T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

GAUSS VE KUATERNİYON TAM SAYILARINDAN KUANTUM KOD ELDE ETME

DOKTORA TEZİ

Murat GÜZELTEPE

Enstitü Anabilim Dalı : MATEMATİK

Tez Danışmanı : Doç. Dr. Mehmet ÖZEN

Mayıs 2011

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

GAUSS VE KUATERNİYON TAM SAYILARINDAN KUANTUM KOD ELDE ETME

DOKTORA TEZİ

Murat GÜZELTEPE

Enstitü Anabilim Dalı : MATEMATİK

Bu tez 25.05.2011 tarihinde aşağıdaki jüri tarafından ~~Oyçokluğu~~ / Oybirliği ile kabul edilmiştir.

Prof. Dr. İrfan ŞİAP	**Doç. Dr. Mehmet ÖZEN**	**Prof. Dr. Abdullah YILDIZ**
Jüri Başkanı	**Üye**	**Üye**
Yrd. Doç. Dr. A. Serdar ARIKAN		**Yrd. Doç. Dr. Bahattin YILDIZ**
Üye		**Üye**

ÖNSÖZ

Bu konunun seçiminde ve çalışmamın her safhasında büyük bir özveri ile bana yardımcı olan, bilgi ve tecrübelerinden yararlandığım, değerli hocam Doç. Dr. Mehmet ÖZEN'e şükranlarımı sunarım.

Ayrıca, değerli tavsiye ve yardımlarından dolayı Prof. Dr. İrfan ŞİAP'a, tezin hazırlanmasında emek ve katkılarından dolayı tez izleme jürisine, özellikle Mathematica programı kullanımındaki yardımlarından dolayı Yrd. Doç. Dr. Mustafa ERÖZ'e ve benden her zaman yardım ve desteklerini esirgemeyen aileme ve özellikle eşime teşekkürü bir borç bilirim.

İÇİNDEKİLER

SİMGELER VE KISALTMALAR LİSTESİ

$\mathbb{Z}$: Tam sayılar kümesi

$\mathbb{R}$: Reel sayılar kümesi

$\mathbb{C}$: Karmaşık sayılar kümesi

$|\cdot\rangle$: Ket vektörü

$\langle\cdot|$: Bra vektörü

$M^{\dagger}$: M matrisinin eşlenik transpozesi

$A \otimes B$: A ile B matrisinin tensör çarpımı

I_n : $n \times n$ boyutlu birim matris

H : Hadamard mantık kapısı

$\mathbb{H}(\mathbb{R})$: Reel kuaterniyonlar kümesi

$\mathbb{H}(\mathbb{Z})$: Kuaterniyon tam sayılar kümesi (Lipschitz sayıları)

$\langle\cdot\rangle$: İç çarpım

$\in$: Elemanıdır

$\mathbb{Z}[i]$: Gauss tam sayılar kümesi

$\mathcal{H}$: Hilbert uzay

$\mathcal{A}^{\otimes n}$: $\mathcal{A}$ kümesinin n defa tensör çarpımı

$M(S)$: S kümesinin merkezleştiricisi

$N(S)$: S kümesinin normalleştiricisi

$N(q)$: q elemanının normu

ξ : Birimin m. kökü, $\xi = e^{2\pi i/m}, \pi = 3{,}14...$

$[n,k,d]_q$: q elemanlı cisim üzerinde tanımlı, n uzunluklu, k boyutlu, d minimum mesafeli lineer kod

$[[n,k,d]]_q$: q elemanlı cisim üzerinde tanımlı, n uzunluklu, k boyutlu, d

	minimum mesafeli kuantum kod
A^{tr}	: A matrisinin transpozu
Tr	: İz fonksiyonu
$Tr(M)$	: M matrisinin izi
NOT	: Kuantum NOT mantık kapısı
$CNOT$	: Kuantum CNOT mantık kapısı
G_n	: n kubitli Pauli matris grubu
$C(S)$	: Stabilizer kod
CSS	: Calderbank-Shor-Steane kuantum kodu
$(a\|b)$	: $2n$ girdili vektör

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

ÖZET

Anahtar kelimeler: Kuantum kod, stabilizer kod, nonbinary kuantum kod, lineer kod, devirli kod, toplamsal kod

Bu tez dört bölümden oluşmaktadır. Birinci bölümde cebir ve kodlama teorisinin temel tanım ve teoremleri, ikinci bölümde kısa bir literatür taraması, kuantum hesaplama ve kuantum bilgi hakkında temel tanım ve teoremler verilmektedir. Yine bu bölümde ikili olan ve ikili olmayan hata düzeltebilen kuantum kodlar açıklanmaktadır.

Üçüncü bölümde Mannheim metriğine göre Gauss tamsayıları üzerindeki klasik kodlar yardımı ile Calderbank-Shor-Steane (kısaca CSS) kodları oluşturulmaktadır. Ayrıca bu bölümde Gauss tam sayıları için iyi hata bazları da tanımlanmaktadır.

Dördüncü bölümde Lipschitz sayıları üzerindeki klasik kodlar yardımı ile CSS kodların nasıl inşa edileceği açıklanmakta ve bu sayılar için iyi hata bazları tanımlanmaktadır.

QUANTUM CODES OBTAINED FROM GAUSSIAN AND QUATERNION INTEGERS

SUMMARY

Key Words: Quantum code, stabilizer code, nonbinary quantum code, linear code, cyclic code, additive code

This thesis consist of four chapters. In the first chapter, some notations and some basic definitions and theorems of abstract algebra are given.

In the second chapter, the fundamental elements needed to perform quantum computation and quantum information are described and many elementary operations which may be used to develop more sophisticated applications of quantum computation and quantum information are presented. Moreover, binary and nonbinary quantum error-correcting codes are explained.

In the third chapter, the CSS codes are constructed from codes over Gaussian integers with respect to the Mannheim metric. Moreover, the set of the nice error bases over Gaussian integers is introduced.

In the fourth chapter, the CSS codes are constructed via codes over quaternion integers with respect to the Lipschitz metric. Moreover, the set of the nice error bases over quaternion integers is introduced.

BÖLÜM 1. GİRİŞ

1.1. Cebirsel Tanımlar

Bu bölümde verilecek tanım, önerme ve teoremler diğer bölümler için bir hazırlık niteliğinde olup diğer bölümlerde bu tanım ve teoremler kullanılacaktır.

Tanım 1.1.1. S boştan farklı bir küme olsun. S kümesinin elemanlarından oluşan her sıralı ikiliye S' de bir ve yalnız bir eleman karşılık getiren bir fonksiyona S üzerinde bir ikili işlem denir. Bu işlem "$*$" sembolü ile gösterilirse;

$$S \times S \to S$$

$$(a,b) \mapsto a * b$$

ile tanımlanır [13].

Tanım 1.1.2. G boştan farklı bir küme ve "$\cdot$" G'de bir ikili işlem olsun. Eğer $\forall g_1, g_2, g_3 \in G$ için $g_1 \cdot g_2 \in G$, $g_1 \cdot (g_2 \cdot g_3) = (g_1 \cdot g_2) \cdot g_3$ oluyorsa, $\forall g \in G$ için sırasıyla $g \cdot e = e \cdot g = g$ ve $g \cdot g^{-1} = g^{-1} \cdot g = e$ olacak şekilde $e \in G$ ve $g^{-1} \in G$ varsa $(G, \cdot)$ yapısına grup denir [13].

Tanım 1.1.3. G bir grup ve $g_1, g_2, \ldots, g_l \in G$ olsun. Eğer G'nin her elemanı $g_1, g_2, \ldots, g_l$ elemanlarından elde ediliyorsa bu elemanlara G grubunun üreteçleri denir ve G'nin bu elemanlar tarafından üretildiği $G = \langle g_1, g_2, \ldots, g_l \rangle$ şeklinde gösterilir [13].

Tanım 1.1.4. Eğer G grubu bir a elemanı tarafından üretiliyorsa bu gruba devirli grup denir ve $G=\langle a\rangle$ ile gösterilir. Bu durumda $\forall g\in G$ için $g=a^k$ olacak şekilde $\exists k\in\mathbb{N}$ vardır [13].

Tanım 1.1.5. G bir grup ve M_n de $n\times n$ tipindeki tüm tersinir kompleks matrislerin kümesi olsun. G'den M_n'ye tanımlanan ρ homomorfizmasına G'nin bir gösterimi ve n sayısına da ρ'nun derecesi denir [35].

Tanım 1.1.6. G bir grup olsun.

$$M=\{a\in G:\forall g\in G, ag=ga\}$$

kümesine bu grubun merkezi denir.

Tanım 1.1.7. G bir grup ve H de bu grubun bir alt grubu olsun.

$$N(H)=\{g\in G:gH=Hg\}$$

kümesine H kümesinin normalleştiricisi denir.

Tanım 1.1.8. $R\neq\varnothing$ kümesi üzerinde tanımlı ikili işlem $\oplus$ ve $\otimes$ olsun. Aşağıdaki aksiyomları sağlayan $(R,\oplus,\otimes)$ cebirsel yapısına bir halka denir.

i. $(R,\oplus)$ bir değişmeli gruptur.

ii. $\otimes$ işleminin R'de birleşme özelliği vardır.

iii. $\otimes$ işleminin $\oplus$ işlemi üzerine R'de sağdan ve soldan dağılma özelliği vardır [13].

Tanım 1.1.9. R birimli değişmeli bir halka olsun. Eğer $R^* = R - \{0_R\}$ kümesi $\otimes$ işlemine göre bir grup ise R'ye bir cisim denir [13].

Tanım 1.1.10. R bir halka ve $\varnothing \neq I \subseteq R$ olsun.

i. $\forall a, b \in I$ için $a - b \in I$ ve

ii. $\forall r \in R$ ve $\forall a \in I$ için, $ra \in I$ (veya $ar \in I$) ise I'ya R'nin bir sol (veya sağ) ideali denir. Hem sol hem de sağ ideale iki taraflı ideal ya da kısaca ideal denir [13].

Tanım 1.1.11. R değişmeli bir halka ve M bir değişmeli grup olsun.

$$\bullet : R \times M \to M$$
$$(r, m) \mapsto r.m$$

dönüşümü altında, $\forall r, r_1, r_2 \in R$ ve $\forall m, m_1, m_2 \in M$ için aşağıdaki şartlar sağlanıyorsa M bir sol $R-$modüldür.

$i.$ $r(m_1 + m_2) = rm_1 + rm_2$,

$ii.$ $(r_1 + r_2)m = rm_1 + r_2 m$,

$iii.$ $(r_1 r_2)m = r_1(r_2 m)$,

$iv.$ $1_R m = m.$

Eğer R halkasının yerine $\mathbb{F}$ cismi alınırsa M, $\mathbb{F}$ cismi üzerinde bir vektör uzayıdır [15].

Tanım 1.1.12. R birimli bir halka ve $1_R \neq 0_R$ olsun. Eğer R'nin sıfırdan farklı her elemanının bir çarpımsal tersi varsa, yani $\forall 0_R \neq a \in R$ için $ab = b'a = 1_R$ olacak

şekilde $b,b' \in R$ varsa R halkasına çarpık cisim (skew field) denir. Değişmeli bir çarpık cisim cisimdir [15].

Tanım 1.1.13. $A=\{a_1,\ a_2,\ \cdots\ a_q\}$ sonlu cümlesine $q-$lu alfabe ya da kısaca alfabe denir. A cümlesinin elemanlarından oluşan $n-$lilerin oluşturduğu A^n kümesine sözler ailesi denir. A^n'nin herhangi bir C altkümesine $q-$lu blok kodu denir. C'nin elemanlarına ise kodsöz denir. $C \subset A^n$'nin M tane elemanı varsa C'ye n uzunluğunda, M büyüklüğünde bir kod denir ve (n,M) parametreleri ile gösterilir [41].

Tanım 1.1.14. u ve v aynı uzunlukta ve aynı alfabe üzerinde tanımlanmış $n-$liler olsun. u ile v'nin farklı bileşenlerinin sayısına u ile v arasındaki Hamming mesafesi denir ve $d(u,v)$ ile gösterilir. $d: A^n \times A^n \to \mathbb{N}$, $d(u,v)=\left|\{i:\ u_i \neq v_i,\ 1 \leq i \leq n\}\right|$ olmak üzere (A^n,d) ikilisi bir metrik uzay oluşturur [41].

Tanım 1.1.15. (n,M) parametrelerine sahip bir C kodunun minimum mesafesi $d(C)$ ile gösterilir ve $d(C)=\min\limits_{u,v\in C,u\neq v} d(u,v)$ şeklinde tanımlanır. n uzunluğunda, M elemana sahip ve minimum mesafesi d olan bir kod kısaca (n,M,d) şeklinde gösterilir [41].

Tanım 1.1.16. q elemanlı $\mathbb{F}_q$ cismi üzerinde n uzunluklu bütün vektörlerden oluşan $\mathbb{F}_q^n$ kümesi bir vektör uzayıdır ve bu vektör uzay $V(n,q)$ ile gösterilir. C kümesi $V(n,q)$ vektör uzayının k boyutlu bir alt uzayı olsun. C'ye n uzunluğunda ve k boyutlu bir lineer kod denir ve $[n,k]$ ile gösterilir. Eğer C kodunun minimum mesafesi d ise bu kod $[n,k,d]$ parametreleri ile gösterilir.

$c \in C$'nin Hammimg ağırlığı bu koddaki sıfırdan farklı bileşenlerin sayısı olarak tanımlanır ve $w(c)$ biçiminde gösterilir. C'nin sıfır vektörü hariç geri kalan elemanlarının ağırlıklarının en küçüğüne ise C kodunun minimum ağırlığı denir ve $w(C)$ ile gösterilir.

Lineer kodlarda $d(C) = w(C)$'dir [41].

Tanım 1.1.17. Hamming metriğine göre iç çarpım, $u, v \in C \subset V(n, q)$ olmak üzere

$$\langle u, v \rangle = \sum_{i=1}^{n} u_i v_i$$

şeklinde tanımlanır [41].

Tanım 1.1.18. C kodu bir $[n, k]$ lineer kod olsun.

$$C^{\perp} = \{u \in V(n, q) : \langle u, v \rangle = 0, \quad \forall v \in C\}$$

kümesine C kodunun diki (duali) denir [41].

Teorem 1.1.1. $\mathbb{F}_q$ cismi üzerinde bir lineer $[n, k, d]$ kodu verildiğinde, ilk k sütunu k boyutlu I_k birim matrisi olan $G = [I_k, A]$ standart formdaki üreteç matrisine sahip bir koda denktir [41].

Teorem 1.1.2. C kodu $G = [I_k, A]$ standart formdaki üreteç matrisine sahip $[n, k]$ parametreli bir lineer kod ise C'nin diki de $H = [-A^{tr}, I_{n-k}]$ üreteç matrisine sahip bir $[n, n-k]$ lineer kod olur. H matrisine C kodunun kontrol matrisi denir [41].

Tanım 1.1.19. Eğer $(c_0 \quad c_1 \quad \cdots \quad c_{n-1}) \in C$ iken $(c_{n-1} \quad c_0 \quad \cdots \quad c_{n-2}) \in C$ oluyorsa $C \subset V(n,q)$ lineer koduna devirli kod denir [41].

Önerme 1.1.1. $R_n = \mathbb{F}_q[x] \big/ \langle x^n - 1 \rangle$ polinom halkası bir temel ideal halkasıdır.

Bir lineer kodun elemanlarını polinom olarak göstermek kodlama açısından oldukça önemlidir ve kodlamaya büyük zenginlikler katar. Bir lineer kod ile Önerme 1.1.1'de geçen R_n polinom halkası arasında bir izomorfizma

$$\begin{aligned} &\phi : V(n,q) \to R_n \\ &(u_0, \quad u_1, \quad \cdots \quad u_{n-1},) \mapsto u_0 + u_1 x + \cdots + u_{n-1} x^{n-1} \end{aligned}$$

olarak tanımlanabilir. Bu izomorfizma kullanılarak iki kodsözün çarpımı da sağlanmış olur. C, n uzunluğunda bir devirli kod ise $\phi(C)$, R_n'de bir ideal olur [41].

Teorem 1.1.3. C, R_n'de bir ideal olsun. Bu durumda C, n uzunluğunda bir devirli kod olur ve;

i. C'de derecesi minimum olan tekbir monik polinom $g(x)$ vardır. Bu polinomun ürettiği ideal C koduna karşılık gelir. Bu $g(x)$ polinomuna C kodunun üreteç polinomu denir.

ii. $g(x)$ polinomu $x^n - 1$ polinomunu böler.

iii. $g(x) = g_0 + g_1 x + \cdots + g_r x^{n-r}$ polinomu bir devirli kodun üreteci ise $g_0 \neq 0$ olur ve bu polinomun ürettiği kod;

$$G=\begin{pmatrix} g_0 & \cdots & g_r & 0 & 0 & \cdots & 0 \\ 0 & g_0 & \cdots & g_r & 0 & \cdots & 0 \\ 0 & 0 & g_0 & \cdots & g_r & & \vdots \\ \vdots & \vdots & \ddots & \ddots & \cdots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & g_0 & \cdots & g_r \end{pmatrix}$$

matrisinin ürettiği koda karşılık gelir [41].

Tanım 1.1.20. Baş katsayısı 1 olan polinoma monik polinom denir [41].

Önerme 1.1.2. $p(x)$ polinomu R_n'de bir monik polinom olsun. $p(x)$ polinomunun bir devirli C kodunun üreteci olması için gerek ve yeter şart $p(x)\big|x^n-1$ olmasıdır.

R_n'de bir devirli kodun üreteç polinomu olan $p(x)$, x^n-1 polinomunu böldüğünden $x^n-1=g(x)h(x)$ olur. $h(x)$ polinomuna C'nin kontrol polinomu denir [41].

Teorem 1.1.4. $C_1=\langle g_1(x)\rangle$ ve $C_2=\langle g_2(x)\rangle$ kodları R_n'de iki devirli kod olsun. Bu durumda;

i. $C_1\subset C_2$ olması için gerek ve yeter şart $g_2(x)\big|g_1(x)$ olmasıdır.

ii. $C_1\cap C_2=\langle obeb\{g_1,g_2\}\rangle$,

iii. $C_1+C_2=\langle okek\{g_1,g_2\}\rangle$ dir [41].

Teorem 1.1.5. $h(x)$ polinomu R_n'de C devirli kodunun kontrol polinomu olsun. Bu durumda;

i. C devirli kodu

$$C = \left\{ p(x) \in R_n : p(x)h(x) \equiv 0 \bmod(x^n - 1) \right\}$$

olarak tanımlanır.

ii. Eğer $h(x) = h_0 + h_1 x + \cdots + h_{n-r} x^{n-r}$ ise bu durumda C kodunun kontrol matrisi

$$H = \begin{pmatrix} h_{n-r} & \cdots & h_0 & 0 & 0 & \cdots & 0 \\ 0 & h_{n-r} & \cdots & h_0 & 0 & \cdots & 0 \\ 0 & 0 & h_{n-r} & \cdots & h_0 & & \vdots \\ \vdots & \vdots & \ddots & \ddots & \cdots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & h_{n-r} & \cdots & h_0 \end{pmatrix}$$

olur.

iii. C kodunun diki olan $C^{\perp}$ kodu da r boyutlu bir devirli koddur ve
$h^{\perp} = h_0^{-1} x^{n-r} h\left(x^{-1}\right)$

polinomu $C^{\perp}$'nin üreteç polinomudur [41].

Tanım 1.1.21. C kodu $g(x)$ polinomu ile üretilen $[n, n-r]$ parametreli bir devirli kod ve $g(x)$ polinomunun derecesi r olsun. Bir $u(x)$ polinomunun sendromu $S(u(x))$ ile gösterilir ve bu sendrom $u(x)$ polinomunun $g(x)$ polinomuna bölümünden elde edilen kalana eşittir. Yani

$$u(x) = q(x)g(x) + S(u(x)),\ der\left(S(u(x))\right) < r$$

dir [41].

Tanım 1.1.22. Mümkün olabilecek en büyük minimum uzaklığa sahip $[n, k, n-k+1]$ parametrelerine sahip lineer koda maksimum uzaklığa ayrışabilen kod veya kısaca MDS kod denir [31].

Önerme 1.1.3. C kodu $\mathbb{F}_q$ cismi üzerinde Hamming metriğine göre bir $[n, k, d]$ lineer kod olsun. Bu durumda Singleton sınırı

$$q^k \leq q^{n-d+1}$$

dir. Bu eşitliği sağlayan kodlar MDS'dir [31].

Tanım 1.1.24. Kompleks bir $U_{m\times n}$ matrisinin Hermit eşleniği, bu matrisin transpozesinin eşleniği olarak tanımlanır ve $U^{\dagger}$ sembolü ile gösterilir [22].

Tanım 1.1.25. Eğer $U^{\dagger}U = I$ ise U matrisine üniter matris denir [22].

BÖLÜM 2. KUANTUM HESAPLAMAYA GİRİŞ VE HATA DÜZELTEBİLEN KUANTUM KODLAR

2.1. Giriş

Değişen ve gelişen çağımızda, hayatın hemen her alanında kullanılan bilgisayarların daha hızlı, daha güvenilir olması, bilgiyi daha iyi saklama, daha iyi iletme ve daha fazla bilgi depolama amacı ile birçok araştırmacı yeni teknikler geliştirmektedir. Son zamanlarda özellikle kuantum bilgisayarlarının düşünülmesi ile kuantum bilginin taşınması sırasında oluşabilecek hataların tespiti ve bu hataların düzeltilmesi için hata düzeltebilen kuantum kodları geliştirilmektedir. Kuantum hesaplama kuantum fiziğinin kurallarını kullanarak çok daha hızlı hesaplama yapmayı hedeflemektedir. Günümüz bilgisayarlarında işlemci hızı için iletkenliği yüksek malzemeler kullanılmaktadır. Kuantum bilgisayarlarda ise bu malzemeler yerine foton çiftlerinin kullanılması düşünülmektedir. Bu yolla tek işlemci ile süper bilgisayar hızına ulaşılması planlanmaktadır. Örneğin klasik kodla çalışan bir bilgisayarın 400 basamaklı bir sayıyı çarpanlarına ayırma işlemini yapması aylarca belki yıllarca sürerken kuantum bilgisayarı aynı soruyu birkaç dakikada çözebilecektir. Kuantum bilgisinin işlenmesi, bilgi saklanması, bilgiye daha hızlı erişim gibi birçok uygulama için yararlı olabilir. Kuantum kodlar sadece bilgi taşınmasında, saklanmasında ve bilgiye erişim hızında değil, aynı zamanda tıpta (her organın kodlarının kopyalanıp saklanması gibi), askeri alanlarda da kullanılabilir olması için özellikle son dönemlerde yoğun çalışmalar yapılmaktadır.

Kuantum bilgi bilimi; kuantum mekanik, bilgisayar bilimleri ve bilgi teorisinin bir birleşimi olarak doğmuş, yeni ve hızla gelişmekte olan bir daldır. Kuantum mekaniğin ana hatları 1920–30 yılları arasında tamamlanmış ve günümüzde kuantum fiziği ve kuantum mekaniğindeki standart şeklini almıştır. Özellikle bilgisayar bilimleri ve bilgi teorisinin doğmasıyla beraber 1970'lerde karmaşıklık, şifreleme ve kodlama teorileri gibi alanlara kuantum mekaniğinin prensiplerinin uygulamasıyla

kuantum dolanıklık, kuantum şifreleme ve kuantum kodlama gibi yeni dalların ortaya çıkması kaçınılmaz olmuştur.

İlk kuantum hata düzeltebilen kod Shor [45] ve Steane [46] tarafından birbirinden bağımsız çalışmalar olarak geliştirilmiştir. Shor'un geliştirdiği kod bir kubiti dokuz kubite kodlayarak bir kubitteki herhangi bir hatayı düzeltebilmektedir. Steane ise bir kubiti yedi kubite kodlamıştır. Daha sonra bu alanda birçok çalışma olmuştur. 1996 yılında Calderbank ve Shor klasik kodlardan kuantum kodlarına geçiş için yeni bir yöntem bulmuş ve bu yeni yöntemde özellikle kendine ortogonal ve kendine dik klasik kodları kullanmışlardır [10]. Klasik kodlar hakkında daha geniş bilgi için [7,31,43] referanslı kaynaklara bakılabilir. 1998'de Calderbank, Rains, Shor ve Sloane $GF(4)$ üzerindeki klasik kodlardan yararlanarak kuantum kodlara geçiş için bir yöntem geliştirdiler [11]. Bu yöntemde $GF(4)$ üzerindeki toplamsal kendine dik ya da kendine ortogonal klasik kodlar kullanılmıştır. Klasik kodlardan yararlanarak kuantum kod elde edilebilme yöntemi kullanılarak birçok çalışma yapılmıştır. 2001'de $GF(4^m)$ üzerindeki klasik kodların $GF(4)$ üzerine görüntüsü kullanılarak kuantum kod elde edilmiştir [48]. 2004'de minimum mesafesi 3 veya 4 olan ikili kuantum kodlar [30], 2004'de kuantum BCH kodlar [44], 2007'de Clifford cebri üzerinden kuantum kodlar [50], projektif geometri kullanılarak kuantum kod [49] bu konuda yazılmış binlerce makaleden bazılarıdır. Klasik kodlardan yararlanarak kuantum kod elde edilen belli başlı makaleler [8, 9, 10, 11, 16, 18, 19, 20, 21, 33, 34, 36, 44, 48, 49] kaynaklarında bulunabilir. Ayrıca kuantum kodların hata düzeltme sınırları [2, 3, 5, 17, 25], stabilizer kuantum kodlar [6, 12, 25, 26, 42, 50], nonstabilizer kuantum kodlar [4] hakkında da birçok çalışma vardır.

Bu bölümde kuantum hesaplamaya bir giriş yapılıp, kullanılacak notasyonlar ele alınacaktır.

2.2. Dirac Notasyonu ve Hilbert Uzaylar

Dirac notasyonunu ilk olarak Paul Adrien Maurice Dirac kuantum mekanikte kullanmaya başlamıştır. Vektörler alışık olunduğu üzere genellikle $\vec{u}$ veya **u** gibi sembollerle gösterilir. Bra-Ket notasyonu olarak da bilinen Dirac notasyonunda da $|u\rangle$ (ket u diye okunur) ile esasen bir vektör belirtilmektedir. Bra $(\langle\cdot|)$ notasyonu ile ise ket vektörünün eşlenik transpozesi gösterilmektedir. Örneğin

$$|u\rangle = \begin{pmatrix} 1 \\ i \end{pmatrix} \text{ ise } \langle u| = \begin{pmatrix} 1 & -i \end{pmatrix}$$

olur. Ket $|u\rangle$ ile bra $\langle v|$ vektörleri arasındaki iç çarpım $\langle v|u\rangle$ biçiminde gösterilir. Kuantum kodlama sonlu boyutlu Hilbert uzayları üzerinde tanımlanır. Genellikle sonlu boyutlu Hilbert uzayı olarak kompleks vektör uzayı alınır. iki boyutlu Hilbert uzayı olarak $\mathbb{C}^2$ alınırsa, bu uzay için bir baz olarak

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

alınabilir.

Tanım 2.2.1. $A = (a_{ij})_{m\times n}$ ve B de herhangi bir matris olmak üzere A ile B matrislerinin tensör çarpımı $A \otimes B$ şeklinde gösterilir ve

$$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{bmatrix}$$

olarak tanımlanır. Bu matrislerin tensör çarpımı $A \otimes B$ yerine AB olarak da gösterilmektedir. Örnek olarak

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

için

$$|0\rangle|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = |00\rangle, |1\rangle|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = |11\rangle$$

$$|0\rangle|1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = |01\rangle, |1\rangle|0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = |10\rangle$$

elde edilir. Bu durum $n-$ boyuta;

$$\left|\underbrace{00\cdots00}_{n}\right\rangle, \left|\underbrace{00\cdots01}_{n}\right\rangle, \cdots, \left|\underbrace{11\cdots10}_{n}\right\rangle, \left|\underbrace{11\cdots11}_{n}\right\rangle$$

biçiminde genelleştirilebilir. Bu durumda

$$\left|\underbrace{00\cdots00}_{n}\right\rangle \Leftrightarrow \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}, \left|\underbrace{00\cdots01}_{n}\right\rangle \Leftrightarrow \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}, \cdots, \left|\underbrace{11\cdots10}_{n}\right\rangle \Leftrightarrow \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \\ 0 \end{pmatrix}, \left|\underbrace{11\cdots11}_{n}\right\rangle \Leftrightarrow \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

şeklinde bir eşleme olur [24, 35].

Tanım 2.2.2. $|u\rangle = (u_1, u_2, \ldots, u_m)$ vektörü ile $\langle v|^{tr} = (v_1, v_2, \ldots, v_n)$ vektörünün dış çarpımı

$$|u\rangle\langle v| = \begin{pmatrix} u_1v_1 & u_1v_2 & \cdots & u_1v_n \\ u_2v_1 & u_2v_2 & \cdots & u_2v_n \\ \vdots & \vdots & \ddots & \vdots \\ u_mv_1 & u_mv_2 & \cdots & u_mv_n \end{pmatrix}$$

olarak tanımlanır [35].

Örnek 2.2.1. $|\psi\rangle = -|10\rangle + i|11\rangle$ ve $|\varphi\rangle = i|10\rangle + |11\rangle$ alınırsa

$$\langle\varphi| = \begin{pmatrix} 0 & 0 & -i & 1 \end{pmatrix} \text{ ve } \langle\varphi|\psi\rangle = 2i$$

olur. A matrisi ile $|\psi\rangle$ sütun matrisi çarpıma uygun matrisler olmak üzere $\langle\phi|A|\psi\rangle$ ile $|\phi\rangle$ ve $A|\psi\rangle$'nin iç çarpımı veya buna denk olarak $A^\dagger|\phi\rangle$ ve $|\psi\rangle$'nin iç çarpımı gösterilir. $|\psi\rangle\langle\varphi|$ ile ise $|\psi\rangle$ vektörü ile $\langle\varphi|$ vektörünün dış çarpımı gösterilir. Buna göre

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

alınırsa sırası ile $\langle\varphi|A|\psi\rangle$ ve $|\psi\rangle\langle\varphi|$ çarpımı aşağıdaki gibi olur.

$$\langle\varphi|A|\psi\rangle = \begin{pmatrix} 0 & 0 & -i & 1 \end{pmatrix}\left[\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 0 \\ -1 \\ i \end{pmatrix}\right] = \begin{pmatrix} 0 & 0 & -i & 1 \end{pmatrix}\begin{pmatrix} 0 \\ -1 \\ i \\ 0 \end{pmatrix} = 1,$$

$$|\psi\rangle\langle\varphi| = \begin{pmatrix} 0 \\ 0 \\ -1 \\ i \end{pmatrix}\begin{pmatrix} 0 & 0 & -i & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & i & -1 \\ 0 & 0 & 1 & i \end{pmatrix}.$$

Tanım 2.2.3. $\mathcal{H}$ vektör uzayı üzerinde bir lineer operatör bu vektör uzayının kendi üzerine bir lineer dönüşümü $\left(T:\mathcal{H}\to\mathcal{H}\right)$ olarak tanımlanır [24].

Teorem 2.2.1. $B=\left\{\left|b_n\right\rangle\right\}$ kümesi $\mathcal{H}$ vektör uzayının bir ortonormal baz kümesi olsun. Bu durumda $\mathcal{H}$ üzerindeki her lineer operatör $T_{n,m}=\left\langle b_n\right|T\left|b_m\right\rangle$ olmak üzere

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

şeklinde yazılabilir. T operatörünün $\left|\psi\right\rangle\in\mathcal{H}$ elemanına etkisi

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

dir.

Örnek 2.2.2. $X=\begin{pmatrix}0&1\\1&0\end{pmatrix}$, $Z=\begin{pmatrix}1&0\\0&-1\end{pmatrix}$ ve $Y=\begin{pmatrix}0&-1\\1&0\end{pmatrix}$ olarak bilinen Pauli matrislerinden X ve Z matrisleri için

$$X=\left|0\right\rangle\left\langle 1\right|+\left|1\right\rangle\left\langle 0\right|,\ Z=\left|0\right\rangle\left\langle 0\right|-\left|1\right\rangle\left\langle 1\right|$$

olur [24].

Tanım 2.2.4. $\mathcal{H}^*=\left\{\left\langle\psi'\right|:\left|\psi\right\rangle\mapsto\left\langle\psi'\middle|\psi\right\rangle\in\mathbb{C}\right\}$ olmak üzere, eğer T operatörü $\mathcal{H}$ vektör uzayında bir lineer operatör ise $T^\dagger$ da $\mathcal{H}^*$ üzerinde bir lineer operatör olur [24].

Tanım 2.2.5. Eğer $\mathcal{H}$ vektör uzayında bir P lineer operatörü için $P^2=P$ oluyorsa bu operatöre bir projektör (iz düşüm operatörü) denir. Eğer $P^\dagger=P$ ise P lineer operatörüne bir ortogonal projektör denir [24].

Tanım 2.2.6. T bir operatör olmak üzere, $T|\psi\rangle = c|\psi\rangle$ olacak biçimde c sabiti varsa $|\psi\rangle$ vektörüne T operatörünün bir öz vektörü ve c sabitine de bu öz vektöre karşılık gelen öz değeri denir [24].

Tanım 2.2.7. Eğer bir A lineer operatörü $AA^\dagger = A^\dagger A$ eşitliğini sağlarsa bu operatöre bir normal operatör denir. Üniter ve Hermit operatörler normal operatörlerdir [24].

Teorem 2.2.2. Sonlu boyutlu bir $\mathcal{H}$ Hilbert uzayı üzerinde tanımlı her normal T operatörü için, $\mathcal{H}$ Hilbert uzayının bir ortonormal bazı T matrisinin $|T_i\rangle$ öz vektörlerinden oluşacak biçimde mevcuttur [24].

Teorem 2.2.3. Λ bir köşegen matris olmak üzere her sonlu boyutlu normal T matrisi için $T = P\Lambda P^\dagger$ olacak şekilde bir P tersinir matrisi vardır.

Burada, Λ matrisinin köşegen elemanları T'nin öz değerleridir. P'nin sütunları T'nin öz vektörlerinden elde edilir [24].

Örnek 2.2.3. X Pauli matrisi için

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$$

olduğundan

$$P = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \text{ ve } \Lambda = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

olur. Böylece X'in öz değerleri 1 ve -1, X'in öz vektörleri de

$$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \text{ ve } \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix}$$

olur. Dirac notasyonları kullanılarak

$$X = |0\rangle\langle 1| + |1\rangle\langle 0|,$$

$$P = \frac{1}{\sqrt{2}}|0\rangle\langle 0| + \frac{1}{\sqrt{2}}|0\rangle\langle 1| + \frac{1}{\sqrt{2}}|1\rangle\langle 0| - \frac{1}{\sqrt{2}}|1\rangle\langle 1|,$$

$$= |+\rangle\langle 0| + |-\rangle\langle 1|,$$

$$\Lambda = |0\rangle\langle 0| - |1\rangle\langle 1| = Z$$

elde edilir. Öz değerler ise

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

şeklinde yazılır.

Teorem 2.2.4. Eğer $|\psi\rangle$ vektörü $\mathcal{H}_1 \otimes \mathcal{H}_2$ tensör çarpım uzayında bir vektör ise $p_0, p_1, \ldots, p_i$ sayıları negatif olmayan reel sayılar olmak üzere

$$|\psi\rangle = \sum_i \sqrt{p_i}\,|\varphi_i^1\rangle|\varphi_i^2\rangle$$

ve $\{|\varphi_i^1\rangle\}$ kümesi $\mathcal{H}_1$ için, $\{|\varphi_i^2\rangle\}$ kümesi de $\mathcal{H}_2$ için ortonormal bazları olur [24].

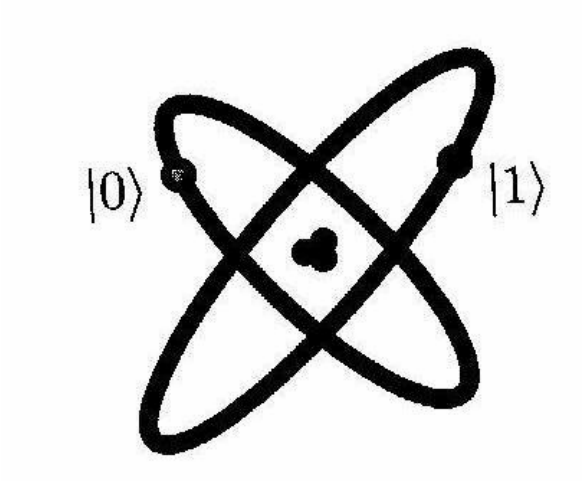
2.3. Kuantum Bitler (Kubitler)

Klasik hesaplamada bilgi birimi olarak kullanılan bit yerine kuantum hesaplamada kuantum bit veya kısaca kubit kullanılır. Klasik hesaplamada bir bit ya 0 ya da 1 halinde olabilir. Kubitlerin bulundukları hal durumunu bu kadar kolay söylemek mümkün değildir. Örneğin iki boyutlu bir kuantum hal uzayında bir kubit $|0\rangle$, $|1\rangle$ ya da bunların süperpozisyonu (lineer kombinasyonu) olan

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

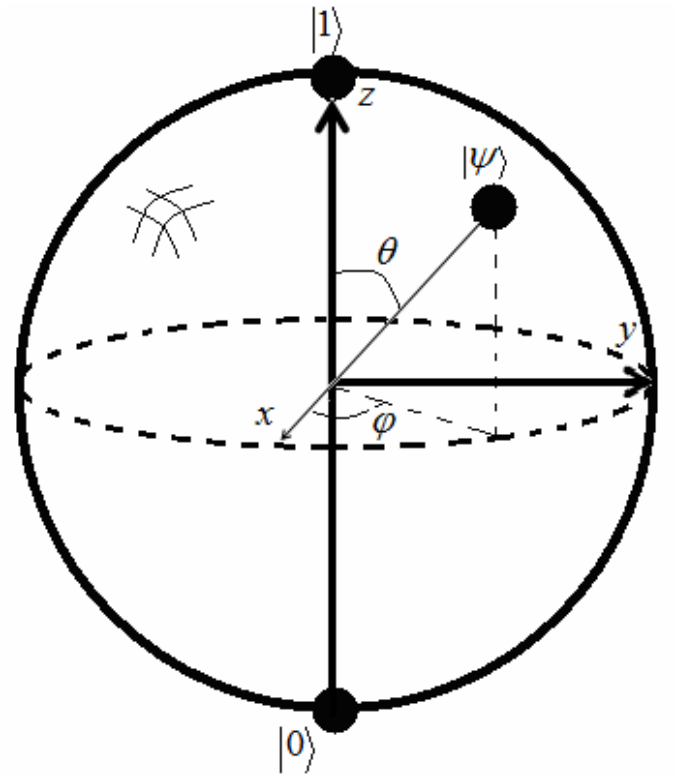
halinde olabilir. Bu kuantum hal uzayı için $|0\rangle$ ve $|1\rangle$ ortonormal baz durumundadır. Eğer $|\psi\rangle$, $a|0\rangle$ haline de ise $\langle\psi|\psi\rangle = |a|^2 = 1$ olmalıdır. $|\psi\rangle = a|0\rangle + b|1\rangle$ halinde ise $\langle\psi|\psi\rangle = |a|^2 + |b|^2 = 1$ olur. Çünkü $|\psi\rangle$'nin konumunun olasılıklarının toplamı daima 1'dir.

Bir bitin 0 halinde mi yoksa 1 halinde mi olup olmadığı incelenebilir. Örneğin bilgisayarlar hafızalarındaki bilgiye ulaşmak için her defasında bunu yaparlar. Fakat bunu kubitler için yapmak mümkün değildir. Kuantum hali hakkında daha az bilgi bilinir. Bir kubit ölçüldüğü zaman sonuç ya sıfırdır ya da birdir. Şekil 2.1'de bir atomdaki iki elektronik seviyenin kubit gösterimi verilmektedir. E=0 enerji düzeyinde atom taban haldedir ve atomun bu hali ket $|0\rangle$ ile diğer durumda (uyarılma) ise ket $|1\rangle$ ile gösterilir.



Şekil 2.1 Bir atomdaki iki elektronik seviyenin kubit gösterimi

E=0 durumundan elektron başka bir enerji düzeyine, foton gönderilmesi ile geçirilebilir. Elektron $|0\rangle$ halinden $|1\rangle$ haline geçerken "yolun yarısında" $|+\rangle$ halinde olacaktır. Örneğin $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$. Bu da kuantum sisteminde gözlemler, ihtimaller ve süperpozisyon hallerinin yorumlanabilmesi için son derece önemlidir. Şekil 2.2 kubitlerin geometrik olarak gösterimi hakkında daha detaylı bilgi vermektedir.



Şekil 2.2 Bir kubitin Bloch küresindeki gösterimi

$|a|^2 + |b|^2 = 1$ denkleminden yaralanarak $|\psi\rangle$ kubitinin bulunduğu hal durumu

$$|\psi\rangle = a|0\rangle + b|1\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\right), \quad \gamma,\varphi,\theta \in \mathbb{R}$$

şeklinde daha genel olarak yazılabilir. $e^{i\gamma}$ 'nın bu eşitliğe görülebilir bir etkisi olmadığından

$$|\psi\rangle = a|0\rangle + b|1\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$$

elde edilir. Bu eşitlik [32] numaralı referansta daha açık olarak yazılmıştır.

Klasik iki bit olduğunda bunların mümkün durumları 00, 01, 10, 11 şeklindedir. Çoklu kubitlerde de benzer bir gösterim kullanılır. Örneğin iki tek kubit $|0\rangle$ ve $|1\rangle$ kullanarak ikili kubitler $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ şeklinde gösterilebilir. Fakat ikili kubitler yalnızca bunları değil aynı zamanda bunların süperpozisyonlarını da içerir. O halde tüm ikili kubitler

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

şeklinde gösterilebilir. Tekli kubitlerde olduğu gibi burada da

$$|\alpha|_{00}^2 + |\alpha|_{01}^2 + |\alpha|_{10}^2 + |\alpha|_{11}^2 = 1 \quad \alpha_{00},\alpha_{01},\alpha_{10},\alpha_{11} \in \mathbb{C}$$

olur. Bu yolla çoklu kubit halleri genel olarak oluşturulabilir. EPR (Einstein, Podolsky, Rosen) çifti veya Bell hali olarak bilinen $\left(|00\rangle + |11\rangle\right)/\sqrt{2}$ hali bilinen iki kubit halelerinin en önemlilerinden biridir. Burada $|x_1x_2\rangle$ gösterimi $|x_1\rangle$ ile $|x_2\rangle$ hallerinin tensör çarpımını göstermektedir [35].

2.4. Kuantum Mantık Kapıları

Klasik devreler, teller ve mantık kapılarından oluşur. Teller bilgiyi devreye taşır. Mantık kapıları ise bilgiyi bir halden başka bir hale dönüştürür. Örneğin *NOT* kapısı 0 halini 1 ve 1 halini 0 olarak değiştirir. Kodlama açısından kanalda oluşabilecek hatalara neden olan bu mantık kapılarını belirlemek (ya da her hataya bir mantık kapısı karşı getirmek) oldukça önemlidir. Kanalda meydana gelen hataya neden olan mantık kapısı bilinmezse, hatalı hali her zaman geri düzeltme ihtimali mümkün değildir. Kuantum mantık kapıları da kuantum kanalında hataların karakterize edilmesini sağlar. Sonsuz tane kuantum mantık kapısı vardır. Fakat bütün bu mantık kapılarının bir prototipi, bazı mantık kapıları kullanılarak elde edilmektedir. Bunun için önce tekli kubit mantık kapıları daha sonra da çoklu kubit mantık kapıları oluşturulmalı. $|\psi\rangle = a|0\rangle + b|1\rangle$ tekli kubitine etki eden mantık kapılarından bazıları şunlardır:

$$\textit{Pauli X Kapısı}(\textit{NOT Kapısı}) \rightarrow \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\textit{Pauli Z Kapısı} \rightarrow \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$\textit{Pauli Y Kapısı} \rightarrow \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \left(\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \right)$$

$$\textit{Hadamard Kapısı } H \rightarrow \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Bu mantık kapıları $|\psi\rangle = a|0\rangle + b|1\rangle$ kubitine şöyle etki eder:

$$X|\psi\rangle = a|1\rangle + b|0\rangle,\ Z|\psi\rangle = a|0\rangle - b|1\rangle,\ Y|\psi\rangle = a|1\rangle - b|0\rangle$$

ve

$$H|\psi\rangle = a\frac{|0\rangle + |1\rangle}{\sqrt{2}} + b\frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

Klasik kodlamada bir hata kodsöze iki kere uygulanırsa (ikili kodlarda) sonunda yine kodsözün kendisi elde edilir. Kuantum kodlamada buna benzer. Örneğin

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

kubitine X Pauli matrisi etki ederse

$$X|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$$

olur. Tekrar uygulanırsa

$$X|1\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

olur. Hadamard kapısı aynı kubite ard arda iki kez uygulanırsa;

$$H|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{|0\rangle + |1\rangle}{\sqrt{2}},$$

$$H\frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 2 \\ 0 \end{pmatrix} = |0\rangle$$

olur. Pauli matrisleri üniter matris olduklarından kuantum hallerine yukarıdaki gibi etki etmeleri beklenirdi. Tekli mantık kapıları sonsuz tane olmasına rağmen çok daha küçük bir kümenin özellikleri bilinirse tüm kümenin özellikleri anlaşılır. Herhangi bir U üniter matrisi α, β, γ ve δ reel sayı olmak üzere

$$U = e^{i\alpha}\begin{pmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{pmatrix}\begin{pmatrix} \cos\gamma/2 & -\sin\gamma/2 \\ \sin\gamma/2 & \cos\gamma/2 \end{pmatrix}, \quad \begin{pmatrix} e^{-i\delta/2} & 0 \\ 0 & e^{i\delta/2} \end{pmatrix}$$

biçiminde ayrıştırılabilir. Böylece herhangi bir 2×2 tipindeki tekli kubit mantık kapısı kuantum kapılarının bir sonlu kümesi kullanılarak oluşturulabilir [35].

Keyfi sayıdaki kubitler için bu durum kuantum kapılarının bir sonlu kümesi kullanılarak üretilebilir. Keyfi sayıdaki kubitler için oluşturulan bu kümeye "evrensel kapılar" kümesi denir. Bu kümenin oluşturulması için öncelikle çoklu kubit mantık kapılarının oluşturulması gerekir. Çoklu kubit kapılarından birisi olan *CNOT* mantık kapısı

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

matrisi ile gösterilir. *CNOT* mantık kapısı ikili kubitlere aşağıdaki gibi etki eder:

$$CNOT\left|00\right\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}\left[\begin{pmatrix} 1 \\ 0 \end{pmatrix}\otimes\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right] = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \left|00\right\rangle,$$

$$CNOT\left|01\right\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}\left[\begin{pmatrix} 1 \\ 0 \end{pmatrix}\otimes\begin{pmatrix} 0 \\ 1 \end{pmatrix}\right] = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \left|01\right\rangle,$$

$$CNOT\left|10\right\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}\left[\begin{pmatrix} 0 \\ 1 \end{pmatrix}\otimes\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right] = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \left|11\right\rangle,$$

$$CNOT|11\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \left[\begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right] = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = |10\rangle .$$

Diğer mantık kapılarının bir prototipi tekli kubit mantık kapıları ve *CNOT* kullanılarak elde edilebilir. Örneğin swap kapısı olarak bilinen

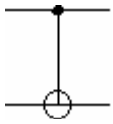
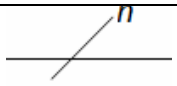
$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

mantık kapısı ile aynı işlevi yapan bir prototip vardır. Bu prototip verilmeden önce bir kuantum devresi ve bu devrenin işlevinin açıklanması gerekir.

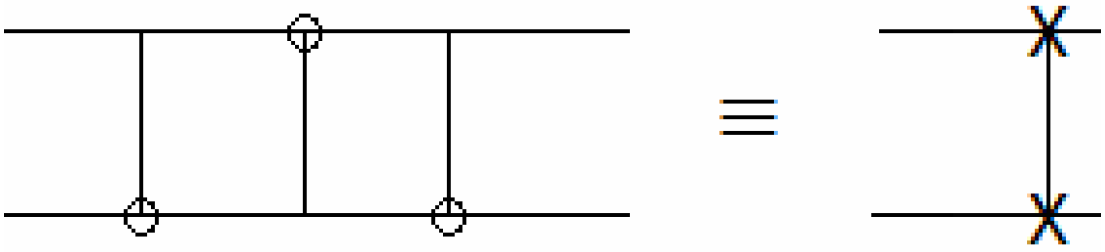
2.5. Kuantum Devre

Bir kuantum devresinde kuantum mantık kapılarından bazıları ve devre elemanları Tablo 2.1 de gösterilmektedir. Bu tabloda gösterilen mantık kapıları dışında da mantık kapısı vardır. Fakat diğer mantık kapıları bu mantık kapılarının bir prototipi olarak elde edilebilir.

Tablo 2.1 Kuantum mantık kapılarından bazıları

Mantık Kapısı	Devredeki Gösterimi	Matris Gösterimi
X	$-\boxed{X}-$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
Z	$-\boxed{Z}-$	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
Y	$-\boxed{Y}-$	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$
H	$-\boxed{H}-$	$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
P	$-\boxed{S}-$	$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$
$T = \pi/8$	$-\boxed{T}-$	$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$
CNOT		$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$
Ölçüm		
Kuantum bit		
Klasik bit		
n Kubit		

Şekil 2.3'de bir kuantum devresi görülmektedir. Bu devrede her satır bir tele karşılık gelir. Kuantum devre soldan sağa doğru okunur. Şekil 2.3'de görülen teller, fiziksel tellere karşılık gelmek zorunda değildir. Bunun yerine zaman akışı ya da foton gibi bir fiziksel parçacığın uzayda bir yerden başka bir yere hareketine de karşılık gelebilir.



Şekil 2.3 Swap kuantum mantık kapısı: İkili bir kubitte kubitlerin yer değiştirmesi

Klasik devre ile kuantum devresi arasında bazı farklılıklar vardır. Bu farklılıklar şöyle sıralanabilir.

i . Kuantum devrede döngü (loops) yoktur.

ii . Kuantum devrede teller arasında bir geçiş yoktur.

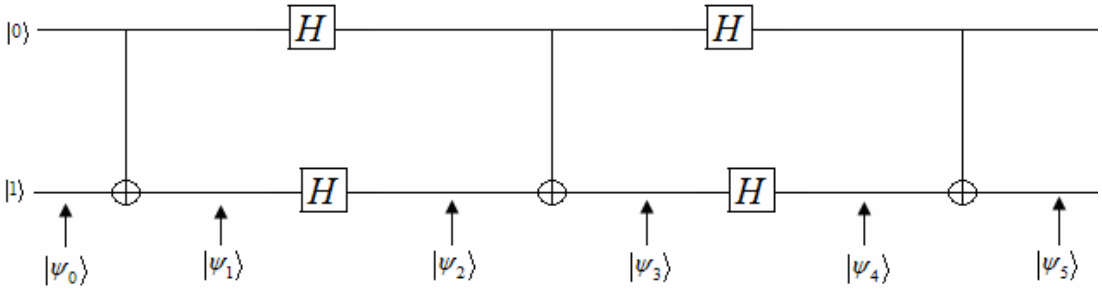
iii . Kuantum devre devresel değildir. Bu sebeple devreden aynı yolla geri dönülmez [35].

Şimdi swap kuantum mantık kapısının bir prototipi incelenebilir.

Örnek 2.5.1 Swap mantık kapısı kubitlere şöyle etki eder:

$$SWAP|00\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = |00\rangle,\ SWAP|11\rangle = |11\rangle,\ SWAP|10\rangle = |01\rangle,\ SWAP|01\rangle = |10\rangle.$$

Bu mantık kapısının prototipi Şekil 2.4'de verilmektedir.



Şekil 2.4 Swap mantık kapısının prototipi

Bu devreye göre birinci satırdan $|0\rangle$ ve ikinci satırdan $|1\rangle$ kuantum hali devreye girmektedir. Yani ilk hal $|\psi_0\rangle = |01\rangle$'dir. Bu hal devrede ilk kapı olan *CNOT* kapısından geçtikten sonra $|\psi_1\rangle = |01\rangle$ olur ve daha sonra Hadamard kapısından geçince

$$|\psi_2\rangle = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = \frac{|00\rangle + |10\rangle - |01\rangle - |11\rangle}{2}$$

halini alır. Bu mantığa göre hareket edilirse;

$$|\psi_3\rangle = CNOT\,|\psi_3\rangle = \frac{|00\rangle + |11\rangle - |01\rangle - |10\rangle}{2},$$

$$|\psi_4\rangle = H\,\frac{|00\rangle + |11\rangle - |01\rangle - |10\rangle}{2}\,H = H\left(\frac{|0\rangle - |1\rangle}{2}\right)\left(\frac{|0\rangle - |1\rangle}{2}\right)H = |11\rangle,$$

$$|\psi_5\rangle = CNOT\,|\psi_4\rangle = CNOT\,|11\rangle = |10\rangle$$

elde edilir. Diğer haller için de aynı devre kullanılırsa;

$$|\psi_0\rangle = |00\rangle \Rightarrow |\psi_5\rangle = |00\rangle, \quad |\psi_0\rangle = |11\rangle \Rightarrow |\psi_5\rangle = |11\rangle, \quad |\psi_0\rangle = |10\rangle \Rightarrow |\psi_5\rangle = |01\rangle$$

olur. Görüldüğü gibi bu devre ile swap kapısının yaptığı iş aynıdır. Bu sebeple bu devre swap mantık kapısının bir prototipidir.

Kuantum kodların dekodlamasını kavrayabilmek için bu prototiplerle beraber kuantum dolanıklık ve kuantum ışınlamaya da değinmek gerekir.

2.6. Kuantum Dolanıklık (Entanglement)

Dolanıklık bir kuantum olgusudur. Klasik hesaplamada karşımıza çıkmayan bu durum çoklu kubit hallerinde meydana gelir. Örneğin $\mathcal{H}_1$ ve $\mathcal{H}_2$ iki kuantum hal uzayı olsun. Bu hal uzayları ile ikili kuantum hal uzayını; elemanları birinci hal uzayının elemanları ile ikinci hal uzayının elemanlarının tensör çarpımı şeklinde alınıp oluşturulur. Yani

$$\mathcal{H}=\mathcal{H}_1\otimes\mathcal{H}_2=\left\{|\psi_1\rangle\otimes|\psi_2\rangle : |\psi_1\rangle\in\mathcal{H}_1, |\psi_2\rangle\in\mathcal{H}_2\right\}$$

biçiminde bir hal uzayı yazılabilir. İşte bu noktada dolanıklık ortaya çıkar. Şöyle ki $|\psi_1\psi_2\rangle\in\mathcal{H}$, $|\psi_1\rangle\in\mathcal{H}_1, |\psi_2\rangle\in\mathcal{H}_2$ iken bu hale bir U operatörü etki ettikten sonra $|\psi_1'\psi_2'\rangle$ oluşan yeni hali verecek $|\psi_1'\rangle\in\mathcal{H}_1, |\psi_2'\rangle\in\mathcal{H}_2$ olmayabilir. Aşağıdaki örnek bu durum için verilmiştir [35].

Örnek 2.6.1. $|\psi_1\rangle=|0\rangle$ kubiti göz önüne alınır ve Hadamard kapısı bu kubite uygulanırsa

$$|\psi_1'\rangle=H|\psi_1\rangle=\frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right)$$

olur. $|\psi_2\rangle=|0\rangle$ kubiti alınır ve bu iki kubit tensör çarpılırsa, iki kubitli hal uzayında

$$|\psi\rangle=|\psi_1'\rangle\otimes|\psi_2\rangle=|\psi_1'\psi_2\rangle=\frac{1}{\sqrt{2}}\left(|00\rangle+|10\rangle\right)$$

olur. Bu son duruma

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

uygulanırsa

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

elde edilir. Fakat $\frac{1}{\sqrt{2}}\left(\left|00\right\rangle + \left|11\right\rangle\right)$ hali bu iki kubitli hal uzayında $\left|\varphi_1\right\rangle \otimes \left|\varphi_2\right\rangle$ şeklinde ayrışamaz. O halde hal uzayı bileşenlerine ayrılamaz. Bu durum kodlama içinde oldukça ciddi bir durumdur. Zira bu bir kodsöz ve dolanıklık da kanalda oluşan bir hata olarak düşünülür. Aşağıdaki örnekte dolanıklığın ölçüme etkisi ele alınmaktadır.

Tanım 2.6.1. Kuantum ölçümleri, $\{M_m\}$ ölçüm operatörlerinin (matrislerinin) kümesi tarafından tanımlanır. Bu ölçüm operatörleri ölçülmekte olan hal uzayına (ilk hale) etki eden operatörlerdir. m indisi deneyde oluşabilecek ölçüm çıktılarına karşılık gelir. Ölçümden hemen önce kuantum sisteminin durumu $\left|\psi\right\rangle$ ise m çıktısının olma ihtimali $p(m)$ ile gösterilir ve $p(m) = \left\langle\psi\right| M_m^\dagger M_m \left|\psi\right\rangle$ olarak tanımlanır. Ölçümden sonra son halin ihtimali

$$\frac{M_m\left|\psi\right\rangle}{\sqrt{\left\langle\psi\right| M_m^\dagger M_m \left|\psi\right\rangle}}$$

ile hesaplanır. Ölçüm operatörleri $\sum_m M_m^\dagger M_m = I$ eşitliğini sağlamalıdır.

Örnek 2.6.2.

$$M_0 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \text{ ve } M_1 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

ölçüm operatörleri göz önüne alınsın. Ölçüm operatörleri $p(m=0)$ ile ilk halin ihtimali gösterilir ve bu ihtimal

$$\sqrt{\langle\psi|M_0^{\dagger}M_0|\psi\rangle}=1$$

olarak hesaplanır. İlk hal olan $|\psi_1'\psi_2\rangle$ haline $CNOT$ uygulamadan önce ölçüm yapılırsa

$$\frac{M_0|\psi\rangle}{\sqrt{\langle\psi|M_0^{\dagger}M_0|\psi\rangle}}=\begin{pmatrix}\frac{1}{\sqrt{2}}\\0\\\frac{1}{\sqrt{2}}\\0\end{pmatrix}|\psi_1'\psi_2\rangle=|\psi\rangle$$

olur. Bu hale $CNOT$ uyguladıktan sonra ölçüm yapılırsa

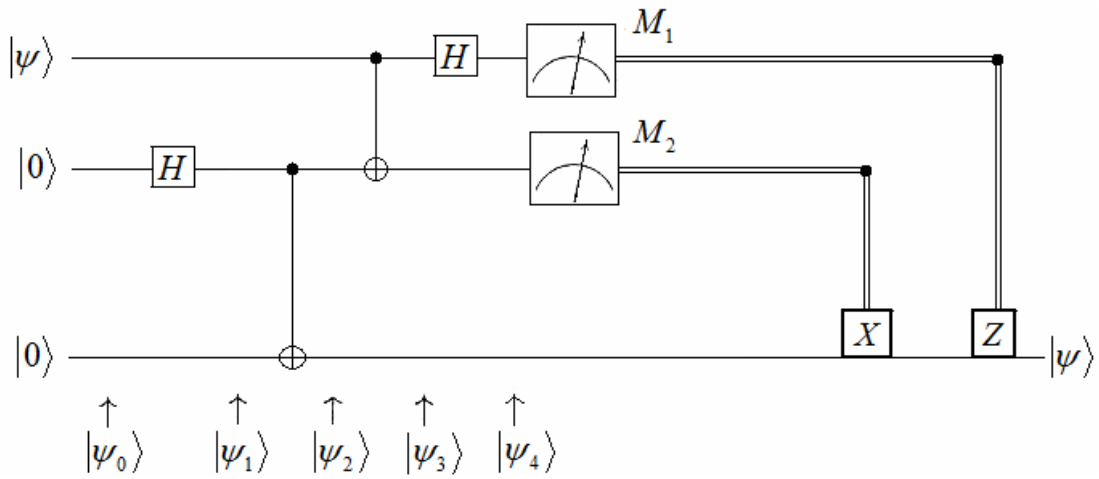
$$\frac{M_0|\psi'\rangle}{\sqrt{\langle\psi'|M_0^{\dagger}M_0|\psi'\rangle}}=\begin{pmatrix}1\\0\\0\\0\end{pmatrix}=|00\rangle$$

olur. İhtimal ise $p(0)=\sqrt{\langle\psi'|M_0^{\dagger}M_0|\psi'\rangle}=\frac{1}{2}$ dir.

Görüldüğü gibi ölçüm kuantum halini geri getirilemez şekilde bozmaktadır. Bu ölçüm sonrası elde edilen değer muhtemel değerlerden sadece birisidir. Bu ölçüm sistemin bilgisini tek bir duruma indirgemiş diğer tüm bilgiyi silmiştir. Oysa kuantum bilgisine ulaşmak için tüm veriye ihtiyaç vardır. Üstelik sistem üzerinde tekrar ölçüm yapmak da mümkün değildir. Oysa klasik kodlamada belli bir ölçümle (sendrom dekodlaması gibi) bilgiye yeniden ulaşılabilir.

2.7. Kuantum Işınlama

Kuantum ışınlama; kuantum halini gönderen ile alan arasında bir kuantum iletişim kanalı olmasa bile kuantum hallerini taşımak için kullanılan bir tekniktir. Şekil 2.5 kuantum ışınlama için bir örnektir. Bu örnekte $|\psi\rangle = a|0\rangle + b|1\rangle$ kuantum halinin, kuantum kanalındaki süreci gösterilmektedir.



Şekil 2.5 Kuantum ışınlama örneği

$|\psi\rangle = a|0\rangle + b|1\rangle$ hali kanala girerken iki yardımcı kubitle (ancilla) tensör çarpılarak

$$|\psi_0\rangle = (a|0\rangle + b|1\rangle)|0\rangle|0\rangle = a|000\rangle + b|100\rangle$$

hali elde edilir. Kuantum devresi konusundaki bilgiler ışığı altında, $|\psi_0\rangle, |\psi_2\rangle, |\psi_3\rangle$ ve $|\psi_4\rangle$ halleri sırası ile aşağıdaki gibi hesaplanır:

$|\psi_1\rangle$ için ikinci kubit Hadamard kapısından geçirilir. Bu durumda;

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(a|0\rangle + b|1\rangle)(|0\rangle + |1\rangle)|0\rangle$$

$$= \frac{1}{\sqrt{2}}(a|000\rangle + b|100\rangle + a|010\rangle + b|110\rangle)$$

olur. $|\psi_2\rangle$ için son iki kubite $CNOT$ uygulanır. Bu durumda;

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}\left(a|000\rangle + b|100\rangle + a|011\rangle + b|111\rangle\right)$$

olur. $|\psi_3\rangle$ için ilk iki kubite $CNOT$ uygulanır. Bu durumda;

$$|\psi_3\rangle = \frac{1}{\sqrt{2}}\left(a|000\rangle + b|110\rangle + a|011\rangle + b|101\rangle\right)$$

ve son olarak $|\psi_4\rangle$ için birinci kubite H uygulanır. Bu durumda da

$$|\psi_4\rangle = \frac{1}{2}\left(a|000\rangle + a|100\rangle + b|010\rangle - b|110\rangle + a|011\rangle + a|111\rangle + b|001\rangle - b|101\rangle\right)$$

$$= \frac{1}{2}\left[|00\rangle\left(a|0\rangle + b|1\rangle\right) + |01\rangle\left(b|0\rangle + a|1\rangle\right) + |10\rangle\left(a|0\rangle - b|1\rangle\right) + |11\rangle\left(a|1\rangle - b|0\rangle\right)\right]$$

olur. M_1 ölçümü faz hatasının tespit edilmesini, M_2 ölçümü ise bit değişimi hatasının tespit edilmesini sağlar. Buna göre M_1 ölçümü aşağıdaki gibi hesaplanır:

$$\frac{M_1|\psi_4\rangle}{\sqrt{\langle\psi_4|M_1|\psi_4\rangle}} = |10\rangle(a|0\rangle - b|1\rangle).$$

Burada $M_1 = M_{10} = |100\rangle\langle 100| + |101\rangle\langle 101|$'dir. Son olarak $|10\rangle(a|0\rangle - b|1\rangle)$ haline Z kapısı uygulanırsa

$$|10\rangle Z(a|0\rangle - b|1\rangle) = |10\rangle\underbrace{(a|0\rangle + b|1\rangle)}_{|\psi\rangle}$$

elde edilir. Tablo 2.2'de ölçümlerin sonuçları ve oluşan hatayı düzeltmek için uygulanacak işlem gösterilmiştir.

Tablo 2.2 Ölçüm sonuçları ve mantık kapıları

Ölçüm türü	Ölçüm	Kuantum mantık kapısı
$M_0 = M_{00}$	$\|00\rangle(a\|0\rangle + b\|1\rangle)$	I birim operator
$M_1 = M_{10}$	$\|10\rangle(a\|0\rangle - b\|1\rangle)$	*Pauli Z*
$M_2 = M_{01}$	$\|01\rangle(a\|1\rangle + b\|0\rangle)$	*Pauli X*
$M_3 = M_{11}$	$\|11\rangle(a\|1\rangle - b\|0\rangle)$	*Pauli* $Y = ZX$

Böylece hata düzeltebilen kuantum kodlara başlamak için gerekli alt yapı oluşturulmuştur.

2.8. Hata Düzeltebilen Kuantum Kodlar

Kuantum hallerini kuantum kanalında hatalara karşı korumak amacı ile "hata düzeltebilen kuantum kodlar" geliştirilmiştir.

En genel olarak kuantum kod "sonlu boyutlu bir Hilbert uzayın alt uzayı" olarak tanımlanır.

Klasik kodlar ile kuantum kodlar arasında bazı önemli farklar vardır. Bu farklılıklar şunlardır:

1. Kopyalanamama *(No-Cloning)*: Klasik kodlamada kullanılan yöntemlerden biri de kopyalanarak üretilen tekrarlı kodlardır. Bir kuantum halinin kopyalanması "Kopyalanamama teoremi"ne (The No-cloning Theorem) göre imkânsızdır.

2. Hataların sürekliliği: Bir kubite farklı hataların bir dizisi etki edebilir.

3. Ölçüm kuantum bilgisini yıkar: Klasik kodlamada kanaldan çıkan veri gözlemlenir ve düzeltmek için nasıl bir dekodlama tekniği uygulayacağına karar verilir. Fakat kuantum mekanikte gözlem kuantum halinin "gözlem altında" bozulmasına neden olabilir. Bu durumda orijinal hali elde etmek imkânsız olur [35]. Dolanıklık bunun için ideal bir örnektir.

Bu problemlerin hepsi düşünüldüğünde kuantum kod yapmak imkânsızmış gibi görünebilir. Fakat bu imkânsız değildir. Klasik kodlamanın tersine kuantum kanalında kodsöze etki eden hata çok küçük olabilir ya da içinden çıkılması çok zor bir durum da (dolanıklık gibi) ortaya çıkabilir. Buna rağmen kuantum kodlamada uygulanan yöntem çok iyi çalışır. Hataların bir dizisinin bir kubitte olması durumunda hatayı düzeltmek için bu hataların bir ayrık alt kümesini düzeltmek yeterlidir. Böylece diğer bütün hatalar kendiliğinden düzelmiş olur. Bu hataların ayrıştırılması hata düzeltebilen kuantum kodlarının çalışma prensibini gösterir. Klasik sistemde hatalar böyle ayrıştırılamaz.

Teorem 2.8.1. (Kopyalanamama) Keyfi bir kuantum hali kopyalanamaz [24, 35].

İspat. Bir U operatörü keyfi kuantum hallerini kopyalasın. Keyfi kuantum halleri olarak $|\psi\rangle$ ve $|\phi\rangle$ alınırsa,

$$U\left(|\psi\rangle|K\rangle\right)=|\psi\rangle|\psi\rangle,$$

$$U\left(|\phi\rangle|K\rangle\right)=|\phi\rangle|\phi\rangle$$

olur. Bu eşitliğin iç çarpımından

$$\langle K|\langle\phi|U^{\dagger}U|\psi\rangle|K\rangle=\left(\langle\phi|\psi\rangle\right)^2\Rightarrow\langle\phi|\psi\rangle=\left(\langle\phi|\psi\rangle\right)^2$$

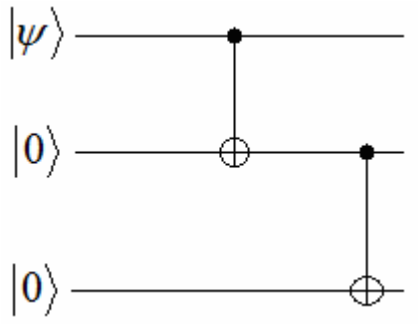
elde edilir. Buradan ya $|\phi\rangle$'nin $|\psi\rangle$'ye eşit ya da $|\phi\rangle$ ile $|\psi\rangle$'nin ortogonal olduğu görülür. O halde keyfi bir kuantum hali kopyalanamaz. ■

Tanım 2.8.1. Bit değişimi kanalı $|0\rangle$ kuantum halini $|1\rangle$ kuantum haline ve $|1\rangle$ kuantum halini de $|0\rangle$ kuantum haline çeviren kanaldır. Bu bir bit değişim hatası örneğidir [35].

Tanım 2.8.2. Faz değişimi kanalı $|0\rangle$ kuantum halini $|0\rangle$ kuantum haline ve $|1\rangle$ kuantum halini $-|1\rangle$ kuantum haline çeviren kanaldır. Bu tür hatalara faz değişimi hata denir [35].

Tanım 2.8.3. Hem bit değişimi hem faz değişimi aynı kubitte meydana gelebilir. Bu tür hatalara neden olan kanala bit ve faz değişimi kanalı denir [35].

Pauli sigma x operatörü ya da bit değişimi operatörü olarak bilinen X Pauli matrisinin kuantum kanalında $|\psi\rangle$ kuantum halinde yaptığı değişikliğe bit değişimi hata ve bu kanala da bit değişimi kanalı denir. Bu kanaldan gelen etkilere karşı $|\psi\rangle = a|0\rangle + b|1\rangle$ halinin nasıl korunabileceği şöyle gösterilebilir: $|\psi\rangle = a|0\rangle + b|1\rangle$ başlangıç hali Şekil 2.6'da görüldüğü gibi kodlansın.



Şekil 2.6 $|\psi\rangle = a|0\rangle + b|1\rangle$ halinin 3 kubite kodlanması

Buna göre $|\psi\rangle = a|0\rangle + b|1\rangle$ halinin kodlanmış hali $|\psi\rangle = a|000\rangle + b|111\rangle$ olur. Bu kodlanmış halde üç farklı hata meydana gelebilir.

i. Bit değişimi kanalından gelen etkiler sonucu oluşan bit değişimi hataları. Örneğin $|\psi\rangle = a|000\rangle + b|111\rangle$ haline XII operatörü etki ederse;

$$XII|\psi\rangle = a|100\rangle + b|011\rangle$$

olur. Bu bir bit değişimi hatası örneğidir.

ii. Faz değişimi kanalından gelen etkiler sonucu oluşan faz değişimi hataları. Örneğin $|\psi\rangle = a|000\rangle + b|111\rangle$ haline ZII operatörü etki ederse;

$$ZII|\psi\rangle = a|000\rangle - b|111\rangle$$

olur. Bu tür hatalara faz değişimi hatası denir. Faz değişimi hatası Pauli Z operatörünün etkisi ile meydana gelir.

iii. Hem faz hem de bit değişimi hatası aynı kubitte meydana gelebilir. Kuantum kanalında bu hataya $Y = ZX$ Pauli matrisi neden olur.

Aşağıdaki örneklerde sırası ile bit değişimi, faz değişimi ve hem bit değişimi hem de faz değişimi hata düzeltebilen kuantum kodlar ve dekodlama yöntemleri verilmektedir. Pauli matrislerinin tensör çarpımlarında, kolaylık amacı ile birim matrisler yazılmamaktadır. Bu durumda diğer matrislerin yerlerini belirtmek amacı ile indisler kullanılacaktır. Bu indisler matrisin bulunduğu yeri belirtir. Yani $XIIZ$ Pauli matrislerinin tensör çarpımı X_1Z_4 veya $ZIXIZIX$ tensör çarpımı $Z_1X_3Z_5X_7$ olarak gösterilebilir.

Örnek 2.8.1. (Bit değişimi hata düzeltebilen 3 kubitli kuantum kod) $|\psi\rangle = a|0\rangle + b|1\rangle$ kuantum hali Şekil 2.6'da gösterildiği gibi $|\psi\rangle = a|000\rangle + b|111\rangle$ şeklinde kodlanırsa bit değişimi hatalarını düzeltebilir. Bu bit değişimi hatalarına karşı faz operatörlerinden yararlanılır. $|\psi\rangle = a|000\rangle + b|111\rangle$ kuantum haline $ZZI = Z_1Z_2$ operatörünün yaptığı etki bu hali değiştirmez. Aynı şekilde Z_2Z_3 operatörünün etkisi de bu hali değiştirmez. Kuantum kanalında $|\psi\rangle = a|000\rangle + b|111\rangle$ halinin transferi sırasında X_1 operatörü bu hale etki ederse $|\psi'\rangle = X_1|\psi\rangle = a|100\rangle + b|011\rangle$ olur. Bu, ilk halde birinci kubitte bir bit değişimi hatası meydana geldiğini gösterir. Bunun anlaşılması ve düzeltilmesi için Z_1Z_2 ve Z_2Z_3 operatörlerinden yararlanılır. Bu operatörlerin ilk halde yaptığı etki bu hali değiştirmezken $|\psi'\rangle = a|100\rangle + b|011\rangle$ haline etkisi incelendiğinde

$$Z_1 Z_2 \left|\psi^{'}\right\rangle = -a\left|100\right\rangle - b\left|011\right\rangle = -\left(a\left|100\right\rangle + b\left|011\right\rangle\right)$$

$$Z_2 Z_3 \left|\psi^{'}\right\rangle = a\left|100\right\rangle + b\left|011\right\rangle = +\left(a\left|100\right\rangle + b\left|011\right\rangle\right)$$

olur. Bu da kanalda ilk halin bozulduğunu gösterir. Eğer bir bozulma olmasaydı bu operatörlerin etkisi altında $\left|\psi^{'}\right\rangle$ hali değişmezdi. Bu durumda hatanın hangi kubitte meydana geldiğinin tespiti ve dekodlama Tablo 2.3'de gösterildiği gibi yapılır.

Tablo 2.3 $\left|\psi\right\rangle = a\left|000\right\rangle + b\left|111\right\rangle$ halinde meydana gelebilecek bit değişimi hatalarının yerleri ve düzeltilmesi

$Z_1 Z_2$	$Z_2 Z_3$	Hatanın yeri	Düzeltme
+	+	Hatasız	I
−	+	1. kubit	X_1
−	−	2. kubit	X_2
+	−	3. kubit	X_3

Bir kuantum hali iz düşüm operatörleri kullanılarak da dekodlanabilir. Örnek 2.8.1 için iz düşüm operatörleri;

$$P_0 = \left|000\right\rangle\left\langle 000\right| + \left|111\right\rangle\left\langle 111\right|$$

$$P_1 = \left|100\right\rangle\left\langle 100\right| + \left|011\right\rangle\left\langle 011\right|$$

$$P_2 = \left|010\right\rangle\left\langle 010\right| + \left|101\right\rangle\left\langle 101\right|$$

$$P_3 = \left|001\right\rangle\left\langle 001\right| + \left|110\right\rangle\left\langle 110\right|$$

dir. Bu operatörlerle dekodlama şu şekilde yapılır: Kanaldan gelen kuantum hali $\left|\psi\right\rangle$ olsun. Hatanın yerini bulmak için $k = 0,1,2,3$ olmak üzere $\left\langle\psi\right|P_k\left|\psi\right\rangle$ çarpımına bakılır. Eğer $\left\langle\psi\right|P_k\left|\psi\right\rangle = 1$ ise k. kubitte hata olduğu anlaşılır. Örneğin kanaldan gelen hal $\left|\psi^{'}\right\rangle = a\left|100\right\rangle + b\left|011\right\rangle$ olsun. Bu durumda $\left\langle\psi^{'}\right|P_1\left|\psi^{'}\right\rangle = 1$ olup hatanın 1. kubitte olduğu anlaşılır. Bu tür kodlar için hatalar karakterize edilebilir. $\left|\psi\right\rangle$ haline

bir kanalda E hata operatörü etki etsin. Eğer $PEP = \lambda P$ olacak şekilde $\lambda \in \mathbb{C}$ varsa E hatası düzeltilebilir. Aksi halde düzeltilemez. Örneğin $|\psi\rangle$ haline kanalda $E = XII$ etki etsin. Bu durumda

$$P_1 XIIP_1 = \begin{pmatrix} 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0 \end{pmatrix} \begin{pmatrix} 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&1\\ 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0 \end{pmatrix} \begin{pmatrix} 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0 \end{pmatrix}$$

$$= \begin{pmatrix} 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0 \end{pmatrix} = 0.P_1$$

olur. Bu da hatanın düzeltilebilir olduğunu gösterir. Gelen hale ZII etki ederse

$$P_1 ZIIP_1 = \begin{pmatrix} 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0 \end{pmatrix} \begin{pmatrix} 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&-1&0&0&0\\ 0&0&0&0&0&-1&0&0\\ 0&0&0&0&0&0&-1&0\\ 0&0&0&0&0&0&0&-1 \end{pmatrix} \begin{pmatrix} 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0 \end{pmatrix}$$

$$= \begin{pmatrix} 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&-1&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0 \end{pmatrix} = |100\rangle\langle 100| - |011\rangle\langle 011| \neq \lambda P_k$$

elde edilir. Diğer iz düşüm operatörleri için de bu işlem yapıldığında bir λ sabitinin olmadığı görülür. O halde $|\psi\rangle = a|000\rangle + b|111\rangle$ kuantum kodu Z_1 hatasını düzeltemez.

Teorem 2.8.2. C bir kuantum kod ve P de bu kod üzerine bir iz düşüm operatörü olsun. $\{E_i\}$ kümesi bazı hataların kümesi olsun. C kodunun $\{E_i\}$ kümesindeki hataları tespit edebilmesi için gerek ve yeter şart

$$PE_i^{\dagger}E_jP = \lambda_{ij}P$$

olacak şekilde bir kompleks bileşenli λ_{ij} matrisinin olmasıdır [35].

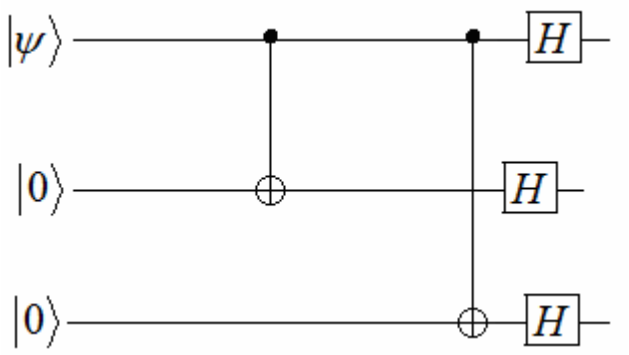
Örnek 2.8.2. (Faz değişimi hata düzeltebilen 3 kubitli kuantum kod) $|\psi\rangle = a|0\rangle + b|1\rangle$ kuantum hali Şekil 2.7'de gösterildiği gibi

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

şeklinde kodlanırsa faz değişimi hatalarını düzeltebilir. Eğer $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$ ve $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$ alınırsa kodlanmış hal

$$|\psi\rangle = a|+++\rangle + b|---\rangle$$

biçiminde yazılır.



Şekil 2.7 $|\psi\rangle = a|0\rangle + b|1\rangle$ halinin faz değişimi hatalara karşı kodlanması

Faz değişimi hatalarına karşı bit değişimi operatörlerinden yararlanılır. Kodlanmış $|\psi\rangle$ kuantum haline X_1X_2 operatörünün yaptığı etki bu hali değiştirmez. Aynı şekilde X_2X_3 operatörünün etkisi de bu hali değiştirmez. Kuantum kanalında kodlanmış $|\psi\rangle$ halinin transferi sırasında $ZII = Z_1$ operatörü bu hale etki ederse

$$|\psi'\rangle = ZII|\psi\rangle = a\frac{|000\rangle+|001\rangle+|010\rangle+|011\rangle-|100\rangle-|110\rangle-|101\rangle-|111\rangle}{2\sqrt{2}}$$

$$= b\frac{|000\rangle-|001\rangle-|010\rangle+|011\rangle+|100\rangle-|110\rangle-|101\rangle+|111\rangle}{2\sqrt{2}}$$

$$= a|-++\rangle + b|+--\rangle$$

olur. Kanaldan gelen bu $|\psi'\rangle$ hali eğer bozulmamış olsaydı X_1X_2 ve X_2X_3 operatörlerinin etkisi altında değişmezdi. Oysa X_1X_2 operatörünün etkisi altında bu hal

$$X_1X_2|\psi'\rangle = a\frac{-|000\rangle-|001\rangle-|010\rangle-|011\rangle+|100\rangle+|110\rangle+|101\rangle+|111\rangle}{2\sqrt{2}}$$

$$= b\frac{-|000\rangle+|001\rangle+|010\rangle-|011\rangle-|100\rangle+|110\rangle+|101\rangle-|111\rangle}{2\sqrt{2}}$$

$$= -a|-++\rangle - b|+--\rangle = -\left(a|-++\rangle + b|+--\rangle\right)$$

olur. Eğer $|\psi'\rangle$ hali bozulmamış olsaydı X_1X_2 operatörünün etkisi altında değişmezdi. Tablo 2.4'de hatanın hangi kubitte meydana geldiğinin tespiti ve dekodlama için yapılacak işlem gösterilmiştir.

Tablo 2.4 Faz hatalarına karşı kodlanmış $|\psi\rangle$ halinde meydana gelebilecek faz değişimi hatalarının yerleri ve düzeltilmesi

X_1X_2	X_2X_3	Hatanın yeri	Düzeltme
+	+	Hatasız	I
−	+	1. kubit	Z_1
−	−	2. kubit	Z_2
+	−	3. kubit	Z_3

Örnek 2.8.3. (Shor Kodu) Aşağıda verilen kod P. W. Shor tarafından tanımlanmıştır. Bu kod, bir kubit 9 kubite kodlanarak elde edilmiş ve bir kubitte oluşabilecek herhangi bir hatayı (hem bit hem de faz değişimi hatasını) düzeltebilen bir kuantum koddur. $|\psi\rangle = a|0\rangle + b|1\rangle$ kuantum hali Şekil 2.8'de görüldüğü gibi kodlanırsa;

$$a|0\rangle + b|1\rangle \to \frac{a}{2\sqrt{2}}\big(|000\rangle + |111\rangle\big)\big(|000\rangle + |111\rangle\big)\big(|000\rangle + |111\rangle\big)$$

$$+\frac{b}{2\sqrt{2}}\big(|000\rangle - |111\rangle\big)\big(|000\rangle - |111\rangle\big)\big(|000\rangle - |111\rangle\big)$$

olur. Daha açık olarak $a|0\rangle + b|1\rangle$ kuantum halinin kodlanmış hali

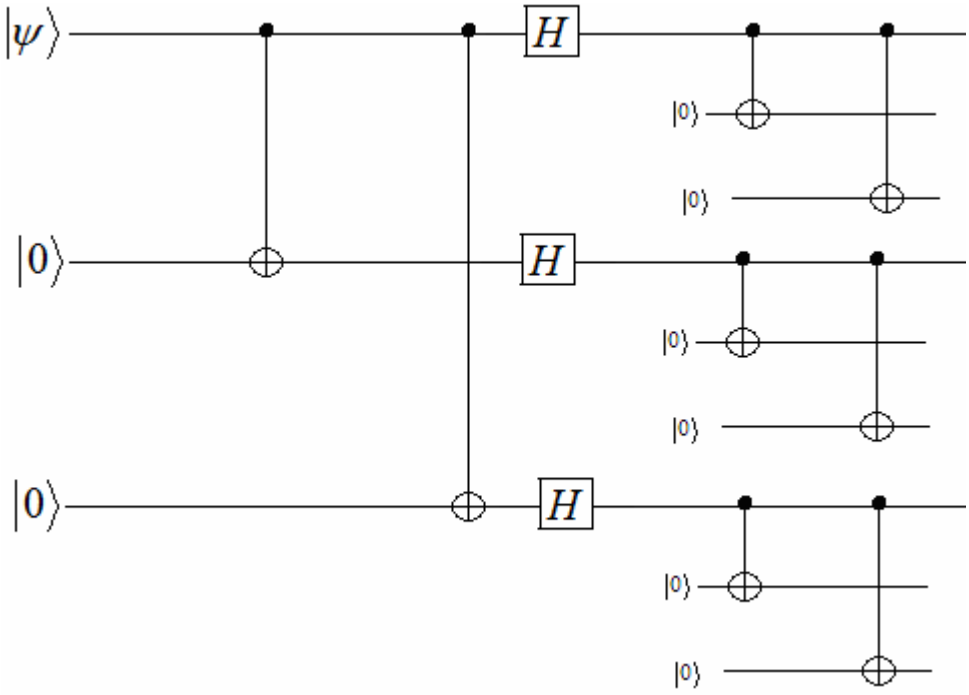
$$\frac{a}{2\sqrt{2}}\big(|000000000\rangle + |000000111\rangle + |000111000\rangle + |000111111\rangle$$

$$+|111000000\rangle + |111000111\rangle + |111111000\rangle + |111111111\rangle\big)$$

$$\frac{b}{2\sqrt{2}}\big(|000000000\rangle - |000000111\rangle - |000111000\rangle + |000111111\rangle$$

$$-|111000000\rangle + |111000111\rangle + |111111000\rangle - |111111111\rangle\big)$$

olur.



Şekil 2.8 Shor kodu: Bir kubitin 9 kubite kodlanması

Bu kuantum kodun bir kubitinde meydana gelebilecek bir faz hatası için $X_1X_2X_3X_4X_5X_6$ ve $X_4X_5X_6X_7X_8X_9$ operatörlerinden yararlanılır. Bu operatörlerin kodlanmış $|\psi\rangle$ haline etkisi bu halde bir hataya neden olmaz. Kodlanmış $|\psi\rangle$ haline kuantum kanalında Z_1 operatörü etki etsin. Bu etki sonucu bozulmuş hal aşağıdaki gibi olur.

$$|\psi'\rangle = \frac{a}{2\sqrt{2}}\left(|000000000\rangle + |000000111\rangle + |000111000\rangle + |000111111\rangle \right.$$

$$\left. - |111000000\rangle - |111000111\rangle - |111111000\rangle - |111111111\rangle\right)$$

$$\frac{b}{2\sqrt{2}}\left(|000000000\rangle - |000000111\rangle - |000111000\rangle + |000111111\rangle \right.$$

$$\left. + |111000000\rangle - |111000111\rangle - |111111000\rangle + |111111111\rangle\right).$$

Bu kanaldan gelen halde, bir hata oluşmasaydı $X_1X_2X_3X_4X_5X_6$ ve $X_4X_5X_6X_7X_8X_9$ operatörleri bu hale etki ettiğinde değişmezdi. Oysa kanaldan gelen bu hale $X_1X_2X_3X_4X_5X_6$ ve $X_4X_5X_6X_7X_8X_9$ operatörlerinin etkisi

$$X_1X_2X_3X_4X_5X_6\left|\psi'\right\rangle = \frac{a}{2\sqrt{2}}\left(\left|111111000\right\rangle + \left|111111111\right\rangle + \left|111000000\right\rangle + \left|111000111\right\rangle\right.$$

$$\left. - \left|000111000\right\rangle - \left|000111111\right\rangle - \left|000000000\right\rangle - \left|000000111\right\rangle\right)$$

$$\frac{b}{2\sqrt{2}}\left(\left|111111000\right\rangle - \left|111111111\right\rangle - \left|111000000\right\rangle + \left|111000111\right\rangle\right.$$

$$\left. + \left|000111000\right\rangle - \left|000111111\right\rangle - \left|000000000\right\rangle + \left|000000111\right\rangle\right)$$

$$= -\left|\psi'\right\rangle$$

olur. Bu, kuantum halinin kanaldan hatalı çıktığını gösterir. Aynı kubite farklı hatalar da etki edebilir. Örneğin birinci kubite Z_1X_1 operatörü etki ederse kodlanmış kuantum hali

$$\left|\psi'\right\rangle = \frac{a}{2\sqrt{2}}\left(-\left|100000000\right\rangle - \left|100000111\right\rangle - \left|100111000\right\rangle - \left|100111111\right\rangle\right.$$

$$\left. + \left|011000000\right\rangle + \left|011000111\right\rangle + \left|011111000\right\rangle + \left|011111111\right\rangle\right)$$

$$\frac{b}{2\sqrt{2}}\left(-\left|100000000\right\rangle + \left|100000111\right\rangle + \left|100111000\right\rangle - \left|100111111\right\rangle\right.$$

$$\left. - \left|011000000\right\rangle + \left|011000111\right\rangle + \left|011111000\right\rangle - \left|011111111\right\rangle\right)$$

biçiminde bozulur. Bu hataların yerlerinin tespiti ve düzeltilmesi için kodlanmış kuantum haline etki etmeyen operatörlerin bozuk hallere etkisi incelenir. Dekodlama için Örnek 2.8.1 ve Örnek 2.8.2'de gösterildiği gibi benzer bir tablo ile tüm hata durumları incelenir.

2.9. Calderbank-Shor-Steane Kodları

CSS kodları olarak bilinen bu tür kuantum kodlar Calderbank, Shor ve Steane tarafından bulunmuştur. Bu kuantum kodlar temelde iki klasik lineer kod yardımı ile oluşturulur.

Teorem 2.9.1. C_1 ve C_2 sırası ile $[n, k_1]$ ve $[n, k_2]$ parametreli iki klasik lineer kod ve $C_2 \subset C_1$ olsun. Eğer C_1 ile $C_2^{\perp}$ klasik kodlarının minimum mesafesi d ise bu kodlar yardımı ile $t = \lfloor (d-1)/2 \rfloor$ hata düzeltebilen $[[n, k_1 - k_2, d]]$ parametrelerine sahip bir kuantum kod vardır [10, 35].

Teorem 2.9.1 kullanılarak elde edilen kuantum kodlara CSS kodları denir.

Tanım 2.9.1. C_1 ve C_2 sırası ile $[n, k_1]$ ve $[n, k_2]$ parametreli iki klasik lineer kod ve $C_2 \subset C_1$ olsun. C_1 ile $C_2^{\perp}$ klasik kodlarının minimum mesafesi sırası ile d_1 ve d_2 olsun. Eğer $[[n, k_1 - k_2, d]]$ kuantum kodunun minimum mesafesi $d = \min\{d_1, d_2\}$ ise bu tür kuantum kodlara saf (pure), $d \neq \min\{d_1, d_2\}$ ise saf olmayan (impure) kuantum kod denir.

C_1 ve C_2 sırası ile $[n, k_1]$ ve $[n, k_2]$ parametreli iki klasik lineer kod, $C_2 \subset C_1$ ve C_1 ile $C_2^{\perp}$ klasik kodlarının minimum mesafesi d olsun. Bu durumda $[[n, k_1 - k_2, d]]$ CSS kuantum kodunun elemanları; $u \in C_1$ ve $v \in C_2$ olmak üzere $|u + C_2\rangle$ kuantum hali

$$|u + C_2\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{v \in C_2} |u + v\rangle$$

ile tanımlanır. $u_1, u_2 \in C_1$ olmak üzere eğer $u_1 - u_2 \in C_2$ ise $|u_1 + C_2\rangle = |u_2 + C_2\rangle$ olur. Bu durumda tüm farklı $|u + C_2\rangle$ kuantum halleri için C_1/C_2 'nin temsilcilerinin incelenmesi yeterlidir. Bu durumda CSS kuantum kodun kodsözlerinin sayısı

$|C_1|/|C_2| = 2^{k_1-k_2}$ dir. $[[n, k_1-k_2, d]]$ CSS kuantum kodu bit değişimi ve faz değişimi hatalarını düzeltirken sırasıyla C_1 ve $C_2^{\perp}$ klasik kodlarının hata düzeltmesinden yararlanır.

$$|u+C_2\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{v \in C_2} |u+v\rangle \tag{2.1}$$

kuantum halinde bir kubitte e_1 bit değişimi hatası ve e_2 faz değişimi hatası oluşursa (2.1) durumu

$$\frac{1}{\sqrt{|C_2|}} \sum_{v \in C_2} (-1)^{(u+v)e_2} |u+v+e_1\rangle \tag{2.2}$$

biçiminde bozulur. $u+v \in C_1$ olduğundan C_1 kodunun kontrol matrisi ile $u+v$ vektörünün transpozu çarpımının sonucu 0 olur. Bu bilgi ışığında H_1 matrisi C_1 klasik kodunun kontrol matrisi olmak üzere, başlangıçta $|H_1(u+v)^{tr}\rangle = |0\rangle$ halindeki yardımcı kubit yardımı ile bit değişimi hatanın meydana geldiği yer bulunabilir. Buradan da görüleceği gibi bir CSS kuantum kodun bit değişimi hatasını düzeltme kabiliyeti C_1 klasik koduna bağlıdır. $|H_1(u+v+e_1)^{tr}\rangle = |H_1 e_1^{tr}\rangle$ olup $|H_1 e_1^{tr}\rangle$ yardımcı kubiti hatanın yerinin ve değerinin bulunmasını sağlar. Dekodlama ise yeri bulunan kubite *NOT* mantık kapısının uygulanması ile kolayca yapılır. Böylece (2.2) bozulmuş kuantum hali

$$\frac{1}{\sqrt{|C_2|}} \sum_{v \in C_2} (-1)^{(u+v)e_2} |u+v\rangle \tag{2.3}$$

haline dönüşür. Faz değişimi hatasını düzeltmek için ise $C_2^{\perp}$ klasik kodunun hata düzeltme kabiliyetinden yararlanılır. Faz değişimi hatasını tespit etmek için her kubite Hadamard mantık kapısı uygulanır. Bu durumda (2.3) bozuk kuantum hali

$$\frac{1}{\sqrt{|C_2|2^n}}\sum_{z}\sum_{v\in C_2}(-1)^{(u+v)(z+e_2)}\left|z\right\rangle \tag{2.4}$$

olur. $z=z_1+e_2\ (\mathrm{mod}\ 2)$ alınırsa (2.4) hali

$$\frac{1}{\sqrt{|C_2|2^n}}\sum_{z_1}\sum_{v\in C_2}(-1)^{(u+v)(z_1)}\left|z_1+e_2\right\rangle \tag{2.5}$$

olur. $z_1\in C_2^{\perp}$ iken $\sum_{v\in C_2}(-1)^{vz_1}=|C_2|$ ve $z_1\notin C_2^{\perp}$ iken $\sum_{v\in C_2}(-1)^{vz_1}=0$ olduğundan (2.5) hali

$$\frac{1}{\sqrt{2^n/|C_2|}}\sum_{z_1\in C_2^{\perp}}(-1)^{uz_1}\left|z_1+e_2\right\rangle \tag{2.6}$$

şeklini alır. Bu aşamadan sonra e_2 hatasının yerinin tespiti tıpkı yukarıda e_1 hatasının yerinin tespiti gibi yapılır. Ancak burada artık $C_2^{\perp}$ klasik lineer kodunun hata tespit edebilme özelliği kullanılır. $C_2^{\perp}$ klasik kodunun kontrol matrisi H_2 ise $H_2(e_2)^{tr}$ faz değişimi hatasının yerini verecektir. e_2 bit değişimi hatası düzeltildiği zaman (2.6) hali

$$\frac{1}{\sqrt{2^n/|C_2|}}\sum_{z_1\in C_2^{\perp}}(-1)^{uz_1}\left|z_1\right\rangle$$

olur. Böylece kanala giren kuantum halini elde etmek için geri kalan son işlem her kubite tekrar Hadamard kapısının uygulanmasıdır [10, 35].

Örnek 2.9.1. Örnek 2.8.1'de verilen bir bit değişimi hatası düzeltebilen kuantum kod için C_1 ve C_2 klasik kodları

$$C_1=C_2=\{(000),(111)\}$$

seçilirse kuantum kod

$$\frac{1}{\sqrt{2}}\left(|000\rangle+|111\rangle\right)$$

olur. Bu kuantum kod bir bit değişimi hata düzeltebilir. Çünkü C_1 klasik kodunun minimum mesafesi üçtür. Ancak faz değişimi hata düzeltemez. Çünkü $C_2^{\perp}$ klasik kodunun minimum mesafesi birdir. Örnek 2.8.1'de de bu kodun yalnız bit değişimi hata düzeltebileceği gösterilmiştir.

2.10. Stabilizer Kodlar

Stabilizer kuantum kodlar kuantum kodların çok önemli bir sınıfıdır. Klasik lineer kodların klasik kodlardaki önemi gibi düşünülebilir. Bazen Stabilizer kuantum kod yerine toplamsal kod da denilmektedir. Stabilizer kuantum kodlar için önce stabilizer formülasyon açıklanmalıdır. Temelde grup teoriye dayanan bu formülasyon bir örnekle şu şekilde özetlenebilir. $|\psi\rangle=\frac{1}{\sqrt{2}}\left(|000\rangle+|111\rangle\right)$ kuantum haline etki ettiği halde değiştirmeyen mantık kapılarından bazıları ZZI, IZZ veya III'dır. Gerçekten $ZZI|\psi\rangle=|\psi\rangle, IZZ|\psi\rangle=|\psi\rangle, III|\psi\rangle=|\psi\rangle$ olur. $|\psi\rangle$ halini değiştirmeyen bu tür mantık kapılarının hepsinin düşünülmesi stabilizer kuantum kodların doğmasına sebep olmuştur. $|\psi\rangle$ halini etkilemeyen mantık kapılarının tümünün oluşturduğu küme bir grup olur. Bu değişmeli grubun üreteçlerinin bazıları kullanılarak stabilizer kuantum kodun stabilizerinin üreteçleri elde edilir [35].

Tanım 2.10.1. $G_1=\{\pm I,\pm iI,\pm X,\pm iX,\pm Z,\pm iZ,\pm Y,\pm iY\}$ kümesine 1 kubit üzerinde tanımlanmış Pauli matris grubu denir. Bu küme matrisler arası çarpma işlemine göre değişmeli olmayan bir gruptur. n kubit üzerine tanımlanmış G_n Pauli matris grubu ise Pauli matrislerinin $n-$defa tensör çarpılmış hallerinin tümünün oluşturduğu küme olarak tanımlanır [35].

Tanım 2.10.2. $S \subset G_n$ olmak üzere stabilizer kuantum kod $C(S)$ ile gösterilir ve

$$C(S) = \{|\psi\rangle : M|\psi\rangle = |\psi\rangle, \forall M \in S\}$$

şeklinde tanımlanır. S kümesine stabilizer kuantum kodun stabilizeri denir. S kümesi, n kubitli Pauli matris grubunun değişmeli alt grubu olmalıdır [47].

Örnek 2.10.1. Stabilizer kuantum kodun stabilizerinin üreteçleri ZZI ve IZZ olan kuantum kodun stabilizeri ve bu stabilizer ile oluşturulan kuantum kod sırası ile

$$S = \langle ZZI, IZZ \rangle = \{III, ZZI, ZIZ, IZZ\},$$

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

dir. Stabilizer kuantum kod, stabilizerin her elemanının etki etmediği kuantum hallerinin oluşturduğu kümelerin kesişimi olarak da tanımlanabilir. Bu örnek için III, ZZI, ZIZ ve IZZ 'nin etkisi altında değişmeyen kuantum hallerinin oluşturduğu kümeler sırası ile

$III \rightarrow$ 3 kubitli tüm haller,
$ZZI \rightarrow \{|000\rangle, |001\rangle, |110\rangle, |111\rangle\}$,

$IZZ \rightarrow \{|000\rangle, |100\rangle, |011\rangle, |111\rangle\}$,

$ZIZ \rightarrow \{|000\rangle, |010\rangle, |101\rangle, |111\rangle\}$

olup kuantum kod

$$C(S) = \{|000\rangle, |111\rangle, a|000\rangle + b|111\rangle : |a|^2 + |b|^2 = 1\}$$

olarak elde edilir.

Stabilizerin bazı özellikleri vardır. Bu özellikler şu şekilde sıralanabilir:

i. $-I, \mp iI \notin S$ olmalıdır. Aksi halde, örneğin $-I \in S$ olsaydı $-I|\psi\rangle = |\psi\rangle$ olacağından, $|\psi\rangle = 0$ olurdu.

ii. S stabilizer kümesi değişmeli gruptur. Değişmeli olmasaydı bu durumda; $A, B \in S$ için $A|\psi\rangle = B|\psi\rangle = |\psi\rangle$ olduğundan $|\psi\rangle = AB|\psi\rangle = -BA|\psi\rangle = -|\psi\rangle$ olup $|\psi\rangle = 0$ olurdu. Pauli matrisleri için $AB \neq BA$ ise $AB = -BA$ ($\mathbb{Z}_2$ üzerindeki Pauli matrisleri için) olur.

iii. Eğer bir stabilizer yukarıdaki şartları sağlıyorsa bu stabilizerden yararlanarak stabilizer kuantum kod yazılır. Eğer bu hallerden birini sağlamıyorsa yazılabilecek n kubitli kuantum kod $|0\rangle^{\otimes n}$ olur [35].

Örnek 2.10.2. Her CSS kuantum kod bir stabilizer kuantum koddur.

Örnek 2.10.3. $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$ stabilizer kuantum kodunun stabilizeri

$$S = \{II, XI, IZ, XZ\} = \langle XI, IZ \rangle$$

dir. $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$ haline $CNOT$ etki ederse;

$$CNOT\left|\psi\right\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \frac{1}{\sqrt{2}}\left(|00\rangle+|10\rangle\right) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

$$= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \left(\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right) = \frac{1}{\sqrt{2}}\left(|00\rangle+|11\rangle\right)$$

elde edilir. Bu durumda bu yeni halin stabilizeri

$$S' = \left\langle CNOT\left(XI\right)(CNOT)^{\dagger}, CNOT\left(IZ\right)(CNOT)^{\dagger} \right\rangle$$

$$= \left\langle XX, ZZ \right\rangle = \left\{ II, XX, ZZ, -YY \right\}$$

olur. Orijinal kuantum halinin stabilizerinin üreteçleri XI, IZ iken bozuk halin stabilizerinin üreteçleri XX, ZZ 'dir. Orijinal hali elde etmek için bu bozuk hale $CNOT$ uygulamak yeterlidir.

Stabilizer formülasyon ile grup teori arasındaki ilişki genelleştirilebilir. S, G_n Pauli matris grubunun bir alt grubu olsun. S 'nin her elemanının etkisi altında değişmeyen kuantum hallerinden oluşan küme V_s olsun. S stabilizeri sonlu bir gruptur ve S 'nin elemanlarından bazıları bu grubu üretir. (Örnek olarak Örnek 2.10.1'de S 'nin üreteçleri gösterilmiştir). S 'nin üreteçleri $g_1, g_2, \ldots, g_l$ ise $S = \left\langle g_1, g_2, \ldots, g_l \right\rangle$ olur. S kümesinin G_n Pauli matris grubunun bir değişmeli alt grubu olması grup teorinin bilinen kurallarının kuantum kodlarına uygulanmasını ve hataların sınıflandırılmasını sağlar. Bu durumda stabilizer kuantum kodun alternatif bir tanımı yapılır. Bu tanıma geçmeden önce son olarak aşağıdaki bilgi ilerideki konular için gerekli olacaktır.

Stabilizer kuantum kodların önemli bir özelliği de dekodlamasıdır. Kanaldan gelen kuantum halinin bozulmasına neden olan mantık kapısı aynı zamanda orijinal halin

stabilizerinin üretecine etki edip son halin stabilizerinin üretecini oluşturur. Böylece kodsözlerdeki hataları aramak yerine sadece stabilizerin üretecine etki eden mantık kapısı aranır. $S=\langle g_1,g_2,\ldots,g_l\rangle$ stabilizer kümesi ve S kümesinin yardımı ile oluşturulan vektör uzayı da V_s olsun. Bu durumda V_s'nin elemanlarına S'nin elemanları etki etmez. Yani $\forall|\psi\rangle\in V_s$ ve $\forall g\in S$ için $g|\psi\rangle=|\psi\rangle$ olur. Bu $|\psi\rangle$ kuantum haline kuantum kanalında bir üniter U mantık kapısı etki etsin. Bu durumda $\forall g\in S$ için;

$$U|\psi\rangle=Ug|\psi\rangle=UgU^{\dagger}U|\psi\rangle$$

olacağında $U|\psi\rangle$ bozuk kuantum halinin stabilizeri de

$$S'=\left\{UgU^{\dagger}:g\in S\right\}$$

olur. Eğer S'nin üreteçleri $g_1,g_2,\ldots,g_l$ ise S''nün üreteçleri de $Ug_1U^{\dagger},Ug_2U^{\dagger},\ldots,Ug_lU^{\dagger}$ dir. Örnek 2.10.3'de de denildiği gibi dekodlama için sadece stabilizerin üretecine etki eden üniter mantık kapısını bulmak hatayı düzeltebilmek için yeterli olacaktır [35].

Tanım 2.10.3. $S\subset G_n$ ve $-I\notin S$ olmak üzere S'nin $n-k$ tane bağımsız ve değişmeli üreteci olsun. S'den yararlanılarak elde edilen V_s vektör uzayı bir $[[n,k]]$ parametreli kuantum stabilizer kod olarak tanımlanır ve $C(S)$ ile gösterilir [35].

Hataların sınıflandırılması şu şekilde yapılabilir: $|\psi\rangle\in V_s$ haline $E\in G_n$ etki etsin.

i. Eğer E ile S'nin bir elemanı değişmeli değilse bu durumda E operatörü $C(S)$ kuantum kodunu bir ortonormal altuzaya taşır. Hata, uygun bir ölçüm uygulanarak tespit edilebilir.

ii. Eğer $E \in S$ ise bu durumda E üniter hata operatörü $C(S)$ kuantum koduna etki etmez.

iii. Asıl işi zorlaştıran durum $E \notin S$ iken E'nin S'nin elemanları ile değişmeli olmasıdır. Bu tür hataların kümesi

$$\{E \in G_n : \forall g \in S, Eg = gE\}$$

biçiminde tanımlanır. Aslında bu küme S'nin merkezleştiricisidir ve $M(S)$ ile gösterilir. S'nin merkezleştiricisi ile çok benzer bir grup daha vardır. Bu grup S'nin normalleştiricisidir. S'nin normalleştiricisi

$$N(S) = \{E \in G_n : ES = SE\}$$

olarak tanımlanır. Eğer $-I \notin S$ ise $N(S) = M(S)$ olur [35].
Aşağıdaki teorem hataların sınıflandırılması için oldukça önemlidir.

Teorem 2.10.1. $C(S)$ kuantum kodunun stabilizer S olsun. Bu durumda

$$\{E_k \in G_n : \forall k,l, E_k^\dagger E_l \notin N(S) - S\}$$

kümesi $C(S)$ kuantum kodunun düzeltebileceği hatalardır [35].

Örnek 2.10.4. $S = \{II, -II, XI, -XI\}$ olarak alınırsa $S \subset M(S) \subset N(S) \subset G_2$ olur. Örneğin $XX \notin S$ iken $XX \in M(S)$, $XX \in N(S)$ ve $ZI \notin M(S)$ iken $ZI \in N(S)$'dir. Eğer $-II$ elemanı S stabilizer kümesinden çıkarılırsa $S = \{II, XI\}$ olur. Bu durumda $S \subset M(S) = N(S)$ olur.

Örnek 2.10.5.

$$S = \langle XZZXI, IXZZX, XIXZZ, ZXIXZ \rangle$$
$$= \{IIIII, XZZXI, IXZZX, XIXZZ, ZXIXZ, XYIYX, IZYYZ, YYZIZ,$$
$$XXYIY, ZIZYY, YXXYI, IYXXY, YZIZY, ZYYZI, YIYXX, ZZXIX\}$$

stabilizerine sahip $C(S)$ kuantum kodunun kodsözleri

$$|0_L\rangle = IIIII|00000\rangle + XZZXI|00000\rangle + IXZZX|00000\rangle + XIXZZ|00000\rangle$$
$$+ZXIXZ|00000\rangle + XYIYX|00000\rangle + IZYYZ|00000\rangle + YYZIZ|00000\rangle$$
$$+XXYIY|00000\rangle + ZIZYY|00000\rangle + YXXYI|00000\rangle + IYXXY|00000\rangle$$
$$+YZIZY|00000\rangle + ZYYZI|00000\rangle + YIYXX|00000\rangle + ZZXIX|00000\rangle$$
$$= |00000\rangle + |10010\rangle + |01001\rangle + |10100\rangle$$
$$+|01010\rangle - |11011\rangle - |00110\rangle - |11000\rangle$$
$$-|11101\rangle - |00011\rangle - |11110\rangle - |01111\rangle$$
$$-|10001\rangle - |01100\rangle - |10111\rangle + |00101\rangle$$

ve

$$|1_L\rangle = XXXXX|0_L\rangle = |11111\rangle + |01101\rangle + |10110\rangle + |01011\rangle$$
$$+|10101\rangle - |00100\rangle - |11001\rangle - |00111\rangle$$
$$-|00010\rangle - |11100\rangle - |00001\rangle - |10000\rangle$$
$$-|01110\rangle - |10011\rangle - |01000\rangle + |11010\rangle$$

olur. $|0_L\rangle$ ve $|1_L\rangle$ 'ye kuantum kodun mantıksal bazları denir.

2.11. Stabilizer Kodun Kontrol Matrisi

n kubitli kuantum kodun stabilizeri $S=\langle g_1, g_2, \ldots, g_l \rangle$ olsun. Bu kod için üreteç matrisi $l \times 2n$ formundadır ve bu matrisin sol tarafı stabilizerdeki Pauli matrislerine göre ya 0 ya da 1 değerini alır. Matrisin sol tarafı I ve Z matrislerine karşılık 0, X ve Y matrislerine karşılık 1 değerini alır. Matrisin sağ tarafı ise I ve X matrislerine karşılık 0, Z ve Y matrislerine karşılık 1 değerini alır [35].

Örnek 2.11.1. 7 kubitli Steane kodunun stabilizerinin üreteçleri Tablo 2.5'de gösterilmiştir.

Tablo 2.5 7 kubitli Steane kodunun stabilizerinin üreteçleri

Üreteçler	Operatorler
g_1	*IIIXXXX*
g_2	*IXXIIXX*
g_3	*XIXIXIX*
g_4	*IIIZZZZ*
g_5	*IZZIIZZ*
g_6	*ZIZIZIZ*

Bu kod için kontrol matrisi

$$\left[\begin{array}{ccccccc|ccccccc} 0&0&0&1&1&1&1&0&0&0&0&0&0&0 \\ 0&1&1&0&0&1&1&0&0&0&0&0&0&0 \\ 1&0&1&0&1&0&1&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&1&1&1&1 \\ 0&0&0&0&0&0&0&0&1&1&0&0&1&1 \\ 0&0&0&0&0&0&0&1&0&1&0&1&0&1 \end{array}\right]$$

olur. Genel olarak $[[n,k]]$ parametreli C kuantum kodunun kontrol matrisi $G=[G_1|G_2]$ şeklinde ise r, G_1'in rankı olmak üzere

$$\begin{matrix} r & \{ \\ n-k-r & \{ \end{matrix} \left[\begin{array}{cc|cc} \overbrace{I}^{r} & \overbrace{A}^{n-r} & \overbrace{B}^{r} & \overbrace{C}^{n-r} \\ 0 & 0 & D & E \end{array}\right]$$

olur. E için Gauss eleme metodu uygulanırsa

$$\begin{matrix} r & \{ \\ n-k-r-s & \{ \\ s & \{ \end{matrix} \left[\begin{array}{ccc|ccc} I & A_1 & A_2 & B & C_1 & C_2 \\ 0 & 0 & 0 & D_1 & I & E_2 \\ 0 & 0 & 0 & D_2 & 0 & 0 \end{array}\right]$$

elde edilir. Örnek 2.11.1 için $s=0$ alınırsa standart form matrisi

$$\begin{matrix} r \to \\ \hline n-k-r \to \end{matrix} \left\{\left[\begin{array}{ccc|ccc} \overbrace{I}^{r} & \overbrace{A_1}^{n-k-r} & \overbrace{A_2}^{k} & \overbrace{B}^{r} & \overbrace{0}^{n-k-r} & \overbrace{C}^{k} \\ 0 & 0 & 0 & D & I & E \end{array}\right.\right.$$

olur. Kontrol matrisini, klasik kodlardan kuantum kod elde etmek için iyi bir geçiş sağlayan bu forma getirmek önemlidir. Yukarıdaki 7 kubitli Steane kodunun standart formu, önce 1. ve 4. kubitin yeri sonra 3. ve 4. kubitin yeri daha sonra 6. ve 7. kubitin yeri değiştirildikten sonra sırası ile 4. satıra 6. satır, 5. satıra 6. satır, 5. satıra 4. satır, 6. satıra 5. satır eklenerek

$$\left[\begin{array}{ccccccc|ccccccc} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \end{array}\right]$$

elde edilir. Bu standart şeklin önemi aşağıdaki gibi örneklenebilir. Bu standart formda $A_2 = (1 \quad 1 \quad 0)$'dır. Bu da $(0000000|1100001)$ kodlanmış haline karşılık gelir. Aslında esas form $\left[\underbrace{00\cdots0}_{n \text{ kubit}} \middle| A_2^T 0 I\right]$ şeklindedir. Bu durumda $(0000000|1100001)$ kodlamasına $ZZIIIIZ$ operatörü karşılık gelir. Fakat 1. ve 4. kubit, 3. ve 4. kubit, 6. ve 7. kubit yer değiştirdiğinden, bu işlemler geri uygulanırsa $IZIZIZI$ elde edilir. Z'nin kodlanmış hali $ZZZZZZZ$ olduğundan $(ZZZZZZZ)(IZIZIZI) = ZIZIZIZ$ olup, bu da stabilizerin üreteçlerinden g_6'yı verir.

Klasik kodlardan kuantum kod elde etmek şu şekilde de olabilir: $C_2 \subset C_1$ olmak üzere C_1 ve C_2 kodları sırası ile $[n, k_1]$ ve $[n, k_2]$ parametreli klasik lineer kod olsun ve hem C_1 hem de $C_2^{\perp}$ t hata düzeltsin. Bu durumda

$$\left[\begin{array}{c|c} H(C_2^{\perp}) & 0 \\ 0 & H(C_1) \end{array}\right]$$

kontrol matrisi kuantum kodun kontrol matrisidir ve bu matris klasik lineer kodlardan elde edilmiştir. Son olarak $H(C_2^{\perp})\left(H(C_1)\right)^{tr} = 0$ olup olmadığı kontrol edilir. $C_2 \subset C_1$ olduğundan

$$H(C_2^{\perp})\left(H(C_1)\right)^{tr} = \left[H\left(C_1\right)\left(G(C_2)\right)\right]^{tr} = 0$$

elde edilir [35].

Yukarıdaki 7 kubitli Steane kodu ele alınırsa, $C_2 \subset C_1$ olmak üzere C_1 yerine $C_2^{\perp}$ alınabilir. C_1 kodunun üreteç matrisi

$$G_1 = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

olup, $C_2 \subset C_1$, $C_2 = C_1^{\perp}$ ve $C_2^{\perp} = C_1$ olduğu görülür. Bu durumda 7 kubitli Steane kuantum kodunun kontrol matrisi

$$\left[\begin{array}{c|c} H(C_2^{\perp}) & 0 \\ 0 & H(C_1) \end{array}\right] = \left[\begin{array}{ccccccc|ccccccc} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \end{array}\right]$$

olur.

2.12. $GF(4)$ Üzerindeki Klasik Kodlar Yardımı İle Kuantum Kodlar Üretme

Bu konu başlığı altındaki asıl amaç; klasik lineer kodlarla $GF(4)$ üzerindeki kodlar arasında bir geçiş elde etmek ve kuantum kod bulma işini $GF(4)$ üzerindeki kodları araştırma işine çevirmeye çalışmak olacaktır.

n kubitli kuantum hal uzayı $\mathbb{C}^{2^n}$ alınabilir. Kuantum kod, k kubiti n kubite kodlama olarak düşünülebilir. Bu durum $\mathbb{C}^{2^k}$ hal uzayından $\mathbb{C}^{2^n}$ hal uzayının 2^k boyutlu bir alt uzayına bir lineer dönüşüm yapmaktır. Bu alt uzaya hata düzeltebilen kuantum kod denir. Bu temel fikirden yararlanarak aşağıdaki yöntem geliştirilmiştir.

$\overline{E}$, $2n$ boyutlu ikili vektör uzay olsun. Bu uzayın elemanları $(a|b)$ şeklindedir ve bu uzay üzerindeki iç çarpım

$$\left\langle \left(a|b\right),\left(a'|b'\right)\right\rangle = ab' + a'b$$

olarak tanımlanır. Ayrıca

$$\left\langle \left(a|b\right),\left(a|b\right)\right\rangle = ab + ab = 2ab \equiv 0 \pmod 2$$

olduğundan bu iç çarpım simpletiktir. Bu uzayın bir elemanının ağırlığı ise

$$\left(a|b\right) = \left(a_1 a_2 \cdots a_n | b_1 b_2 \cdots b_n\right)$$

olmak üzere

$$w\left(\left(a|b\right)\right) = \left|\left\{i : \left(a_i|b_i\right) \neq \left(0|0\right)\right\}\right|$$

şeklinde tanımlanır. Bu uzayın iki elemanı arasındaki mesafe de bu elemanların farkının ağırlığı olarak tanımlanır. Bu bilgiler ışığında aşağıdaki teorem yazılabilir [11].

Teorem 2.12.1. $\overline{S}$, $\overline{E}$'nin $\left(n-k\right)$ boyutlu lineer alt uzayı ve $\overline{S} \subset \overline{S}^{\perp}$ olsun. ($\overline{S}^{\perp}$ yukarıda tanımlanan iç çarpıma göre tanımlanır). $\overline{S}^{\perp} - \overline{S}$ kümesinde ağırlığı d den küçük vektör olmasın. Bu durumda k kubiti n kubite eşleyerek $\left[\left(d-1\right)/2\right]$ hata düzeltebilen bir kuantum kod elde edilir [11].

Bu kod $\overline{S}$'nin öz uzaylarından biridir. Bu teoremle elde edilen koda toplamsal (additive) kod da denir.

Örnek 2.12.1. $n = 4$ için $\left|\overline{E}\right| = 256$ olur.

$$\overline{S} = \left\{\left(0000|0000\right),\left(1110|1100\right),\left(1011|0011\right),\left(0101|1111\right)\right\}$$

olarak seçilirse $\overline{S} \subset \overline{S}^{\perp}$ olur. $d = 2$ olduğu kolayca görülebilir. Örneğin $(0011|0000) \in \overline{S}^{\perp}$'dir. Fakat $\overline{S}^{\perp}$'nin bir ağırlığına sahip elemanı yoktur. $\overline{S}^{\perp}$'nin öz uzaylarından biri $\{(0000),(1110),(1011),(0101)\}$ olarak alınırsa kuantum kod $i^2 = -1$ olmak üzere

$$|\psi\rangle = (i)^{(0000)(0000)}|0000\rangle + (i)^{(1110)(1100)}|1110\rangle$$
$$+ (i)^{(1011)(0011)}|1011\rangle + (i)^{(0101)(1111)}|0101\rangle$$
$$= |0000\rangle - |1110\rangle - |1011\rangle - |0101\rangle$$

olur. Bu yeni $2n$ boyutlu $\overline{E}$ ikili vektör uzayı ile $GF(4)^n$ yapısı arasında bir geçiş kurulur ve bu böylece $GF(4)^n$ üzerindeki kodlardan yararlanılarak kuantum kod elde edilir.

$GF(4) = \{0,1,\omega,\overline{\omega}\}$ ve $\omega^2 = \overline{\omega}, \omega^2 + \omega + 1 = 0, \omega^3 = 1$ dir. $x \in GF(4)$ elemanının eşleniği $\overline{x} = x^2$ ve iz fonksiyonu

$$Tr : GF(4) \to \mathbb{Z}_2$$
$$x \mapsto x + \overline{x}$$

olarak tanımlanır. Bir $u \in GF(4)^n$ vektörünün Hamming ağırlığı $wt(u)$ ile gösterilir ve bu vektörün ağırlığı vektördeki sıfır olmayan bileşenlerin sayısına eşittir. $u, u' \in GF(4)$ elemanları arasındaki mesafe $d(u,u') = w(u-u')$ ile tanımlanır.

$$\phi : \overline{E} \to GF(4)^n,\ \phi((a|b)) = \omega a + \overline{\omega} b \qquad (2.7)$$

bir ϕ fonksiyonu tanımlanırsa $\left(a|b\right)$ vektörünün ağırlığı $\phi\left(\left(a|b\right)\right) \in GF\left(4\right)^n$ elemanının ağırlığına eşit olur. Buradan $v=\left(a|b\right)$ ile $v'=\left(a'|b'\right)$ vektörleri arasındaki mesafe de $d\left(v,v'\right)$'ye eşit olur. Ayrıca v ile v' vektörleri arasındaki simpletik iç çarpım

$$Tr\left(\phi(v).\overline{\phi(v')}\right)=Tr\left[\left(\omega a+\overline{\omega}b\right)\left(\overline{\omega}a'+\omega b'\right)\right]$$

$$=ab'+a'b=Tr\left(\phi(v).\overline{\phi(v')}\right)$$

dir. Eğer $\overline{S}$, $\overline{E}$'nin bir lineer alt uzayı ise $C=\phi\left(\overline{S}\right)$ de $GF(4)^n$'nin toplamsal kapalı bir alt kümesidir. Bu C alt kümesine $GF(4)$ üzerinde bir toplamsal kod denir ve $\left(n,2^k\right)$ şeklinde gösterilir. Bu toplamsal kod 2^k vektör içerir. Eğer C aynı zamanda ω ile çarpım altında da kapalı ise C koduna lineer kod denir. C kodunun diki de

$$C^{\perp}=\left\{u\in GF(4)^n : u\bullet v=0,\ \forall v\in C\right\}$$

şeklinde tanımlanır. Burada

$$u\bullet v=Tr\left(u\overline{v}\right)=\sum_{j=1}^{n}\left(u_j\overline{v_j}+\overline{u_j}v_j\right) \tag{2.8}$$

dir. Eğer C, $\left(n,2^{n-k}\right)$ parametreli bir kod ise bu durumda $C^{\perp}$ de $\left(n,2^{n+k}\right)$ parametrelerine sahip bir kod olur. Eğer $C\subset C^{\perp}$ ise C'ye kendine ortogonal, $C=C^{\perp}$ ise C'ye kendine dik kod denir [11].

Örnek 2.12.2. Yukarıdaki Örnek 2.12.1'de $n=4$ için

$$\overline{S}=\{(0000|0000),(1110|1100),(1011|0011),(0101|1111)\}$$

idi. Buna karşılık $GF(4)^4$ üzerindeki toplamsal kod

$$\phi((0000|0000))=(0000),\ \phi((1110|1100))=(11\omega 0),$$

$$\phi((1011|0011))=(\omega 011),\ \phi((0101|1111))=(\overline{\omega}1\overline{\omega}1)$$

olduğundan $C=\{(0000),(11\omega 0),(\omega 011),(\overline{\omega}1\overline{\omega}1)\}$ olur. Gerçekten C kodunun ve $\overline{S}$'nin minimum mesafesi üçtür. Üstelik iç çarpımlarda korunmaktadır. Yani

$C^{\perp}=\phi(\overline{S}^{\perp})$ olur.

Bu bilgiler ışığında Teorem 2.12.1 yeniden düzenlenebilir.

Teorem 2.12.2. C kodu $GF(4)^n$ üzerinde kendine ortogonal bir toplamsal kodu olsun ve 2^{n-k} tane kodsöz içersin. Eğer $C^{\perp}-C$'de sıfır vektör hariç ağırlığı d'den küçük vektör yoksa, $\phi^{-1}(C)$'nin öz uzaylarından her birine bir $[[n,k,d]]$ hata düzeltebilen toplamsal kuantum kod denir [11].

Eğer $C^{\perp}$'de ağırlığı d'den küçük eleman yoksa (sıfır vektör hariç) C'ye saf (pure) aksi takdire saf olmayan (impure) denir.

Böylece kuantum kod bulma problemi $GF(4)$ üzerinde toplamsal kendine ortogonal ya da kendine dik kod bulma problemine dönüştürülür. Bu geçiş kullanılarak kodlar polinomlara aktarılıp daha zengin çalışmalar yapılabilir. Aşağıdaki teorem

$GF(4)$'den katsayılı polinomdan yararlanarak toplamsal ortogonal klasik kod elde etme şartlarını vermektedir.

Teorem 2.12.3. *i*. Bir $\left(n, 2^k\right)$ parametreli toplamsal devirli C kodunu $p(x), q(x), r(x) \in \mathbb{Z}_2[x]$ olmak üzere $\omega p(x) + q(x)$ ve $r(x)$ şeklinde iki polinom üretir. Burada $p(x)$ ve $q(x)$ polinomları "$x^n - 1$" polinomunu, $r(x)$ polinomu da $\left(q(x)\left(x^n - 1\right)\right) / p(x)$ polinomunu böler ve $k = 2n - der(p) - der(q)$ olur. Bu durumda $C = \langle \omega p(x) + q(x), r(x) \rangle$ şeklinde gösterilir.

ii. C kodunun kendine ortogonal olması için gerek ve yeter şart

$$p(x)r(x^{n-1}) \equiv p(x^{n-1})r(x) \equiv 0 \mod(x^n - 1),$$

$$p(x)q(x^{n-1}) \equiv p(x^{n-1})q(x) \mod(x^n - 1)$$

olmasıdır [11].

Örnek 2.12.3. $n = 5$ için $p(x) = q(x) = 1 + x$ ve $r(x) = 1 + x + x^2 + x^3 + x^4$ olarak seçilirse Teorem 2.12.3'deki şartlar sağlanır ve $k = 5$ olur. Bu durumda kendine ortogonal C toplamsal devirli kodu

$$C = \langle wp(x) + q(x), r(x) \rangle = \langle w^2 + w^2 x, 1 + x + x^2 + x^3 + x^4 \rangle$$

$$= \{(0\ 0\ 0\ 0\ 0), (w^2\ w^2\ 0\ 0\ 0), (1\ 1\ w\ 1\ w), (0\ 0\ w^2\ w^2\ 0),$$
$$(0\ 0\ 0\ w^2\ w^2), (w^2\ 0\ 0\ 0\ w^2), (1\ 1\ w\ w\ 1), (w\ w\ 1\ w\ w),$$
$$(0\ w^2\ 0\ w^2\ 0), (0\ 0\ w^2\ 0\ w^2), (0\ w^2\ w^2\ 0\ 0), (1\ w\ 1\ 1\ w),$$
$$(w\ w\ 1\ 1\ 1), (w^2\ w^2\ 0\ w^2\ w^2), (w\ 1\ 1\ 1\ w), (w^2\ 0\ 0\ w^2\ 0),$$
$$(1\ 1\ 1\ 1\ 1), (w^2\ 0\ w^2\ w^2\ w^2), (1\ 1\ 1\ w\ w), (w^2\ w^2\ w^2\ 0\ w^2),$$
$$(w\ 1\ w\ 1\ 1), (w\ w\ w\ 1\ w), (w\ w\ w\ w\ 1), (w^2\ 0\ w^2\ 0\ 0),$$

$$(1\ \ w\ \ 1\ \ w\ \ 1),(w^2\ \ w^2\ \ w^2\ \ w^2\ \ 0),(1\ \ w\ \ w\ \ 1\ \ 1),(1\ \ w\ \ w\ \ w\ \ w),$$
$$(w\ \ 1\ \ w\ \ w\ \ w),(0\ \ w^2\ \ 0\ \ 0\ \ w^2),(0\ \ w^2\ \ w^2\ \ w^2\ \ w^2),(w\ \ 1\ \ 1\ \ w\ \ 1)\}$$

olur. (2.8)'de verilen iç çarpıma göre $C \subset C^{\perp}$'dir. (2.7)'de verilen ϕ fonksiyonuna göre $\phi^{-1}(C)$ kümesinin öz alt uzaylarından herhangi biri ile bir $[[5,0,2]]$ parametreli kuantum kod yazılır. $\phi^{-1}(C)$ kümesinin elemanları ve öz uzaylarından biri Tablo 2.6'da verilmiştir.

Tablo 2.6 $\phi^{-1}(C)$ kümesi ve öz uzaylarından biri

C	$\phi^{-1}(C)$	Öz uzay	C	$\phi^{-1}(C)$	Öz uzay
(00000)	$(00000\|00000)$	(00000)	(11111)	$(11111\|11111)$	(11111)
(w^2w^2000)	$(00000\|11000)$	(11000)	$(w^20w^2w^2w^2)$	$(00000\|10111)$	(10111)
$(11w1w)$	$(11111\|11010)$	(11010)	$(111ww)$	$(11111\|11100)$	(11100)
$(00w^2w^20)$	$(00000\|00110)$	(00110)	$(w^2w^2w^20w^2)$	$(00000\|11101)$	(11101)
$(000w^2w^2)$	$(00000\|00011)$	(00011)	$(w1w11)$	$(11111\|01011)$	(01011)
(w^2000w^2)	$(00000\|10001)$	(10001)	$(www1w)$	$(11111\|00010)$	(00010)
$(11ww1)$	$(11111\|11001)$	(11001)	$(wwww1)$	$(11111\|00001)$	(00001)
$(ww1ww)$	$(11111\|00100)$	(00100)	(w^20w^200)	$(00000\|10100)$	(10100)
$(0w^20w^20)$	$(00000\|01010)$	(01010)	$(1w1w1)$	$(11111\|10101)$	(10101)
$(00w^20w^2)$	$(00000\|00101)$	(00101)	$(1ww11)$	$(11111\|10011)$	(10011)
$(0w^2w^200)$	$(00000\|01100)$	(01100)	$(1wwww)$	$(11111\|10000)$	(10000)
$(1w11w)$	$(11111\|10110)$	(10110)	$(w^2w^2w^2w^20)$	$(00000\|11110)$	(11110)
$(ww111)$	$(11111\|00111)$	(00111)	$(w1www)$	$(11111\|01000)$	(01000)
$(w^2w^20w^2w^2)$	$(00000\|11011)$	(11011)	$(0w^200w^2)$	$(00000\|01001)$	(01001)
$(w111w)$	$(11111\|01110)$	(01110)	$(0w^2w^2w^2w^2)$	$(00000\|01111)$	(01111)
(w^200w^20)	$(00000\|10010)$	(10010)	$(w11w1)$	$(11111\|01101)$	(01101)

$\phi^{-1}(C)$ 'nin öz uzaylarından biri Tablo 2.6'da gösterildiği gibi ya

$$\{(00000),(11111)\}$$

ya da

$$\{(00000),(10000),(01000),(00100),(00010),(00001),(11000),(01100),$$

$$(00110),(00011),(10100),(10010),(10001),(01010),(01001),(00101),$$

$$(11100),(01110),(00111),(10110),(11010),(11001),(01101),(01011),$$

$$(10011),(10101),(11110),(01111),(10111),(11011),(11101),(11111)\}$$

olarak alınabilir. ilk öz uzay için kuantum kod

$$\frac{1}{\sqrt{2}}(|00000\rangle - |11111\rangle)$$

ve ikinci öz uzay için

$$\frac{1}{4\sqrt{2}}(|00000\rangle - |10000\rangle - |01000\rangle - |00100\rangle - |00010\rangle - |00001\rangle + |11000\rangle + |01100\rangle$$
$$+ |00110\rangle + |00011\rangle + |10100\rangle + |10010\rangle + |10001\rangle + |01010\rangle + |01001\rangle + |00101\rangle$$
$$- |11100\rangle - |01110\rangle - |00111\rangle - |10110\rangle - |11010\rangle - |11001\rangle - |01101\rangle - |01011\rangle$$
$$- |10011\rangle - |10101\rangle + |11110\rangle + |01111\rangle - |10111\rangle + |11011\rangle + |11101\rangle - |11111\rangle)$$

olur. İkinci öz uzay için elde edilen yukarıdaki kuantum kodun stabilizerlerinden biri de $XXXXX$ olduğundan bu kuantum kod mantıksal bazlar kullanılarak

$$|0_L\rangle = \frac{1}{4}\big(|00000\rangle - |00100\rangle - |00010\rangle + |11000\rangle + |00110\rangle + |10001\rangle + |01001\rangle - |11100\rangle$$

$$-|11010\rangle - |01101\rangle - |01011\rangle - |10011\rangle - |10101\rangle + |11110\rangle + |01111\rangle - |10111\rangle\big)$$

ve

$$|1_L\rangle = \frac{1}{4}\big(|00101\rangle + |10010\rangle + |10100\rangle + |01100\rangle + |01010\rangle + |00011\rangle + |11011\rangle + |11101\rangle$$

$$-|00001\rangle - |10000\rangle - |01000\rangle - |00111\rangle - |11001\rangle - |01110\rangle - |10110\rangle - |11111\rangle\big)$$

olup $a|0_L\rangle + b|1_L\rangle$ $\left(|a|^2 + |b|^2 = 1\right)$ olarak yazılır.

Teorem 2.12.3 kullanılarak elde edilen kuantum kodlar ile yine bu teoreme bazı ilave şartlar getirilerek elde edilen DNA kodlar arasında ilişki kurmak mümkündür. [1] referanslı makalenin 12. teoremine göre DNA kod elde etmek için kullanılan $p(x), q(x), r(x) \in \mathbb{Z}_2[x]$ polinomları Teorem 2.12.3 ii. şartlarını sağlarsa bu polinomlar kullanılarak aynı zamanda kuantum kod da elde edilir. Örnek 2.12.3'de verilen $p(x), q(x)$ ve $r(x)$ polinomları DNA kod elde etmek için de kullanılabilir. Bu polinomlar kullanılarak yazılan C klasik kodunun kodsözlerinde $0 \to A, 1 \to T, w \to C, w^2 \to G$ değişikliği yapılırsa 5 uzunluğunda bir DNA kod elde edilir.

2.13. İkili Olmayan Kuantum Stabilizer Kodlar

1995 yılında Shor ilk kez hata düzeltebilen kuantum kod elde ettikten sonra bu alanda birçok çalışma yapılmıştır. Tıpkı klasik kodlarda olduğu gibi önce çalışmalar ikili sistemde yapılmış daha sonra bu çalışmalar ikili olmayan sistemler için de formüle edilmeye çalışılmıştır. Bu tür kodlara ikili olmayan (nonbinary) kuantum kod denilmektedir. İkili olmayan kuantum kodların ilk örneklerinden biri [42] referanslı kaynakta verilmiştir. [27] ve [28] numaralı referanslarda $\mathbb{Z}_n$ üzerindeki klasik kodlar ile kuantum kodlar arasındaki bir ilişki verilmiştir. İkili olmayan

kuantum stabilizer kodlar üzerine de bir çok çalışma yapılmıştır. Bu çalışmalardan bazıları [6, 16, 25, 26, 27, 28, 42] kaynaklarında bulunabilir. Özellikle [25] referanslı kaynakta ikili olmayan kuntum kodlar için daha kapsamlı sonuçlar bulunmuştur.

Bu alt bölümde ikili olmayan kuantum stabilizer kodlara giriş yapılıp bazı temel tanımlar verilecektir.

q bir p asal sayısının pozitif bir kuvveti ve $\mathbb{F}_q$ da q elemanlı sonlu bir cisim olsun ve $\mathbb{C}^q$, q boyutlu kompleks vektör uzayı kuantum mekaniksel sistem hal uzayını göstersin. $\forall i$ için $x_i \in \mathbb{F}_q$ olmak üzere $|x_1 x_2 \cdots x_n\rangle$ ile $\mathbb{C}^q$'nun ortonormal bazlarını gösterelim. Bu durumda $\mathbb{C}^{q^n}$'nin her k-boyutlu alt uzayına hata düzeltebilen kuantum kod denir ve $[[n,k,d]]_q$ parametreleri ile gösterilir. Bundan önceki bölümde $q=2$ için kuantum kodlar incelenmişti. n kubitli ikili sistem stabilizer kuantum kodun stabilizeri $2^n \times 2^n$ şeklindeki kompleks matrislerden oluşan G_n Pauli matris grubunun değişmeli bir alt grubu olarak tanımlanır ve bu stabilizer ile kuantum kod yazılabilir. Nonbinary kuantum stabilizer kod yazmak için de yine tüm hatalardan oluşan E_n kümesini tanımlamak gereklidir. E_n hata kümesi $q^n \times q^n$ kompleks matrislerden oluşur.

İkili sistem kuantum kodlarda hata bazları olarak $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ ve $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ üniter Pauli matrisleri alınmıştı. İkili olmayan kuantum sistemleri için de üniter Pauli matrisleri tanımlanabilir. Aşağıda bu matrislerin nasıl elde edileceği açıklanmıştır.

m bir pozitif tamsayı, p bir asal sayı ve $q = p^m$ olmak üzere $tr : \mathbb{F}_q \to \mathbb{F}_p$, $tr(x) = \sum_{k=0}^{m-1} x^{q^k}$ fonksiyonu iz fonksiyonu olarak tanımlanır. $a, b \in \mathbb{F}_q$ olmak üzere $\mathbb{C}^q$ üzerinde üniter operatörler $X_a |x\rangle = |x + a\rangle$ ve $Z_b |b\rangle = \omega^{tr(bx)} |x\rangle$ olarak tanımlanır. Burada $\omega = e^{2\pi i / p}$'dir. Bu durumda hata operatörlerinin kümesin $E = \{ X_a Z_b : a, b \in \mathbb{F}_q \}$ olarak tanımlanır. Bu kümenin şu özellikleri vardır:

i . Birim matrisi kapsar,

ii . Bu kümenin iki elemanının çarpımı yine bu kümeden bir elemanın bir sabitle çarpımına eşittir,

iii . $A, B \in E$ ve $A \neq B$ olmak üzere $Tr(A^{\dagger}B) = 0$ dır.

$Tr(A)$ ile A matrisin köşegen elemanlarının toplamı verilir. Eğer q^2 tane matristen oluşan bu hata operatörlerinin sonlu kümesi yukarıdaki 3 şartı sağlıyorsa bu kümeye 'iyi hata bazları' denir [25, 27, 28].

Lemma 2.13.1. $E = \left\{ X_a Z_b : a, b \in \mathbb{F}_q \right\}$ kümesi $\mathbb{C}^q$ için iyi hata bazlar kümesidir [25].

Örnek 2.13.1. $q = 4$ için $\alpha^3 + 1 = 0$ ve $\alpha^2 + \alpha + 1 = 0$ ve $\mathbb{F}_4 = \left\{ 0, 1, \alpha, \alpha^2 \right\}$ olmak üzere $\mathbb{C}^4$ için standart bazlar olarak

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, |1\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, |\alpha\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}, |\alpha^2\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

seçilebilir. I_2 ile 2×2 tipindeki birim matris ve $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ matrisleri gösterilirse, bu durumda iyi hata bazlarını oluşturacak matrisler şu şekilde yazılır:

$$X(0) = I_2 \otimes I_2, \quad X(1) = I_2 \otimes \sigma_x, \quad X(\alpha) = \sigma_x \otimes I_2, \quad X(\alpha^2) = \sigma_x \otimes \sigma_x,$$

$$Z(0) = I_2 \otimes I_2, \quad Z(1) = \sigma_z \otimes I_2, \quad Z(\alpha) = \sigma_z \otimes \sigma_z, \quad Z(\alpha^2) = I_2 \otimes \sigma_z.$$

Gerçekten $X(1)|1\rangle = |(1+1)(\bmod 2)\rangle = |0\rangle$ olduğu

$$X(1)|1\rangle = \left[\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right] \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = |0\rangle$$

şeklinde hesaplanarak da bulunabilir.

Farklı bir yöntemle de X ve Y matrisleri tespit edilebilir. Bu yöntem [28] referanslı kaynakta etraflıca incelenmiştir. Buna göre; ω birimin ilkel n. kökü olsun. Bu durumda n boyut için bir hata baz kümesi $(X_a)_{i,j} = \delta_{j,i+a \,(\mathrm{mod}\, n)}$ ve $(Z_b)_{i,j} = \delta_{i,j}\omega^{ib}$ matrisleri kullanılarak

$$\varepsilon_n = \left\{E_{i,j} = X_a^i Z_b^j\right\}, i, j \in \mathbb{Z}_n$$

şeklinde yazılır [28].

Örnek 2.13.2. $\mathbb{F}_q = \mathbb{Z}_5$ olsun. Bu durumda

$$X_0|0\rangle = |0\rangle, X_0|1\rangle = |1\rangle, X_0|2\rangle = |2\rangle, X_0|3\rangle = |3\rangle, X_0|4\rangle = |4\rangle,$$

$$X_1|0\rangle = |1\rangle, X_1|1\rangle = |2\rangle, X_1|2\rangle = |3\rangle, X_1|3\rangle = |4\rangle, X_1|4\rangle = |0\rangle,$$

$$X_2|0\rangle = |2\rangle, X_2|1\rangle = |3\rangle, X_2|2\rangle = |4\rangle, X_2|3\rangle = |0\rangle, X_2|4\rangle = |1\rangle,$$

$$X_3|0\rangle = |3\rangle, X_3|1\rangle = |4\rangle, X_3|2\rangle = |0\rangle, X_3|3\rangle = |1\rangle, X_3|4\rangle = |2\rangle,$$

$$X_4|0\rangle = |4\rangle, X_4|1\rangle = |0\rangle, X_4|2\rangle = |1\rangle, X_4|3\rangle = |2\rangle, X_4|4\rangle = |3\rangle$$

ve $\omega = \mathrm{e}^{2\pi i/5}$ olmak üzere

$Z_0|0\rangle = |0\rangle, Z_0|1\rangle = |1\rangle, Z_0|2\rangle = |2\rangle, Z_0|3\rangle = |3\rangle, Z_0|4\rangle = |4\rangle,$

$Z_1|0\rangle = |0\rangle, Z_1|1\rangle = \omega|1\rangle, Z_1|2\rangle = \omega^2|2\rangle, Z_1|3\rangle = \omega^3|3\rangle, Z_1|4\rangle = \omega^4|4\rangle,$

$Z_2|0\rangle = |0\rangle, Z_2|1\rangle = \omega^2|1\rangle, Z_2|2\rangle = \omega^4|2\rangle, Z_2|3\rangle = \omega|3\rangle, Z_2|4\rangle = \omega^3|4\rangle,$

$Z_3|0\rangle = |0\rangle, Z_3|1\rangle = \omega^3|1\rangle, Z_3|2\rangle = \omega|2\rangle, Z_3|3\rangle = \omega^4|3\rangle, Z_3|4\rangle = \omega^2|4\rangle,$

$Z_4|0\rangle = |0\rangle, Z_4|1\rangle = \omega^4|1\rangle, Z_4|2\rangle = \omega^3|2\rangle, Z_4|3\rangle = \omega^2|3\rangle, Z_4|4\rangle = \omega|4\rangle$

olarak bulunur. Bu matrisler aşağıdaki gibi tanımlanabilir.

$X_0 = I_5 = Z_0$ birim matris,

$$X_1 = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix}, X_2 = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix}, X_3 = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix},$$

ve

$$X_4 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}, Z_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & \omega^4 & 0 & 0 & 0 \\ 0 & 0 & \omega^3 & 0 & 0 \\ 0 & 0 & 0 & \omega^2 & 0 \\ 0 & 0 & 0 & 0 & \omega \end{bmatrix}, Z_2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & \omega^3 & 0 & 0 & 0 \\ 0 & 0 & \omega & 0 & 0 \\ 0 & 0 & 0 & \omega^4 & 0 \\ 0 & 0 & 0 & 0 & \omega^2 \end{bmatrix},$$

$$Z_4 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & \omega & 0 & 0 & 0 \\ 0 & 0 & \omega^2 & 0 & 0 \\ 0 & 0 & 0 & \omega^3 & 0 \\ 0 & 0 & 0 & 0 & \omega^4 \end{bmatrix}, Z_3 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & \omega^2 & 0 & 0 & 0 \\ 0 & 0 & \omega^4 & 0 & 0 \\ 0 & 0 & 0 & \omega & 0 \\ 0 & 0 & 0 & 0 & \omega^3 \end{bmatrix}$$

olarak elde edilir. $\mathbb{C}^{\otimes 5} = \mathbb{C} \otimes \mathbb{C} \otimes \mathbb{C} \otimes \mathbb{C} \otimes \mathbb{C}$ için standart bazlar

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, |1\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}, |2\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}, |3\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, |4\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix},$$

olarak alınırsa yukarıda yazılanlar kolayca elde edilir. Örneğin

$X_3 |4\rangle = |(3+4) \bmod 5\rangle = |2\rangle$ olduğu

$$X_3 |4\rangle = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = |2\rangle$$

şeklinde matrislerin çarpımı kullanılarak elde edilebilir. Aynı şekilde faz hatasına da şu şekilde örnek verilebilir: $Z_4 |2\rangle = \omega^{tr(4.2)} |2\rangle = \omega^3 |2\rangle$ olduğu

$$Z_4 |2\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & \omega & 0 & 0 & 0 \\ 0 & 0 & \omega^2 & 0 & 0 \\ 0 & 0 & 0 & \omega^3 & 0 \\ 0 & 0 & 0 & 0 & \omega^4 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ \omega^3 \\ 0 \end{bmatrix} = \omega^3 |2\rangle$$

şeklinde matrislerin çarpımı kullanılarak elde edilebilir.

Tanım 2.13.1. $\mathbb{F}_q$, q elemanlı bir cisim ve $u = (a|b), v = (a'|b') \in \mathbb{F}_q^{2n}$ olsun. Bu durumda u ile v'nin $\mathbb{F}_q$ üzerindeki simpletik iç çarpımı

$$\langle u,v\rangle = tr_{q/p}\left(ba' - ab'\right)$$

olarak tanımlanır [25].

Teorem 2.13.1. Eğer $\mathbb{F}_q^{2n}$ üzerinde q^n/q^k elemanlı bir C toplamsal kodu Tanım 2.13.1'de verilen iç çarpıma göre $C \subset C^{\perp}$ ise bu durumda bir $\left[\left[n,k,d\right]\right]_q$ kuantum kodu vardır. Bu kodun minimum mesafesi ise $C^{\perp} - C$ kümesindeki vektörlerin Hamming ağırlığının en küçüğüne eşittir. Minimum Hamming mesafesi

$$d = \min\left\{wt\left(a|b\right) : \left(a|b\right) \in C^{\perp} - C\right\}$$

ve $\left(a|b\right) \in \mathbb{F}_q^{2n}$ vektörünün ağırlığı da

$$wt\left(\left(a|b\right)\right) = \left|\left\{i : \left(a_i|b_i\right) \neq \left(0|0\right)\right\}\right|$$

olarak tanımlanır [25].

Teorem 2.13.2. $\mathbb{F}_q$ üzerinde $\left[n,k_1,d_1\right]_q$ ve $\left[n,k_2,d_2\right]_q$ parametreli iki klasik kod sırasıyla C_1 ve C_2 olsun. Eğer $C_2 \subset C_1$ ise $\left[\left[n,k_1-k_2,d\right]\right]_q$ parametreli ve

$$d = \min\left\{wt\left(u\right) : u \in \left(C_1 - C_2\right) \cup \left(C_2^{\perp} - C_1^{\perp}\right)\right\}$$

minimum mesafesine sahip bir kuantum kod vardır. Eğer $d = \min\left\{d_1,d_2\right\}$ ise bu kuantum koda saf aksi halde saf olmayan kuantum kod denir [25].

Teorem 2.13.3. Teorem 2.13.2' verilen şartlar altında, H_1 matrisi $C_1^{\perp}$ klasik kodunun üreteç matrisi ve G_2 matrisi de C_2 klasik kodunun üreteç matrisi olmak üzere kuantum kodun kontrol matrisi

$$G=\left(\begin{array}{c|c} H_1 & 0 \\ 0 & G_2 \end{array}\right)$$

olur [35].

Örnek 2.13.3. $\mathbb{F}_7$ cismi üzerinde $[3,1,3]_7$ parametreli ve

$$H_1=\begin{pmatrix}3 & 3 & 4\end{pmatrix}$$

üreteç matrisine sahip $C_1^{\perp}$ klasik kodu ile aynı parametrelere sahip

$$G_2=\begin{pmatrix}5 & 3 & 1\end{pmatrix}$$

üreteç matrisine sahip C_2 klasik kodu göz önüne alınırsa

$$G=\left(\begin{array}{ccc|ccc} 3 & 3 & 4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 5 & 3 & 1 \end{array}\right)$$

kontrol matrisine sahip $[[3,1,2]]_7$ kuantum kodu elde edilir.

Burada

$$H_2=\begin{pmatrix}1 & 2 & 3 \\ 2 & 1 & 1\end{pmatrix} \text{ ve } G_1=\begin{pmatrix}1 & 0 & 1 \\ 0 & 1 & 1\end{pmatrix}$$

dir.

BÖLÜM 3. GAUSS TAM SAYILARI ÜZERİNDEKİ KLASİK KODLARDAN KUANTUM KOD ELDE ETME

3.1. Giriş

Bu bölümde Gauss tam sayılarından yararlanılarak elde edilen klasik kodlardan yardımı ile kuantum kod elde etme yöntemi verilmektedir. Gauss tam sayıları üzerindeki klasik kodlar [23, 34] referanslı kaynaklarda bulunabilir.

3.2. Gauss Tam Sayıları Üzerindeki Klasik Kodlar ve Mannheim Metriği

Tanım 3.2.1. $H=\left\{a+bi : a,b\in\mathbb{Z}, i^2=-1\right\}$ olarak tanımlanan kümeye Gauss tam sayılar kümesi denir.

Gauss tam sayılar kümesi adi toplama ve çarpma işlemleri ile bir Öklid bölgesidir. p bir asal tam sayı ve $a,b,n\in\mathbb{Z}$ olmak üzere $p=4n+1$ şeklinde yazılabilen asal sayılar H Gauss tam sayılar halkasında $p=(a+bi)(a-bi)$ şeklinde yazılabilir. Bu durumda $\pi=a+bi$ sayısı Gauss tam sayılar halkasında asal olur. Aynı zamanda π'nin eşleniği olan $\overline{\pi}=a-bi$ sayısı da bu halkada asaldır. Bu bölümde aksi söylenmedikçe p asal tam sayısı $p\equiv 1 \pmod 4$ ve π asal Gauss tam sayısı da $\pi\overline{\pi}=p\equiv 1 \pmod 4$ olarak alınacaktır [23].

Tanım 3.2.2. p bir asal tam sayı ve $\pi\in H$ da $\pi\overline{\pi}=p$ biçiminde bir asal Gauss tam sayısı olsun. π modülosuna göre asal kalan sınıfları kümesi H_π ile gösterilirse, $\mu: H\to H_\pi$ modülo fonksiyonu

$$\mu(a+bi) = a+bi \bmod \pi = a+bi - \left[\frac{(a+bi)\overline{\pi}}{p}\right]\pi \tag{3.1}$$

şeklinde tanımlanır. Burada $[\cdot]$ ile bir Gauss tam sayısının yuvarlaması gösterilmektedir. Bir Gauss tam sayısının yuvarlaması reel ve sanal kısımlarının ayrı ayrı yuvalaması ile elde edilir. $p = \pi\overline{\pi} \equiv 1 \pmod 4$ şeklinde bir asal tam sayı ve $\mathbb{F}_p$, karakteristiği p olan bir cisim olmak üzere, μ modülo fonksiyonu $\mathbb{F}_p$'den iki boyutlu H_π cismine bire bir, örten bir homomorfizma olur.

Tanım 3.2.3. $p = \pi\overline{\pi} \equiv 1 \pmod 4$ şeklinde bir asal tam sayı, $\alpha, \beta \in H_\pi$ ve $\gamma = \alpha - \beta \pmod \pi$ olsun. γ'nın Mannheim ağırlığı $w_m(\gamma)$ biçiminde gösterilir ve

$$w_m(\gamma) = \left|\mathrm{Re}(\gamma)\right| + \left|\mathrm{Im}(\gamma)\right| \tag{3.2}$$

olarak, α ile β arasındaki Mannheim mesafesi ise $d_m(\alpha,\beta)$ biçiminde gösterilir ve $d_m(\alpha,\beta) = w_m(\gamma)$ olarak tanımlanır [23].

Not: Yukarıdaki tanımda verilen Mannheim metriğinin her H_π cismi üzerinde doğru çalışmadığı [32] referanslı makalede gösterilmiştir. Bu hatayı düzeltmek için yukarıdaki tanımda verilen $w_m(\gamma) = \left|\mathrm{Re}(\gamma)\right| + \left|\mathrm{Im}(\gamma)\right|$ ifadesinde $\left|\mathrm{Re}(\gamma)\right| + \left|\mathrm{Im}(\gamma)\right|$ minimum olma şartı getirilmiştir. Bu tezde Mannheim metriği kullanılırken bu ayrıntı göz önüne alınmaktadır.

Örnek 3.2.1. $p = 13$ için $\pi = 3+2i$ alınabilir. Bu durumda $\mathbb{Z}_{13} \cong H_{3+2i}$ olur. $7 \in \mathbb{Z}_{13}$ için

$$\mu(7) = 7 - \left[\frac{7(3-2i)}{13}\right](3+2i) \equiv 7 - (2-i)(3+2i) = -1-i \in H_{3+2i} \tag{3.3}$$

olur. Aynı yolla

$$H_{3+2i}=\{0,\pm 1,\pm i,\pm 2,\pm 2i,\pm(1+i),\pm(1-i)\} \tag{3.4}$$

olarak elde edilir. $1+i$ ile $-1-i$ elemanları arasındaki Mannheim mesafesi $1+i-(-1-i)\equiv -1 \pmod{3+2i}$ olduğundan $d_m(1+i,-1-i)=1$ olur.

Tanım 3.2.4. π bir Gauss tam sayısı ve $\alpha\in H_\pi$ de mertebesi $p-1$ olan bir eleman olsun. Bu durumda üreteç ve kontrol matrisi sırasıyla

$$G=\begin{pmatrix} -\alpha & 1 & 0 & 0 & \cdots & 0 \\ -\alpha^2 & 0 & 1 & 0 & \cdots & 0 \\ \vdots & & \ddots & \ddots & & \vdots \\ -\alpha^{(p-1)/4-1} & 0 & 0 & \cdots & 0 & 1 \end{pmatrix},\ H=\begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{p-1/4-1} \end{pmatrix} \tag{3.5}$$

şeklinde tanımlanan $n=(p-1)/4$ uzunluğuna sahip $C\subset H_\pi^{(p-1)/4}$ kodu Mannheim ağırlığı 1 olan tüm bir hatalı vektörleri düzeltebilen kod olarak tanımlanır. ± 1 ve $\pm i$ elemanlarının Mannheim ağırlı birdir [23].

Örnek 3.2.2. $\pi=3+2i$ ve $\alpha=2\in H_{3+2i}$ alınırsa

$$\begin{aligned} x^3+i &= (x-\alpha)(x-\alpha^5)(x-\alpha^9) \\ &= (x-2)(x-(1+i))(x-i) \end{aligned} \tag{3.6}$$

olup 3 uzunluğundaki C kodunun üreteç polinomu $g(x)=x-2$ olur. Bu kodun üreteç ve kontrol matrisleri ise sırasıyla

$$G=\begin{pmatrix} -2 & 1 & 0 \\ 0 & -2 & 1 \end{pmatrix},\ H=\begin{pmatrix} 1 & 2 & -1+i \end{pmatrix} \tag{3.7}$$

olur. Bu kodun minimum Mannheim mesafesi 3 minimum Hamming mesafesi ise 2'dir.

Bu tür kodlar için dekodlama şu şekilde açıklanabilir: Kanaldan gelen söz r olsun. Bu sözün sendromu $S(r)=Hr^{tr}$ ile hesaplanır. Bu sendromun ilkel eleman α'nın kuvvetlerinden birine eşit olup olmadığı incelenir. Eğer $S(r)=Hr^{tr}=\alpha^{l}$ ise α'nın kuvveti olan l hatanın yerinin bulunmasını, $l\equiv m\,(\mathrm{mod}\,n)$ olmak üzere α^{l}/α^{m} ise hatanın değerinin hesaplanmasını sağlar. Ayrı bir yöntem ise; r'nin sendromunun C kodunun kontrol matrisinin bir sütununa, bir sütununun ilgilisine, bu sendromun kontrol matrisinin $d-1$ sütununun toplamlarına ya da sütunların ilgililerinin toplamlarına eşit olup olmadığının kontrol edilmesi ile de bulunabilir. Örnek 3.2.3 için gelen söz $r=(-2\quad 1\quad -i)$ olsun. Bu durumda $S(r)=1+i=\alpha^{5}$ olur. $5\equiv 2\,(\mathrm{mod}\,3)$ olduğundan hatanın, 3. bileşende meydana geldiği anlaşılır. Hatanın değeri ise $\alpha^{5}/\alpha^{2}=-i$ olur. Diğer yandan r'nin sendromu C kodunun kontrol matrisinin 3. sütununun bir ilgilisi olduğu görülmektedir. O halde hata 3. bileşende meydana gelmiştir. Ayrıca $1+i=-i(-1+i)$ olduğundan hatanın değeri $-i$ olarak elde edilir.

Tanım 3.2.5. π bir asal Gauss tam sayısı, r bir pozitif tam sayı ve $\alpha\in H_{\pi}$ bir ilkel eleman olmak üzere

$$H=\begin{pmatrix}1 & \alpha & \alpha^{2} & \cdots & \alpha^{\left(\left(p^{r}-1\right)/4\right)-1}\end{pmatrix} \tag{3.8}$$

kontrol matrisine sahip $n=\left(\left(p^{r}-1\right)/4\right)-1$ uzunluklu, $k=n-r$ boyutlu ve $d_{m}=3$ minimum mesafeli kodlar H_{π} üzerinde blok kodlardır [23].

π bir asal Gauss tam sayısı olsun. $\alpha_{1}^{(p-1)/4}\equiv -i$ ve $\alpha_{2}^{(p-1)/4}\equiv i$ olmak üzere $\alpha_{1},\alpha_{2}\in H_{\pi}$ olsun. Bu durumda $x^{(p-1)/4}+i$ ve $x^{(p-1)/4}-i$ polinomları sırası ile H_{π} üzerinde

$$x^{(p-1)/4}+i=(x-\alpha_1)(x-\alpha_1^5)\cdots(x-\alpha_1^{p-4}),$$
$$x^{(p-1)/4}-i=(x-\alpha_2)(x-\alpha_2^5)\cdots(x-\alpha_2^{p-4}) \tag{3.9}$$

şeklinde çarpanlarına ayrılır. Ayrıca (3.9) kullanılarak $x^{(p-1)/2}+1$ polinomu da

$$x^{(p-1)/2}+1=(x-\alpha_1)(x-\alpha_1^5)\cdots(x-\alpha_1^{p-4})(x-\alpha_2)(x-\alpha_2^5)\cdots(x-\alpha_2^{p-4}) \tag{3.10}$$

biçiminde çarpanlarına ayrılır. (3.10) kullanılarak $g_1 \mid x^{(p-1)/2}+1$, $g_2 \mid x^{(p-1)/2}+1$ ve $g_1 \mid g_2$ olacak şekilde $g_1, g_2 \in H_\pi[x]$ polinomları kolayca yazılabilir. Önerme 1.1.2'ye göre g_1 ve g_2 polinomları bir devirli kodun üreteç polinomları olur. Üstelik $g_1 \mid g_2$ olduğundan g_1 polinomunun ürettiği devirli kod C_1 ve g_2 polinomunun ürettiği devirli kod C_2 olmak üzere $C_2 \subset C_1$ olur.

Örnek 3.2.3. $\pi = 3+2i$ için $\alpha_1 = 2$ ve $\alpha_2 = -2$ alınabilir. Bu durumda

$$x^6+1=(x-2)(x-(1+i))(x-i)(x+2)(x+(1+i))(x+i) \tag{3.11}$$

olur. Buradan $g_1(x)=x-2$ ve $g_2(x)=(x-2)(x+i)=x^2-2ix-2i$ şeklinde seçilebilir. Böylece g_1 ve g_2 polinomlarının ürettiği klasik devirli kodlara sırasıyla C_1 ve C_2 denirse bu kodların üreteç matrisleri de sırasıyla

$$G_1=\begin{pmatrix} -2 & 1 & 0 & 0 & 0 & 0 \\ 0 & -2 & 1 & 0 & 0 & 0 \\ 0 & 0 & -2 & 1 & 0 & 0 \\ 0 & 0 & 0 & -2 & 1 & 0 \\ 0 & 0 & 0 & 0 & -2 & 1 \end{pmatrix},\ G_2=\begin{pmatrix} -2i & -2i & 1 & 0 & 0 & 0 \\ 0 & -2i & -2i & 1 & 0 & 0 \\ 0 & 0 & -2i & -2i & 1 & 0 \\ 0 & 0 & 0 & -2i & -2i & 1 \end{pmatrix}$$

olur.

3.3 Gauss Tam Sayıları Üzerinde Kuantum Kodlar İçin Hata Bazları

Tanım 3.3.1. π bir asal Gauss tam sayısı, $a,b,g \in H_\pi$, δ Kronecker delta fonksiyonu ve ξ birimin p. kökü olmak üzere $\mathbb{C}^p$ üzerinde üniter hata bazları

$$\left(X_g\right)_{s,t} = \delta_{\mu(t),\mu(s+g)}, \left(Z_g\right)_{s,t} = \delta_{s,t}\xi^{\left(p-\mu^{-1}(g)\right)s(\mathrm{mod}\,p)} \tag{3.12}$$

olarak tanımlanır. Bu bazları [6] referanslı kaynakta $\mathbb{Z}_p$ üzerinde

$$X_{s,t} = \delta_{s,t-1(\mathrm{mod}\,p)}, Z_{s,t} = \delta_{s,t}\xi^s \tag{3.13}$$

şeklinde tanımlanmıştır. Burada çalışılan küme H_π olduğundan μ fonksiyonu kullanılmıştır. Çünkü μ fonksiyonu, $\pi\overline{\pi} = p$ olmak üzere $\mathbb{Z}_p$'den H_π'ye (3.1)'de gösterildiği gibi bir izomorfizma tanımlar. Bu operatörlerin $|u\rangle$ haline etkisi ise [25] referanslı kaynakta gösterilmiştir. $u \in H_\pi$ olmak üzere bu hata bazları $|u\rangle$ kuantum haline

$$X_a|u\rangle = |\mu(a+u)\rangle, Z_b|u\rangle = \xi^{\mu^{-1}(bu)(\mathrm{mod}\,p)}|u\rangle \tag{3.14}$$

şeklinde etki eder. Burada μ fonksiyonu (3.1)'de tanımlanmıştır.

X_a ve Z_b, H_π üzerinde Tanım 3.3.1'de tanımlanan üniter matrisleri için aşağıdaki durumlar vardır. Bu durumlar yine [6] referanslı kaynakta gösterilmiştir.

$$i.\ X_aZ_b = \xi^{\left(p-\mu^{-1}(ba)\right)(\mathrm{mod}\,p)}Z_bX_a, \tag{3.15}$$

$ii.$ X_aZ_b ve $X_{a'}Z_{b'}$ için

$$\left(X_a Z_b\right)\left(X_{a'} Z_{b'}\right) = X_a \left(Z_b X_{a'}\right) Z_{b'} = \xi^{-\left(p-\mu^{-1}(ba)\right)(\mathrm{mod}\, p)} X_{a+a'} Z_{b+b'}$$

ve

iii. I_p matrisi $p \times p$ tipindeki birim matrisi göstermek üzere

$$\left(X_a\right)^{\dagger} = \left(X_a\right)^{p-1}, \left(Z_b\right)^{\dagger} = \left(Z_b\right)^{p-1}, \left(X_a\right)^{p} = \left(Z_b\right)^{p} = I_p \tag{3.16}$$

olur.

Tanım 3.3.2. π bir asal Gauss tam sayısı olmak üzere $\varepsilon = \left\{X_a Z_b : a,b \in H_\pi\right\}$ olarak tanımlanan küme hata operatörleri için bir baz kümesidir. Eğer bu küme aşağıdaki özellikleri sağlarsa bu kümeye bir iyi hata bazları (nice error basis) kümesi denir.

i. ε kümesi birim matrisi içerir.

ii. ε kümesinin iki elemanının çarpımı, bir skalerle ε kümesindeki bir elemanın çarpımına eşittir.

iii. Bir M matrisinin izi $Tr\left(M\right)$ ile gösterilir ve bu matrisin köşegen elemanlarının toplamı olarak tanımlanırsa A, B operatörleri ε'nin farklı elemanları olmak üzere $Tr\left(AB\right) = 0$ olur.

Önerme 3.3.1. π bir asal Gauss tam sayısı olmak üzere $\varepsilon = \left\{X_a Z_b : a,b \in H_\pi\right\}$ kümesi $\mathbb{C}^p$ için bir iyi hata bazlar kümesidir.

İspat: *i*. $X_0 Z_0$ birim matristir.

ii. (3.15) eşitliğinden görülür.

iii . $X_a Z_b = \xi^{\left(p-\mu^{-1}(b)\right)\mu^{-1}(a)} Z_b X_a$ olduğundan

$$\left(X_a Z_b\right)\left(X_{a'} Z_{b'}\right) = \xi^{p-\left(p-\mu^{-1}(b)\right)\mu^{-1}(a)(\mathrm{mod}\, p)} X_{\mu\left(a+a'\right)} Z_{\mu\left(b+b'\right)}$$

olur. $\left(X_a Z_b\right)\left(X_{a'} Z_{b'}\right)$ matrisinin köşegen elemanlarının toplamı 0 olduğundan $Tr\left(\left(X_a Z_b\right)\left(X_{a'} Z_{b'}\right)\right) = 0$ olur. ■

Örnek 3.3.1. $\pi = 2 + i$ olsun. Bu durumda ξ birimin 5. kökü olmak üzere $\mathbb{C}^5$ üzerinde iyi hata bazlar kümesi için üniter operatörler aşağıdaki gibi yazılabilir.

$$X_0 = Z_0 = I_5 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}, X_1 = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}, X_{-i} = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix},$$

$$X_i = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}, X_{-1} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}, Z_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & \xi^4 & 0 & 0 & 0 \\ 0 & 0 & \xi^3 & 0 & 0 \\ 0 & 0 & 0 & \xi^2 & 0 \\ 0 & 0 & 0 & 0 & \xi \end{pmatrix},$$

$$Z_{-i} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & \xi^1 & 0 & 0 & 0 \\ 0 & 0 & \xi & 0 & 0 \\ 0 & 0 & 0 & \xi^4 & 0 \\ 0 & 0 & 0 & 0 & \xi^2 \end{pmatrix}, Z_i = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & \xi^2 & 0 & 0 & 0 \\ 0 & 0 & \xi^4 & 0 & 0 \\ 0 & 0 & 0 & \xi & 0 \\ 0 & 0 & 0 & 0 & \xi^3 \end{pmatrix}, Z_{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & \xi & 0 & 0 & 0 \\ 0 & 0 & \xi^2 & 0 & 0 \\ 0 & 0 & 0 & \xi^3 & 0 \\ 0 & 0 & 0 & 0 & \xi^4 \end{pmatrix}.$$

Bu operatörler

$$|0\rangle=\begin{pmatrix}1\\0\\0\\0\\0\end{pmatrix},|-1\rangle=\begin{pmatrix}0\\1\\0\\0\\0\end{pmatrix},|i\rangle=\begin{pmatrix}0\\0\\1\\0\\0\end{pmatrix},|-i\rangle=\begin{pmatrix}0\\0\\0\\1\\0\end{pmatrix},|1\rangle=\begin{pmatrix}0\\0\\0\\0\\1\end{pmatrix}$$

kuantum hallerine şöyle etki eder:

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

$$X_{-i}|0\rangle=|-i\rangle, X_{-i}|-1\rangle=|1\rangle, X_{-i}|i\rangle=|0\rangle, X_{-i}|-i\rangle=|-1\rangle, X_{-i}|1\rangle=|i\rangle,$$

$$X_i|0\rangle=|i\rangle, X_i|-1\rangle=|-i\rangle, X_i|i\rangle=|1\rangle, X_i|-i\rangle=|0\rangle, X_i|1\rangle=|-1\rangle,$$

$$X_{-1}|0\rangle=|-1\rangle, X_{-1}|-1\rangle=|i\rangle, X_{-1}|i\rangle=|-i\rangle, X_{-1}|-i\rangle=|1\rangle, X_{-1}|1\rangle=|0\rangle,$$

$$Z_1|0\rangle=|0\rangle, Z_1|-1\rangle=\xi^4|-1\rangle, Z_1|i\rangle=\xi^3|i\rangle, Z_1|-i\rangle=\xi^2|-i\rangle, Z_1|1\rangle=\xi|1\rangle,$$

$$Z_i|0\rangle=|0\rangle, Z_i|-1\rangle=\xi^3|-1\rangle, Z_i|i\rangle=\xi^4|i\rangle, Z_i|-i\rangle=\xi|-i\rangle, Z_i|1\rangle=\xi^2|1\rangle,$$

$$Z_{-i}|0\rangle=|0\rangle, Z_{-i}|-1\rangle=\xi^3|-1\rangle, Z_{-i}|i\rangle=\xi|i\rangle, Z_{-i}|-i\rangle=\xi^4|-i\rangle, Z_{-i}|1\rangle=\xi^2|1\rangle,$$

$$Z_{-1}|0\rangle=|0\rangle, Z_{-1}|-1\rangle=\xi|-1\rangle, Z_{-1}|i\rangle=\xi^2|i\rangle, Z_{-1}|-i\rangle=\xi^3|-i\rangle, Z_{-1}|1\rangle=\xi^4|1\rangle.$$

$X_{-i}|-1\rangle=|(-1-i)\,(\mathrm{mod}\,2+i)\rangle=|1\rangle$ olduğu

$$X_{-i}|-1\rangle=\begin{pmatrix}0&0&1&0&0\\0&0&0&1&0\\0&0&0&0&1\\1&0&0&0&0\\0&1&0&0&0\end{pmatrix}\begin{pmatrix}0\\1\\0\\0\\0\end{pmatrix}=\begin{pmatrix}0\\0\\0\\0\\1\end{pmatrix}=|1\rangle$$

veya

$Z_{-i}\left|-i\right\rangle = \xi^{\mu^{-1}((-i)(-i))}\left|-i\right\rangle = \xi^4\left|-i\right\rangle$ olduğu

$$Z_{-i}\left|-i\right\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & \xi^1 & 0 & 0 & 0 \\ 0 & 0 & \xi & 0 & 0 \\ 0 & 0 & 0 & \xi^4 & 0 \\ 0 & 0 & 0 & 0 & \xi^2 \end{pmatrix}\begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \xi^4 \\ 0 \end{pmatrix} = \xi^4\left|-i\right\rangle$$

şeklinde de hesaplanabilir.

$n=1$ kubitli kuantum kodlar için gerekli hata operatörleri yukarıda verilmiştir. n kubitli kuantum kodlar için de hata operatörleri tanımlanabilir.

Tanım 3.3.3. π bir asal Gauss tam sayısı ve $u=\begin{pmatrix} u_0 & u_1 & \cdots & u_{n-1}\end{pmatrix} \in H_\pi^n$ olsun. Bu durumda $\left(\mathbb{C}^p\right)^{\otimes n} = \mathbb{C}^p \otimes \mathbb{C}^p \otimes \cdots \otimes \mathbb{C}^p$ için hata operatörleri $X_u = X_{u_0} \otimes X_{u_1} \otimes \cdots \otimes X_{u_{n-1}}$ ve $Z_u = Z_{u_0} \otimes Z_{u_1} \otimes \cdots \otimes Z_{u_{n-1}}$ şeklinde tanımlanır.

Önerme 3.3.2. π bir asal Gauss tam sayısı olmak üzere $\varepsilon_n = \left\{X_u Z_v : u,v \in H_\pi^n\right\}$ kümesi $\left(\mathbb{C}^p\right)^{\otimes n}$ için bir iyi hata bazlar kümesidir.

İspat. Tanım 3.3.3'den ispat görülür. ■

n kubitli kuantum hal uzayı üzerinde tanımlı tüm Pauli matrislerinin oluşturduğu küme G_n ile gösterilirse

$$G_n = \left\{\xi^{\mu^{-1}(c)} X_u Z_v : u,v \in H_\pi^n, c \in H_\pi\right\} \tag{3.17}$$

şeklinde tanımlanır. Bazı kaynaklarda ikili olmayan kuantum sistemleri için kubit yerine kudit kelimesi kullanılmaktadır. Bu G_n kümesi değişmeli olmayan p^{2n+1}

mertebeli bir sonlu gruptur. G_n grubunun merkezi olan $M(G_n)$ kümesi ξI_n ile üretilen p. mertebeden bir grup olur.

3.4 Gauss Tam Sayıları Üzerinde Kuantum Kodlar

Tanım 3.4.1. $u=(u_0 \quad u_1 \quad \cdots \quad u_{n-1}), v=(v_0 \quad v_1 \quad \cdots \quad v_{n-1}) \in H_\pi^n$ olmak üzere u ile v vektörleri arasındaki iç çarpım

$$u.v=\sum_i u_i v_i$$

olarak tanımlanırsa $(u|v),(u'|v') \in H_\pi^{2n}$ elemanları arasında iç çarpım $Tr: H_{\pi^k} \to H_\pi$ olmak üzere,

$$(u|v)*(u'|v')=Tr(vu'-v'u) \tag{3.18}$$

şeklinde tanımlanır. $k=1$ için

$$(u|v)*(u'|v')=vu'-v'u \tag{3.19}$$

olacağı açıktır. Bu iç çarpıma göre H_π^{2n} üzerindeki bir C lineer kodunun diki

$$C^{\perp_*}=\left\{(u|v)\in H_\pi^{2n} : (u|v)*(u'|v')=0, \forall (u'|v') \in C\right\}$$

şeklinde tanımlanır.

Tanım 3.4.2. $(u|v),(u'|v') \in H_\pi^{2n}$ olmak üzere

$$w=(u|v)-(u'|v')=(w_i|w_i') \pmod{\pi}$$

elemanın Mannheim ağırlığı ve $(u|v)$ elemanı ile $(u'|v')$ elemanı arasındaki Mannheim mesafesi sırasıyla

$$wt_m(w)=\left\lceil \left[\begin{array}{l} |\mathrm{Re}(w_0)|+|\mathrm{Im}(w_0)|+\cdots+|\mathrm{Re}(w_{n-1})|+|\mathrm{Im}(w_{n-1})| \\ +|\mathrm{Re}(w_0')|+|\mathrm{Im}(w_0')|+\cdots+|\mathrm{Re}(w_{n-1}')|+|\mathrm{Im}(w_{n-1}')| \end{array} \right] \Big/ 2 \right\rceil,$$

$$d_m\left((u|v),(u'|v')\right)=wt_m(w)$$

şeklinde tanımlanır.

Teorem 3.4.1. Gauss tam sayıları üzerinde Mannheim metriğine göre tanımlı sırasıyla $[n,k_1,d_1]_\pi$ ve $[n,k_2,d_2]_\pi$ parametreli ve $C_2\subset C_1$ şeklinde iki klasik kod olsun ve C_1 ile $C_2^\perp$ klasik kodları t hata düzeltebilsin. Bu durumda t hata düzeltebilen $\left[[n,k_1-k_2,d]\right]_\pi$ parametrelerine sahip bir kuantum kod vardır.

İspat. $C=\left(C_2|C_1^\perp\right)=\left\{(u|v):u\in C_2,v\in C_1^\perp\right\}$ olarak alınırsa (3.19)'de verilen iç çarpıma göre $C_1^\perp\subset C_2^\perp$ olduğundan $C\subset C^\perp$ olur. Teorem 2.13.1 göz önüne alınırsa $\left[[n,k_1-k_2,d]\right]_\pi$ kodunun varlığı elde edilir. ■

Kabul edelim ki C_1 ve $C_2^\perp$ kodlarının minimum Mannheim mesafesi d_m olsun. Bu kodlar kullanılarak elde edilen C kodunun düzeltebileceği hata vektörlerinin sayısı, $t=\lfloor d_m-1/2\rfloor$ olmak üzere

$$4\binom{n}{1}+4^2\binom{n}{2}+\cdots+4^t\binom{n}{t}$$

olarak hesaplanır.

Örnek 3.4.1. $\pi = 4+i$ olsun. H_{4+i} üzerinde x^8+1 polinomu (3.10)'da verilen yönteme göre çarpanlarına ayrılırsa $g_1(x) = 1+2i+(-1+i)x-ix^2+x^3$ ve $g_2(x) = 1-i+(2-i)x+(-1+i)x^2-ix^3-ix^4+x^5$ olarak seçilebilir. Bu durumda $C_2 \subset C_1$ olur. C_1 ile $C_2^{\perp}$ klasik kodlarının minimum Hamming mesafesi 4, minimum Mannheim mesafesi ise 5'tir. Bu durumda C_1 ile C_2 klasik kodları Hamming metriğine göre yazılırsa bu kodlar kullanılarak $[[8,2,4]]_{4+i}$ kuantum kodu elde edilir. Bu kuantum kod Bölüm 2.9'da verilen CSS kod oluşturma tekniğine göre her hangi bir kubitte meydana gelen hataları düzeltebilir. Ancak farklı iki kubitte meydana gelen hataları düzeltemez. $[[8,2,4]]_{4+i}$ kuantum kodu Hamming metriğine göre MDS (maksimum uzaklığa ayrılabilen) koddur. Diğer yandan C_1 ile $C_2^{\perp}$ kodlarının minimum Mannheim mesafesi 5 olduğundan $[[8,2,5]]_{4+i}$ kuantum kodu elde edilir. Bu kod kuantum stabilizer kod değildir ancak CSS kod yapısındadır. Bu kod bir kubitte meydana gelen bir ağırlıklı tüm hatalarla beraber herhangi iki kubitte meydana gelen bir ağırlıklı tüm hataları da düzeltebilir. Örneğin $|1-i \quad 2-i \quad -1+i \quad -i \quad -i \quad 1 \quad 0 \quad 0\rangle$ kuantum haline kuantum kanalında $IIIX_1X_1III = X_1^4X_1^5$ operatörü etki ederse gelen hal

$$X_1^4X_1^5|1-i \quad 2-i \quad -1+i \quad -i \quad -i \quad 1 \quad 0 \quad 0\rangle = |1-i \quad 2-i \quad -1+i \quad -i+1 \quad -i+1 \quad 1 \quad 0 \quad 0\rangle$$

olur. Hamming metriğine göre yazılan C_1 klasik kodunun minimum mesafesi 4 olduğundan bu bit değişimi hatasını düzeltemez. Bölüm 2.9'da verilen yönteme göre bu bit değişimi hatası Mannheim metriği kullanılarak tespit edilebilir. Bu hatanın yeri ve hatanın düzeltilmesi şu şekilde açıklanır: C_1 klasik kodunun kontrol matrisi olan H_1,

$$H_1 = \begin{pmatrix} 1 & i & -i & 1-i & 2-i & -1+i & 0 & 0 \\ 0 & 1 & i & -i & 1-i & 2-i & -1+i & 0 \\ 0 & 0 & 1 & i & -i & 1-i & 2-i & -1+i \end{pmatrix}$$

olup,

$$H_1\left(1-i \quad 2-i \quad -1+i \quad -i \quad -i \quad 1 \quad 0 \quad 0\right)=\begin{pmatrix}-2+i\\ 2i\\ 0\end{pmatrix}$$

olduğundan hatanın 4. ve 5. kubitte olduğu ve hataların değinin 1 olduğu görülür. Dekodlama için hatanın değerine karşılık gelen hata operatörünün tersinin kuantum haline uygulanması yeterlidir. Hatanın değeri 1 olduğundan X_1 operatörünün tersi X_{-1} olup hatalı kuantum haline $IIIX_{-1}X_{-1}III = X_{-1}^4X_{-1}^5$ operatörü etki ederse

$$X_{-1}^4X_{-1}^5\left|1-i \quad 2-i \quad -1+i \quad -i+1 \quad -i+1 \quad 1 \quad 0 \quad 0\right\rangle=\left|1-i \quad 2-i \quad -1 \quad -i+1 \quad -i \quad 1 \quad 0 \quad 0\right\rangle$$

olur. Hamming metriğe göre $r=\left(1-i \quad 2-i \quad -1+i \quad -i+1 \quad -i+1 \quad 1 \quad 0 \quad 0\right)$ gelen 2 hatalı vektörü dekodlayamaz. Çünkü Hamming metriğe göre gelen vektör r ile $c_1=\left(1-i \quad 2-i \quad -1+i \quad -i \quad -i \quad 1 \quad 0 \quad 0\right)$ kodsözü arasındaki mesafe $d_H\left(r,c_1\right)=2$ ve yine r ile $c_2=\left(2i \quad 1+i \quad -1+i \quad 1-i \quad 1-i \quad 1 \quad 0 \quad 0\right)$ kodsözü arasındaki mesafe de $d_H\left(r,c_2\right)=2$'dir. Dolayısı ile Hamming metrik bu sözü dekodlayamaz. Burada r vektörü ile diğer kodsözler arasındaki mesafe ya 2'dir ya da 2'den büyüktür. Mannheim metriğe göre $d_m\left(r,c_1\right)=2$, $d_m\left(r,c_2\right)=4$ olacağından kanaldan gelen hatalı vektör dekodlanır. $\left[\left[8,2,4\right]\right]_{4+i}$ kuantum kodunun düzeltebildiği bit değişimi hatalarının sayısı 136 dır. $\left[\left[8,2,5\right]\right]_{4+i}$ kuantum kodunun düzeltebildiği bit değişimi hatalarının sayısı ise 480 dir. Düzeltebildikleri faz değişim hatalarının sayısı da bit değişimi sayıları kadardır.

Örnek 3.4.2. $\pi=2+i$ olsun. H_{2+i} üzerinde x^4-1 polinomu (3.10)'da verilen yönteme benzer olarak çarpanlarına ayrılırsa $g_1\left(x\right)=i+x$ ve $g_2\left(x\right)=-i-x+ix^2+x^3$ olarak seçilebilir. Bu durumda $C_2\subset C_1$ olur. C_1 ile $C_2^{\perp}$ klasik kodlarının minimum Mannheim mesafesi 2'dir. Bu durumda C_1 ile C_2 klasik

kodları kullanılarak Mannheim metriğine göre $\left[\left[4,2,2\right]\right]_{2+i}$ kuantum kodu elde edilir. Bu kuantum kodun kodsözlerinde biri

$$\left|0_L\right\rangle = \frac{1}{\sqrt{5}}\begin{pmatrix}\left|0 \quad 0 \quad 0 \quad 0\right\rangle + \left|-i \quad -1 \quad i \quad 1\right\rangle + \left|i \quad 1 \quad -i \quad -1\right\rangle \\ +\left|1 \quad -i \quad -1 \quad i\right\rangle + \left|-1 \quad i \quad 1 \quad -i\right\rangle\end{pmatrix}$$

dir. Bu kodun stabilizerlerinden birisi $X_{-1}X_iX_1X_{-i}$'dir. Bu stabilizer yukarıdaki kuantum haline etki ederse kuantum hali değişmez. Yani

$$X_{-1}X_iX_1X_{-i}\left|0_L\right\rangle = X_{-1}X_iX_1X_{-i}\frac{1}{\sqrt{5}}\begin{pmatrix}\left|0 \quad 0 \quad 0 \quad 0\right\rangle + \left|-i \quad -1 \quad i \quad 1\right\rangle + \left|i \quad 1 \quad -i \quad -1\right\rangle \\ +\left|1 \quad -i \quad -1 \quad i\right\rangle + \left|-1 \quad i \quad 1 \quad -i\right\rangle\end{pmatrix}$$

$$= \frac{1}{\sqrt{5}}\begin{pmatrix}\left|-1 \quad i \quad 1 \quad -i\right\rangle + \left|1 \quad -i \quad -1 \quad i\right\rangle + \left|-i \quad -1 \quad i \quad 1\right\rangle \\ +\left|0 \quad 0 \quad 0 \quad 0\right\rangle + \left|i \quad 1 \quad -i \quad -1\right\rangle\end{pmatrix}$$

$$= \left|0_L\right\rangle$$

olur. Bu kodun stabilizeri Bölüm 2'de verilen stabilizer kuantum kodların stabilizerlerinin oluşturulması ile aynı anlam içermemektedir. Bölüm 2'de verilen yöntemle yazılan stabilizer kuantum kodların kullandıkları kuantum kanalları Hamming metriğine göre dizayn edilmiştir. Mannheim metriğine göre bir kuantum kodun stabilizerlerinin tamamının yazılabilmesi için bu metriğe göre yeni bir kuantum kanalı inşa edilmelidir. Bu kod mantıksal bazlar cinsinden

$$\left|1_L\right\rangle = X_1X_1X_1X_1\frac{1}{\sqrt{5}}\begin{pmatrix}\left|0 \quad 0 \quad 0 \quad 0\right\rangle + \left|-i \quad -1 \quad i \quad 1\right\rangle + \left|i \quad 1 \quad -i \quad -1\right\rangle \\ +\left|1 \quad -i \quad -1 \quad i\right\rangle + \left|-1 \quad i \quad 1 \quad -i\right\rangle\end{pmatrix}$$

$$= \frac{1}{\sqrt{5}}\begin{pmatrix}\left|1 \quad 1 \quad 1 \quad 1\right\rangle + \left|i \quad 0 \quad -1 \quad -i\right\rangle + \left|-1 \quad -i \quad i \quad 0\right\rangle \\ +\left|-i \quad i \quad 0 \quad -1\right\rangle + \left|0 \quad -1 \quad -i \quad i\right\rangle\end{pmatrix}$$

olup

$a|0_L\rangle + b|1_L\rangle \ \left(|a|^2 + |b|^2 = 1\right)$

olarak yazılır. $X_{-1}X_iX_1X_{-i}$ kuantum hali bu $a|0_L\rangle + b|1_L\rangle$ kodu için bir stabilizerdir.

Tablo 3.1'de Hamming ve Mannheim metriğine göre Gauss tam sayıları kullanılarak elde edilen klasik kodlar yardımı ile üretilen kuantum kodların karşılaştırılması verilmiştir. Tablo 3.1'in HM sütununda Hamming metriğe göre yazılan klasik kodlar yardımı ile elde edilmiş kuantum kodlar ve MM sütununda Mannheim metriğine göre yazılan klasik kodlar yardımı ile elde edilmiş kuantum kodlar gösterilmektedir. Tablodaki kodların minimum mesafesinin hesaplanmasında Mathematica 6 programından yararlanılmıştır.

Tablo 3.1 Hamming ve Mannheim metriğine göre Gauss tam sayıları üzerindeki klasik kodlar yardımı ile elde edilen kuantum kodların karşılaştırılması

p	α_1	α_2	h_1	g_2	HM	MM
5	i	$-i$	$x^3 - ix^2$ $-x + i$	$x^3 + ix^2$ $-x - i$	$[[4,2,2]]_{2+i}$	$[[4,2,2]]_{2+i}$
13	2	–2	$1 - i - x$ $+x^2$	$1 - i + x$ $+x^2$	$[[6,2,3]]_{3+2i}$	$[[6,2,4]]_{3+2i}$
13	2	–2	$-i - 2x$ $+2ix^2 + x^3$	$1 - i + x$ $+x^2$	$[[6,1,3]]_{3+2i}$	$[[6,1,4]]_{3+2i}$
13	2	–2	$x - 2$	$x + 2$	$[[6,4,2]]_{3+2i}$	$[[6,4,2]]_{3+2i}$
13	2	–2	$-1 + ix + x^2$	$-i + (-1+i)x$ $+x^2$	$[[6,2,2]]_{3+2i}$	$[[6,2,2]]_{3+2i}$
17	$1+i$	$-2+i$	$-1 + i + (2-i)x$ $+(1-i)x^2 - ix^3$ $+ix^4 + x^5$	$-i - 2ix$ $+x^3 + x^4$	$[[8,1,4]]_{4+i}$	$[[8,1,5]]_{4+i}$
17	$1+i$	$-2+i$	$-2 + i + (1+i)x$ $+(2-i)x^2 + x^3$	$2 - i + (1+i)x$ $-(2-i)x^2 + x^3$	$[[8,2,4]]_{4+i}$	$[[8,2,5]]_{4+i}$
17	$1+i$	$-2+i$	$-1 + (1+i)x$ $+x^2$	$-1 - (1+i)x$ $+x^2$	$[[8,4,3]]_{4+i}$	$[[8,4,\geq 3]]_{4+i}$
17	$1+i$	$-2+i$	$-1 - i + x$	$1 + i + x$	$[[8,6,2]]_{4+i}$	$[[8,6,\geq 2]]_{4+i}$
29	$-1+$	$-2+i$	$-2 + x$	$2 + x$	$[[14,12,\geq 2]]_{5+2i}$	$[[14,12,\geq 2]]_{5+2i}$

BÖLÜM 4. KUATERNİYON TAM SAYILARI ÜZERİNDEKİ KLASİK KODLARDAN KUANTUM KOD ELDE ETME

4.1 Giriş

Bu bölümde kuaterniyon tam sayıları üzerinde tanımlanan klasik kodlar yardımı ile kuantum kod elde etme yöntemi verilmektedir. Kuaterniyon tam sayıları üzerindeki klasik kodlar [32, 38, 39] referanslı kaynaklarda bulunabilir. [38] referanslı kaynakta sözü edilen kuaterniyon Mannheim metrik ile [32, 39] referanslı kaynaklarda tanımlanan Lipschitz metrik eş zamanlı çalışmalarda farklı isimlerle tanımlanmıştır.

4.2. Kuaterniyon Tam Sayıları Üzerindeki Klasik Kodlar ve Lipschitz Metrik

İlk olarak 1843 yılında Hamilton tarafından tanımlanan kuaterniyonlar karmaşık sayıların bir genişlemesidir.

Tanım 4.2.1. $\mathbb{R}$ reel sayılar kümesi olmak üzere $\mathbb{R}$ üzerinde kuaterniyon cebri $\mathcal{H}(\mathbb{R})$ ile gösterilir ve aşağıdaki gibi tanımlanır.

i. $\mathcal{H}(\mathbb{R}) = \{a_0 + a_1 i + a_2 j + a_3 k : a_0, a_1, a_2, a_3 \in \mathbb{R}\}$ ile tanımlanır ve $\mathcal{H}(\mathbb{R})$ bir free $\mathbb{R}-$modüldür.

ii. 1 çarpmanın birimidir.

iii. $i^2 = j^2 = k^2 = -1$ dir.

iv. $ij = -ji = k,\ jk = -kj = i,\ ki = -ik = j$ dir [14].

$q = a_0 + a_1 i + a_2 j + a_3 k$ bir kuaterniyon sayısı olmak üzere q'nun eşleniği $\bar{q}$ ile gösterilir ve $\bar{q} = a_0 - a_1 i - a_2 j - a_3 k$'dır. Bu kuaterniyon sayısının normu ise $N(q)$ ile gösterilir ve $N(q) = q\bar{q} = a_0^2 + a_1^2 + a_2^2 + a_3^2$ olarak tanımlanır. Bu norm çarpımsaldır. Yani $q_1, q_2 \in \mathbb{H}(\mathbb{R})$ için $N(q_1 q_2) = N(q_1) N(q_2)$'dir. Bir kuaterniyon sayısı tam kısım ve vektör kısım olarak iki kısma ayrılır. $q = a_0 + a_1 i + a_2 j + a_3 k$ kuaterniyon sayısının tam kısmı a_0 ve vektör kısmı da $a_1 i + a_2 j + a_3 k$'dır. Genel olarak kuaterniyonlar üzerinde çarpma işleminin değişme özelliği yoktur. Ancak eğer iki kuaterniyon sayısının vektör kısımları birbirine paralel ise çarpımları değişmelidir. Ayrıca $\mathbb{H}(\mathbb{R})$ bir çarpık (skew) cisimdir.

Kuaterniyon tam sayıları ise $\mathbb{H}(\mathbb{Z}) = \{a_0 + a_1 i + a_2 j + a_3 k : a_0, a_1, a_2, a_3 \in \mathbb{Z}\}$ olarak tanımlanır. Kuaterniyon tamsayılarının bazı temel cebirsel özellikleri aşağıdaki tanım ve teoremlerle verilmektedir.

Tanım 4.2.2. $q \in \mathbb{H}(\mathbb{Z})$ olmak üzere eğer $N(q) \in \mathbb{Z}$ tek tam sayı ise q'ya tek, $N(q) \in \mathbb{Z}$ çift tam sayı ise q'ya çift denir [14].

Tanım 4.2.3. $\mathbb{H}(\mathbb{Z})$'nin birimsel elemanları $\mp 1, \mp i, \mp j, \mp k$'dır. $q_1, q_2 \in \mathbb{H}(\mathbb{Z})$ olmak üzere eğer $q_1 = \varepsilon_1 q_2 \varepsilon_2$ olacak şekilde $\varepsilon_1, \varepsilon_2 \in \{\mp 1, \mp i, \mp j, \mp k\}$ varsa q_1 ile q_2 ilgilidir denir [14].

Önerme 4.2.1. Her kuaterniyon tam sayısı asal kuaterniyon sayılarının bir çarpımına eşittir [14].

Önerme 4.2.2. Her $p \in \mathbb{N}$ asal tek sayısı için $N(\alpha) = p$ olacak şekilde bir $\alpha \in \mathbb{H}(\mathbb{Z})$ vardır [14].

Sonuç 4.2.1. $\alpha \in \mathbb{H}(\mathbb{Z})$ elemanının asal olması için gerek ve yeter şart $N(\alpha)$'nın $\mathbb{Z}$'de asal olmasıdır [14].

Önerme 4.2.3. $\alpha, \beta \in \mathbb{H}(\mathbb{Z})$ ve β tek olsun. Bu durumda

$$\alpha = \gamma\beta + \delta, \quad N(\delta) < N(\beta) \tag{4.1}$$

olacak şekilde $\gamma, \delta \in \mathbb{H}(\mathbb{Z})$ elemanları vardır [14].

Tanım 4.2.4. $\pi \neq 0$ bir kuaterniyon tam sayısı olsun. $\beta \in \mathbb{H}(\mathbb{Z})$ elemanı için $q_1 - q_2 = \beta\alpha$ oluyorsa q_1, q_2'ye π modülosuna göre sağdan denktir denir ve $q_1 \equiv_r q_2 \pmod{\pi}$ şeklinde gösterilir. Böylece π modülosuna göre

$$\mathbb{H}(\mathbb{Z})_\pi = \{q \pmod{\alpha} : q \in \mathbb{H}(\mathbb{Z})\} \tag{4.2}$$

olur [32].

Teorem 4.2.1. $\pi \in \mathbb{H}(\mathbb{Z})$ olmak üzere $\mathbb{H}(\mathbb{Z})_\pi$'nın $N(\pi)^2$ tane elemanı vardır [32].

Önerme 4.2.4. $\pi \neq 0$ ve $\beta, \gamma \in \mathbb{H}(\mathbb{Z})_\pi$ olsun. Eğer $\beta - \gamma \equiv_r a_0 + a_1 i + a_2 j + a_3 k \pmod{\pi}$ ve $|a_0| + |a_1| + |a_2| + |a_3|$ minimum ise β ile γ arasındaki Lipschitz mesafesi

$$d_L(\beta, \gamma) = |a_0| + |a_1| + |a_2| + |a_3| \tag{4.3}$$

olarak hesaplanır [32].

Tanım 4.2.5. $\pi \neq 0$ ve $\beta, \gamma \in \mathbb{H}(\mathbb{Z})_\pi$, $\delta = \beta - \gamma \equiv_r a_0 + a_1 i + a_2 j + a_3 k \pmod{\pi}$ ve $|a_0| + |a_1| + |a_2| + |a_3|$ minimum olmak üzere δ'nın Lipschitz ağırlığı

$$wt_L(\delta) = |a_0| + |a_1| + |a_2| + |a_3| \tag{4.4}$$

olarak tanımlanır.

$\pi \in \mathbb{H}(\mathbb{Z})$ bir asal sayı olursa $\mathbb{H}(\mathbb{Z})_\pi$ bir çarpık cisim olur.

$\alpha \in \mathbb{H}(\mathbb{Z})_\pi$ mertebesi $p-1=\pi\overline{\pi}-1$ olan bir eleman olsun. Bu durumda bir Lipschitz ağırlıklı bir hata düzeltebilen $n=(p-1)/2$ uzunluğuna sahip klasik kodun üreteç ve kontrol matrisi sırasıyla aşağıdaki gibi yazılabilir.

$$G=\begin{pmatrix} -\alpha & 1 & 0 & 0 & \cdots & 0 \\ -\alpha^2 & 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & & \ddots & & \vdots \\ -\alpha^{(p-1)/2-1} & 0 & 0 & \cdots & 0 & 1 \end{pmatrix},\ H=\begin{pmatrix} 1 & \alpha & \cdots & \alpha^{(p-1)/2-1} \end{pmatrix}$$ [3].

Lipschitz ağırlığı bir olan sekiz eleman vardır. Bunlar $\mp 1, \mp i, \mp j, \mp k$ 'dır. Bu kodların dekodlaması ise şöyle olur: Kaynaktan çıkan orijinal vektör c ve kanalda bu vektöre etki eden hata vektörü e olursa dekodere gelen vektör $r=c+e$ olur. r vektörünün sendromu $S(r)=Hr^{tr}$ ve hatanın değeri $S(r)\alpha^{-l}$ ile hesaplanır. Burada $l \pmod n$ hatanın yerinin bulunmasını sağlar. $\mathbb{H}(\mathbb{Z})_\pi$ üzerinde değişme özelliği olmadığından $Hr^{tr} \neq \left(rH^{tr}\right)^{tr}$ dir. Eğer r 'nin sendromu α 'nın kuvvetleri arasında yoksa α 'nın kuvvetlerinin ilgilileri kontrol edilir [38, 39].

Örnek 4.2.1. $\pi=2+i+j+k$ ve $\alpha=1-i-j-k$ olsun. Bu durumda

$$\begin{aligned}\mathbb{H}(\mathbb{Z})_\pi = \{&0, \mp 1, \mp i, \mp j, \mp k, \mp(1+i), \mp i(1+i), \mp j(1+i), \mp k(1+i), \mp(1+j), \mp i(1+j), \\ &\mp k(1+j), \mp j(1+j), \mp(1+k), \mp i(1+k), \mp j(1+k), \mp(1-i-j-k), \\ &\mp(-1+i+j+k), \mp(1-i+j+k), \mp k(1+k), \mp(1+i+j-k), \\ &\mp(1+i-j+k), \mp(1+i-j), \mp(1-i+k), \mp(1+j-k)\}\end{aligned}$$

ve

$$G=\begin{pmatrix} -1+i+j+k & 1 & 0 \\ i+j+k & 0 & 1 \end{pmatrix},\ H=\begin{pmatrix} 1 & 1-i-j-k & -i-j-k \end{pmatrix}$$

olur. Dekodere gelen söz $r=\begin{pmatrix} i+j & 0 & 1 \end{pmatrix}$ olsun. Bu durumda

$$S(r)=Hr^{tr}=-k=-k\alpha^{0} \tag{4.5}$$

olduğundan hata vektörü $e=\begin{pmatrix} -k & 0 & 0 \end{pmatrix}$ olarak bulunur. Kodsöz $c=r-e=\begin{pmatrix} i+j+k & 0 & 1 \end{pmatrix}$ olarak elde edilir.

Lipschitz ağılığı 1 olan iki farklı bileşende meydana gelen hataları düzeltebilen klasik kodlar da vardır.

$\pi\in\mathbb{H}(\mathbb{Z})$ bir asal ve $\beta\in\mathbb{H}(\mathbb{Z})_{\pi}$ mertebesi $p-1=2n$ olan bir eleman olsun. (β'nın kuvvetleri birbirine paralel olmalıdır. Aksi takdirde bu bölümde anlatılan teknik çalışmaz). $t<n$ bir negatif olmayan tamsayı olmak üzere C kodu için H kontrol matrisi;

$$H=\begin{pmatrix} 1 & \beta & \beta^{2} & \cdots & \beta^{n-1} \\ 1 & \beta^{3} & \beta^{6} & \cdots & \beta^{3(n-1)} \\ \vdots & & & & \\ 1 & \beta^{2t+1} & \beta^{2(2t+1)} & \cdots & \beta^{(n-1)(2t+1)} \end{pmatrix} \tag{4.6}$$

olarak tanımlanır. $c\in\mathbb{H}(\mathbb{Z})_{\pi}^{n}$ elemanının C kodunun bir kodsözü olması için gerek ve yeter şart $cH^{tr}=0$ olmasıdır [39].

Teorem 4.2.2. C kodu (4.1) kontrol matrisine sahip bir kod olsun. Bu durumda C kodu $0\le wt_{L}(e_{s}),wt_{L}(e_{s'})\le 1$ olmak üzere $e(x)=e_{s}x^{s}+e_{s'}x^{s'}$ formundaki bazı hataları düzeltebilir [39].

Örnek 4.2.2. $\pi = 1+2i+2j+2k$ ve $\beta = 2$ alınırsa Lipsichtz ağılığı bir olan 2 farklı bileşende meydana gelen hatayı düzeltebilen C klasik kodunun kontrol matrisi

$$H = \begin{pmatrix} 1 & 2 & -2+i+j+k & 1-i-j-k & 3 & i+j+k \\ 1 & 1-i-j-k & -1 & -1+i+j+k & 1 & 1-i-j-k \end{pmatrix}$$

olur. $c = (3 \quad 3 \quad 1 \quad 0 \quad 0 \quad 0)$ kodsözüne kanalda $e = (0 \quad 0 \quad 0 \quad j \quad 0 \quad -j)$ hatası etki ederse kanaldan gelen söz $r = (3 \quad 3 \quad 1 \quad j \quad 0 \quad -j)$ olur. bu gelen sözü dekodlamak için önce gelen sözün sendromu sonra bu sendromdan yararlanarak hataların yerleri ve değerleri hesaplanır. Buna göre

$$S(r) = Hr^{tr} = \begin{pmatrix} s_1 \\ s_3 \end{pmatrix} = \begin{pmatrix} 2-2i+j+2k \\ -2+2i-2j-2k \end{pmatrix} \equiv \begin{pmatrix} 2j \\ -3j \end{pmatrix} (\text{mod } \pi)$$

ve $s_3 \neq s_1^3$ olduğundan gelen sözde 2 hata meydana geldiği görülür. $\theta_1 = j$ seçilirse $s_1^{'} = \theta_1 s_1 = -2$ ve $s_2^{'} = \theta_1 s_2 = 3$ olup

$$3s_1^{'}\varepsilon = \left(s_1^{'}\right)^3 - s_3^{'} \Rightarrow \varepsilon = -2+i+j+k$$

ve ε'nu kullanarak hataların yerlerinin ve değerlerinin bulunmasını sağlayan $\sigma(z) = z^2 - s_1 z + \varepsilon$ polinomunun kökleri β^3, β^{11} olarak bulunur. Bu da 1. hatanın 4. bileşende ve 2. hatanın da 6. bileşende meydana geldiğini gösterir. Birinci hatanın değeri $\theta_1\left(\beta^3/\beta^3\right) = j$ ve 2. hatanın değeri de $\theta_1\left(\beta^{11}/\beta^5\right) = -j$ olarak elde edilir. Böylece gelen söz

$$c = r - e = (3 \quad 3 \quad 1 \quad j \quad 0 \quad -j) - (0 \quad 0 \quad 0 \quad j \quad 0 \quad -j)$$

$$= (3 \quad 3 \quad 1 \quad 0 \quad 0 \quad 0)$$

şeklinde dekodlanır.

$\pi \in \mathbb{H}(\mathbb{Z})$ bir asal olmak üzere $\mathbb{H}(\mathbb{Z})_\pi$ üzerinde kontadevirli (contacyclic) kodlar aşağıdaki gibi tanımlanır.

Tanım 4.2.6. Eğer $(c_0,\ c_1,\ \ldots\ c_{n-1}) \in C$ iken $\theta \in \{\mp i, \mp j, \mp k\}$ olmak üzere $(\theta c_{n-1},\ c_0,\ \ldots\ c_{n-2}) \in C$ ise $\mathbb{H}(\mathbb{Z})_\pi$ üzerinde tanımlı bu C koduna kontadevirli ($\theta-$devirli) kod denir.

$\pi \in \mathbb{H}(\mathbb{Z})$ bir asal, $\pi\overline{\pi} = p = 4m+3$ bir asal tam sayı ve $\alpha^{p-1} = \mp i, \mp j, \mp k$ olsun. Bu durumda $n = p-1$ uzunluğunda ki bir $\theta-$devirli kodunun kontrol matrisi

$$H = \begin{pmatrix} \alpha^0 & \alpha^1 & \cdots & \alpha^{p-1} \end{pmatrix} \tag{4.7}$$

olarak tanımlanır.

Örnek 4.2.3. $\pi = 2+i+j+k$ ve $\alpha = 1+i$ olsun. Bu durumda $[6,5,3]$ mükemmel kodu elde edilir. Bu kod Lipschitz ağırlığı 1 olan tüm bir hatalı sözleri düzeltebilir [39].

$\pi \in \mathbb{H}(\mathbb{Z})$ bir asal ve $\pi\overline{\pi} = p = 4m+3 \geq 17$ olmak üzere $\mathbb{H}(\mathbb{Z})_\pi$ üzerinde Lipschit ağırlığı 1 olan bazı iki hatalı vektörleri de düzeltebilen $\theta-$devirli kodlar da tanımlanabilir. $\gamma \in \mathbb{H}(\mathbb{Z})_\pi$ elemanının mertebesi $4n$ olsun. (γ'nın kuvvetler birbirine paralel olmalıdır. Aksi halde burada tanımlanan teknik çalışmaz). $\mathbb{H}(\mathbb{Z})_\pi$ üzerinde bir $\theta-$devirli C kodunun kontrol matrisi $t < n$ olmak üzere;

$$H = \begin{pmatrix} \gamma^0 & \gamma^1 & \cdots & \gamma^{n-1} \\ \gamma^0 & \gamma^5 & \cdots & \gamma^{5(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ \gamma^0 & \gamma^{4t+1} & \cdots & \gamma^{(4t+1)(n-1)} \end{pmatrix} \tag{4.8}$$

şeklinde tanımlanır.

Örnek 4.2.4. $\pi = 4 + k$ alınırsa $\gamma = 1 + k$ seçilebilir. Bu durumda C kodunun kontrol matrisi;

$$H = \begin{pmatrix} \gamma^0 & \gamma^1 & \gamma^2 & \gamma^3 \\ \gamma^0 & \gamma^5 & \gamma^{10} & \gamma^{15} \end{pmatrix}$$

olur. Gelen hatalı vektör $r = \begin{pmatrix} -2 & -2k & 1-i & i \end{pmatrix}$ olsun. Bu durumda

$$S(r) = rH^{tr} = \begin{pmatrix} s_1 \\ s_5 \end{pmatrix} = \begin{pmatrix} -2i \\ -i + j \end{pmatrix} (\mathrm{mod}\ \pi)$$

olur. $\theta_1 = i$ seçilirse $s_1^{'} = \theta_1 s_1, s_5^{'} = \theta_1 s_5$ olup

$$\varepsilon^2 - \left(s_1^{'}\right)^2 \varepsilon + \frac{\left(s_1^{'}\right)^5 - s_5^{'}}{5 s_1^{'}} = 0 \Rightarrow \varepsilon = 1 - k \left(\mathrm{mod}\ \pi\right)$$

olarak elde edilir. Böylece hatanın yerlerini ve değerlerini bulan $\sigma(z)$ polinomunun kökleri γ^3, γ^{10} olarak hesaplanır. Buda hataların $l_1 = 3 \equiv 3 (\mathrm{mod}\, 4)$ olduğunda 4. bileşende ve $l_2 = 10 \equiv 2 (\mathrm{mod}\, 4)$ olduğundan 3. bileşende meydana geldiğini gösterir. 4. bileşendeki hatanın değeri $\theta_1 \gamma^3 / \gamma^3 = i$ ve 3. bileşendeki hatanın değeri $\theta_1 \gamma^{10} / \gamma^2 = -i$ olarak hesaplanır. Böylece gelen söz

$$c = r - e = \begin{pmatrix} -2 & -2k & 1 & 0 \end{pmatrix}$$

şeklinde düzeltilir.

Bu konu hakkında daha geniş bilgi [38, 39] referanslı kaynakta bulunabilir.

4.3. Kuaterniyon Tam Sayıları Üzerinde Kuantum Kodlar İçin Hata Bazları

$\pi \in \mathbb{H}(\mathbb{Z})$ bir asal kuaterniyon sayı, δ Kronecker delta fonksiyonu, $p(x)$ polinomu $\mathbb{Z}_{N(\pi)}[x]$ üzerinde indirgenemez ikinci dereceden bir monik polinom ve α da bu polinomun bir kökü olsun. Bu durumda $f : \mathbb{H}(\mathbb{Z})_\pi \to \mathbb{Z}_{N(\pi)}[x] \big/ \langle p(x) \rangle$'e tanımlı her zaman bir grup homomorfizması vardır. (Çünkü $\mathbb{H}(\mathbb{Z})_\pi$'nin bazları $\{b_1, b_2\} \subset \{1, i, j, k\}$ ve $\mathbb{Z}_{N(\pi)}[x] \big/ \langle p(x) \rangle$'in bazları da $\{a_0, \alpha\}$ şeklinde tanımlanabilir). $a_1, a_2 \in \mathbb{Z}_{N(\pi)}$ olmak üzere bir $b \in \mathbb{H}(\mathbb{Z})_\pi$ elemanı $f(b) = a_1 + a_2\alpha \in \mathbb{F}_{N(\pi)^2}$ olarak yazılabilir. $a \in \mathbb{Z}_{N(\pi)}$ olmak üzere $\mathbb{Z}_{N(\pi)}$ üzerinde Pauli matrisleri

$$\left(X_a\right)_{s,t} = \delta_{t,s+a \pmod{N(\pi)}} \text{ ve } Z_a = \xi^{as \pmod{N(\pi)}} \delta_{s,t} \tag{4.9}$$

şeklinde tanımlanır [4,6,25]. Bu durumda $b \in \mathbb{H}(\mathbb{Z})_\pi$ ve $f(b) = a_1 + a_2\alpha$ olmak üzere $\mathbb{H}(\mathbb{Z})_\pi$ üzerinde hata bazları

$$X_b^{'} = X_{a_1} \otimes X_{a_2} \text{ ve } Z_b^{'} = Z_{N(\pi)-a_1} \otimes Z_{N(\pi)-a_2} \tag{4.10}$$

olarak tanımlanabilir. $\mathbb{H}(\mathbb{Z})_\pi$ üzerindeki bu hata bazları [25] referanslı kaynakta gösterilmiştir. Burada kullanılan f fonksiyonu, $\pi\overline{\pi} = p$ olmak üzere $\mathbb{H}(\mathbb{Z})_\pi$'den $\mathbb{F}_{p^2}$'ye tanımlı bir grup izomorfizmasıdır.

Örnek 4.3.1. $\pi = 1 + i + j$ ve $p(x) = x^2 + x + 1$ olsun. Bu durumda $N(\pi) = 3$ olup, $\mathbb{H}(\mathbb{Z})_\pi = \{0, \mp 1, \mp i, \mp j, \mp k\}$, $\mathbb{F}_9 = \{0, 1, 2, \alpha, 2\alpha, 1+\alpha, 2+2\alpha, 2+\alpha, 1+2\alpha\}$ ve $1 \to 1$, $-i \to 2\alpha$, $-j \to 1+\alpha, j \to 2+2\alpha, -k \to 2+\alpha, i \to \alpha, k \to 1+2\alpha, -1 \to 2, 0 \to 0$ bir eşleme ile $\mathbb{H}(\mathbb{Z})_\pi \cong \mathbb{F}_9$ elde edilir. $\mathbb{Z}_3$ üzerinde hata bazları olarak $\xi = e^{2\pi\iota/p}$, $\iota^2 = -1$ ve $p = N(\pi)$ olmak üzere

$X_0 = I_3 = Z_0$,

$$X_1 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, X_2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, Z_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \xi & 0 \\ 0 & 0 & \xi^2 \end{pmatrix}, Z_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \xi^2 & 0 \\ 0 & 0 & \xi \end{pmatrix}$$

alınabilir.

Bu durumda $\mathcal{H}(\mathbb{Z})_\pi$ üzerinde hata bazları da

$X_0^{'} = I_3 \otimes I_3 = Z_0^{'}$,

$$X_i^{'} = I_3 \otimes X_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

ve aynı yolla

$X_{-1}^{'} = X_2 \otimes I_3, X_i^{'} = I_3 \otimes X_1, X_{-i}^{'} = I_3 \otimes X_2, X_j^{'} = X_2 \otimes X_2,$

$X_{-j}^{'} = X_1 \otimes X_1, X_k^{'} = X_1 \otimes X_2, X_{-k}^{'} = X_2 \otimes X_1$

elde edilir.

İz fonksiyonu $Tr : \mathbb{F}_{p^2} \to \mathbb{Z}_p, a_1 + a_2\alpha \mapsto a_1$ olarak tanımlanır.

$f:\mathbb{H}(\mathbb{Z})_\pi \to \mathbb{F}_{N(\pi)^2} \cong \mathbb{Z}_{N(\pi)}[x]/\langle p(x)\rangle$ bir grup izomorfizması, $f(b)=a_1+a_2\alpha$ ve $f(u)=a_3+a_4\alpha$ olmak üzere, yukarıda $X_b^{'}=X_{a_1}\otimes X_{a_2}$ ve $Z_b^{'}=Z_{N(\pi)-a_1}\otimes Z_{N(\pi)-a_2}$ şeklinde tanımlanan operatörler $|u\rangle$ kuantum haline [25] referanslı kaynakta gösterildiği gibi

$$X_b^{'}|u\rangle=|(u+b)\,(\mathrm{mod}\,\pi)\rangle \text{ ve } Z_b^{'}|u\rangle=\xi^{(a_1a_3+a_2a_4)\,(\mathrm{mod}\,N(\pi))}|u\rangle \tag{4.11}$$

şeklinde etki eder.

Örnek 4.3.2. $\pi=1+i+j$ için yukarıdaki örnekte verilen hata bazları $|k\rangle$ haline aşağıdaki gibi etki eder.

$$X_i^{'}|j\rangle=|(i+j)\,(\mathrm{mod}\,1+i+j)\rangle=|-1\rangle$$

olduğu

$$X_i^{'}|j\rangle=\begin{pmatrix}0&1&0&0&0&0&0&0&0\\0&0&1&0&0&0&0&0&0\\1&0&0&0&0&0&0&0&0\\0&0&0&0&1&0&0&0&0\\0&0&0&0&0&1&0&0&0\\0&0&0&1&0&0&0&0&0\\0&0&0&0&0&0&0&1&0\\0&0&0&0&0&0&0&0&1\\0&0&0&0&0&0&1&0&0\end{pmatrix}\begin{pmatrix}0\\0\\0\\0\\1\\0\\0\\0\\0\end{pmatrix}=\begin{pmatrix}0\\0\\0\\1\\0\\0\\0\\0\\0\end{pmatrix}=|-1\rangle$$

şeklinde hesaplanarak da elde edilebilir. Baz vektörleri olarak

$$|0\rangle=\begin{pmatrix}1\\0\\0\\0\\0\\0\\0\\0\\0\\0\end{pmatrix},|1\rangle=\begin{pmatrix}0\\0\\0\\0\\0\\0\\1\\0\\0\\0\end{pmatrix},|-1\rangle=\begin{pmatrix}0\\0\\0\\1\\0\\0\\0\\0\\0\\0\end{pmatrix},|i\rangle=\begin{pmatrix}0\\0\\1\\0\\0\\0\\0\\0\\0\\0\end{pmatrix},|-i\rangle=\begin{pmatrix}0\\1\\0\\0\\0\\0\\0\\0\\0\\0\end{pmatrix},|j\rangle=\begin{pmatrix}0\\0\\0\\0\\1\\0\\0\\0\\0\\0\end{pmatrix},|-j\rangle=\begin{pmatrix}0\\0\\0\\0\\0\\0\\0\\0\\0\\1\end{pmatrix},$$

$$|k\rangle=\begin{pmatrix}0\\0\\0\\0\\0\\0\\0\\0\\1\\0\end{pmatrix},|-k\rangle=\begin{pmatrix}0\\0\\0\\0\\0\\1\\0\\0\\0\\0\end{pmatrix}$$

alınabilir. Faz hatası örneği olarak da $Z_j^{'}|-k\rangle$ verilebilir. $f(j)=2+2\alpha$ ve $f(-k)=2+\alpha$ olduğundan

$$Z_j^{'}|-k\rangle=\xi^{(2.2+2.1)(\mathrm{mod}3)}|-k\rangle=|-k\rangle$$

olur.

4.4. Kuaterniyonlar Üzerindeki Klasik Kodlardan Kuantum Kod Elde Etme

π bir asal kuaterniyon sayısı, $p = N(\pi)$, α_1 ve α_2 mertebeleri sırasıyla $p-1$ ve $p-1/2$ olan $\mathbb{H}(\mathbb{Z})_\pi$'nin elemanları olsunlar. Bu durumda $x^{p-1/2}+1$ ve $x^{p-1/2}-1$ polinomları

$$x^{p-1/2}+1=(x-\alpha_1)(x-\alpha_1^3)\cdots(x-\alpha_1^{p-2}),$$

$$x^{p-1/2}-1=(x-\alpha_2)(x-\alpha_2^3)\cdots(x-\alpha_2^{p-2})$$

ve

$$x^{p-1}-1=(x-\alpha_1)(x-\alpha_1^3)\cdots(x-\alpha_1^{p-2})(x-\alpha_2)(x-\alpha_2^3)\cdots(x-\alpha_2^{p-2})$$

şeklinde çarpanlarına ayrılır. $x^{p-1}-1$ polinomunun çarpanlarına ayrılışından yararlanılarak $g_1 \mid g_2$ olacak şekilde $g_1, g_2 \in \mathbb{H}(\mathbb{Z})_\pi[x]$ polinomları seçilebilir. Bu polinomlar sırasıyla C_1 ve C_2 devirli kodlarının üreteçleri olarak alınırsa $C_2 \subset C_1$ olur. Bu kodlar sırası ile $[p-1,k_1,d_1]$ ve $[p-1,k_2,d_2]$ parametrelerine sahip olsunlar. Bu durumda $d_2^\perp$, C_2 kodunun diki olan klasik kodun minimum mesafesi ve $d=\min\{d_1,d_2^\perp\}$ olmak üzere bir $[[p-1,k_1-k_2,d]]_\pi$ parametreli kuantum kod vardır. Aşağıdaki teorem bu iddianın ispatı için yeterlidir.

Teorem 4.4.1. C_1 ve C_2 $[n,k_1,d_1]$ ve $[n,k_2,d_2]$ iki klasik lineer kod ve $C_2 \subset C_1$ olsun. Bu durumda bir $[[n,k_1-k_2,d]]_q$ kuantum kodu vardır [25].

Örnek 4.4.1. $\pi = 2+i+j+k$ ve $\alpha_1, \alpha_2 \in \mathbb{H}(\mathbb{Z})_\pi$ olmak üzere $\alpha_1 = 1-i-j-k$ ve $\alpha_2 = -1+i+j+k$ olsun. Bu durumda

$$x^6 - 1 = (x-\alpha_1)(x-\alpha_1^3)(x-\alpha_1^5)(x-\alpha_2)(x-\alpha_2^3)(x-\alpha_2^5)$$

olup

$$g_1(x) = x-(1-i-j-k),$$

$$g_2(x) = x^5 + (i+j+k)x^4 + (-1+i+j+k)x^3 - x^2 - (i+j+k)x - (-1+i+j+k)$$

alınırsa $[[6,4,4]]_{2+i+j+k}$ kuantum kodu elde edilir.

Örnek 4.4.2. $\pi = 1+2i+2j+2k$ ve $\alpha_1, \alpha_2 \in \mathbb{H}(\mathbb{Z})_\pi$ olmak üzere $\alpha_1 = 2$ ve $\alpha_2 = -2+i+j+k$ olsun. Bu durumda

$$x^{12} - 1 = (x-\alpha_1)(x-\alpha_1^3)(x-\alpha_1^5)(x-\alpha_1^7)(x-\alpha_1^9)(x-\alpha_1^{11})$$
$$(x-\alpha_2)(x-\alpha_2^3)(x-\alpha_2^5)(x-\alpha_2^7)(x-\alpha_2^9)(x-\alpha_2^{11})$$

şeklinde çarpanlarına ayrılır. Eğer $g_1(x) = x-\alpha_2$ ve $g_2(x) = (x-\alpha_1)(x-\alpha_1^3)$ $(x-\alpha_1^5)(x-\alpha_1^7)(x-\alpha_1^9)(x-\alpha_1^{11})(x-\alpha_2^3)(x-\alpha_2^5)(x-\alpha_2^7)(x-\alpha_2^9)(x-\alpha_2^{11})$ olarak salınırsa $[[12,10,4]]_{1+2i+2j+2k}$ kuantum kodu, $g_1(x) = x-\alpha_2$ ve $g_2(x) = (x-\alpha_1)(x-\alpha_2)$ alınırsa $[[12,1,4]]_{1+2i+2j+2k}$ kuantum kodu, $g_1(x) = (x-\alpha_1)(x-\alpha_2)$ ve $g_2(x) = (x-\alpha_1)(x-\alpha_2)(x-\alpha_1^3)(x-\alpha_2^3)$ olarak alınırsa $[[12,2,4]]_{1+2i+2j+2k}$ kuantum kodu elde edilir.

Örnek 4.4.3. $\pi = 1+i+j$ olsun. $\mathbb{H}(\mathbb{Z})_{1+i+j}$ üzerinde iki klasik kodun üreteç matrisleri sırası ile

$$G_1 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}, G_2 = \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix}$$

olsun. Bu durumda G_1 matrisinin ürettiği klasik kod C_1 ve G_2 matrisinin ürettiği klasik kod C_2 olmak üzere $C_2 \subset C_1$ ve $C_1^{\perp} \subset C_2^{\perp}$ olur. Teorem 4.4.1'e göre $\left[\left[4,2,2\right]\right]_{1+i+j}$ kuantum kodu elde edilir. Bu kodun kodsözlerinden birisi

$$\left|0_L\right\rangle = \frac{1}{3}\begin{pmatrix} \left|0 \quad 0 \quad 0 \quad 0\right\rangle + \left|1 \quad -1 \quad 1 \quad -1\right\rangle + \left|-1 \quad 1 \quad -1 \quad 1\right\rangle \\ + \left|i \quad -i \quad i \quad -i\right\rangle + \left|-i \quad i \quad -i \quad i\right\rangle + \left|j \quad -j \quad j \quad -j\right\rangle \\ + \left|-j \quad j \quad -j \quad j\right\rangle + \left|k \quad -k \quad k \quad -k\right\rangle + \left|-k \quad k \quad -k \quad k\right\rangle \end{pmatrix}$$

dır. Bu kodun stabilizerlerinden birisi ise $X_1^{'}X_{-1}^{'}X_1^{'}X_{-1}^{'}$'dir. C kuantum kodunun kodsözleri bu stabilizerin etkisi altına değişmez. Yani

$$X_1^{'}X_{-1}^{'}X_1^{'}X_{-1}^{'}\left|0_L\right\rangle = X_1^{'}X_{-1}^{'}X_1^{'}X_{-1}^{'}\frac{1}{3}\begin{pmatrix} \left|0 \quad 0 \quad 0 \quad 0\right\rangle + \left|1 \quad -1 \quad 1 \quad -1\right\rangle + \left|-1 \quad 1 \quad -1 \quad 1\right\rangle + \\ \left|i \quad -i \quad i \quad -i\right\rangle + \left|-i \quad i \quad -i \quad i\right\rangle + \left|j \quad -j \quad j \quad -j\right\rangle + \\ \left|-j \quad j \quad -j \quad j\right\rangle + \left|k \quad -k \quad k \quad -k\right\rangle + \left|-k \quad k \quad -k \quad k\right\rangle \end{pmatrix}$$

$$= \frac{1}{3}\begin{pmatrix} \left|1 \quad -1 \quad 1 \quad -1\right\rangle + \left|-1 \quad 1 \quad -1 \quad 1\right\rangle + \left|0 \quad 0 \quad 0 \quad 0\right\rangle + \\ \left|-j \quad j \quad -j \quad j\right\rangle + \left|k \quad -k \quad k \quad -k\right\rangle + \left|-i \quad i \quad -i \quad i\right\rangle + \\ \left|-k \quad k \quad -k \quad k\right\rangle + \left|j \quad -j \quad j \quad -j\right\rangle + \left|i \quad -i \quad i \quad -i\right\rangle \end{pmatrix}$$

$$= \left|0_L\right\rangle$$

olur. $X_1^{'}X_{-1}^{'}X_1^{'}X_{-1}^{'}$ operatörünün kuantum hallerine nasıl etki ettiği Örnek 4.3.2'de gösterilmektedir. $X_1^{'}X_{-1}^{'}X_1^{'}X_{-1}^{'}$ operatörü matrisi $3^8 \times 3^8$ tipinde bir matristir. Diğer bir stabilizeri ise $Z_1^{'}Z_1^{'}Z_1^{'}Z_1^{'}$'dir. Bu $Z_1^{'}Z_1^{'}Z_1^{'}Z_1^{'}$ stabilizeri de

$$|0_L\rangle = \frac{1}{3}\begin{pmatrix} |0 \quad 0 \quad 0 \quad 0\rangle + |1 \quad -1 \quad 1 \quad -1\rangle + |-1 \quad 1 \quad -1 \quad 1\rangle \\ +|i \quad -i \quad i \quad -i\rangle + |-i \quad i \quad -i \quad i\rangle + |j \quad -j \quad j \quad -j\rangle \\ +|-j \quad j \quad -j \quad j\rangle + |k \quad -k \quad k \quad -k\rangle + |-k \quad k \quad -k \quad k\rangle \end{pmatrix}$$

kodsözüne etki etmez. Yani

$$Z_1^{'}Z_1^{'}Z_1^{'}Z_1^{'}|0_L\rangle = Z_1^{'}Z_1^{'}Z_1^{'}Z_1^{'}\left[\frac{1}{3}\begin{pmatrix} |0 \quad 0 \quad 0 \quad 0\rangle + |1 \quad -1 \quad 1 \quad -1\rangle + |-1 \quad 1 \quad -1 \quad 1\rangle \\ +|i \quad -i \quad i \quad -i\rangle + |-i \quad i \quad -i \quad i\rangle + |j \quad -j \quad j \quad -j\rangle \\ +|-j \quad j \quad -j \quad j\rangle + |k \quad -k \quad k \quad -k\rangle + |-k \quad k \quad -k \quad k\rangle \end{pmatrix}\right]$$

$$= \frac{1}{3}\begin{pmatrix} |0 \quad 0 \quad 0 \quad 0\rangle + \xi\xi^2\xi\xi^2|1 \quad -1 \quad 1 \quad -1\rangle + \xi^2\xi\xi^2\xi|-1 \quad 1 \quad -1 \quad 1\rangle \\ +|i \quad -i \quad i \quad -i\rangle + |-i \quad i \quad -i \quad i\rangle + \xi^2\xi\xi^2\xi|j \quad -j \quad j \quad -j\rangle \\ +\xi\xi^2\xi\xi^2|-j \quad j \quad -j \quad j\rangle + \xi\xi^2\xi\xi^2|k \quad -k \quad k \quad -k\rangle \\ +\xi^2\xi\xi^2\xi|-k \quad k \quad -k \quad k\rangle \end{pmatrix}$$

$$= \frac{1}{3}\begin{pmatrix} |0 \quad 0 \quad 0 \quad 0\rangle + |1 \quad -1 \quad 1 \quad -1\rangle + |-1 \quad 1 \quad -1 \quad 1\rangle \\ +|i \quad -i \quad i \quad -i\rangle + |-i \quad i \quad -i \quad i\rangle + |j \quad -j \quad j \quad -j\rangle \\ +|-j \quad j \quad -j \quad j\rangle + |k \quad -k \quad k \quad -k\rangle + |-k \quad k \quad -k \quad k\rangle \end{pmatrix}$$

$$= |0_L\rangle$$

olur. Bu kod mantıksal bazlar cinsinden

$$|1_L\rangle = X_1' X_1' X_1' X_1' \frac{1}{3}\begin{pmatrix} |0\ \ 0\ \ 0\ \ 0\rangle + |1\ \ -1\ \ 1\ \ -1\rangle + |-1\ \ 1\ \ -1\ \ 1\rangle + \\ |i\ \ -i\ \ i\ \ -i\rangle + |-i\ \ i\ \ -i\ \ i\rangle + |j\ \ -j\ \ j\ \ -j\rangle + \\ |-j\ \ j\ \ -j\ \ j\rangle + |k\ \ -k\ \ k\ \ -k\rangle + |-k\ \ k\ \ -k\ \ k\rangle \end{pmatrix}$$

$$= \frac{1}{3}\begin{pmatrix} |1\ \ 1\ \ 1\ \ 1\rangle + |-1\ \ 0\ \ -1\ \ 0\rangle + |0\ \ -1\ \ 0\ \ -1\rangle + \\ |-j\ \ k\ \ -j\ \ k\rangle + |k\ \ -j\ \ k\ \ -j\rangle + |-i\ \ -k\ \ -i\ \ -k\rangle + \\ |-k\ \ -i\ \ -k\ \ -i\rangle + |j\ \ i\ \ j\ \ i\rangle + |i\ \ j\ \ i\ \ j\rangle \end{pmatrix}$$

olup

$$a|0_L\rangle + b|1_L\rangle \ \left(|a|^2 + |b|^2 = 1\right)$$

olarak yazılır.

BÖLÜM 5. TARTIŞMA VE ÖNERİLER

Bu tezde ikili kuantum kodlar ve ikili olmayan kuantum kodlar incelenmiş ve kuantum kodların klasik kodlardan elde edildiği ve kuantum kodların hata düzeltme kabiliyetlerinin klasik kodlara bağlı olduğu görülmüştür. Bu çalışmada ortaya konulan problemler ve çözümleri şöyle sıralanabilir.

Gauss tam sayıları üzerinde tanımlı C_1 ve C_2 klasik kodlarının $C_2 \subset C_1$ şartını sağladığı durumlar araştırılmakta ve bu kodlar vasıtası ile kuantum kodlar elde edilmektedir. Ayrıca Gauss tam sayıları üzerindeki kuantum kodlar için iyi hata bazları tanımlanmaktadır. Gauss tam sayıları üzerinde elde edilen kuantum kodların klasik anlamda MDS oldukları görülmektedir. Mannheim metriğine göre oluşturulan klasik kodlar üzerinden elde edilen kuantum kodların daha fazla hata düzeltebildiği gösterilmektedir. Buradan elde edilen sonuçlar makale haline getirilmiş ve uluslar arası bir dergide yayına kabul edilmiştir [40].

Kuaterniyon tam sayıları üzerinde tanımlı C_1 ve C_2 klasik kodlarının $C_2 \subset C_1$ şartını sağladığı durumlar incelenmekte ve bu kodlar vasıtasıyla kuantum kodlar elde edilmektedir. Ayrıca kuaterniyon tam sayıları üzerinde yazılan kuantum kodlar için iyi hata bazlar kümesi de tanımlanmaktadır. Kuaterniyonlar üzerinde tanımlanan bu klasik kodlar vasıtasıyla elde edilen kuantum kodların daha fazla bit flip ve faz flip hata düzeltebildiği gösterilmektedir. Buradan elde edilen sonuçlar makale haline getirilmiş ve uluslar arası bir dergide yayına kabul edilmiştir [41].

Konu ile ilgili açık problemler halen mevcuttur. Örneğin bu farklı metriklere göre tanımlanan kuantum kodlar için yeniden bir kuantum kanalı inşa edilebilir. Ayrıca Gauss ve kuaterniyon tam sayıları üzerindeki hem klasik kodlar için hem de kuantum kodlar için Mannheim ve Lipschitz metriğine göre sınır çalışmaları yapılabilir.

KAYNAKLAR

[1] ABUALRUB, T., GHRAYEB, A., XIANG, N. Z., Construction of cyclic codes over $GF(4)$ for DNA computing, Journal of the Franklin Institute, pp. 448-457, 2006.

[2] ALY, S. A., GRASSL, M., KLAPPENECKER, A., RÖTTELER, M., SARVEPALLI, P. K., Quantum convolutional BCH codes, in 10^{th} Canadian Workshop on Information Theory, CWIT'07, pp. 180-183, 6-8 Jun. 2007,.

[3] ALY, S. A., A note on quantum Hamming bound, arXiv:quant-ph/0711.4603, Nov. 2007.

[4] ARVIND, A., KURUR, P. P., PARTHASARATHY, K. R., Nonstabilizer quantum codes from Abelian subgroups of the error group, Quantum Physics e-print, quant-ph/0210097, 2002.

[5] ASHIKHMIN, A. E., LITSYN, S., Upper bound on the size of quantum codes, IEEE Trans. Inform, vol. 45, no.4, pp. 1206-1215, 1999.

[6] ASHIKHMIN, A. E., KNILL, E., Nonbinary quantum stabilizer codes, IEEE Trans. Inform. Theory, vol. 47, no. 7, pp. 3065-3072, 2001.

[7] BERLEKAMP, E. R., Algebraic coding theory, New York: McGraw-Hill, 1968.

[8] BETH, T., GRASSL, M., The quantum Hamming and hexacodes, Fortschr. Phys., 46(4-5): 459-491, 1998.

[9] CALDERBANK, A. R., RAINS, E. M., SHOR, P. W., SLOANE, N. J. A., Quantum error correction and orthogonal geometry, Phys. Rev. Lett., 76: 405-409, 1997.

[10] CALDERBANK, A. R., SHOR, P. W., Good quantum error-correcting codes exist, Phys. Rev. A., 54: 1098-1105, 1996.

[11] CALDERBANK, A. R., RAINS, E. M., SHOR, P. W., SLOANE, N. J. A., Quantum error correction via codes over $GF(4)$, IEEE Trans. Inform. Theory, 44: 1369-1387, 1998.

[12] CLEVE, R., Quantum stabilizer codes and classical linear codes, Phys. Rev. A., vol. 55, no. 6, pp. 4054-4059, 1997.

[13] ÇALLIALP, F., Örneklerle Soyut Cebir, Birsen yayınevi, 2001.

[14] DAVIDOFF, G., SARNAK, P., VALETTE, A., Elementary number theory, group theory, and Ramanujan graphs, Cambridge University Pres, 2003.

[15] DUMMIT, D. S., FOOTE, R. M., Abstract algebra, John Wiley & Sons, Inc., 2004.

[16] FENG, K., Quantum codes $\left[\left[6,2,3\right]\right]_p$, $\left[\left[7,3,3\right]\right]_p$ $\left(p \geq 3\right)$ exist, IEEE Trans. Inform. Theory, vol. 48, no. 8, pp. 2384-2391, 2002.

[17] FENG, K., MA, Z., A finite Gilbert-Varshamov bound for pure stabilizer quantum codes, IEEE Trans. Inform. Theory, vol. 50, no. 12, pp. 3323-3325, 2004.

[18] GOTTESMAN, D., A class of quantum error-correcting codes saturating the quantum Hamming bound, Phys. Rev. A, vol. 54, pp. 1862-1868, 1996.

[19] GOTTESMAN, D., Fault-tolerant quantum computation with higher-dimensional systems, Chaos, Solitons, Fractals, 10(10): 1749-1758, 1999.

[20] GRASSL, M., BETH, T., Cyclic quantum error-correcting codes and quantum shift registers, in Proc. Royal Soc. London Series A, vol. 456, no. 2003, pp. 2689-2706, 2000.

[21] GRASSL, M., BETH, T.,RÖTTELER, M., On optimal quantum codes, Internat. J. Quantum Information, 2(1): 757-775, 2004.

[22] HORN, R.A., JOHNSON, C.R., Matrix analysis, Cambridge University Press, Cambridge, 1985.

[23] HUBER, K., Codes over Gaussian integers, IEEE Trans. Inform. Theory, vol. 40, pp. 207-216, 1994.

[24] KAYE, P., LAFLAMME, R., MOSCA, M., An introduction to quantum computing, Oxford Unv. Press, 2007.

[25] KETKAR, A., KLAPPENECKER, A., KUMAR, S., SARVEPALLI, P., Nonbinary stabilizer codes over finite fields, IEEE Trans. Inform. Theory, vol. 52, no. 11, pp. 4892-4914, 2006.

[26] KIM, J. L., WALKER, J., Nonbinary quantum error-correcting codes from algebraic curves, submitted to a special issue of Com^{2}MaC Conference on Association Schemes, Codes and Designs in Discrete Math., 2004.

[27] KNILL, E., Group representations, error bases and quantum codes, Los Alamos National Laboratory Report LAUR-96-2807, 1996.

[28] KNILL, E., Non-binary unitary error bases and quantum codes, Los Alamos National Laboratory Report LAUR-96-2717, 1996.

[29] LAFLAMME, R., MIQUEL, C., PAZ, J. P., ZUREK, W. H., Perfect quantum eror correcting code, arxive: quant-ph9602019, 1996.

[30] Lİ, R., Binary construction of quantum codes of minimum distance three and four, IEEE Trans. Inform. Theory, vol. 50, no. 6 Jun. 2004.

[31] MACWILLIAMS, F. J., SLOANE, N. J., The theory of error correcting codes, North Holland Pub. Co., 1977.

[32] MARTINEZ, C., BEIVIDE, R., GABIDULIN, E. M., Perfect codes from Cayley graphs over Lipschitz integers". IEEE Trans. Inf. Theory, Vol. 55, No. 8, Aug. 2009.

[33] MATSUMOTO, R., UYEMATSU, T., Constructing quantum error correcting codes for $p^m -$ state systems from classical error correcting codes, IEICE Trans. Fundamentals, vol. E83-A, no. 10, pp. 1878-1883, 2000.

[34] NETO, T.P. da N., Lattice constellations and codes from quadratic number fields, IEEE Trans. Inform. Theory, vol. 47, pp. 1514-1527, May 2001.

[35] NIELSEN, M. A., CHUANG, I. L., Quantum computation and quantum information, Cambridge: Cambridge University Press, 2000.

[36] OLLIVIER, H., TILLICH, J. P., Description of a quantum convolutional code, Phys. Rev. Lett., vol. 91, no. 17, pp. 1779 021-4, 2003.

[37] OSKIN, M., http://www.cs.washington.edu/homes/oskin/quantum-notes.pdf pp. 22-27, 22.03.2010

[38] ÖZEN, M., GÜZELTEPE, M., Cyclic codes over some finite quaternion integer rings, Journal of the Franklin Ins., doi:10.1016/j.jfranklin.2010.02.008.

[39] ÖZEN, M., GÜZELTEPE, M., Codes over quaternion integers with respect to Lipschitz metric, arXiv:0905.4160v4, 2010.

[40] ÖZEN, M., GÜZELTEPE, M., Quantum codes from codes over Gaussian integers with respect to the Mannheim metric, Antarct. J. Math., (in press)

[41] ÖZEN, M., GÜZELTEPE, M., Quantum codes from codes over Lipschitz integers, Glob. J. Pure Appl. Math., (in press).

[42] RAINS. E., Nonbinary quantum codes, IEEE Trans. Inform. Theory, vol. 45, no. 6, pp. 1827-1832, 1999.

[43] ROMAN, S., Coding and information theory, Graduate Texts in Mathematics, Springer Verlag, 1992.

[44] RÖTTELER, M., GRASSL, M., BETH, T., On quantum MDS codes, in Proc. 2004 IEEE Intl. Symposium on Information Theory, Chicago, USA, p.355, 2004.

[45] SHOR, P. W., Scheme for reducing decoherence in quantum memory, Phys. Rev. A, vol.2 pp. 2493-2496, 1995.

[46] STEANE, A. M., Multiple-particle interference and quantum error correction, in Proc. Roy. Soc., London A, vol. 452, pp. 1551-2577, 1996.

[47] STEEB, W. H., HARDY, Y., Problems and solutions in quantum computing and quantum information, World Scientific Publishing Co. Pte. Ltd., Singapore, 2007.

[48] TANGARAJ, A., Quantum codes from cyclic codes over $GF\left(4^m\right)$, IEEE Trans. Inform. Theory, vol. 47, no. 3, pp. 1176-1178, 2001.

[49] TONCHEV, V. D., Quantum codes from caps, Discrete Mathematics, 3008, pp. 6368-6372, 2008.

[50] ZENG, G., LI, Y., GUO, Y., LEE, M. H., Stabilizer quantum codes over Clifford algebra, Journal of Physics A: Math. Theor. vol. 41 no. 145304, 2008.

ÖZGEÇMİŞ

Murat GÜZELTEPE, 01.01.1978 tarihinde Erzurum'un Hınıs ilçesinde doğdu. İlk, orta ve lise eğitimini 1995 yılında Erzurum'da tamamladı. 1996 yılında Atatürk Üniversitesi Fen Edebiyat Fakültesi Matematik Bölümü'nde lisans eğitimine başladı ve buradan 2000 yılında mezun oldu. 2004 yılında Sakarya Üniversitesi Fen Bilimleri Enstitüsü Matematik EABD'da yüksek lisans programına kaydoldu ve 2007 yılında buradan mezun oldu. 2007 yılında Sakarya Üniversitesi Fen Bilimleri Enstitüsü Matematik EABD'da doktora programına kaydoldu. Eylül 2000 ile Aralık 2006 tarihleri arasında Milli Eğitim Bakanlığı'na bağlı çeşitli eğitim kurumlarında ve bazı illerde matematik öğretmenliği yaptı. Aralık 2006 da Sakarya Üniversitesi Fen Edebiyat Fakültesi Matematik Bölümü'nde Araştırma Görevlisi olarak göreve başladı ve halen bu görevini sürdürmektedir. Evli ve iki çocuk babası olan Murat GÜZELTEPE'nin yabancı dili İngilizcedir.