ANKARA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

KUANTUM HATA DÜZELTME

Haydar KIZILIRMAK

FİZİK ANABİLİM DALI

ANKARA
2020

TEZ ONAYI

Haydar KIZILIRMAK tarafından hazırlanan "**Kuantum Hata Düzeltme**" adlı tez çalışması 22/01/2020 tarihinde aşağıdaki jüri tarafından oy birliği ile Ankara Üniversitesi Fen Bilimleri Enstitüsü Fizik Anabilim Dalı'nda **YÜKSEK LİSANS** olarak kabul edilmiştir.

Danışman : Prof. Dr. Abdullah VERÇİN
Ankara Üniversitesi Fizik Anabilim

Jüri Üyeleri:

Başkan: Prof. Dr. Abdullah VERÇİN
Ankara Üniversitesi Fizik Anabilim Dalı

Üye : Prof. Dr. İnanç ŞAHİN
Ankara Üniversitesi Fizik Anabilim Dalı

Üye : Doç. Dr. İsmet YURDUŞEN
Hacettepe Üniversitesi Uygulamalı Matematik Anabilim Dalı

Yukarıdaki sonucu onaylarım.

Prof. Dr. Özlem YILDIRIM
Enstitü Müdürü

ETİK

Ankara Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına uygun olarak hazırladığım bu tez içindeki bütün bilgilerin doğru ve tam olduğunu, bilgilerin üretilmesi aşamasında bilimsel etiğe uygun davrandığımı, yararlandığım bütün kaynakları atıf yaparak belirttiğimi beyan ederim.

22/01/2020

Haydar KIZILIRMAK

ÖZET

Yüksek Lisans Tezi

KUANTUM HATA DÜZELTME

Haydar KIZILIRMAK

Ankara Üniversitesi
Fen Bilimleri Enstitüsü
Fizik Anabilim Dalı

Danışman: Prof. Dr. Abdullah VERÇİN

Kuantum hata düzeltme, kuantum bilişim süreçlerinin çıktılarının güvenilirliğini temin edeceği için çok önemlidir. Kuantum bilişimde ve kuantum iletişimde kullanılan "bilgi taşıyıcılar" yani kübitler için; başlangıç koşulları, çevreyle ve diğer sistemlerle etkileşim, kanal gürültüsü gibi süreçlerin ve öze-uygunluk değişkeninin kullanılan kuantum devreler boyunca izlenmesi gerekmektedir. Çünkü bir adımda kaybedilen korelasyonun sonraki adımda kazanılması söz konusu değildir. Arzulanan yükümlülükleri yerine getirebilmek için, etkileşim sonucu değişmiş olan kodlanmış bilgi eski haline özüne uygun biçimde döndürülmelidir. Bu sebeple, bilişim sürecinin başlangıcından bitimine kadar kuantum durumların maruz kalabileceği istenmeyen dönüşümleri geri dönüştürmek veya önüne geçmek için kuantum hata düzeltme kodları her devre algoritması ve protokole ilave edilmektedir. Bu çalışmada, Kuantum hata düzeltme yöntemlerinin temelleri, işleyiş mekanizmaları ve bu mekanizmaların kuantum geçitler yoluyla hayata geçirilmesi ve kuantum devrelere uygulanması ele alınmıştır. Kuantum hata modelleri ve en genel hata türü olarak Kraus işlemcileri ve kübit özel durumları; kübit-dönüşü, faz-dönüşü ve bit-faz dönüşü gibi hata modelleri ve bunları azaltacak kuantum hata düzeltme kodları incelenmiştir.

Ocak 2020, 68 sayfa

Anahtar Kelimeler: Kuantum bilişim kuramı, Kuantum bilgisayım kuramı, Klasik hata düzeltme, Kuantum hata düzeltme, Kuantum hata düzeltme kodları, Kararlılaştırıcı kodlar, Hata işlemcileri

ABSTRACT

Master Thesis

QUANTUM ERROR CORRECTION

Haydar KIZILIRMAK

Ankara University
Graduate School of Natural and Applied Sciences
Department of Physics

Supervisor: Prof. Dr. Abdullah VERÇİN

Quantum error correction is very important since it will ensure the reliability of quantum information processes outputs. For the information carriers, qubits in our examples, that are used in quantum computing and quantum communication; processes such as initial conditions, interactions with the environment or other systems, channel noise and fidelity variable should be monitored throughout the quantum circuits. Because the correlation lost in one step cannot be gained in the next steps. In order to fulfill the desired tasks, the encoded information that has changed as a result of the interaction must be transformed to its original state. For this reason, quantum error correction codes are added to each circuit algorithm and protocol to prevent or recover from unwanted transformations to which quantum states may be exposed throughout the computing process. In this study, fundamentals of quantum error correction methods, functioning mechanisms and implementation through quantum gates and application to quantum circuits are discussed. Quantum error models, Kraus operators as the most common error type and special cases for qubits such as qubit-flip, phase-flip and bit-phase flip and quantum error correction codes to reduce them are examined.

January 2020, 68 pages

Key Words: Quantum information theory, Quantum computation theory, Classical error correction, Quantum error correction, Quantum error correction codes, Stabilizer codes, Error operators

TEŞEKKÜR

Sayın hocam Prof. Dr. Abdullah VERÇİN'e saygılarımı ve sevgilerimi sunar, bilgi ve deneyimleriyle her zaman yanımda olduğu için en içten dileklerimle teşekkür ederim. Yardımlarını hiç esirgemeyen ve hep yanımda olan anne ve babama, tez ve ders aşamasında yanımda bulunan sabır ve hoşgörüyle beni destekleyen biricik eşim Duygu Demir KIZILIRMAK'a ve ailesine teşekkür ederim.

Haydar KIZILIRMAK
Ankara, Aralık, 2019

İÇİNDEKİLER

SİMGELER VE KISALTMALAR DİZİNİ

$\otimes$	Tensörel çarpım

Kısaltmalar

$\mathcal{H}$	Hilbert Uzayı
$\|0\rangle, \|\uparrow\rangle$	Spin yukarı durumu
$\|1\rangle, \|\downarrow\rangle$	Spin aşağı durumu
$\|\pm\rangle = \frac{\|0\rangle \pm \|1\rangle}{\sqrt{2}}$	Hadamard bazları
$\|0\rangle_L, \|1\rangle_L$	Mantıksal kübitler
$\langle A\rangle_\psi$	A gözlenebilirinin ψ durumundaki beklenen değeri
α, β	Kompleks katsayılar
I	Birim matris
$\boldsymbol{H}$	Hamilton işlemcisi
$\sigma_x, \sigma_y, \sigma_z$	Pauli spin matrisleri
$A^\dagger$	A işlemcisinin Hermite-sel eşleniği
$\|\Psi\rangle$	Keyfi durum vektörü
$\|\Psi\rangle_{AB}$	Altsistemleri A ve B olan iki-parçalı bir sistemin durum vektörü
ρ	Yoğunluk işlemcisi
ρ_{AB}	Altsistemleri A ve B olan iki-parçalı bir sistemin yoğunluk işlemcisi
ρ_A, ρ_B	İki-parçalı bir sistemin indirgenmiş (marjinal) yoğunluk işlemcileri
F	Öze-uygunluk
P_i	i. izdüşüm işlemcisi
$S(\rho)$	Herhangi bir ρ yoğunluk işlemcisinin Shannon entropisi

CPTP	Tamamen pozitif ve iz koruyan gönderim (Completely Positive and Trace Preserving)
Tr	İz işlemi
D_t	İz-mesafesi
$CNOT$	Kontrollü-değilleme geçidi (Controlled-NOT)
$SWAP$	Değiş-tokuş işlemini sağlayan geçit
$CCNOT$	Çift kontrollü-değilleme geçidi (Controlled-Controlled-NOT)
$EPR\ çifti$	Einstein-Podolsky-Rosen çifti
NMR	Nükleer Manyetik Rezonans
$SPB\ Yuvarı$	Kübitleri görselleştirmek için kullanılan Stokes – Poincaré – Bloch yuvarı
$\boldsymbol{r}$	Bloch vektörü
NOT	Klasik bilişimde kullanılan değilleme geçidi
AND	Klasik bilişimde VE mantıksal işlemini yerine getiren geçit
$NAND$	Klasik bilişimde kullanılan NOT ve AND geçitlerinin birleşimi olan geçit

ŞEKİLLER DİZİNİ

ÇİZELGELER DİZİNİ

1. GİRİŞ

Geleceğin kuantum teknolojilerinin temellerini oluşturan kuantum bilişim ve kuantum bilgisayım kuramları, 1990'lı yılların başından beri yoğun olarak araştırılmaktadır. Burada temel ilke, bazı kuantumlu sistemlerin iki seviyeli durumlarını kübitlere (*qubit*) kodlayarak onları klasik bilgisayımda olduğu gibi hesaplamasal bitler şeklinde kullanıp bilişimin önemli süreçlerini gerçekleştirmektir. Kuantum durumlarının uz-aktarımı (*teleportation*), kuantum yoğun kodlama (*dense-coding*), kuantum kriptoloji ve diğer stratejik ve güvenlik açısından önemli kuantum bilişim süreçlerinin gerçekleşmesi hep aynı ilkelere sadık kalınarak sağlanır.

Her bilişim sürecinin kendine özgü zorlukları vardır. Kuantum bilişimdeki en temel zorluk kuantumlu sistemlerin hızlı zedelenebilir, bozulabilir ve kırılgan (*fragile*) yapıda olmasıdır. Böyle durumlar sistemlerde kuantum hatalar meydana gelmesine sebep olur. Bu hataların sebebi kimi zaman kullanılan kuantum geçitler, etkileşime giren diğer bir sistem, çevre veya verinin iletildiği ortam ve daha birçok başka etken olabilir.

Bilişim sürecine ve sürecin çıktılarına olan güvenin en üst düzeyde olması için hata düzeltme şarttır. Klasikte olduğu gibi kuantum bilişimde de bilgi taşıyıcıların hatalara karşı korunması, oluşan hataların düzeltilmesi veya bu hataların belirli eşiklerde tolere edilebilmesi için önemli mekanizmalar üretilmiştir. Kuantum mantık geçitleri kullanarak, öngörülen hata türleri için bu tarz mekanizmalar kuantum devrelere dahil edilir.Deneysel olarak kuantum geçitlerin elde edilmesi çok kolay değildir. Çok özel laboratuar şartları altında üretilmiş geçitler olduğu uluslararası literatürde mevcuttur ve çalışmalar hız kesmeden devam etmektedir.

Bu tez çalışmasında, klasik bilişim süreci, klasik hata türleri ve hata düzeltme yöntemlerinden başlayan ve kuantum hata düzeltme kodlarına varan bir yol haritası çizmeye çalışılmıştır.

İkinci bölümde; klasik anlamda (kodlanmış) bilgi, bilgiye bakış açısı ve bize kazandırdıklarına değindikten sonra klasik mantık geçitlerinden bahsedilmektedir. Klasik bilişimde karşılaşılan hata türleri ve gerçek hayattan örneklerle temel klasik hata düzeltme yöntemlerine örnekler verdikten sonra çizgisel ikili kodlara kısaca değinilmiştir.

Üçüncü bölümde; kuantum bilişimin temelleri kübit ve SPB yuvarından, saf ve saf olmayan durumlardan bahsedilerek bunların yoğunluk işlemcileri ve bu işlemcilerin özellikleri sıralanmıştır. Kuantum bilişimin başarı ölçütlerinden iz mesafesi ve öze-uygunluk konularına ek olarak kuantum dolanıklık, parçalı iz yöntemi, üniter dönüşümler ve DiVincenzo kriterleri bu bölümde ele alınmıştır. Son kısım, 1 kübit ve çoklu kübit kuantum geçitleri, geçitlerin devre şemasındaki gösterimleri ve kübitlere uygulanış biçimlerine ayrılmıştır.

Dördüncü bölümde; dekoherans tanımıyla başlayarak kübit özel durumları için en genel kuantum hata türleri: kübit-dönüşü, faz-dönüşü, bit-faz dönüşü, kutuplanma yitimi, genlik sönümlenmesi, faz sönümlenmesi hata modellemelerine değinilmiştir. Bu hataların giderilmesi açısından kuantum hata düzeltme işleminin önündeki engeller tartışılmış ve bu yolda en çok başvurulan işçi kübitler konusuna değinilmiştir.

Beşinci bölümde; kuantum hata düzeltme kriteri ve hata düzeltici kodların temel özelliklerinden bahsettikten sonra basitten karmaşığa doğru temel kuantum hata düzeltme kodu örnekleri olarak: kübit-dönüşü için tekrarlı 3-kübit kodu, faz-dönüşü için tekrarlı 3-kübit kodu, faz-yitimi modeli ve Shor'un 9-kübit hata düzeltme kodları sunulmuştur.

2. KLASİK BİLGİSAYIM

2.1 Klasik Anlamda (Kodlanmış) Bilgi Nedir?

Çoğu insan bilgi için; yeni öğrenilen şeyler üzerinden bir tanım getirir. Bu tanım çok öznel, sayımı zor ve içeriğe bağımlıdır. Bilginin gösterimini böyle öznel bazda yapmak matematiksel olarak sıkıntılıdır. Yani bilginin iletişim eylemi esnasında alınması şeklindeki ortak mantık pratikte fayda sağlamaz. Bu konuya bilişim süreçleri açısından yaklaşan Claude Shannon bu eksikliği fark etmiş ve bu konudaki eksikliği çok nazik bir dokunuşla ortadan kaldırmıştır.

Claude Shannon bilgi dendiğinde ne kastedildiğine dair alternatif bir görüş ortaya atmıştır. Shannon için; bilgi, bir mesajı iletmek için gerekli minimum sayıdaki 0'lar ve 1'lerden başka bir şey değildir. (Shannon 1948)

Shannon'un bu görüşü sıradan insanınkinden çok farklıydı. Ama böyle bir çerçeve sayesinde; her şey ikili sayı sistemindeki bitlere karşılık gelen 0 ve 1'e çevrilerek veri olarak tanımlanabilir. Bu tanım; bilgiyi bir mesajı temsil etmek için gerekli minimum kaynaklara eşitleyerek, bilgi miktarının mesajları sıkıştırarak veya gürültülü iletişim kanallarında göndererek nasıl değişeceğine dair kurallar tanımlanmasını mümkün kıldı. Claude Shannon'un temel bilgi birimi olarak Bit'leri tanımlaması bilgi teorisinin temelini oluşturdu. Sonunda, bilginin böyle anlaşılması; verilerin sıkıştırılması, şifrelenmesi ve telekomünikasyon alanlarında çığır açtı.

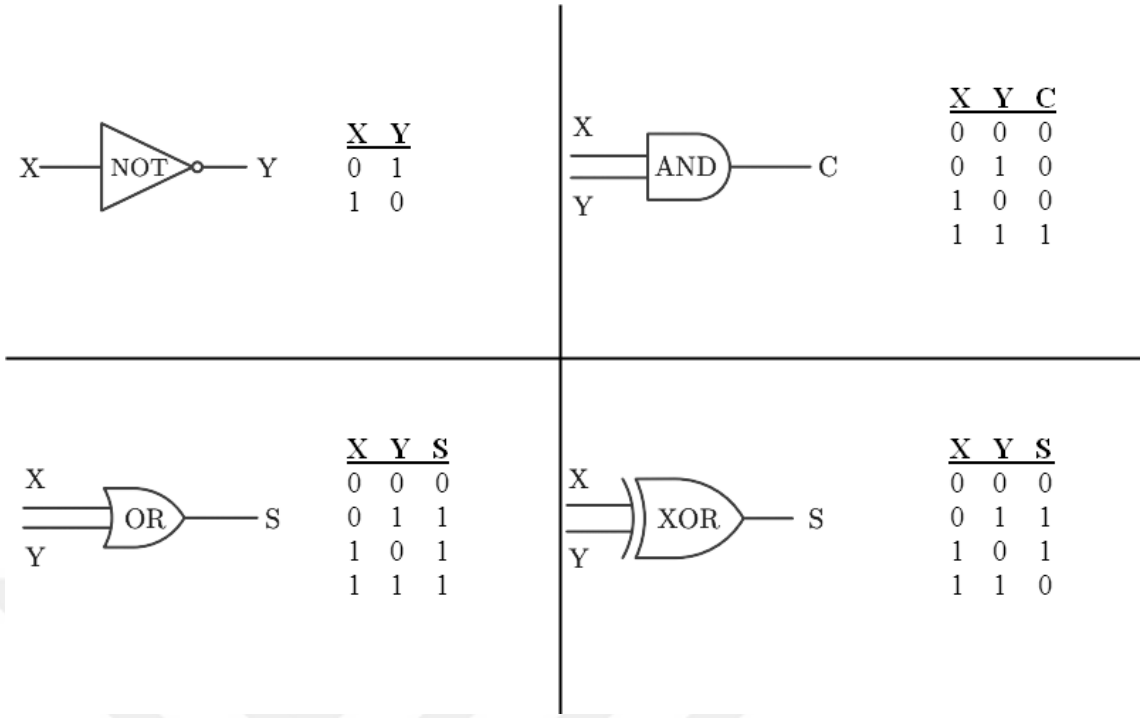
2.2 Klasik Mantık Geçitleri

Bilgi, klasik fizik yasalarına uyan fiziksel sistemlere kodlandığında; Klasik Bilgi adını alır. Klasik bilginin dönüşümü mantık işlemleriyle gerçekleştirilir. Mantık geçitleri bu mantık işlemlerini yerine getirmekle yükümlüdür. Klasik bilgisayarlarda yapılmak istenen işlemler temel işlem basamaklarına bölünerek gerçekleştirilir. Bu temel işlem

basamakları mantık geçitleri ile sağlanır. Mantık geçitleri, bitleri bir durumdan alıp başka bir duruma götüren mantıksal işlemlerdir. Mantık geçitlerinin birleştirilmesi ve farklı kombinasyonları ile mantık devreleri oluşturulur.

19. yüzyılda matematikçi George Boole doğruluk tablolarını kullanarak karmaşık ifadeleri daha küçük mantıksal birimlerine ayrıştıran sistematik bir yöntem ortaya çıkarttı. Boole'nin bu konudaki çalışmaları bilgisayarlara işlem yapabilme kapasitesi sağlayan mantık geçitlerini ortaya çıkarttı ve bu geçitler "Boolean mantık geçitleri" adını aldı.

Temel mantık geçitleri; NOT(değil), AND(ve) ve OR(veya) mantık geçitleridir. Çıktı olarak elde edilen değerlerden benzersiz (biricik, tek) bir şekilde girdi değerleri elde edilebiliyorsa; geçit *tersinebilir*dir denir. Bunun en temel işareti eşit sayıda girdi ve çıktı olmasıdır. AND ve OR mantık geçitleri 2 bitlik giriş ve tek bitlik çıkışa sahip, tersinemez mantık geçitleridir. NOT mantık geçidi ise tek bitlik giriş ve çıkışa sahip tersinebilir bir mantık geçididir. OR, AND ve diğer Boolean geçitleri genellikle tersinemezdir. Örneğin AND geçidinin sonuna AND^{-1} olarak tanımlı AND geçidinin orijinal girdilerini vermesi umulan bir geçit eklensin. AND^{-1}'in aynı girdi için farklı birçok gönderim yaptığı görülür ki bu mantıklı değildir. Buna karşın, NOT geçidi girdi ve çıktı sayısı eşit olan bir klasik geçittir ve $NOT * NOT = 1$ ve $NOT^{-1} = NOT$olduğu için tersine işleme izin verir. Bu sebeple klasik NOT geçidi tersinebilirdir. Mantık geçitlerinin etkisi doğruluk çizelgesi ile açıklanabilir.Örneğin, NOT, OR, XOR ve AND geçitlerinin doğruluk tabloları ve görsel temsilleri aşağıdaki şekilde ifade edilmektedir:



Şekil 2.1 NOT, OR, XOR VE AND geçitleri ve doğruluk tabloları

Tersinemeyen geçitlerde girdi değerleri geri getirilemez şekilde silinmektedir. Bu silme işlemi enerji yitimi olarak karşımıza çıkmaktadır. Bir bitlik bilginin silinmesi için en az Landauer Limiti "$kTln2$" kadar enerji gerekir.

Bu temel mantık geçitleri ile daha karmaşık mantık geçitleri de yapılabilir. Bunlar; NOR (NOT OR), NAND (NOT AND) ve XOR (eXlusive OR) mantık geçitleri şeklinde örneklendirilebilir. Bu mantık geçitlerinden XOR, koşullu bir NOT geçidir ve kontrollü bir mantık geçidini temsil eder. Burada ilk bit kontrol bit, ikinci bit hedef bit olarak işlem görür ve kontrol bit '1' durumunda iken hedef bite NOT geçidi uygulanmakta, '0' durumunda iken ise hiçbir işlem uygulanmamaktadır. Öte yandan NOR ve NAND mantık geçitlerinin uygun şekilde birleştirilmesiyle istenen herhangi bir mantıksal işlem inşa edilebilir. Bu yüzden bu mantık geçitlerine "evrensel mantık geçitleri" denilir. Evrensel mantık geçitleri tersinebilir değildir. Klasik bilgisayarlardaki ana fikir, temel mantık geçitlerini gerçekleştirebilecek donanım ile geçitleri birleştirerek çok komplike devreler kurulmasıdır.Klasik bir devredeki işlemler transistörlere uygulanan gerilimin seviyesiyle gerçekleştirilir. Bu genellikle açma/kapama şeklindedir.

Devrede bitler, bakır kablolar ile iletilir. Geçitler, seri veya paralel şekilde birleştirilebilir. Tek bit girişine sahip N tane geçidi paralel bağlarsak N-bitlik giriş elde ederiz. Klasik bitlerin çizgisel kombinasyonu mümkün değildir.

Bu geçitlerin varlığı ve bu geçitler sayesinde kurulan devreler, aslında klasik bilgisayarların evlere girebilmesini hızlandırdı. Çünkü donanım üreticilerin küçültmesi gereken geçit sayısı 2'ye (NOR ve NAND) düştü.

2.3 Klasik Hata Düzeltme

Herhangi bir X rastgele değişkeni iletilmek istenen bir mesajı temsil etsin. Bu iletişim sürecinde alıcı Y gibi bir değişken teslim alır ve X ile Y aynı veya eşit olmak zorunda değildir. Hatta bunun üzerine alıcı da veri işleme gerçekleştirir ve sonuç olarak Z gibi bir değişken elde eder. Bu sürecin ardından hata olasılığı

$$P_E = \Pr(Z \neq X) = \sum_{z \neq x} p(x,z)\, dir. \tag{2.1}$$

Alıcının, ulaştığı mesaja hangi şartlar altında güvenebileceği ($P_E = 0$) klasik hata düzeltmenin konusudur. İletilen mesajdaki gürültü ve bozulma etkilerinin üstesinden nasıl gelineceği asıl sorudur. Çünkü bir adımda kaybedilen korelasyon diğer adımda telafi edilemez.

Markov süreci veya Markov zinciri bu ve benzeri olasılıksal süreçleri modellemede kullanılır. Bir Markov zincirindeki her aşama yalnızca kendinden önceki aşamanın çıktısını girdi kabul eder. Tanım olarak çok basit görünse de birçok önemli sonuç ortaya çıkarır. Örneğin; ileriki aşamaların daha önceki değişkenlere değil de sadece mevcut değişkene bağlı olması, değişkenlerin "hafızasız" olması şeklinde yorumlanmaktadır.

$$X \xrightarrow{iletişimkanalı} Y \xrightarrow[veriişleme]{} Z$$

Yukarıdaki şekle uygun olarak; gönderilecek mesaj X, iletilen mesaj Y ve ulaşılan nihai mesajın Z olduğu süreç bir Markov zinciridir, çünkü alıcı sadece Y mesajını baz alarak veri işleme yapabilir. Bu durumda X değişkeninin olasılık dağılımı $p(x)$, iletişim kanalından gelen Y değişkeninin koşullu olasılık dağılımı $p(y|x)$ ve alıcının veri işlemesi sonucu elde ettiği Z değişkeninin koşullu olasılık dağılımı da $p(z|y)$ biçiminde ifade edilir. Y değişkeni koşullu olarak X değişkenine bağlıyken, Z değişkeni yalnızca Y değişkenine bağlıdır ve dolaylı olarak X'in kendisine değil Y üzerindeki etkisine bağlıdır.

X ve Z değişkenlerinin bağımsız olması sebebiyle Y değişkeni $p(x,z|y) = p(x|y)p(z|y)$ şeklinde ifade edilebilir. Böyle bir süreci tanımlayan Markov zincirinin entropiler cinsinden bakıldığında daha genel bir özelliği; klasik kuvvetli alt toplanabilirlik ilkesini içermesidir.

$$H(X,Z|Y) = H(X|Y) + H(Z|Y) \tag{2.2}$$

Y değişkeni yukarıdaki eşitlikle Shannon entropisiyle ifade edildiğinde, alt toplanabilirlik ilkesine göre:

$$H(X,Y,Z) + H(Y) = H(X,Y) + H(Y,Z) \tag{2.3}$$

yazılabilir. $H(X|Y) = H(X|Y,Z)$ olduğu için;

$$H(X|Y) \leq H(Z|Y) \tag{2.4}$$

sonucuna ulaşılır. Bu noktada X değişkeniyle diğer 2 aşamadaki değişkenlerin korelasyonuna bakıldığında çok önemli bir özellik kendiliğinden ortaya çıkmaktadır. Karşılıklı bilişim cinsinden;

$$H(X) \geq H(X:Y) \geq H(Y:Z). \quad (2.5)$$

Yukarıdaki ifade veri işleme eşitsizliği adını alır ve şöyle yorumlanabilir: bilişim süreci içerisinde Z değişkeni Y verisi üzerinde yapılan belirli veya rastgele işlemlerin sonucu ise; Y verisinden X mesajı hakkında edinilebilecek bilgiyi artıracak herhangi bir fonksiyon yoktur. Yani Markov sürecindeki tersinmezliği ifade eder. Buradan hareketle; herhangi bir aşamada X değişkeniyle olan karşılıklı bilişim bir defa kaybedilirse, ileriki hiçbir adımda geri kazanılamaz.

2.4 Klasik Hata Algılama ve Düzeltme Yöntemleri

Hata algılama; bilginin hatalı olup olmadığını belirleme işlemidir. Hata düzeltme; hatalı olduğu tespit edilen bilginin orijinal içeriğinin geri kazandırılması işlemidir. Klasik hata düzeltme işlemlerinin amacı; veriyi hatalardan koruyacak fazlalık bilgi ekleyerek taraflar arasındaki iletişimi en yüksek güvenilirlik düzeyine ulaştırmak olarak tanımlanabilir. Bu tarz işleyen bir hata düzeltme kodundaki verimlik; başlangıçtaki verideki bitlerin sayısı "k" ve bu veriye kodlama esnasında fazlalık olarak eklenen bitlerin sayısı "n" şeklinde tanımlanırsa, "k/n" oranıyla değerlendirmeye alınabilir. İletilmek istenen bilgi ardışık olarak gelen her n tane bit için "blok"lara bölünerek iletilir. Fakat bu işlemi başarılı kılacak kodları bulmaya yarayan genel bir yöntem mevcut değildir. Çünkü farklı kanallar, farklı en yüksek verimli kodlara sahiptir.

Bilgi "kod kelimeleri" haline getirilir, hata algılama ve düzeltme işlemleri de yapay olarak bu kod kelimeleri arasında bir miktar "uzaklık" yaratarak, hataların geçerli bir kod kelimesini diğer bir geçerli kod kelimesine çevirmesinin önüne geçer. Bu uzaklığı tasfir etmek için şöyle bir durum örnek gösterilebilir: taşıma esnasında kırılabilir eşyaların zarar görmemeleri için baloncukla sarılıp o şekliyle kutuya konması. Eşyayı sarmak için kullanılan baloncuk kod kelimeleri arasındaki yapay uzaklığı temsil eder. Bu işlem iletilen verinin miktarını artırır ama aynı zamanda iletim esnasında hata oluşmuş bilginin orijinal içeriğini geri kazanma ihtimalini de artırır. Kodlama ise

paketleme için kullanılan materyali ve eşyayı paketleme stratejisini seçmektir. Temel mantığı; en az baloncuk kullanılarak paketleme ve açma için en az eforu sarf etmektir.

Diğer bir örnek olarak: parite kontrolü biti, ISBN kodları ve tekrarlamalı kodlar gösterilebilir. Bunlardan ilk ikisi bilgideki hatanın algılanmasıyla ilgiliyken, 3. hatanın düzeltilmesiyle ilgilidir. Parite kontrolü için iletilecek bilgideki 1ler'in sayısının tek veya çift olmasına göre iletilecek bilginin sonuna 1 veya 0 biti eklenir. Bu örnekle, belirli bir hata algılama ve düzeltme kapasitesine sahip kodun tasarımında bulunmayan hata şekillerini algılama ve düzeltmede başarısız oluşunu gösterir. Örneğin hata sayısı 2 olduğunda 1ler'in sayısı çift kalacağından bu yöntemle hata tespit edilemez.

ISBN yani uluslararası kitap numaralandırma standardı kodu 10 rakamdan oluşmaktadır. Bu kodlama şemasıyla herhangi bir rakamda meydana gelebilecek hata ve komşu rakamlar arasında yer değişikliği algılanabilmektedir. İlk 9 rakam 10'dan 2'ye kadar ağırlıklara sahiptir ve mod 11'e göre rakamlar ile ağırlıkları çarpılıp hepsi toplandığında 10. rakamı vermektedir. Benzer hata algılama şemaları; banka kartları, uçak biletleri ve ürün barkodlarında da kullanılmaktadır.

Hata düzelten kodlar dendiğinde akla gelen ilk örnek tekrarlı kodlamadır. 0 veya 1 şeklinde ikili bir sembol yerine her biti n uzunluklu bir diziye çevirerek aşağıdaki biçimde göndermeye dayalıdır.

$$0 \rightarrow (00 \ldots 00)$$

$$1 \rightarrow (11 \ldots 11)$$

Eğer $n = 2k + 1$ şeklinde bir değere sahipse, "çoğunluk oylaması" şemasını kullanarak kod çözülebilir. Kod kelimesindeki 0'ların sayısı k'dan büyükse kod kelimesi 0'dır, aksi halde 1'dir denir.

Simetrik ikili bir kanalda p olasılıkla rastgele hatalar meydana geliyor olsun. n-bit'lik tekrarlı kodun bir kod kelimesinde hata meydana gelmesi ihtimali de p_{err}^{n} olsun. Bu hata olasılığı aşağıdaki ifadeyle verilir:

$$p_{err}^{n} = 1 - (1-p)^{k+1}\left[(1-p)^{k} + \binom{2k+1}{1} p(1-p)^{k-1} + \cdots + \binom{2k+1}{k} p^{k}(1-p)^{0}\right]. \quad (2.6)$$

k değeri ne kadar büyük olursa hata olasılığı o kadar küçülür ve bu kodlama şeması $p_{err}^{n} < p$ olduğu sürece tek bir bit gönderme işleminden daha iyi sonuç verir. Örneğin $n = 3$ve $k = 1$ olduğunda tek bir bit $0 \rightarrow (000)$ ve $1 \rightarrow (111)$ şeklinde kodlanarak iletilir. Bu iletimde hata meydana gelme olasılığı:

$$p_{err}^{n} = 1 - (1-p)^{2}\left[(1-p)^{1} + \binom{3}{1} p(1-p)^{0}\right] = 3p^{2} - 2p^{3} \quad (2.7)$$

bulunur. $p < \frac{1}{2}$ olduğu sürece bu kodlama şeması iletimin güvenilirliğini artırır.

2.5 Çizgisel İkili Kodlar

Çizgisel kod takımı;2^{n}kelime içeren bir *kesikli uzay* olarak tanımlıdır. N tanesi birbirinden bağımsızdır. İç çarpım, toplama ve çarpma işlemi gibi özellikler bu uzayda tanımlıdır. Toplama ve çarpma işlemleri ikili kodlarda mod 2'ye göre yapılır. Diğer bazı özellikleri şu şekilde sıralanabilir:

Kelime; $\{0,1\}$'den alınmış sıralı öğeler, C kodundaki bir kelimeyi oluşturur.Eğer,2^{n} kelime içeren bir C kod uzayı, toplama işlemine göre kapalılık gösteren ve $k < n$ olacak biçimde 2^{k} kelime tarafından gerilen çizgisel bir C' altuzayına sahipse; C''deki her çizgisel bağımsız kelime grubu C kodu için "kod kelimesi" adını alır ve şu şekilde

gösterilir: $0_L, 1_L, \dots, (2^k - 1)_L$ ve sadece altuzayı geren çizgisel bağımsız kelimeler bu gruba girer.

Hamming ağırlığı değeri H ile ifade edilir. Bir kod kelimesinin H değeri; bu kodu meydana getiren sıfırdan farklı öğelerinin sayısına eşittir ve örnek olarak $wt(1110) = 3$ şeklinde gösterilir.

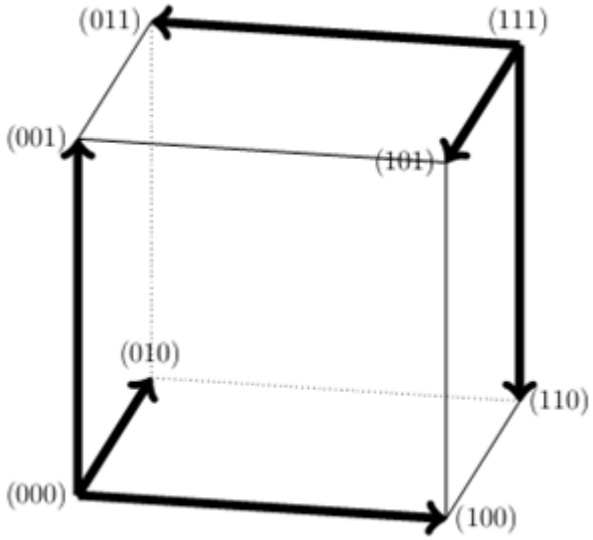
Tüm kod kelimeleri arasında ağırlığı en düşük olanın ağırlık değeri, C'uzayının uzaklığıdır yani d değerini verir.

İkili bir kod $[n, k, d]$ şeklinde ifade edilir. Böyle ifade edilen bir hata tespiti ve düzeltme kodunun kabiliyeti d uzaklığıyla doğrudan bağlantılıdır. d değeri özellikle bit-döndürme hataları için tanımlıdır.

Bir çizgisel hata düzeltme kodu, k-bitlik kodu n-bit kullanarak şifrelerse; d kodun uzaklığı olmak üzere, $t = \frac{(d-1)}{2}$ hatayı düzeltebilir ve $t + 1$ hatayı tespit edebilir. Klasik olarak tekrarlama koduyla koruma sağlamak için aşağıdaki şekilde kopyalanarak kodlanmış mantıksal bitler kullanılır:

$$0_L = (000), \quad 1_L = (111).$$

Bitler bu şekilde kodlanarak iletişim kanalından iletilir. Bu kodun yaptığı işlem birim küp üzerinde incelendiğinde kodun basitliği ve inceliği daha da anlaşılabilir hale gelir.



Şekil 2.2 Tekrarlamalı klasik hata düzeltme kodu modellemesi (Almlöf 2016)

Şekil. 2.2'deki klasik hata düzeltme kodu şifrelenmiş bir bitin kod kelimelerini en az $2k + 1$uzaklıkla ayırarak bu kodu korur. K_L, kodun düzeltebileceği hataların sayısını ifade etmektedir. Yukarıdaki durum 1 bit-döndürme hatasını düzelten tekrarlamalı kodu $[3, 1, 3]$içindir. Açıkça, bu kod keyfi bir bit-döndürme hatasını düzeltmek için gereken uzaklığa $(d = 3)$sahiptir (Almlöf 2016).

3. KUANTUM BİLGİSAYIM

3.1 Kuantum İletişim

Klasik bilgisayarlarda bitleri işlemek üzere transistörler kullanılır. Teknoloji dünyasında, daha az alana daha çok transistör yerleştirerek işlem gücünü artırma yolu tercih edildi. Bunun bir sonucu olarak transistörler nanometre boyutlarına kadar küçültüldü. Ama bu yaklaşım kaçınılmaz bir sona doğru ilerliyor, beklenmedik kuantum olayları. Boyutları küçülen transistör geçitlerinde sızıntı akımları ve kuantum tünelleme gerçekleşmesi durumunda bu cihazlarla başarılı bir şekilde veri işlenmesi garanti altına alınamaz. Klasik fizik kanunlarına dayalı bu yapı kuantum etkilerine karşı savunmasızdır.

Kuantum mekaniği ilkeleri, üzerine kurulduğu sağlam temeller sayesinde bir bilişim teorisine dönüşme kapasitesi çok yüksektir. Bu ilkelere bağlı kalınarak yapılacak bilişim uygulamalarına kuantum bilişim denir. Çeyrek asırdır hız kesmeden gelişme göstermektedir. Klasik bilgisayarla ulaşılması mümkün olmayan işlem hızı sayesinde, birçok bilim dalı için umut vericidir. Kuantum kimyası, yüksek boyutlu matematiksel modeller ve problemler, simülasyonlar, kriptoloji, meteoroloji, nöroloji, astronomi ve daha birçok alanda büyük değişimler yaratacağına kesin gözle bakılmaktadır.

Kuantumlu sistemler bit olarak işlenen veriyi fiziksel durumlarından çözümleyebilecek özelliklere sahiptir. Mesela, bir elektronun spini ölçüldüğünde, şu iki değerden biri bulunur. Bunlardan biri *spin yukarı* $|\uparrow\rangle$ durumuna karşılık gelen spinin ölçüm yapılan eksene paralel olduğu durumdur. Diğeri ise *spin aşağı* $|\downarrow\rangle$ durumuna karşılık gelen durumdur. Bu kuantumlanmış durumlar, örneğin elektronun spininin doğal bir ikili rakam veya bit olarak ele alınabilmesine izin verir. Bu sadece spin için geçerli bir özellik değildir. Herhangi bir ikili duruma sahip kuantum sistemi aynı yapıyı sergilediği taktirde böyle bir uygulama için kullanılabilir. Seçilen fiziksel yapı ne olursa olsun; eğer bir kuantum sistemi ile bit temsil edilecekse, sonuç olarak elde ettiğimiz yapıya kuantum bit veya kısaca "kübit" denir. (Schumacher 1998)

Kuantum bilginin başlangıç konsepti, klasik bilgiden esinlenerek türetildi. Klasik anlamda bilginin bir bit dizisine tekabül etmesi gibi, kuantum bilgi de bir kübit dizisine tekabül etmektedir. Fakat kuantum bilgide mümkün olan ve klasik bilgide herhangi bir karşılığı olmayan yeni ve farklı durumlar söz konusudur. Buradaki en önemli farklılık bilginin süperpozisyon halde iletilmesidir. Kuantumlu sistemlerin bu iki seviyeli yapıları ile gerçekleştirilecek hesaplamalar için, klasik geçitlerin üstesinden gelemeyeceği işlemleri yapabilmek amacıyla kuantum geçitler ve kanallar türetilmiştir. Aynı zamanda bunların birlikte seri ve paralel dizilimiyle elde edilen kuantum devreler de üretilmiştir.

3.2 Kübit

İki seviyeli bir kuantum sisteminde girilebilir durumlar süperpozisyon şekilde bir durum vektörü $|\Psi\rangle$ ile ifade edilir. Girilebilir durumlar, tercih edilen baz durumlarının (hesaplamasal baz) karmaşık katsayılara bağlı çizgisel kombinasyonu şeklindedir. Kuantum durumlarla işlem yaparken Hilbert Uzayında *bra-ket imgelemi* kullanmak kolaylık sağlar.

$$|0\rangle = |\uparrow\rangle = \begin{pmatrix}1\\0\end{pmatrix}, \qquad |1\rangle = |\downarrow\rangle = \begin{pmatrix}0\\1\end{pmatrix} \tag{3.1}$$

$$\langle 0| = \langle\uparrow| = (1 \quad 0), \qquad \langle 1| = \langle\downarrow| = (0 \quad 1). \tag{3.2}$$

Keyfi bir kübit için en genel durum vektörünü yukarıdaki baz durumlarını kullanarak şu şekilde ifade edebiliriz:

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle, \qquad |\alpha^2| + |\beta^2| = 1. \tag{3.3}$$

Somut olarak kübit sistemlerine: spin-1/2 olan parçacıklar, foton kutuplanması, iki kollu *Mach–Zehnder Girişimölçeri*, atomik temel durum geçişleri, iyon tuzakları ve süperiletken yapılar örnek olarak gösterilebilir.

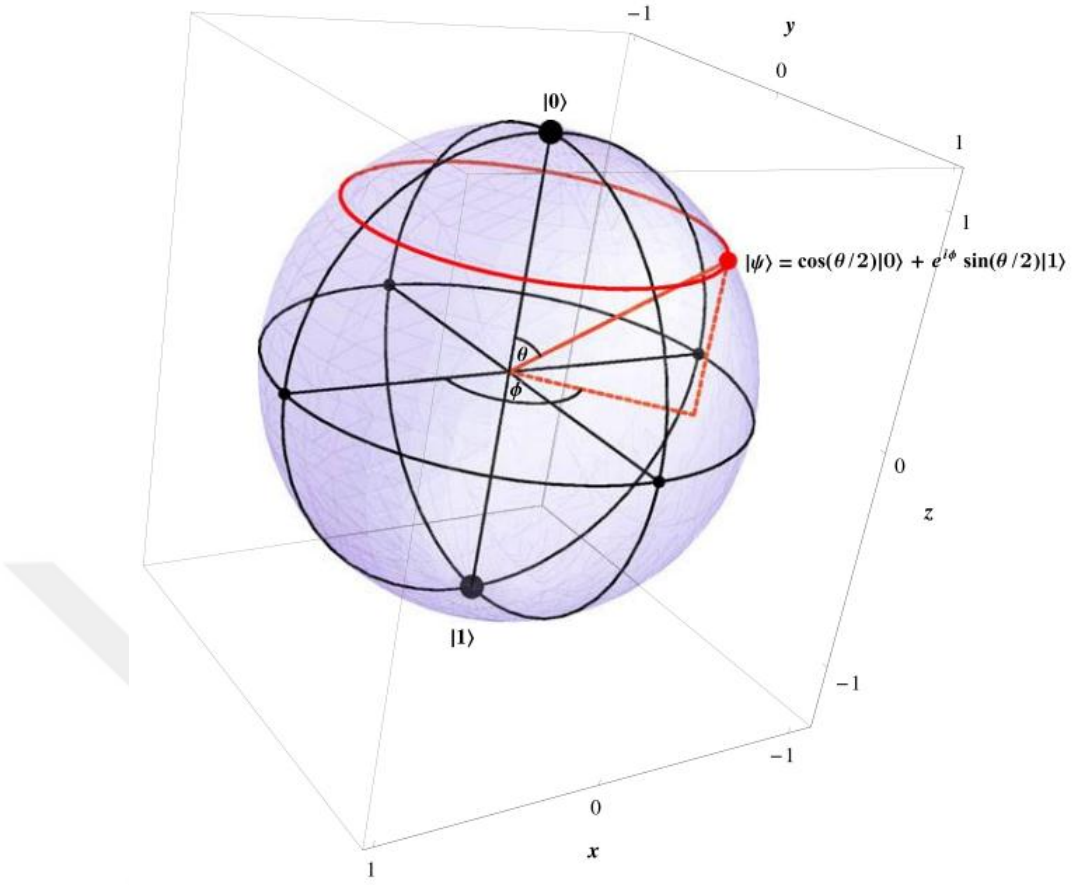
3.3 Stokes-Poincaré-Bloch (SPB) Yuvarı

Bir tek kübiti görselleştirebilmek için, geometrik bir model olarak; birim vektörü çevreleyen bir küre alınır ve bu kürenin adı Bloch küresidir. Kuantum durumunu açıklayan değişkenler; dikey değişken θ açısı ve dönme açısı Φ ile vektörün ucunun küre yüzeyine değdiği nokta belirlenir. Bu gösterimde kuzey kutup noktası $|0\rangle$ durumuna, güney kutup noktası ise $|1\rangle$ durumuna karşılık gelmektedir.

Küre yüzeyinde yer alan noktalar *saf durumları* temsil etmektedir. Ayırt edilebilirlik seviyesi en yüksek olan durum uzayı bu noktalardan oluşur. Kuantum bilişim için kullanımı en uygun olan durum uzayı da bu uzaydır. Küre içerisindeki noktalar ise *saf olmayan* durumları temsil eder. Kuantum bilişim esnasında sıkça karşılaşılan durumlar saf olmayanlardır. Kürenin merkezi ise en saf olmayan durumu $\frac{1}{2}\mathbb{1}$ ifade etmektedir.

Bloch küresinin yüzeyindeki diğer bütün noktalar mümkün olabilecek bütün α ve β değerlerinde $|\alpha^2| + |\beta^2| = 1$ biçimdeki süperpozisyonlara karşılık gelir. Bloch küresi üzerinde $|\alpha^2| + |\beta^2| = 1$ olmak kaydıyla $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ biçimindeki keyfi bir kübit kürenin parametrelerine bağlı olarak şu şekilde ifade edilebilir:

$$|\Psi\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}e^{i\Phi}|1\rangle = \begin{pmatrix} cos\frac{\theta}{2} \\ \sin\frac{\theta}{2}e^{i\Phi} \end{pmatrix}. \qquad (3.4)$$



Şekil 3.1 SPB Yuvarı üzerinde keyfi bir kübit temsili (Williams 2011)

Benzer yapılar birçok diğer bilim insanı tarafından araştırmalarında kullanılmıştır. Bu sebeple bu küreye aynı zamanda *Stokes – Poincare – Bloch Yuvarı* da denmektedir.
Kübitleri böyle matematiksel objeler olarak ele alabilmenin güzel tarafı kuantum iletişimin gerçekleştirilmesi için önceden belirli bir sisteme bağımlı olmayan genel bir teori oluşturulabilmesi açısından özgürlük tanımasıdır.

3.4 Yoğunluk Matrisi ve Özellikleri

Bir kuantum durumu hakkında elde edilebilecek bütün bilgileri içinde barındıran pozitif, birim izli ve *Hermite-sel* olan işlemci türüdür. Yoğunluk işlemcisi ya da geleneksel adıyla yoğunluk matrisi kuantum durumunun saf bir durum mu yoksa saf olmayan bir durum mu olduğunu da gösteren işlevsel bir yapıdır. ρ ile ifade edilen yoğunluk

işlemcisinin *spektral ayrışımıp*$_i$ bulunma olasılıklarını yani özdeğerlerini ve $|\Psi_i\rangle$ bulunulabilecek ortanormal durumları temsil etmek üzere şu şekildedir:

$$\rho = \sum_{i=1}^{n} p_i |\Psi_i\rangle\langle\Psi_i| \tag{3.5}$$

Yukarıdaki formülle verilen ayrışım genellikle *tek* değildir. Yalnızca özdeğerlerin hiçbiri dejenere değilse spektral ayrışım tektir. Saf olmayan durumun aslında saf durumları temsil eden matrislerin olasılıksal bir karışımı olarak yazılabilir. Yukarıdaki ifadede sıfırdan farklı sadece bir tane bulunma olasılığı varsa bu yoğunluk işlemcisi saf durumu temsil etmektedir ve $\rho = |\Psi\rangle\langle\Psi|$ şeklinde ifade edilir.

Kübit durumu irdelendiğinde *Bloch vektörleri*nin $\mathbb{R}^3$ uzayındaki birim kürenin tamamını gerdiği görülür. Yani birim küre üzerinde veya içerisinde kalan $\boldsymbol{r}_{(x,y,z)}$ noktalarının her biri geçerli bir kübit durumuna aittir. Birim kürenin koordinat bileşenleri $0 \leq \theta \leq \pi$, $0 \leq \Phi \leq 2\pi$ ve $0 \leq r \leq 1$ olmak kaydıyla şu şekildedir:

$$x = r sin\theta \cos\Phi$$

$$y = r sin\theta \sin\Phi$$

$$z = r\cos\theta$$

Keyfi bir ρ saf durumunun matris formu şöyle yazılabilir:

$$\rho = |\Psi\rangle\langle\Psi| = \begin{pmatrix} \cos^2\frac{\theta}{2} & e^{-i\Phi}\sin\frac{\theta}{2}\cos\frac{\theta}{2} \\ e^{i\Phi}\sin\frac{\theta}{2}\cos\frac{\theta}{2} & \sin^2\frac{\theta}{2} \end{pmatrix} \tag{3.6}$$

Bilinen trigonometrik dönüşümler yapıldığında yukarıdaki yoğunluk matrisi şu hale

gelir:

$$\rho = \frac{1}{2}\begin{pmatrix} 1+\cos\theta & e^{i\Phi}\sin\theta \\ e^{i\Phi}\sin\theta & 1-\cos\theta \end{pmatrix}. \tag{3.7}$$

Birim kürenin koordinat bileşenleri yerlerine yazıldığında yoğunluk matrisi şu şekilde basitleştirilmiş olur:

$$\rho = \frac{1}{2}\begin{pmatrix} 1+z & x-iy \\ x+iy & 1-z \end{pmatrix} \tag{3.8}$$

Bu eşitliği en basit formuna indirgemek ve saf olmayan durumlar için de geçerli bir hale getirmek üzere *Pauli matrisleri*($\sigma_x, \sigma_y, \sigma_z$) ve *birim matris*($I$) aşağıdaki ifadeleriyle yukarıdaki eşitliğe yerleştirilirse:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\rho = \frac{1}{2}(I + x\sigma_x + y\sigma_y + z\sigma_z) \tag{3.9}$$

ifadesi elde edilir.

Yoğunluk matrisi için en genel ifadeye ulaşmak amacıyla $\boldsymbol{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ ve $\boldsymbol{r} = (x, y, z)$ vektörleri yerlerine yazıldıktan sonra:

$$\rho = \frac{1}{2}(I + \boldsymbol{r}\cdot\boldsymbol{\sigma}) \qquad (r \leq 1), \tag{3.10}$$

sonucuna ulaşılır.

Kübit için en genel yoğunluk işlemcisi elde edilmiş oldu. Hem saf durumlar hem de saf olmayan durumlar için geçerli olan bu ifade sayesinde kübit durumları ile birim küredeki noktalar arasında bire bir eşleşme sağlanır.

En saf olmayan durum için N boyutlu Hilbert uzayında bulunma olasılığı $p = \frac{1}{N}$ ile verilir. Bu üç durumun yoğunluk işlemcilerinin karesinin izi üzerinden *saflılık* miktarlarına dair alt sınırı maksimum saf olmayan durum ve üst sınır saf duruma karşılık gelmek üzere şöyle bir çıkarım yapılmaktadır:

$$\frac{1}{N} \leq Tr(\rho^2) = \sum_{i=1}^{n} p_i^2 \leq 1. \tag{3.11}$$

Sadece saf durumların evrimi ve ölçümünde kullanılan durum vektörleri yerine hem saf durumları hem de saf olmayan durumları kapsayan bir yaklaşım ile yoğunluk işlemcilerini kullanarak, hakkında yeteri kadar bilgimiz olmayan kuantum sistemleri ile ilgili net bilgiler edinilebilir ve kuantum durumların yapıları hakkında çıkarımda bulunulabilir. Yoğunluk matrisiyle ilgili diğer bazı özellikler aşağıdaki gibidir:

- ρ yoğunluk matrisinin köşegen terimlerinin toplamı $Tr(\rho)$ her zaman için 1'e eşittir. Yani ρ boylandırma koşulunu sağlar.
- A ile belirtilen bir gözlenebilirin beklenen değeri $\langle A \rangle = Tr(\rho A)$ ile verilir.
- Yalıtılmış haldeki kapalı bir sistem için yoğunluk işlemcisinin zaman içindeki evrimi $i\hbar \frac{d\rho}{dt} = [\boldsymbol{H}, \rho]$ *Liouville - von Neumann denklemi*ni sağlar.
- Yoğunluk işlemcisi her zaman için $\rho^{\dagger} = \rho$ eşitliğini sağlaması sebebiyle Hermite-sel bir işlemcidir.
- Eğer $\rho^2 = \rho$ eşitliği sağlanıyorsa ρ; izdüşürme özelliğine sahiptir ve bir saf duruma karşılık gelir.

- $Tr(\rho^2) = 1$ ise, ρ durumu **3.11** denkleminde saflık miktarı için verilen aralığın üst sınırındadır ve bir saf durumu ifade eder.

- ρ yoğunluk işlemcisi bir saf duruma aitse, özdeğerlerinden sadece 1 tanesi 1'e eşittir gerisi 0'dır.

3.5 Dolanıklık

Bir elektron-pozitron çiftinin yok oluşu esnasında zıt yönlerde savrulan 2 adet foton ortaya çıkmaktadır. Bu iki foton aynı mesafedeki detektörlerde ölçüme tabi tutulduklarında sürekli olarak birbirinin zıttı spinleri olduğu görülmektedir. Bunun anlamı ölçümün sonucunun diğerinin de sonucunu verdiğidir. Ölçüm işlemi aynı anda yapıldığından, iki fotonun birbiriyle iletişimde olmasına imkan yoktur.
Buna getirilen açıklama; bu iki fotonun spinlerinin dolanık olduğu ve her fotonun spin durumu iki olası spin yöneliminin süperpozisyonudur.

Bu olay, kuantum bilgisayarları klasik bilgisayarlardan daha güçlü hale getirir ve klasik bilgi yoluyla yapılamayan işlemlerin kuantum bilgisi yoluyla yapılmasına izin verir.

Temel olarak bir durumun dolanık veya dolanık olmaması arasındaki fark; onun kuantum durumunun ayrılabilir olup olmamasından anlaşılır. Bu yüzden, söz konusu durumu matematiksel izahı aşağıdaki şekildedir.

Ayrılabilir durum: Bir sistemin durum vektörü $\mathcal{H}_A \otimes \mathcal{H}_B$ biçiminde tanımlı olan bir Hilbert uzayında,

$$\left|\Psi^{(AB)}\right\rangle = \left|\Psi^{(A)}\right\rangle \otimes \left|\Psi^{(B)}\right\rangle \; veya \; \rho^{(AB)} = \sum_i p_i \rho_i^{(A)} \otimes \rho_i^{(B)} \qquad (3.12)$$

biçiminde yazılabiliyorsa $\left|\Psi^{(AB)}\right\rangle \; veya \; \rho^{(AB)}$için ayrılabilir durumdur denir.

Bir durum $\mathcal{H}_A \otimes \mathcal{H}_B$ biçiminde tanımlı bir Hilbert uzayında ayrılabilir bir durum değilse ***dolanık durum***dur. Buna göre bir durum aynı zamanda hem dolanık ve saf hem de dolanık ve saf olmayan durum olabilir.

3.6 İz-Mesafesi

İki kuantum durumu verildiğinde bunlar arasındaki yakınlık, ayırt etmek için kullanılabilecek önemli bir veridir. Böyle bir yakınlık; yoğunluk işlemcileri kümesi üzerine uygun bir mesafe tanımlaması yaparak elde edilebilir. En önemli ve yoğun kullanılan mesafe ölçüsü "iz-mesafesi" denilen ölçümdür. $\rho \; ve \; \sigma$ herhangi bir yoğunluk matrisi ve herhangi bir A operatörü için iz-normu $Tr|M| = Tr\sqrt{A^{\dagger}A}$ şeklinde tanımlı olmak üzere iz mesafesi şu şekilde ifade edilir:

$$D_t(\rho, \sigma) = \frac{1}{2} Tr|\rho - \sigma|. \tag{3.13}$$

İz-mesafesi, yaygın olarak kullanılan mesafenin sahip olduğu bütün özellikleri sağlar:

- Sadece eşitlik $(\rho = \sigma)$ durumunda $D_t(\rho, \sigma) \geq 0 \; ve \; D_t(\rho, \sigma) = 0$ sağlanır.
- İz-mesafesi $D_t(\rho, \sigma) = D_t(\sigma, \rho)$ olacak şekilde simetriktir.
- Herhangi bir τ, ρ, σ yoğunluk işlemcisi için $D_t(\rho, \tau) \leq D_t(\rho, \sigma) + D_t(\rho, \tau)$ olmak üzere üçgen eşitsizliği sağlanır.

Kuantum bilişim alanında iz-mesafesiyle önemli bir yaklaşım gerçekleştirilir. Yoğunluk işlemcileri $\rho \; ve \; \sigma$ olan iki kuantum durumunun başarılı şekilde ayırt edilebilmesinin en yüksek olasılığı iz-mesafelerine bağlı olarak:

$$\frac{1}{2}+\frac{1}{2}D_t(\rho,\sigma)'dir. \tag{3.14}$$

3.7 Öze-Uygunluk

Öze-uygunluk, genellikle iki kuantum durumunun "benzerliğini" ölçmek için kullanılan bir niceliktir. Saf olmayan ρ ve σ durumları için şu şekilde tanımlıdır:

$$F(\rho,\sigma)=\left[Tr(\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}})\right]^2. \tag{3.15}$$

Kimi yayınlarda özeuygunluk, iz ifadesinin karesi olmadan da verilmektedir. ρ bir saf durumu temsil edecek olursa keyfi bir σ yoğunluk işlemcisiyle arasındaki öze-uygunluk şöyle elde edilebilir:

$$F(|\psi\rangle,\sigma)=\left[Tr\left(\sqrt{|\Psi\rangle\langle\Psi|\sigma|\Psi\rangle\langle\Psi|}\right)\right]^2$$

$$=\left[Tr(\sqrt{\langle\psi|\sigma|\psi\rangle|\psi\rangle\langle\psi|})\right]^2$$

$$=\left[Tr(\sqrt{\langle\Psi|\sigma|\Psi\rangle}|\Psi\rangle\langle\Psi|)\right]^2$$

$$=\langle\Psi|\sigma|\Psi\rangle\equiv Tr(\sigma|\Psi\rangle\langle\Psi|)\,. \tag{3.16}$$

Hem ρ hem de σ birer saf durumu temsil edecek olursa, bu iki yoğunluk işlemcisi arasındaki özeuygunluk:

$$F(|\Psi\rangle,|\Phi\rangle)=|\langle\Psi|\Phi\rangle|^2 \tag{3.17}$$

ifadesiyle verilir. Özeuygunluk birbirine dik iki kuantumlu durum için 0 iken özdeş durumlar için 1 değerini alır. Bunu aynı zamanda üst üste gelme durumlarının 1'den

uzaklaşması olarak da yorumlamak mümkündür. İki kuantumlu durumun karşılaştırılması konusunda özeuygunluk kullanımı iz-mesafesi kullanımından daha yaygındır. Özeuygunluğun öne çıkan özellikleri şu şekildedir:

$0 \leq F(\rho, \sigma) \leq 1$ ifadesine bağlı kalarak 0 ile 1 arasında değer alır;

$F(\rho, \sigma) = F(\sigma, \rho)$ şeklinde simetri özelliğine sahiptir;

Her A kuantum kanalı için A: $F(A(\rho), A(\sigma)) \geq F(\rho, \sigma)$ ifadesi geçerlidir, yani kuantum kanallar kuantum durumların ayırt edilebilirliğini azaltır.
$F(\rho_{AB}, \sigma_{AB}) \leq F(\rho_A, \sigma_A)$ alt sistemler üzerinden parçalı iz alınması kuantum durumlarının ayırt edilebilirliğini azaltır.

$1 - \sqrt{F(\rho, \sigma)} \leq \frac{1}{2} Tr|\rho - \sigma| \leq \sqrt{1 - F(\rho, \sigma)}$ (Fuchs-van der Graaf) eşitsizliği, iz mesafesi için alt ve üst sınır değerlerini verir.

Kuantum bilişim için kodlama, hata düzeltme ve diğer işlemlerde ulaşılmak istenen hedef *öze-uygunluk* ölçütünü en yüksek seviyede tutmaktır.

3.8 Üniter Dönüşümler

Kuantum bilişim ile kuantum durumları üzerinde bir takım dönüşümler yapılacaksa bunların saflığı muhafaza etmesi gerekir. Bu tarz bir uygulama için en uygun tür: Hilbert uzayındaki vektörlere uygulanabilen üniter matrislerdir. Bunun sebeplerini şu şekilde sıralayabiliriz:

- Φ durumu bazı özdurumların süperpozisyonuysa bütün özdurumlara eşzamanlı uygulanır. Çünkü çizgiseldir.
- Her ortanormal baz üzerinden iz alınmasına müsaade ederler.

- Üniter matrisler Hilbert uzayının vektörlerinin iç çarpımını korurlar.
- Her üniter dönüşüm için ters dönüşüm de mevcut olduğundan; tersinirdirler.

3.9 DiVincenzo Kriterleri ve Kuantum Bilgisayar

İlk olarak David DiVincenzo tarafından kuantum bilgisayar yapısını bir kalıba oturtmak üzere 5 maddelik bir liste öne sürülmüştür. Bu 5 kriter herhangi bir fiziksel sistemin kullanılabilir bir kuantum bilgisayar olabilmesi için sağlaması gereken özelliklerdir. (DiVincenzo 2000)

1. En az iki seviyeli kuantum sistemler (kübit) ile çalışabilmesi,
2. İşlemlerden önce kübitler bilinen bir seviyede tutulabilmesi,
3. Kübitler yalıtılmalı, beklenmedik etkilerin olmaması,
4. Harici bir kontrol sistemiyle kuantum sistemi herhangi bir $\boldsymbol{H}$ Hamilton işlemcisine göre sürülebilir olması,
5. Son halleri (çıktılar) ölçülebilir olmalı ki sonuç alınabilsin.

Yukarıdaki 5 şarta ek olarak günümüzdeki yerel ağ veya internet ağı benzeri kuantum bilginin gönderilebileceği ve saklanabileceği bir kuantum veri işleme ağı kurulabilmesi için 2 kriter daha eklenmiştir.(Nakahara and Ohmi 2008)

6. Durağan ve uçan (iletimdeki) kübitler arasında dönüşüm yapabilme becerisine sahip olması.
7. Kübitlerin belirtilen yerler arasında güvenilir bir şekilde iletebilir olması.

DiVincenzo kriterlerinin öngördüğü gibi bir kuantum bilgisayarın potansiyelini gerçekleştirebilmesi için takip edilebilecek iki yol mevcuttur:

1. Sonsuz hassasiyete sahip bir kontrol yöntemiyle, mutlak sıfır sıcaklığı civarında başlatılan kuantum sistemlerle yapılan hesaplama sonuçlarının gürültüsüz ölçümle belirlenmesi.

2. Kusurlu başlangıç, kontrol ve ölçüm etkilerini çok iyi derecede kavrayarak kusurlu bir kuantum bilgisayarla yüksek ve bilinen bir olasılıkta Divincenzo kriterlerine uyan kuantum bilgisayarları taklit etmek.

İkinci yol klasik bilgisayarlarda ilerleme vaat etmesi ve gerektirdiği cihazların birincideki kadar uç seviyede olmaması sebebiyle daha mümkün görünmektedir. Bu yol 2 araştırma alanının kombinasyonudur. Bunlar kuantum bilgi teorisi ve hata-toleranslı kuantum bilişimdir (Criger2013).

3.10 Parçalı-İz İşlemi

Kimi zaman bileşik bir sistemin altsistemlerinden yalnızca bir tanesi ilgi çeker. Böyle bir durumla başa çıkmak için indirgenmiş yoğunluk işlemcisine başvurmak gerekir. S^A ve S^B şeklinde iki altsistemden meydana gelmiş sonlu boyuttaki bir S^{AB} kuantum sistemi ve bileşik sistemin ρ_{AB} yoğunluk işlemcisi için sonlu boyuttaki Hilbert uzayı H_{AB}; bağımsız H_A ve H_B Hilbert uzaylarının tensör çarpımıyla elde edilir. $N_A = dimH_A$ ve $N_B = dimH_B$ olsun. "Parçalı-iz" sayesinde altsistemlere ait ρ_A ve ρ_B indirgenmiş yoğunluk işlemcilerini $|\Phi_j\rangle$ $(j = 1, 2, \dots, N_B)$ H_B'nin ortanormal bazı, $|\Psi_j\rangle$ $(j = 1, 2, \dots, N_A)$ H_A'nın ortanormal bazı olmak üzere aşağıdaki şekilde tanımlanabilir:

$$\rho_A = Tr_B\rho_{AB} \equiv \sum_{j=1}^{N_B} (I_A \otimes \langle\Phi_j|)\rho_{AB}(I_A \otimes |\Phi_j\rangle), \tag{3.18}$$

$$\rho_B = Tr_A\rho_{AB} \equiv \sum_{j=1}^{N_A} (\langle\Psi_j| \otimes I_B)\rho_{AB}(|\Psi_j\rangle \otimes I_B). \tag{3.19}$$

Bu ifadedeki Tr_B; B altsistemi üzerinden parçalı-iz alınması şeklinde anılır. A altsistemi için doğru ölçüm istatistiklerini almak için mümkün olan tek yolun parçalı-iz almak olması bu işlemi özel kılar.

3.11 Kuantum Kanal Gösterimi

Kuantumlu sistemlerin devinimini tanımlamak için genellenebilir ve esas sistem ile dış çevresinin etkileşimine de açıklama getirecek gösterim yöntemleri öne sürülmüştür. Esas sistemini ρ_A yoğunluk işlemci temsil ediyor ve sistemin devinimi de $\Phi(\rho_A)$ gönderimi ile ifade edilsin. Bu gönderim sayesinde ρ_A' şeklinde yeni yoğunluk işlemcileri elde edilir:

$$\rho_A^{'} = \Phi(\rho_A).$$

Bu tarz gönderimlere "kuantum işlemi" denir. En bariz örnekleri üniter zaman devinimi

$$\Phi(\rho_A) = U\rho_A U^{\dagger} \tag{3.20}$$

ve kuantum ölçüm işlemleridir:

$$\Phi(\rho_A) = M_m \rho_A M_m^{\dagger}. \tag{3.21}$$

Bu tarz işlemler için daha genel bir ifade bulmak üzere bir grup üniter olması şartı gözetilmeyen A_k işlemcileri için $\varphi(\rho_A)$ kuantum işlemi şu şekilde yazılır:

$$\Phi(\rho_A) = \sum_{k=1}^{n} A_k \rho_A A_k^{\dagger}. \tag{3.22}$$

buna "$\varphi(\rho_A)$'nın operatör toplamı gösterimi" denir. Eğer A_k işlemcileri tamlık bağıntısını

$$\sum_{k=1}^{n} A_k^{\dagger} A_k = I \tag{3.23}$$

sağlıyorsa bu işlemciler "iz-koruyan" demektir ve $\rho_A^{'} = \Phi(\rho_A)$ bağıntısını sağlanır.
Esas sistem ve çevresi birleşik üniter *U* işlemi altında devinime uğradığı durumda A_k işlemcileri hesaplanabilir. Çevreyi temsil eden yoğunluk işlemcisi ρ_E olsun. Esas sistem ve çevresi etkileştikten ve U üniter işlemi uygulandıktan sonra yalnızca esas sistemin durumu parçalı-iz yöntemiyle elde edilebilir.

$$\Phi(\rho_A) = Tr_E(U(\rho_A \otimes \rho_E)U^{\dagger}). \tag{3.24}$$

Çevrenin baz durumları $|e_k\rangle$ ile ifade edilir ve başlangıçta çevre $\rho_E = |e_0\rangle\langle e_0|$ durumunda kabul edilirse yukarıdaki ifade şu şekilde tekrar yazılabilir:

$$\Phi(\rho_A) = Tr_E(U(\rho_A \otimes \rho_E)U^{\dagger}) = \sum_k \langle e_k|(U(\rho_A \otimes \rho_E)U^{\dagger})|e_k\rangle$$

$$= \sum_k \langle e_k|(U(\rho_A \otimes |e_0\rangle\langle e_0|)U^{\dagger})|e_k\rangle = \sum_k \langle e_k|U|e_0\rangle\, \rho_A \langle e_0|U^{\dagger}|e_k\rangle \tag{3.25}$$

operatör toplamı gösterimiyle karşılaştırıldığında A_k işlemcileri için:

$$A_k = \langle e_k|U|e_0\rangle \tag{3.26}$$

ifadesi elde edilir. Bu şekilde ifade edilen işlemcilere *Kraus işlemcileri* denir. Kraus işlemcileri esas sistem üzerine uygulanır.

3.12 Kuantum Geçitler

Bloch küresinde kuantum mekaniği ilkelerinin izin verdiği her dönüşüm kuantum geçittir ve üniter birer işlemcidir. Herhangi bir üniter işlemcinin Hermite-sel eşleniği $U^{\dagger} = U^{-1}$ şeklinde tersine eşittir.Bu özelliğiyle geçitlerin gerçekleştirdiği işlemlerin hepsi tersinebilirdir. Bu en sade biçimiyle:

$$UU^{\dagger} = U^{\dagger}U = I \tag{3.27}$$

şeklinde ifade edilebilir. Kuantum geçitler sadece $|0\rangle$ veya $|1\rangle$ gibi salt durumlar için değil, aynı zamanda bunların süperpozisyonuyla da tanımlı olmalıdır. Kuantum mekaniğindeki işlemler çizgisel olduğundan, kuantum geçitlerin işlemleri matris yardımıyla gösterilebilir. n adet girdiye sahip bir kuantum geçidi 2^n dereceli bir matrisle ifade edilebilir. Yani bir kübit üzerinde 2 x 2'lik üniter matrisle işlem yapılabilir.
Kuantum bilgiişlem için kullanılan temel geçitlerin bir kısmı mantık olarak klasik bilgiişlemdeki gibi işler fakat kuantum mekaniği kanunları sayesinde klasik olarak erişilemeyecek işlem yapma hızlarına ulaşılmasını sağlar. Kuantum geçitlerden meydana gelmiş bir devre şemasına bakıldığında zamanın soldan sağa doğru ilerler ve en soldaki geçit ilk uygulanır.

3.13 1-Kübit Geçitleri

Kuantum bilişimde en sık kullanılan geçitler Pauli dönüşümleridir $(I, \sigma_x, \sigma_y, \sigma_z)$. Hepsi birer üniter ve tersinebilir geçit olduğundan temel kuantum devrelerinin kurulmasında büyük kolaylık sağlarlar.

Klasik bilişimdeki NOT geçidinin aynısı kuantum bilgiişlemde de mevcuttur. Fakat kuantum mekaniğinin ilkeleri gereği kuantum NOT geçidi girdi değerlerinin süperpozisyonlarına da uygulanabilir ve yapısını bozmadan aynı şekilde çıktı olarak verebilir. Kuantum NOT geçidi Pauli-X işlemcisi ile ifade edilir.

$$X \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Geçidin tek bir kübit ve keyfi bir Ψ süperpozisyon durumu üzerinde gerçekleştirdiği işlem aşağıdaki gibidir:

$$\mathrm{X}|0\rangle = |1\rangle, \qquad \mathrm{X}|1\rangle = |0\rangle$$

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

$$\mathrm{X}(\alpha|0\rangle + \beta|1\rangle) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix} \tag{3.28}$$

Aynı zamanda "Bit-döndürme" geçidi olarak da anılmaktadır. Devre şemasındaki gösterimi şu şekildedir:

Şekil 3.2 Pauli-X geçidinin |1⟩ durumuna etkisi

Bir kübitlik girdi ve çıktıya sahiptir. Tersinebilir bir kanaldır. Klasik bilgiişlemdeki NOT geçidi için değilleme demek uygunken kuantum bilişimdeki NOT geçidi için aynı ifadeyi kullanmak mümkün değildir. Çünkü değilleme ifadesiyle geçitte işlem gören durumun tam aksi olarak çıkacağı belirtilmektedir. Bu durum süperpozisyon halindeki durumlar için tek bir geçitle mümkün değildir. Kaldı ki tam anlamıyla değilleme yapabilen bir kuantum geçit mevcut değildir. Bu işlem tam anlamıyla ancak bir kuantum devreyle sağlanabilmektedir.

Pauli-X işlemcisinin klasik bir karşılığı bulunmasına rağmen diğer 2 Pauli işlemcisi Pauli-Z ve Pauli-Y'nin klasik bilişimde karşılıkları yoktur.

Örneğin; Pauli-Z işlemcisi faz-dönüşü geçidi olarak da isimlendirilir. İşleyiş olarak $|0\rangle$ durumunu değişmez bırakırken, $|1\rangle$ durumunu $-|1\rangle$ haline getirir. En genel şekliyle:

$$Z|j\rangle = (-1)^j|j\rangle \tag{3.29}$$

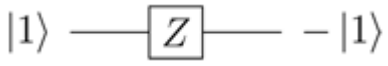
biçiminde ifade edilir. Keyfi bir Ψ durumuna etkisi şu şekildedir:

$$Z|\Psi\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha \\ -\beta \end{pmatrix}. \tag{3.30}$$

Z geçidi aslında daha genel anlamdaki faz-dönüşü geçidi:

$$P = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} \tag{3.31}$$

ifadesinin $\theta = \pi$ olduğu özel durumudur. Z geçidi devre şemasında şu şekilde gösterilir:

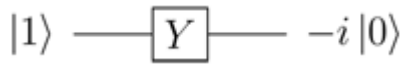


Şekil 3.3 Pauli-Z geçidinin |1⟩ durumuna etkisi

Bir diğer Pauli dönüşümü olan Pauli-Y işlemcisi "bit-faz dönüşü" geçidi olarak da adlandırılır. $|0\rangle$ durumundaki bir kübite etki ettiğinde $i|1\rangle$'ye çevirirken, $|1\rangle$ durumundaki bir kübite etki ettiğinde onu $-i|0\rangle$ durumuna çevirir. Süperpozisyon haldeki bir Ψ kübit durumuna etkisi şöyledir:

$$Y|\Psi\rangle = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} -i\beta \\ i\alpha \end{pmatrix}. \tag{3.32}$$

Pauli-Y geçidinin devre şemasında gösterimi şu şekildedir:



Şekil 3.4 Pauli-Y geçidinin |1⟩ durumuna etkisi

Pauli-X geçidinden türemiş ilginç bir kuantum geçidi; $\sqrt{NOT}$ geçididir. Bu geçidin klasik bilgiişlemde bir karşılığı mevcut değildir. En basit anlamda kırılan yumurtaları ilk önce karıştıran ikinci seferinde ise karışmamış hale getiren bir makine icat etmek gibidir. 1 kere uygulandığında kübiti süperpozisyon hale getirir ve ölçüm sonucu için en az $1/2$ oranında rastgelelik söz konusudur. 2. defa uygulandığında ise kübite tam bir kübit-dönüşü yaptırmış olur ve ölçüm sonucundaki rastgelelik ortadan kalkmış olur.$(\sqrt{NOT})(\sqrt{NOT}) = NOT$ şeklinde bir eşitlik söz konusudur.

$$\sqrt{NOT}|0\rangle = \frac{1}{2}(1+i)|0\rangle + \frac{1}{2}(1-i)|1\rangle \xrightarrow{\sqrt{NOT}} |1\rangle,$$

$$\sqrt{NOT}|1\rangle = \frac{1}{2}(1-i)|0\rangle + \frac{1}{2}(1-i)|1\rangle \xrightarrow{\sqrt{NOT}} |0\rangle. \tag{3.33}$$

Geçidin matris ifadesi şu şekildedir:

$$\sqrt{NOT} = \frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}. \tag{3.34}$$

Matris ifadesine bakarak bir geçidin klasik bilişimde mümkün olup olmadığını anlamak kolaydır. Matrisin satırlarında sadece 0 ve 1 değerleri varsa bu geçit klasik bilgiişlem açısından mümkündür. Eğer matris ifadesinde 0 ve 1'den farklı değerler de mevcutsa bu matris bir kuantum geçidi temsil ediyor demektir.

Şekil 3.5 √NOT geçidinin |1⟩ durumuna etkisi

$\sqrt{NOT}$geçidi kuantum devrelerde yukarıdaki şekilde olduğu gibi temsil edilir.

İlk bakışta $\sqrt{NOT}$geçidine benzer bir işleve sahipmiş gibi görünen çok önemli bir geçit; Hadamard geçididir. Hadamard geçidi, girişteki kübit durumuna etkidiğinde bunu eşit ağırlıklı süperpozisyon durumlara dönüştürür. Bu özelliğiyle kuantum bilgiişlem için hayati bir görev yerine getirir. Hadamard geçidinin matris ifadesi ve hesaplamasal bazlara etkisi aşağıdaki gibidir:

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

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{3.35}$$

En genel haliyle herhangi bir $|j\rangle$ baz durumuna etkidiğinde girdi durumunu şu ifadeye bağlı şekilde dönüştürür:

$$H|j\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^j|1\rangle\right); \quad j = 0,1. \tag{3.36}$$

Hadamard geçidi keyfi bir Ψ süperpozisyon duruma etkidiğinde ise ortaya Hadamard bazları çıkmaktadır:

$$H|\Psi\rangle = H(\alpha|0\rangle + \beta|1\rangle) = \left(\frac{\alpha+\beta}{\sqrt{2}}\right)|0\rangle + \left(\frac{\alpha-\beta}{\sqrt{2}}\right)|1\rangle$$

$$= \alpha\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) + \beta\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = \alpha|+\rangle + \beta|-\rangle. \quad (3.37)$$

Sistem artık α^2 olasılıkla $|0\rangle$ bazı yerine $|+\rangle$ Hadamard bazında, β^2 olasılıkla ise $|1\rangle$ bazı yerine $|-\rangle$ Hadamard bazında bulunabilecek şekilde dönüşür. Hadamard geçidinin devre şemasında ifade edilişi aşağıdaki gibidir:

Şekil 3.6 Hadamard geçidinin $|0\rangle$ durumuna etkisi

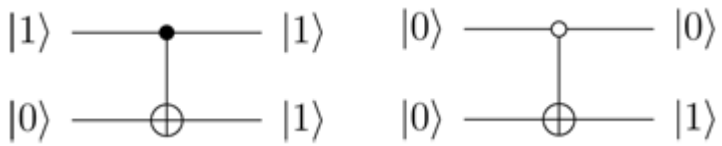
3.14 Çoklu Kübit Geçitleri

Çoklu kübit geçitleri içinde en önemli örnek CNOT(kontrollü-NOT) geçididir. İki girdi ve iki çıktıya sahiptir. Girdi durumlarından biri kontrol diğeri ise hedef olarak adlandırılır. Örneğin; kontrol biti $|0\rangle$ durumunda ise hedefteki kübit mod 2 toplamına göre değişime uğramadan geçerken kontrol biti $|1\rangle$ durumu olduğunda hedefteki kübit mod 2 toplamına göre bit dönüşüne uğrar. CNOT geçidinin işleyişi ve matris ifadesi şu şekildedir:

$$CNOT|A, B\rangle \rightarrow |A, B \oplus A\rangle$$

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

Genellikle kontrol biti üstte hedef biti altta yer alacak şekilde devre şemasındaki çizimi şu şekildedir:



Şekil 3.7 |1⟩ kontrollü ve |0⟩ kontrollü CNOT geçitleri

Soldaki gösteriminde geçidin kontrol kübitinin |1⟩ durumu olması beklenirken, sağdaki gösteriminde kontrol kübitinin |0⟩ olduğu durumlarda hedef kübitte bit dönüşü olur.

Bu geçidin birçok önemli kullanım şekli vardır. Özellikle kuantum hata düzeltme işlemlerinde çok faydalı noktalarda kullanılmaktadır. Mesela; dolanık olmayan 2 durumdan mükemmel şekilde dolanık olan durumlar üretebilir. *Yıkıcı olmayan ölçüm*le kontrol kübitinin süperpozisyon durumunda değilken |0⟩ veya |1⟩ durumunlarından hangisinde olduğunu tespit edebilir. Biraz daha karmaşık bir yıkıcı olmayan ölçümle, çok parçacıklı sistemlerin pariteleri ölçülebilir. Bir diğer özelliği; hem hedef hem de kontrol kübitlerinin çevrilmiş bazda $\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$ olduğu durumda, bu kübitler görev bakımından birbiriyle yer değiştirmesidir.

CNOT geçidi diğer bir adıyla Feynman geçidi ve temel 1-kübit geçitleri, kuantum bilgi-işlem için evrenseldir. Bunun anlamı; herhangi bir çoklu kübit mantık geçidinin CNOT geçidi ile 1-kübit geçitlerinden meydana getirilebilir olduğudur. Yani bu bir bakıma klasik bilgisayımdaki NAND mantık geçidinin evrensellik özelliğinin kuantum bilgisayımdaki paralelidir denebilir. Bu aşamadan sonraki geçitler de bu ilkeye bağlı olarak CNOT geçidi ve 1-kübit geçitlerinin kombinasyonuyla türetilmiş geçitlerdir.

SWAP (değiş-tokuş, Trampa), 3 tane CNOT geçidinin kullanılmasıyla türetilebilen çok yaygın ve faydalı bir kuantum geçididir. Geçidin matris ifadesi şu şekildedir:

$$SWAP = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

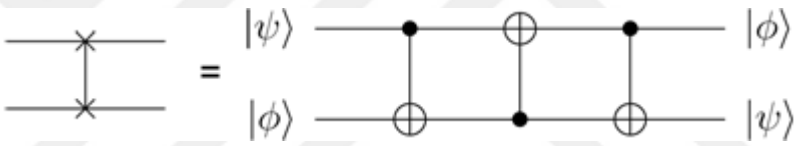
Çok basit ama işe yarar bir işlevi yerine getirir. 2 kübitin durumlarını karşılıklı değiştirir. Bu değiş tokuş işlemini nasıl gerçekleştirdiği, geçitlerin uygulanışı ve sonuçları sırasıyla şöyledir:

$$|A,B\rangle \xrightarrow{CNOT} |A, A \oplus B\rangle$$

$$\xrightarrow{CNOT} |A \oplus (A \oplus B), A \oplus B\rangle = |B, A \oplus B\rangle$$

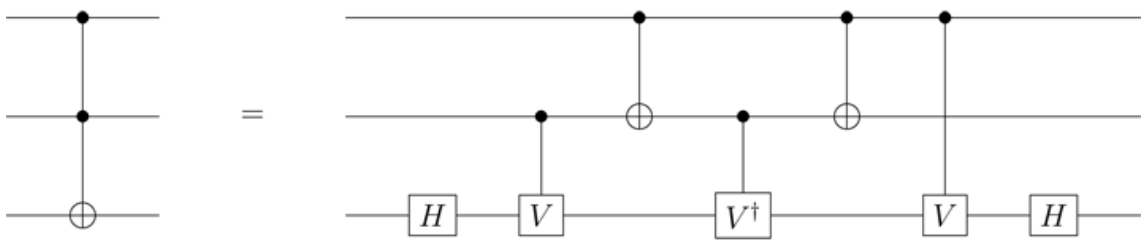
$$\xrightarrow{CNOT} |B, (A \oplus B) \oplus B\rangle = |B, A\rangle. \quad (3.38)$$

SWAP geçidi 3 CNOT geçidinden meydana gelen bir kuantum devresi şeklinde veya kendine özgü geçit biçimiyle aşağıdaki şekillerde devre şemasında gösterilebilir:



Şekil 3.8 SWAP geçidi ve eşdeğer devresi

3-kübit girişine sahip geçitlere pek çok örnek verilebilir. İlk akla gelen ve en önemli örneği Toffoli (CCNOT, TOFF) geçidinin devre şemasında aşağıdaki iki şekilde ifadesi mümkündür:



Şekil 3.9 Toffoli geçidi ve eşdeğer devresi

1-kübit ve CNOT geçitlerinden meydana gelen devrede $V = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$ geçidi z-ekseninde $\pi/2$'lik bir dönüşe karşılık gelmektedir. Hedefteki kübit sadece hem 1. hem de 2. kontrol kübitleri $|1\rangle$ durumundayken bit-dönüşüne uğramaktadır. Toffoli geçidinin matris ifadesi aşağıdaki biçimdedir:

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

Tersinebilir çoklu kübit kuantum geçitlerini devre halinde meydana getirmenin bir maliyeti vardır. Buna "kuantum maliyeti" denir. Kuantum maliyeti, çoklu kübit girişine sahip tersinebilir bir kuantum geçidini meydana getirmek için oluşturulan devredeki temel kuantum geçitlerinin $(V, V^{\dagger}, H, CNOT)$ toplam maliyeti ile hesaplanır. Aynı devreyi oluşturmak için birden çok temel kuantum geçidi kombinasyonu mevcuttur. Bu devreleri en iyi haline getirmek için farklı algoritmalar mevcutsa da tek bir yöntem yoktur.

4. KUANTUM HATA DÜZELTME

Kuantumlu sistemlerdeki iletişim süreci de klasikte olduğu gibi 2 aşamalı olarak ele alınabilir. Bu iki aşamalı açık sistem gelişimi $Q \to Q' \to Q''$ şeklinde ifade edilsin. Başlangıçta Q sistemine ait bir ρ giriş durumu ve gelişim sürecinde durumlar süperoperatörler yardımıyla şu şekilde gösterilebilir:

$$\rho \to \rho' = \mathcal{E}(\rho) \to \rho'' = D(\rho'). \tag{4.1}$$

Bu süreçte sistemin ve çevrenin birinci aşamadaki etkileşimlerine rağmen ikinci aşamada Q sisteminin karşılaştığı çevrenin başlangıçta sistemle korelasyona sahip olmaması kuantum Markov özelliği anlamına gelmektedir. Yani her aşama bağımsız çevreler içerir. Klasiğin aksine kuantum Markov süreçlerinde hafızasız olan çevredir.

Bu bağlamda, birinci aşamadaki $\mathcal{E}$ gelişiminin ardından, asıl durumun D gelişimi ile ne kadar özüne sadık şekilde geri kazanılabileceği sorunu ortaya çıkar. Bu süreç içerisinde tersinemez bilgi kaybı olup olmadığı ve bunun önüne geçmek veya geri kazanabilmek adına kuantum hata düzeltme işlemleri yapılması gerekir.

Kuantum iletişim süreci içerisine bir R seyirci sistemi eklenir. Başlangıçta RQ sisteminin saf $|\Psi^{RQ}\rangle$ durumunda olduğu varsayılır ve Markov süreci (R sisteminin gelişimi önemsiz) $RQ \to RQ' \to RQ''$ şeklini alır. Bu sürecin sonunda okunan bilginin güvenilirliği ve aslına uygunluğu dolanıklık özeuygunluğu ile şu şekilde görülür:

$$F_e = \langle \Psi^{RQ} | \rho^{(RQ)''} | \Psi^{RQ} \rangle. \tag{4.2}$$

Bu bağıntıyla, D gelişiminin ardından $\rho^{(RQ)''}$ durumunun başlangıç durumuna olan benzerliği sınanmış olur. Bunun sonucunda entropinin en yüksek değeri için yani en yüksek benzerlik için F_e'nin $\rho^{(RQ)''}$ durumunun en büyük özdeğeri olması ve diğer

bütün özdeğerlerin eşit olması gerekir. Başarım ölçütü olarak kullanılan bu değer ile kuantum hata düzeltme kodlarının ne kadar fayda sağladığı irdelenebilir.

4.1 Dekoherans (Eş-uyum Yitimi)

Hatalar bilişimin kaçınılmaz birer parçasıdır. Kuantum bilişim esnasında da çok çeşitli ve zorluk seviyeleri değişen hatalarla karşılaşılır. Bu hatalar, kullanılan kübit sistemi ve taşıyıcı ortamın kırılganlığına ve hassasiyetine, çevre koşullarına vb. bağlı olarak farklılık gösterir. Bunlar sistemi eş-evresizliğe sürükler ve hesaplamalardan doğru sonuç alınmasına engel olur. Kuantumlu sistemler dışarıdan etkiye karşı çok hassastır. Bu tarz bir sistemle güvenilir şekilde bilişim yapabilmek için, oluşabilecek hataların önceden belirlenmesi ve/veya bunlara karşı tedbirlerin alınması gerekir.

Model (ideal) neden sağlanamıyor? Uygulamaya geçildiğinde bütün kuantum sistemleri birer açık sistemdir, çevreden mükemmel bir biçimde soyutlanamaz ve sakınılamaz şekilde çevreyle bağlantılı hale gelirler. Kuantum sisteminin yetersiz izolasyonu sonucu çevre kaynaklı gürültüye maruz kalmasından ötürü en geniş tanımıyla: eş-evresizlik durumu ortaya çıkar. Eş-evresizlik; dolanıklığın son bulması, faz değişimi, dönüşler, bit-değişimi, faz sönümü şeklinde görülebilir. Kontrol parametrelerindeki sapmalar ve kalibrasyonla ilgili eksikliklerden ötürü kontrol hataları kaçınılmaz hale gelir.

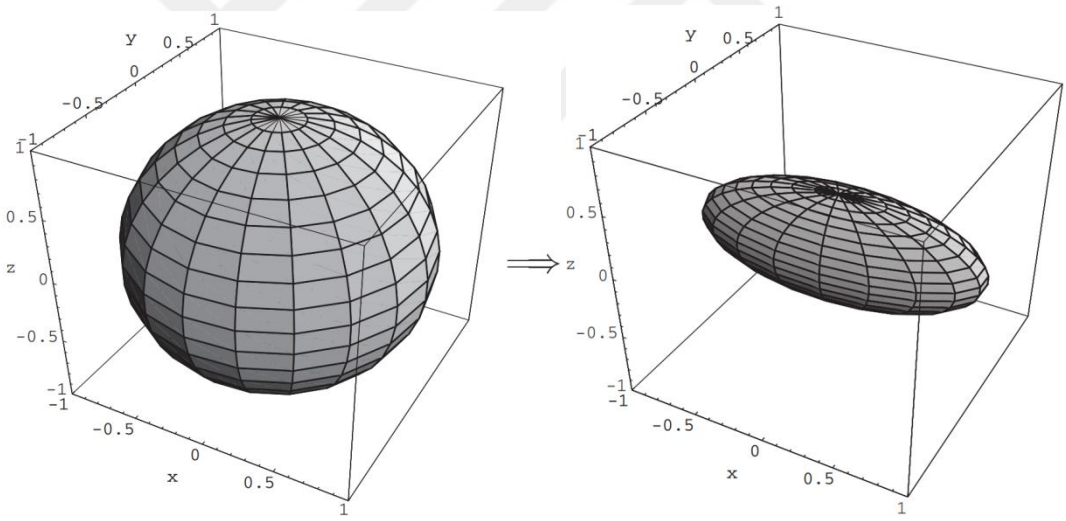
Kuantum bilişim için kullanılan sistemler çok kırılgan yapılardır. Bu yapılarda birden fazla hata aynı anda meydana gelebilmektedir ve hata türleri klasik bilişimin aksine daha çok ve daha karmaşıktır. Bu hata türleri içerisinde en temel veözel olarak kübitler için en sıklıkla karşılaşılan durumlar; kübit-dönüşü, faz dönüşü, bit-faz dönüşü, kutuplanma yitimi, genlik sönümlenmesi ve faz sönümlenmesi hata modelleri aşağıda incelenmiştir.

4.2 Kübit–Dönüşü Hatası

Kuantum devresindeki kübitin, aslında olmaması gerekirken $|0\rangle$ ve $|1\rangle$ arasında veya $|1\rangle$ ve $|0\rangle$ arasında geçiş yapması durumudur. Bu hatanın Kraus işlemcileri şu şekilde ifade edilir:

$$E_0 = \sqrt{p}I = \sqrt{p}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \qquad E_1 = \sqrt{1-p}X = \sqrt{1-p}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}. \tag{4.3}$$

Bu hataya maruz kalmış bir kübit için Bloch küresi, olasılık katsayısına bağlı olarak X-eksenini simetri ekseni kabul eden bir elipsoide dönüşür. Böyle bir dönüşüm p=0,3 için **Şekil 4.1**'deki gibidir.



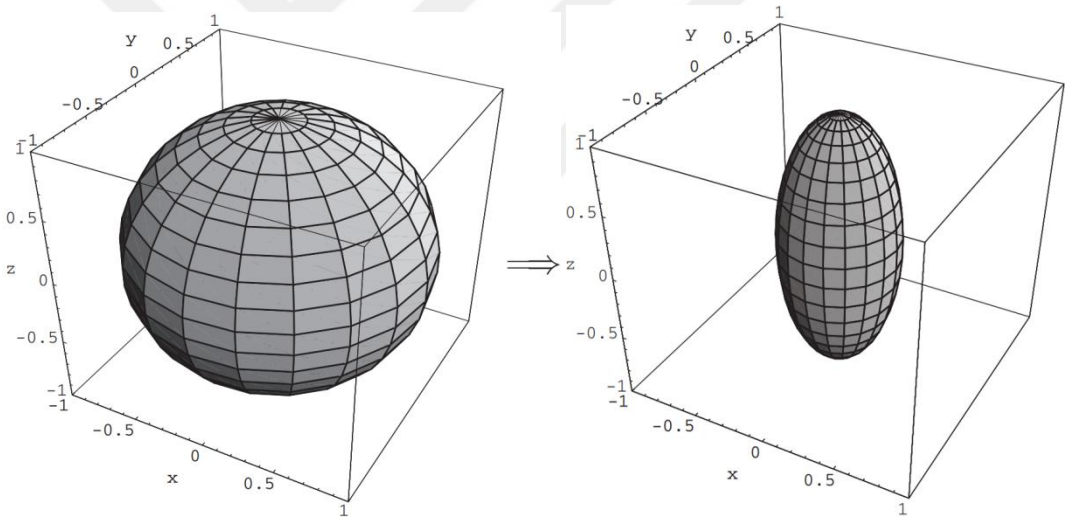
Şekil 4.1 P=0,3 olduğu durumda kübit-dönüştürme hatasının Bloch küresine etkisi (Nielsen and Chuang 2000)

4.3 Faz–Dönüşü Hatası

Bu hata türünün klasik bilişimde karşılığı yoktur. Bu tarz bir hata baz durumları $|0\rangle$ ve $|1\rangle$'in katsayılarının işaretini değiştirmektedir. Bu hatanın Kraus işlemcileri şu şekilde ifade edilir:

$$E_0 = \sqrt{p}\, I = \sqrt{p}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad E_1 = \sqrt{1-p}\, Z = \sqrt{1-p}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{4.4}$$

Bu hata türünün etkisiyle Bloch küresi olasılık katsayısına bağlı olarak simetri ekseni z olan bir elipsoide dönüşür. Böyle bir dönüşüm p=0,3 için **Şekil 4.2**'deki gibidir.



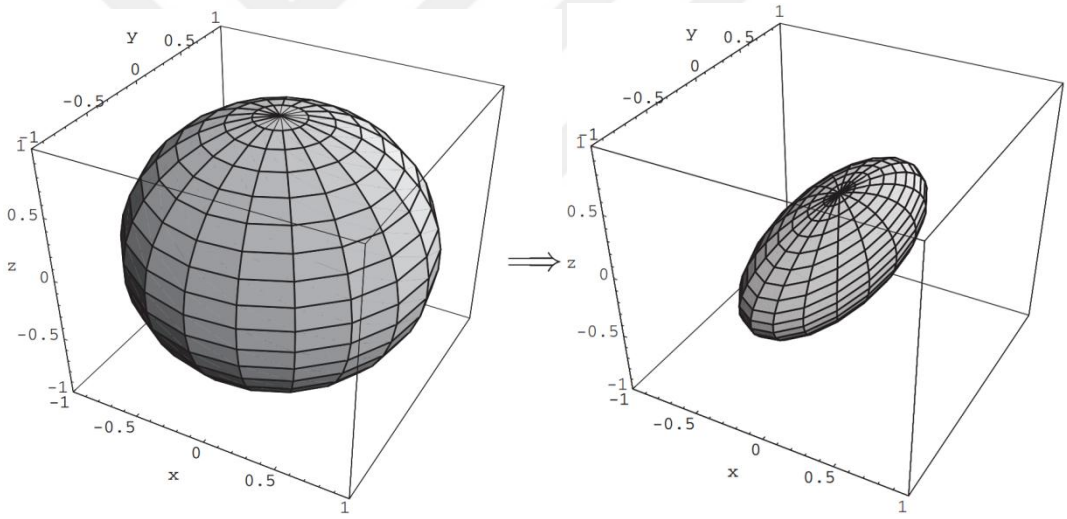
Şekil 4.2 P=0,3 olduğu durumda faz-dönüşü hatasının Bloch küresine etkisi (Nielsen and Chuang 2000)

4.4 Bit-Faz Dönüşü Hatası

Kuantum bilişim esnasında aynı anda oluşabilecek birden çok hataya bir örnektir. Bu tür bir hata aynı anda hem bit hem de faz dönüşümüne sebebiyet verir. Bu hatanın Kraus işlemcileri şu şekilde ifade edilir:

$$E_0 = \sqrt{p}\, I = \sqrt{p}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad E_1 = \sqrt{1-p}Y = \sqrt{1-p}\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}. \tag{4.5}$$

Bu hata türünün etkisiyle Bloch küresi olasılık katsayısına bağlı olarak simetri ekseni y olan bir elipsoide dönüşür. Böyle bir dönüşüm p=0,3 için **Şekil 4.3**'deki gibidir.



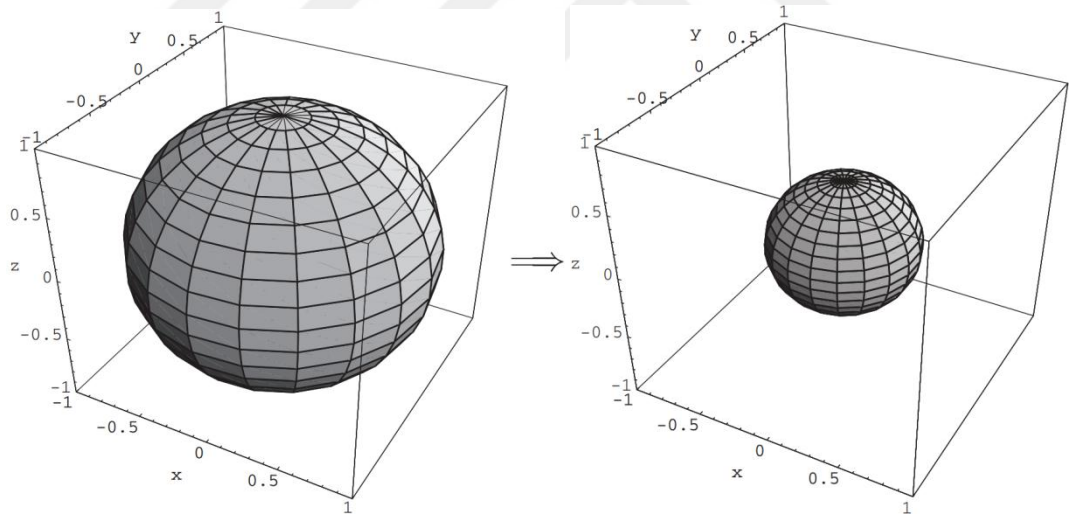
Şekil 4.3 P=0,3 olduğu durumda bit-faz dönüşü hatasının Bloch küresine etkisi (Nielsen and Chuang 2000)

4.5 Kutuplanma Yitimi Hatası

Kübit olarak kullanılabilecek kuantumlu sistemlerden birisi de kutuplanma durumudur. Bu yöntemle hayata geçirilen sistemler de çok kırılgandır ve kutuplanma yitimine (*depolarizing*) uğrama riski vardır.

$$\varepsilon_{(\rho)} = \frac{pI}{2} + (1-p)\rho \tag{4.6}$$

Böyle bir hata oluştuğunda, yönünden bağımsız olmak üzere Bloch vektörünün hatanın meydana gelme olasılığını çarpan kabul ederek ufalması söz konusudur.Böyle bir dönüşüm p=0,3 için **Şekil 4.4**'deki gibidir. Hatta bu çarpanın bazı değerleri için tamamen kutuplanma yitimi de mümkündür (Benenti, Casati and Strini 2007).



Şekil 4.4 P=0,5 olduğu durumda kutuplanma yitimi hatasının Bloch küresine etkisi (Nielsen and Chuang 2000)

Gerçek sistemlerde, hataların sadece $\sigma_x, \sigma_y, \sigma_z$ olması varsayımı zayıftır. Bunların bazı çizgisel kombinasyonları pratikte daha çok karşılaşılabilir hallerdir. Mesela, iyonun temel veya uyarılmış durumda hata kaynağı: kendiliğinden soğurma adını alır.

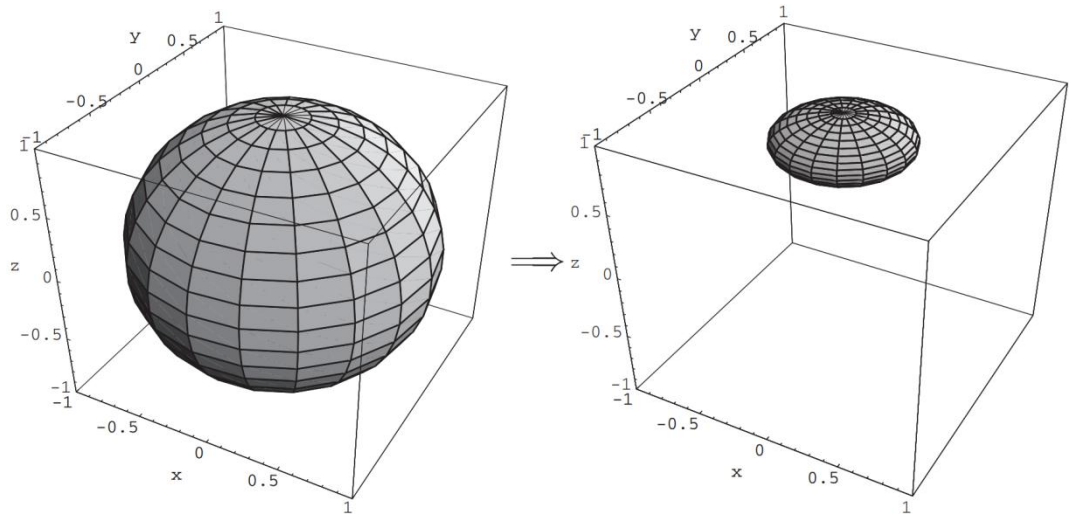
Uyarılmış durumdan zamanla temel duruma ε olasılıkla $\sigma_x + i\sigma_y$ hatasını türetir. Bu durum $|0\rangle$ ve $|1\rangle$'in bağıl genliklerini de değiştirir ve $O_{(\varepsilon^2)}$ derecesinde hata olasılığıyla: $I - \sigma_z$ hatası türetir.Bu tarz bir zaman evrimini gerçekleştiren kanal: genlik sönümlenmesi (*amplitude damping*) olarak modellenebilir (Gottesman 1996).

4.6 Genlik Sönümlenmesi Hatası

Çevreyle etkileşim sonucu oluşabilecek hatalardan biridir. Bu tip bir hatada; p, $|1\rangle$ durumunun $|0\rangle$ durumuna çökme olasılığı (sönümlenmesi olasılığı, $0 < p < 1$) olmak üzere tek yönlüdür. Hata oluşması durumunda başlangıçtaki durum saf olmayan da olsa saf da olsa genlik $|0\rangle$'a doğru çöker. Bu hatanın Kraus işlemcileri şu şekilde ifade edilir:

$$\varepsilon_{AD(\rho)} = E_0 \rho E_0^\dagger + E_1 \rho E_1^\dagger .\ E_0 = \begin{pmatrix} 1 & 0 \\ 1 & \sqrt{1-p} \end{pmatrix}, E_1 = \begin{pmatrix} 0 & \sqrt{p} \\ 0 & 0 \end{pmatrix} \qquad (4.7)$$

Böyle bir hata Bloch küresini elipsoit biçime getirir ve merkezini p kadar $|0\rangle$'a yaklaştırır. Böyle bir dönüşüm p=0,8 için **Şekil 4.5**'deki gibidir.



Şekil 4.5 P=0,8 olduğu durumda genlik sönümlemesi hatasının Bloch küresine etkisi (Nielsen and Chuang 2000)

4.7 Faz Sönümlenmesi Hatası

En genel bir kübit yoğunluk matrisi şu şekilde ifade edilebilir:

$$\begin{pmatrix} p & \alpha \\ \alpha^* & 1-p \end{pmatrix}$$

Sırasıyla, pozitif gerçel p ve 1-p ($0 \leq p \leq 1$) köşegen terimleri kübiti $|0\rangle$ ve $|1\rangle$ durumlarında bulabilme olasılığına denk gelir. α ve α^* kuantum eşfazlılığı (koheranslığı) ifade etmektedir ve klasik bir karşılığı yoktur. Faz sönümlenmesi (*phase-damping*) hatası, bu eş fazlılığın zayıflamasını tetikler, köşegen olmayan terimlerde zayıflamaya sebep olur ve sistemi eşevresizliğe (*decoherence*) sürükler. Bu da sistemin kuantumlu yapısından klasik forma dönüşmesinde önemli bir rol oynar. Hataların fiziksel olarak kaynaklarının anlaşılması kuantum bilgisayar yapımının önemli bir parçasıdır.

Bu tarz hataların etkisini azaltmak için kuantum sistemlerin kontrol edilebilmesi ve ölçülebilmesiyle yola devam edilebilir. Bu sebeplerden dolayı eş-uyumu koruyacak kadar iyi yalıtılmış sistemler ve kontrol cihazlarıyla kuvvetli etkileşim gereklidir. Bir kısım hatayı giderebilecek bu iki temel gerekliliğin dışında kuantum bilişimin temelini oluşturan kuantum mekaniğinin kendine özgü davranış yapısından dolayı ortaya çıkan, aşılması güç bazı durumlar da söz konusudur.

4.8 Kuantum Hata Düzeltmenin Önündeki Engeller

1-) Kuantum bilişimin başlangıç aşamalarında ispat edilmiş olan "No-Cloning teoremi" (Wootters ve Zurek 1982) üniter dönüşümler ile keyfi bir bilinmeyen kuantum durumunun özdeş bir kopyasının yaratılmasının imkansız olduğunu ifade eder. İleri araştırmalar, ancak üniter olmayan kopyalama cihazları ile öze-uygunluktan feragat edilerek birbirine dik olmayan saf durumların kopyalanabileceğini göstermiştir, fakat bu yöntemler genele uygulanabilir değildir. Dolayısıyla, başlangıçta oluşturulan verinin

özdeş bir kopyasını oluşturmak mümkün değildir. Bu sebeple klasik bilişimde olduğu gibi tekrarlı ve gereğinden fazla kodlama yaparak veriyi korumak mümkün değildir.

2-) Kuantum mekaniğinin başa çıkılması en zor ve en tartışmalı varsayımı; yapılan ölçümün kuantum durumunu çöktürmesidir. Öyle ki, durum vektörlerinin direkt ölçümü mevcut süperpozisyonun bir anlık duruma çökmesine sebep olur ve süperpozisyonu ortadan kaldırır. Bundan ötürü gönderilen verinin kontrolünü direkt olarak yaparak eleme veya kabul etme seçeneği ortadan kalkar.

3-) Veri iletimi esnasında kübitler birden fazla hata türüne maruz kalabilir. Böyle çoklu hataların oluşabilmesi de kuantum mekaniğinin doğasından ötürüdür. Bu tarz durumların önceden görülmesi, tespiti ve oluşan hataların düzeltilmesi gerekir.

4-) Devamlı hatalar, her kübitte ufak hataların oluşması ve eş-evresizlik oluşumu durumlarının süregelen sistemler içerisinde nasıl düzeltileceği ve bu sonu yokmuş gibi görünen düzeltme işleminin ne kadar bir sürece yayılacağı da zorlayıcı bir engel teşkil etmektedir.

4.9 İşçi Kübitleri

Bundan böyle işçi kübitler olarak anacağımız Ancilla kübitleri hatalara karşı koymada ve oluşan hataların düzeltilmesi konularında bilişim için hayati önem taşır. İşçi kübitler; bir grup erişilebilir, başlangıçta $\{|0\rangle, |1\rangle\}$ bazında bilinen bir durum olarak hazırlanmış, üniter işlemlerde entropi deposu olarak görev alan kübitlerdir. Ancilla; $|0\rangle$ saf durumu ya da uygulama olarak yaklaşığı alınır. Fakat dengede güvenilir durumlar yaratmak çok zordur. Kodun tekrar kullanımı için yüksek entropiye sahip Ancilla'nın $|0\rangle$'a tazelenmesi gerekir. Bu işlem izdüşüm ölçümleriyle (*projective measurement*) gerçekleştirilebilir. Eğer işlem mükemmel değilse hata düzeltme esnasında kazanılan entropinin bir kısmı Ancilla kübitinde tutulur. Kuantum hata düzeltme kodunu ancilla kübitlerine aktarım esnasında "artan entropiyi dağıtan" şekilde düşünmek faydalıdır.İşçi kübitlerin, hata düzeltme sürecinde sistemle olan dolanıklılığına son verilir (Criger 2013).

5. KUANTUM HATA DÜZELTME KODLARI

5.1 Kuantum Hata Düzeltici Kodların Temel Özellikleri

Kuantum kodlara biçimsel olarak bakıldığında, *k*-boyutlu bir alt uzayın bilinen bazı hatalara karşı korunması, durumların daha büyük boyuttaki *n*-boyutlu bir Hilbert uzayına gönderimi ile sağlanır.

Öncelikle, bir (n,k)-kuantum kodu$n$-boyutlu Hilbert uzayının k-boyutlu alt uzayı şeklinde tanımlanır. Buna *kod uzayı* denir ve $\mathcal{H}$ ile gösterilir. Kod içinse $\mathcal{C}$ sembolü kullanılır. E üniter operatörü, *k*-boyutlu Q Hilbert uzayından $\mathcal{C}$'ye olmak üzere $\mathcal{C}$ için bir şifreleme işlemcisidir. Bu işlemcinin sağ tersi de *şifre çözme işlemcisi* (*decoding*) olacaktır. Uygulama esnasında, k ve n değerleri $d < r$ olmak üzere genellikle ikinin kuvvetleri olarak $k = 2^d$ ve $n = 2^r$ şeklinde ifade edilir.

Şifreleme işlemcisi $Q^d \otimes Q^{r-d} \otimes Q^a$ üzerine üniter bir işlemci olarak, a devrenin girişinde ve çıkışında |0⟩ durumunda olması beklenen iş kübitlerini temsil etmek üzere, uygulanır. İş kübitleri, $\mathcal{C}$ kodunun geri kazanımı için ölçüm esnasında bir yaz-boz gibi kullanılır.

Bu durumda kodlanacak olan Q kod uzayının standart bir alt uzayıdır ve şifreleme işlemcisi istenilen koda gönderimini sağlar. Q üzerinde aynı etkiyi gösterecek birden fazla şifreleme işlemcisi vardır. Çünkü şifreleme, gerekli olan dönüşümün sadece bir parçasını tanımlar. Hangi seçeneğin kullanılacağı verimliliğe bağlıdır. İstenilen hata düzeltme özelliklerine göre değişir.

Kodların hata düzeltme özelliklerini açıklamak için bir geri kazanım süper işlemcisi (*superoperator*) tanımlayabiliriz. R kod uzayında bir süper işlemcidir. Çevreyle etkileşimden etkilenen durumu asıl haline geri çevirmek için kullanılır. Kullanım

şekilleri dışında, geri kazanım ve etkileşim işlemcileri benzer türde objelerdir (Knill ve Laflamme 1997).

5.2 Kuantum Hata Düzeltme Kriteri

Oluşmuş hatanın türüne bakmaksızın düzeltilebilmesi için bir hata düzeltme kodu olup olmadığı merak konusudur. Bu konu üstüne operatör-toplamı gösterimi veya Kraus gösterimi yoluyla düşünülebilir. Hatalar operatör elementleri veya Kraus operatörleri olarak ele alınabilir. Klasik hata düzeltmede 2 ayrı hatayı düzeltebilmek için hata olumuş tüm kod kelimeleri birbirinden farklı olmalıdır. Yani farklı hatalar kod kelimelerini ayrışık altgruplara götürürler ki bu da ortogonallik koşulunu beraberinde getirir ve farklı hata gönderimleri için 0 aynı hata gönderimleri içinse sıfırdan farklı sonuç vermesi gerekir. Eğer kuantum hata düzeltme kodlarının mevcudiyeti için de aynısı geçerli ise farklı hata işlemcileri ve kübit durumları da ortogonallik koşulunu aşağıdaki şekilde karşılamalıdır:

$$\langle 0_L | \mathcal{E}_i^\dagger \mathcal{E}_j | 1_L \rangle = 0. \tag{5.1}$$

Fakat bu eşitlik gerekli koşul değil yeter koşuldur. Yani kuantum hata düzeltme kodunun varlığını garanti altına almaz. Örneğin başlangıçtaki durumların aynı, hata işlemcilerinin farklı olduğu durumda:

$$\langle 0_L | \mathcal{E}_i^\dagger \mathcal{E}_j | 0_L \rangle = \langle 1_L | \mathcal{E}_i^\dagger \mathcal{E}_j | 1_L \rangle = 0 \tag{5.2}$$

Şeklinde bir ifadeye dönüşür ki bu ifadeye ne gerek duyulur ne de tüm hata işlemcileri için geçerlidir.

Klasik hata düzeltme için kabul edilebilir olmayan bir bakış açısından bakılabilir böyle bir duruma. Öyle ki $\mathcal{E}_i$ ve $\mathcal{E}_j$ gibi iki hata işlemcisi kod uzayının aynı altgrubuna gönderim yapıyor olsun. Bu durum klasik anlamda ayırt edilemez durumlar yaratacağı

için kabul görmez. Fakat ters çevrilebilen, hatayı düzeltebilecek ve kod kelimesini geri kazandırabilecek bir işlem sayesinde durum mümkün kılınabilir. Yani kuantum hata düzeltme için koşul ortogonallikten ibaret değildir ve şu ifadeyle verilir:

$$\langle 0_L | \mathcal{E}_i^{\dagger} \mathcal{E}_j | 1_L \rangle = C_{ij} \delta_{ij}. \tag{5.3}$$

Bu ifadeye göre; eğer $\mathcal{E}$ hata kümesi bu şartı sağlıyorsa, geri kazandırma gerçekleştirecek bir işlem bulunabilir (Knill ve Laflamme 1997).

5.3 Tekrarlamalı 3-kübit Kodu (Bit–Dönüşü)

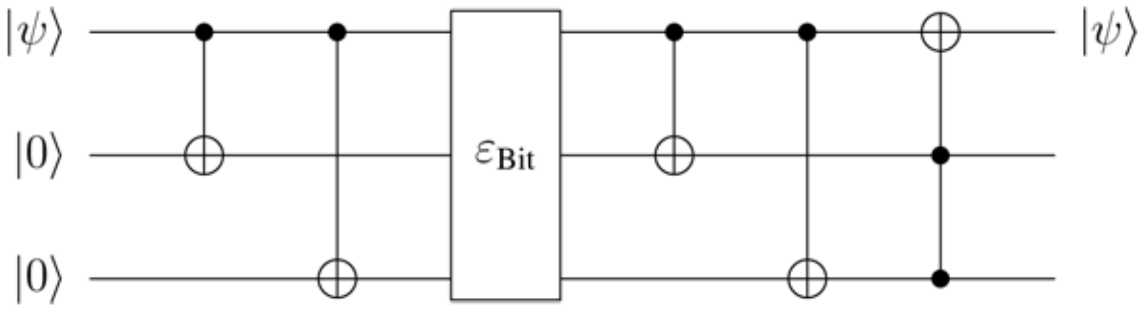
En temel kuantum hata düzeltme kodu olan tekrarlamalı 3-kübit kodu detaylı bir şekilde incelendiğinde kuantum hata düzeltme kavramının ne anlama geldiği daha anlaşılır hale gelecektir.

Öncelikle, uygulamaya döküldüğünde hiçbir iletişim kanalı gürültüsüz değildir. Bir A kaynağı B alıcısına böyle bir iletişim kanalından kuantum bilgi göndermek istiyorsa, üstün körü bir şekilde kuantum bitleri kanaldan göndermeden önce kanaldaki gürültü hakkında bilgi sahibi olmalıdır. Bu aşamada önceden kabul edilmiş 2 koşul bulunmaktadır:

Birincisi, gürültünün her kübite birbirinden bağımsız şekilde etki ettiğidir.

İkincisi, belirli bir kübit üzerindeki etkisi rastgele olarak kübitin durumunda hiçbir değişiklik gerçekleşmemesi ($1 - p$ olasılıkla) veya Pauli-X (kübit-dönüşü) işlemcisini uygulamasıdır ($p < {}^{1}/_{2}$ olasılıkla).

Bu yapay tipteki gürültünün etkisini düzeltmek ileride daha gerçekçi gürültü problemlerini çözmede işe yarayacak sonuçlar sağlayacaktır.



Şekil 5.1 Kübit-dönüşü hatası için tekrarlamalı 3 kübit kodu devresi

A kaynağı rastgele σ_x hatası ($|0\rangle \leftrightarrow |1\rangle$) ortaya çıkaran bir kanaldan B alıcısına bir tek kübit durumu $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ göndermek ister. Bu duruma ek olarak kaynak tarafında 2 ayrı işçi kübit $|0\rangle$ durumunda hazırlanır. Bunları da kullanarak tek kübit durumu 2 tane *CNOT* işlemi ile 3 kübitlik bir birleşik duruma kodlanır. Böylelikle başlangıç durumu $\alpha|000\rangle + \beta|111\rangle$ şeklini alır. Bu bileşik durum iletişim kanalına gönderilir. B alıcısı bu gönderiyi aldığında iletişim kanalındaki gürültüye maruz kalmış 3 kübit söz konusudur. B kaynağı, ulaşan bu birleşik durumu bir sendrom çıkarımı yaparak sendroma uygun şekilde geri kazanmaya çalışır. Düzeltme; kübitlerden birine (veya hiçbirine) σ_x işleminin uygulanmasıyla gerçekleştirilir. Son olarak kod çözme yöntemiyle başlangıçtaki tek kübitin diğerleriyle dolanıklığı sonlandırılır ve $1 - O(p^2)$derecesinde bir olasılıkla $|\Psi\rangle$ durumunda bir tek kübit elde edilir. Bu adımlar ve oluşabilecek durumların olasılıkları şu şekilde gerçekleşir:

Hiç hata meydana gelmediği durumda;

$$\alpha|000\rangle + \beta|111\rangle; \quad (1-p)^3. \tag{5.4}$$

En fazla 1 kübite hata meydana gelmesi olasılığı;

$$\alpha|100\rangle + \beta|011\rangle;\ p(1-p)^2,$$

$$\alpha|010\rangle + \beta|101\rangle;\ p(1-p)^2,$$

$$\alpha|001\rangle + \beta|110\rangle;\ p(1-p)^2. \tag{5.5}$$

En fazla 2 kübite hata meydana gelmesi olasılığı;

$$\alpha|110\rangle + \beta|001\rangle;\ p^2(1-p),$$

$$\alpha|101\rangle + \beta|010\rangle;\ p^2(1-p),$$

$$\alpha|011\rangle + \beta|100\rangle;\ p^2(1-p). \tag{5.6}$$

3 kübite de hata meydana gelmesi olasılığı;

$$\alpha|111\rangle + \beta|000\rangle; p^3. \tag{5.7}$$

Hata düzeltme işleminin daha şeffaf ve anlaşılabilir gerçekleşmesi için alıcı tarafında $|00\rangle$ şeklinde hazırlanmış 2 iş kübiti mevcuttur. Bu kübitler sayesinde gürültü hakkında bilgi edinilebilir.

Çizelge 5.1 Mantıksal kübitin sendrom ölçümünden hemen önce bulunabileceği durumlar (Devitt vd. 2013)

Hatanın konumu	Durum; |veri⟩|işçi kübit⟩
Hata yok	$\alpha\|000\rangle\|00\rangle + \beta\|111\rangle\|00\rangle$
1. Kübit	$\alpha\|100\rangle\|11\rangle + \beta\|011\rangle\|11\rangle$
2. Kübit	$\alpha\|010\rangle\|10\rangle + \beta\|101\rangle\|10\rangle$
3. Kübit	$\alpha\|001\rangle\|01\rangle + \beta\|110\rangle\|01\rangle$

Seri bir biçimde uygulanan CNOT geçitlerinin ardından alıcı 5 kübitin aşağıdaki durumlarından birini elde edebilir:

Hata meydana gelmediği durumda sendrom ölçümü;

$$(\alpha|000\rangle + \beta|111\rangle)|00\rangle; \quad (1-p)^3. \tag{5.8}$$

Kübitlerden 1 tanesinde hata meydana geldiğinde sendrom ölçümü;

$$(\alpha|100\rangle + \beta|011\rangle)|11\rangle;\ p(1-p)^{2,}$$

$$(\alpha|010\rangle + \beta|101\rangle)|10\rangle;\ p(1-p)^2,$$

$$(\alpha|001\rangle + \beta|110\rangle)|01\rangle;\ p(1-p)^2. \tag{5.9}$$

Kübitlerden 2 tanesinde hata meydana geldiğinde sendrom ölçümü;

$$(\alpha|110\rangle + \beta|001\rangle)|01\rangle;\ p^2(1-p),$$

$$(\alpha|101\rangle + \beta|010\rangle)|10\rangle;\ p^2(1-p),$$

$$(\alpha|011\rangle + \beta|100\rangle)|11\rangle;\ p^2(1-p). \tag{5.10}$$

Kübitlerin hepsinde hata meydana geldiğinde sendrom ölçümü;

$$(\alpha|111\rangle + \beta|000\rangle)|00\rangle;\ p^3. \tag{5.11}$$

Son eklenen bu 2 iş kübitinin $\{|0\rangle, |1\rangle\}$ bazında ölçülmesiyle 2 klasik bitlik bilgi elde edilir ve bu bilgiye *hata sendromu* adı verilir. Bu sayede alıcıya ulaşan kübitlerdeki hatanın türü ve yeri şu şekilde tespit edilir:

$$00 \leftrightarrow hiçbir\ şey\ yapma$$

$$01 \leftrightarrow 3.kübite\ \sigma_x\ uygula$$

$$10 \leftrightarrow 2.kübite\ \sigma_x\ uygula$$

$$11 \leftrightarrow 1.kübite\ \sigma_x\ uygula$$

Burada hata düzeltme adımına geçerken hatalar arasından en olası olanlara öncelik verilir. Mesela, ölçüm sonucu 10 ise olası hatalı durumlar ve o durumların oluşma olasılığı şu şekildedir:

$$\alpha|010\rangle + \beta|101\rangle;\ p(1-p)^2 \quad (5.12)$$

$$\alpha|101\rangle + \beta|010\rangle;\ p^2(1-p) \quad (5.13)$$

Çizelge 5.2 İşçi kübitler üzerinden yapılan ölçümlerin sonuçları (Devitt vd. 2013)

İşçi kübit ölçümü	Çöktüğü durum	Sonuç
00	$\alpha\|000\rangle + \beta\|111\rangle$	Hata yok
01	$\alpha\|001\rangle + \beta\|110\rangle$	3. kübitte σ_x hatası
10	$\alpha\|010\rangle + \beta\|101\rangle$	2. kübitte σ_x hatası
11	$\alpha\|100\rangle + \beta\|011\rangle$	1. kübitte σ_x hatası

Burada alıcı, daha olası bir durum olan 1. durumu kabul ederek 2. kübite σ_x uygular ve şu iki durumdan birini elde eder:

$$\alpha|000\rangle + \beta|111\rangle$$

$$\alpha|111\rangle + \beta|000\rangle$$

Ardından 1. kübitle 2. ve 3. kübit arasında birer CNOT geçidi uygulayarak adımları tamamlar ve şu sonuçlardan birini elde eder:

$$(\alpha|0\rangle + \beta|1\rangle)|00\rangle$$

$$(\alpha|1\rangle + \beta|0\rangle)|00\rangle$$

Alıcı, gönderilen kübitlerin birebir aynını veya σ_x uygulanmış halini elde eder fakat hangisi olduğunu bilemez. Ama burada önemli olan yöntemin başlangıçta$1-p$ olan hata düzeltmesiz durumdan daha yüksek bir başarı olasılığı olmasıdır. Bu yöntemle kanal sebebiyle en muhtemel durumlar olan hata oluşmadığı veya en fazla bir hata oluştuğu durumda başarılı bir şekilde hatanın düzeltilmesi hedeflenmiştir.

Çizelge 5.3 Çoklu hata oluşması durumunda sendrom ölçümü sonuçlarındaki belirsizlikler (Devitt vd. 2013)

Hata konumu	Durum; |veri⟩|işçi kübit⟩	Varsayılan hata türü
1. ve 2. kübit	$\alpha\|110\rangle\|01\rangle + \beta\|001\rangle\|01\rangle$	3. kübitte σ_x
2. ve 3. kübit	$\alpha\|011\rangle\|11\rangle + \beta\|100\rangle\|11\rangle$	1. kübitte σ_x
1. ve 3. kübit	$\alpha\|101\rangle\|10\rangle + \beta\|010\rangle\|10\rangle$	2. kübitte σ_x
1. , 2. ve 3. kübit	$\alpha\|111\rangle\|00\rangle + \beta\|000\rangle\|00\rangle$	Hata yok

Yöntemin başarısızlık olasılığıysa kanal tarafından en az 2 kübitte hata meydana gelmesiyle:

$$3p^2(1-p) + p^3 = 3p^2 - 2p^3 \tag{5.14}$$

olarak bulunur. Bu ifade $p < \frac{1}{2}$ olduğu sürece p'den küçüktür. Hata düzeltme yapılmamış olsaydı bu olasılık $O(p)$derecesinde olacakken, tekrarlı 3-kübit hata düzeltmeyle $O(p^2)$derecesine inmiştir. (Steane2006)

5.4 Tekrarlamalı 3-kübit Kodu (Faz–Dönüşü)

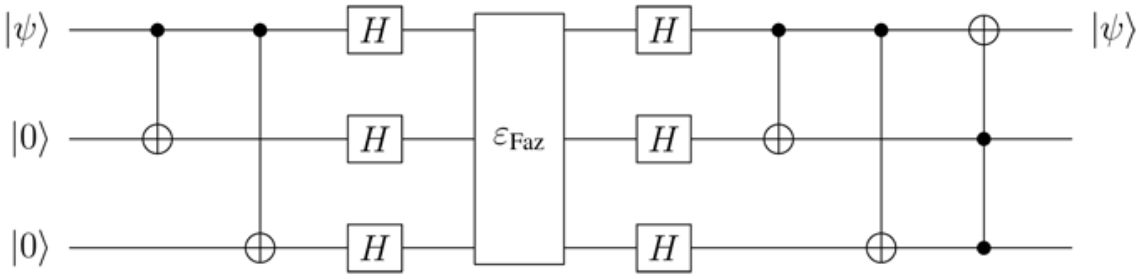
Benzer bir yaklaşım en fazla bir faz-dönüşü hatası için de uygulanabilir. Faz-dönüşü hatasının klasik bir karşılığı yoktur. Bu yaklaşımda da faz-dönüşü hatası bit-dönüşüne

çevrilmiş gibi işlem yapılır fakat kullanılan baz vektörleri farklıdır. Yukarıda kullanılan standart bazlar $\{|0\rangle, |1\rangle\}$ yerine bu hata türünü tespit etmeyi ve düzeltmeyi kolaylaştıran $\{|+\rangle, |-\rangle\}$ bazlarına Hadamard geçidi kullanılarak gönderim yapılır ve geri kazanma yoluna gidilir.

$$\{|0\rangle, |1\rangle\} \xrightarrow{H} \{|+\rangle, |-\rangle\} \xrightarrow{H} \{|0\rangle, |1\rangle\}$$

Standart bazlardaki bit-dönüşü hatasının etkisiyle yeni baz vektörlerindeki faz-dönüşü hatasının etkisi birbirine benzer. Bit-dönüşü hatasını gidermek için kullanılan Pauli-X işlemcisi gibi faz-dönüşü hatasını gidermek için Pauli-Z işlemcisini uygulamak yeterlidir:

$$Z|+\rangle = |-\rangle, \qquad Z|-\rangle = |+\rangle$$



Şekil 5.2 Faz-dönüşü hatası için tekrarlamalı 3-kübit kodu devresi

Devrenin birinci ve ikinci adımları bir önceki kodla aynı şekilde keyfi bir $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ kuantum durumu 2 ayrı işçi kübit $|0\rangle$ durumu kullanarak 2 tane *CNOT* işlemi ile 3 kübitlik bir birleşik duruma kodlar. Böylelikle başlangıç durumu $\alpha|000\rangle + \beta|111\rangle$ şeklinde kodlanmış olur. Fakat bir önceki devreye ek olarak bu devrede eşit dağılmış süperpozisyon üretecek şekilde paralel halde Hadamard geçitleri uygulanır. Yukarıdaki yol haritası izlendiğinde yeni baz vektörleri şu şekilde ifade edilir:

$$|+\rangle = H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \qquad |-\rangle = H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \tag{5.15}$$

Şekil 5.2'deki devrenin sonucu olarak bu baz vektörleriyle kodlanmış mantıksal kübit $|0_L\rangle = |000\rangle \rightarrow |+++\rangle, |1_L\rangle = |111\rangle \rightarrow |---\rangle$ olmak üzere $|\Psi\rangle_L = \alpha|+++\rangle + \beta|---\rangle$ şeklinde yazılır. Bu mantıksal kübit devreden iletilir:

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

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

İletilen mantıksal kübitte hata oluşup oluşmadığını ve oluştuysa hangi kübitte olduğunu öğrenmek için izdüşüm ölçümü yapılabilir. $|\Psi_i^F\rangle, i = 0,1,2,3$ olmak üzere sırasıyla hata gerçekleşmediği, hatanın birinci kübitte, ikinci kübitte, üçüncü kübitte gerçekleştiği durumlara karşılık gelecek şekilde şöyle ifade edilir:

$$|\Psi_0^F\rangle = |+++\rangle + |---\rangle,$$

$$|\Psi_1^F\rangle = |-++\rangle + |+--\rangle,$$

$$|\Psi_2^F\rangle = |+-+\rangle + |-+-\rangle,$$

$$|\Psi_3^F\rangle = |++-\rangle + |--+\rangle. \tag{5.16}$$

İzdüşüm ölçümü katsayılar a veya b hakkında bilgi vermez, sadece hangi kübitin hata düzeltici Pauli-Z işlemcisi uygulanmasına ihtiyacı olduğunu söyler. Bu devreye uygulanacak izdüşüm işlemcileri P_i^F, $i = 0,1,2,3$ olmak üzere şu şekilde hesaplanır:

$$P_i^F = |\Psi_i^{F(+)}\rangle\langle\Psi_i^{F(+)}| + |\Psi_i^{F(-)}\rangle\langle\Psi_i^{F(-)}| \tag{5.17}$$

$$P_0^F = |+++\rangle\langle+++| + |---\rangle\langle---|,$$

$$P_1^F = |-++\rangle\langle-++| + |+--\rangle\langle+--|,$$

$$P_2^F = |+-+\rangle\langle+-+| + |-+-\rangle\langle-+-|,$$

$$P_3^F = |++-\rangle\langle++-| + |--+\rangle\langle--+|. \quad (5.18)$$

Aynı izdüşüm ölçümü işlemlerini bit-dönüşü hatalarını düzeltmek üzere geliştirilen kodlarda kullanmak da mümkündür. Bit-dönüşü hatası düzeltmesinde sendrom çıkarımı aşaması yerine bu ölçüm eklenebilir. Bu işlem için faz-dönüşü için kullanılan izdüşüm işlemcilerini $P_i^B = H^{\otimes 3} P_i^F H^{\otimes 3}$ $(i = 0, 1, 2, 3)$ eşitliğinde kullanarak bit-dönüşü için geçerli olacak izdüşüm işlemcileri elde edilir.

Hata gerçekleşmiş olan kübit ile izdüşüm ölçümü sonucunda elde edilen sendrom arasında birebir örtüşme söz konusudur. Yani uygulandığı durumla örtüşmeyen izdüşüm işlemi 0 sonucu verir.

$$\langle \Psi_1^F | P_0^F | \Psi_1^F \rangle = 0, \quad \langle \Psi_3^F | P_2^F | \Psi_3^F \rangle = 0, \quad \langle \Psi_2^F | P_1^F | \Psi_2^F \rangle = 0$$

Devrede bulunabilecek durumlara uygulanan izdüşüm işlemcileri aşağıdaki şekildedir. Üçüncü kübitte hata oluştuğu varsayılırsa, bu durum için izdüşüm ölçümleri şu şekilde sonuçlanır:

$$\langle \Psi_0^F | P_0^F | \Psi_0^F \rangle = 0,$$

$$\langle \Psi_1^F | P_1^F | \Psi_1^F \rangle = 0,$$

$$\langle \Psi_2^F | P_2^F | \Psi_2^F \rangle = 0,$$

$$\langle \Psi_3^F | P_3^F | \Psi_3^F \rangle = 1. \quad (5.19)$$

İzdüşüm ölçümünün sonucuna göre tespit edilen hata için kübite o konuma özgü Z_i $(i = 1, 2, 3)$ işlemcisi bit-dönüşü kodunda olduğu gibi uygulanır. Devrenin

devamında süperpozisyon haldeki kübitlere birer Hadamard geçidi uygulanır. Bu geçidin ardından kuantum durum, daha önce işlem yapılan $|0_L\rangle = |000\rangle, |1_L\rangle = |111\rangle$ mantıksal durumlara dönüşmüş olur. Bu geçitten sonra uygulanacak 2 adet *CNOT* geçidi sayesinde gönderilmek istenen kübit işçi kübitlerden ayrılarak alıcıya iletilir.

5.5 Bütüncül Faz-Yitimi Modeli

Eş-uyum yitimi; kuantum sisteminin dış çevreyle etkileşiminden ötürü eş-uyumunu (*coherence*) yitirmesidir ve şu şekilde modellenebilir:

$$|0\rangle \rightarrow |0\rangle, \qquad |1\rangle \rightarrow e^{i\theta}|1\rangle$$

Bu modele göre keyfi bir $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ kübiti eş-uyum yitimine uğradığında $|\Psi\rangle = \alpha|0\rangle + e^{i\theta}\beta|1\rangle$ ifadesine dönüşür. Fakat keyfi bir kübit durumu $|\Psi\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ şeklinde ifade edildiğinde yoğunluk matrisi:

$$\rho = \frac{1}{2}\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix} \rightarrow \frac{1}{2}\begin{pmatrix}1 & e^{-i\theta}\\ e^{i\theta} & 1\end{pmatrix} \tag{5.20}$$

şeklinde dönüşüme uğrar ve köşegen dışı terimlerin faz yitiminden benzer şekilde etkilendiği görülür. Eş-uyum yitimini azaltmak için kullanılan bu modele ortaklaşa faz-yitimi denir. Çevreyle etkileşimin sebep olabileceği bu tarz hataların önüne geçmekte kullanılan yaygın modellerden biridir.

Çıkış noktası; süperpozisyon terimlerinin bir veya birkaçına etkiyen *bağıl faz* (*relative phase*) çarpanı ölçüm sonuçlarını değiştirirken, hepsine etkiyen bir *bütüncül faz* (*global phase*) çarpanının ölçüm sonuçlarına etki etmeyecek olmasıdır. Mantıksal kübitler ($|0_L\rangle \, ve \, |1_L\rangle$) devreye alınarak eş-uyum yitiminden müstesna altuzay gönderimi yapmak suretiyle problem giderilir. $|0_L\rangle \, ve \, |1_L\rangle$ mantıksal kübitleri şu şekilde ifade edilmektedir:

$$|0_L\rangle = \frac{|0\rangle|1\rangle - i|1\rangle|0\rangle}{\sqrt{2}}, \qquad |1_L\rangle = \frac{|0\rangle|1\rangle + i|1\rangle|0\rangle}{\sqrt{2}}. \tag{5.21}$$

Ortaklaşa faz yitimi modeline göre eş-uyum yitimine maruz kalan bu mantıksal kübitlerin dönüşümleri sırasıyla şöyle gerçekleşir:

$$|0_L\rangle \to \frac{|0\rangle e^{i\theta}|1\rangle - ie^{i\theta}|1\rangle|0\rangle}{\sqrt{2}} = e^{i\theta}\frac{|0\rangle|1\rangle - i|1\rangle|0\rangle}{\sqrt{2}} = e^{i\theta}|0_L\rangle \tag{5.22}$$

$$|1_L\rangle \to \frac{|0\rangle e^{i\theta}|1\rangle + ie^{i\theta}|1\rangle|0\rangle}{\sqrt{2}} = e^{i\theta}\frac{|0\rangle|1\rangle + i|1\rangle|0\rangle}{\sqrt{2}} = e^{i\theta}|1_L\rangle. \tag{5.23}$$

Dönüşümlerin ardından keyfi mantıksal kübitlerin ikisi de eş-uyum yitiminden etkilenmeyecek şekilde sadece bütüncül faz çarpanına sahiptir.

$$|\Psi\rangle_L = \alpha|0_L\rangle + \beta|1_L\rangle \to e^{i\theta}\alpha|0_L\rangle + e^{i\theta}\beta|1_L\rangle = e^{i\theta}|\Psi\rangle_L. \tag{5.24}$$

Kuantum durumu da yukarıdaki şekilde evrilmesi sayesinde hataya maruz kalmaz (McMahon 2007).

5.6 Bit-Faz Dönüşü ve 4-Boyutlu Hata Altuzayı

Göndermek istenilen kübitte oluşabilecek hem bit-dönüşü hem de faz-dönüşü hatalarını gideren bir kod olsa bile bunların dışında sonsuz sayıda başka hata oluşamaz mı? Bu sebeple kullanılacak koda sonsuz miktarda ekleme yapılması gerekmez mi? Kuantum mekaniğinin estetik yönlerinden biri tam da burada devreye girer. Eğer ki bir kuantum hata düzeltme kodu hem bit-dönüşü hem de faz-dönüşü hatalarına karşı koruma sağlıyorsa, mümkün olan tüm tek-kübit hatalarına karşı koruma için de yeterli olur. Bu önemli tespit keyfi bir kübit durumu ele alınmak suretiyle aşağıda şekilde ifade edilebilir:

Dolanık bir $|\Psi_0\rangle = \alpha|0\rangle|v\rangle + \beta|1\rangle|w\rangle$ durumunun birinci kübitinde hata olduğu varsayılır. Birinci kübitte bir bit-dönüşü hatası olursa; başlangıçtaki durum $|\Psi_1\rangle = \alpha|1\rangle|v\rangle + \beta|0\rangle|w\rangle$ halini alır. Yine birinci kübitte bir faz-dönüşü hatası gerçekleşirse; $|\Psi_2\rangle = \alpha|0\rangle|v\rangle - \beta|1\rangle|w\rangle$ olur.

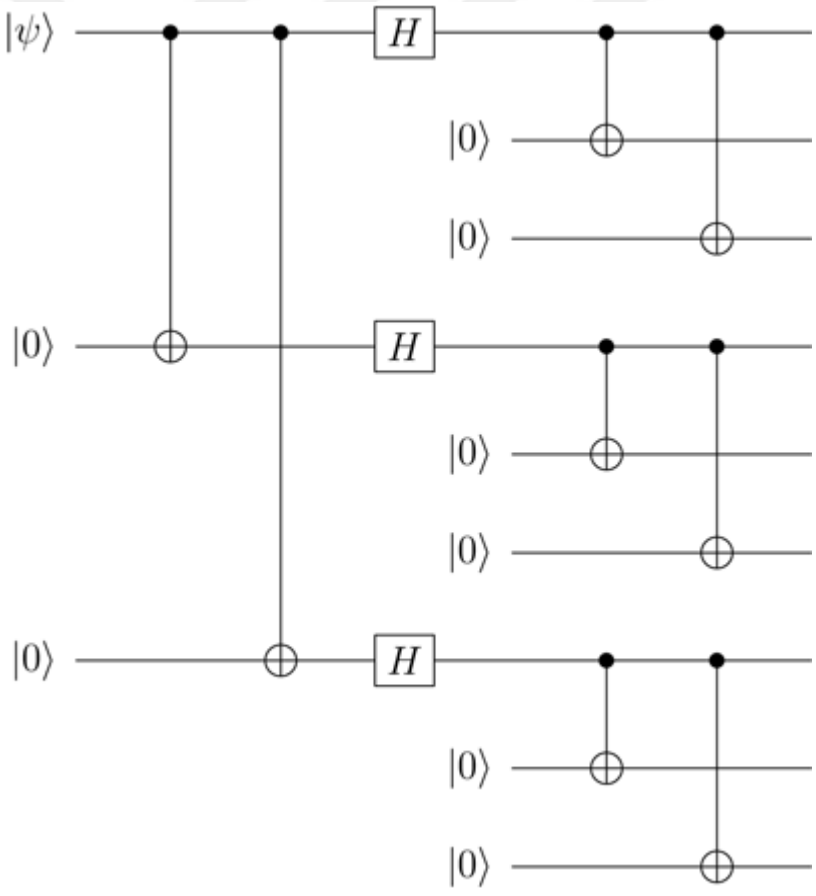
Hem bit-dönüşü hem de faz-dönüşü olması (bit-faz dönüşü); $|0\rangle \rightarrow |1\rangle$, $|1\rangle \rightarrow -|0\rangle$ şeklinde gerçekleşmektedir. Bu dönüşüm gerçekleşirse; $|\Psi_3\rangle = \alpha|1\rangle|v\rangle - \beta|0\rangle|w\rangle$ şeklinde dördüncü bir ifadeye ulaşılır.

Böylelikle yukarıdaki koda sonsuz ekleme yapma açmazını çözecek, $|\Psi_0\rangle$'dan başlayarak birinci kübite uygulanacak dönüşümlerle ulaşılabilecek bütün durumların 4-boyutlu altuzayının baz vektörleri elde edilmiş olur. Yani hatanın birinci kübitte olduğu varsayımıyla, bu 4-boyutlu hata uzayında hangi durum olursa olsun $|\Psi_0\rangle$ başlangıç durumuna dönebilir. Mümkün olan bütün üniter dönüşümler kapsandığında, otomatik olarak mümkün olan bütün hatalar da kapsanmış olur. Keyfi bir hata saf bir durumu saf olmayan bir duruma çevirebilir fakat yine de aynı 4-boyutlu alt uzay içerisinde kalır. Yani bir ölçüm ancak ortogonal $|\Psi_0\rangle, |\Psi_1\rangle, |\Psi_2\rangle, |\Psi_3\rangle$ durumlarından birine izdüşürebilir ve başlangıçtaki $|\Psi_0\rangle$ durumuna ulaşmak için tek yapılması gereken bit-dönüşleri ve faz-dönüşlerini uygulamaktır (Aaronson 2018).

5.7 Shor'un 9-kübit Hata Düzeltme Kodu

Kuantum hata düzeltme şemalarının ilki örneği olan Shor'un 9-kübit kodunun (Shor 1996) hataları algılamak ve düzeltmek için nasıl kullanıldığını incelemek, önceki konularda bahsedilen yöntemlerin nasıl harmanlanıp eşgüdümlü hale gelebileceğini görmek açısından önemlidir. Her biri 3'er tane fiziksel kübitten oluşan mantıksal kübitler tanımlayarak aynı anda hem bit-dönüşü hem de faz-dönüşü hatalarının giderilebilmesi kuantum bilgiişlem açısından kilometre taşı niteliğindedir. Kuantum hata düzeltmenin akademik çevrelerce onay görmesi ve bu yöndeki araştırmaların ivme kazanmasını sağlamıştır.

Keyfi bir $|\Psi\rangle = \alpha|1\rangle + \beta|0\rangle$ kuantum durumunda oluşabilecek hem Pauli-X, hem Pauli-Z, hem de Pauli-Y hatalarına karşı bu durumu koruyabilen bu kodun çalışma prensibi; bit-dönüşü ve faz-dönüşü için tekrarlamalı 3-kübit kodlarının bir kombinasyonu şeklindedir. Shor'un 9-kübit koduna ait devrede kodlama önce faz-dönüşü kodundaki gibi yapılır ardından elde edilen kodlanmış kübit bu sefer bit-dönüşü kodu için geçerli dönüşümlere uğrar. Bu hiyerarşik seviyeli kodlama yapısıyla *birleştirmeli kodlara* basit ve güzel bir örnektir. Bahsedilen 3 farklı hatayı da algılayabilmesi ve düzeltebilmesi sebebiyle de 4-boyutlu hata altuzayını kapsar. Bu sayede bir kübitin kaybolması veya kübitlerden birinin $\frac{\Pi}{88}$ gibi bir fazla dönüşü gibi oluşabilecek keyfi hataları da düzeltebilir. Shor 9-kübit koduna şu şekilde ulaşılır:



Şekil 5.3 Shor 9-kübit koduna ait kodlama devresi

$$|0\rangle \rightarrow |+++\rangle, \qquad |1\rangle \rightarrow |---\rangle$$

şeklinde faz-dönüşü koduna uygun şekilde süperpozisyon hale getirilir. Ardından bit-dönüşü koduna ait devredeki ilk iki adım uygulanır:

$$|+\rangle = \frac{|000\rangle + |111\rangle}{\sqrt{2}}, \qquad |-\rangle = \frac{|000\rangle - |111\rangle}{\sqrt{2}}. \tag{5.25}$$

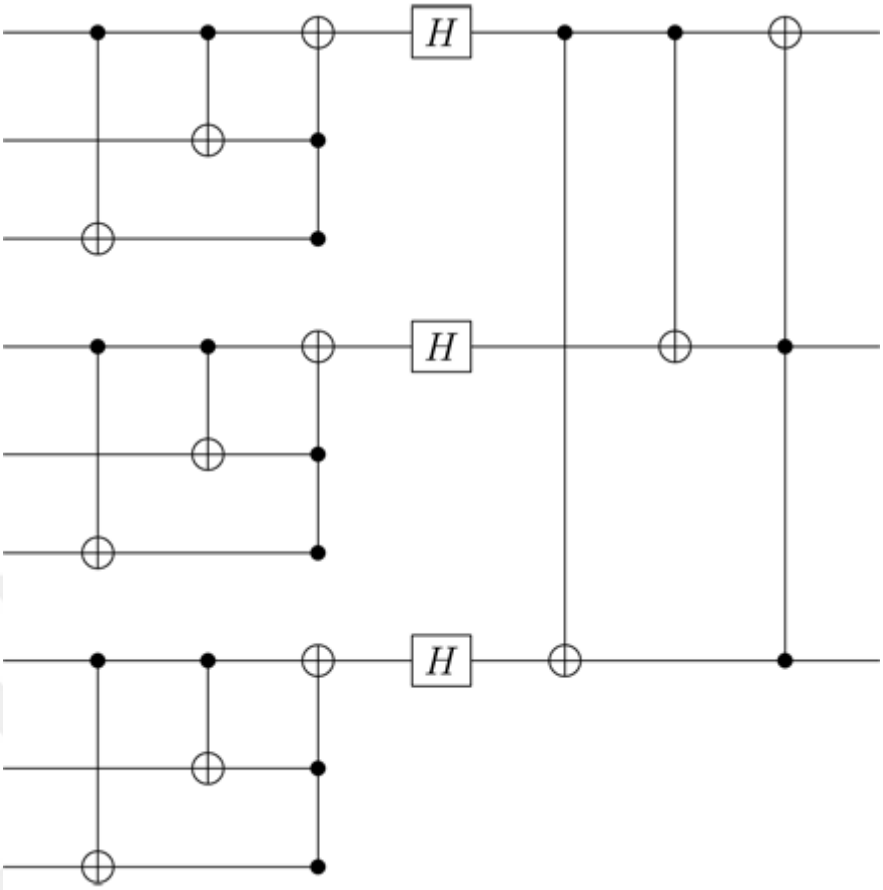
Bu dönüşümün ardından Shor'un koduna ait mantıksal kübitler şu şekilde yazılır:

$$|0_L\rangle = \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle) \tag{5.26}$$

$$|1_L\rangle = \frac{1}{2\sqrt{2}}(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle). \tag{5.27}$$

İlk bakışta böyle bir kodlamanın sağladığı avantajlar fark edilemese de 9-kübit kodunun devresi incelendiğinde, kodlamadaki sadelik ve basitlik harikadır.

Kodlama işlemi tamamlandığında artık 3 tane 3-kübitlik blok mevcuttur. Bunlar hataları tespit etmekte karşılıklı olarak ölçüt yerine kullanılır ve bu sayede ölçüm yaparak süperpozisyona zarar verme durumu ortadan kalkar.



Şekil 5.4 Shor 9-kübit koduna ait kod çözme devresi

Devre, hata oluşumunu sorgulamaya bit-dönüşünü olup olmamasını kontrol ederek başlar. Bunu yaparken her kod kelimesi blokunu kendi içinde, kübitler arası karşılaştırma yaparak sınar. Öncelikle 1. ve 2. kübit, ardından 2. ve 3. kübit karşılaştırılır ve bit-dönüşü gerçekleşmiş olan varsa tespit edilir. Bu sınama her blokta uygulanır. Bit-dönüşü tespit edilen kübite Pauli-X işlemcisi uygulanarak geri kazanılır. İkincil olarak faz-dönüşü hatasını tespit etmek için işaret karşılaştırması yapılır. Fakat bu karşılaştırma yapılırken bit-dönüşünde olduğu gibi kübitler üzerinden değil bloklar üzerinden ilerlenir. Aynı sıraya uyarak blokların işaretleri ikişerli olarak karşılaştırılır ve hata oluşmuş olan blok tespit edilir. Faz-dönüşüne uğramış olan 3 kübitlik blok Pauli-Z işlemcisi uygulanarak hatadan arındırılır (Shor 1995).

Shor'un 9-kübit kodunun en göze çarpan özelliklerinden biri de ayrı kübitlerde oluşabilecek bit-dönüşü ve faz-dönüşünü hatalarını düzeltebilmesidir. Bunun yanı sıra

bit-faz dönüşünü de düzeltebiliyor olması ortaklaşa faz yitimi modeliyle benzerliğinden ileri gelmektedir. Pauli işlemcileri arasındaki $Y = iXZ$ eşitliğindeki i katsayısının bir bütüncül fazı temsil etmesi sayesinde bu sebeple oluşabilecek eş-uyum yitiminin önüne geçmektedir.

6. SONUÇ

Kuantum mekaniği yasalarının hem sınırlayıcı hem de bir o kadar çığır açıcı yaklaşımlar ortaya çıkmasına sebep olması kuantum bilişimin gerçekleşmesini mümkün kılmaktadır. Bunun da en büyük örneği kuantum hata düzeltmedir. 3. bölümünde bahsi geçen engeller, öncelikle aşılması zor birer bariyer niteliğindedir. Fakat kuantum mekaniğinin elverişli yapısı sayesinde bilişim sürecindeki engeller aşılabilmektedir.

No-Cloning teoremi, işçi kübitlerin kullanımı ile tekrarlı kodlama ve benzeri yaklaşımlar sayesinde bir engel olmaktan çıkmış ve en temel kuantum hata düzeltme kodlarının önü açılmıştır. Sendrom çıkarımı ve izdüşüm ölçümleri sayesinde süperpozisyona zarar vermeden durumlar hakkında ihtiyaç duyulan (olasılık katsayıları hariç) bilginin elde edilmesi mümkün hale gelmiştir. Hatta Gottesman tarafından öne sürülen kararlılaştırıcı kodlar sayesinde bu işlemlerin gerçekleştirilmesi hem daha güvenli hem de daha hızlı bir hale gelmiş ve birçok algoritma buna göre güncellenmiştir. Bahsi geçen bu iki engelin aşılması, sonraki iki engeli de aşmak için ön ayak olmuştur. Birleştirmeli kodlar sayesinde (örn. Shor 9-kübit), farklı türde hatalara karşı hazırlanmış devreler bir araya getirilerek bir veya birden çok türde hata oluşması durumlarında da etkili olabilecek hiyerarşik seviyeli devreler oluşturulmuştur. Son olarak, sürekli hataların düzeltilmesinin sınırsız kaynak gerektireceği görüşü de hata altuzayları yaklaşımı yardımıyla bir engel olmaktan çıkmıştır.

Mantıksal işlemlerin mükemmel algoritmaları etkidiği sistemde hata üretmiyor gibi bir varsayım vardır ve bu algoritma tasarımını kolaylaştırır ama gerçekçi değildir. Fakat bunu sağlamak için çok sayıda mükemmel olmayan cihazı kullanarak kabul edilebilir hata olasılığı eşiği (*treshold*) yardımıyla mükemmel bir cihazın yaptığı işlemleri taklit etmek üzere tasarlanmış hata toleranslı kuantum bilişim modeli kullanılmaktadır (Shor 1996). Aynı yıl içinde eşik değeri çalışmaları bir hayli öne çıkmıştır ve farklı kuantum bilişim süreçlerine uygulanması çalışmaları başlamıştır. Hata toleranslı kuantum bilişimde önemli noktalar; hataların sayısının azaltılması ve kaynak kullanımının mümkün olan en düşük seviyeye indirilmesidir. Bu yöntemin gerekliliklerini sıralamak

gerekirse; geçitlerden kaynaklı hata oranın düşük olması, işlemlerin paralel yürütülebilmesi, hesaplamasal bazların Hilbert uzayına dönme veya orada kalma yollarının üretilmesi, hesaplama esnasında yeni kübitler sağlayabilecek bir kaynak, büyük çaplı korale hataların olmayışı ve hata oranının bilgisayar boyutu arttıkça artmaması şeklindedir.

Günümüzde hata toleranslı mantıksal kübitlerin elde edilmesi konusuna hem devletler hem de teknoloji devi şirketler (D-Wave, IBM, Microsoft, Google) büyük ilgi göstermektedir. Bunun sağlanması ve işlemci ve bileşen bazında iyileştirmeler sayesinde kuantum bilişimin bir hayal olmaktan çıkıp günlük hayatta yerini almaması için hiçbir sebep kalmayacak.

KAYNAKLAR

Aaronson, S. 2018. Quantum Error Correction. Ders notu. Bağlantı: https://www.scottaaronson.com/qclec/

Alizadeh, Y. 2016. Quantum Error Correction Methods. Yüksek Lisans Tezi. Eastern Mediterranean University. Gazimağusa.

Almlöf, J. 2016. Quantum error correction. Doktora tezi. Stockholm.

Barnum, H., Nielsen, M. A., and Schumacher, B.1997. Information transmission through a noisy quantum channel. arXiv:quant-ph/9702049. Phys. Rev. A 57, 4153.

Benenti, G., Casati, G. and Strini, G.2007. Principles of Quantum Computation and Information Volume II: Basic Tools and Special Topics. World Scientific.

Bennett, C. H., DiVincenzo, D. P., Smolin, J. A. and Wootters, W. K.1996. Mixed-state entanglement and quantum error correction. Phys. Rev. A, 54:3824-3851.

Criger, D. B. 2013. Practical Advances in Quantum Error Correction and Communication. Doktora Tezi. Waterloo University, Canada.

Devitt, S. J., Munro, W. J. and Nemoto, K. 2013. Quantum error correction for beginners. Rep. Prog. Phys. 76 (2013) 076001.

DiVincenzo D. P. and Shor, P. 1996. Fault-tolerant error correction with efficient quantum codes. Phys. Rev. Lett.77, 3260.

DiVincenzoD. P.2000. The physical implementation of quantum computation. Fortschritte der Physik, 48 (9-11):771-783.

Gaitan, F. 2008. Quantum Error Correction and Fault Tolerant Quantum Computing. CRC Press. Illinois.

Gottesman, D. 1996. Class of quantum error-correcting codes saturating the quantum Hamming bound. Phys. Rev. A54, 1862.

Gottesman, D. 2004. Stabilizer Codes and Quantum Error Correction. Doktora Tezi. California Institute of Technology. Pasadena, California.

Kempe, J. 2007. Quantum Decoherence - Poincare' Seminars 2005: Approaches to Quantum Error Correction. Birkhäuser Basel.

Knill, E. and Laflamme, R. 1997. A theory of quantum error-correcting codes. Phys. Rev. A55, 900.

Knill, E.2005. Quantum computing with realistically noisy devices. Nature, 434(7029):3944.

Knill, E., Laflamme, R., Ashikhmin, A., Barnum, H., Viola, L. and Zurek, W. H. 2008. Introduction to Quantum Error Correction. arXiv:quant-ph/0207170v1. Los Alamos Science 27, 188.

Marinescu, D. C., Marinescu, G. M. 2012. Classical and Quantum Information. Elsevier.

McMahon, D. 2007. Quantum Computing Explained. Wiley-IEEE Press.

Nakahara, M. and Ohmi, T. 2008. Quantum Computing: From Linear Algebra to Physical Realizations. CRC Press. Japan.

Nielsen, M. A. and Chuang, I. L.2000. Quantum Computation and Quantum Information. Cambridge University Press, Cambridge.

Schumacher, B. 1996. Sending entanglement through noisy quantum channels. Phys. Rev. A, 54:2614-2628.

Schumacher, B. and Westmoreland, M. D.1997. Sending classical information via noisy quantum channels. Phys. Rev. A, 56:131-138.

Shannon, C. E. 1948. A mathematical theory of communication. Bell Sys. Tech.J.27, 379, 623.

Shor, P. W. 1995. Scheme for reducing decoherence in quantum computer memory. Phys. Rev. A, 52:R2493.

Shor, P. W. 1996. Fault-tolerant quantum computation. arXiv:quant-ph/9605011. Proceedings of the 1996 Symposium on Foundations of Computer Science, Burlington, Vermont, USA.

Steane, A. M. 2006. A Tutorial on Quantum Error Correction, IOS Press, Amsterdam.

Verçin, A. ve Dereli, T. 2009. Kuantum Mekaniği Temel Kavramlar ve Uygulamaları. Tüba Yayınları, Ankara.

Watrous, J. 2011. Theory of quantum information. Ders notları. Bağlantı: https://cs.uwaterloo.ca/~watrous/LectureNotes.html

Williams, C. 2011. Explorations in Quantum Computing. 2nd Ed. Springer BBS.

Wootters, W. and Zurek, W. 1982. A Single Quantum Cannot be Cloned. Nature Vol. 299, p. 802–803

ÖZGEÇMİŞ

Adı Soyadı	: Haydar KIZILIRMAK
Doğum Yeri	: ANKARA
Doğum Tarihi	: 26.03.1989
Medeni Hali	: Evli
Yabancı Dil	: İngilizce

Eğitim Durumu

Lise	: Çağlayan Lisesi (YDL) (2007)
Lisans	: Gazi Üniversitesi Fizik Bölümü (2013)
Yüksek Lisans	: Ankara Üniversitesi Fen Bilimleri Enstitüsü Fizik Anabilim Dalı (Şubat 2020)

Çalıştığı Kurum/Kurumlar ve Yıl

Ercem İnşaat Ltd. Şti. 2016-2017

Kitapçı Dağıtım Ltd. Şti. 2018-2019