

**T.C.
YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ**

KLASİK LİNEER KODLARDAN KUANTUM KOD ELDE ETME

MUSTAFA SARI

**YÜKSEK LİSANS TEZİ
MATEMATİK ANABİLİM DALI
MATEMATİK PROGRAMI**

**DANIŞMAN
PROF. DR. İRFAN ŞİAP**

İSTANBUL, 2013

T.C.
YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

KLASİK LİNEER KODLARDAN KUANTUM KOD ELDE ETME

Mustafa SARI tarafından hazırlanan tez çalışması 25.07.2013 tarihinde aşağıdaki jüri tarafından Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalı'nda **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Tez Danışmanı

Prof. Dr. İrfan ŞİAP
Yıldız Teknik Üniversitesi

Jüri Üyeleri

Prof. Dr. İrfan ŞİAP
Yıldız Teknik Üniversitesi



Doç. Dr. Bahattin YILDIZ
Fatih Üniversitesi



Doç. Dr. Bayram Ali ERSOY
Yıldız Teknik Üniversitesi



ÖNSÖZ

Yüksek lisans boyunca maddi ve manevi her türlü desteklerini gördüğüm sevgili aileme teşekkürü kendime bir borç bilirim.

Bu tezin hazırlanmasında hiçbir yardımını esirgemeyen saygıdeğer hocam Prof. Dr. İrfan ŞİAP'a şükranlarımı sunarım.

Tez jüriliğinde yer alan Doç. Dr. Bahattin YILDIZ'a ve Doç. Dr. Bayram Ali ERSOY'a yapıcı katkılarından dolayı teşekkür ederim.

Yardımlarından dolayı Yrd. Doç. Dr. Murat GÜZELTEPE'ye ve özellikle tezin yazımında çok yardımı bulunan Arş. Gör. Mehmet Emin KÖROĞLU'na ayrıca teşekkür ederim.

Ağustos, 2013

Mustafa SARI

İÇİNDEKİLER

	Sayfa
SİMGE LİSTESİ.....	vi
KISALTMA LİSTESİ.....	viii
TABLO LİSTESİ	ix
ÖZET	x
ABSTRACT	xi
BÖLÜM 1.....	1
GİRİŞ	1
1.1 Literatür Özeti	1
1.2 Tezin Amacı	2
1.3 Hipotez	2
BÖLÜM 2.....	3
TEMEL TANIMLAR.....	3
2.1 Bazı Cebirsel Tanımlar	3
2.2 Klasik Kodlarla İle İlgili Temel Bilgiler	8
BÖLÜM 3.....	23
KUANTUM HATA DÜZELTEN KODLARA GİRİŞ	23
3.1 Dirac Notasyonu ve Hilbert Uzayı Üzerinde Lineer Cebir.....	23
3.2 Kubitler	32
3.3 Kuantum Mantık Kapıları.....	33
3.4 Kuantum Hata Düzeltme	36

BÖLÜM 4.....	44
CSS KOD	44
4.1 CSS Kod İnşası	44
4.2 CSS Kuantum Kodlarda Dekodlama	46
4.3 Klasik Lineer Kodlardan CSS Kod İnşası İle Kuantum Kod Elde Etme	49
BÖLÜM 5.....	54
STABİLİZER KODLAR.....	54
5.1 Stabilizer Kuantum Kod	54
5.2 Stabilizer Kodlarda Dekodlama	58
5.3 Klasik Lineer Kodlardan Stabilizer Kodun Kontrol Matrisi Yardımıyla Kuantum Kod Elde Etme	66
BÖLÜM 6.....	70
SONUÇ VE ÖNERİLER	71
KAYNAKLAR.....	72
ÖZGEÇMİŞ.....	75

SİMGE LİSTESİ

$\emptyset$	Boş küme
$\mathbb{Z}$	Tam sayılar kümesi
$\mathbb{R}$	Reel sayılar kümesi
$GL(n, \mathbb{R})$	Reel bileşenli determinantları sıfırdan farklı $n \times n$ tipindeki kare matrislerin kümesi
$\langle S \rangle$	S kümesi ile üretilen grup
$\mathbb{Z}_p$	Tam sayıların p ile bölümünden kalan sınıfı
$\mathbb{Z}_p^*$	$\mathbb{Z}_p - \{0\}$
$Z(G)$	G grubunun merkezleştiricisi
$N(G)$	G grubunun normalleştiricisi
$ C $	C kodun eleman sayısı
$d(x, y)$	x ile y vektörleri arasındaki uzaklık
(n, M)	n uzunluğunda M elemanlı kod
(n, M, d)	n uzunluğunda M elemanlı d minimum uzaklığa sahip kod
F_q	q elemanlı cisim
F_q^n	F_q üzerinde n boyutlu vektör uzayı
$C^\perp$	C kodun duali
$C \leq F_q^n$	n uzunluklu lineer kod
$[n, k]$	n uzunluğunda k boyutlu lineer kod
$[n, k, d]$	n uzunluğunda k boyutlu d minimum uzaklığa sahip lineer kod
$\text{boy}(C)$	C kodun boyutu
$\text{wt}(C)$	C kodun minimum ağırlığı
$d(C)$	C kodun minimum uzaklığı
$S(w)$	w sözün sendromu
$F_q[x]$	Katsayıları F_q cisminden olan polinom halkası
$C = \langle g(x) \rangle$	$g(x)$ ile üretilen C devirli kodu
$(n, q) = 1$	n ile q aralarında asal
$M^{(i)}(x)$	α^i elemanının minimal polinomu
$ \ \rangle$	Ket vektörü
$\langle \ $	Bra vektörü
$\langle \phi \psi \rangle$	$ \psi\rangle$ ile $ \phi\rangle$ vektörlerinin iç-çarpımı
$ \psi\rangle \langle \phi $	$ \psi\rangle$ ile $ \phi\rangle$ vektörlerinin dış-çarpımı
$H^{\otimes n}$	2^n boyutlu Hilbert vektör uzayı
$A \otimes B$	A ile B matrislerinin tensör çarpımı
$\ \psi\rangle \ $	$ \psi\rangle$ vektörünün normu

$U^\top$	U matrisinin normu
$U^\dagger$	U matrisinin eşlenik transpozu
U^{-1}	U matrisinin tersi
$\text{iz}(T)$	T operatörünün öz değerlerinin toplamı
P_n	n kubite etki eden Pauli matris grubu
$[[n, k]]$	n uzunluğunda k boyutlu kuantum kod
$[[n, k, d]]$	n uzunluğunda k boyutlu d minimum uzaklığa sahip kuantum kod
$[x]$	x sayısından büyük en küçük tamsayı
$\lfloor x \rfloor$	x sayısından küçük en büyük tamsayı
$CSS(C_1, C_2)$	C_1 ve C_2 lineer kodlarından elde edilen Calderbank-Shor-Steane kuantum kod
V_S	S stabilizer grubun sabit bıraktığı kuantum hal uzayı
$C(S)$	S stabilizer grubu ile elde edilen kuantum kod
$gw(x)$	x vektörünün genelleştirilmiş Hamming ağırlığı

KISALTMA LİSTESİ

<i>NOT</i>	Kuantum <i>NOT</i> mantık kapısı
<i>CNOT</i>	Kuantum <i>CNOT</i> mantık kapısı
<i>CSS</i>	Calderbank-Shor-Steane

ÇİZELGE LİSTESİ

	Sayfa
Çizelge 2.1 $[6,3,3]$ lineer kodu için sendrom tablosu	17
Çizelge 5.1 7 kubitli Steane kodun stabilizer grubunun üreteçleri.....	56
Çizelge 5.2 9 kubitli Shor kodun stabilizer grubunun üreteçleri	58
Çizelge 5.3 1 bit hatası düzelten kuantum kod için düzeltilebilen hataların sendromu ve dekodlaması.....	59
Çizelge 5.4 5 kubitli kuantum kod için düzeltilebilen hataların sendromu ve dekodlaması.....	62
Çizelge 5.5 9 kubitli Shor kuantum kodu için sendrom tablosu.....	64

KLASİK LİNEER KODLARDAN KUANTUM KOD ELDE ETME

Mustafa SARI

Matematik Anabilim Dalı

Yüksek Lisans Tezi

Tez Danışmanı: Prof. Dr. İrfan ŞİAP

Günlük hayatta kullanılan bilgisayarlar her ne kadar kapasiteleri günden güne gelişiyor olsa da yine de bazı ihtiyaçları karşılamakta yetersiz kalmaktadır. Örneğin, bir sayıyı asal çarpanlarına ayırma problemi küçük sayılar için kolay çözülebilsen de büyük sayılar (40 basamaklı sayılar gibi) için en iyi bilgisayarlar da bile aylar süren vakit almaktadır. Fakat eğer gerçekleştirilebilirse bir kuantum bilgisayarın aynı problemi sadece birkaç dakika içinde çözebileceği düşünülmektedir. Kuantum mekaniğinin temellerine göre çalışan kuantum bilgisayarlarda kuantum bilginin (kubitin) transferi sırasında oluşabilecek hataları düzeltmek amacıyla kuantum hata düzelten kodlar geliştirilmiştir.

Bu tezde öncelikle kuantum kodları daha iyi anlamak için gerekli olan cebir ve klasik kodlama bilgileri verilmiştir. Üçüncü bölümde kuantum kodlamada çalışılan uzay olan Hilbert uzayı üzerinde lineer cebir bilgileri, kuantum bilgi birimi olan kubitler, kuantum mantık kapıları ve kuantum kodlar için hata farketme ve düzeltme koşullarından bahsedilmiştir. Dördüncü bölümde Calderbank-Shor-Steane kodun yapısı ve BCH kodlardan elde edilen kuantum kodların parametreleri verilmiştir. Beşinci bölümde ise stabilizer kodların yapısı ve belirli şartları sağlayan kontrol matrislerine sahip lineer kodlardan elde edilen kuantum kodların parametreleri verilmiştir.

Anahtar Kelimeler: Hilbert uzay, kubit, hata operatörü, CSS kod, stabilizer kod.

YILDIZ TEKNİK ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ

OBTAINING QUANTUM CODES FROM CLASSICAL LINEAR CODES

Mustafa SARI

Department of Mathematics

MSc. Thesis

Advisor: Prof. Dr. İrfan ŞİAP

Although the capacities of the computers which are being used in daily life have been increased day by day, they are not enough to overcome some problems. For instance, while the problem of factoring a number to its primes is accomplished easily for small numbers, it takes months for higher numbers (like numbers with forty digits) even with the best computers. However, if succeeded, it is believed that a quantum computer can overcome the same problem within just a few minutes. Quantum error correcting codes have been developed in order to correct errors which can happen through transition of quantum information (qubit) in the quantum computers working with respect to principals of quantum mechanic.

In the second section, some topics in algebra and classical coding which are needed to understand quantum coding are given. In the third section, some topics in linear algebra on Hilbert spaces which is studied in quantum coding, qubits which are units of quantum information, quantum logic gates and the conditions of error detection and correction for quantum codes are mentioned. In the fourth section, the structure of Calderbank-Shor-Steane codes and the parameters of quantum codes obtained from BCH codes are given. In the fifth section, the structure of stabilizer codes and the parameters of quantum codes obtained from classical codes which have control matrices satisfying certain conditions are given.

Key words: Hilbert space, qubit, error operator, CSS code, stabilizer code.

1.1 Literatür Özeti

Klasik bilgisayarlarda ve dijital ortamlarda bilgiyi iletme veya bu süreçte bilgide oluşabilecek hataları düzeltebilmek için hata düzelten kodlar geliştirilmiştir. Günümüzde ise klasik bilgisayarların yerine, klasik bilgisayarlara göre çok daha hızlı ve bilgi depolamaya elverişli olan kuantum bilgisayarlar düşünülmektedir. Klasik kodlamada olduğu gibi kuantum bilgiyi depolamak ve kuantum bilgide meydana gelebilecek hataları düzeltmek amacıyla kuantum hata düzelten kodlar üzerine çalışılmaktadır. İlk olarak 1995'te Peter Shor, bir kubit dokuz kubit kodlayarak bir hata düzeltebilen kuantum kodun varlığını gösterdi [1]. 1996'ta Andrew Steane, bir kubit yedi kubit kodlayarak bir hata düzeltebilen kuantum kod elde etti [2]. Yine 1996'da A. R. Calderbank ve Peter Shor, klasik kodlardan kuantum kod elde etmeyi başardılar [3]. Bu çalışmaya göre, kuantum kod elde etmek için dualini içeren klasik lineer kod bulmak yeterli idi. 1997'de Daniel Gottesman, grup teorisinden yararlanarak stabilizer kuantum kod yapısını geliştirdi ve kuantum kodlar için hata düzeltme koşullarını verdi [4]. Stabilizer kuantum kod yapısı, bir kuantum kodun stabilizer grubu ile klasik kodlar arasında geçişi sağladı. 1998'de A. R. Calderbank, E. M. Rains, Peter Shor ve N. S. Sloane, dört elemanlı bir cisim üzerindeki ($GF(4)$) klasik kodlardan kuantum kod elde etme yöntemini verdiler [5]. Bu yöntemle birlikte hata düzeltebilen kuantum kod bulma problemi $GF(4)$ üzerinde kendine dik toplamsal klasik kodlar bulmaya döndü. Daha sonraki yıllarda başka cebirler üzerinde kuantum kodlar elde edildi. [6], [7], [8], [9] nolu makaleler, bu çalışmalardan bazılarıdır.

Hata düzelten kuantum kodlar üzerine de son zamanlarda çok sayıda çalışma yapılmıştır. [3] nolu makaleyi esas alarak yapılan çalışmalardan bazıları [10], [11], [12], [13], [14], [15], [16], [17] dir. Stabilizer kod ve non-stabilizer kod üzerine [18], [33], [20] nolu makalelerde durulmuştur. [20], [21], [22], [23], nolu makalelerde ise $GF(4)$ üzerinde kuantum kod oluşturulmuştur. [24], [25], [26] da kuantum kodların minimum uzaklığını arttırmaya yönelik ve [27], [28] de ise kuantum kodlar için sınır çalışması yapılmıştır.

1.2 Tezin Amacı

Yapılan bu çalışmada bilinen klasik lineer kodlardan kuantum kod elde etme yöntemlerinden bazıları araştırılmış ve öğrenilen bu yöntemlerin yeni bir lineer kod sınıfına uygulanması amaçlanmıştır. Ayrıca bu tezin, kuantum kodlama çalışmak isteyenler için yararlı bir kaynak olması düşünülmüştür.

1.3 Hipotez

Kuantum kodların klasik kodlara göre çok daha üstün özellikleri vardır. Dolayısıyla kuantum kodların kullanıldığı kuantum bilgisayarlar, klasik kodların kullanıldığı günümüz bilgisayarlarından daha üstündür.

TEMEL TANIMLAR

Bu bölümde daha sonraki bölümler için gerekli olan temel tanımlar verilecektir. Bölüm 2.1 de cebirsel tanımlar ve Bölüm 2.2 de ise klasik lineer kodlarla ilgili temel tanımlar verilecektir. Genel olarak [29] ve [30] nolu kaynaklar kullanılacaktır.

2.1 Bazı Cebirsel Tanımlar

Tanım 2.1 $G \neq \emptyset$ bir küme olsun. Eğer $*: G \times G \rightarrow G$ bir fonksiyon ise “*” a G üzerinde bir ikili işlem denir [30].

Tanım 2.2 $G \neq \emptyset$ bir küme ve $*$, G üzerinde bir ikili işlem olsun. Eğer

- i. $\forall a, b, c \in G$ için $a * (b * c) = (a * b) * c$.
- ii. $\forall a \in G$ için $a * e = e * a = a$ olacak şekilde bir $e \in G$ var.
- iii. $\forall a \in G$ için $a * a^{-1} = a^{-1} * a = e$ olacak şekilde $a^{-1} \in G$ var.

aksiyomları sağlanıyorsa $(G, *)$ ikilisine bir grup denir. Burada a^{-1} elemanına, a nın $*$ işlemine göre tersi denir. Eğer her $a, b \in G$ için $a * b = b * a$ ise $(G, *)$ ikilisine değişmeli grup denir [30]. Eğer G bilinen çarpma işlemine göre bir grup ise G ye çarpımsal grup denir ve bu bölümde aksi belirtilmedikçe G bir çarpımsal grup olarak alınacaktır.

Örnek 2.1 $\mathbb{Z}$, $+$ işlemine göre bir değişmeli gruptur.

Örnek 2.2 $GL(n, \mathbb{R})$ $n \times n$ tipinde terslenebilir matrisler kümesi, matrislerde çarpma işlemine göre değişmeli olmayan bir gruptur.

Tanım 2.3 G bir grup ve H , G nin bir alt kümesi olsun. Eğer H , G deki işleme göre bir grup ise H kümesine G nin bir alt grubu denir ve $H \leq G$ ile gösterilir [30].

Teorem 2.1 G bir grup ve H , G nin bir alt kümesi olsun. Bu durumda H ın G nin bir alt grubu olması için gerek ve yeter koşul her $a, b \in H$ için $ab^{-1} \in H$ olmasıdır.

Tanım 2.4 G bir grup ve S , G nin boştan farklı bir alt kümesi olsun. S tarafından üretilen grup $\bigcap_{\substack{H \leq G \\ S \subseteq H}} H$ ile tanımlanır ve $\langle S \rangle$ ile gösterilir. Bu durumda $\langle S \rangle$, G nin bir alt grubudur [30].

Teorem 2.2 G bir grup ve S , G nin boştan farklı bir alt kümesi olsun. Bu durumda

$\langle S \rangle = \{s_1^{e_1} s_2^{e_2} \dots s_n^{e_n} \mid s_i \in S, i = 1, \dots, n, e_i = \pm 1\}$ dir. Eğer $S = \{x\}$ ise $\langle S \rangle = \{x^n, n \in \mathbb{Z}\}$ olur [30].

Tanım 2.5 G bir grup olsun. Eğer bir $x \in G$ için $G = \langle x \rangle$ oluyorsa G ye devirli grup denir [30].

Örnek 2.3 $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$ olduğundan $\mathbb{Z}$ bir devirli gruptur.

Örnek 2.4 $\mathbb{Z}_m = \langle \bar{1} \rangle$ olduğundan $\mathbb{Z}_m$ bir devirli gruptur.

Tanım 2.6 $H \leq G$ ve $a \in G$ olsun. $aH = \{ah, h \in H\}$ ve $Ha = \{ha, h \in H\}$ kümelerine sırasıyla H ın G deki sol ve sağ kosetleri denir [30].

Tanım 2.7 G bir grup ve $H \leq G$ olsun. Eğer her $a \in G$ için $aH = Ha$ oluyorsa H alt grubuna G nin normal alt grubu denir ve $H \triangleleft G$ ile gösterilir [30].

Örnek 2.5 $Z(G) = \{a \in G \mid ag = ga, \forall g \in G\}$ kümesine G nin merkezi denir ve $Z(G) \triangleleft G$ dir.

Örnek 2.6 G bir grup ve $H \leq G$ olsun. $N(H) = \{a \in G \mid aH = Ha\}$ kümesine H ın normalleştiricisi denir ve $N(H) \triangleleft G$ dir.

Tanım 2.8 G bir grup ve $H \triangleleft G$ olsun. $G/H = \{aH \mid a \in G\}$ kümesi $\forall aH, bH \in G/H$ için $(aH)(bH) = abH$ işlemiyle bir gruptur. Bu gruba bölüm grubu denir [30].

Örnek 2.7 $(G = \mathbb{Z}, +)$ ve $(H = 2\mathbb{Z}, +)$ olsun. Bu durumda $G/H = \mathbb{Z}/2\mathbb{Z}$
 $= \{a + 2\mathbb{Z} \mid a \in \mathbb{Z}\} = \{2\mathbb{Z}, 1 + 2\mathbb{Z}\}$ olur.

Tanım 2.9 $(G, *)$ ve $(G_1, *_1)$ birer grup ve $f : G \rightarrow G_1$ bir fonksiyon olsun. Eğer her $a, b \in G$ için $f(a * b) = f(a) *_1 f(b)$ ise f ye G den G_1 e bir homomorfizma denir [30].

Örnek 2.8 $f : \mathbb{Z} \rightarrow \mathbb{Z}_p, a \rightarrow \bar{a}$ şeklinde tanımlanan f fonksiyonu $\mathbb{Z}$ den $\mathbb{Z}_p$ ye bir homomorfizmadır.

Tanım 2.10 $f : G \rightarrow G_1$ bir grup homomorfizması ve e_1, G_1 in birim elemanı olsun. f nin çekirdeği, $\text{Çekf} = \{g \in G, f(g) = e_1\}$ olarak tanımlanır ve $\text{Çekf} \triangleleft G$ dir [30].

Örnek 2.9 $f : \mathbb{Z} \rightarrow \mathbb{Z}_p, a \rightarrow \bar{a}$ etkisiyle bir homomorfizma olsun. Bu durumda $\text{Çekf} = \{a \in \mathbb{Z}, f(a) = \bar{0}\} = \{a \in \mathbb{Z}, a = pk, k \in \mathbb{Z}\} = p\mathbb{Z}$ olur.

Tanım 2.11 $f : G \rightarrow G_1$ bir grup homomorfizması olsun. Eğer f , birebir ve örten ise f homomorfizmasına G den G_1 e bir izomorfizma denir. Bu durumda G ile G_1 birbirlerine izomorfturlar ve kısaca $G \cong G_1$ ile gösterilir [30].

Teorem 2.3 $f : G \rightarrow G_1$ bir grup homomorfizması olsun. Bu durumda $G/\text{Çekf} \cong f(G)$ dir. Eğer f örten ise $G/\text{Çekf} \cong G_1$ [30].

Örnek 2.10 $f : \mathbb{Z} \rightarrow \mathbb{Z}_p, a \rightarrow \bar{a}$ şeklinde tanımlanan bir homomorfizma olsun. O zaman, $g : \mathbb{Z}/\text{Çekf} \rightarrow \mathbb{Z}_p, a + \text{Çekf} \rightarrow \bar{a}$ şeklinde tanımlanan g homomorfizması bir izomorfizmadır ve $\mathbb{Z}/\text{Çekf} \cong \mathbb{Z}_p$.

Tanım 2.12 $R \neq \emptyset$ bir küme olsun ve R de $+$ ve $.$ işlemleri tanımlı olsun Eğer

- i. $(R, +)$ bir değişmeli grup,
- ii. Her $a, b, c \in R$ için $(ab)c = a(bc)$,

iii. Her $a, b, c \in R$ için $a(b + c) = ab + ac$ ve $(a + b)c = ac + bc$

şartları sağlanıyorsa R ye bir halka denir. Eğer her $a, b \in R$ için $ab = ba$ oluyorsa R ye değişmeli halka denir. Eğer R halkası çarpmaya göre birim elemanı içeriyorsa R ye birimli halka denir [30].

Örnek 2.11 $\mathbb{Z}$ ve $\mathbb{Q}$ birer birimli ve değişmeli halkadır.

Tanım 2.13 I , R nin boştan farklı bir alt kümesi olsun. Eğer

- i. Her $a, b \in I$ için $a - b \in I$,
- ii. Her $r \in R$ ve her $a \in I$ için $ra \in I$ ($ar \in I$)

ise I ya R nin sol(sağ) ideali denir. Eğer I hem sağ hem sol ideal ise I ya R nin ideali denir ve $I \triangleleft R$ ile gösterilir [30].

Örnek 2.12 Her n tamsayısı için $\langle n \rangle = n\mathbb{Z} = \{kn, n \in \mathbb{Z}\} \triangleleft \mathbb{Z}$ dir.

Tanım 2.14 $(F, +, \cdot)$ birimli ve değişmeli halka olsun. $F^* = F \setminus \{0\}$ olmak üzere eğer $(F^*, \cdot)$ bir grup ise $(F^*, +, \cdot)$ üçlüsüne cisim denir [29].

Örnek 2.13 $(\mathbb{Q}, +, \cdot)$ ve $(\mathbb{R}, +, \cdot)$ birer cisimdir.

Örnek 2.14 p asal olmak üzere $(\mathbb{Z}_p, +, \cdot)$ bir cisimdir.

Tanım 2.15 V bir küme ve F bir cisim olsun. Eğer

- i. $(V, +)$ bir değişmeli grup
- ii. Her $a, b \in F$ ve her $u, v \in V$ için
 - a. $a(u + v) = au + av$,
 - b. $a(bv) = (ab)v$,
 - c. $(a + b)v = av + bv$,
 - d. $1_F v = v$

şartları sağlanıyorsa V ye F üzerinde tanımlı bir vektör uzayı denir. Burada V nin elemanlarına vektör, F nin elemanlarına ise skaler denir [29].

Örnek 2.15 F bir cisim ve $n \geq 1$ olsun. $F^n = \{(a_1, a_2, \dots, a_n) : a_i \in F\}$ kümesi bileşen toplama işlemi ile bir değişmeli gruptur. Her $x \in F$ ve her $(a_1, a_2, \dots, a_n) \in F^n$ için $x(a_1, a_2, \dots, a_n) = (xa_1, xa_2, \dots, xa_n)$ olarak tanımlanan skalerle çarpma işlemi ile F^n , F üzerinde bir vektör uzayıdır [29].

Tanım 2.16 V , F cismi üzerinde vektör uzayı ve $U \subseteq V$ olsun. Eğer U , V deki toplama ve skalerle çarpma işlemleri ile birlikte bir vektör uzayı ise U ya V nin alt vektör uzayı, kısaca alt uzayı denir [29].

Teorem 2.4 V , F cismi üzerinde vektör uzayı ve $U \subseteq V$ olsun. U nun V nin alt uzayı olması için gerek ve yeter koşul

- i. $0 \in V$,
- ii. Her $u, v \in V$ için $u - v \in V$,
- iii. Her $a \in F$ ve her $u \in V$ için $au \in V$

şartlarının sağlanmasıdır [29].

Tanım 2.17 V , F cismi üzerinde vektör uzayı ve $v_1, v_2, \dots, v_r$, V nin farklı vektörleri olsun. Eğer $\lambda_1 v_1 + \lambda_2 v_2 + \dots + \lambda_r v_r = 0$ iken $\lambda_1 = \lambda_2 = \dots = \lambda_r = 0$ ise $v_1, v_2, \dots, v_r$ vektörleri lineer bağımsızdır. Bir $i \in \{1, 2, \dots, r\}$ için $\lambda_i = 0$ ise $v_1, v_2, \dots, v_r$ vektörleri lineer bağımlıdır [29].

Örnek 2.16 F^n vektör uzayı içerisinde $(1, 0, 0, \dots, 0), (0, 1, 0, \dots, 0), \dots, (0, 0, \dots, 0, 1)$ vektörleri lineer bağımsızdır.

Tanım 2.18 V , F cismi üzerinde vektör uzayı olsun. $v_1, v_2, \dots, v_n \in V$ ve $\lambda_1, \lambda_2, \dots, \lambda_n \in F$ olsun. Eğer her $v \in V$, $v = \lambda_1 v_1 + \lambda_2 v_2 + \dots + \lambda_n v_n$ şeklinde yazılabiliyorsa $v_1, v_2, \dots, v_n$ vektörleri V yi geriyor(üretiyor) denir [29].

Örnek 2.17 Her $v = (\lambda_1, \lambda_2, \dots, \lambda_n) \in F^n$ için $v = \lambda_1 (1, 0, 0, \dots, 0) + \lambda_2 (0, 1, 0, \dots, 0) + \dots + \lambda_n (0, 0, 0, \dots, 1)$ olduğundan $(1, 0, 0, \dots, 0), (0, 1, 0, \dots, 0), \dots, (0, 0, \dots, 0, 1)$ vektörleri F^n uzayını gerer.

Tanım 2.19 V, F cismi üzerinde vektör uzayı ve $v_1, v_2, \dots, v_n \in V$ olsun. Eğer $v_1, v_2, \dots, v_n$ vektörleri lineer bağımsız ve V vektör uzayını geriyorsa $\{v_1, v_2, \dots, v_n\}$ kümesine V nin bir bazı (tabanı) denir. V nin herhangi bir bazındaki vektörlerin sayısına V nin boyutu denir [29].

Örnek 2.18 F^n vektör uzayı için $(1, 0, 0, \dots, 0), (0, 1, 0, \dots, 0), \dots, (0, 0, \dots, 0, 1)$ vektörleri hem lineer bağımsız olduğundan hem de F^n uzayını gerdiğinden $\{(1, 0, 0, \dots, 0), (0, 1, 0, \dots, 0), \dots, (0, 0, \dots, 0, 1)\}$ kümesi F^n vektör uzayı için bir tabandır. Bu durumda F^n vektör uzayının boyutu n dir ve $\text{boy}(F^n) = n$ ile gösterilir.

2.2 Klasik Kodlarla İle İlgili Temel Bilgiler

İletişim sistemleri ve bilgi depolama araçları gibi bilgi medyalarında bilginin transferi sırasında oluşabilecek hataları farkedip düzeltebilen yapılara hata düzeltebilen kodlar denir. Bu bölümde bu kodlarla ilgili temel bilgiler verilecektir ve genel olarak [37] nolu kaynak kullanılacaktır.

Tanım 2.20 $A = \{a_1, \dots, a_q\}$, q elemanlı bir küme olsun.

- i. A üzerinde n uzunluğunda bir q -lu söz, her $i \in \{1, \dots, n\}$ için $u_i \in A$ olmak üzere $u = u_1 \dots u_n$ şeklindedir. u aynı zamanda $u = (u_1 \dots u_n)$ şeklinde bir n -li olarak da düşünülebilir.
- ii. A üzerinde n uzunluğunda bir q -lu blok kod, n uzunluğuna sahip q -lu sözlerden oluşan boştan farklı bir C kümesidir.
- iii. C deki bir elemana kodsöz denir.
- iv. C deki kodsözlerin sayısı, C nin eleman sayısıdır ve kısaca $|C|$ ile gösterilir.
- v. M elemanlı ve n uzunluğunda bir kod (n, M) ile gösterilir.
- vi. A kod alfabesi ve A nin elemanlarına da kod sembolleri denir.

Örnek 2.19

- i. $A = \{0,1\}$ şeklinde 2 elemanlı bir alfabe olsun. $C_1 = \{00,01,10,11\}$ kümesi A üzerinde 4 elemanlı 2 uzunluğunda ikili blok koddur ve $(2,4)$ şeklinde gösterilir.
- ii. $A = \{0,1,2\}$ şeklinde 3 elemanlı bir alfabe olsun. $C_2 = \{012,110,101,211,220\}$ kümesi A üzerinde 5 elemanlı 3 uzunluğunda üçlü blok koddur ve $(3,5)$ şeklinde gösterilir.

Tanım 2.21 x ve y , A alfabeti üzerinde n uzunluğunda birer söz olsunlar. x in y ye Hamming uzaklığı, x ve y nin farklı bileşenlerinin sayısı olarak tanımlanır ve $d(x, y)$ ile gösterilir. Yani;

$$d(x, y) = |\{i : x_i \neq y_i, i = 1, \dots, n\}|.$$

Eğer $x = x_1 \dots x_n$ ve $y = y_1 \dots y_n$ ise

$$d(x, y) = d(x_1, y_1) + \dots + d(x_n, y_n)$$

olarak yazılabilir. Burada,

$$d(x_i, y_i) = \begin{cases} 0, & x_i = y_i \\ 1, & x_i \neq y_i \end{cases}$$

[37].

Örnek 2.20

- i. $A = \{0,1\}$ ve $x = 111011$, $y = 001110$ olsun. Bu durumda $d(x, y) = 4$ olur.
- ii. $A = \{0,1,2,3\}$ ve $x = 301102$, $y = 102112$ olsun. Bu durumda $d(x, y) = 3$ olur.

Önerme 1 x, y ve z, A üzerinde n uzunluğunda sözler olsun. Bu durumda aşağıdaki özellikler sağlanır [37]:

- i. $0 \leq d(x, y) \leq n$
- ii. $d(x, y) = 0 \Leftrightarrow x = y$
- iii. $d(x, y) = d(y, x)$
- iv. $d(x, z) \leq d(x, y) + d(y, z)$ (Üçgen eşitsizliği)

İspat:

- i. $d(x, y) = \sum_{i=1}^n d(x_i, y_i)$ ve her $i = 1, \dots, n$ için $d(x_i, y_i) = 0$ veya $d(x_i, y_i) = 1$ olduğundan $0 \leq d(x, y) \leq n$ elde edilir.
- ii. $d(x, y) = 0 \Leftrightarrow$ Her $i = 1, \dots, n$ için $x_i = y_i \Leftrightarrow x_1 \dots x_n = y_1 \dots y_n \Leftrightarrow x = y$
- iii. $d(x, y) = |\{i, x_i \neq y_i, i = 1, \dots, n\}| = |\{i, y_i \neq x_i, i = 1, \dots, n\}| = d(y, x)$
- iv. $d(x, z) = d(x_1, z_1) + \dots + d(x_n, z_n) = \sum_{i=1}^n d(x_i, z_i)$ olduğundan bir i için $d(x_i, z_i) \leq d(x_i, y_i) + d(y_i, z_i)$ olduğunu göstermek yeterlidir. Eğer $x_i = z_i$ ise $d(x_i, z_i) \leq d(x_i, y_i) + d(y_i, z_i)$ olduğu açıktır. $x_i \neq z_i$ ise ya $x_i \neq y_i$ ya da $y_i \neq z_i$ olacağından $d(x_i, z_i) \leq d(x_i, y_i) + d(y_i, z_i)$ olur. Her i için bu eşitsizlik geçerli olduğundan ispat tamamlanır.

Tanım 2.22 C , en az iki elemanlı bir kod olsun. C kodun minimum uzaklığı $d(C)$ ile gösterilir ve

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

olarak tanımlanır [37].

Tanım 2.23 n uzunluklu, M elemanlı ve d minimum uzaklığa sahip bir kod (n, M, d) ile gösterilir. n, M ve d sayılarına kodun parametreleri denir [37].

Örnek 2.21

i. $C = \{00000, 00111, 11111\}$ olsun.

$d(00000, 00111) = 3$, $d(00000, 11111) = 5$ ve $d(00111, 11111) = 2$ olduğundan $d(C) = 2$ dir. Sonuç olarak C kodu, $(5, 3, 2)$ parametrelerine sahip bir ikili koddur.

ii. $C = \{012210, 221100, 121012, 001122\}$ olsun.

$d(012210, 221100) = 5$, $d(012210, 121012) = 5$, $d(221100, 121012) = 4$,
 $d(012210, 001122) = 5$, $d(221100, 001122) = 4$, $d(121012, 001122) = 4$ olduğundan $d(C) = 4$ tür. Böyle bir C kodu, $(6, 4, 4)$ parametrelerine sahip bir üçlü koddur.

Tanım 2.24 $t > 0$ olsun. Eğer C kodundaki herhangi bir kodsözün en az 1 en fazla t bileşeninde hata oluşmasıyla elde edilen söz C nin kodsözü değilse C kodu, t hata farkedebilen bir koddur. Eğer C , t hatayı farkedebilirken $(t+1)$ hatayı farkedemiyorsa C kodu tam olarak t hata farkedebilen koddur [37].

Örnek 2.22 $C = \{00000, 00111, 11111\}$, bir ikili kod olsun.

$00000 \rightarrow 00111$ şeklinde bozulması için 3 bileşende hata meydana gelmeli.

$00000 \rightarrow 11111$ şeklinde bozulması için 5 bileşende hata meydana gelmeli.

$00111 \rightarrow 11111$ şeklinde bozulması için 2 bileşende hata meydana gelmeli.

Bu durumda $u \in \{10000, 01000, 00100, 00010, 00001\}$ olmak üzere, her $c \in C$ için $u + c \notin C$ dir. Sonuç olarak C , 1 hatayı farkedebilen bir koddur. Fakat $11000 \notin C$ ve $11000 + 00111 = 11111 \in C$ olduğundan C , 2 hatayı farkedemez.

Teorem 2.5 Bir C kodun t hatayı fark edebilmesi için gerek ve yeter koşul $d(C) \geq t+1$ olmasıdır [37].

Tanım 2.25 $t > 0$ olsun. Eğer C kodundaki herhangi bir kodsözün en az 1 en fazla t bileşeninde hata oluşmasıyla elde edilen söz C nin başka bir kodsözünden en az 1 en

fazla t bileşeninde hata meydana gelmesiyle elde edilemiyorsa C kodu, t hata düzeltebilen bir koddur. Eğer C , t hatayı düzeltebilirken $(t+1)$ hatayı düzletemiyorsa C kodu tam olarak t hata düzeltebilen koddur [37].

Örnek 2.23 $C = \{000, 111\}$ olsun. 000 ve 111 kodsözlerinin herhangi bir bileşeninde 1 hata meydana gelmesi ile oluşabilecek sözler sırasıyla $\{100, 010, 001\}$ ve $\{011, 101, 110\}$ dir. $\{100, 010, 001\} \cap \{011, 101, 110\} = \emptyset$ olduğundan C , 1 hata düzeltebilir. $000 + 110 = 111 + 100$ olduğundan C , 2 hata düzletemez. Bu durumda C , tam olarak 1 hata düzelten koddur.

Teorem 2.6 Bir C kodun t hatayı düzeltebilmesi için gerek ve yeter koşul $d(C) \geq 2t+1$ olmasıdır [37].

Tanım 2.26 C , F_q^n nin bir alt uzayı ise C ye F_q^n üzerinde tanımlı n uzunluklu lineer kod denir. Kısaca $C \leq F_q^n$ ile gösterilir [37].

Tanım 2.27 $C \leq F_q^n$ bir lineer kod olsun [37].

- i. C lineer kodun boyutu, C nin F_q^n vektör uzayındaki boyutudur. Eğer $\text{boy}(C) = k$ ise C kodu kısaca $[n, k]$ şeklinde gösterilir.
- ii. C kodun duali, $C^\perp = \left\{ y \in F_q^n : \langle x, y \rangle = \sum_{i=1}^n x_i y_i = 0, \forall x \in C \right\}$ kodudur.

Teorem 2.7 [37] $C \leq F_q^n$ bir lineer kod olsun.

- i. $|C| = q^{\text{boy}(C)}$
- ii. $C^\perp$ de bir lineer koddur ve $\text{boy}(C) + \text{boy}(C^\perp) = n$ dir.
- iii. $(C^\perp)^\perp = C$.

Tanım 2.28 C , F_q^n üzerinde bir lineer kod, $\text{boy}(C) = k$ ve $d(C) = d$ olsun. Bu durumda C kodu kısaca $[n, k, d]$ ile gösterilir [37].

Örnek 2.24 $C = \{00000, 10101, 01010, 11111\}$ kodu F_2^5 in alt uzayı olduğundan bir lineer koddur. $\{01010, 10101\}$, C için bir taban ve $d(C) = 2$ olduğundan C kodu F_2^5 de bir $[5, 2, 2]$ lineer koddur.

Tanım 2.29 C bir lineer kod olsun.

- i. Eğer $C \subseteq C^\perp$ ise C ye kendine dik (ortogonal) denir.
- ii. Eğer $C = C^\perp$ ise C ye kendine dual denir.

Örnek 2.25 $C = \{0000, 1100, 0011, 1111\}$ kodu F_2^4 ün bir alt uzayı ve $C = C^\perp$ olduğundan kendine dual bir koddur.

Tanım 2.30 [37] $x \in F_q^n$ olsun. x in Hamming ağırlığı, x in sıfırdan farklı bileşenlerin sayısı olarak tanımlanır ve $wt(x)$ ile gösterilir. Yani;

$$wt(x) = |\{i : x_i \neq 0, i = 1, \dots, n\}| = d(x, 0).$$

Teorem 2.8 C , F_q^n üzerinde bir lineer kod olsun. Bu durumda $d(C) = wt(C)$ eşitliği vardır [37].

İspat: $d(C) = d(x, y)$ olacak şekilde $x, y \in C$ ($x \neq y$) vardır.

$d(C) = d(x, y) = wt(x - y) \geq wt(C) \Rightarrow d(C) \geq wt(C)$ bulunur. Diğer yandan

$wt(C) = wt(x) = d(x, 0) \geq d(C) \Rightarrow wt(C) \geq d(C)$ olduğundan $d(C) = wt(C)$ elde edilir.

Örnek 2.26 $C = \{00000, 10010, 11100, 01100\}$ olsun. $wt(10010) = 2, wt(11100) = 3$ $wt(01100) = 2$ olduğundan $d(C) = wt(C) = 2$ dir.

Tanım 2.31 [37] C bir lineer kod olsun.

- i. C kodun taban elemanlarını satır kabul eden matrise C kodun üreteç matrisi denir.
- ii. $C^\perp$ kodun taban elemanlarını satır kabul eden matrise C kodun kontrol matrisi denir.

Tanım 2.32 [37]

- i. $(I_k | X)$ tipindeki bir üreteç matrisine standart formdadır denir.
- ii. $(Y | I_{n-k})$ tipindeki bir kontrol matrisine standart formdadır denir.

Örnek 2.27 $C = \{000, 101, 121, 211, 020, 012, 001, 100\}$ lineer kodu için bir taban

$\{101, 121, 211\}$ olduğundan C kodun üreteç matrisi $G = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 2 & 1 \\ 2 & 1 & 1 \end{pmatrix}$ dir.

Teorem 2.9 C, F_q üzerinde bir $[n, k]$ lineer kod olsun. Bu durumda $v \in C^\perp$ olması için gerek ve yeter koşul $vG^T = 0$ olmasıdır. Eğer H ve G, C kodun sırasıyla kontrol ve üreteç matrisleri ise $HG^T = 0$ dır [37].

Teorem 2.10 [37] C bir lineer kod ve H, C nin kontrol matrisi olsun.

- i. $d(C) \geq d \Leftrightarrow H$ matrisinin herhangi $d - 1$ sütunu lineer bağımsızdır.
- ii. $d(C) \leq d \Leftrightarrow H$ matrisinin herhangi d sütunu lineer bağımlıdır.
- iii. $d(C) = d \Leftrightarrow H$ matrisinin herhangi $d - 1$ sütunu lineer bağımsız ve en az bir takım d sütunu lineer bağımlıdır.

Örnek 2.28 C lineer kodun kontrol matrisi $H = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$ olsun. H

matrisinin sıfır sütunu olmadığından ve herhangi iki sütunu lineer bağımsız olduğundan $d(C) \geq 3$ tür. 1., 2. ve 6. satırlar lineer bağımlı olduğundan $d(C) \leq 3$ tür. Bu durumda $d(C) = 3$ olur. Bu kontrol matrisine sahip kod $[7, 4, 3]$ parametrelili ikili Hamming koddur.

Teorem 2.11 C bir $[n, k]$ lineer kod olsun. Eğer C nin üreteç matrisi $G = (I_k | X)$ şeklinde ise C kodun kontrol matrisi $H = (-X^T | I_{n-k})$ şeklindedir [37].

Tanım 2.33 C bir $[n, k]$ lineer kod ve G , C kodun üreteç matrisi olsun. Bir $u \in F_q^k$ mesajı $uG = v \in C$ şeklinde kodlanır [37].

Örnek 2.29 C bir $[5, 3]$ lineer kod ve C kodun üreteç matrisi $G = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$

olsun. Bir $u = 101 \in F_2^3$ mesajı $uG = (101) \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix} = (10011)$ şeklinde

kodlanır.

Tanım 2.34 C , F_q üzerinde n uzunluklu bir lineer kod ve $u \in F_q^n$ olsun. C nin u ile belirli koseti $C + u = \{x + u : x \in C\} = u + C$ kümesidir [37].

Teorem 2.12 [37] C , F_q üzerinde $[n, k, d]$ lineer kod olsun. Aşağıdaki özellikler sağlanır:

- i. F_q^n deki her eleman C nin bir kosetinde yer alır.
- ii. Her $u \in F_q^n$ için $|C + u| = |C| = q^k$ dir.
- iii. Her $u, v \in F_q^n$ için $u \in C + v$ ise $u + C = v + C$ dir.
- iv. Herhangi iki koset ya aynıdır ya da ayrıktır.
- v. C nin q^{n-k} farklı koseti vardır.
- vi. Her $u, v \in F_q^n$ için $u - v \in C$ olması için gerek ve yeter koşul u ile v nin aynı kosette yer almasıdır.

Tanım 2.35 C , F_q üzerinde $[n, k, d]$ lineer kod ve H , C kodun kontrol matrisi olsun. Bir $w \in F_q^n$ sözü için w nin sendromu $S(w) = wH^T \in F_q^{n-k}$ olarak hesaplanır [37].

Teorem 2.13 [37] C , F_q üzerinde $[n, k, d]$ lineer kod ve H , C kodun kontrol matrisi olsun. Her $u, v \in F_q^n$ için aşağıdaki özellikler vardır:

- i. $S(u + v) = S(u) + S(v)$.

- ii. $S(u) = 0$ olması için gerek ve yeter koşul $u \in C$ olmasıdır.
- iii. $S(u) = S(v)$ olması için gerek ve yeter koşul u ile v nin aynı kosette yer almasıdır.

Tanım 2.36 Bir kosetteki en düşük ağırlıklı söze koset lideri denir [37].

C bir lineer kod ve H, C kodun kontrol matrisi olmak üzere sendrom tablosu oluşturmak için gerekli adımlar şunlardır:

Adım 1. C kodun tüm kosetleri belirlenir ve her bir kosetteki en düşük ağırlıklı söz koset lideri olarak seçilir.

Adım 2. Her bir koset liderinin sendrom değeri hesaplanır.

C bir lineer kod ve H, C kodun kontrol matrisi olmak üzere sendrom dekodlama süreci aşağıda belirtildiği gibidir:

Adım 1. Alınan w sözü için sendrom değeri $S(w)$ hesaplanır.

Adım 2. $S(u) = S(w)$ olacak şekilde u koset lideri sendrom tablosundan belirlenir.

Adım 3. $v = w - u$ olarak dekodlanır.

Örnek 2.30 $C = \{000000, 100110, 010101, 001011, 110011, 101101, 011110, 111000\}$ bir

$[6, 3, 3]$ ikili kod olsun. Bu kodun üreteç matrisi $G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$ dir. Teorem

2.11 den C kodun kontrol matrisi $H = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$ dir. Bu durumda C nin

F_2^6 da $\frac{q^n}{q^k} = \frac{2^6}{2^3} = 8$ farklı koseti vardır. C nin F_2^6 da kosetleri şunlardır:

$$000000 + C = \{000000, 100110, 010101, 001011, 110011, 101101, 011110, 111000\}$$

$$100000 + C = \{100000, 000110, 110101, 101011, 010011, 001101, 111110, 011000\}$$

$$010000 + C = \{010000, 110110, 000101, 011011, 100011, 111101, 001110, 101000\}$$

$$001000 + C = \{001000, 101110, 011101, 000011, 111011, 100101, 010110, 111000\}$$

$$000100 + C = \{000100, 100010, 010001, 001111, 110111, 101001, 011010, 111100\}$$

$$000010 + C = \{000010, 100100, 010111, 001001, 110001, 101111, 011100, 111010\}$$

$$000001 + C = \{000001, 100111, 010100, 001010, 110010, 101100, 011111, 111001\}$$

$$100001 + C = \{100001, 000111, 110100, 101010, 010010, 001100, 111111, 011001\}$$

Burada 000000, 100000, 010000, 001000, 000100, 000010, 000001, 100001 sözleri koset liderleridir. Koset liderlerinin sendromlarını gösteren sendrom tablosu aşağıdaki gibidir:

w	$S(w)$
000000	000
100000	100
010000	010
001000	001
000100	110
000010	101
000001	011
100001	111

Çizelge 2.1 $[6, 3, 3]$ lineer kodu için sendrom tablosu

Alınan söz $w = 100111$ olsun. $S(w) = 011 = S(000001)$ olduğundan gönderilen kodsöz $v = w - u = 100111 - 000001 = 100110$ olarak bulunur.

Tanım 2.37 $r \geq 2$ olsun. $n = 2^r - 1$ uzunluklu ve sütunları F_2^r nin sıfırdan farklı tüm elemanlarından oluşan kontrol matrisine sahip lineer koda ikili Hamming kod denir ve $Ham(r, 2)$ ile gösterilir [37].

Örnek 2.31 $r = 3$ olsun. $2^3 - 1 = 7$ uzunluklu Hamming kod için bir kontrol matris

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \text{ şeklindedir. } H \text{ kontrol matrisinden } d(H(3, 2)) = 3$$

olduğu görülür. Aslında tüm $r \geq 2$ için ikili Hamming kodlarının minimum uzaklığı 3 tür. Bu da ikili Hamming kodlarının tek hata düzeltebildiğini gösterir.

Tanım 2.38 $C \subseteq F_q^n$ olsun. Her $c = (c_0, \dots, c_{n-2}, c_{n-1}) \in C$ için $c' = (c_{n-1}, c_0, \dots, c_{n-2}) \in C$ ise C ye devirli kod denir [37].

Önerme 2.2 Devirli kodlar bir halkada idealdir.

$$\pi : C \subseteq F_q^n \rightarrow \frac{F_q[x]}{\langle x^n - 1 \rangle} = R_n, (a_0, a_1, \dots, a_{n-1}) \rightarrow a_0 + a_1x + \dots + a_{n-1}x^{n-1} \text{ fonksiyonu}$$

bir izomorfizmadır. Bu durumda R_n in her idealine karşılık F_q^n de bir C devirli kodu vardır. Dahası C , F_q^n de devirli koddur ancak ve ancak $\pi(C)$, R_n de bir idealdir [37].

Önerme 2.3 $\frac{F_q[x]}{\langle x^n - 1 \rangle} = R_n$ ve olsun. R_n bir temel ideal bölgesi olduğundan

$I = \langle g(x) \rangle$ olacak şekilde I idealinin içinde en küçük dereceli monik $g(x) \in R_n$ polinomu vardır. Bu $g(x)$ polinomuna I idealinin üreteç polinomu denir ve $g(x) \mid x^n - 1$ dir. Ayrıca bir $C \subseteq F_q^n$ devirli kodu için $\pi(C)$ idealinin üreteç polinomuna C kodun üreteç polinomu denir [37].

Örnek 2.32 $C = \{000, 111, 222\} \subseteq F_3^3$ bir devirli koddur.

$$\pi(C) = \{0, 1 + x + x^2, 2 + 2x + 2x^2\}, \quad R_n = \frac{F_3[x]}{\langle x^3 - 1 \rangle} \text{ de bir idealdir.}$$

$\pi(C) = \langle 1 + x + x^2 \rangle$ ve $1 + x + x^2 \mid x^3 - 1$ dir. Bu durumda $1 + x + x^2$ polinomu, C kodun üreteç polinomudur.

Teorem 2.14 $x^n - 1$ in her bir monik böleni F_q^n de bir devirli kodun üreteç polinomudur. Ayrıca, F_q^n de devirli kodlar ile $F_q[x]$ deki $x^n - 1$ in monik bölenleri arasında birebir eşleme vardır [37].

Teorem 2.15 $g(x)$, C devirli kodun üreteç polinomu olsun. Eğer $g(x)$ polinomunun derecesi $n - k$ ise C kodun boyutu k dır [37].

Teorem 2.16 $C = \langle g(x) \rangle$ ve $g(x) = g_0 + g_1x + \dots + g_{n-k}x^{n-k}$ olsun. Bu durumda C devirli kodun üreteç matrisi

$$G = \begin{pmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{k-1}g(x) \end{pmatrix} = \begin{pmatrix} g_0 & g_1 & \dots & g_{n-k} & 0 & \dots & \dots & 0 \\ 0 & g_0 & g_1 & \dots & g_{n-k} & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & g_0 & g_1 & \dots & g_{n-k} & 0 \\ 0 & 0 & \dots & 0 & g_0 & g_1 & \dots & g_{n-k} \end{pmatrix}$$

şekindedir [37].

Örnek 2.33 $F_2[x]$ ' te $x^9 - 1 = (x+1)(x^2 + x + 1)(x^6 + x^3 + 1)$ dir. $x^9 - 1$ in her bir böleni 9 uzunluğunda ikili kod üretir. Eğer $C = \langle x^6 + x^3 + 1 \rangle$ olarak seçilirse C bir devirli kod olur. Bu durumda C devirli kodun üreteç matrisi

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

dir.

Tanım 2.39 F bir cisim olsun. $F[x] = \left\{ \sum_{i=0}^n a_i x^i : a_i \in F, n \geq 0 \right\}$ kümesi F üzerinde polinom toplama ve çarpma işlemi ile birlikte bir polinom halkasıdır [37].

Tanım 2.40 $\alpha \in F_q$ olsun. Eğer $F_q = \{0, \alpha, \alpha^2, \dots, \alpha^{q-1} = 1\}$ ise α ya F_q cisminin ilkel elemanı denir [37].

Tanım 2.41 Bir $\alpha \in F_q$ elemanın $F_q[x]$ daki minimal polinomu, $F_q[x]$ polinom halkasında $f(\alpha) = 0$ şartını sağlayan en küçük dereceli sıfırdan farklı monik $f(x)$ polinomudur [37].

Tanım 2.42 $(n, q) = 1$ olsun. q nun $\text{mod } n$ e göre i yi içeren devirsel koseti

$$C_i = \{iq^j \pmod{n} \in \mathbb{Z}_n : j = 0, 1, \dots\}$$

olarak tanımlanır [37].

Önerme 2.4 [37] $(n, q) = 1$ olsun.

- i. İki devirsel koset ya aynıdır ya da ayrıktır. Dolayısıyla devirsel kosetler $\mathbb{Z}_n$ in bir ayrışımıdır.
- ii. Eğer bir $m \geq 1$ tamsayısı için $n = q^m - 1$ ise her bir devirsel koset en fazla m eleman içerir.
- iii. Bir m pozitif tamsayısı için $n = q^m - 1$ olsun. Eğer $(i, q^m - 1) = 1$ ise $|C_i| = m$ olur.

Teorem 2.17 $\alpha \in F_{q^m}$ olsun. α^i nin F_q daki minimal polinomu

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

dir. Burada C_i , q nun $\text{mod}(n-1)$ e göre i yi içeren devirsel kosetidir [37].

Örnek 2.34 2 nin $\text{mod } 7$ ye göre devirsel kosetleri $C_0 = \{0\}$, $C_1 = \{1, 2, 4\}$, $C_3 = \{3, 5, 6\}$ dir. α , $1 + x + x^3 \in F_2[x]$ in kökü olsun. Bu durumda α , F_8 in ilkel elemanı ve $1 + x + x^3$ de α nın minimal polinomu olur. α^3 ün F_2 deki minimal polinomu

$$M^{(3)}(x) = (x - \alpha^3)(x - \alpha^5)(x - \alpha^6) = x^3 - (\alpha^6 + \alpha^5 + \alpha^3)x^2 + (\alpha^{11} + \alpha^9 + \alpha^8)x - \alpha^{14}$$

şeklinde dir. $\alpha^3 = \alpha + 1$, $\alpha^4 = \alpha^2 + \alpha$, $\alpha^5 = \alpha^2 + \alpha + 1$, $\alpha^6 = \alpha^2 + 1$, $\alpha^8 = \alpha$, $\alpha^9 = \alpha^2$, $\alpha^{11} = \alpha^2 + \alpha$, $\alpha^{14} = 1$ olduğundan $M^{(3)}(x) = x^3 + x^2 + 1$ elde edilir.

Tanım 2.43 α , F_{q^m} nin ilkel elemanı ve $M^{(i)}(x)$, α^i nin $F_q[x]$ daki minimal polinomu olsun. $g(x) = \text{ekok}(M^{(a)}(x), M^{(a+1)}(x), \dots, M^{(a+\delta-2)}(x))$ üreteç polinomuna sahip q -lu devirsel koda, F_q üzerinde δ minimum tasarlanmış uzaklığa sahip $n = q^m - 1$ uzunluklu bir BCH kod denir ($a > 0$). Eğer $a = 1$ ise böyle bir koda dar anlamda BCH kod denir [37].

Örnek 2.35 $\alpha \in F_8$, $1 + x + x^3$ ün kökü olsun. Bu durumda α , F_8 in ilkel elemanıdır. Örnek 34 ten $M^{(1)}(x) = M^{(2)}(x) = 1 + x + x^3$ elde edilir. $a = 1$, $\delta = 3$ olmak üzere $g(x) = \text{ekok}(M^{(1)}(x), M^{(2)}(x)) = 1 + x + x^3$ üreteç polinomuna sahip kod, 7 uzunluğunda dar anlamda ikili $[7, 4]$ BCH koddur.

Teorem 2.18 [37]

- i. δ tasarlanmış uzaklığa sahip bir BCH kodun minimum uzaklığı en az δ dir.
- ii. δ tasarlanmış uzaklığa sahip $n = q^m - 1$ uzunluklu q -lu BCH kodun boyutu en az $q^m - 1 - m(\delta - 1)$ dir.

Tanım 2.44 C , F_q üzerinde $g(x)$ polinomu tarafından üretilen n uzunluğunda bir devirli kod olsun. Eğer her $i \in I$ için $g(\alpha^i) = 0$ oluyorsa $I \subseteq \mathbb{Z}_n$ kümesine C kodun tanımlayıcı (defining) kümesi denir [38].

Örnek 2.36 C , F_2 üzerinde Örnek 2.34 te tanımlanan $M^{(3)}(x) = x^3 + x^2 + 1$ polinomu tarafından üretilen 7 uzunluğunda devirli kod olsun. $M^{(3)}(x) = (x - \alpha^3)(x - \alpha^5)(x - \alpha^6)$ olduğundan C kodun tanımlayıcı (defining) kümesi $\{3, 5, 6\}$ dir.

Önerme 2.5 $(n, q) = 1$ ve C , F_q üzerinde n uzunluğunda bir devirli kod olsun. Ayrıca Z , C kodun tanımlayıcı (defining) kümesi olsun. Bu durumda $C^\perp \subseteq C$ olması için gerek ve yeter koşul $Z \cap Z^{-1} = \emptyset$ şartının sağlanmasıdır. Burada $Z^{-1} = \{-z(\text{mod } n), z \in Z\}$ [13].

İspat: Z_C ve $Z_{C^\perp}$, sırasıyla C ve $C^\perp$ kodlarının tanımlayıcı (defining) kümeleri olsun.

$N = \{0, 1, \dots, n-1\}$ olmak üzere

$$C^\perp \subseteq C \Leftrightarrow Z_C \subseteq Z_{C^\perp}, Z_{C^\perp} = (N \setminus Z_C)^{-1}$$

$$\Leftrightarrow Z_C \subseteq (N \setminus Z_C)^{-1}$$

$$\Leftrightarrow Z_C \cap (N \setminus (N \setminus Z_C)^{-1}) = \emptyset$$

$$\Leftrightarrow Z \cap Z^{-1} = \emptyset .$$

KUANTUM HATA DÜZELTEN KODLARA GİRİŞ**3.1 Dirac Notasyonu ve Hilbert Uzayı Üzerinde Lineer Cebir**

Kuantum hesaplamada çalışılan vektör uzayı, kompleks (karmaşık) sayılar üzerinde sonlu boyutlu bir uzaydır. Böyle bir vektör uzayı için Hilbert vektör uzayı alınabilir. Hilbert uzay genellikle H ile gösterilir. Dolayısıyla kuantum kodlar sonlu boyutlu Hilbert uzayı üzerinde tanımlanır. Bölüm 3.4 te anlatılacağı üzere, n uzunluğunda bir kuantum kod 2^n boyutlu Hilbert uzayının bir alt uzayıdır. Kuantum hesaplamaya girmeden önce gösterimi kolaylaştıran dirac notasyonunun ve Hilbert uzayı üzerinde bazı lineer cebir bilgilerinin bilinmesi gerekir.

İlk olarak Paul Adrien Maurice Dirac tarafından kullanılan dirac notasyonunda “ $| \rangle$ ” ile bir sütun vektörü belirtilir ve ket diye okunur. “ $\langle |$ ” notasyonu ise ket vektörünün eşlenik transpozesidir ve bra diye okunur. Örneğin, $|x\rangle = \begin{pmatrix} 1+i \\ 1 \end{pmatrix}$ ise $\langle x| = (1-i \ 1)$ olur.

Bir boyutlu Hilbert uzayı kompleks sayılar kümesidir. İki boyutlu Hilbert uzayının elemanları, bileşenleri kompleks sayılar olan 2×1 şeklindeki sütun vektörleridir. Bu durumda iki boyutlu Hilbert uzayın elemanları $a, b \in \mathbb{C}$ olmak üzere

$$\begin{pmatrix} a \\ b \end{pmatrix}$$

şeklindedir. Sonlu boyutlu vektör uzayları için bir taban seçilebilir. Her $\begin{pmatrix} a \\ b \end{pmatrix} \in H$ için

$$\begin{pmatrix} a \\ b \end{pmatrix} = a \begin{pmatrix} 1 \\ 0 \end{pmatrix} + b \begin{pmatrix} 0 \\ 1 \end{pmatrix}, a, b \in \mathbb{C}$$

olduğundan $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ ve $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ vektörleri iki boyutlu Hilbert uzayının bir tabanıdır. Burada

$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ ve $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ olarak alınırsa $\{|0\rangle, |1\rangle\}$ kümesi bu uzay için bir taban olur. Bu

durumda iki boyutlu Hilbert uzayı $H = \{a|0\rangle + b|1\rangle : a, b \in \mathbb{C}\}$ kümesidir. Bundan sonra $|\psi\rangle$ ile Hilbert uzayındaki bir vektör belirtilecektir.

$n \geq 1$ olmak üzere 2^n boyutlu Hilbert uzayını anlamak için matrislerin tensör çarpımının bilinmesi gerekir.

Tanım 3.1 A bir $m \times n$ matris ve B bir $r \times s$ matris olmak üzere A ile B matrislerinin tensör çarpımı, A nın her bileşeninin B matrisi ile çarpımı olarak tanımlanır ve $A \otimes B$ ile gösterilir [34]:

$$A \otimes B = \begin{pmatrix} a_{11}[B] & a_{12}[B] & \dots & a_{1n}[B] \\ a_{21}[B] & a_{22}[B] & \dots & a_{2n}[B] \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}[B] & a_{m2}[B] & \dots & a_{mn}[B] \end{pmatrix}_{mr \times ns}$$

Örnek 3.1 $A = \begin{pmatrix} 1 & 3 \\ i & 2 \end{pmatrix}$ ve $B = \begin{pmatrix} 1 \\ i \end{pmatrix}$ olsun. A ile B nin tensör çarpımı

$$A \otimes B = \begin{pmatrix} \begin{pmatrix} 1 \\ i \end{pmatrix} & 3 \begin{pmatrix} 1 \\ i \end{pmatrix} \\ i \begin{pmatrix} 1 \\ i \end{pmatrix} & 2 \begin{pmatrix} 1 \\ i \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ i & 3i \\ i & 2 \\ -1 & 2i \end{pmatrix}$$

şeklindedir.

Genel olarak, $|\varphi\rangle$ ile $|\phi\rangle$ vektörleri için $|\varphi\rangle \otimes |\phi\rangle = |\varphi\rangle |\phi\rangle = |\varphi\phi\rangle$ gösterimleri aynı şeyi ifade eder.

Örnek 3.2 $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ ve $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ olsun. Bu durumda

$$|0\rangle \otimes |0\rangle = |0\rangle|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = |00\rangle,$$

$$|0\rangle \otimes |1\rangle = |0\rangle|1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = |01\rangle,$$

$$|1\rangle \otimes |0\rangle = |1\rangle|0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = |10\rangle \text{ ve}$$

$$|1\rangle \otimes |1\rangle = |1\rangle|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = |11\rangle$$

olur. $|0\rangle$ ve $|1\rangle$ vektörlerinin tensör çarpımı aşağıdaki gibi genelleştirilebilir:

$$|0\rangle \otimes |0\rangle \otimes \dots \otimes |0\rangle = \left| \underbrace{00\dots 00}_n \right\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}_{2^n \times 1},$$

$$|0\rangle \otimes |0\rangle \otimes \dots \otimes |1\rangle = \left| \underbrace{00\dots 01}_n \right\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}_{2^n \times 1},$$

$\vdots$
 $\vdots$

$$|1\rangle \otimes |1\rangle \otimes \dots \otimes |0\rangle = \left| \underbrace{11\dots 10}_n \right\rangle = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ 0 \end{pmatrix}_{2^n \times 1} \quad \text{ve}$$

$$|1\rangle \otimes |1\rangle \otimes \dots \otimes |1\rangle = \left| \underbrace{11\dots 11}_n \right\rangle = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}_{2^n \times 1} .$$

Buradan dirac notasyonunun gösterimi nasıl kolaylaştırdığı görülebilir.

$n = 2$ olmak üzere $2^n = 4$ boyutlu Hilbert uzayın elemanları bileşenleri kompleks sayılar olan 4×1 şeklindeki sütun vektörleridir. Bu durumda bu uzayın elemanları $a_{00}, a_{01}, a_{10}, a_{11} \in \mathbb{C}$ olmak üzere

$$\begin{pmatrix} a_{00} \\ a_{01} \\ a_{10} \\ a_{11} \end{pmatrix}$$

şeklinde dir. Her $\begin{pmatrix} a_{00} \\ a_{01} \\ a_{10} \\ a_{11} \end{pmatrix}$ vektörü $\begin{pmatrix} a_{00} \\ a_{01} \\ a_{10} \\ a_{11} \end{pmatrix} = a_{00} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + a_{01} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + a_{10} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + a_{11} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$ olarak

yazılabildiğinden ve $|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$, $|01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$, $|10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$, $|11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$ olduğundan $|00\rangle$,

$|01\rangle$, $|10\rangle$ ve $|11\rangle$ vektörleri 2^2 boyutlu Hilbert uzayı için bir tabandır. Sonuç olarak bu

uzay $\{a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle : a_{00}, a_{01}, a_{10}, a_{11} \in \mathbb{C}\}$ kümesidir.

Bu durum herhangi $n > 0$ için düşünülduğünde 2^n boyutlu Hilbert uzayının bir tabanının $|00\cdots 00\rangle, |00\cdots 01\rangle, \dots, |11\cdots 10\rangle, |11\cdots 11\rangle$ vektörleri olduğu görülür. Bu durumda 2^n boyutlu Hilbert uzayı

$$\{a_1|00\cdots 00\rangle + a_2|00\cdots 01\rangle + \cdots + a_{2^n-1}|11\cdots 10\rangle + a_{2^n}|11\cdots 11\rangle : a_i \in \mathbb{C}, i=1,2,\dots,2^n\}$$

kümesidir.

Tanım 3.2 [34]

- i. $|\psi\rangle$ ile $|\phi\rangle$ vektörlerinin iç-çarpımı $\langle\phi|\psi\rangle$ olarak tanımlanır.
- ii. Eğer $\langle\phi|\psi\rangle = 0$ ise $|\psi\rangle, |\phi\rangle$ ye diktir denir.
- iii. $|\psi\rangle$ vektörünün normu $\| |\psi\rangle \| = \sqrt{\langle\psi|\psi\rangle}$ olarak tanımlanır.
- iv. Eğer $\| |\psi\rangle \| = 1$ ise $|\psi\rangle$ vektörüne birim vektör denir.

Tanım 3.3 H , 2^n boyutlu Hilbert uzayı ve $B = \{|b_m\rangle\}$ kümesi H Hilbert uzayının bir

bazı olsun. $\delta_{n,m} = \begin{cases} 0, & n \neq m \\ 1, & n = m \end{cases}$ olmak üzere her $|b_m\rangle, |b_n\rangle \in H$ için $\langle b_n | b_m \rangle = \delta_{n,m}$ ise

$B = \{|b_m\rangle\}$ kümesine H Hilbert uzayının bir ortonormal bazı denir [34].

Örnek 3.3 2^2 boyutlu Hilbert uzayı için $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ kümesi bir ortonormal tabandır.

Tanım 3.4 H , bir vektör uzayı olsun. $T : H \rightarrow H$ lineer dönüşümüne H vektör uzayı üzerinde tanımlı bir lineer operatör denir [34].

Örnek 3.4 H , iki boyutlu Hilbert uzayı olsun. $T : H \rightarrow H$, $a|0\rangle + b|1\rangle \rightarrow a|1\rangle + b|0\rangle$ şeklinde tanımlı bir lineer dönüşüm olduğundan H vektör uzayı üzerinde bir lineer operatördür. Sonlu boyutlu bir vektör uzayında her lineer dönüşüm bir matris tarafından ifade edilebildiğinden T lineer operatörüne karşılık gelen matris $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ şeklindedir.

Tanım 3.5 $|\psi\rangle$ ile $|\phi\rangle$ vektörlerinin dış çarpımı $|\psi\rangle\langle\phi|$ olarak tanımlanır. $|\psi\rangle\langle\phi|$ nin bir $|\phi\rangle$ vektörüne etkisi

$$(|\psi\rangle\langle\phi|)|\phi\rangle = |\psi\rangle(\langle\phi|\phi\rangle) = (\langle\phi|\phi\rangle)|\psi\rangle \quad (3.1)$$

şeklindedir. Bir $|\psi\rangle$ vektörünün kendisi ile dış çarpımı $|\psi\rangle\langle\psi|$ şeklindedir ve $|\psi\rangle\langle\psi|$ nin bir $|\phi\rangle$ vektörüne etkisi

$$(|\psi\rangle\langle\psi|)|\phi\rangle = |\psi\rangle(\langle\psi|\phi\rangle) = (\langle\psi|\phi\rangle)|\psi\rangle \quad (3.2)$$

olduğundan $|\psi\rangle\langle\psi|$ bir lineer operatördür. $\langle\psi|\phi\rangle$ iç-çarpım sonucu bir skaler olduğundan $|\psi\rangle\langle\psi|$, bir $|\phi\rangle$ vektörünü $|\psi\rangle$ tarafından üretilen alt uzaya resmeder [34].

Örnek 3.5 $|\psi\rangle = |0\rangle + i|1\rangle$ olsun. $|\psi\rangle$ vektörünün kendisi ile dış çarpımı

$$|\psi\rangle\langle\psi| = \begin{pmatrix} 1 \\ i \end{pmatrix} (1 \quad -i) = \begin{pmatrix} 1 & -i \\ i & 1 \end{pmatrix} \text{ şeklindedir. } |\phi\rangle = (i+1)|0\rangle + 2|1\rangle \text{ olmak üzere } |\psi\rangle\langle\psi|$$

$$\text{nin } |\phi\rangle \text{ vektörüne etkisi } (|\psi\rangle\langle\psi|)|\phi\rangle = \begin{pmatrix} 1 & -i \\ i & 1 \end{pmatrix} \begin{pmatrix} i+1 \\ 2 \end{pmatrix} = \begin{pmatrix} -i+1 \\ i+1 \end{pmatrix} = (1-i) \begin{pmatrix} 1 \\ i \end{pmatrix} = (1-i)|\psi\rangle$$

şeklindedir.

Teorem 3.1 $B = \{|b_m\rangle\}$ kümesi H vektör uzayının bir ortonormal bazı olsun. H üzerindeki her lineer operatör, taban elemanların dış çarpımlarının bir lineer toplamı olarak yazılabilir. Yani T , H üzerinde bir lineer operatör ve $T_{n,m} = \langle b_n | T | b_m \rangle$ olmak üzere

$$T = \sum_{b_n, b_m \in B} T_{n,m} |b_n\rangle\langle b_m| \quad (3.3)$$

olur. Bu durumda T lineer operatörünün bir $|\phi\rangle$ vektörüne etkisi

$$T|\phi\rangle = \left(\sum_{b_n, b_m \in B} T_{n,m} |b_n\rangle\langle b_m| \right) |\phi\rangle = \sum_{b_n, b_m \in B} T_{n,m} |b_n\rangle\langle b_m | \phi \rangle = \sum_{b_n, b_m \in B} T_{n,m} \langle b_m | \phi \rangle |b_n\rangle \quad (3.4)$$

şeklindedir [34].

Örnek 3.6 H , iki boyutlu Hilbert uzayı ise $\{|0\rangle, |1\rangle\}$ kümesi H için bir ortonormal tabandır. $T: H \rightarrow H$ fonksiyonu $a|0\rangle + b|1\rangle \rightarrow a|0\rangle - b|1\rangle$ şeklinde tanımlı bir lineer dönüşüm olduğundan H üzerinde bir lineer operatördür. T lineer dönüşümü matris cinsinden $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ olarak ifade edilebilir. $T_{1,1} = 1$, $T_{1,2} = 0$, $T_{2,1} = 0$, $T_{2,2} = -1$ ve $|0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $|1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ olduğundan $T = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ lineer operatörü $T = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1|$ olarak yazılabilir.

Tanım 3.6 $U^\dagger$, U nun eşlenik trasnpozu olmak üzere U operatörü için $U^\dagger = U^{-1}$ eşitliği sağlanıyorsa U ya üniter denir. Bu durumda $UU^\dagger = I$ olur. Üniter matrisler vektörlerin normunu korur. Yani, $\|U|\psi\rangle\| = \|U|\psi\rangle\|$ [34].

Örnek 3.7 $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ ve $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ matrisleri birer üniter matrislerdir.

Tanım 3.7 H Hilbert uzayı üzerinde bir T operatörü $T^\dagger = T$ şartını sağlıyorsa T ye Hermityen denir [34].

Tanım 3.8 H vektör uzayı üzerinde bir P lineer operatörü $P^2 = P$ şartını sağlıyorsa P ye projektör denir. Eğer $P^2 = P$ ve $P^\dagger = P$ ise P ye ortogonal projektör denir [34].

Örnek 3.8 H iki boyutlu Hilbert uzayı üzerinde $|0\rangle\langle 0|$, $|0\rangle\langle 1|$, $|1\rangle\langle 0|$ ve $|1\rangle\langle 1|$ matrisleri birer ortogonal projektördür.

Tanım 3.9 T bir operatör ve c bir skaler olmak üzere eğer bir $|\psi\rangle$ vektörü için $T|\psi\rangle = c|\psi\rangle$ eşitliği sağlanıyorsa $|\psi\rangle$ vektörüne T nin bir özvektörü, c sabitine de T nin $|\psi\rangle$ vektörüne karşılık gelen özdeğeri denir [34].

Örnek 3.9 H , iki boyutlu Hilbert vektör uzayı ve $T: H \rightarrow H$, $a|0\rangle + b|1\rangle \rightarrow a|1\rangle + b|0\rangle$ şeklinde tanımlı bir lineer operatör olsun. Bu durumda T lineer operatörünün temsil matrisi $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ şeklindedir. $\begin{pmatrix} a \\ b \end{pmatrix} \in H$ vektörünün T altındaki görüntüsü $\begin{pmatrix} b \\ a \end{pmatrix}$

olduğundan eğer $\begin{pmatrix} a \\ b \end{pmatrix}$, T nin bir özvektörü ise ya $a = b$ ya da $a = -b$ olmalıdır. Eğer $a = b$ ise $T(a|0\rangle + a|1\rangle) = 1(a|0\rangle + a|1\rangle)$ olduğundan 1 , T operatörünün özdeğeridir. Eğer $a = -b$ ise $T(a|0\rangle - a|1\rangle) = -1(a|0\rangle - a|1\rangle)$ olduğundan -1 , T operatörünün bir diğer özdeğeridir.

Teorem 3.2 T bir operatör olsun. Eğer $T^\dagger = T$ ve $T|\psi\rangle = c|\psi\rangle$ ise c bir reel sayıdır. Yani, Hermityen operatörlerinin özdeğerleri reeldir [34].

Örnek 3.9 dan görüldüğü gibi Hermityen operatörünün özdeğerleri reeldir. Bu teorem kuantum mekanikte ölçümler için önemli bir teoremdir.

Tanım 3.10 Bir T operatörünün özdeğerlerinin toplamına T nin izi denir ve kısaca $iz(T)$ ile gösterilir. A , T operatörüne karşılık gelen matris ise $iz(T)$, A nın esas köşegen elemanlarının toplamına eşittir [34].

Tanım 3.11 $\{|b_n\rangle\}$, H uzayın bir ortonormal tabanı olsun. T , H uzayı üzerinde bir operatör olmak üzere $iz(T) = \sum_{b_n} \langle b_n | A | b_n \rangle$ eşitliği vardır [34].

Örnek 3.10 H iki boyutlu Hilbert uzayı olmak üzere $a|0\rangle + b|1\rangle \rightarrow (3a + b)|0\rangle + (a + 3b)|1\rangle$ şeklinde tanımlı $T : H \rightarrow H$ fonksiyonu H üzerinde bir lineer operatördür. T operatörüne karşılık gelen matris $A = \begin{pmatrix} 3 & 1 \\ 1 & 3 \end{pmatrix}$ olduğundan $iz(T) = 3 + 3 = 6$ olur. $\{|0\rangle, |1\rangle\}$ kümesi H için bir ortonormal taban olduğundan $iz(T) = 6 = (1 \ 0) \begin{pmatrix} 3 & 1 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} + (0 \ 1) \begin{pmatrix} 3 & 1 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ olarak yazılabilir.

Tanım 3.12 [34] H_1 ve H_2 sırasıyla 2^n ve 2^m boyutlu Hilbert vektör uzayları olsun. $\{|b_i\rangle\}_{i \in \{1, 2, \dots, 2^n\}}$ ve $\{|c_j\rangle\}_{j \in \{1, 2, \dots, 2^m\}}$ sırasıyla H_1 ve H_2 uzaylarının birer ortonormal tabanları olsun.

- i. H_1 ile H_2 nin tensör çarpımı $H_1 \otimes H_2$ ile gösterilir ve 2^{n+m} boyutlu daha büyük bir vektör uzayıdır.

- ii. $\left\{ |b_i\rangle \otimes |c_j\rangle \right\}_{i \in \{1,2,\dots,2^n\}, j \in \{1,2,\dots,2^m\}}$ kümesi $H_1 \otimes H_2$ uzayı için bir ortonormal tabandır.

Tensör çarpım için aşağıdaki özellikler sağlanır. Her $c \in \mathbb{C}$ ve her $|\psi_1\rangle, |\phi_1\rangle \in H_1$ ve her $|\psi_2\rangle, |\phi_2\rangle \in H_2$ için

- i. $c(|\psi_1\rangle \otimes |\psi_2\rangle) = (c|\psi_1\rangle) \otimes |\psi_2\rangle = |\psi_1\rangle \otimes (c|\psi_2\rangle),$
- ii. $(|\psi_1\rangle + |\phi_1\rangle) \otimes |\psi_2\rangle = |\psi_1\rangle \otimes |\psi_2\rangle + |\phi_1\rangle \otimes |\psi_2\rangle,$
- iii. $|\psi_1\rangle \otimes (|\psi_2\rangle + |\phi_2\rangle) = |\psi_1\rangle \otimes |\psi_2\rangle + |\psi_1\rangle \otimes |\phi_2\rangle$

özellikleri vardır. A ve B sırasıyla H_1 ve H_2 üzerinde lineer operatör olmak üzere $A \otimes B$, $H_1 \otimes H_2$ üzerinde $(A \otimes B)(|\psi_1\rangle \otimes |\psi_2\rangle) = A|\psi_1\rangle \otimes B|\psi_2\rangle$ şeklinde tanımlı bir lineer operatördür. Bu etki lineer olarak genişletilirse

$$(A \otimes B) \left(\sum_{ij} \lambda_{ij} |b_i\rangle \otimes |c_j\rangle \right) = \sum_{ij} \lambda_{ij} A|b_i\rangle \otimes B|c_j\rangle \text{ elde edilir.}$$

Örnek 3.11 H , iki boyutlu Hilbert uzayı olsun. Bu durumda $H \otimes H$, 2^2 boyutlu bir Hilbert uzayıdır ve kısaca $H^{\otimes 2}$ ile gösterilir. $H^{\otimes 2}$ için $\{|0\rangle \otimes |0\rangle = |00\rangle, |0\rangle \otimes |1\rangle = |01\rangle, |1\rangle \otimes |0\rangle = |10\rangle, |1\rangle \otimes |1\rangle = |11\rangle\}$ bir ortonormal taban kümesidir. $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ ve $B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, H üzerinde tanımlı birer lineer operatör

$$\text{olduklarından } A \otimes B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix} \text{ operatörü } H^{\otimes 2} \text{ üzerinde}$$

bir lineer operatördür. $A \otimes B$ operatörün $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ tabanına etkisi aşağıdaki gibidir:

$$(A \otimes B)|00\rangle = (A \otimes B)(|0\rangle \otimes |0\rangle) = A|0\rangle \otimes B|0\rangle = |10\rangle,$$

$$(A \otimes B)|01\rangle = A|0\rangle \otimes B|1\rangle = -|11\rangle,$$

$$(A \otimes B)|10\rangle = A|1\rangle \otimes B|0\rangle = |00\rangle \text{ ve}$$

$$(A \otimes B)|11\rangle = A|1\rangle \otimes B|1\rangle = -|01\rangle.$$

Teorem 3.3 Eğer $|\psi\rangle$, $H_A \otimes H_B$ uzayında bir vektör ise $|\psi\rangle = \sum_i \sqrt{p_i} |\phi_i^A\rangle |\phi_i^B\rangle$ olacak şekilde H_A ve H_B uzaylarının sırasıyla $\{|\phi_i^A\rangle\}$ ve $\{|\phi_i^B\rangle\}$ ortonormal tabanları ve negatif olmayan $\{p_i\}$ reel sayıları vardır [34].

Örnek 3.12 $|\psi\rangle = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$ olsun. Bu durumda,

$$|\psi\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \right) \otimes \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \right) \text{ olarak ayrılır. } H_A \text{ ile } H_B \text{ için ortonormal}$$

$$\text{bir taban sırasıyla } \left\{ |\phi_0^A\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, |\phi_1^A\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \right\} \text{ ve}$$

$$\left\{ |\phi_0^B\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, |\phi_1^B\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \right\} \text{ olarak seçilebilir.}$$

3.2 Kubitler

Günümüzde klasik hesaplamanın ve klasik bilginin temel birimi bitlerdir. Kuantum hesaplamada ve kuantum bilgide kullanılan temel birim ise kuantum bitler ya da kısaca kubitlerdir. Bir klasik bit 0 veya 1 değerini alabilirken buna karşılık bir kuantum bit $|0\rangle$ ya da $|1\rangle$ değerini alır. Bitler ile kubitler arasındaki fark ise bir kubitin $|0\rangle$ ve $|1\rangle$ halinden başka $|0\rangle$ ve $|1\rangle$ in lineer kombinasyonu (süperpozisyonları) halinde bulunabilmesidir. Bu durumda $a, b \in \mathbb{C}$ olmak üzere $|\psi\rangle = a|0\rangle + b|1\rangle$ değeri bir kubitin bulunabileceği hallerdir. Dolayısıyla bir kubitin durumu, iki boyutlu Hilbert vektör uzayındaki bir vektör olarak düşünülebilir [33].

Bir klasik bitin 0 ya da 1 durumunda olup olmadığı kolayca öğrenilebilirken bir kuantum bitin durumunu belirlemek yani a ve b değerlerini saptamak o kadar kolay değildir. Kuantum hali hakkında çok az bilgi bilinir. Kuantum hali hakkında bilgi edinmek için bazı ölçümler yapılır. $|\psi\rangle = a|0\rangle + b|1\rangle$, $a, b \in \mathbb{C}$ halindeki bir kuantum

bitin ölçüm sonucundaki değeri $|a|^2$ olasılığı ile $|0\rangle$, $|b|^2$ olasılığı ile $|1\rangle$ dir. Tüm olasılıklar toplamı 1 olduğundan $|a|^2 + |b|^2 = 1$ olmalıdır. Bu durum geometrik olarak bir kuantum halinin 1 uzunluğuna normalize edilmesi koşuluna karşılık gelir. Sonuç olarak bir kubitin

alabileceği değerler aşağıdaki gibidir:

$$|\psi\rangle = a|0\rangle + b|1\rangle, \quad a, b \in \mathbb{C}, \quad |a|^2 + |b|^2 = 1$$

İkili kubitler, tekli kubitler kullanılarak elde edilir. Klasik iki bit 00, 01, 10 veya 11 değerinde olabilirken ikili kubitler $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ ve $a_{00}, a_{01}, a_{10}, a_{11} \in \mathbb{C}$ olmak üzere bunların süperpozisyonları $a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle$ halini alabilir. Bu durumda iki kubitli kuantum hal uzayı 2^2 boyutlu Hilbert vektör uzayıdır. Normalleştirme koşulundan $|a_{00}|^2 + |a_{01}|^2 + |a_{10}|^2 + |a_{11}|^2 = 1$ olmalıdır. Sonuç olarak $a_{00}, a_{01}, a_{10}, a_{11} \in \mathbb{C}$ olmak üzere ikili kubitlerin bulunabileceği hal aşağıdaki gibidir:

$$|\psi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle, \quad |a_{00}|^2 + |a_{01}|^2 + |a_{10}|^2 + |a_{11}|^2 = 1$$

Bu durum benzer mantıkla n kubit için genelleştirilebilir. Bir n kubitli kuantum hal ise 2^n boyutlu Hilbert uzayındaki normu 1 olan vektördür.

3.3 Kuantum Mantık Kapıları

Günümüz bilgisayarlarında kullanılan klasik devrelerde mantık kapıları olduğu gibi bir kuantum bilgisayardaki devrelerde kuantum mantık kapıları bulunmaktadır. Mantık kapıları bir bilgiyi diğer bir bilgiye dönüştürür. Örneğin, bir klasik devredeki *NOT* kapısının işlevi

$$0 \rightarrow 1 \text{ ve } 1 \rightarrow 0$$

şeklindedir. Bu *NOT* kapısının kuantumdaki karşılığı

$$|0\rangle \rightarrow |1\rangle \text{ ve } |1\rangle \rightarrow |0\rangle$$

şeklindedir. Genel olarak bir kubitli kuantum hali $a|0\rangle + b|1\rangle$ olarak ifade edildiğinden kuantum *NOT* kapısının işlevi

$$a|0\rangle + b|1\rangle \rightarrow b|0\rangle + a|1\rangle$$

gibidir. Bu durumda kuantum *NOT* kapısı Örnek 3.4 den anlaşılacağı üzere tekli kubitler üzerinde bir lineer dönüşümdür ve matris formunda ifade edilebilir. Bu kuantum mantık kapısı X ile gösterilir ve $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ şeklindedir [33].

Bir kubitli kuantum haline etki eden bir diğer kuantum mantık kapısı Z ile gösterilir. Bu mantık kapısının işlevi

$$|0\rangle \rightarrow |0\rangle \text{ ve } |1\rangle \rightarrow -|1\rangle$$

şeklindedir. Bu etki genel olarak

$$a|0\rangle + b|1\rangle \rightarrow a|0\rangle - b|1\rangle$$

şeklinde olacağından bu mantık kapısı matris formunda $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ olarak ifade edilir[33].

Çok kullanılan mantık kapılarından olan *Hadamard* mantık kapısı ise H ile gösterilir ve işlevi

$$|0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \text{ ve } |1\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

şeklindedir. Benzer şekilde *Hadamard* mantık kapısının etkisi genel olarak

$$a|0\rangle + b|1\rangle \rightarrow \frac{a}{\sqrt{2}}(|0\rangle + |1\rangle) + \frac{b}{\sqrt{2}}(|0\rangle - |1\rangle)$$

şeklindedir. Bu durumda *Hadamard* mantık kapısı matris formunda $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ olarak ifade edilir [33].

X , Z ve H kuantum mantık kapıları gibi tekli kubit üzerindeki mantık kapıları 2×2 lik matrisler tarafından ifade edilebilir. U matrisi tekli kubite etki eden kuantum mantık kapısı olsun. Bir $|\psi\rangle$ kuantum halinin normalleştirme koşulundan dolayı normu 1 olacağından $\langle\psi|\psi\rangle=1$ dir. Ayrıca $U|\psi\rangle$ hali içinde aynı koşul geçerli olacağından

$\langle \psi | U^\dagger U | \psi \rangle = 1$ olmalıdır. Bu ise $U^\dagger U = I$ olmasını gerektirir. Bu durum üniter matris olma şartı olduğundan tüm kuantum mantık kapıları üniter matris olmak zorundadır.

Örneğin, X kapısı için $X^\dagger = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ olduğundan $X^\dagger X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = I$ dir. Z ve

H kapıları için de bu eşitlik görülebilir [33].

İkili kubit üzerinde kuantum mantık kapılarından biri $CNOT$ kapısıdır. Bu kapının etkisi

$$|00\rangle \rightarrow |00\rangle, |01\rangle \rightarrow |01\rangle, |10\rangle \rightarrow |11\rangle, |11\rangle \rightarrow |10\rangle$$

şeklindedir. İkili kubit genel olarak $a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle$ halinde olduğundan $CNOT$ kapısının iki kubitli kuantum haline etkisi

$$a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle \rightarrow a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|11\rangle + a_{11}|10\rangle$$

şeklindedir. Bu durumda $CNOT$ mantık kapısı matris formunda

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \text{ olarak ifade edilir. } CNOT \text{ kapısı için de}$$

$$CNOT^\dagger CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = I \text{ eşitliği vardır [33].}$$

Tekli kubit üzerindeki kuantum mantık kapılarına tekli kubit kapıları, çoklu kubit üzerindeki kuantum mantık kapılarına ise çoklu kubit kapıları denir. Tüm kuantum mantık kapıları birer üniter matris ve sonsuz sayıda üniter matris olduğundan sonsuz çoklu kubit kapısı vardır. Fakat bu sonsuz sayıdaki çoklu kubit kapılarını bilmeye gerek yoktur. Çünkü herhangi çoklu kubit kapısı $CNOT$ ve tekli kubit kapıları kullanılarak elde edilebilir [33].

Kuantum hesaplamada önemli bir yere sahip olan ve kuantum mantık kapılarından oluşan matris grubu vardır. Bu gruba *Pauli* matris grubu denir.

$Y = iXZ = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ olmak üzere tek kubitli kuantum haline etki eden *Pauli* matrisleri

$P = \{\pm I, \pm iI, \pm X, \pm iX, \pm Z, \pm iZ, \pm Y, \pm iY\}$ kümesidir ve P , matris çarpma işlemi ile birlikte bir değişmeli olmayan gruptur. Genel olarak n kubite etki eden *Pauli* matris grubu ile P_n gösterilir ve bu grup, P nin elemanlarının tensör çarpımından oluşur. Dolayısıyla P_n , 4^{n+1} elemanlı bir kümedir.

5 kubitli bir kuantum haline etki eden bir *Pauli* operatörü $ZIXYI$ olsun. Bu operatör kısaca birimden farklı *Pauli* operatörlerinin bileşen numaraları altlarına yazılarak $Z_1X_3Y_4$ şeklinde ifade edilir. Bu operatörün bir $|11110\rangle$ kuantum haline etkisi Tanım 3.12 de tanımlandığı gibidir. Bu durumda

$$\begin{aligned} Z_1X_3Y_4|11110\rangle &= (Z|1\rangle) \otimes (I|1\rangle) \otimes (X|1\rangle) \otimes (Y|1\rangle) \otimes (I|0\rangle) \\ &= (-|1\rangle) \otimes |1\rangle \otimes |0\rangle \otimes (-|0\rangle) \otimes |0\rangle \\ &= |11000\rangle \end{aligned}$$

olur.

3.4 Kuantum Hata Düzeltme

Kuantum kodlar Hilbert uzayı üzerinde tanımlanır. H iki boyutlu Hilbert uzayı olmak üzere $H^n = \underbrace{H \otimes H \otimes \dots \otimes H}_n$, 2^n boyutlu bir Hilbert uzayıdır. n uzunluğunda bir kuantum kod, 2^n boyutlu Hilbert uzayının bir alt uzayı olarak tanımlanır. Dolayısıyla, k kubit n kubite kodlayan n uzunluğunda bir kuantum kod, 2^n boyutlu Hilbert uzayının 2^k boyutlu alt uzayı olarak tanımlanır ve $[[n, k]]$ ile gösterilir. Kuantum kod uzayının taban elemanlarına ise kodsöz denir [39].

Örnek 3.13 3 kubitli kuantum hal uzayı 2^3 boyutlu Hilbert uzayıdır. $\{a|000\rangle + b|111\rangle : |a|^2 + |b|^2 = 1\}$ kümesi, 2^3 boyutlu Hilbert uzayın 2^1 boyutlu alt uzayıdır ve bu uzay $[[3, 1]]$ parametrelerine sahip bir kuantum koddur. Bu kuantum kodun kodsözleri ise $\{|000\rangle, |111\rangle\}$ kümesinin elemanlarıdır.

Kuantum kodlar üzerinde hataların karakterize edilmesi gerekir. Bir kuantum kod üzerinde üç tür hata meydana gelebilir:

1. Bit değişimi hatası: $|0\rangle$ halinin $|1\rangle$ e, $|1\rangle$ halinin $|0\rangle$ a dönüşmesidir. Bu

hataya *Pauli X* $= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ kapısı neden olur.

2. Faz değişimi hatası: $|0\rangle$ halinin $|0\rangle$ a, $|1\rangle$ halinin $-|1\rangle$ e dönüşmesidir. Bu

hataya *Pauli Z* $= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ kapısı neden olur.

3. Bit ve faz değişimi hatası: $|0\rangle$ halinin $|1\rangle$ e, $|1\rangle$ halinin $-|0\rangle$ a dönüşmesidir.

Bu hataya *Pauli Y* $= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ kapısı neden olur.

Klasikte olduğu gibi bir hata bir kubitte iki kere meydana gelse kuantum halini değiştirmez. Dolayısıyla kuantum kodlamada dekodlama, hatanın yerini ve hataya sebep olan *Pauli* operatörünü bulup yeri tespit edilen kubitte tekrar uygulayarak yapılır. Örneğin, $a|000\rangle + b|111\rangle$ kuantum halinde X_1 hatası meydana gelse bozulmuş hal $X_1(a|000\rangle + b|111\rangle) = a|100\rangle + b|011\rangle$ şeklinde olur. Son hale tekrar X_1 uygulanırsa $X_1(a|100\rangle + b|011\rangle) = a|000\rangle + b|111\rangle$ elde edilir ve ilk hale geri dönülür.

Bir kuantum kod kubitlerden oluşur. Kubitler ise klasik bitlerden çok farklı olduklarından kuantum hata düzeltmede bir takım zorluklar vardır. Örneğin, pek çok klasik hata düzelten kodlar geliştirilmiştir fakat bu kodlar kuantuma direkt uygulanamaz. Bunun sebebi, klasik kodlamada sadece bit hatasının düzeltilmesi yeterli iken kuantum kodlamada ise bit hatasının yanı sıra faz hatasının da düzeltilmesi gerekir. Bir başka problem ise klasik kodlamada var olan tekrarlı kod mantığının kuantum kodlamada geçerli olmamasıdır. Örneğin klasik kodlamada 00, 01, 10, 11 bilgileri 3 defa tekrar edilerek $\{000000, 010101, 101010, 111111\}$ tekrarlı kodu oluşturulabilir. Fakat keyfi bir kuantum halini $|\psi\rangle \rightarrow |\psi\rangle \otimes |\psi\rangle \otimes |\psi\rangle$ şeklinde kodlamak mümkün değildir ve bu durum kopyalanamama (no-cloning) teoremi olarak ifade edilir [31], [36].

Teorem 3.4 (Kopyalanamama) Her $|\psi\rangle$ kuantum halini $|\psi\rangle \otimes |\psi\rangle$ kuantum haline kodlayacak bir kuantum operatörü yoktur [31].

İspat: Teoremin aksi farzedilerek böyle bir kuantum operatörü var ve bu operatör U olsun. Ayrıca, $|\psi\rangle$ ve $|\phi\rangle$ farklı kuantum halleri olsun. Bu durumda

$$U|\psi\rangle \rightarrow |\psi\rangle|\psi\rangle \quad (3.5)$$

$$U|\phi\rangle \rightarrow |\phi\rangle|\phi\rangle \quad (3.6)$$

$$U(|\psi\rangle + |\phi\rangle) \rightarrow (|\psi\rangle + |\phi\rangle)(|\psi\rangle + |\phi\rangle) \quad (3.7)$$

olur. Kuantum operatör lineer olduğundan

$$U(|\psi\rangle + |\phi\rangle) \rightarrow U|\psi\rangle + U|\phi\rangle = |\psi\rangle|\psi\rangle + |\phi\rangle|\phi\rangle \quad (3.8)$$

elde edilir. Fakat

$$(|\psi\rangle + |\phi\rangle)(|\psi\rangle + |\phi\rangle) \neq |\psi\rangle|\psi\rangle + |\phi\rangle|\phi\rangle \quad (3.9)$$

olduğundan çelişki elde edilir.

Nielsen ve Chuang [33] da kuantum kodlamadaki zorlukları şöyle özetlemiştir:

- i. Kopyalanamama teoremine göre keyfi bir $|\psi\rangle$ hali kopyalanamaz. Bu durumda, tekrarlı kod üretilemez.
- ii. Ölçüm kuantum bilgiyi yıkar. Gözlem, gözlem altındaki kuantum halini geri dönüşümü mümkün olmayacak şekilde zarar verebilir.
- iii. Bir kubit sürekli olduğundan tek kubit üzerinde farklı hatalar süreklilik oluşturur. Yani, kuantum kanalında bir kubite farklı hataların bir dizisi etki eder. Bu yüzden hatayı saptamak için sonsuz tahmin gerekir.

Birinci zorluk $\{|0\rangle, |1\rangle\}$ tabanını kod uzayının $\{|0_L\rangle, |1_L\rangle\}$ mantıksal (logical) tabanına kodlayarak aşılabılır.

$$|0\rangle \rightarrow |0_L\rangle, |1\rangle \rightarrow |1_L\rangle$$

Dolayısıyla bir $|\psi\rangle = a|0\rangle + b|1\rangle$ kuantum hali $|\psi\rangle = a|0\rangle + b|1\rangle \rightarrow |\psi'\rangle = a|0_L\rangle + b|1_L\rangle$

olarak kodlanır. Bu kodlama yöntemi klasikteki tekrarlı kodun kuantumdaki karşılığı olarak düşünülebilir [36]. Örneğin, $|0\rangle \rightarrow |0_L\rangle = |000\rangle$, $|1\rangle \rightarrow |1_L\rangle = |111\rangle$ olsun. Bu durumda $|\psi\rangle = a|0\rangle + b|1\rangle$ kuantum halinin kodlanmış hali $|\psi'\rangle = a|000\rangle + b|111\rangle$ olur.

İkinci zorluk klasik hata düzeltmede olduğu gibi kuantumda da sendrom ölçümü yapılarak aşılır [36].

Üçüncü zorluğun aşılmasında ise *Pauli* matris grubu işe yarar. Bir kubitte etki eden herhangi bir hata *Pauli* matrislerinin bir lineer toplamı olarak yazılabilir. Dolayısıyla *Pauli X*, *Pauli Z* ve *Pauli Y* hataları düzeltilebildiği sürece tüm hatalar düzeltilebilir [36].

Kuantum kodların hata farketme ve düzeltme koşulları üzerine çalışılmıştır. Bu koşullar verilmeden önce klasik kodlarla ilgili şu gözlemler yapılmalıdır [35]:

- i. C bir klasik kod ve $E = \{e_0, e_1, \dots\}$, C kodun farkedebildiği hataların kümesi olsun. Bu durumda E deki herhangi bir hatanın C deki herhangi bir kodsözde meydana gelmesi ile oluşan sözün C de olmaması gerekir. Yani, her $c \in C$ ve her $e_i \in E$ için $e_i c \notin C$ olmalıdır.
- ii. C bir klasik kod ve $E = \{e_0, e_1, \dots\}$, C kodun düzeltilebildiği hataların kümesi olsun. Bu durumda E deki herhangi bir hatanın C deki herhangi bir kodsözde meydana gelmesi ile oluşan sözün yine, E deki herhangi bir hatanın C deki farklı bir kodsözde meydana gelmesi ile elde edilememelidir. Yani, $c_i \neq c_j$ olmak üzere her $c_i, c_j \in C$ ve her $e_k, e_l \in E$ için $e_k c_i \neq e_l c_j$ olmalıdır.
- iii. ii. nin bir sonucu olarak klasik kodlar için hata düzeltme koşulu tekrar düzenlenebilir. Hata düzeltme şartı $c_i \neq c_j$ olmak üzere her $c_i, c_j \in C$ ve her $e_k, e_l \in E$ için $e_k c_i \neq e_l c_j$ idi. Bu durumda $e_l^{-1} e_k c_i \neq c_j$ olur. Bu ise i. den $e_l^{-1} e_k$ hatasının farkedilebilir olması demektir.
- iv. iii. sonucu bir C klasik kodun minimum uzaklığı ile düzeltilebildiği hatalar arasındaki ilişkiyi verir. Bu durumda C kodun t hata düzeltilebilmesi için gerek ve yeter koşul $d(C) \geq 2t + 1$ olmasıdır.

Örnek 3.14 $C = \{000, 111\}$ klasik kodun farkedebileceği hatalar $A = \{000, 100, 010, 001, 110, 011, 101\}$ kümesi iken düzeltebileceği hatalar $B = \{000, 100, 010, 001\}$ kümesidir. B kümesindeki herhangi iki hatanın toplamının A da olduğu görülür.

C bir kuantum kod ve P , C üzerinde bir projeksiyon operatör olsun. C kuantum kodundaki herhangi bir $|\psi\rangle$ kuantum halinde E hatası meydana geldikten sonra $|\psi\rangle$ kuantum hali P projektörü altında katsayı hariç sabit kalıyorsa E ye C kuantum kodu tarafından farkedilebilir denir. Yani, her $|\psi_i\rangle \in C$ için $PE|\psi_i\rangle = \lambda_E |\psi_i\rangle$ dir. Her $|\psi_i\rangle \in C$ için $P|\psi_i\rangle \in C$ olduğundan $PEP = \lambda_E P$ elde edilir [36].

Teorem 3.5 P , C üzerinde bir projeksiyon operatör olsun. $E = \{E_0 = I, E_1, \dots\}$ kümesi C kuantum kodu tarafından farkedilebilir hatalardır ancak ve ancak $\lambda_i \in \mathbb{C}$ olmak üzere her $E_i \in E$ için $PEP = \lambda_i P$ dir [36].

Bu teorem aşağıdaki gibi düzenlenebilir.

Teorem 3.6 $E = \{E_0 = I, E_1, \dots\}$ kümesi C kuantum kodun fark edebildiği hataların kümesi olması için gerek ve yeter koşul $\lambda_i \in \mathbb{C}$ olmak üzere her $|\psi\rangle, |\phi\rangle \in C$ ve her $E_i \in E$ için $\langle\psi|E_i|\phi\rangle = \lambda_i \langle\psi|\phi\rangle$ olmasıdır [36].

$|\psi\rangle, |\phi\rangle \in C$ olmak üzere eğer $|\psi\rangle, |\phi\rangle$ ye dik ise $\langle\psi|\phi\rangle = 0$ dir. E hata operatörü C kodu tarafından farkedilebilir ise $\langle\psi|E_i|\phi\rangle = \lambda_i \langle\psi|\phi\rangle$ olacağından $|\psi\rangle$ nin $|\phi\rangle$ haline dik olması durumunda $\langle\psi|E_i|\phi\rangle = 0$ olur. Bu durum teoremle ifade edilebilir.

Teorem 3.7 $E = \{E_0 = I, E_1, \dots\}$ kümesi C kuantum kodu tarafından farkedilebilir hatalardır ancak ve ancak $\langle\psi|\phi\rangle = 0$ olmak üzere her $|\psi\rangle, |\phi\rangle \in C$ için $\langle\psi|E_i|\phi\rangle = 0$ eşitliği sağlanır [36].

C bir kuantum kod olsun. $E = \{E_0 = I, E_1, \dots\}$ kümesinin C kuantum kodun düzeltebildiği hatalar olması halinde her $E_i, E_j \in E$ ve her $|\psi\rangle, |\phi\rangle \in C$ için

$E_i|\psi\rangle \neq E_j|\phi\rangle$ olmalıdır. Bu durumda $E_j^{-1}E_i|\psi\rangle \neq |\phi\rangle$ olur. Bu ise $E_j^{-1}E_i$ hatasının farkedilebilir olması demektir. Teorem 3.5 ten aşağıdaki sonuç elde edilir.

Teorem 3.8 P, C üzerinde bir projeksiyon operatör olsun. $E = \{E_0 = I, E_1, \dots\}$ kümesi C kuantum kodu tarafından düzeltilebilir hatalardır ancak ve ancak $\lambda_{ij} \in \mathbb{C}$ olmak üzere her $E_i, E_j \in E$ için $PE_i^\dagger E_j P = \lambda_{ij} P$ eşitliği vardır [36].

Bu teorem, Teorem 3.6 sayesinde yeniden ifade edilebilir.

Teorem 3.9 $E = \{E_0 = I, E_1, \dots\}$, C kuantum kodu tarafından düzeltilebilir hataların kümesi olması için gerek ve yeter koşul $\lambda_{ij} \in \mathbb{C}$ olmak üzere her $|\psi\rangle, |\phi\rangle \in C$ ve her $E_i, E_j \in E$ için $\langle\psi|E_i^\dagger E_j|\phi\rangle = \lambda_{ij} \langle\psi|\phi\rangle$ eşitliğinin sağlanmasıdır [36].

$E = \{E_0 = I, E_1, \dots\}$ kümesi C kuantum kodun düzeltebildiği hatalar ise her $E_i, E_j \in E$ için $E_i^\dagger E_j$, C tarafından farkedilebilir olmalıdır. Teorem 3.7 den $\langle\psi|\phi\rangle = 0$ olmak üzere her $|\psi\rangle, |\phi\rangle \in C$ için $E_i^\dagger E_j|\psi\rangle, |\phi\rangle$ ya dik yani $\langle\phi|E_i^\dagger E_j|\psi\rangle = 0$ olmalıdır. Bu ise $E_j|\psi\rangle$ nin $E_i|\phi\rangle$ ye dik olması anlamına gelir.

Teorem 3.10 $E = \{E_0 = I, E_1, \dots\}$ kümesi C kuantum kodun düzeltebildiği hatalardır ancak ve ancak $\langle\psi|\phi\rangle = 0$ olmak üzere her $|\psi_k\rangle, |\psi_l\rangle \in C$ ve her $E_i, E_j \in E$ için $\langle\phi|E_i^\dagger E_j|\psi\rangle = 0$ olmalıdır [36].

Daha genel olarak $E = \{E_0 = I, E_1, \dots\}$ kümesi C kuantum kodun düzeltebildiği hatalardır ancak ve ancak her $|\psi_k\rangle, |\psi_l\rangle \in C$ ve her $E_i, E_j \in E$ için $\langle\psi_k|E_j^\dagger E_i|\psi_l\rangle = \lambda_{ij} \delta_{kl}$ olmalıdır. Burada $\lambda_{ij} \in \mathbb{C}$ ve δ_{kl} , Kronecker deltasıdır [31], [32].

Bir E Pauli hatasının ağırlığı I dan farklı bileşenlerin sayısı olarak tanımlanır. Örneğin, $E = XIZI$ hatasının ağırlığı 2 dir. Bir C kuantum kodun minimum uzaklığı, C kodun farkedemediği hataların ağırlıklarının en küçüğü olarak tanımlanır. Bu durumda C kuantum kodun minimum uzaklığı ile düzeltebildiği hataların ağırlığı arasındaki ilişki verilebilir.

Teorem 3.11 Bir C kuantum kodun minimum uzaklığı $2t+1$ ise C kodu en fazla t ağırlıklı hata düzeltebilir [36].

Örnek 3.15 (Shor Kod)

$$|0_L\rangle = \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)$$

ve

$$|1_L\rangle = \frac{1}{2\sqrt{2}}(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)$$

olmak üzere bir $|\psi\rangle = a|0\rangle + b|1\rangle$ kuantum halinin

$$|\psi\rangle = a|0\rangle + b|1\rangle \rightarrow |\psi'\rangle = a|0_L\rangle + b|1_L\rangle$$

şeklinde kodlanmasıyla elde edilen kuantum koduna Shor kodu denir. Shor kodun açık hali ise

$$\begin{aligned} |\psi'\rangle = & \frac{a}{2\sqrt{2}} \left(|000000000\rangle + |000000111\rangle + |000111000\rangle + |000111111\rangle \right) \\ & + \frac{b}{2\sqrt{2}} \left(|000000000\rangle - |000000111\rangle - |000111000\rangle + |000111111\rangle \right) \\ & + \frac{a}{2\sqrt{2}} \left(|111000000\rangle + |111000111\rangle + |111111000\rangle + |111111111\rangle \right) \\ & + \frac{b}{2\sqrt{2}} \left(|111000000\rangle - |111000111\rangle - |111111000\rangle + |111111111\rangle \right) \end{aligned}$$

şeklindedir. Bu durumda Shor kodun kodsözleri $|0_L\rangle$ ve $|1_L\rangle$ olur. $|0_L\rangle$ ve $|1_L\rangle$ kodsözlerinin iç-çarpımı $\langle 0_L | 1_L \rangle = 0$ dir. $E = \{X_1, \dots, X_9, Z_1, \dots, Z_9, Y_1, \dots, Y_9\}$, 1 ağırlıklı tüm hataların kümesi olsun. Her $E_i, E_j \in E$ için $\langle 0_L | E_j^\dagger E_i | 1_L \rangle = 0$ olduğundan Shor kodu 1 ağırlıklı tüm hataları düzeltebilir. E' , 2 ağırlıklı hataların kümesi olmak üzere her $E_i \in E'$ için $\langle 0_L | E_i | 1_L \rangle = 0$ olduğundan Teorem 3.4.6 dan Shor kodu 2 ağırlıklı hataları farkedebilir. 3 ağırlıklı bir hata $Z_1 Z_4 Z_7$ olsun. $|1_L\rangle$ kodsözünde $Z_1 Z_4 Z_7$ hatası meydana gelirse son durum

$$Z_1 Z_4 Z_7 |1_L\rangle = \frac{1}{2\sqrt{2}} \left(|000000000\rangle + |000000111\rangle + |000111000\rangle + |000111111\rangle \right) \\ + \frac{1}{2\sqrt{2}} \left(|111000000\rangle + |111000111\rangle + |111111000\rangle + |111111111\rangle \right)$$

olur. Bu durumda $\langle 0_L | Z_1 Z_4 Z_7 | 1_L \rangle = 8 \neq 0$ olduğundan Teorem 3.4.6 dan $Z_1 Z_4 Z_7$, Shor kodun farkedemediği 3 ağırlıklı bir hatadır. Dolayısıyla Shor kodun minimum uzaklığı 3 tür.

4.1 CSS Kod İnşası

CSS (Calderbank, Shor, Steane) kod, Calderbank, Shor ve eş zamanlı olarak Steane tarafından ortaya konulan bir kuantum kod yapısıdır [2,3]. Bu kod yapısı klasik lineer kodlar ile kuantum kod arasında bir köprü olmuş ve kuantum kod bulma prblemini dualini içeren lineer kod bulma problemine çevirmiştir.

Tanım 4.1 C_1 ve C_2 sırasıyla $[n, k_1]$ ve $[n, k_2]$ parametrelerine sahip iki klasik lineer kod ve $C_2 \subseteq C_1$ olsun. $x \in C_1$ olmak üzere kodsözleri,

$$|x + C_2\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x + y\rangle \quad (4.1)$$

olarak tanımlanan kuantum koda $\llbracket n, k_1 - k_2 \rrbracket$ parametrelerine sahip bir CSS kod denir ve kısaca $CSS(C_1, C_2)$ ile gösterilir. Burada $+$, mod 2 ye göre bit toplamıdır. Eğer $d(C_1) = d_1$ ve $d(C_2^\perp) = d_2$ ise $CSS(C_1, C_2)$ kuantum kodun parametreleri $\llbracket n, k_1 - k_2, \min\{d_1, d_2\} \rrbracket$ dir. Eğer $d(C_1) = d(C_2^\perp) = d$ ise $CSS(C_1, C_2)$, $\llbracket n, k_1 - k_2, d \rrbracket$ parametrelili bir kuantum koddur [33].

$C_1^\perp \subseteq C_1$ ise $C_2 = C_1^\perp$ olarak seçilir. Bu durumda $d(C_1) = d((C_1^\perp)^\perp) = d(C_2^\perp) = d$ olur.

Dolayısıyla $\llbracket n, k_1 - k_2, d \rrbracket$ parametrelili bir kuantum kod elde etmek için d minimum uzaklığında sahip dualini içeren klasik lineer kod bulmak yeterlidir.

Tanımdan da anlaşılacağı üzere bir $CSS(C_1, C_2)$ kodun parametreleri tamamen C_1 ve $C_2^\perp$ klasik lineer kodların parametrelerine bağlıdır. $x_1, x_2 \in C_1$ olmak üzere $x_1 - x_2 \in C_2$ ise $|x_1 + C_2\rangle = |x_2 + C_2\rangle$ olur. Bu durumda $CSS(C_1, C_2)$ kodun kodsözleri C_2 nin C_1 deki farklı kosetlerine bağlıdır. Dolayısıyla $CSS(C_1, C_2)$ kodun farklı kodsözlerinin sayısı C_2 nin C_1 deki farklı kosetlerinin sayısı $\frac{|C_1|}{|C_2|} = 2^{k_1 - k_2}$ kadardır. Buradan $CSS(C_1, C_2)$ kuantum kodun boyutunun $k_1 - k_2$ olduğu görülür.

Örnek 4.1 (Steane Kod) $C_1, [7, 4, 3]$ Hamming kod ve $C_2 = C_1^\perp$ olsun. Bu durumda C_1 ve C_2 lineer kodları açık olarak sırasıyla

$$C_1 = \left\{ \begin{array}{l} 0000000, 0001011, 0010110, 0011101, 0100111, 0101100, 0110001, 0111010, \\ 1000101, 1001110, 1010011, 1011000, 1100010, 1101001, 1110100, 1111111 \end{array} \right\}$$

ve

$C_2 = \{0000000, 0011101, 0100111, 0111010, 1001110, 1010011, 1101001, 1110100\}$ şeklindedir. Buradan C_2 nin bir $[7, 3, 4]$ lineer kod ve $C_2 \subset C_1$ olduğu görülür.

$$\frac{|C_1|}{|C_2|} = \frac{2^4}{2^3} = 2 \quad \text{ve} \quad \min\{d(C_1), d(C_2^\perp)\} = 3 \quad \text{olduğundan Tanım 4.1 den } [[7, 1, 3]]$$

parametrelili bir CSS kuantum kod vardır. Bu kuantum kodun kodsözleri ise

$$|0000000 + C_2\rangle = \frac{1}{2\sqrt{2}} \left(|0000000\rangle + |0011101\rangle + |0100111\rangle + |0111010\rangle + |1001110\rangle + |1010011\rangle + |1101001\rangle + |1110100\rangle \right)$$

ve

$$|1111111 + C_2\rangle = \frac{1}{2\sqrt{2}} \left(|0001011\rangle + |0010110\rangle + |0101100\rangle + |0110001\rangle + |1000101\rangle + |1011000\rangle + |1100010\rangle + |1111111\rangle \right)$$

şeklindedir.

4.2 CSS Kuantum Kodlarda Dekodlama

Bir $CSS(C_1, C_2)$ kuantum kodun hata düzeltme kapasitesi C_1 ve $C_2^\perp$ klasik lineer kodların hata düzeltme kapasitelerine bağlıdır. Kuantum kodda oluşabilecek bit hatasını düzeltmek için C_1 den, faz hatasını düzeltmek için de $C_2^\perp$ den yararlanılır. Dekodlamanın nasıl yapıldığı verilmeden önce şu bilgilere ihtiyaç vardır:

- i. E hata operatöründeki bit ve faz hatalarına karşılık gelen klasik hatalar sırasıyla e_1 ve e_2 olsun. Bu durumda E nin bir $|x\rangle$ kuantum haline etkisi

$$E|x\rangle = (-1)^{\langle x, e_2 \rangle} |x + e_1\rangle \quad (4.2)$$

şeklindedir. Örneğin, $E = XZX$ ve $|x\rangle = |011\rangle$ olsun. Bu durumda $e_1 = 101$ ve $e_2 = 010$ olur. E nin $|x\rangle$ haline etkisi ise $E|x\rangle = (XZX)|011\rangle = -|110\rangle$ şeklindedir. Ayrıca $E|x\rangle = (-1)^{\langle 011, 010 \rangle} |011 + 101\rangle = -|110\rangle$ olur.

- ii. n kubitli bir $|x\rangle$ halinin her bir kubitine *Hadamard* kapısı etki ederse son durum

$$\frac{1}{\sqrt{2^n}} \sum_{z \in \mathbb{Z}_2^n} (-1)^{\langle x, z \rangle} |z\rangle \quad (4.3)$$

olur. Örneğin, $|x\rangle = |010\rangle$ kuantum halinin her bir kubitine *Hadamard* kapısı etki ederse

$$\begin{aligned} HHH|010\rangle &= \frac{1}{2\sqrt{2}} (|0\rangle + |1\rangle)(|0\rangle - |1\rangle)(|0\rangle + |1\rangle) \\ &= \frac{1}{2\sqrt{2}} \left(|000\rangle + |001\rangle - |010\rangle - |011\rangle \right. \\ &\quad \left. + |100\rangle + |101\rangle - |110\rangle - |111\rangle \right) \end{aligned}$$

olur. Aynı zamanda

$$HHH|010\rangle = \frac{1}{2\sqrt{2}} \begin{pmatrix} (-1)^{\langle 010, 000 \rangle} |000\rangle + (-1)^{\langle 010, 001 \rangle} |001\rangle + (-1)^{\langle 010, 010 \rangle} |010\rangle + \\ (-1)^{\langle 010, 100 \rangle} |100\rangle + (-1)^{\langle 010, 011 \rangle} |011\rangle + (-1)^{\langle 010, 101 \rangle} |101\rangle + \\ (-1)^{\langle 010, 110 \rangle} |110\rangle + (-1)^{\langle 010, 111 \rangle} |111\rangle \end{pmatrix}$$

$$= \frac{1}{2\sqrt{2}} \left(|000\rangle + |001\rangle - |010\rangle + |100\rangle - |011\rangle + |101\rangle - |110\rangle - |111\rangle \right).$$

- iii. Klasik kodlamada yardımcı bitler kullanıldığı gibi kuantum kodlamada da ancilla adı verilen yardımcı kubitler kullanılmaktadır.

Bir $|x + C_2\rangle$ kuantum halinde E hatası meydana gelsin. E hatasındaki bit ve faz hatalarına karşılık gelen klasik hatalar sırasıyla e_1 ve e_2 olmak üzere bozulmuş hal

$$\frac{1}{\sqrt{C_2}} \sum_{y \in C_2} (-1)^{\langle x+y, e_2 \rangle} |x + y + e_1\rangle \quad (4.4)$$

şeklinde dir. Bit hatasını düzeltmek için C_1 in hata düzeltmesinden yararlanılır. e_1 hatasının sendromunu öğrenmek için yeterli miktarda ancilla eklenir. C_1 kodun kontrol matrisi H_1 olmak üzere $x + y \in C_1$ olduğundan $H_1(x + y + e_1)^{tr} = H_1 e_1^{tr}$ olur. Bu durumda $|x + y + e_1\rangle |H_1(x + y + e_1)^{tr}\rangle = |x + y + e_1\rangle |H_1 e_1^{tr}\rangle$ olduğundan

$$\frac{1}{\sqrt{C_2}} \sum_{y \in C_2} (-1)^{\langle x+y, e_2 \rangle} |x + y + e_1\rangle |H_1 e_1^{tr}\rangle \quad (4.5)$$

elde edilir. $H_1 e_1^{tr}$ sonucunu elde etmek için eklenen ancilla göz ardı edilirse son hal

$$\frac{1}{\sqrt{C_2}} \sum_{y \in C_2} (-1)^{\langle x+y, e_2 \rangle} |x + y + e_1\rangle \quad (4.6)$$

olur. $\frac{1}{\sqrt{C_2}} \sum_{y \in C_2} (-1)^{\langle x+y, e_2 \rangle} |x + y + e_1\rangle$ hata sendromu bilindiğinden e_1 hatası bilinir. Bit

hatasının dekodlaması ise kuantum haline, e_1 e karşılık gelen hata operatörünü uygulamaktır. Böylece son durum

$$\frac{1}{\sqrt{C_2}} \sum_{y \in C_2} (-1)^{\langle x+y, e_2 \rangle} |x + y\rangle \quad (4.7)$$

olur. Faz hatasını düzeltmek için $C_2^\perp$ kodun hata düzeltmesinden yararlanılır. Öncelikle her bir kubitte *Hadamard* mantık kapısı uygulanır. Bu durumda son hal

$$\frac{1}{\sqrt{2^n C_2}} \sum_{z \in \mathbb{Z}_2^n} \sum_{y \in C_2} (-1)^{\langle x+y, e_2+z \rangle} |z\rangle \quad (4.8)$$

olur. Burada $z = z' + e_2 \pmod{2}$ alınır

$$\frac{1}{\sqrt{2^n C_2}} \sum_{z' \in \mathbb{Z}_2^n} \sum_{y \in C_2} (-1)^{\langle x+y, z' \rangle} |z' + e_2\rangle \quad (4.9)$$

elde edilir. $z' \notin C_2^\perp$ iken $\sum_{y \in C_2} (-1)^{\langle y, z' \rangle} = 0$ ve $z' \in C_2^\perp$ iken $\sum_{y \in C_2} (-1)^{\langle y, z' \rangle} = |C_2|$

olduğundan

$$\sqrt{\frac{|C_2|}{2^n}} \sum_{z' \in C_2^\perp} (-1)^{\langle x, z' \rangle} |z' + e_2\rangle \quad (4.10)$$

olur. e_2 hatasının tespiti e_1 hatasının tespiti gibi yapılır ve $H_2, C_2^\perp$ kodun kontrol matrisi olmak üzere $H_2 e_2^{tr}$ sonucu e_2 hatasını verecektir. Faz hatasının dekodlaması için yapılması gereken ise kuantum haline e_2 ye karşılık gelen hata operatörünü uygulamaktır. Böylece son durum

$$\sqrt{\frac{|C_2|}{2^n}} \sum_{z' \in C_2^\perp} (-1)^{\langle x, z' \rangle} |z'\rangle \quad (4.11)$$

olur. İlk hali elde etmek için yapılması gereken işlem her bir kubite tekrar *Hadamard* kapısını uygulamaktır [3], [33].

Örnek 4.2 Örnek 4.1 deki $\frac{1}{2\sqrt{2}} \left(|0000000\rangle + |0011101\rangle + |0100111\rangle + |0111010\rangle + |1001110\rangle + |1010011\rangle + |1101001\rangle + |1110100\rangle \right)$

kuantum hali $\frac{1}{2\sqrt{2}} \left(|0100000\rangle - |0111101\rangle + |0000111\rangle - |0011010\rangle + |1101110\rangle - |1110011\rangle + |1001001\rangle - |1010100\rangle \right)$ şeklinde

bozulsun. Örnek 4.1 deki $[7, 4, 3]$ Hamming kodun kontrol matrisi

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix} \text{ olduğundan } H(0100000)^{tr} = 110 \text{ elde edilir. Örnek 2.30}$$

daki gibi $[7, 4, 3]$ Hamming kodun sendrom tablosundan e_1 hatasının 0100000 olduğu görülür. e_1 hatasına karşılık gelen hata operatörü $IXIIII$ şeklindedir. Bu hata operatörü bozulmuş hale uygulandığında

$$\frac{1}{2\sqrt{2}} \left(|0000000\rangle - |0011101\rangle + |0100111\rangle - |0111010\rangle - |1001110\rangle + |1010011\rangle + |1101001\rangle - |1110100\rangle \right)$$

elde edilir ve böylece kuantum halinde meydana gelen bit hatası düzeltilmiş olur. Bu son halin herbir kubitine *Hadamard* kapısı uygulanır ve geri kalan işlemler gerçekleştirilirse e_2 hatasının 0010000 olduğu görülür. Bu durumda e_2 hatasına karşılık gelen hata operatörü $IIZIII$ şeklindedir. Dekodlama ise kuantum haline $IIZIII$ uygulandıktan sonra tekrar herbir kubitte *Hadamard* kapısını uygulayarak yapılır.

4.3 Klasik Lineer Kodlardan CSS Kod İnşası İle Kuantum Kod Elde Etme

CSS kod yapısı ile kuantum kod bulma problemi dualini içeren klasik lineer kod bulma problemine dönüşmüş ve bu alanda pek çok çalışma yapılmıştır. [13] te BCH kodların dualini içerme şartı araştırılmış ve *CSS* kod inşası yardımıyla elde edilen kuantum kodun parametreleri verilmiştir. Aşağıdaki önermede her bir devirsel kosetin eleman sayısının aynı olma şartı verilmiştir.

Önerme 4.1 $n \geq 1$, q bir asalın kuvveti ve $(n, q) = 1$ olsun. Ayrıca $q^m \equiv 1 \pmod{n}$ ve $q^{\lfloor m/2 \rfloor} < n \leq q^m - 1$ olsun. $1 \leq x \leq nq^{\lfloor m/2 \rfloor} / (q^m - 1)$ koşulunu sağlayan her x için devirsel kosetin eleman sayısı m kadardır [13].

İspat: $m = 1$ ise tüm x ler için $|C_x| = 1$ olur. $m > 1$ ve $|C_x| < m$ olsun. Bu durumda $xq^j \equiv x \pmod{n}$ yani $x(q^j - 1) \equiv 0 \pmod{n}$ olacak şekilde m nin bir j böleni vardır.

Eğer m çift ise $j|m$ olduğundan $1 \leq j \leq m/2$ dir. Fakat

$x(q^j - 1) \leq nq^{m/2} (q^{m/2} - 1) / (q^m - 1) < n$ olduğundan $x(q^j - 1) \not\equiv 0 \pmod{n}$ elde edilir.

Bu ise $|C_x| < m$ olması ile çelişir. m tek ise $j|m$ olduğundan $1 \leq j \leq m/3$ tür. $m \geq 3$ için $q^{(m+1)/2} \leq q^{2m/3}$ olduğundan

$$x(q^j - 1) \leq nq^{(m+1)/2} (q^{m/3} - 1) / (q^m - 1) \leq nq^{2m/3} (q^{m/3} - 1) / (q^m - 1) < n$$

dir ve dolayısıyla $x(q^j - 1) \not\equiv 0 \pmod{n}$ elde edilir. Bu ise $|C_x| < m$ olması ile çelişir.

Bir sonraki önermede ise herhangi iki devirsel kosetin ayrık olma koşulu verilmiştir.

Önerme 4.2 $n \geq 1$, q bir asalın kuvveti ve $(n, q) = 1$ olsun. Ayrıca $q^m \equiv 1 \pmod{n}$ ve $q^{\lfloor m/2 \rfloor} < n \leq q^m - 1$ olsun. Eğer $x, y \not\equiv 0 \pmod{n}$ olmak üzere x ve y tamsayıları için $1 \leq x, y \leq \min \left\{ \left\lfloor \left(nq^{\lfloor m/2 \rfloor} / (q^m - 1) \right) - 1 \right\rfloor, n - 1 \right\}$ ise x ve y nin $\text{mod } n$ ye göre q -lu devirsel kosetleri ayrıktır [13].

İspat: $m = 1$ için $C_x = \{x\}$, $C_y = \{y\}$ olacağından C_x ve C_y ayrıktır. $m > 1$ ise $x, y \leq \left\lfloor \left(nq^{\lfloor m/2 \rfloor} / (q^m - 1) \right) - 1 \right\rfloor < n - 1$ dir. $q^{\lfloor m/2 \rfloor} \times \left\lfloor \left(nq^{\lfloor m/2 \rfloor} / (q^m - 1) \right) - 1 \right\rfloor < n$ olduğundan $xq^j \pmod{n}$ lerin hiçbiri aynı değildir. Aynı şekilde $yq^j \pmod{n}$ lerin de hiçbiri aynı değildir. Dolayısıyla $S = \{xq^j \pmod{n}, yq^j \pmod{n} : 0 \leq j \leq \lfloor m/2 \rfloor\}$ kümesi $2(\lfloor m/2 \rfloor + 1) \geq m + 1$ tane eleman içerir. İki devirsel koset ayrık olmadığında aynı olacağından C_x ile C_y ayrık değilse $C_x = C_y$ olur. Bu durumda $|C_x| = |C_y| \geq |S| \geq m + 1$ dir. Bu ise Önerme 4.1 den bir devirsel kosetin eleman sayısının en fazla m olması ile çelişir. Sonuç olarak C_x ve C_y devirsel kosetleri ayrıktır.

Örnek 4.3 $q = 2$ ve $n = 15$ olsun. $q^m \equiv 1 \pmod{n}$ olacağından $m = 4$ tür ve $2^{\lfloor 4/2 \rfloor} < n = 15 \leq 2^4 - 1$ şartı sağlanır. 2 nin $\text{mod } 15$ e göre devirsel kalan sınıfları $C_0 = \{0\}$, $C_1 = \{1, 2, 4, 8\}$, $C_3 = \{3, 6, 12, 9\}$, $C_5 = \{5, 10\}$, $C_7 = \{7, 14, 13, 11\}$ şeklindedir. Önerme 4.1 e göre her $1 \leq x \leq \frac{15 \times 2^{\lfloor 4/2 \rfloor}}{15} = 4$ için $|C_x| = 4$ olduğu görülür.

Ayrıca Önerme 4.2 ye göre her $1 \leq x, y \leq \min \left\{ \left\lfloor \frac{15 \times 2^{\lfloor 4/2 \rfloor}}{15} - 1 \right\rfloor, 15 - 1 \right\} = \min \{3, 14\}$ tamsayıları için C_1 ile C_3 kosetleri ayrık olmalıdır. Gerçekten de C_1 ile C_3 ayrık devirsel kosetlerdir.

Önerme 4.1 ve Önerme 4.2 nin bir sonucu olarak dar anlamda BCH kodların boyutu için aşağıdaki teorem verilebilir.

Teorem 4.1 $n \geq 1$, q bir asalın kuvveti ve $q^m \equiv 1 \pmod{n}$ olmak üzere $(n, q) = 1$ olsun. F_q üzerinde $q^{\lfloor m/2 \rfloor} < n \leq q^m - 1$ uzunluklu $2 \leq \delta \leq \min \left\{ \left\lfloor \frac{nq^{\lceil m/2 \rceil}}{(q^m - 1)} \right\rfloor, n \right\}$ tasarlanmış minimum uzaklığa sahip bir dar anlamda BCH kodun boyutu $k = n - m \lceil (\delta - 1)(1 - 1/q) \rceil$ kadardır [13].

İspat: Bir BCH kodun tanımlayıcı kümesi $Z = C_1 \cup C_2 \cup \dots \cup C_{\delta-1}$, en fazla $\delta - 1$ ayrık devirsel kosetin birleşimidir. Fakat $1 \leq x \leq \delta - 1$ iken $q \nmid x$ ise $C_{q/x} = C_x$ dir. Bu şekildeki kosetlerin sayısı ise $\lfloor (\delta - 1)/q \rfloor$ kadardır. Böylece $\delta - 1 - \lfloor (\delta - 1)/q \rfloor = \lceil (\delta - 1)(1 - 1/q) \rceil$ ayrık koset vardır ve Önerme 4.1 den her bir kosetin eleman sayısı m kadardır. Bu durumda BCH kodun üreteç polinomunun derecesi $m \lceil (\delta - 1)(1 - 1/q) \rceil$ olur. Bir BCH kodun boyutu $k = n - \deg(g(x))$ olduğundan $k = n - m \lceil (\delta - 1)(1 - 1/q) \rceil$ elde edilir.

Bir BCH kodun δ tasarlanmış uzaklığı ile dual kodun minimum uzaklığı arasındaki ilişki aşağıdaki gibi verilebilir.

Önerme 4.3 C , F_q üzerinde $2 \leq \delta \leq \delta_{\max} = \left\lfloor \frac{n(q^{\lceil m/2 \rceil} - 1 - (q - 2)[m, \text{tek}])}{(q^m - 1)} \right\rfloor$ tasarlanmış minimum uzaklığa sahip n uzunluğunda bir BCH kod ise dual kodun minimum uzaklığı $d^\perp \geq \delta_{\max} + 1$ dir [13].

İspat: $N = \{0, 1, \dots, n - 1\}$ ve Z_δ , C nin tanımlayıcı kümesi olsun. $Z_{\delta_{\max}} \supseteq Z_\delta \supseteq \{1, \dots, \delta - 1\}$ olduğundan $N/Z_{\delta_{\max}} \subseteq N/Z_\delta$ dir. Ayrıca, Teorem 4.3 ve Önerme 2.5 ten $2 \leq \delta \leq \delta_{\max}$ için $Z \cap Z^{-1} = \emptyset$ dir. Bu durumda $Z_{\delta_{\max}}^{-1} \subseteq N/Z_{\delta_{\max}} \subseteq N/Z_\delta$ elde edilir. T_δ , dual kodun tanımlayıcı kümesi ise $T_\delta = (N/Z_\delta)^{-1} \supseteq Z_{\delta_{\max}}$ şeklindedir. $\{0\} \in N/Z_\delta$ olduğundan $\{0\} \in T_\delta$ dir. Dolayısıyla T_δ da en az $\delta_{\max}$ kadar ayrık kök vardır. Sonuç olarak dual kodun minimum uzaklığı için $d^\perp \geq \delta_{\max} + 1$ sağlanır.

Teorem 4.1 ve Önerme 4.3 den yararlanılarak CSS kod inşası yardımıyla elde edilen kuantum kodun parametreleri verilebilir.

Teorem 4.2 q , bir asalın kuvveti olmak üzere $q^m \equiv 1 \pmod{n}$, $m \geq 2$ olsun. Ayrıca

$$2 \leq \delta_1 < \delta_2 \leq \delta_{\max} = \frac{n}{q^m - 1} \left(q^{\lceil m/2 \rceil} - 1 - (q-2)[m, \text{tek}] \right) \quad \text{olsun.} \quad \text{Bu} \quad \text{durumda}$$

$\llbracket n, m(\delta_2 - \delta_1 - \lfloor (\delta_2 - 1)/q \rfloor + \lfloor (\delta_1 - 1)/q \rfloor), \geq \delta_1 \rrbracket_q$ parametrelerine sahip kuantum kod vardır [13].

İspat: C_1 ve C_2 , sırasıyla, Teorem 4.2 de verilen δ_1 ve δ_2 tasarlanmış minimum uzaklığa sahip iki BCH kod olsunlar. Bu durumda $C_2 \subseteq C_1$ olduğu açıktır. Teorem 4.1 ten C_1 ve C_2 kodlarının parametreleri sırasıyla $\llbracket n, n - m(\delta_1 - 1) + m \lfloor (\delta_1 - 1)/q \rfloor, \geq \delta_1 \rrbracket_q$ ve $\llbracket n, n - m(\delta_2 - 1) + m \lfloor (\delta_2 - 1)/q \rfloor, \geq \delta_2 \rrbracket_q$ şeklindedir. k_1 ve k_2 , sırasıyla, C_1 ve C_2 BCH kodlarının boyutları olsun. Bu durumda CSS kuantum kod inşası ile elde edilen kuantum kodun boyutu $k_1 - k_2 = m(\delta_2 - \delta_1 - \lfloor (\delta_2 - 1)/q \rfloor + \lfloor (\delta_1 - 1)/q \rfloor)$ olarak elde edilir. Ayrıca d_1 ve $d_2^\perp$ sırasıyla, C_1 ve $C_2^\perp$ kodlarının minimum uzaklıkları olsun. Önerme 4.3 ten $d_2^\perp \geq d_{\max} + 1 \geq d_1 \geq \delta_1$ elde edilir. Bu durumda C_1 ve C_2 kodları kullanılarak oluşturulan kuantum kodun minimum uzaklığı $\min\{d_1, d_2^\perp\}$ olduğundan elde edilen kuantum kodun minimum uzaklığı için $\geq \delta$ eşitsizliği vardır.

Teorem 4.3 $q^m \equiv 1 \pmod{n}$ olsun. F_q üzerinde n uzunluğunda BCH kodun

$$\text{tasarlanmış minimum uzaklığı } \delta \text{ için } 2 \leq \delta \leq \delta_{\max} = \frac{n}{q^m - 1} \left(q^{\lceil m/2 \rceil} - 1 - (q-2)[m, \text{tek}] \right)$$

ise BCH kod dualini içerir [13].

Teorem 4.3 ve Önerme 4.3 ten yararlanılarak elde edilen kuantum kodun parametreleri aşağıdaki gibi verilebilir.

Teorem 4.4 q , bir asalın kuvveti olmak üzere $q^m \equiv 1 \pmod{n}$, $m \geq 2$ olsun. Ayrıca

$\delta_{\max} = \frac{n}{q^m - 1} \left(q^{\lceil m/2 \rceil} - 1 - (q-2)[m, tek] \right)$ olmak üzere $2 \leq \delta \leq \delta_{\max}$ olsun. Bu durumda

$\llbracket n, n - 2m \lceil (\delta - 1)(1 - 1/q) \rceil, \geq \delta \rrbracket_q$ parametrelerine sahip bir kuantum kod vardır [13].

İspat: Teorem 4.1 ve Teorem 4.3 ten $\llbracket n, n - m \lceil (\delta - 1)(1 - 1/q) \rceil, \geq \delta \rrbracket_q$ parametrelili δ tasarlanmış minimum uzaklığa sahip dualini içeren bir BCH kod vardır. Bu durumda böyle bir BCH kodun dualinin boyutu $m \lceil (\delta - 1)(1 - 1/q) \rceil$ kadardır. CSS kuantum kod inşası ile elde edilen kuantum kodun boyutu $n - 2m \lceil (\delta - 1)(1 - 1/q) \rceil$ olur. $d^\perp$, dual kodun minimum uzaklığı olmak üzere Önerme 4.3 ten $d^\perp \geq \delta_{\max} + 1 \geq \delta$ eşitsizliği vardır. Sonuç olarak elde edilen kuantum kod, $\geq \delta$ minimum uzaklığına sahiptir.

STABİLİZER KODLAR

5.1 Stabilizer Kuantum Kod

Stabilizer kuantum kod, Danniei Gottesman tarafından 1997 yılında ortaya konulan kuantum kod yapısıdır ve temelde gruplar teorisine dayanır. Bölüm 3.3 de tanımlandığı gibi tekli kubitlere etki eden *Pauli* matris grubu $P = \{\pm I, \pm iI, \pm X, \pm iX, \pm Z, \pm iZ, \pm Y, \pm iY\}$ kümesidir. n kubitte etki eden *Pauli* matris grubu P_n , P nin elemanlarının n defa tensör çarpımından oluşur. Bu durumda $P_n = \underbrace{P \otimes P \otimes \dots \otimes P}_n$ şeklindedir. $H^{\otimes n}$, n kubitli kuantum hal uzayı olmak üzere $P_n \times H^{\otimes n} \rightarrow H^{\otimes n}$, $(E, |\psi\rangle) \rightarrow E|\psi\rangle$ etkisiyle bir grup etkisidir. Stabilizer fikri ise bir $|\psi\rangle$ kuantum halini sabit bırakan tüm $E \in P_n$ hata operatörlerinin düşünülmesi ile ortaya çıkmıştır. Örneğin, $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ halini sabit bırakan hata operatörleri II , XX , ZZ , YY dir.

$$II \left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \right) = \left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \right) = |\psi\rangle,$$

$$XX \left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \right) = \frac{1}{\sqrt{2}}(XX|00\rangle + XX|11\rangle) = \frac{1}{\sqrt{2}}(|11\rangle + |00\rangle) = |\psi\rangle,$$

$$ZZ \left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \right) = \frac{1}{\sqrt{2}}(ZZ|00\rangle + ZZ|11\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\psi\rangle \text{ ve}$$

$$YY\left(\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)\right)=\frac{1}{\sqrt{2}}(YY|00\rangle+YY|11\rangle)=\frac{1}{\sqrt{2}}(|11\rangle+|00\rangle)=|\psi\rangle.$$

$S = \{II, XX, ZZ, YY\}$ kümesi P_2 nin XX ve ZZ tarafından üretilen bir değişmeli alt grubudur. $|\psi\rangle$ hali ise S tarafından sabit bırakılan kuantum halidir.

S , P_n Pauli matris grubunun alt grubu ve V_S de S nin herbir elemanı tarafından sabit bırakılan n kubitli hal uzayı olsun. Bu durumda V_S ye S tarafından sabit bırakılan vektör uzayı ve S ye de V_S uzayın stabilizeri denir. V_S uzayı, S nin herbir elemanının sabit bıraktığı hal uzaylarının kesişimi olarak ta tanımlanabilir [33].

Örnek 5.1 $S = \{III, Z_1Z_2, Z_2Z_3, Z_1Z_3\}$ olsun. III in sabit bıraktığı uzay $H^{\otimes 3}$ dir. Z_1Z_2 , Z_2Z_3 , Z_1Z_3 kuantum operatörlerinin sabit bıraktığı hal uzayları sırasıyla aşağıdaki gibidir:

$$V_1 = \{|000\rangle, |110\rangle, |001\rangle, |111\rangle\},$$

$$V_2 = \{|000\rangle, |011\rangle, |100\rangle, |111\rangle\},$$

$$V_3 = \{|000\rangle, |101\rangle, |010\rangle, |111\rangle\}.$$

Bu durumda S tarafından sabit bırakılan hal uzayı $V_S = \{a|000\rangle + b|111\rangle, |a|^2 + |b|^2 = 1\}$ kümesidir. Burada $(Z_1Z_2)^2 = III$ ve $(Z_1Z_2)(Z_2Z_3) = Z_1Z_3$ olduğundan $S = \langle Z_1Z_2, Z_2Z_3 \rangle$ olur.

$S \leq P_n$ olsun. S stabilizer grubu tarafından sabit bırakılan kuantum hal uzayının tasvir edilmesinde sadece grubun üreteçlerinin sabit bıraktığı hal uzaylarının kesişimlerine bakmak yeterlidir [33]. Dolayısıyla grubun tüm elemanlarının sabit bıraktığı hal uzayına bakmaya gerek yoktur. Örnek 5.1 de $S = \langle Z_1Z_2, Z_2Z_3 \rangle$ olduğundan sadece Z_1Z_2 ve Z_2Z_3 operatörlerinin sabit bıraktığı kuantum hal uzaylarına bakılarak stabilizer kod oluşturulabilir.

$S \leq P_n$ olsun. V_S uzayının sıfırdan farklı olması için S stabilizer grubu aşağıdaki şartları sağlamalıdır [33]:

- i. $-I \notin S$ olmalıdır. $-I \in S$ olması halinde her $|\psi\rangle \in V_S$ için $-|\psi\rangle = -I|\psi\rangle = |\psi\rangle$ olacağından $|\psi\rangle = 0$ olur. Bu ise V_S nin sıfır uzay olması demektir.
- ii. S değişmeli grup olmalıdır. Aksi takdirde $s_1, s_2 \in S$ olmak üzere s_1 ile s_2 değişmeli değilse $s_1 s_2 = -s_2 s_1$ olur. Her $|\psi\rangle \in V_S$ için $|\psi\rangle = s_1 s_2 |\psi\rangle = -s_2 s_1 |\psi\rangle = -|\psi\rangle$ elde edilir. Bu durumda $|\psi\rangle = -|\psi\rangle$ olacağından $|\psi\rangle = 0$ dır. Buradan V_S nin sıfır uzay olduğu görülür.

Örnek 5.2 Örnek 4.1 de $[7, 4, 3]$ Hamming kodu ve duali kullanılarak elde edilen Steane kuantum kodun stabilizer grubunun üreteçleri Çizelge 5.1 deki gibidir:

Çizelge 5.1 7 kubitli Steane kodun stabilizer grubunun üreteçleri

g_1	$IIIXXXX$
g_2	$IXXIIXX$
g_3	$XIXIXIX$
g_4	$IIIZZZZ$
g_5	$IZZIIZZ$
g_6	$ZIZIZIZ$

Bir grubun üreteçleri değişmeli ise grubun kendisi de değişmeli olacağından S stabilizer grubun değişmeliliğini incelemek için üreteçlerinin değişmeliliğine bakmak yeterlidir. g_1, g_2, g_3 üreteçlerinin kendi aralarında ve g_4, g_5, g_6 üreteçlerinin de kendi aralarında değişmeli olduğu açıktır. g_1 ile g_4 için

$$g_1 g_4 = (IIIXXXX)(IIIZZZZ) = IIIYYYY \text{ ve}$$

$$g_4 g_1 = (IIIZZZZ)(IIIXXXX) = IIIYYYY$$

olduğundan g_1 ile g_4 değişmelidir ve diğerlerinin de değişmeli olduğu kontrol edilebilir. Ayrıca bu kuantum kodun boyutu, uzunluğu ve üreteçlerinin sayısı arasında $1 = 7 - 6$ ilişkisi vardır. Bu durum üreteç sayısı l olan bir $[[n, k]]$ stabilizer kod için $k = n - l$ şeklinde genelleştirilebilir.

Önerme 5.1 $g_1, \dots, g_{n-k}, P_n$ in $n-k$ tane bağımsız ve değişmeli elemanı olsun. Eğer $S = \langle g_1, \dots, g_{n-k} \rangle$ ve $-I \notin S$ ise V_S , 2^k boyutlu bir vektör uzayıdır [33].

Tanım 5.1 $g_1, \dots, g_{n-k}, P_n$ in $n-k$ tane bağımsız ve değişmeli elemanı olsun. Ayrıca, $S = \langle g_1, \dots, g_{n-k} \rangle$ ve $-I \notin S$ olsun. S tarafından sabit bırakılan V_S vektör uzayına $[[n, k]]$ parametrelili kuantum stabilizer kod denir ve $C(S)$ ile gösterilir [33].

Örnek 5.3 $S = \langle XZZXI, IXZZX, XIXZZ, ZXIXZ \rangle$ stabilizer grubu ile üretilen kuantum kodun boyutu $5 - 4 = 1$ olduğundan bu bir $[[5, 1]]$ parametrelili kuantum koddur. Bu kodun kodsözleri ise

$$|0_L\rangle = \frac{1}{4} \begin{pmatrix} |00000\rangle + |10010\rangle + |01001\rangle + |10100\rangle + \\ |01010\rangle - |11011\rangle - |00110\rangle - |11000\rangle - \\ |11101\rangle - |00011\rangle - |11110\rangle - |01111\rangle - \\ |10001\rangle - |01100\rangle - |10111\rangle + |00101\rangle \end{pmatrix}$$

ve

$$|1_L\rangle = \frac{1}{4} \begin{pmatrix} |11111\rangle + |01101\rangle + |10110\rangle + |01011\rangle + \\ |10101\rangle - |00100\rangle - |11001\rangle - |00111\rangle - \\ |00010\rangle - |11100\rangle - |00001\rangle - |10000\rangle - \\ |01110\rangle - |10011\rangle - |01000\rangle + |11010\rangle \end{pmatrix}$$

şeklindedir [33].

Örnek 5.4 Örnek 3.15 de 1 kubitin 9 kubite kodlanmasıyla elde edilen Shor kuantum kodun stabilizerinin üreteçleri Çizelge 5.2 deki gibidir:

Çizelge 5.2 9 kubitli Shor kodun stabilizer grubunun üreteçleri

g_1	$ZZIIIIII$
g_2	$IZZIIIIII$
g_3	$IIIIZZIIII$
g_4	$IIIIZZIII$
g_5	$IIIIIZZII$
g_6	$IIIIIZZ$
g_7	$XXXXXXIII$
g_8	$IIIXXXXXX$

$k = 9 - 8 = 1$ olduğundan Shor kodu $[[9,1]]$ parametrelili bir koddur.

5.2 Stabilizer Kodlarda Dekodlama

S bir stabilizer grup ve $C(S)$, S ile elde edilen kuantum kod olsun. Bu durumda her $|\psi\rangle \in C(S)$ kodsözü ve her $g \in S$ için $g|\psi\rangle = |\psi\rangle$ sağlanır. Bu ise $C(S)$ kodun kodsözlerinin S nin herbir elemanı için $+1$ özdeğerli özvektörleri olması demektir. h , S nin en az bir elemanı ile değişmeli olmayan hata operatörü olsun. Bu durumda bir $g \in S$ için $gh = -hg$ ve $h|\psi\rangle$ bozuk hali için $g(h|\psi\rangle) = (gh)|\psi\rangle = (-hg)|\psi\rangle = -h(g|\psi\rangle) = -h|\psi\rangle$ olur. Bu da $h|\psi\rangle$ nin g hata operatörünün -1 özdeğerli özvektörü olması demektir. Yani, h hata operatörü g nin $+1$ özdeğerli özvektörünü -1 özdeğerli özvektörüne dönüştürmüştür. Bu durum stabilizer kuantum kodlarda hatayı farketmenin temel mantığıdır [32].

Örnek 5.5 S stabilizer grubu Örnek 5.1 deki gibi tanımlansın. S ile üretilen $C(S)$ kuantum kod $a|000\rangle + b|111\rangle$, $|a|^2 + |b|^2 = 1$ şeklindedir. $a|000\rangle + b|111\rangle$ kuantum halinde X_1 hatası meydana gelirse son durum $X_1(a|000\rangle + b|111\rangle) = a|100\rangle + b|011\rangle$ olur. Hatanın tespiti S nin üreteçlerinin bozulmuş hale etkisine bakılarak yapılır.

$$Z_1 Z_2 (a|100\rangle + b|011\rangle) = -(a|100\rangle + b|011\rangle)$$

$$Z_2 Z_3 (a|100\rangle + b|011\rangle) = +(a|100\rangle + b|011\rangle)$$

Buradan hatanın 1. kubitte olduğu anlaşılır. Eğer hata 2. veya 3. kubitte meydana gelseydi bozuk halin $Z_2 Z_3$ altındaki görüntüsü değişecekti. Dekodlama ise bozuk hale X_1 uygulanarak yapılır. Bu koda 1 bit hatası düzeltebilen kuantum kod denir. Bu kodun düzeltebildiği hataların sendromu Çizelge 5.3 te verilmiştir.

Çizelge 5.3 1 bit hatası düzelten kuantum kod için düzeltilebilen hataların sendromu ve dekodlaması

$Z_1 Z_2$	$Z_2 Z_3$	Dekodlama
+	+	Hata yok
-	+	X_1 uygulanır
-	-	X_2 uygulanır
+	-	X_3 uygulanır

S bir stabilizer grup ve $C(S)$, S ile elde edilen kuantum kod olsun. Bu durumda stabilizer koduna etki eden hata operatörleri 3 sınıfa ayrılır [33]:

1. S stabilizer grubun elemanlarıdır.
2. S stabilizer grubun en az 1 elemanı ile değişmeli olmayan hata operatörleridir.
3. S stabilizer grubun elemanları ile değişmeli olup S de olmayan hata operatörleridir.

E bir hata operatörü olsun. Eğer $E \in S$ ise E , $C(S)$ kuantum koduna etki etmez. E , S nin elemanları ile değişmeli olmaması halinde S nin +1 özdeğerli özvektörlerini -1

özdeğerli özvektörlerine dönüştüreceğinden E hatası farkedilir. Asıl sorun E hatasının S nin elemanları ile değişmeli olup S de olmamasıdır. Bu durumda $g \in S$ olmak üzere $g(E|\psi\rangle) = (gE)|\psi\rangle = (Eg)|\psi\rangle = E(g|\psi\rangle) = E|\psi\rangle$ olacağından E hatası $C(S)$ tarafından farkedilemez dolayısıyla düzeltilemez.

Örnek 5.6 $S = \langle Z_1 Z_2, Z_2 Z_3 \rangle$ stabilizer grubu ile üretilen $a|000\rangle + b|111\rangle$, $|a|^2 + |b|^2 = 1$ kuantum kodunda Z_1 hatası meydana gelsin. Bu durumda $Z_1(a|000\rangle + b|111\rangle) = a|000\rangle - b|111\rangle$ olur ve kuantum hali bozulur. Fakat $Z_1(Z_1 Z_2) = (Z_1 Z_2)Z_1 = Z_2$ ve $Z_1(Z_2 Z_3) = (Z_2 Z_3)Z_1 = Z_1 Z_2 Z_3$ olduğundan Z_1 hatası S stabilizer grubunun elemanları ile değişmelidir. Z_1 , $C(S)$ kuantum kodunu bozduğu halde S ile değişmeli olduğundan düzeltilemez. Benzer durum Z_2 ve Z_3 hataları için de geçerlidir.

$S \leq P_n$ bir stabilizer grup olsun. Grup teoriden bilindiği üzere S nin herbir elemanı ile değişmeli olan elemanların kümesi S nin merkezileştiricisidir ve $Z(S)$ ile gösterilir.

$$Z(S) = \{g \in P_n : gs = sg, \forall s \in S\}$$

Ayrıca S stabilizer grubu ile değişmeli elemanların kümesi de S nin normalleştiricisidir ve $N(S)$ ile gösterilir.

$$N(S) = \{g \in P_n : gS = Sg\}$$

Bu durumda $S \subseteq Z(S) \subseteq N(S)$ olduğu açıktır. S bir stabilizer grup olduğundan $-I \notin S$ dir. Sonuç olarak bir S stabilizer grubu için $Z(S) = N(S)$ eşitliği vardır. $N(S) - S$ deki hata operatörleri, S ile değişmeli olup S de olmayan hatalardır. Dolayısıyla bir E hata operatörün farkedilebilmesi için $E \notin N(S) - S$ şartı sağlanmalıdır. Teorem 5.1 de bir $C(S)$ stabilizer kuantum kodun hata düzeltme koşulu verilmiştir.

Teorem 5.1 S bir stabilizer grup ve $C(S)$, S ile üretilen kuantum kod olsun. $\{E_j\}$, her j, k için $E_j^\dagger E_k \notin N(S) - S$ şartını sağlayan hata operatörlerinin kümesi ise $\{E_j\}$ hataları $C(S)$ stabilizer kuantum kodu tarafından düzeltilebilen hatalardır [33].

Pauli operatörleri için $E_j^\dagger = E_j$ olduğundan hata düzeltme koşulu her j, k için $E_j E_k \notin N(S) - S$ olarak düzenlenebilir [33].

İspat: P , $C(S)$ kod uzayı üzerinde bir projektör olsun. Teorem 3.8 den her j, k için $E_j^\dagger E_k \notin N(S) - S$ şartını sağlayan hata operatörleri için $PE_j^\dagger E_k P = \lambda_{jk} P$ olacak şekilde λ_{jk} sabitinin varlığının gösterilmesi ispat için yeterlidir.

$E_j^\dagger E_k \notin N(S) - S$ olsun. Bu durumda $E_j^\dagger E_k \in S$ veya $E_j^\dagger E_k \in P_n - N(S)$ dir. $E_j^\dagger E_k \in S$ ise P , S nin elemanları ile değişmeli ve $|\psi\rangle \in C(S)$ olmak üzere $PE_j^\dagger E_k P |\psi\rangle = PPE_j^\dagger E_k |\psi\rangle = P |\psi\rangle$, $P^2 = P$ olduğundan $PE_j^\dagger E_k P = P$, $\lambda_{jk} = 1$ olur. $E_j^\dagger E_k \in P_n - N(S)$ olsun. İspat için λ_{jk} sabiti elde edilecek şekilde bir P projektörü oluşturulmalıdır. $E_j^\dagger E_k \in P_n - N(S)$ olduğundan bir $g_1 \in S$ için $E_j^\dagger E_k$, g_1 ile değişmeli değildir. $g_1, \dots, g_{n-k}$, S nin bağımsız üreteçleri olmak üzere P projektörü

$$P = \frac{\prod_{x=1}^{n-k} (I + g_x)}{2^{n-k}} \quad (5.1)$$

olsun. $(E_j^\dagger E_k) g_1 = -g_1 (E_j^\dagger E_k)$ olduğundan

$$\begin{aligned} (E_j^\dagger E_k)(I + g_1) &= E_j^\dagger E_k + (E_j^\dagger E_k) g_1 \\ &= E_j^\dagger E_k - g_1 (E_j^\dagger E_k) \\ &= (I - g_1)(E_j^\dagger E_k) \end{aligned} \quad (5.2)$$

elde edilir. Bu durumda

$$(E_j^\dagger E_k) P = (I - g_1)(E_j^\dagger E_k) \frac{\prod_{x=2}^{n-k} (I + g_x)}{2^{n-k}} \quad (5.3)$$

olur. $(I + g_1)(I - g_1) = I - g_1^2 = I - I = 0$ olduğundan $P(I + g_1) = 0$ dir ve böylece $PE_j^\dagger E_k P = 0.P$, $\lambda_{jk} = 0$ elde edilir. Sonuç olarak için $E_j^\dagger E_k \notin N(S) - S$ şartını sağlayan hata operatörleri $C(S)$ kuantum kodun düzeltebildiği hatalardır.

Bölüm 3.4 de tanımlandığı üzere bir kuantum kodun minimum uzaklığı, kodun farkedemediği hataların minimum ağırlığıdır. Teorem 5.1 den yararlanarak bir stabilizer kuantum kod için minimum uzaklık tanımlanabilir.

Tanım 5.2 Bir $C(S)$ kuantum kodun minimum uzaklığı, $N(S) - S$ deki elemanların minimum ağırlığıdır [33].

Tanım 5.3 $C(S)$, $[[n, k]]$ parametrelili bir kuantum kod ve $N(S) - S$ deki elemanların minimum ağırlığı d olsun. Bu durumda $C(S)$, $[[n, k, d]]$ parametrelerine sahip bir kuantum koddur [33].

Örnek 5.6 Örnek 5.3 te tanımlanan stabilizer grup ile üretilen 5 kubitli kuantum kod için sendrom tablosu Çizelge 5.4 teki gibidir:

Çizelge 5.4 5 kubitli kuantum kod için düzeltebilen hataların sendromu ve dekodlaması

$XZZXI$	$IXZZX$	$XIXZZ$	$ZXIXZ$	Dekodlama
+	+	+	+	Hata yok
+	+	+	-	X_1
-	+	+	+	X_2
-	-	+	+	X_3
+	-	-	+	X_4
+	+	-	-	X_5
-	+	-	+	Z_1
+	-	+	-	Z_2
+	+	-	+	Z_3
-	+	+	-	Z_4
+	-	+	+	Z_5

–	+	–	–	Y_1
–	–	+	–	Y_2
–	–	–	+	Y_3
–	–	–	–	Y_4
+	–	–	–	Y_5

Bu kuantum kod için stabilizer grubunun elemanları açık olarak

$$S = \left\{ II II, XZZXI, IXZZX, XIXZZ, ZXIXZ, XYIYX, IZYYZ, YYZIZ, \right. \\ \left. ZIZYY, XIYIY, YXXYI, IYXXY, YZIZY, ZYYZI, YXYXX, ZZXIX \right\}$$

şeklinde dir. Bir ağırlıklı hatalar sendrom tablosu yardımıyla düzeltilebilir. İki ağırlıklı tüm hatalar S nin üreteçlerinden en az biri ile değişmeli olmadığından farkedilebilirler. Fakat $ZXZII$ hatası, S nin üreteçleri ile değişmeli olduğu halde S de olmadığından $ZXZII \in N(S) - S$ dir. $ZXZII$ hatasının bu koda etkisi

$$ZXZII(a|0_L\rangle + b|1_L\rangle) = a(ZXZII|0_L\rangle) + b(ZXZII|1_L\rangle)$$

$$= a \left(\begin{array}{l} |01000\rangle - |11110\rangle + |00001\rangle + |11100\rangle + \\ |00010\rangle + |10011\rangle + |01110\rangle + |10000\rangle - \\ |10101\rangle - |01011\rangle - |10110\rangle + |00111\rangle + \\ |11001\rangle + |00100\rangle + |11111\rangle - |01101\rangle \end{array} \right) + \\ b \left(\begin{array}{l} |10111\rangle - |00101\rangle + |11100\rangle + |00011\rangle + \\ |11101\rangle + |01100\rangle + |10001\rangle + |01111\rangle - \\ |01010\rangle - |10100\rangle - |01001\rangle + |11000\rangle + \\ |00110\rangle + |11011\rangle - |00000\rangle - |10010\rangle \end{array} \right)$$

şeklinde dir. Görüldüğü gibi $ZXZII$, S nin elemanları ile değişmeli olduğu halde kuantum halini bozan $N(S) - S$ deki en düşük ağırlığa sahip elemanlardan biridir. Dolayısıyla bu kuantum kodun minimum uzaklığı 3 tür ve bu kod bir $[[5,1,3]]$ kuantum koddur.

Örnek 5.7 Shor kuantum kodu için sendrom tablosu Çizelge 5.5 deki gibidir.

Çizelge 5.5 9 kubitli Shor kuantum kodu için sendrom tablosu

Z_1Z_2	Z_2Z_3	Z_4Z_5	Z_5Z_6	Z_7Z_8	Z_8Z_9	$X_1X_2X_3X_4X_5X_6$	$X_4X_5X_6X_7X_8X_9$	
+	+	+	+	+	+	+	+	I
-	+	+	+	+	+	+	+	X_1
-	-	+	+	+	+	+	+	X_2
+	-	+	+	+	+	+	+	X_3
+	+	-	+	+	+	+	+	X_4
+	+	-	-	+	+	+	+	X_5
+	+	+	-	+	+	+	+	X_6
+	+	+	+	-	+	+	+	X_7
+	+	+	+	-	-	+	+	X_8
+	+	+	+	+	-	+	+	X_9
+	+	+	+	+	+	-	+	$Z_{1,2,3}$
+	+	+	+	+	+	-	-	$Z_{4,5,6}$
+	+	+	+	+	+	+	-	$Z_{7,8,9}$
-	+	+	+	+	+	-	+	Y_1
-	-	+	+	+	+	-	+	Y_2
+	-	+	+	+	+	-	+	Y_3
+	+	-	+	+	+	-	-	Y_4
+	+	-	-	+	+	-	-	Y_5
+	+	+	-	+	+	-	-	Y_6
+	+	+	+	-	+	+	-	Y_7
+	+	+	+	-	-	+	-	Y_8
+	+	+	+	+	-	+	-	Y_9

Çizelge 5.5 den görüleceği gibi Z_1 , Z_2 ve Z_3 hatalarının Shor koduna etkileri aynıdır.

Dolayısıyla bu hatalardan herhangi biri meydana gelse dekodlama bozulmuş hale Z_1 ,

Z_2 veya Z_3 operatörlerinden biri uygulanarak yapılır. Örneğin, Shor kodunda Z_3 hatası meydana gelse bozulmuş hal

$$|\psi'\rangle = \frac{a}{2\sqrt{2}} \left(|000000000\rangle + |000000111\rangle + |000111000\rangle + |000111111\rangle \right) \\ - \frac{a}{2\sqrt{2}} \left(|111000000\rangle - |111000111\rangle - |111111000\rangle - |111111111\rangle \right) \\ + \frac{b}{2\sqrt{2}} \left(|000000000\rangle - |000000111\rangle - |000111000\rangle + |000111111\rangle \right) \\ + \frac{b}{2\sqrt{2}} \left(|111000000\rangle - |111000111\rangle - |111111000\rangle + |111111111\rangle \right)$$

olur. Dekodlama için Z_2 uygulanırsa

$$Z_2 |\psi'\rangle = \frac{a}{2\sqrt{2}} \left(Z_2 |000000000\rangle + Z_2 |000000111\rangle + Z_2 |000111000\rangle + Z_2 |000111111\rangle \right) \\ - \frac{a}{2\sqrt{2}} \left(-Z_2 |111000000\rangle - Z_2 |111000111\rangle - Z_2 |111111000\rangle - Z_2 |111111111\rangle \right) \\ + \frac{b}{2\sqrt{2}} \left(Z_2 |000000000\rangle - Z_2 |000000111\rangle - Z_2 |000111000\rangle + Z_2 |000111111\rangle \right) \\ + \frac{b}{2\sqrt{2}} \left(+Z_2 |111000000\rangle - Z_2 |111000111\rangle - Z_2 |111111000\rangle + Z_2 |111111111\rangle \right) \\ Z_2 |\psi'\rangle = \frac{a}{2\sqrt{2}} \left(|000000000\rangle + |000000111\rangle + |000111000\rangle + |000111111\rangle \right) \\ + \frac{a}{2\sqrt{2}} \left(|111000000\rangle + |111000111\rangle + |111111000\rangle + |111111111\rangle \right) \\ + \frac{b}{2\sqrt{2}} \left(|000000000\rangle - |000000111\rangle - |000111000\rangle + |000111111\rangle \right) \\ + \frac{b}{2\sqrt{2}} \left(-|111000000\rangle + |111000111\rangle + |111111000\rangle - |111111111\rangle \right)$$

olur ve ilk hale geri dönülür. Z_1 veya Z_3 uygulanırsa da ilk hale geri dönülür. Benzer durum Z_4, Z_5, Z_6 ve Z_7, Z_8, Z_9 için de geçerlidir. Dolayısıyla Shor kodu 1 ağırlıklı tüm hataları düzeltebilir. İki ağırlıklı tüm hatalar S nin üreteçlerinden en az biri ile değişmeli olmadığından farkedilebilirler. 3 ağırlıklı hatalardan $Z_1 Z_4 Z_7$ hatası stabilizer grubun tüm üreteçleri ile değişmeli olduğu halde kuantum halini bozar. $Z_1 Z_4 Z_7$ hatasının kuantum hali bozduğu Örnek 3.15 de gösterilmiştir. Dolayısıyla $Z_1 Z_4 Z_7$ hatası $N(S) - S$ deki en düşük ağırlıklı elemanlardan biri olduğundan Shor kodun minimum uzaklığı 3 tür. Sonuç olarak Shor kodu bir $[[9,1,3]]$ kuantum koddur.

5.3 Klasik Lineer Kodlardan Stabilizer Kodun Kontrol Matrisi Yardımıyla Kuantum Kod Elde Etme

Bir kuantum kodun stabilizer grubunun kontrol matrisi, kuantum kodlar ile klasik lineer kodlar arasında geçişi sağlamıştır. [18] nolu makalede $[2n, n+k, d' \geq 4t+1]$ parametrelili klasik lineer koddan $[[n, k, d \geq 2t+1]]$ parametrelerine sahip kuantum kod elde edilmiştir. Bu bölümde bu geçişin nasıl yapıldığı verilecektir.

P_n matris grubu $2n$ boyutlu $\mathbb{Z}_2^{2n}$ vektör uzayı ile yakından ilişkilidir. Tek kubite etki eden $P = \{\pm I, \pm iI, \pm X, \pm iX, \pm Z, \pm iZ, \pm Y, \pm iY\}$ grubunda X ve Z hataları düzeltildiği sürece diğerleri de düzeltilebilir. $K = \{\pm I, \pm iI\}$ olmak üzere P/K ile $\mathbb{Z}_2^2$ arasında aşağıdaki gibi bir homomorfizma kurulabilir:

$$P/K \rightarrow \mathbb{Z}_2^2, IK \rightarrow (0,0), XK \rightarrow (1,0), ZK \rightarrow (0,1), YK \rightarrow (1,1) \quad (5.4)$$

$M_1, \dots, M_n \in P_n$ olmak üzere $g = M_1 \otimes \dots \otimes M_n \in P_n$ operatörü $g = i^c X_\alpha Z_\beta$ olarak ifade edilebilir. Burada α ve β sırasıyla X ve Z operatörlerinin bulunduğu bileşenleri göstermektedirler. Örneğin, $g = iX \otimes I \otimes Y \otimes iZ$ için $\alpha = (1,0,1,0)$ ve $\beta = (0,0,1,1)$ dir. Bu durumda $K' = \{\pm I^{\otimes n}, \pm iI^{\otimes n}\}$ olmak üzere

$$\psi: P_n \rightarrow P_n/K', i^c X_\alpha Z_\beta \rightarrow X_\alpha Z_\beta K \quad (5.5)$$

bir homomorfizmadır. Ayrıca,

$$\eta: P_n/K' \rightarrow \mathbb{Z}_2^{2n}, X_\alpha Z_\beta K' \rightarrow (\alpha, \beta) \quad (5.6)$$

dönüşümü bir izomorfizmadır. Bu durumda

$$\varphi: P_n \rightarrow \mathbb{Z}_2^{2n}, i^c X_\alpha Z_\beta \rightarrow (\alpha, \beta) \quad (5.7)$$

dönüşümü de örten bir homomorfizma olur. Bir $x = (\alpha, \beta) \in \mathbb{Z}_2^{2n}$ vektörünün genelleştirilmiş Hamming ağırlığı $gw(x) = wt(\alpha) + wt(\beta) - wt(\alpha \bullet \beta)$ şeklindedir. Burada $\alpha \bullet \beta$, α ile β nın bileşen çarpımıdır [18].

Örnek 5.8 $g = X_\alpha Z_\beta$, $\alpha = (1, 0, 1)$, $\beta = (1, 1, 0)$ olsun. Bu durumda $\varphi(g) = (101110)$ ve $gw(\varphi(g)) = wt(101) + wt(110) - wt(100) = 2 + 2 - 1 = 3$ olur.

$S \leq P_n$ ve $g_1, \dots, g_k \in S$ olsun. Eğer $g_1, \dots, g_k$, S nin bağımsız üreteçleri ise $\varphi(g_1), \dots, \varphi(g_k)$, $\mathbb{Z}_2^{2n}$ de lineer bağımsız vektörlerdir. $g_1, \dots, g_k$, S nin bağımsız üreteçleri olmak üzere S stabilizer grubunun kontrol matrisi H , i . satırı $\varphi(g_i)$ olarak tanımlanır ve $H = [H_x | H_z]$ şeklinde gösterilir [18].

Örnek 5.9 7 kubitli Steane kuantum kodun üreteçleri ve φ altındaki görüntüleri aşağıdaki gibidir:

$$g_1 = IIIXXX \Rightarrow \varphi(g_1) = (0001111 \ 0000000),$$

$$g_2 = IXXIIX \Rightarrow \varphi(g_2) = (0110011 \ 0000000),$$

$$g_3 = XIXIXI \Rightarrow \varphi(g_3) = (1010101 \ 0000000),$$

$$g_4 = IIIZZZ \Rightarrow \varphi(g_4) = (0000000 \ 0001111),$$

$$g_5 = IZZIIZ \Rightarrow \varphi(g_5) = (0000000 \ 0110011) \text{ ve}$$

$$g_6 = ZIZIZI \Rightarrow \varphi(g_6) = (0000000 \ 1010101).$$

Bu durumda Steane kodun kontrol matrisi

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

şeklinde olur.

S bir stabilizer grup iken değişmeli olacağından her $g, h \in S$ için $gh = hg$ dir. Bu değişmeliliğin $\varphi(S)$ deki karşılığı her $\varphi(g), \varphi(h) \in \varphi(S)$ için $\varphi(g) \Lambda_{2n}(\varphi(h))^T = 0$

şeklindedir. Burada $\Lambda_{2n} = \begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix}$ dır. Bu durumda H, S stabilizer grubunun

kontrol matrisi olmak üzere H matrisinin değişmelilik koşulu

$$H\Lambda_{2n}H^T = H_X H_Z^T + H_Z H_X^T \quad (5.8)$$

şeklindedir [18].

Klasik kodlamada düzeltilebilen hatalar, her biri farklı hata sendromuna sahip olan hatalardır. Stabilizer kodda ise hata sendromu düşüncesi değişmeliliğe dayanır. Buna göre düzeltilebilen her bir hata operatörü, stabilizer grubun herbir üretici ile değişmeliliği gösteren bir ikiliye atanır. $g \in P_n$ olmak üzere

$$f_g : P_n \rightarrow \mathbb{Z}_2, f_g(h) = \begin{cases} 0, & gh = hg \\ 1, & gh = -hg \end{cases} \quad (5.9)$$

dönüşümü bir grup homomorfizmasıdır. $g_1, \dots, g_r, S$ nin bağımsız üreteçleri olmak üzere

$$f_S : P_n \rightarrow \mathbb{Z}_2^r, f_S(h) = (f_{g_1}(h), f_{g_2}(h), \dots, f_{g_r}(h))^T \quad (5.10)$$

olsun. Bu durumda f_S bir grup homomorfizmasıdır ve $E \in P_n$ bir operatörünün hata sendromu $f_S(E)$ olarak tanımlanır. E_1 ve E_2 düzeltilebilen hata operatörleri olmak üzere $f_S(E_1 E_2) \neq 0$ olacak şekilde bir stabilizer grup oluşturabilmek için

$$f_S(E_1 E_2) \neq 0 \Leftrightarrow f_S(E_1) \neq f_S(E_2) \quad (5.11)$$

olmalıdır. Sonuç olarak, her bir düzeltilebilen hata operatörüne farklı hata sendromları atanmalıdır [18].

Eğer $\{X_1, \dots, X_n, Z_1, \dots, Z_n\}$ hata operatörlerinden herhangi t tanesinin tensör çarpımı düzeltilebiliyorsa t ve daha düşük ağırlıklı hatalar düzeltilebilir. H, S stabilizer grubunun kontrol matrisi ve $E \in P_n$ olmak üzere $f_S(E) = H\Lambda_{2n}(\varphi(E))^T$ eşitliği vardır. Bu eşitlikten kontrol matrisinin sırasıyla ilk n sütunun $f_S(Z_1), f_S(Z_2), \dots, f_S(Z_n)$ e ve son n sütununun $f_S(X_1), f_S(X_2), \dots, f_S(X_n)$ e karşılık geldiği görülür.

Örnek 5.10 S stabilizer grubun üreteçleri $g_1 = XZZXI$, $g_2 = IXZZX$, $g_3 = XIXZZ$, $g_4 = ZXIXZ$ olsun. Bu durumda S stabilizer grubun kontrol matrisi

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

şeklinde dir. X_1, X_2, X_3, X_4, X_5 ve Z_1, Z_2, Z_3, Z_4, Z_5 hata operatörlerinin sendromları aşağıdaki gibidir:

$$f_s(X_1) = (0001)^T, \quad f_s(Z_1) = (1001)^T,$$

$$f_s(X_2) = (1000)^T, \quad f_s(Z_2) = (0101)^T,$$

$$f_s(X_3) = (1100)^T, \quad f_s(Z_3) = (0010)^T,$$

$$f_s(X_4) = (0110)^T, \quad f_s(Z_4) = (1001)^T,$$

$$f_s(X_5) = (0011)^T \text{ ve } f_s(Z_5) = (0100)^T.$$

Buradan $f_s(X_1), f_s(X_2), f_s(X_3), f_s(X_4), f_s(X_5)$ in H kontrol matrisinin sırasıyla 6., 7., 8., 9., 10. sütunları ve $f_s(Z_1), f_s(Z_2), f_s(Z_3), f_s(Z_4), f_s(Z_5)$ in H kontrol matrisinin sırasıyla 1., 2., 3., 4., 5. sütunları olduğu görülür.

$E = X_\alpha Z_\beta$, $\alpha = (a_1, \dots, a_n)$, $\beta = (b_1, \dots, b_n)$ ağırlığı $\leq t$ olan bir hata operatörü olsun.

Bu durumda S , bir stabilizer grup olmak üzere

$$f_s(E) = f_s(X_\alpha Z_\beta) = \sum_{i=1}^n a_i f_s(X_i) + \sum_{i=1}^n b_i f_s(Z_i) \quad (5.12)$$

toplamı en fazla $2t$ terimin lineer kombinasyonudur. $E_1 = X_{\alpha_1} Z_{\beta_1}$, $\alpha_1 = (a_1, \dots, a_n)$, $\beta_1 = (b_1, \dots, b_n)$ ve $E_2 = X_{\alpha_2} Z_{\beta_2}$, $\alpha_2 = (u_1, \dots, u_n)$, $\beta_2 = (v_1, \dots, v_n)$ ağırlıkları $\leq t$ olan iki hata operatörü olsun. E_1 ve E_2 operatörlerinin hata sendromlarının farklı olduklarını garantilemek için

$$f_S(E_1) \neq f_S(E_2) \Leftrightarrow f_S(E_1) + f_S(E_2) \neq 0 \quad (5.13)$$

$$\Leftrightarrow \sum_{i=1}^n (a_i + u_i) f_S(X_i) + \sum_{i=1}^n (b_i + v_i) f_S(Z_i) \neq 0 \quad (5.14)$$

olmalıdır. (5.16) daki toplam ifadesi en fazla $4t$ terimin toplamıdır. Dolayısıyla ağırlığı t olan hata operatörlerine ait hata sendromlarının farklılığını garantilemek için gerekli koşul, $\{f_S(X_1), \dots, f_S(X_n), f_S(Z_1), \dots, f_S(Z_n)\}$ kümesindeki herhangi $4t$ elemanın lineer bağımsızlığıdır. Bu ise minimum uzaklığı $4t+1$ olan klasik lineer kodun kontrol matrisinin özelliğidir. Sonuç olarak, minimum uzaklığı $4t+1$ olan ve kontrol matrisi değişmelilik koşulunu sağlayan klasik lineer koddan minimum uzaklığı $2t+1$ olan kuantum kod elde edilebilir [18].

Teorem 5.2 $C, [2n, n+k, d' \geq 4t+1]$ parametrelerine sahip bir klasik lineer kod olsun. H, C kodun kontrol matrisi olsun ve değişmelilik koşulunu sağlasın. Bu durumda $\llbracket n, k, d \geq 2t+1 \rrbracket$ parametrelili ve H kontrol matrisine sahip bir stabilizer kuantum kod vardır [18].

SONUÇ VE ÖNERİLER

Hazırlanan bu çalışmada klasik lineer kodlardan kuantum kod elde yöntemleri araştırıldı ve literatür taraması yapıldı. Bu yöntemlerden ikisi ayrıntılı ve anlaşılır bir şekilde örneklerle anlatılmaya çalışıldı. Ayrıca kuantum kodlar için hata farketme ve düzeltme koşulları verildi.

Klasik kodlardan daha iyi parametrelili kuantum kodlara bir geçiş araştırması yapılabilir. Her zaman için daha iyi parametrelilere sahip bir kuantum kod bulmak açık problemidir.

- [1] W. Shor, P., (1995). "Scheme for reducing decoherence in quantum computer memory", *Physc. Review A*, 52:R2493-R2496.
- [2] Andrew, S. (1996). "Multiple-partical interference and quantum error correction", *Proc. Roy. Soc. Lond.*, A452:2551-2577.
- [3] Calderbank, A. R. ve W. Shor, P., (1996). "Good Quantum Error Correcting Codes Exist", *Physc. Review A*, 54:1098-1105.
- [4] Danniell, G. (1997). *Stabilizer Codes and Quantum Error Correction*, Ph. D. Thesis, California Institute of Technology, California.
- [5] Calderbank, A. R., Rains, E. N., W. Shor, P. ve Sloane, N. S., (1998). "Quantum Error Correction via Codes Over $GF(4)$ ", *IEEE Trans. Infor. Theory*, 44:1369-1387.
- [6] Güzeltepe, M. ve Özen, M., (2011). "Quantum Codes From Codes Over Lipschitz Integers", *Glornal of Pure and Appl. Math.*, 7:201.
- [7] Hurley, T., (2007). "Self-dual, dual containig and related quantum codes from group rings", *arXiv:0911-3983v1 [cs.IT]*.
- [8] Güzeltepe, M. ve Özen, M., (2012). "Quantum Codes From Codes Over Gaussian Integers With Respect To Mannheim Metric", *arXiv:1003-3754v2 [cs.IT]*.
- [9] Qian, J., Ma, W. ve Guo, W., (2009). "Quantum Codes Fron Cyclic Codes Over Finite Ring", *International Journal of Quantum Information*, 7:1277-1283.
- [10] Andrew, S., (1999). "Enlargement of Calderbank-Shor-Steane Quantum Codes", *IEEE Trans. Infor. Theory*, 45:2492-2495.
- [11] Grassl, M. ve Beth, T., (1999). "Quantum BCH Codes", *arXiv:quant-ph/9910060v1*.
- [12] Cohen, G., Encheva, S. ve Litsyn, S., (1999). "On binary conscructions of quantum codes", *Proocedings of the 1999 IEEE Inform. Theory Communications Workshop*, 20-25 June 1999, Paris.
- [13] A. Aly, S., Klappenecker, A. ve Sarvepelli, P., (2007). "On Quantum and Classical BCH Codes", *IEEE Trans. Infor. Theory*, 53:1183-1188.

- [14] Iryna, A., Maurice, D ve Jean-Pierre, T., (2012). "New Consructions of CSS Codes Obtaining By Moving To Higher Alphabets", arXiv:1202.3338v1 [quant-ph].
- [15] A. Aly, S., Klappenecker, A. ve Sarvepelli, P., (2006). "Primitive Quantum BCH Codes Over Finite Field", IEEE Trans. Infor. Theory, 9-14 July 2006, Seattle, W.A.
- [16] Guo, L., Ma, Y. Ve Feng, Y., (2012). "Quantum Codes Consructed From Self-Dual Codes and Maximal Self-Orthogonal Over F_5 ", International Workshop on Information and Electronic Engineering, 29:3848-3453.
- [17] Andrew, S., (1996). "Simple Quantum Error Correcting Codes", Physc. Review A, 54:4741-4751.
- [18] Lai, C. ve Lu, C., (2011). "A Consruction of Quantum Stabilizer Codes on Syndrome Assignment by Classical Parity-Check Matrices", IEEE Trans. Infor. Theory, 57:7167-7179.
- [19] Cleve, R., (1997). "Quantum Stabilizer Codes and Classical Linear Codes", Physc. Review A, 55:4054-4059
- [20] Ketkar, A., Klappenecker, A., Kumar, S. ve Sarvepelli, P.K., (2006). "Nonbinary Stabilizer Codes Over Finite Field", IEEE Trans. Infor. Theory, 52:4892-4914.
- [21] Matthew G., D. ve Lars Eirik, D., (2006). "On the classification of all self-dual additive codes over $GF(4)$ ", Journal of Combinatorial Theory, 113:1351-1367.
- [22] Thangaraj, A. ve McLaughlin, S.W., (2001). "Quantum Codes From Cyclic Codes From $GF(4^m)$ ", IEEE Trans. Infor. Theory, 47:1176-1178.
- [23] Ma, Y., Li, R., Zhau, X. Ve Feng, Y., (2007). "Three Quantum Error Correcting Codes Consructed From Self-Orthogonal Codes Over $GF(4)$ ", Proocedings of 2007 International Symposium on Intelligent Signal Processing and Communication System", 28 November-01 December, Xiamen.
- [24] Yu, S., Bierbraver, J., Dang Y., Chen, Q. ve Oh., C.H., (2011). "All the stabilizer codes of distance 3", arXiv:0901.1968v3 [quant-ph].
- [25] Li, R. ve Li, X., (2004). "Binary Consruction of Quantum Codes of Minimum Distance Three and Four", IEEE Trans. Infor. Theory, 50:1331-1336.
- [26] Li, R. ve Li, X., (2008). "Binary Consruction of Quantum Codes of Minimum Distance Five and Six", Discrete Mathematics, 308:1603-1611.
- [27] Grassl, M. ve Beth, T., (2003). "On Optimal Quantum Codes", arXiv:quant-ph/0312164v1.
- [28] A. Aly, S., (2007). "A note on quantum Hamming bound", arXiv:quant-ph/0711.4603.
- [29] Karakaş, H.İ., (2010). Cebir Dersleri, 2. Baskı, Türkiye Bilimler Akademisi, ANKARA.

- [30] D.S., M., N. Mordeson, J. ve Sen, M.K., (2007). "MTH 581-582 Introduction to Abstract Algebra", <https://people.creighton.edu/~dsm33733/MTH581/Introduction%20to%20Abstract%20Algebra.pdf> (07.01.2013).
- [31] Gottesman, D., (2009). "An Introduction to Quantum Error Corrction and Fault-Tolerant Quantum Computation", arXiv:0904.2557v1 [quant-ph].
- [32] Bocan, D., <http://www.cs.washington.edu/education/courses/cse599d/06wi/lecturenotes18.pdf> (07.01.2013).
- [33] A. Nielsen ve L. Chuang, I., (2008). Quantum Computation and Quantum Information, First Edition, The Press Syndicate of the University of Cambridge, CAMBRIDGE.
- [34] Kaye, P., Laflamme, R. ve Mosca, M., (2007). An Introduction to Quantum Computing, Oxford University Press, NEW YORK.
- [35] Chang, H. H., (2006). "An Introduction to Error Correcting Codes: From Classical to Quantum", arXiv:quant-ph/06002157v1.
- [36] Knill, E., Laflamme, R. Ashikhmin, A., N. Barnum, H., Viola, L. ve H. Zurek, W., (2002). "Introduction to Quantum Error Correction", (07.01.2013).
- [37] Ling, S. ve Xing, C., (2004). A First Course In Coding Theory, Cambridge University Press, NEW YORK.
- [38] Huffman ,W.C. ve Pless, V., (2003). Fundamental of Error Correcting Codes, First Edition, Cambridge University Press, NEW YORK.
- [39] Preskill, J., "Quantum Error Correction", <theory.caltech.edu/~preskill/ph229/notes/chap7.pdf>, (07.01.2013).
- [40] Güzeltepe, M. , (2011). Gauss ve Kuaterniyon Tam Sayılarından Kuantum Kod Elde Etme, Doktora Tezi, Sakarya Üniversitesi Fen Bilimleri Enstitüsü, SAKARYA.

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Adı Soyadı : Mustafa SARI
Doğum Tarihi ve Yeri : 30.10.1988 AYDIN
Yabancı Dili : İNGİLİZCE
E-posta : mustafasar7@gmail.com

ÖĞRENİM DURUMU

Derece	Alan	Okul/Üniversite	Mezuniyet Yılı
Lisans	Matematik	Yıldız Teknik Üniversitesi	2011
Lise	Fen Bilimleri	Adnan Menderes Anadolu Lisesi	2006

İŞ TECRÜBESİ

Yıl	Firma/Kurum	Görevi
2013	Yıldız Teknik Üniversitesi	Araştırma Görevlisi