ olsun. Bu durumda $\omega = -1$ ve $iz : \mathbb{F}_2 \rightarrow \mathbb{F}_2$, $iz(x) = x$ olur. $\mathbb{C}^2$ için bir ortonormal taban $\left\{ |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$ seçilebilir. X_0, X_1, Z_0 ve Z_1 lineer dönüşümleri için

$$X_0 |0\rangle = |0\rangle, X_0 |1\rangle = |1\rangle,$$

$$X_1 |0\rangle = |1\rangle, X_1 |1\rangle = |0\rangle,$$

$$Z_0 |0\rangle = |0\rangle, Z_0 |1\rangle = |1\rangle,$$

$$Z_1 |0\rangle = |0\rangle, Z_1 |1\rangle = -|1\rangle,$$

sağlandığından X_0, X_1, Z_0 ve Z_1 lineer dönüşümleri $I_2 = X_0 = Z_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $X_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ ve $Z_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ olarak ifade edilebilir. $\{I, X_1, Z_1, X_1 Z_1\}$ kümesi $\mathbb{C}^2$ uzayındaki bir kubit üzerinde meydana gelebilecek kuantum hatalar için bir taban oluşturur.

$\mathbf{a} = (a_1, \dots, a_n) \in \mathbb{F}_q^n$ olsun ve $\otimes$, matrislerin tensör çarpımını ifade etsin. $X_{a_1}, \dots, X_{a_n}$ matrislerinin tensör çarpımı $X_{a_1} \otimes \dots \otimes X_{a_n}$ kısaca $X(\mathbf{a})$ ve $Z_{a_1}, \dots, Z_{a_n}$ matrislerinin tensör çarpımı $Z_{a_1} \otimes \dots \otimes Z_{a_n}$ ise kısaca $Z(\mathbf{a})$ olarak yazılır. $\mathbb{C}^{q^n} = \underbrace{\mathbb{C}^q \otimes \mathbb{C}^q \otimes \dots \otimes \mathbb{C}^q}_{n \text{ defa}}$ olsun. $\mathbb{C}^q$ uzayı üzerinde bir n kubit, $\mathbb{C}^{q^n}$ kompleks vektör uzayındaki bir vektördür. $\mathbb{C}^q$ uzayı üzerinde bir n kubit üzerinde oluşabilecek kuantum hatalar için bir taban, bir kubit üzerinde meydana gelen kuantum hataların taban elemanlarının tensör çarpımından oluşur. Yani, $\{X(\mathbf{a})Z(\mathbf{b}) : \mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n\}$ kümesi, n kubit üzerindeki kuantum hatalar için bir tabandır [6].

Örnek 2.4. $q = 2$ ve $n = 2$ olsun. Bu durumda $\mathbb{F}_2^2 = \{(0, 0), (0, 1), (1, 0), (1, 1)\}$ olmak üzere

$$\begin{aligned} X(0, 0) &= X_0 \otimes X_0, \\ X(0, 1) &= X_0 \otimes X_1, \\ X(1, 0) &= X_1 \otimes X_0, \\ X(1, 1) &= X_1 \otimes X_1, \\ Z(0, 0) &= Z_0 \otimes Z_0, \\ Z(0, 1) &= Z_0 \otimes Z_1, \\ Z(1, 0) &= Z_1 \otimes Z_0, \\ Z(1, 1) &= Z_1 \otimes Z_1 \end{aligned}$$

olarak hesaplanır. Ayrıca, $X(1, 0)$ dönüşümünün $|00\rangle$ 2 kubitinde meydana getirdiği hata aşağıdaki gibidir.

$$\begin{aligned} X(1, 0)(|00\rangle) &= (X_1 \otimes X_0)(|0\rangle \otimes |0\rangle) \\ &= X_1 |0\rangle \otimes X_0 |0\rangle \\ &= |1\rangle \otimes |0\rangle \\ &= |10\rangle. \end{aligned}$$

2.3.2 Stabilizer Kuantum Kodlar

Tanım 2.12. [6] $\mathbb{F}_q$ üzerinde n uzunluğunda M boyutlu bir kuantum kod, $\mathbb{C}^{q^n}$ kompleks vektör uzayının M boyutlu bir alt uzayıdır ve $((n, M))_q$ ile gösterilir. Özel olarak, $M = q^k$ ise bu kuantum kod $[[n, k]]_q$ ile gösterilir. Kuantum kodun elemanlarına kuantum kodsöz denir.

Kuantum kodların bir sınıfı olan stabilizer kuantum kodlar Daniel Gottesman tarafından tanımlanmıştır [4]. Stabilizer kuantum kodların tanımı için hata grubunun tanımı gereklidir. Her $a, b \in \mathbb{F}_q$ için X_a ve Z_b lineer dönüşümleri (2.8) ve (2.9)'daki gibi tanımlasın.

$$G_n = \{ \omega^c X(\mathbf{a}) Z(\mathbf{b}) : \mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n, c \in \mathbb{F}_p \}$$

olarak tanımlanan G_n , pq^{2n} elemanlı bir sonlu gruptur. G_n sonlu grubuna, $\{X(\mathbf{a})Z(\mathbf{b}) : \mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n\}$ hata tabanına bağlı hata grubu denir [6].

Tanım 2.13. [6] $S \leq G_n$ olsun. S alt grubuna bağlı Q stabilizer kuantum kodu

$$Q = \{ |x\rangle \in \mathbb{C}^{q^n} : E|x\rangle = |x\rangle, \forall E \in S \}$$

olarak tanımlanır.

Tanım 2.14. [6] Bir $(\mathbf{a}|\mathbf{b}) \in \mathbb{F}_q^{2n}$ vektörün simplektik ağırlığı

$$swt((\mathbf{a}|\mathbf{b})) = \{i \in \{1, \dots, n\} : (a_i|b_i) \neq (0, 0)\}$$

olarak tanımlanır. Bir $E = \omega^c X(\mathbf{a})Z(\mathbf{b})$ elemanının ağırlığı

$$w(E) = swt((\mathbf{a}|\mathbf{b}))$$

olarak tanımlanır.

Bir kuantum kodun minimum uzaklığı farkedemediği hataların en küçük ağırlığı olarak tanımlanır. Diğer bir ifade ile bir Q kuantum kodu d minimum uzaklığına sahiptir ancak ve ancak Q , G_n grubundaki ağırlığı d 'den küçük tüm hataları farkedirken d ağırlıklı bazı hataları farkedemez [6]. $\mathcal{D} \subseteq G_n$ olmak üzere bir kuantum kod $\mathcal{D}$ kümesindeki hataları farkedebiliyorsa $\mathcal{D}$ kümesinin gerdiği uzaydaki tüm hataları da farkedebilir. Ayrıca, d minimum uzaklığına sahip bir kuantum kod ağırlığı $\lfloor \frac{d-1}{2} \rfloor$ ve $\lfloor \frac{d-1}{2} \rfloor$ 'den küçük olan tüm hataları düzeltebilir [6].

Tanım 2.15. [6] $\mathbb{C}^{q^n}$ kompleks vektör uzayının d minimum uzaklıklı M boyutlu alt vektör uzayına $\mathbb{F}_q$ üzerinde $((n, M, d))_q$ parametrelili bir kuantum kod denir. Özel olarak, $M = q^k$ ise bu kuantum kod $[[n, k, d]]_q$ ile gösterilir.

$S \subseteq G_n$ olsun. S alt grubuna bağılı olarak verilen Q stabilizer kuantum kodun farkedemediği hatalar, G_n grubunda S 'deki elemanlarla değişmeli olup Q stabilizer kuantum kodun kodsözlerinde hataya sebep olan elemanlardır [6]. S alt grubunun G_n grubundaki merkezleyeni

$$C_{G_n}(S) = \{F \in G_n : EF = FE, \forall E \in S\}$$

alt grubudur. $Z(G_n)$, G_n 'in merkezi olmak üzere S ve $Z(G_n)$ tarafından üretilen alt grup $SZ(G_n)$ olsun.

Lemma 2.6. [6] Q , $S \subseteq G_n$ alt grubu ile verilen bir stabilizer kuantum kod olsun. Bir $E \in G_n$ hatasını Q stabilizer kuantum kodu tarafından farkedilebilir bir hata olması için gerek ve yeter koşul $E \in SZ(G_n)$ ya da $E \notin C_{G_n}(S)$ olmasıdır.

Lemma 2.6'ya göre $S \subseteq G_n$ alt grubu ile verilen bir stabilizer kuantum kodun farkedemeği hatalar, $C_{G_n}(S) \setminus SZ(G_n)$ kümesindeki elemanlardır. Bir $E = \omega^c X(\mathbf{a})Z(\mathbf{b}) \in G_n$ elemanını $(\mathbf{a}|\mathbf{b}) \in \mathbb{F}_q^{2n}$ vektörüne karşılık getiren dönüşüm altında $SZ(G_n)$ alt grubunun görüntüsü $\mathbb{F}_q$ üzerinde $2n$ uzunluğuna sahip

$$C = \{(\mathbf{a}|\mathbf{b}) \in \mathbb{F}_q^{2n} : \omega^c X(\mathbf{a})Z(\mathbf{b}) \in SZ(G_n)\}$$

toplamsal kodudur [6]. $C_{G_n}(S)$ alt grubunun görüntüsünü belirlemek için aşağıdaki tanıma ihtiyaç vardır. $(\mathbf{a}|\mathbf{b}), (\mathbf{a}'|\mathbf{b}') \in \mathbb{F}_q^{2n}$ vektörlerinin iz-simplektik iç çarpımı

$$\langle (\mathbf{a}|\mathbf{b}), (\mathbf{a}'|\mathbf{b}') \rangle_s = tr_{q/p}(\mathbf{b}\mathbf{a}' - \mathbf{b}'\mathbf{a})$$

olarak tanımlanır [6]. Burada $\mathbf{a}\mathbf{b}$, $\mathbf{a}$ ve $\mathbf{b}$ vektörlerinin Öklid iç çarpımıdır. Bu durumda $C_{G_n}(S)$ alt grubunun görüntüsü C kodun iz-simplektik iç çarpımına göre duali olan

$$C^{\perp_s} = \{(\mathbf{a}|\mathbf{b}) \in \mathbb{F}_q^{2n} : \omega^c X(\mathbf{a})Z(\mathbf{b}) \in C_{G_n}(S)\}$$

toplamsal kodudur. Bir sonraki teorem $\mathbb{F}_q$ üzerindeki $2n$ uzunluğundaki toplamsal kodlar ile stabilizer kuantum kodlar arasındaki geçişi verir.

Teorem 2.7. [6] $((n, M, d))_q$ parametrelerine sahip bir stabilizer kuantum kod vardır ancak ve ancak $M > 1$ iken $swt(C^{\perp_s} \setminus C) = d$, $M = 1$ iken $swt(C^{\perp_s}) = d$ ve $C \subseteq C^{\perp_s}$ şartlarını sağlayan $|C| = \frac{q^n}{M}$ elemanlı bir $C \leq \mathbb{F}_q^{2n}$ toplamsal kodu vardır.

C_1 ve C_2 , $\mathbb{F}_q$ üzerinde $C_2^{\perp} \subseteq C_1$ olacak şekilde $[n, k_1, d_1]_q$ ve $[n, k_2, d_2]_q$ parametrelili iki kod olsun ve $C = C_1^{\perp} \times C_2^{\perp}$ olarak tanımlansın. Bu durumda $C \subseteq C^{\perp_s}$ olduğundan Teorem 2.7'den minimum uzaklığı $d = \min\{w_h(c) : c \in (C_1 \setminus C_2^{\perp}) \cup (C_2 \setminus C_1^{\perp})\}$ olan

$[[n, k_1 + k_2 - n, d]]_q$ parametrelili bir stabilizer kuantum kod vardır. Özel olarak, $C_1^\perp \subseteq C_1$ ve $C_2 = C_1$ seçilirse aşağıdaki inşa elde edilir [6].

Teorem 2.8 (CSS İnşası). $[6]$ C bir $[n, k, d]_q$ parametrelili kod olsun. $C^\perp \subseteq C$ ise $[[n, 2k - n, \geq d]]_q$ parametrelili bir kuantum kod vardır.

$\mathbb{F}_{q^2}$ 'nin F_q üzerindeki bir tabanı $\{\beta, \beta^q\}$ olmak üzere $v, w \in \mathbb{F}_{q^2}^n$ vektörlerinin iz-alternatif iç çarpımları

$$\langle v | w \rangle_a = iz_{q/p} \left(\frac{vw^q - v^q w}{\beta^{2q} - \beta^q} \right)$$

olarak tanımlanır. $\phi : \mathbb{F}_q^{2n} \rightarrow \mathbb{F}_{q^2}^n$, $\phi((\mathbf{a}|\mathbf{b})) = \beta\mathbf{a} + \beta^q\mathbf{b}$ dönüşümü tanımlansın. Bu durumda, $\text{swt}((\mathbf{a}|\mathbf{b})) = w_h(\phi((\mathbf{a}|\mathbf{b})))$ olur ve ayrıca $\langle \mathbf{a}|\mathbf{b} \rangle_s = \langle \phi(\mathbf{a}) | \phi(\mathbf{b}) \rangle_a$ eşitliği sağlanır [6]. Teorem 2.7 aşağıdaki gibi yeniden düzenlenebilir.

Teorem 2.9. $[6]$ $((n, M, d))_q$ parametrelerine sahip bir stabilizer kuantum kod vardır ancak ve ancak $M > 1$ iken $w_h(C^{\perp_a} \setminus C) = d$, $M = 1$ iken $w_h(C^{\perp_a}) = d$ ve $C \subseteq C^{\perp_a}$ şartlarını sağlayan $|C| = \frac{q^n}{M}$ elemanlı bir $C \leq \mathbb{F}_{q^2}^n$ toplamsal kodu vardır.

$\mathbb{F}_{q^2}$ üzerinde bir C lineer kodu için $C^{\perp_h} = C^{\perp_a}$ eşitliği vardır. Bu durumda Teorem 2.9'un bir sonucu olarak $\mathbb{F}_{q^2}$ üzerinde Hermit iç çarpımına göre dualini içeren lineer kodlardan stabilizer kuantum kodların bir inşası verilmiş ve elde edilen stabilizer kuantum kodların parametreleri aşağıdaki gibi belirlenmiştir.

Teorem 2.10 (Hermityen İnşası). $[6]$ C bir $[n, k, d]_{q^2}$ parametrelili kod olsun. $C^{\perp_h} \subseteq C$ ise $[[n, 2k - n, \geq d]]_q$ parametrelili bir stabilizer kuantum kod vardır.

Lineer kodlarda olduğu gibi stabilizer kuantum kodların parametreleri üzerine de sınır vardır.

Tanım 2.16 (Stabilizer Kuantum Kodlar İçin Singleton Sınırı). $[5, 6]$ Bir $[[n, k, d]]_q$ stabilizer kuantum kodu için $k \leq n - 2d + 2$ dir. $k = n - 2d + 2$ eşitliğini sağlayan stabilizer kuantum koda maksimum uzaklığa ayrışabilen (MDS) stabilizer kuantum kod denir.

Örnek 2.5. $q = 2$ için bir kubit üzerindeki $I_2 = X_0 = Z_0$, X_1 ve Z_1 lineer dönüşümleri Örnek 2.3'teki gibi olsun. Notasyon kolaylığı olarak $I = I_2$, $X_1 = X$, $Z_1 = Z$ ve $Y = X_1 Z_1$ olarak tanımlansın. 3 kubit üzerinde G_3 hata grubunun bir alt grubu $S = \{E_0 = I \otimes I \otimes I, E_1 = Z \otimes Z \otimes I, E_2 = X \otimes X \otimes I, E_3 = Y \otimes Y \otimes I\}$ ve Q, S alt grubuna bağlı stabilizer kuantum kod olsun. $G_3 \rightarrow \mathbb{F}_2^6$, $(-1)^c X(\mathbf{a}) Z(\mathbf{b}) \rightarrow (\mathbf{a}|\mathbf{b})$

dönüşümü altında E_0, E_1, E_2 ve E_3 elemanlarının görüntüsü

$$\begin{aligned} I \otimes I \otimes I &\rightarrow (000|000) \\ Z \otimes Z \otimes I &\rightarrow (000|110) \\ X \otimes X \otimes I &\rightarrow (110|000) \\ Y \otimes Y \otimes I &\rightarrow (110|110) \end{aligned}$$

şeklinde. S alt grubunun bu dönüşüm altındaki görüntüsü $C = \{000|000, 000|110, 110|000, 110|110\} \subseteq \mathbb{F}_2^6$ bir lineer koddur ve $C^\perp = \{000|000, 000|110, 000|001, 000|111, 110|000, 110|110, 110|001, 110|111, 001|000, 001|110, 001|001, 001|111, 111|000, 111|110, 111|001, 111|111\}$ elde edilir. Buradan $C \subseteq C^\perp$ olduğu görülür. $\text{swt}(001|001) = 1$ olduğundan $\text{swt}(C^\perp \setminus C) = 1$ olur. Teorem 2.7'den $[[3, 1, 1]]_2$ parametrelili bir stabilizer kuantum kod vardır.

2.3.3 Dolaşık Destekli Kuantum Kodlar

Kuantum kodların önemli bir sınıfı da dolaşık destekli (entanglement-assisted) kuantum kodlardır. İlk olarak Brun ve arkadaşları tarafından geliştirilen bu kuantum kod gönderici ile alıcı arasında dolaşık haldeki kuantum durumlarından yararlanıp kodun performansını arttırmayı amaçlar [22]. Daha detaylı bilgi için [22, 30, 39, 40] referanslarına bakılabilir.

Tanım 2.17 (Dolaşık Destekli Kuantum Kod). [22] Bir $[[n, k, d; c]]_q$ dolaşık destekli kuantum kod, c dolaşık haldeki kuantum durumunu kullanarak k kubitini n kubitine kodlayan d minimum uzaklıklı bir kuantum koddur.

Dolaşık destekli kuantum kodlar için Singleton sınırı aşağıdaki gibi verilmiştir.

Tanım 2.18 (Dolaşık Destekli Kuantum Kodlar İçin Singleton Sınırı). [22] Bir $[[n, k, d; c]]_q$ kuantum kodu için $k \leq n - 2d + 2 + c$ dir. $k = n - 2d + 2 + c$ eşitliğini sağlayan dolaşık destekli kuantum koda dolaşık destekli kuantum maksimum uzaklığa ayrışabilen (MDS) kod denir.

Ayrıca, $c = n - k$ eşitliğini sağlayan dolaşık destekli kuantum koda maksimum dolaşıklıkla dolaşık destekli kuantum kod denir.

Sonlu cisimler üzerindeki lineer kodlardan dolaşık destekli kuantum kodların inşası verilmiş ve elde edilen kuantum kodların parametreleri belirlenmiştir. Bu inşaya göre $\mathbb{F}_{q^2}$ üzerindeki bir lineer kodun Hermit iç çarpımına göre dualini içermesi şartı aranmadığından bu inşaya $\mathbb{F}_{q^2}$ üzerindeki tüm lineer kodların bir kuantum koda dönüştürülebileceği imkanı sağlar.

Teorem 2.11. *[30] $C, [n, k, d]_{q^2}$ parametrelili ve kontrol matrisi $H = (h_{i,j})_{(n-k) \times n}$ olan bir kod olsun. Bu durumda $c = \text{rank}(HH^\dagger)$ olmak üzere $\llbracket n, 2k - n + c, d; c \rrbracket_q$ parametrelili dolaşıklık destekli bir kuantum kod vardır. Burada $H^\dagger = (h_{j,i}^q)_{n \times (n-k)}$ matrisidir.*



[41]'de $\mathbb{F}_q$ üzerinde bir devirli kodun tanımlayıcı kümesinin en az iki ardışık eleman içermesi şartı verilmiş ve bu şartı sağlayan dualini içeren devirli kodlardan CSS inşası ile kuantum kodlar elde edilmiştir. [42]'de ise $\mathbb{F}_q$ üzerinde çift uzunluklu bir nega-devirli kodun tanımlayıcı kümesinin en az iki ardışık eleman içermesi şartı verilmiş ve bu şartı sağlayan dualini içeren nega-devirli kodlardan CSS inşası ile elde kuantum kodların parametreleri verilmiştir. Bu bölümde ise $\mathbb{F}_{q^2}$ üzerinde bir sabit devirli kodun tanımlayıcı kümesinin en az üç ardışık eleman içermesi şartı verilecek, Hermityen inşası ile kuantum MDS kodların bir sınıfı yeniden elde edilecek ve [41]'de elde edilen kuantum kodların minimum uzaklıkları artırılarak daha iyi kuantum kodlar elde edilecektir.

3.1 Kuantum MDS Kodların Bir Sınıfının İnşası

Aşağıdaki önermede [41]'de $\mathbb{F}_q$ üzerinde devirli kodların ve [42]'de $\mathbb{F}_q$ üzerinde nega-devirli kodların tanımlayıcı kümeleri için verilen sonuç $\mathbb{F}_{q^2}$ üzerinde sabit devirli kodların tanımlayıcı kümelerine genelleştirilmiş ve bir q^2 -devirsel kosetin m ardışık eleman içermesi için yeter koşul verilmiştir.

Önerme 3.1. q , bir asalın kuvveti ve n , $(n, q) = 1$ eşitliğini sağlayan bir pozitif tamsayı olsun. $1 \leq j \leq m - 2$ için $\lambda_j = \left(\frac{q^{2a_{j+1}-1}}{r}\right)^{-1} - \left(\frac{q^{2a_1-1}}{r}\right)^{-1} - jr$ olmak üzere $n | (\lambda_1, \lambda_2, \dots, \lambda_{m-2})$ şartını sağlayan $1 \leq a_1, a_2, \dots, a_{m-1} \leq o_{rn}(q^2)$, $m \geq 3$ tamsayıları varsa $\mathbb{F}_{q^2}$ üzerinde $[n, n - \delta, d \geq m + 1]_{q^2}$ parametrelerine sahip bir α -sabit devirli kod vardır. Burada δ , m ardışık elemanı içeren q^2 -devirsel kosetin eleman sayısıdır.

İspat. $m \geq 3$ olmak üzere

$$\begin{aligned}
kq^{2a_1} &\equiv k + r \pmod{rn} \\
(k + r)q^{2a_2} &\equiv k + 2r \pmod{rn} \\
(k + 2r)q^{2a_3} &\equiv k + 3r \pmod{rn} \\
&\vdots \\
(k + (m - 2)r)q^{2a_{m-1}} &\equiv k + (m - 1)r \pmod{rn}
\end{aligned}$$

kongrüans denklem sistemi sağlansın. Bu denklem sistemi her $0 \leq j \leq m - 2$ için $(k + jr)\left(\frac{q^{2a_{j+1}} - 1}{r}\right) \equiv 1 \pmod{n}$ denkleğini gerektirdiğinden aşağıdaki denklem sistemi elde edilir.

$$\begin{aligned}
k &\equiv \left(\frac{q^{2a_1} - 1}{r}\right)^{-1} \pmod{n} \\
k &\equiv \left(\frac{q^{2a_3} - 1}{r}\right)^{-1} - 2r \pmod{n} \\
&\vdots \\
k &\equiv \left(\frac{q^{2a_{m-1}} - 1}{r}\right)^{-1} - (m - 2)r \pmod{n}
\end{aligned}$$

Bu sistem bir çözüme sahiptir ancak ve ancak her $i, j = 1, 2, \dots, m - 2$ için

$$\left(\frac{q^{2a_{j+1}} - 1}{r}\right)^{-1} - jr \equiv \left(\frac{q^{2a_{i+1}} - 1}{r}\right)^{-1} - ir \pmod{n}$$

ve her $j = 1, 2, \dots, m - 2$ için

$$\left(\frac{q^{2a_1} - 1}{r}\right)^{-1} \equiv \left(\frac{q^{2a_{j+1}} - 1}{r}\right)^{-1} - jr \pmod{n}$$

olur. Bu durumda her $j = 1, 2, \dots, m - 2$ için $n \mid \left(\frac{q^{2a_{j+1}} - 1}{r}\right)^{-1} - \left(\frac{q^{2a_1} - 1}{r}\right)^{-1} - jr$ olduğundan $j = 1, 2, \dots, m - 2$ için $\lambda_j = \left(\frac{q^{2a_{j+1}} - 1}{r}\right)^{-1} - \left(\frac{q^{2a_1} - 1}{r}\right)^{-1} - jr$ olmak üzere $n \mid (\lambda_1, \lambda_2, \dots, \lambda_{m-2})$ elde edilir. C , $\mathbb{F}_{q^2}$ üzerinde tanımlayıcı kümesi $C_{q^2, rn}(k)$ olan bir α -sabit devirli kod olsun. Yukarıdaki inşadan $C_{q^2, rn}(k)$, m ardışık eleman içerir. $|C_{q^2, rn}(k)| = \delta$ ve BCH sınırından istenen parametrelere sahip bir kuantum kod vardır. ■

Lemma 3.1. $k \geq 1$ bir tamsayı olsun. Aşağıdakiler sağlanır.

1. $(2^k + 1, 2^{2k} + 1) = 1.$
2. $(2^k - 1, 2^{2k} + 1) = 1.$

İspat. 1. $(2^k + 1)(2^{2k} - 2^{2k-1} - 2^{k-1} + 1) = 1 + (2^k - 2^{k-1})(2^{2k} + 1)$ eşitliğinden $(2^k + 1)(2^{2k} - 2^{2k-1} - 2^{k-1} + 1) \equiv 1 \pmod{(2^{2k} + 1)}$ elde edilir. Bu durumda $(2^k + 1, 2^{2k} + 1) = 1$ sağlanır.

2. $(2^k - 1)(2^k - 1)2^{k-1} = 1 + (2^{k-1} - 1)(2^{2k} + 1)$ eşitliğinden $(2^k - 1)(2^k - 1)2^{k-1} \equiv 1 \pmod{(2^{2k} + 1)}$ elde edilir. Bu durumda $(2^k - 1, 2^{2k} + 1) = 1$ sağlanır.

■

Lemma 3.2. $k \geq 1$ olmak üzere $q = 2^k$, $r = q + 1$ ve $n = \frac{q^2+1}{\lambda} \geq 5$ olsun. Aşağıdakiler sağlanır:

1. $0 \leq j \leq q - 1$ için $C_{q^2, rn}(1 + rj) = \{1 + rj, 1 + r(q - 1 - j)\}$.

2. $-qC_{q^2, rn}\left(1 + \frac{(q+1)q}{2}\right) \neq C_{q^2, rn}\left(1 + \frac{(q+1)q}{2}\right)$.

İspat. 1. $q^2r \equiv -r \pmod{rn}$ denkleğinden $q^2(1 + rj) \equiv 1 + r(q - 1 - j) \pmod{rn}$ olduğı görülür. $o_{rn}(q^2) = 2$ olduğundan $0 \leq j \leq q - 1$ için $C_{q^2, rn}(1 + rj) = \{1 + rj, 1 + r(q - 1 - j)\}$ elde edilir.

2. $-qC_{q^2, rn}\left(1 + \frac{(q+1)q}{2}\right) = C_{q^2, rn}\left(1 + \frac{(q+1)q}{2}\right)$ olsun. Bu durumda $-q\left(1 + \frac{(q+1)q}{2}\right) \equiv 1 + \frac{(q+1)q}{2} \pmod{rn}$ veya $-q\left(1 + \frac{(q+1)q}{2}\right) \equiv 1 + \frac{(q+1)(q-2)}{2} \pmod{rn}$ durumları vardır.

$-q\left(1 + \frac{(q+1)q}{2}\right) \equiv 1 + \frac{(q+1)q}{2} \pmod{rn}$ olsun. Bu durumda $1 + \frac{(q+1)q}{2} \equiv 0 \pmod{n}$ elde edilir. $(2, n) = 1$ olduğundan $q^2 + q + 2 \equiv 0 \pmod{n}$ ve dolayısıyla $q + 1 \equiv 0 \pmod{n}$ olur. Bu ise Lemma 3.1 1. ile çelişir.

$-q\left(1 + \frac{(q+1)q}{2}\right) \equiv 1 + \frac{(q+1)(q-2)}{2} \pmod{rn}$ olsun. Bu durumda $\frac{(q+1)q}{2} \equiv 0 \pmod{n}$ elde edilir. $(2, n) = 1$ olduğundan $q^2 + q \equiv 0 \pmod{n}$ ve dolayısıyla $q - 1 \equiv 0 \pmod{n}$ olur. Bu ise Lemma 3.1 2. ile çelişir.

■

Teorem 2.10 ve Lemma 3.2'nin bir sonucu olarak kuantum MDS kodların bir sınıfı inşa edilebilir.

Teorem 3.3. $k \geq 1$ olmak üzere $q = 2^k$ olsun. $\frac{q^2+1}{\lambda} \geq 5$ olacak şekilde $q^2 + 1$ in her λ böleni için $\left\lfloor \frac{q^2+1}{\lambda}, \frac{q^2+1}{\lambda} - 4, 3 \right\rfloor_q$ parametrelerine sahip bir kuantum MDS kod vardır.

İspat. $\frac{q^2+1}{\lambda} \geq 5$ ve $r = q + 1$ olsun. C , $\mathbb{F}_{q^2}$ üzerinde n uzunluklu $C_{q^2, rn}(1 + r\frac{q}{2})$ tanımlayıcı kümesine sahip bir α -sabit devirli kod olsun. Lemma 3.2 2.'den

$-qC_{q^2, rn}(1+r\frac{q}{2}) \neq C_{q^2, rn}(1+r\frac{q}{2})$ ve Lemma 2.5'ten $C^{\perp_H} \leq C$ olur. Lemma 3.2 1.'den $C_{q^2, rn}(1+r\frac{q}{2})$ ardışık iki elemanlı bir kümedir. Bu durumda Teorem 2.10'den $[[n, n-4, 3]]_q$ parametrelili kuantum MDS kodu elde edilir. ■

3.2 İyileştirilmiş Parametrelere Sahip Kuantum Kodlar

Burada $\mathbb{F}_{q^2}$ üzerindeki devirli kodları ve kuantum kodlar için Hermityen inşasını düşünerek literatürdeki bazı kuantum kodlardan daha iyi parametrelere sahip kuantum kodlar inşa edilecektir.

q bir asalın pozitif kuvveti, $(n, q) = 1$ ve $o_n(q) = 2m$, $m \geq 1$ olsun. Bu durumda $o_n(q^2) = m$ ve dolayısıyla eğer bir i için $|C_{q, n}(i)| = 2t$, $t|m$ ise $|C_{q^2, n}(i)| = t$ olur. $C_{q, n}(i), -C_{q, n}(i) \neq C_{q, n}(i)$ eşitsizliğini sağlayan ve d ardışık terim içeren devirli koset olsun. $C, \mathbb{F}_q$ üzerinde n uzunluğunda tanımlayıcı kümesi $C_{q, n}(i)$ olan bir devirli kod olsun. Bu durumda $C^{\perp} \leq C$ ve $d(C) \geq d+1$ olur. CSS inşası ile C devirli kodundan $[[n, n-4t, \geq d+1]]_q$ kuantum kodu elde edilir. Ayrıca $C_{q^2, n}(i) = \{i, iq^2, \dots, iq^{2t-2}\}$ ve $C_{q^2, n}(iq) = \{iq, iq^3, \dots, iq^{2t-1}\}$ olduğundan $C_{q, n}(i) = C_{q^2, n}(i) \cup C_{q^2, n}(iq)$ eşitliği vardır. O zaman $\mathbb{F}_{q^2}$ üzerinde $C_{q^2, n}(i) \cup C_{q^2, n}(iq)$ tanımlayıcı kümesine sahip devirli koddan Hermityen inşası ile $[[n, n-4t, \geq d+1]]_q$ parametrelili kuantum kod elde etmek için $-C_{q, n}(i) \cap C_{q, n}(i) = \emptyset$ eşitliğinin $-qC_{q, n}(i) \cap C_{q, n}(i) = \emptyset$ eşitliğini gerektirdiğini göstermek yeterlidir.

Önerme 3.2. $-C_{q, n}(i) \cap C_{q, n}(k) = \emptyset$ ancak ve ancak $-qC_{q, n}(i) \cap C_{q, n}(k) = \emptyset$.

İspat. $(n, q) = 1$ ve iki devirli koset ya ayrık ya da aynı olduğundan $-i \equiv kq^j \pmod{n}$ ancak ve ancak $-qi \equiv kq^{j+1} \pmod{n}$ önermesi sağlanır. ■

Önerme 3.2'de özel olarak $k = i$ alınırsa $-C_{q, n}(i) \cap C_{q, n}(i) = \emptyset \Leftrightarrow -qC_{q, n}(i) \cap C_{q, n}(i) = \emptyset$ önermesi elde edilir. Bu ise $\mathbb{F}_q$ üzerinde dualini içeren devirli kodlardan CSS inşası ile üretilen kuantum tüm kodların ve dolayısıyla [41]'de verilen tüm kuantum kodların $\mathbb{F}_{q^2}$ üzerinde Hermityen dualini içeren devirli kodlardan Hermityen inşası ile elde edilebileceğini garanti eder. İleride $C_{q, n}(i) \cup C_{q, n}(k)$ yerine $C_{q, n}(i, k)$ notasyonu kullanılacaktır.

Örnek 3.1. $q = 7$ ve $n = 65$ olsun. Bu durumda $65|7^6+1$ dir ve Önerme 3.2'ten her i için $-C_{7, 65}(i) = C_{7, 65}(i)$ eşitliği sağlanır. Dolayısıyla $\mathbb{F}_7$ üzerinde 65 uzunluğunda dualini içeren devirli kod yoktur ve [41]'de verilen yöntemle bu kodlardan kuantum kod elde edilemez. Fakat $-7C_{7^2, 65}(2) = C_{7^2, 65}(9)$ ve $C_{7^2, 65}(2) = \{2, 8, 32, 33, 57, 63\}$ olduğundan $C_{7^2, 65}(2)$ tanımlayıcı kümesine sahip $\mathbb{F}_{7^2}$ üzerinde 65 uzunluğunda bir C_1 devirli kodu $C_1^{\perp_H} \leq C_1$ şartını sağlar. Hermityen inşası ile $[[65, 53, d \geq 3]]_7$ kuantum kodu elde edilir.

$-7C_{7^2,65}(6) = C_{7^2,65}(22)$ ve $C_{7^2,65}(6) = \{6, 24, 31, 34, 41, 59\}$ dur. $\mathbb{F}_{7^2}$ üzerinde 65 uzunluğunda $C_{7^2,65}(2, 6)$ tanımlayıcı kümesine sahip bir C_1 devirli kodu için $C_2^{\perp_h} \leq C_2$ dir ve Hermityen inşası ile $[[65, 41, d \geq 5]]_7$ kuantum kodu vardır.

Eğer $2 \mid |C_{q,n}(i)|$ ise $2 \mid |C_{q^2,n}(i)| = |C_{q,n}(i)|$ olduğu açıktır. Bu durumda $\mathbb{F}_q$ üzerinde bir devirsel koset $\mathbb{F}_{q^2}$ üzerinde iki devirsel kosetin birleşimi olacağından daha yüksek boyutlu ve minimum uzaklıklı Hermityen dualini içeren devirli kodlar bulunur.

Örnek 3.2. $q = 11$ ve $n = 63$ olsun. [41]'de $[[63, 39, d \geq 4]]_{11}$ kuantum kodu elde edilmiştir. C_1 , $\mathbb{F}_{11^2}$ üzerinde uzunluklu $C_{11^2,63}(3, 8, 9, 10) = \{3, 8, 9, 10, 11, 12, 13, 18, 23, 36, 48, 61\}$ tanımlayıcı kümesine sahip devirli kod olsun. Bu durumda $C_1^{\perp_h} \leq C_1$ olduğundan Hermityen inşası ile $[[63, 39, d \geq 7]]_{11}$ elde edilir ki bu kod yukarıdaki kuantum kodun minimum uzaklığını artırmıştır. Ayrıca, $\mathbb{F}_{11}$ üzerinde dualini içeren devirli kodlar ile bulunabilen en iyi kuantum kod $[[63, 45, d \geq 4]]_{11}$ iken $\mathbb{F}_{11^2}$ üzerinde $C_{11^2,63}(3, 8, 10) = \{3, 8, 10, 11, 12, 13, 23, 48, 61\}$ tanımlayıcı kümesine sahip C_2 devirli kodu $C_2^{\perp_h} \leq C_2$ şartını sağladığından Hermityen inşası ile $[[63, 45, d \geq 5]]_{11}$ elde edilir.

Tablo 3.1 [41]'de elde edilen kuantum kodlar ile bir kıyaslama

[41]	$[[n, k, d]]_q$	Tanımlayıcı Küme
$[[63, 39, d \geq 4]]_{11}$	$[[63, 39, d \geq 7]]_{11}$	$C_{11^2,63}(3, 8, 9, 10)$
$[[63, 39, d \geq 4]]_{11}$	$[[63, 45, d \geq 5]]_{11}$	$C_{11^2,63}(3, 8, 10)$
$[[35, 19, d \geq 4]]_{27}$	$[[35, 19, d \geq 5]]_{27}$	$C_{27^2,35}(1, 2, 3, 4)$

Bir sonraki tablo ise [41]'de verilen inşası ile elde edilemeyen fakat Hermityen inşası ile türetilen kuantum kodların bazılarının bir listesidir.

Tablo 3.2 [41]'deki inşası ile elde edilemeyen kuantum kodların bazıları

n	q	k	Kuantum Kod	Tanımlayıcı Küme
17	7	2	$[[17, 1, d \geq 4]]_7$	$C_{7^2,17}(3)$
25	13	5	$[[25, 5, d \geq 3]]_{13}$	$C_{13^2,25}(2)$
37	23	3	$[[37, 13, d \geq 5]]_{23}$	$C_{23^2,37}(1, 9)$
41	32	2	$[[41, 29, d \geq 4]]_{32}$	$C_{32^2,41}(1, 2, 3)$
73	17	6	$[[73, 25, d \geq 7]]_{17}$	$C_{17^2,73}(4, 13)$

$\frac{q^2+1}{13}$ ve $\frac{q^2+1}{17}$ Uzunluklu Kuantum MDS Kodlar

Lineer kodlar içerisinde önemli ailelerden bir tanesi de sabit devirli kodlardır. Sabit devirli kodlar devirli kodların bir genelleştirmesi olup zengin cebirsel yapıya sahiptirler. Sonlu cisimler üzerindeki lineer kodlardan Hermityen inşası ile kuantum kodlar elde etmek için bu lineer kodların Hermityen duallerini içermeleri yeterlidir. Sabit devirli kodların cebirsel yapıları bu kodların Hermityen duallerini içermeye koşullarını belirlemekte kolaylık sağlar. Bu bölümde sabit devirli kodların cebirsel yapılarından faydalananarak $\frac{q^2+1}{13}$ ve $\frac{q^2+1}{17}$ uzunluğunda kuantum MDS kodların bir sınıfı için literatürden farklı bir inşaya verilecektir.

p bir asal ve $q, p|q^2 + 1$ olacak şekilde tek asalın pozitif kuvveti olsun. $\alpha, \mathbb{F}_{q^2}$ üzerinde birimin $(q + 1)$. ilkel kökü yani $r = q + 1$ olsun. Bu durumda q^2 nin mod rn ye göre çarpımsal mertebesi en fazla 2 dir.

Lemma 4.1. *Mod rn ye göre tüm q^2 -devirsel kosetler aşağıdaki gibidir.*

1. $C_{1+(q+1)j} = \{1 + (q + 1)j, 1 + (q + 1)(q - 1 - j)\}, 0 \leq j < \frac{q-1}{2}.$
2. $C_{1+(q+1)j} = \{1 + (q + 1)j\}, j = \frac{q-1}{2}.$
3. $C_{1+(q+1)j} = \{1 + (q + 1)j, 1 + (q + 1)(n + q - 1 - j)\}, q - 1 < j < \frac{q-1}{2} + \frac{n}{2}.$
4. $C_{1+(q+1)j} = \{1 + (q + 1)j\}, j = \frac{q-1}{2} + \frac{n}{2}.$

4.1 $\frac{q^2+1}{13}$ Uzunluklu Kuantum MDS Kodlar

$q, 13m + 5$ ya da $13m + 8$ formunda tek asalın kuvveti ve $n = \frac{q^2+1}{13}$ olsun. $q = 13m + 5$ için $O_{r,n}$ nin bir alt kümesi $Z_1 = \bigcup_{j=4m+2}^{\frac{q-1}{2}} C_{1+(q+1)j}$ ve $q = 13m + 8$ için ise $O_{r,n}$ nin bir alt kümesi $Z_2 = \bigcup_{j=4m+3}^{\frac{q-1}{2}} C_{1+(q+1)j}$ olarak tanımlansın. İki durum için de aşağıdaki geçerlidir.

Lemma 4.2. $Z_1 \cap -qZ_1 = \emptyset$ ve $Z_2 \cap -qZ_2 = \emptyset$.

İspat. $q = 13m + 5$ ve $Z_1 \cap -qZ_1 \neq \emptyset$ olsun. Bu durumda $-q(1 + (q + 1)j) \equiv 1 + (q + 1)k \pmod{rn}$ denkleğini sağlayan bazı $4m + 2 \leq j, k \leq 9m + 2$ vardır. Bu denklik aynı zamanda $1 + k + qj \equiv 0 \pmod{n}$ denkleğini gerektirir. $4m + 2 \leq j, k \leq 9m + 2$ olduğundan $\frac{q^2+1}{2} - (q + 1)\frac{5m}{2} \leq 1 + qj + k \leq \frac{q^2+1}{2} + (q + 1)\frac{5m}{2}$ elde edilir. $q = 13m + 5$ olduğundan $52m^2 + 50m + 13 \leq 1 + qj + k \leq 117m^2 + 80m + 13$ ve $n = 13m^2 + 10m + 2$ elde edilir. Ayrıca, $4n < 52m^2 + 50m + 13 < 5n$ ve $8n < 117m^2 + 80m + 13 < 9n$ eşitsizlikleri $1 + qj + k$ nin tüm mümkün değerlerinin nz , $5 \leq z \leq 8$ olmasını gerektirir. $4m + 3 \leq 1 + k \leq 9m + 3 < 13m + 5 = q$ olduğundan $1 + qj + k$ nin q ile bölümünden kalan $1 + k$ olduğu görülür. $5n, 6n, 7n$ ve $8n$ sayılarının q ile bölümünden kalanlar sırasıyla $12m + 5, 4m + 2, 9m + 4$ ve $m + 1$ olur fakat bu kalanların hiçbirisinin $[4m + 3, 9m + 3]$ aralığında olmaması çelişkidir.

$q = 13m + 8$ ve $Z_2 \cap -qZ_2 \neq \emptyset$ olsun. Bu durumda $-q(1 + (q + 1)j) \equiv 1 + (q + 1)k \pmod{rn}$ denkleğini sağlayan bazı $4m + 3 \leq j, k \leq 9m + 4$ vardır. Bu denklik aynı zamanda $1 + k + qj \equiv 0 \pmod{n}$ denkleğini gerektirir. Yukarıdaki hesaplamalara benzer olarak $1 + qj + k$ nin tüm mümkün değerlerinin nz , $5 \leq z \leq 8$ olduğu görülür. $4m + 4 \leq 1 + k \leq 9m + 5 < 13m + 8 = q$ olduğundan $1 + qj + k$ nin q ile bölümünden kalan $1 + k$ olduğu görülür. $5n, 6n, 7n$ ve $8n$ sayılarının q ile bölümünden kalanlar sırasıyla $m + 1, 9m + 6, 4m + 3$ ve $12m + 8$ olur fakat bu kalanların hiçbirisinin $[4m + 4, 9m + 5]$ aralığında olmaması çelişkidir. ■

Teorem 4.3. q , $13m + 5$ ya da $13m + 8$ formunda tek asalın kuvveti olsun. $q = 13m + 5$ durumunda her $2 \leq d$ (çift) $\leq 5m + 2$ ve $q = 13m + 8$ durumunda her $2 \leq d$ (çift) $\leq 5m + 3$ için $\left[\frac{q^2+1}{13}, \frac{q^2+1}{13} - d + 1, d \right]_{q^2}$ parametrelerine sahip ve Hermityen duallerini içeren α -sabit devirli kodların bir sınıfı vardır.

İspat. $q = 13m + 5$ olsun. Her $0 \leq i \leq \frac{5m}{2}$ için $S_i = \bigcup_{j=\frac{q-1}{2}-i}^{\frac{q-1}{2}} C_{1+(q+1)j}$ kümesi tanımlansın. Bu durumda S_i , Z_1 in ardışık eleman içeren bir alt kümesidir ve $|S_i| = 2i + 1$ olur. C_i , tanımlayıcı kümesi S_i olan bir α -sabit devirli kod olsun. Bu durumda C_i istenen parametrelere sahip MDS koddur. Ayrıca, $S_i \subseteq Z_1$ olduğundan Lemma 4.2'ten $-qS_i \cap S_i = \emptyset$ ve Lemma 2.5'ten $C_i^{\perp_h} \subseteq C_i$ elde edilir. $q = 13m + 8$ durumu benzerdir. ■

Teorem 4.4. q , $13m + 5$ ya da $13m + 8$ formunda tek asalın kuvveti olsun. $q = 13m + 5$ durumunda her $2 \leq d$ (çift) $\leq 5m + 2$ ve $q = 13m + 8$ durumunda her $2 \leq d$ (çift) $\leq 5m + 3$ için $\left[\frac{q^2+1}{13}, \frac{q^2+1}{13} - 2d + 2, d \right]_q$ parametrelerine sahip kuantum MDS kodların bir ailesi vardır.

İspat. Teorem 4.3'de inşa edilen α -sabit devirli kodlar Hermityen duallerini içerdiğinden Teorem 2.4 kullanılarak istenen parametrelere sahip kuantum kodlar

elde edilir. Ayrıca, bu kuantum kodlar kuantum Singleton sınırını sağladığından MDS kodlardır. ■

Lingfei Jin ve arkadaşları tarafından [8]'de inşa edilen kuantum MDS kod ailesi Teorem 4.4'te farklı bir şekilde yeniden inşa edilmiştir.

Örnek 4.1. $q = 31 = 13m + 5$ olsun. Bu durumda $n = 74$, $r = 32$ ve $m = 2$ olur. $0 \leq j \leq 30$ için $1+32j$ 'yi içeren mod 2368'e göre 31^2 -devirsel kosetler aşağıdaki gibidir:

$$\begin{aligned} j &= 0, 30, & C_1 &= \{1, 961\} \\ j &= 1, 29, & C_{33} &= \{33, 929\} \\ &\vdots & &\vdots \\ j &= 9, 21, & C_{289} &= \{289, 673\} \\ j &= 10, 20, & C_{321} &= \{321, 641\} \\ j &= 11, 19, & C_{353} &= \{353, 609\} \\ j &= 12, 18, & C_{385} &= \{385, 577\} \\ j &= 13, 17, & C_{417} &= \{417, 545\} \\ j &= 14, 16, & C_{449} &= \{449, 513\} \\ j &= 15, & C_{481} &= \{481\} \end{aligned}$$

Ayrıca aşağıdaki eşitlikler sağlanır.

$$\begin{aligned} -31C_{289} &= C_{449} \\ -31C_{321} &= C_{1441} \\ -31C_{353} &= C_{65} \\ -31C_{385} &= C_{1057} \\ -31C_{417} &= C_{1281} \\ -31C_{449} &= C_{289} \\ -31C_{481} &= C_{1665} \end{aligned}$$

$-31C_{289} = C_{449}$ olduğundan her $0 \leq i \leq 5$ için $S_i = \bigcup_{j=15-i}^{15} C_{1+32j}$ olarak tanımlanır. α , $\mathbb{F}_{31^2}^\times$ grubunda çarpımsal mertebesi 32 olan bir eleman olmak üzere $\mathcal{C}_i$, $\mathbb{F}_{31^2}$ üzerinde S_i tanımlayıcı kümesine sahip bir α -sabit devirli kod olsun. Bu durumda $-qS_i \cap S_i = \emptyset$ olduğundan $\mathcal{C}_i$, Hermityen dualini içeren $[74, 74 - 2i + 1, 2i + 2]_{31^2}$ parametrelili bir koddur. Hermityen inşası ile $[[74, 74 - 4i - 2, 2i + 2]]_{31}$ quantum MDS kodu elde edilir.

Teorem 4.4 ile elde edilen bazı kuantum MDS kodlar Tablo 4.1'de verilmiştir.

Tablo 4.1 Teorem 4.4 ile elde edilen bazı kuantum MDS kodların parametreleri

q	m	$[[n, k, d]]_q$	d (çift)
31	2	$[[74, 74 - 2d + 2, d]]_{31}$	$2 \leq d \leq 12$
47	3	$[[170, 170 - 2d + 2, d]]_{47}$	$2 \leq d \leq 18$

4.2 $\frac{q^2+1}{17}$ Uzunluklu Kuantum MDS Kodlar

q , $17m+4$ ya da $17m+13$ formunda tek asalın kuvveti ve $n = \frac{q^2+1}{17}$ olsun. $q = 17m+4$

için $O_{r,n}$ nin bir alt kümesi $Z_3 = \bigcup_{j=6m+2}^{\frac{q-1}{2}} C_{1+(q+1)j}$ ve $q = 17m+13$ için ise $O_{r,n}$ nin bir alt

kümesi $Z_4 = \bigcup_{j=6m+5}^{\frac{q-1}{2}} C_{1+(q+1)j}$ olarak tanımlansın. İki durum için de aşağıdaki geçerlidir.

Lemma 4.5. $Z_3 \cap -qZ_3 = \emptyset$ ve $Z_4 \cap -qZ_4 = \emptyset$.

İspat. $q = 17m+4$ ve $Z_3 \cap -qZ_3 \neq \emptyset$ olsun. Bu durumda $-q(1+(q+1)j) \equiv 1+(q+1)k \pmod{rn}$ denkleğini sağlayan bazı $6m+2 \leq j, k \leq 11m+2$ vardır. Bu denklik aynı zamanda $1+k+qj \equiv 0 \pmod{n}$ denkleğini gerektirir. $6m+2 \leq j, k \leq 11m+2$ olduğundan $\frac{q^2+1}{2} - (q+1)\frac{5m-1}{2} \leq 1+qj+k \leq \frac{q^2+1}{2} + (q+1)\frac{5m-1}{2}$ elde edilir. $q = 17m+4$ olduğundan $102m^2 + 64m + 11 \leq 1+qj+k \leq 187m^2 + 72m + 6$ ve $n = 17m^2 + 8m + 1$ elde edilir. Ayrıca, $6n < 102m^2 + 64m + 11 < 7n$ ve $10n < 187m^2 + 72m + 6 < 11n$ eşitsizlikleri $1+qj+k$ nin tüm mümkün değerlerinin nz , $7 \leq z \leq 10$ olmasını gerektirir. $6m+3 \leq 1+k \leq 11m+2 < 17m+4 = q$ olduğundan $1+qj+k$ nin q ile bölümünden kalan $1+k$ olduğu görülür. $7n$, $8n$, $9n$ ve $10n$ sayılarının q ile bölümünden kalanlar sırasıyla $11m+3$, $15m+4$, $2m+1$ ve $6m+2$ olur fakat bu kalanların hiçbirisinin $[6m+3, 11m+2]$ aralığında olmaması çelişkidir.

$q = 17m+13$ ve $Z_4 \cap -qZ_4 \neq \emptyset$ olsun. Bu durumda $-q(1+(q+1)j) \equiv 1+(q+1)k \pmod{rn}$ denkleğini sağlayan bazı $6m+5 \leq j, k \leq 11m+7$ vardır. Bu denklik aynı zamanda $1+k+qj \equiv 0 \pmod{n}$ denkleğini gerektirir. Yukarıdaki hesaplamalara benzer olarak $1+qj+k$ nin tüm mümkün değerlerinin nz , $7 \leq z \leq 10$ olduğu görülür. $6m+6 \leq 1+k \leq 11m+8 < 17m+13 = q$ olduğundan $1+qj+k$ nin q ile bölümünden kalan $1+k$ olduğu görülür. $7n$, $8n$, $9n$ ve $10n$ sayılarının q ile bölümünden kalanlar sırasıyla $6m+14$, $2m+2$, $15m+12$ ve $11m+9$ olur fakat bu kalanların hiçbirisinin $[6m+6, 11m+8]$ aralığında olmaması çelişkidir. ■

Teorem 4.6. q , $17m+54$ ya da $17m+13$ formunda tek asalın kuvveti olsun. $q = 17m+4$ durumunda her $2 \leq d$ (çift) $\leq 5m+1$ ve $q = 17m+13$ durumunda her $2 \leq d$ (çift) $\leq 5m+4$ için $\left[\frac{q^2+1}{17}, \frac{q^2+1}{17} - d + 1, d \right]_{q^2}$ parametrelerine sahip ve Hermityen duallerini içeren α -sabit devirli kodların bir sınıfı vardır.

İspat. $q = 17m + 4$ olsun. Her $0 \leq i \leq \frac{5m-1}{2}$ için $S_i = \bigcup_{j=\frac{q-1}{2}-i}^{\frac{q-1}{2}} C_{1+(q+1)j}$ kümesi tanımlansın. Bu durumda S_i, Z_3 'ün ardışık eleman içeren bir alt kümesidir ve $|S_i| = 2i + 1$ dir. C_i , tanımlayıcı kümesi S_i olan bir α -sabit devirli kod olsun. Bu durumda C_i istenen parametrelere sahip MDS koddur. Ayrıca, $S_i \subseteq Z_3$ olduğundan Lemma 4.5'ten $-qS_i \cap S_i = \emptyset$ ve Lemma 2.5'ten $C_i^{\perp_h} \subseteq C_i$ elde edilir. $q = 17m + 13$ durumu benzerdir. ■

Teorem 4.7. $q, 17m+4$ ya da $17m+13$ formunda tek asalın kuvveti olsun. $q = 17m+4$ durumunda her $2 \leq d$ (çift) $\leq 5m + 1$ ve $q = 17m + 13$ durumunda her $2 \leq d$ (çift) $\leq 5m + 4$ için $\left[\left[\frac{q^2+1}{17}, \frac{q^2+1}{17} - 2d + 2, d \right] \right]_q$ parametrelerine sahip kuantum MDS kodların bir ailesi vardır.

İspat. Teorem 4.6'te inşa edilen α -sabit devirli kodlar Hermityen duallerini içerdiğinden Teorem 2.4 kullanılarak istenen parametrelere sahip kuantum kodlar elde edilir. Ayrıca, bu kuantum kodlar kuantum Singleton sınırını sağladığından MDS kodlardır. ■

Lingfei Jin ve arkadaşları tarafından [8]'de inşa edilen kuantum MDS kod ailesi Teorem 4.7'de farklı bir şekilde yeniden inşa edilmiştir.

Örnek 4.2. $q = 47 = 17m + 13$ olsun. Bu durumda $n = 130, r = 48$ ve $m = 2$ olur. $0 \leq j \leq 46$ için mod 6240'a göre 47^2 -devirsel kosetler aşağıda verilmiştir:

$$\begin{aligned}
 j &= 0, 46, & C_1 &= \{1, 2209\} \\
 j &= 1, 45, & C_{49} &= \{49, 2161\} \\
 &\vdots & &\vdots \\
 j &= 16, 30, & C_{769} &= \{769, 1441\} \\
 j &= 17, 29, & C_{817} &= \{817, 1393\} \\
 j &= 18, 28, & C_{865} &= \{865, 1345\} \\
 j &= 19, 27, & C_{913} &= \{913, 1297\} \\
 j &= 20, 26, & C_{961} &= \{961, 1249\} \\
 j &= 21, 25, & C_{1009} &= \{1009, 1201\} \\
 j &= 22, 24, & C_{1057} &= \{1057, 1153\} \\
 j &= 23, & C_{1105} &= \{1105\}
 \end{aligned}$$

Ayrıca aşağıdaki eşitlikler sağlanır.

$$\begin{aligned}
-47C_{769} &= C_{913} \\
-47C_{817} &= C_{3169} \\
-47C_{865} &= C_{3025} \\
-47C_{913} &= C_{769} \\
-47C_{961} &= C_{3697} \\
-47C_{1009} &= C_{2497} \\
-47C_{1057} &= C_{241} \\
-47C_{1105} &= C_{4225}
\end{aligned}$$

$-47C_{769} = C_{913}$ olduğundan her $0 \leq i \leq 6$ için $S_i = \bigcup_{j=23-i}^{23} C_{1+48j}$ olarak tanımlanır. α , $\mathbb{F}_{47^2}^\times$ grubunda çarpımsal mertebesi 48 olan bir eleman olmak üzere $\mathcal{C}_i$, $\mathbb{F}_{47^2}$ üzerinde S_i tanımlayıcı kümesine sahip bir α -sabit devirli kod olsun. Bu durumda $-qS_i \cap S_i = \emptyset$ olduğundan $\mathcal{C}_i$, Hermityen dualini içeren $[130, 130 - 2i + 1, 2i + 2]_{47^2}$ parametrelili bir koddur. Hermityen inşası ile $[[130, 130 - 4i - 2, 2i + 2]]_{47}$ quantum MDS kodu elde edilir.

Teorem 4.7 ile elde edilen bazı kuantum MDS kodlar Tablo 4.2’de verilmiştir.

Tablo 4.2 Teorem 4.7 ile elde edilen bazı kuantum MDS kodların parametreleri

q	m	$[[n, k, d]]_q$	d (çift)
47	2	$[[130, 130 - 2d + 2, d]]_{47}$	$2 \leq d \leq 14$
89	5	$[[466, 466 - 2d + 2, d]]_{89}$	$2 \leq d \leq 26$

Dolaşıklık destekli kuantum kodların inşası üzerine yoğun bir şekilde çalışılmaktadır. Lineer kodlardan dolaşıklık destekli kuantum kodların inşasında gerekli olan paylaşılan çiftlerin sayısını (c sayısını) belirlemek kolay değildir. Jianzhang Chen ve arkadaşları nega-devirli kodların tanımlayıcı kümelerinin bir ayrışımı tanımlamış ve bu ayrışımından yararlanarak $\mathbb{F}_{q^2}$ üzerindeki nega-devirli kodlardan elde edilen dolaşıklık destekli kuantum kodların dolaşıklık çiftlerin sayısı (c) belirlemiştir [23]. Daha sonra Yang Liu ve arkadaşları bu ayrışım tanımını sabit devirli kodların tanımlayıcı kümelerine taşımış ve $\mathbb{F}_{q^2}$ üzerindeki sabit devirli kodlardan elde edilen dolaşıklık destekli kuantum kodların dolaşıklık çiftlerin sayısı (c) belirlemiştir [24]. Bu bölümde sabit devirli kodların tanımlayıcı kümeleri için tanımlanan ayrışım kullanılarak dolaşıklık destekli kuantum MDS kodların bazı aileleri elde edilecektir.

$\mathbb{F}_{q^2}$ sonlu cismi üzerinde tanımlayıcı kümesi Z olan sabit devirli bir C kodu için $Z_\beta = \{i \in Z : -qi \in Z\}$ ve $Z_\delta = \{i \in Z : -qi \notin Z\}$ kümeleri tanımlansın. Bu durumda $Z = Z_\beta \cup Z_\delta$, $Z_\beta \cap Z_\delta = \emptyset$ ve $Z_\beta = Z \cap -qZ$ olur. Burada $Z = Z_\beta \cup Z_\delta$ ayrışımına Z 'nin bir ayrışımı denir. Z_β ve Z_δ bazı q^2 -devirsel kosetlerin birleşimi olduğundan tanımlayıcıları kümeleri sırasıyla Z_β ve Z_δ olan C_β ve C_δ kodları $\mathbb{F}_{q^2}$ üzerinde birer sabit devirli kodlardır ve $C = C_\beta \cap C_\delta$ eşitliği sağlanır. Ayrıca, Z_δ kümesinin tanımından $-qZ_\delta \cap Z_\delta = \emptyset$ ve Lemma 2.5'ten $C_\delta^{\perp_h} \subseteq C_\delta$ elde edilir.

Önerme 5.1. [24] $(n, q) = 1$ olmak üzere C , $\mathbb{F}_{q^2}$ üzerinde n uzunluklu Z tanımlayıcı kümesine sahip bir sabit devirli kod ve $Z = Z_\beta \cup Z_\delta$, Z 'nin yukarıdaki gibi bir ayrışımı olsun. C 'den elde edilen dolaşıklık destekli kuantum kod için dolaşıklık çiftlerin sayısı $c = |Z_\beta|$ kadardır.

5.1 $q^2 + 1$ Uzunluklu Dolaşıklık Destekli Kuantum MDS Kodlar

Jianfa Qian ve Lina Zhang tarafından $q \equiv 1 \pmod{4}$ denkleğini sağlayan tek asal kuvvetleri için $q^2 + 1$ uzunluklu dolaşıklık destekli kuantum MDS kodlar inşa edilmiş fakat $q \equiv 3 \pmod{4}$ durumu düşünülmemiştir [25]. Burada $q \equiv 3 \pmod{4}$ olmak

üzere $q^2 + 1$ uzunluğuna sahip dolaşık destekli kuantum MDS kodlar inşa edilecektir.

Lemma 5.1. $m \geq 1$ olmak üzere $q = 4m + 3$ bir asal kuvveti, $n = q^2 + 1$ ve $s = \frac{n}{2}$ olsun. $0 \leq i \leq \frac{q^2-1}{4}$ için $\text{mod } 2n$ 'ye göre $s - 2i$ 'yi içeren q^2 -devirsel kosetler aşağıdaki gibidir:

1. $C_{s-2i} = \{s - 2i, s + 2i\}$, $0 < i \leq \frac{q^2-1}{4}$.
2. $C_s = \{s\}$.

İspat. $o_{2n}(q^2) = 2$ olduğundan $\text{mod } 2n$ 'ye göre bir q^2 -devirsel kosetin eleman sayısı en fazla 2 olur. $q^2(1 + 2j) \equiv 1 + 2\left(\frac{q^2-1}{2} - j\right) \pmod{2n}$ denkliği sağlandığından $q^2(s - 2i) = q^2\left(1 + 2\left(\frac{q^2-1}{4} - i\right)\right) \equiv 1 + 2\left(\frac{q^2-1}{4} + i\right) = s + 2i \pmod{2n}$ elde edilir. Dolayısıyla, $C_{s-2i} = \{s - 2i, s + 2i\}$ ve özel olarak, $i = 0$ ise $C_s = \{s\}$ olur. ■

Lemma 5.2. $m \geq 1$ olmak üzere $q = 4m + 3$ bir asal kuvveti, $n = q^2 + 1$ ve $s = \frac{n}{2}$ olsun. Aşağıdakiler sağlanır:

1. $-qC_s = C_s$.
2. $-qC_{s-2(q-1)} = C_{s-2(q+1)}$.
3. Her $1 \leq \lambda \leq q - 1$ için $Z = \bigcup_{i=1}^{\lambda} C_{s-2i}$ tanımlayıcı kümesi $-qZ \cap Z = \emptyset$ eşitliğini sağlar.
4. $-qC_{s-2} = C_{s-2q}$.

İspat. 1. $(q + 1)\frac{q^2+1}{2} \equiv 0 \pmod{2n}$ denkleğinden $-q\frac{q^2+1}{2} \equiv \frac{q^2+1}{2} \pmod{2n}$ elde edilir. Dolayısıyla, $-qC_s = C_s$ eşitliği sağlanır.

2. $q^2 \equiv -1 \pmod{2n}$ ve $-qs \equiv s \pmod{2n}$ denklileri sağlanır. Buradan $-q(s - 2(q - 1)) \equiv s - 2(q + 1) \pmod{2n}$ ve dolayısıyla $-qC_{s-2(q-1)} = C_{s-2(q+1)}$ elde edilir.

3. Lemma 5.1'den $Z = \{s - 2(q - 1), s - 2(q - 2), \dots, s - 2, s + 2, \dots, s + 2(q - 2), s + 2(q - 1)\}$ yazılabilir. $-qZ \cap Z \neq \emptyset$ olsun. Bu durumda bazı $1 \leq i, j \leq q - 1$ tamsayıları için $-q(s \pm 2i) \equiv (s \pm 2j) \pmod{2n}$ denkliği sağlanır ve buradan $\pm qi \pm j \equiv 0 \pmod{n}$ elde edilir. Fakat $1 \leq qi - j < n - q - 2$ ve $q + 1 \leq qi + j < n - 2$ olduğundan hiçbir $1 \leq i, j \leq q - 1$ tamsayıları için $\pm qi \pm j \equiv 0 \pmod{n}$ denkliği sağlanmaz. Bu ise kabul ile çelişir.

4. $-qs \equiv s \pmod{2n}$ ve $C_{s-2q} = \{s - 2q, s + 2q\}$ eşitliklerinden elde edilir.

■

$Z_1 = C_s \cup C_{s-2} \cup C_{s-2q}$ ve $Z = Z_1 \cup \left(\bigcup_{i=2}^{q-1} C_{s-2i} \right)$ olsun. Lemma 5.2'den $-qZ_1 = Z_1$ ve $\left(-q \bigcup_{i=2}^{q-1} C_{s-2i} \right) \cap \left(\bigcup_{i=2}^{q-1} C_{s-2i} \right) = \emptyset$ elde edilir. Bu durumda $|-qZ \cap Z| = 5$ olur. C , $\mathbb{F}_{q^2}$ üzerinde $q^2 + 1$ uzunluğunda Z tanımlayıcı kümeli bir nega-devirli kod olsun. Bu durumda C bir $[q^2 + 1, q^2 - 2q, 2q + 2]_{q^2}$ koddur. C kodu için Teorem 2.11 ve Önerme 5.1 uygulanırsa dolaşık destekli kuantum MDS kodların bir sınıfı elde edilir.

Teorem 5.3. $m \geq 1$ olmak üzere her $q = 4m + 3$ asal kuvveti için $[[q^2 + 1, q^2 - 4q + 4, 2q + 2; 5]]_q$ parametrelili dolaşık destekli kuantum MDS kod vardır.

Teorem 5.3 ile elde edilen bazı dolaşık destekli kuantum MDS kodlar Tablo 5.1'de verilmiştir.

Tablo 5.1 Teorem 5.3 ile elde edilen bazı dolaşık destekli kuantum MDS kodların parametreleri

q	n	$[[n, k, d; c]]_q$
7	50	$[[50, 25, 16; 5]]_7$
11	122	$[[122, 81, 24; 5]]_{11}$
19	362	$[[362, 289, 40; 5]]_{19}$

Teorem 5.4. $m \geq 1$ olsun. $q = 4m + 3$ asal kuvveti olmak üzere her $q + 1 \leq \lambda \leq 2q - 2$ tamsayısı için $[[q^2 + 1, q^2 - 4\lambda + 8, 2\lambda + 2; 9]]_q$ parametrelerine sahip bir dolaşık destekli kuantum MDS kod vardır.

İspat. Her $q + 1 \leq \lambda \leq 2q - 2$ tamsayısı için $Z_\lambda = \bigcup_{i=0}^{\lambda} C_{s-2i}$ ve $Z' = \left(\bigcup_{i=0}^1 C_{s-2i} \right) \cup \left(\bigcup_{j=q-1}^{q+1} C_{s-2j} \right)$ kümeleri tanımlansın. Özel olarak $\lambda = q + 1$ için $Z_{q+1} = Z' \cup \left(\bigcup_{i=2}^{q-2} C_{s-2i} \right)$ olur ve bu durumda Lemma 5.2'den $|Z_{q+1} \cap Z_{q+1}| = 9$ elde edilir. $q + 1 \leq \lambda \leq 2q - 2$ tamsayıları için $Z_\lambda = Z' \cup \left(\bigcup_{i=2}^{q-2} C_{s-2i} \right) \cup \left(\bigcup_{j=q+2}^{\lambda} C_{s-2j} \right)$ olur. Lemma 5.2'den $-qZ' = Z'$ olduğundan $-qZ_\lambda = Z' \cup \left(-q \bigcup_{i=2}^{q-2} C_{s-2i} \right) \cup \left(-q \bigcup_{j=q+2}^{\lambda} C_{s-2j} \right)$ elde edilir. $Z' \subseteq -qZ_\lambda \cap Z_\lambda$ olduğundan $|-qZ_\lambda \cap Z_\lambda| \geq 9$ dur. $|-qZ_\lambda \cap Z_\lambda| = 9$ eşitliğini elde etmek için aşağıdaki eşitlikleri ispatlamak yeterlidir:

$$\left(-q \bigcup_{i=2}^{q-2} C_{s-2i} \right) \cap \left(\bigcup_{i=2}^{q-2} C_{s-2i} \right) = \emptyset, \quad (5.1)$$

$$\left(-q \bigcup_{i=2}^{q-2} C_{s-2i} \right) \cap \left(\bigcup_{j=q+2}^{\lambda} C_{s-2j} \right) = \emptyset, \quad (5.2)$$

$$\left(\bigcup_{i=2}^{q-2} C_{s-2i}\right) \cap \left(-q \bigcup_{j=q+2}^{\lambda} C_{s-2j}\right) = \emptyset, \quad (5.3)$$

$$\left(-q \bigcup_{i=q+2}^{\lambda} C_{s-2i}\right) \cap \left(\bigcup_{i=q+2}^{\lambda} C_{s-2i}\right) = \emptyset. \quad (5.4)$$

Lemma 5.2'den (5.1) eşitliğinin sağlandığı görülür. $\left(-q \bigcup_{i=2}^{q-2} C_{s-2i}\right) \cap \left(\bigcup_{j=q+2}^{\lambda} C_{s-2j}\right) \neq \emptyset$ olsun. Bu durumda $2 \leq i \leq q-2$ ve $q+2 \leq j \leq \lambda$ tamsayıları için dört durum vardır:

1. $-q(s-2i) \equiv s-2j \pmod{2n}$: Bu durumda $qi+j \equiv 0 \pmod{n}$ olur. Bu ise $0 < 3q+2 \leq qi+j \leq q^2-2 < n$ olması ile çelişir.
2. $-q(s-2i) \equiv s+2j \pmod{2n}$: Bu durumda $qi-j \equiv 0 \pmod{n}$ olur. Bu ise $0 < 2 \leq qi-j \leq q^2-3q-2 < n$ olması ile çelişir.

$-q(s+2i) \equiv s-2j \pmod{2n}$ ve $-q(s+2i) \equiv s+2j \pmod{2n}$ durumlarında önceki iki durumda elde edilen çelişkilere benzer şekilde çelişki elde edilir. Dolayısıyla $\left(-q \bigcup_{i=2}^{q-2} C_{s-2i}\right) \cap \left(\bigcup_{j=q+2}^{\lambda} C_{s-2j}\right) = \emptyset$ olur ve (5.2) eşitliği sağlanır. $\left(\bigcup_{i=2}^{q-2} C_{s-2i}\right) \cap \left(-q \bigcup_{j=q+2}^{\lambda} C_{s-2j}\right) = \emptyset$ olduğundan (5.3) eşitliği de sağlanmış olur. $\left(-q \bigcup_{i=q+2}^{\lambda} C_{s-2i}\right) \cap \left(\bigcup_{i=q+2}^{\lambda} C_{s-2i}\right) \neq \emptyset$ olsun. Bu durumda $q+2 \leq i, j \leq \lambda$ tamsayıları için aşağıdaki durumlar vardır:

1. $-q(s-2i) \equiv s-2j \pmod{2n}$: Bu durumda $qi+j \equiv 0 \pmod{n}$ dir. Bu ise $n < q^2+3q+2 \leq qi+j \leq 2q^2-2 < 2n$ olması ile çelişir.
2. $-q(s-2i) \equiv s+2j \pmod{2n}$: Bu durumda $qi-j \equiv 0 \pmod{n}$ dir. Bu ise $n < q^2+2 \leq qi-j \leq 2q^2-3q-2 < 2n$ olması ile çelişir.

$-q(s+2i) \equiv s-2j \pmod{2n}$ ve $-q(s+2i) \equiv s+2j \pmod{2n}$ durumlarında önceki iki durumda elde edilen çelişkilere benzer şekilde çelişki elde edilir. Dolayısıyla $\left(-q \bigcup_{i=q+2}^{\lambda} C_{s-2i}\right) \cap \left(\bigcup_{i=q+2}^{\lambda} C_{s-2i}\right) = \emptyset$ olduğundan (5.4) eşitliği de sağlanmış olur. Sonuç olarak $|-qZ_{\lambda} \cap Z_{\lambda}| = 9$ elde edilir.

Her $q+1 \leq \lambda \leq 2q-2$ için $\mathcal{C}_{\lambda}$, $\mathbb{F}_{q^2}$ üzerinde q^2+1 uzunluğunda Z_{λ} tanımlayıcı kümesine sahip bir nega-devirli kod olsun. O zaman $\mathcal{C}_{\lambda}$, bir $[q^2+1, q^2-2\lambda, 2\lambda+2]_{q^2}$ parametrelili koddur. $|-qZ_{\lambda} \cap Z_{\lambda}| = 9$ olduğundan Teorem 2.11 ve Önerme 5.1'den istenen parametrelere sahip dolaşık destekli kuantum MDS kodlar vardır. ■

Örnek 5.1. $q = 7$ olsun. Bu durumda $n = 50$ olur ve $0 \leq j \leq 24$ için $1 + 2j$ 'yi içeren mod 100'e göre 49-devirsel kosetler aşağıda verilmiştir.

$$\begin{aligned}
 j &= 0, 24, & C_1 &= \{1, 49\} \\
 j &= 1, 23, & C_3 &= \{3, 47\} \\
 j &= 2, 22, & C_5 &= \{5, 45\} \\
 j &= 3, 21, & C_7 &= \{7, 43\} \\
 j &= 4, 20, & C_9 &= \{9, 41\} \\
 j &= 5, 19, & C_{11} &= \{11, 39\} \\
 j &= 6, 18, & C_{13} &= \{13, 37\} \\
 j &= 7, 17, & C_{15} &= \{15, 35\} \\
 j &= 8, 16, & C_{17} &= \{17, 33\} \\
 j &= 9, 15, & C_{19} &= \{19, 31\} \\
 j &= 10, 14, & C_{21} &= \{21, 29\} \\
 j &= 11, 13, & C_{23} &= \{23, 27\} \\
 j &= 12, & C_{25} &= \{25\}
 \end{aligned}$$

Ayrıca aşağıdaki eşitlikler sağlanır:

$$\begin{aligned}
 -7C_1 &= C_{57} \\
 -7C_3 &= C_{71} \\
 -7C_5 &= C_{65} \\
 -7C_7 &= C_{51} \\
 -7C_9 &= C_{13} \\
 -7C_{11} &= C_{23} \\
 -7C_{13} &= C_9 \\
 -7C_{15} &= C_{55} \\
 -7C_{17} &= C_{69} \\
 -7C_{19} &= C_{67} \\
 -7C_{21} &= C_{53} \\
 -7C_{23} &= C_{11} \\
 -7C_{25} &= C_{25}
 \end{aligned}$$

Burada her $8 \leq \lambda \leq 12$ tamsayısı için $Z_\lambda = \bigcup_{i=0}^{\lambda} C_{25-2i}$ olmak üzere $|-7Z_\lambda \cap Z_\lambda| = 9$ olduğu görülür. $\mathcal{C}_\lambda$, $\mathbb{F}_{49}$ üzerinde 50 uzunluğunda Z_λ tanımlayıcı kümesine sahip

bir nega-devirli kod olsun. Bu durumda $\mathcal{C}_\lambda$, parametreleri $[50, 49 - 2\lambda, 2\lambda + 2]_{49}$ olan bir koddur. $|-7Z_\lambda \cap Z_\lambda| = 9$ olduğundan her $8 \leq \lambda \leq 12$ tamsayısı için $[[50, 49 - 4\lambda + 8, 2\lambda + 2; 9]]_7$ parametrelili dolaşık destekli kuantum MDS kod vardır.

Teorem 5.4 ile elde edilen bazı dolaşık destekli kuantum MDS kodlar Tablo 5.2'de verilmiştir.

Tablo 5.2 Teorem 5.4 ile elde edilen bazı dolaşık destekli kuantum MDS kodların parametreleri

q	n	$[[n, k, d; c]]_q$	λ
7	50	$[[50, 57 - 4\lambda, 2\lambda + 2; 9]]_7$	$8 \leq \lambda \leq 12$
11	122	$[[122, 129 - 4\lambda, 2\lambda + 2; 9]]_{11}$	$12 \leq \lambda \leq 20$
19	362	$[[362, 369 - 4\lambda, 2\lambda + 2; 9]]_{19}$	$20 \leq \lambda \leq 36$

5.2 $\frac{q^2-1}{4}$ Uzunluklu Dolaşık Destekli Kuantum MDS Kodlar

$q = 4m + 3 > 3$ eşitliğini sağlayan bir tek asal kuvveti, $n = \frac{q^2-1}{4}$ ve α , $\mathbb{F}_{q^2}$ üzerinde birimin $r = 4$ 'üncü ilkel kökü olsun. $\mathbb{F}_{q^2}$ üzerinde $\frac{q^2-1}{4}$ uzunluklu α -sabit devirli kodlar kullanılarak $\frac{q^2-1}{4}$ uzunluklu dolaşık destekli kuantum MDS kodlar inşa edilecektir. $1 + 4j$ 'yi içeren $\text{mod } rn$ 'ye göre q^2 -devirsel kosetler $C_{1+4j} = \{1 + 4j\}$, $0 \leq j \leq n-1$ olarak belirlenmiştir [13].

Lemma 5.5. [13] $m \geq 1$ olmak üzere $q = 4m + 3$ bir asal kuvveti ve $n = \frac{q^2-1}{4}$ olsun.

Eğer $Z = \bigcup_{j=-\frac{q-3}{4}}^{\frac{q-3}{2}} C_{1+4j}$ ise $-qZ \cap Z = \emptyset$ eşitliği sağlanır.

Ayrıca $1 + 4(n - (\frac{q+1}{4})) = 4n - q \equiv -q \pmod{rn}$ denkleğinden aşağıdaki sonuç elde edilir.

Lemma 5.6. $m \geq 1$ olmak üzere $q = 4m + 3$ bir asal kuvveti, $n = \frac{q^2-1}{4}$ ve $r = 4$ olsun. Bu durumda $\text{mod } rn$ 'ye göre C_1 ve C_{-q} q^2 -devirsel kosetleri için $-qC_1 = C_{-q}$ eşitliği sağlanır.

Teorem 5.7. $m \geq 1$ olsun. $q = 4m + 3$ asal kuvveti olmak üzere her $\frac{q+9}{4} \leq d \leq q$ tamsayısı için $[[\frac{q^2-1}{4}, \frac{q^2-1}{4} - 2d + 4, d; 2]]_q$ parametrelerine sahip bir dolaşık destekli kuantum MDS kod vardır.

İspat. Her $0 \leq \lambda \leq \frac{q-3}{4}$ ve $0 \leq \delta \leq \frac{q-3}{2}$ için $Z_{\lambda,\delta} = \bigcup_{j=-\frac{q+1}{4}-\lambda}^{\delta} C_{1+4j}$, $Z_\lambda = \bigcup_{j=-\frac{q+1}{4}-\lambda}^{-\frac{q+1}{4}} C_{1+4j}$ ve $Z_\delta = \bigcup_{j=-\frac{q-3}{4}}^{\delta} C_{1+4j}$ kümeleri tanımlansın. $Z_{\lambda,\delta} = Z_\lambda \cup Z_\delta$ olduğundan $Z_{\lambda,\delta} \cap -qZ_{\lambda,\delta} =$

$(Z_\lambda \cup Z_\delta) \cap (-qZ_\lambda \cup -qZ_\delta) = (Z_\lambda \cap -qZ_\lambda) \cup (Z_\lambda \cap -qZ_\delta) \cup (Z_\delta \cap -qZ_\lambda) \cup (Z_\delta \cap -qZ_\delta)$ elde edilir. $C_1 \subseteq -qZ_\lambda \cap Z_\delta$ ve $C_{-\frac{q+1}{4}} \subseteq Z_\lambda \cap -qZ_\delta$ olduğundan $|Z_{\lambda,\delta} \cap -qZ_{\lambda,\delta}| = 2$ eşitliğini elde etmek için aşağıdaki eşitlikleri ispatlamak yeterlidir.

$$Z_\delta \cap -qZ_\delta = \emptyset. \quad (5.5)$$

$$Z_\lambda \cap -qZ_\lambda = \emptyset. \quad (5.6)$$

$$-qZ_\lambda \cap Z_\delta = C_1. \quad (5.7)$$

$$Z_\lambda \cap -qZ_\delta = C_{-q}. \quad (5.8)$$

Lemma 5.5'ten (5.5) eşitliğinin sağlandığı görülür. $Z_\lambda \cap -qZ_\lambda \neq \emptyset$ olsun. Bu durumda $-q(1+4i) \equiv 1+4j \pmod{rn}$ denkleğini sağlayan bazı $-\frac{q+1}{4} - \lambda \leq i, j \leq -\frac{q+1}{4}$ tamsayıları vardır. $-q(1+4i) \equiv 1+4j \pmod{rn}$ denkliği $\frac{q+1}{4} + qi + j \equiv 0 \pmod{n}$ denkleğini gerektirir. $-\frac{q-1}{2} \leq -\frac{q+1}{4} - \lambda \leq i, j \leq -\frac{q+1}{4}$ eşitsizliğinden $-\frac{q^2-1}{2} + \frac{q+1}{4} \leq \frac{q+1}{4} + qi + j \leq -\frac{(q+1)^2}{4} + \frac{q+1}{4}$ eşitsizliği vardır. Bu durumda $-2n < -\frac{q^2-1}{2} + \frac{q+1}{4} \leq \frac{q+1}{4} + qi + j \leq -\frac{(q+1)^2}{4} + \frac{q+1}{4} < -n$ eşitsizliği $\frac{q+1}{4} + qi + j \equiv 0 \pmod{n}$ denkliği ile çelişir ve dolayısıyla (5.6) eşitliği sağlanır. (5.7) eşitliğinin ispatı için $-\frac{q-3}{4} \leq j \leq \delta$ olmak üzere $-q(1+4i) \equiv 1+4j \pmod{rn}$ ya da denk olarak $\frac{q+1}{4} + qi + j \equiv 0 \pmod{n}$ denkleğini sağlayan $-\frac{q+1}{4} - \lambda \leq i \leq -\frac{q+1}{4}$ tamsayısı ya da tamsayıları sayılacaktır. $-\frac{q-1}{2} \leq -\frac{q+1}{4} - \lambda \leq i \leq -\frac{q+1}{4}$ ve $-\frac{q-3}{4} \leq j \leq \delta \leq \frac{q-3}{2}$ eşitsizliklerinden $\frac{-q^2+q+2}{2} \leq \frac{q+1}{4} + qi + j \leq \frac{-q^2+2q-5}{4}$ elde edilir. $-2n < \frac{-q^2+q+2}{2}$ ve $\frac{-q^2+2q-5}{4} < 0$ olduğundan $\frac{q+1}{4} + qi + j$ sadece $-n$ olabilir. Bu durumda $\frac{q+1}{4} + qi + j = -n$ eşitliğinden $j \equiv 0 \pmod{q}$ elde edilir. $-\frac{q-3}{4} \leq j \leq \delta \leq \frac{q-3}{2}$ olduğundan $j = 0$ ve dolayısıyla $i = -\frac{q+1}{4}$ olur. O zaman (5.7) eşitliği sağlanır. Ayrıca, $Z_\lambda \cap -qZ_\delta = -q(-qZ_\lambda \cap Z_\delta) = -qC_1 = C_{-q}$ olduğundan (5.8) eşitliği de ispatlanmış olur. Sonuç olarak $|Z_{\lambda,\delta} \cap -qZ_{\lambda,\delta}| = 2$ elde edilir.

Her $0 \leq \lambda \leq \frac{q-3}{4}$ ve $0 \leq \delta \leq \frac{q-3}{2}$ tamsayıları için $\mathcal{C}_{\lambda,\delta}$, $\mathbb{F}_{q^2}$ üzerinde $\frac{q^2-1}{4}$ uzunluklu $Z_{\lambda,\delta}$ tanımlayıcı kümesine sahip α -sabit devirli kod olsun. Bu durumda $\mathcal{C}_{\lambda,\delta}$, $d = \frac{q+9}{4} + \lambda + \delta$ olmak üzere $\left[\frac{q^2-1}{4}, \frac{q^2-1}{4} - d + 1, d\right]_{q^2}$ parametrelili bir koddur. $|Z_{\lambda,\delta} \cap -qZ_{\lambda,\delta}| = 2$ olduğundan Teorem 2.11 ve Önerme 5.1'den istenen parametrelere sahip dolaşık destekli kuantum MDS kodlar vardır. ■

Teorem 5.7 ile elde edilen bazı dolaşık destekli kuantum MDS kodlar Tablo 5.3'de verilmiştir.

Lemma 5.8. $m \geq 1$ olmak üzere $q = 4m+3$ bir asal kuvveti, $n = \frac{q^2-1}{4}$ ve $r = 4$ olsun. Bu durumda $\text{mod } rn$ 'ye göre C_{q-2} ve C_{2q-1} q^2 -devirsel kosetleri için $-qC_{q-2} = C_{2q-1}$ eşitliği sağlanır.

Teorem 5.9. $m \geq 1$ olsun. $q = 4m+3$ asal kuvveti olmak üzere her $\frac{3q+7}{4} \leq d \leq$

Tablo 5.3 Teorem 5.7 ile elde edilen bazı dolaşık destekli kuantum MDS kodların parametreleri

q	n	$\llbracket n, k, d; c \rrbracket_q$	d
7	12	$\llbracket 12, 16 - 2d, d; 2 \rrbracket_7$	$4 \leq d \leq 7$
11	30	$\llbracket 30, 34 - 2d, d; 2 \rrbracket_{11}$	$5 \leq d \leq 11$
19	90	$\llbracket 90, 94 - 2d, d; 2 \rrbracket_{19}$	$7 \leq d \leq 19$
23	132	$\llbracket 132, 136 - 2d, d; 2 \rrbracket_{23}$	$8 \leq d \leq 23$
27	182	$\llbracket 182, 186 - 2d, d; 2 \rrbracket_{27}$	$9 \leq d \leq 27$
31	240	$\llbracket 240, 244 - 2d, d; 2 \rrbracket_{31}$	$10 \leq d \leq 31$

$\frac{5q+1}{4}$ tamsayısı için $\llbracket \frac{q^2-1}{4}, \frac{q^2-1}{4} - 2d + 6, d; 4 \rrbracket_q$ parametrelerine sahip bir dolaşık destekli kuantum MDS kod vardır.

İspat. Her $0 \leq \lambda, \delta \leq \frac{q-3}{4}$ için $Z_{\lambda, \delta} = \bigcup_{j=-\frac{q+1}{4}-\lambda}^{\frac{q+1}{2}+\delta} C_{1+4j}$, $Z_\lambda = \bigcup_{j=-\frac{q+1}{4}-\lambda}^{-\frac{q+1}{4}} C_{1+4j}$ ve $Z_\delta = \bigcup_{j=-\frac{q-3}{4}}^{\frac{q+1}{2}+\delta} C_{1+4j}$ kümeleri tanımlansın. $Z_{\lambda, \delta} = Z_\lambda \cup Z_\delta$ olduğundan $Z_{\lambda, \delta} \cap -qZ_{\lambda, \delta} = (Z_\lambda \cup Z_\delta) \cap (-qZ_\lambda \cup -qZ_\delta) = (Z_\lambda \cap -qZ_\lambda) \cup (Z_\lambda \cap -qZ_\delta) \cup (Z_\delta \cap -qZ_\lambda) \cup (Z_\delta \cap -qZ_\delta)$ elde edilir. $|Z_{\lambda, \delta} \cap -qZ_{\lambda, \delta}| = 4$ eşitliğini elde etmek için aşağıdaki eşitlikleri ispatlamak yeterlidir.

$$Z_\lambda \cap -qZ_\lambda = \emptyset. \quad (5.9)$$

$$-qZ_\lambda \cap Z_\delta = C_1. \quad (5.10)$$

$$Z_\lambda \cap -qZ_\delta = C_{-q}. \quad (5.11)$$

$$Z_\delta \cap -qZ_\delta = C_{q-2} \cup C_{2q-1}. \quad (5.12)$$

(5.6) eşitliğinin (5.9) eşitliğini sağladığı görülür. (5.10) ispatı için $-\frac{q+1}{4}-\lambda \leq i \leq -\frac{q-1}{4}$ olmak üzere $-q(1+4i) \equiv 1+4j \pmod{rn}$ ya da denk olarak $\frac{q+1}{4} + qi + j \equiv 0 \pmod{n}$ denkleğini sağlayan $-\frac{q-3}{4} \leq j \leq \frac{q-1}{2} + \delta$ tamsayısı ya da tamsayıları sayılacaktır. $-\frac{q-1}{2} \leq -\frac{q+1}{4} - \lambda \leq i \leq -\frac{q-1}{4}$ ve $-\frac{q-3}{4} \leq j \leq \frac{q-1}{2} + \delta \leq \frac{3q-5}{4}$ eşitsizliklerinden $-\frac{q^2-q-2}{2} \leq \frac{q+1}{4} + qi + j \leq -\frac{q^2-3q+4}{4}$ elde edilir. $-2n < -\frac{q^2-q-2}{2}$ ve $-\frac{q^2-3q+4}{4} < 0$ olduğundan $\frac{q+1}{4} + qi + j$ sadece $-n$ olabilir. Bu durumda $\frac{q+1}{4} + qi + j = -n$ eşitliğinden $j \equiv 0 \pmod{q}$ elde edilir. $-\frac{q-3}{4} \leq j \leq \frac{3q-5}{4}$ olduğundan $j = 0$ ve dolayısıyla (5.10) eşitliği sağlanır. Ayrıca, $Z_\lambda \cap -qZ_\delta = -q(-qZ_\lambda \cap Z_\delta) = -qC_1 = C_{-q}$ olduğundan (5.11) eşitliği de ispatlanmış olur. (5.12) eşitliğinin ispatı için $-\frac{q-3}{4} \leq i \leq \frac{q-1}{2} + \delta$ olmak üzere $-q(1+4i) \equiv 1+4j \pmod{rn}$ ya da denk olarak $\frac{q+1}{4} + qi + j \equiv 0 \pmod{n}$ denkleğini sağlayan $-\frac{q-3}{4} \leq j \leq \frac{q-1}{2} + \delta$ tamsayısı ya da tamsayıları sayılacaktır. $-\frac{q-3}{4} \leq i, j \leq \frac{q-1}{2} + \delta \leq \frac{3q-5}{4}$ eşitsizliğinden $-n < -\frac{q^2-3q-4}{2} \leq \frac{q+1}{4} + qi + j \leq \frac{3q^2-q-4}{4} < 3n$ elde edilir. Bu durumda $\frac{q+1}{4} + qi + j$ nin

mümkün değerleri 0, n ve $2n$ tamsayılarıdır.

1. $\frac{q+1}{4} + qi + j = 0$ ise $4j + 1 \equiv 0 \pmod{q}$ olur. $-q < -q + 4 \leq 4j + 1 \leq 3q - 4 < 3q$ olduğundan $4j + 1$ in mümkün değerleri 0, q ve $2q$ dür. Bu ise $q \equiv 3 \pmod{4}$ ve j bir tamsayı olduğundan bir çelişkidir.
2. $\frac{q+1}{4} + qi + j = n$ ise $4j + 2 \equiv 0 \pmod{q}$ olur. $-q < -q + 5 \leq 4j + 2 \leq 3q - 3 < 3q$ olduğundan $4j + 2$ nin mümkün değerleri 0, q ve $2q$ dür. $q \equiv 3 \pmod{4}$ ve j bir tamsayı olduğundan $4j + 2 = 2q$ dür. Buradan $j = \frac{q-1}{2}$ ve $i = \frac{q-3}{4}$ elde edilir.
3. $\frac{q+1}{4} + qi + j = 2n$ ise $4j + 3 \equiv 0 \pmod{q}$ olur. $-q < -q + 6 \leq 4j + 3 \leq 3q - 2 < 3q$ olduğundan $4j + 3$ ün mümkün değerleri 0, q ve $2q$ dür. $q \equiv 3 \pmod{4}$ ve j bir tamsayı olduğundan $4j + 3 = q$ dür. Buradan $j = \frac{q-3}{4}$ ve $i = \frac{q-1}{2}$ elde edilir.

C_{q-2} ve C_{2q-1} $\frac{q+1}{4} + qi + j$ nin mümkün durumlarından $Z_\delta \cap -qZ_\delta = C_{q-2} \cup C_{2q-1}$ elde edilir ve dolayısıyla (5.12) eşitliği sağlanır. Sonuç olarak $|Z_{\lambda,\delta} \cap -qZ_{\lambda,\delta}| = 4$ 'tür.

Her $0 \leq \lambda, \delta \leq \frac{q-3}{4}$ tamsayıları için $\mathcal{C}_{\lambda,\delta}$, $\mathbb{F}_{q^2}$ üzerinde $\frac{q^2-1}{4}$ uzunluklu $Z_{\lambda,\delta}$ tanımlayıcı kümesine sahip α -sabit devirli kod olsun. Bu durumda $\mathcal{C}_{\lambda,\delta}$, $d = \frac{3q+7}{4} + \lambda + \delta$ olmak üzere $\left[\frac{q^2-1}{4}, \frac{q^2-1}{4} - d + 1, d \right]_{q^2}$ parametrelili bir koddur. $|Z_{\lambda,\delta} \cap -qZ_{\lambda,\delta}| = 4$ olduğundan Teorem 2.11 ve Önerme 5.1'den istenen parametrelere sahip dolaşık destekli kuantum MDS kodlar vardır. ■

Örnek 5.2. $q = 7$ ve $r = 4$ olsun. Bu durumda $n = 12$ olur ve $49 \equiv 1 \pmod{48}$ olduğundan $0 \leq j \leq 11$ için $1 + 4j$ 'yi içeren mod48'e göre 49-devirsel kosetler aşağıdaki gibidir.

$$\begin{aligned}
 j &= 0, & C_1 &= \{1\} \\
 j &= 1, & C_5 &= \{5\} \\
 j &= 2, & C_9 &= \{9\} \\
 j &= 3, & C_{13} &= \{13\} \\
 j &= 4, & C_{17} &= \{17\} \\
 j &= 5, & C_{21} &= \{21\} \\
 j &= 6, & C_{25} &= \{25\} \\
 j &= 7, & C_{29} &= \{29\} \\
 j &= 8, & C_{33} &= \{33\} \\
 j &= 9, & C_{37} &= \{37\} \\
 j &= 10, & C_{41} &= \{41\} \\
 j &= 11, & C_{45} &= \{45\}
 \end{aligned}$$

Ayrıca aşağıdaki eşitlikler sağlanır.

$$\begin{aligned}
-7C_1 &= C_{41} \\
-7C_5 &= C_{13} \\
-7C_9 &= C_{33} \\
-7C_{13} &= C_5 \\
-7C_{17} &= C_{25} \\
-7C_{21} &= C_{45} \\
-7C_{25} &= C_{17} \\
-7C_{29} &= C_{37} \\
-7C_{33} &= C_9 \\
-7C_{37} &= C_{29} \\
-7C_{41} &= C_1 \\
-7C_{45} &= C_{21}
\end{aligned}$$

Burada her $0 \leq \lambda, \delta \leq 1$ tamsayıları için $Z_{\lambda, \delta} = \bigcup_{j=-2-\lambda}^{4+\delta} C_{1+4j}$ olmak üzere $|Z_{\lambda, \delta} \cap -qZ_{\lambda, \delta}| = 4$ olduğu görülür. $\mathcal{C}_{\lambda, \delta}$, $\mathbb{F}_{49}$ üzerinde 12 uzunluğunda $Z_{\lambda, \delta}$ tanımlayıcı kümesine sahip bir α -sabit devirli kod olsun. Bu durumda $\mathcal{C}_{\lambda, \delta}$, $d = 7 + \lambda + \delta$ olmak üzere $[12, 12 - d + 1, d]_{49}$ parametrelili bir koddur. Her $0 \leq \lambda, \delta \leq 1$ tamsayıları için $|Z_{\lambda, \delta} \cap -qZ_{\lambda, \delta}| = 4$ olduğundan $[[12, 18 - 2d, d; 4]]_7$, $7 \leq d \leq 9$ parametrelerine sahip dolaşık destekli kuantum MDS kodların bir ailesi vardır.

Teorem 5.9 ile elde edilen bazı dolaşık destekli kuantum MDS kodlar Tablo 5.4’de verilmiştir.

Tablo 5.4 Teorem 5.9 ile elde edilen bazı dolaşık destekli kuantum MDS kodların parametreleri

q	n	$[[n, k, d; c]]_q$	d
7	12	$[[12, 18 - 2d, d; 4]]_7$	$7 \leq d \leq 9$
11	30	$[[30, 36 - 2d, d; 4]]_{11}$	$10 \leq d \leq 14$
19	90	$[[90, 96 - 2d, d; 4]]_{19}$	$16 \leq d \leq 24$
23	132	$[[132, 138 - 2d, d; 4]]_{23}$	$19 \leq d \leq 29$
27	182	$[[182, 188 - 2d, d; 4]]_{27}$	$22 \leq d \leq 34$
31	240	$[[240, 246 - 2d, d; 4]]_{31}$	$25 \leq d \leq 39$

5.3 Kıyaslama

[13]'te $\frac{q^2-1}{4}$ uzunluklu kuantum MDS kodlar elde edilmiştir. Bölüm 5.2'de elde edilen $\frac{q^2-1}{4}$ uzunluklu dolaşık destekli kuantum MDS kodların minimum uzaklıkları dolayısıyla hata düzeltme kapasiteleri [13]'te inşa edilen kuantum MDS kodların minimum uzaklıklarından daha yüksektir. Tablo 5.5 bu kıyaslamayı göstermektedir. Örneğin, $q = 7$ için [13]'e göre $[[12, 8, 3]]_7$, $[[12, 6, 4]]_7$ ve $[[12, 4, 5]]_7$ kuantum MDS kodları inşa edilirken Teorem 5.7'ye göre aynı uzunluk ve boyutlara sahip $[[12, 8, 4; 2]]_7$, $[[12, 6, 5; 2]]_7$ ve $[[12, 4, 6; 2]]_7$ dolaşık destekli kuantum MDS kodlar elde edilir.

Tablo 5.5 [13]'te elde edilen kuantum MDS kodlar ile Bölüm 5.2'de elde edilen dolaşık destekli kuantum MDS kodların bir kıyaslaması

Dolaşık destekli kuantum MDS kod	Kuantum MDS kod	referans
$[[\frac{q^2-1}{4}, \frac{q^2-1}{4} - 2d + 4, d; 2]]_q$ $\frac{q+9}{4} \leq d \leq q$ $q \equiv 3 \pmod{4}, q > 3$	$[[\frac{q^2-1}{4}, \frac{q^2-1}{4} - 2d + 2, d]]_q$ $2 \leq d \leq \frac{3q-1}{4}$	[13]
$[[\frac{q^2-1}{4}, \frac{q^2-1}{4} - 2d + 6, d; 4]]_q$ $\frac{3q+7}{4} \leq d \leq \frac{5q+1}{4}$ $q \equiv 3 \pmod{4}, q > 3$	$[[\frac{q^2-1}{4}, \frac{q^2-1}{4} - 2d + 2, d]]_q$ $2 \leq d \leq \frac{3q-1}{4}$	[13]

Öte yandan Bölüm 5.2'de elde edilen dolaşık destekli kuantum MDS kodlar [24]'te elde edilen dolaşık destekli kuantum MDS kodları içerir ve dolayısıyla daha geniş bir sınıftır. Tablo 5.6'da bu kıyaslama yapılmıştır. Örneğin, $q = 11$ için [24]'e göre $[[30, 34 - 2d, d; 2]]_{11}$, $9 \leq d \leq 11$ ve $[[30, 36 - 2d, d; 4]]_{11}$, $12 \leq d \leq 14$ dolaşık destekli kuantum MDS kodlar inşa edilirken Teorem 5.7 ve Teorem 5.9'a göre aynı uzunluk için daha geniş sınıf olan $[[30, 34 - 2d, d; 2]]_{11}$, $5 \leq d \leq 11$ ve $[[30, 36 - 2d, d; 4]]_{11}$, $10 \leq d \leq 14$ dolaşık destekli kuantum MDS kodları elde edilir.

Tablo 5.6 [24]'te ve Bölüm 5.2'de elde edilen dolaşık destekli kuantum MDS kodların bir kıyaslaması

Dolaşık destekli kuantum MDS kod	Bu çalışma	[24]
$[[\frac{q^2-1}{4}, \frac{q^2-1}{4} - 2d + 4, d; 2]]_q$	$\frac{q+9}{4} \leq d \leq q$	$\frac{3(q+1)}{4} \leq d \leq q$
$[[\frac{q^2-1}{4}, \frac{q^2-1}{4} - 2d + 6, d; 4]]_q$	$\frac{3q+7}{4} \leq d \leq \frac{5q+1}{4}$	$q + 1 \leq d \leq \frac{5q+1}{4}$

6 Sonuç ve Öneriler

Bu tez çalışmasında sabit devirli kodların cebirsel yapılarından faydalanarak kuantum MDS kodlar ve dolaşık destekli kuantum MDS kodlar inşa edilmiştir. Sabit devirli kodların özel bir sınıfı olan devirli kodlar kullanılarak literatürde var olan kuantum kodların parametreleri iyileştirilmiş ve kuantum MDS kodların bir sınıfı yeniden inşa edilmiştir. Sabit devirli kodların tanımlayıcı kümeleri üzerine çalışılmış ve kuantum kodlar için Hermityen inşası ile $\frac{q^2+1}{13}$ ve $\frac{q^2+1}{17}$ uzunluklu kuantum MDS kodlar için ayrı bir inşa verilmiştir. Sabit devirli kodlardan $q \equiv 3 \pmod{4}$ denkleğini sağlayan tek asal kuvveti q için $q^2 + 1$ uzunluklu yeni dolaşık destekli kuantum MDS kodlar elde edilmiş ve bazılarının parametreleri tablolandırılmıştır. Ayrıca, $\frac{q^2-1}{4}$ uzunluklu dolaşık destekli kuantum MDS kodlar türetilmiş ve literatürde var olan kuantum kodlarla kıyaslaması yapılarak onlardan daha iyi parametrelere sahip olduğu gösterilmiştir.

Daha iyi parametrelili kuantum kod bulma veya yeni kuantum kod bulma problemi her zaman açık problemdir. Bir kuantum MDS kodun uzunluğunun $q^2 + 1$ 'den daha fazla olamayacağı gösterilmiştir [6]. Dolayısıyla lineer kodların sabit devirli kod ailesi dışında diğer sınıflarından da yararlanarak uzunluğu $q^2 + 1$ ve $q^2 + 1$ 'den daha küçük olmak üzere yeni kuantum MDS kodlar bulmak ilgi çekici bir problemdir. Ayrıca hem maksimum dolaşıklı hem de maksimum uzaklığa ayrışabilme şartını sağlayan yeni dolaşık destekli kuantum kodlar inşa etmek diğer bir problemdir.

- [1] P. W. Shor, "Scheme for reducing decoherence in quantum memory," *Physical Review A*, vol. 52, no. 4, p. 2493, 1995.
- [2] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. Sloane, "Quantum error correction via codes over $gf(4)$," *IEEE Transactions on Information Theory*, vol. 44, no. 4, pp. 1369–1387, 1998.
- [3] A. M. Steane, "Enlargement of calderbank-shor-steane quantum codes," *IEEE Transactions on Information Theory*, vol. 45, no. 7, pp. 2492–2495, 1999.
- [4] D. Gottesman, "Stabilizer codes and quantum error correction," 1997, caltech ph. d," PhD thesis, eprint: quant-ph/9705052.
- [5] A. Ashikhmin and E. Knill, "Nonbinary quantum stabilizer codes," *IEEE Transactions on Information Theory*, vol. 47, no. 7, pp. 3065–3072, 2001.
- [6] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli, "Nonbinary stabilizer codes over finite fields," *IEEE Transactions on Information Theory*, vol. 52, no. 11, pp. 4892–4914, 2006.
- [7] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli, "On quantum and classical bch codes," *IEEE Transactions on Information Theory*, vol. 53, no. 3, pp. 1183–1188, 2007.
- [8] L. Jin, S. Ling, J. Luo, and C. Xing, "Application of classical hermitian self-orthogonal mds codes to quantum mds codes," *IEEE Transactions on Information Theory*, vol. 56, no. 9, pp. 4735–4740, 2010.
- [9] G. G. La Guardia, "New quantum mds codes," *IEEE Transactions on Information Theory*, vol. 57, no. 8, pp. 5551–5554, 2011.
- [10] X. Kai and S. Zhu, "New quantum mds codes from negacyclic codes," *IEEE Transactions on Information Theory*, vol. 59, no. 2, pp. 1193–1197, 2013.
- [11] X. Kai, S. Zhu, and P. Li, "Constacyclic codes and some new quantum mds codes," *IEEE Transactions on Information Theory*, vol. 60, no. 4, pp. 2080–2086, 2014.
- [12] L. Jin and C. Xing, "A construction of new quantum mds codes," *IEEE Transactions on Information Theory*, vol. 60, no. 5, pp. 2921–2925, 2014.
- [13] G. Zhang and B. Chen, "New quantum mds codes," *International Journal of Quantum Information*, vol. 12, no. 04, p. 1450019, 2014.
- [14] L. Wang and S. Zhu, "New quantum mds codes derived from constacyclic codes," *Quantum Information Processing*, vol. 14, no. 3, pp. 881–889, 2015.
- [15] S. Li, M. Xiong, and G. Ge, "Pseudo-cyclic codes and the construction of quantum mds codes," *IEEE Transactions on Information Theory*, vol. 62, no. 4, pp. 1703–1710, 2016.

- [16] L. Hu, Q. Yue, and X. Zhu, "New quantum mds code from constacyclic codes," *Chinese Annals of Mathematics, Series B*, vol. 37, no. 6, pp. 891–898, 2016.
- [17] J. Qian and L. Zhang, "Improved constructions for quantum maximum distance separable codes," *Quantum Information Processing*, vol. 16, no. 1, p. 20, 2017.
- [18] L. Jin, H. Kan, and J. Wen, "Quantum mds codes with relatively large minimum distance from hermitian self-orthogonal codes," *Designs, Codes and Cryptography*, vol. 84, no. 3, pp. 463–471, 2017.
- [19] X. Shi, Q. Yue, and Y. Chang, "Some quantum mds codes with large minimum distance from generalized reed-solomon codes," *Cryptography and Communications*, vol. 10, no. 6, pp. 1165–1182, 2018.
- [20] W. Fang and F.-W. Fu, "Two new classes of quantum mds codes," *Finite Fields and Their Applications*, vol. 53, pp. 85–98, 2018.
- [21] G. Guo, R. Li, and L. Guo, "On the construction of quantum mds codes," *International Journal of Theoretical Physics*, vol. 57, no. 11, pp. 3525–3539, 2018.
- [22] T. Brun, I. Devetak, and M.-H. Hsieh, "Correcting quantum errors with entanglement," *Science*, vol. 314, no. 5798, pp. 436–439, 2006.
- [23] J. Chen, Y. Huang, C. Feng, and R. Chen, "Entanglement-assisted quantum mds codes constructed from negacyclic codes," *Quantum Information Processing*, vol. 16, no. 12, p. 303, 2017.
- [24] Y. Liu, R. Li, L. Lv, and Y. Ma, "Application of constacyclic codes to entanglement-assisted quantum maximum distance separable codes," *Quantum Information Processing*, vol. 17, no. 8, p. 210, 2018.
- [25] J. Qian and L. Zhang, "On mds linear complementary dual codes and entanglement-assisted quantum codes," *Designs, Codes and Cryptography*, vol. 86, no. 7, pp. 1565–1572, 2018.
- [26] J. Fan, H. Chen, and J. Xu, "Constructions of q -ary entanglement-assisted quantum mds codes with minimum distance greater than $q+1$," *Quantum Information and Computation*, vol. 16, no. 5–6, pp. 0423–0434, 2016.
- [27] K. Guenda, S. Jitman, and T. A. Gulliver, "Constructions of good entanglement-assisted quantum error correcting codes," *Designs, Codes and Cryptography*, vol. 86, no. 1, pp. 121–136, 2018.
- [28] L. Lu, R. Li, L. Guo, Y. Ma, and Y. Liu, "Entanglement-assisted quantum mds codes from negacyclic codes," *Quantum Information Processing*, vol. 17, no. 3, p. 69, 2018.
- [29] M. E. K ro glu, "New entanglement-assisted mds quantum codes from constacyclic codes," *Quantum Information Processing*, vol. 18, no. 2, p. 44, 2019.
- [30] M. M. Wilde and T. A. Brun, "Optimal entanglement formulas for entanglement-assisted quantum coding," *Physical Review A*, vol. 77, no. 6, p. 064302, 2008.
- [31] R.-H. Li, F. Zuo, and Y. Liu, "A study of skew symmetric q^2 -cyclotomic coset and its application," *Journal of Air Force Engineering University (Natural Science Edition)*, no. 1, p. 20, 2011.

- [32] C. E. Shannon, "A mathematical theory of communication," *Bell system technical journal*, vol. 27, no. 3, pp. 379–423, 1948.
- [33] S. Ling and C. Xing, *Coding theory: a first course*. Cambridge University Press, 2004.
- [34] R. W. Hamming, "Error detecting and error correcting codes," *The Bell system technical journal*, vol. 29, no. 2, pp. 147–160, 1950.
- [35] E. Berlekamp, *Algebraic Coding Theory (Revised Edition)*. World Scientific Publishing Co. Pte. Ltd., 2015.
- [36] A. Krishna and D. V. Sarwate, "Pseudocyclic maximum-distance-separable codes," *IEEE transactions on information theory*, vol. 36, no. 4, pp. 880–884, 1990.
- [37] N. Aydın, İ. Şiap, and D. K. Ray-Chaudhuri, "The structure of 1-generator quasi-twisted codes and new linear codes," *Designs, Codes and Cryptography*, vol. 24, no. 3, pp. 313–326, 2001.
- [38] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.
- [39] C.-Y. Lai and T. A. Brun, "Entanglement increases the error-correcting ability of quantum error-correcting codes," *Physical Review A*, vol. 88, no. 1, p. 012 320, 2013.
- [40] T. A. Brun, I. Devetak, and M.-H. Hsieh, "Catalytic quantum error correction," *IEEE Transactions on Information Theory*, vol. 60, no. 6, pp. 3073–3089, 2014.
- [41] G. G. La Guardia, "Quantum codes derived from cyclic codes," *International Journal of Theoretical Physics*, vol. 56, no. 8, pp. 2479–2484, 2017.
- [42] J. Gao and Y. Wang, "Quantum codes derived from negacyclic codes," *International Journal of Theoretical Physics*, vol. 57, no. 3, pp. 682–686, 2018.

Tezden Üretilmiş Yayınlar

İletişim Bilgileri: mustafasar7@gmail.com

Makale

1. M. Sarı, E. Kolotoğlu, "An application of constacyclic codes to entanglement-assisted quantum mds codes", Computational&Applied Mathematics, vol. 38, no. 2, p. 75, 2019.
2. E. Kolotoğlu, M. Sarı, "Quantum codes with improved minimum distance", Bulletin of Korean Mathematical Society, vol. 56, no. 3, p. 609-619, 2019.

Konferans Bildirisi

1. M. Sarı, E. Kolotoğlu, "An application of constacyclic codes to entanglement-assisted quantum mds codes", International Conference on Mathematics and Mathematics Education (ICMME 2018), ORDU, TÜRKİYE, 27-29 Haziran 2018.