# KUANTUM BİLGİSAYARLARA GİRİŞ

Prof. Dr. İhsan YILMAZ

4 Mayıs 2018

# İçindekiler

# Bölüm 1

# Kuantum Bilgisayarlar

Molekül, atom, atom altı parçacıklar ve foton davranışlarının bilgi iletişiminde kullanılmasına dayanan bilgisayarlardır. Kuantum bilgisayarlar denilmesinin sebebi moleküli atom, atom altı parçacıklar ve fotonun davranışlarını inceleyen bilim dalı Kuantum Fiziği olduğundan dolayıdır.

## 1.1 Kuantum Bilgisayarların Ortaya Çıkış Nedeni ve Diğer Bilgisayarlardan Farkları

**1)** Kuantum bilgisayarlar diğerlerinin aksine 0 ve 1'i aynı zamanda 0,1 arasındaki tüm olası durumları aynı anda değerlendirdiklerinden klasik bilgisayarlara göre üstün ve hızlı işlem yapabilme kapasitesine sahiptirler. Örneğin 64 bitlik klasik bilgisayar ile 64 qubitlik (kuantum biti) kuantum bilgisayar karşılaştıracak olursak bu tür bir kuantum bilgisayar klasik bilgisayara göre $2^{64}$ tane işlemi aynı anda yapabilecek üstün kapasiteye sahip demektir. Bu hızın sebebi 0 ve 1'in aynı anda değerlendirilmesi (süper pozisyon durumu)ndan dolayıdır.

Bununla birlikte klasik bilgisayarlardaki transistör teknolojisi gelebileceği (küçülebileceği) en son noktaya gelmiş durumdadır. Daha alt durumlarda işin içine molekül, atom, atom altı parçacıkları girdiğinden bu parçacıkların davranışları da kuantum yasalarla açıklandığından Kuantum Bilgisayar fikri ortaya çıkmıştır.

**2)** Molekül, atom, atom altu parçacıkları ve fotonun doğasında bulunan dolanıklık (entanglement) durumu klasik bilgisayarlarda olmayan fakat kuantum bilgisayarlarda mevcut olup diğer bilgisayarlara göre üstünlük oluşturmaktadır.

**Tanım 1. (Dolanıklık):** A ve B gibi iki olay birbirinden çok çok uzakta olsalar bile daha önce var olan ilişkiden yararlanarak A olayında yapılan ölçümde B olayında hiç ölçüm yapmadan B olayı hakkında bilgi edinilmesidir.

Kuantum bilgisayarlarda bu özellikten yararlanılarak başlangıçta dolanık olmayan durumlar kapılar yardımıyla dolanık hale getirilebilmektedir.

Dolanıklık özelliği Kuantum kriptoloji, teleportasyon ve çeşitli algoritmalarla büyük kolaylıklar ve aynı zamanda farkındalıklar sağlamaktadır.

**3)** Dolanıklık özelliği bir verinin aynı anda bir yerden başka bir yere aktarılmasına (Teleportasyon) olanak sağlamaktadır. (bir anlamda arada kablo hat olmadan ışınlanma birebir var olan anlamda) Bu işlem dolanıklık sayesind arada hiç bir bağlantı olmadan yapılabilmektedir.

**4)** Kuantum bilgisayarda ölçme tüm olası durumların tek bir duruma çökmesi demektir. Bu nedenle kuantum bilgisayarda iki iletişim kanalı arasına giren kişi ölçme yapacağından ölçme sonucunda da ona sistemin durumu değişeceğinden kişi almak istediği bilgiyi tam olarak alamamış olacaktır. Yani kuantum bilgisyarda kopyalama işlemi klasik anlamda mümkün değildir. (nc-claning theorem)

**5)** Yukarıdaki özelliklerden de görüldüğü gibi insanoğlu daha önce 0 veya 1'leri kullanarak elektirik vasıtasıyla klasik bilgisayarda işlem yaptırırken bugünki teknoloji ile artık molekül, atom, atom altı parçacıklar ve fotonlar vasıyasıyla bilgisayarlara iş yaptırır duruma gelmiştir.

Bu teknoloji ile uzay yolculuğu da farklı noktaya gelecektir. Bu konuşulanlar bilgi ışınlanmasıdır. Fakat canlı ışınlanması ile de çalışmalar mevcuttur.

**Not 1.** Bugünlerde her ne kadar kuantum bilgisayarlar önde gözükse de bu (kuantum teknoloji) aslında insanoğlu yaşamında sanayi ve bilişim çağı devrimi gibi bir devrim niteliğindedir çünkü kuantum teknoloji alanındaki gelişmeler, tıp teknolojisinde, sanayi teknolojisinde ve diğer bütün alanlarda da olmaktadır. Bu bağlamda bu alanlardaki gelişmeler insanlık yaşamında çok büyük algılamalara da sebep olacaktır. Örneğin bu teknolojinin gelişmesi ile birlikte evrendeki bilinmeyenler hakkında bilgi sahibi olunabilecek, algılanamayan nesneler bu teknoloji ile kolay algılanabilecektir, anlık iletişim sayesinde insanlık başka bilinmeyenleri de bilir duruma gelebilecektir. Belki de yakın gelecekte insanlık aynı anda tüm dünyadaki insanlarla görüntülü olarak anlık olarak görüşme imkanı bulabilecektir.

## 1.2 Kuantum Bilgisayarların Gerçekleştirme (Yapılış) Yöntemleri

Kuantum bilgisayarlar molekül, atom, atom altı parçacıklar ve fotonun davranışlarından yararlanılarak çeşitli yöntemlerle gerçekleştirilmeye çalışılmaktadır. Bunlardan şu anda en

çok kullanılanlar nükleer manyetik rezonans (NMR), kuantum dot'lar, iyon tuzaklama yöntemleri, süper iletkenler ve ışığın polarizasyonu gibi yöntemlerdir.

### NMR Yöntemi:

Bu yöntemin ana dayandığı molekül, atom, atom altı parçacıkların manyetik alanlardaki davranışlarıdır. Çünkü molekül, atom, atom altı parçacıklar manyetik alanın etkisi ile farklı davranışlar gösterebilmektedir. Bu farklı davranışlar her bir atomun kendisine has özelliği olan Larmar frekansı yardımıyla ölçülebilmektedir. Bu bağlamda 3, 7, 16, 64 ve 128 qubitlik kuantum bilgisayarlar dünyada çeşitli laboratuvarlarda üretilmiştir.

### İyon Tuzaklama Yöntemi:

Bu yöntemin ana kaynağı çeşitli molekül ve atomların iyonlarının belli bölgeye hapsedilerek bu bölgedeki kuantum davranışlarının bilgi iletişiminde kullanılmasına dayanmaktadır. En çok kullanılan atom ve moleküller klor, flor, karbon ve bunların oluşturdukları moleküllerdir. (Niye bunlar: kararlı yapıda olmalarından) Bu yöntemle 215 qubitlik kuantum bilgisayarlar oluşturulduğu söylenmektedir.

### Işığın Polarizasyon Yöntemi:

Bu yöntem adındanda anlaşılacağı gibi ışığın farklı açılarda polarizasyonuna dayanmaktadır. Işığın polarize olmamış ve olmuş durumları kalsik anlamda 0 ve 1 lere karşılık getirilir. Şu anda mevcut hemen hemen tüm kuantum anahtar dağıtım cihazları (quantum key distribition) bu temelli çalışmaktadır. Çünkü şu anda dünyadaki bigisayarlar arasındaki iletişim fiber optik kablo ile yani fotonla yapılmaktadır.

### Kuantum Dotlar (Noktalar):

Bu yöntemde atom ve ya molekül bir noktada hapsedilip noktalar arasındaki geçişler diğer bir değişle enerji farkları kullanılmaktadır.

**Not 2.** Yukarıdaki yöntemlerin yanısıra süper iletken teknoloji yöntemleri çeşitli moleküllerin birleştirilmesi yöntemleri nano düzeye geliştirilmeye çalışılmaktadır. Bütün bu gelişmelere rağmen şuanda en çok kullanılan yöntem ışığın polarizasyon yönetimidir. Bunun sebebi ise şuanda tüm dünyadaki veri iletişiminde kullanılan fiber optik kabloların mevcut olması ki bu kablolarda da veri fotonla (ışıkla) iletildiğindendir.

## 1.3 Kuantum Bilgisayarlar ile İlgili Çalışmalar

Kuantum bilgisayarlar ile ilgili dünyada birçok alanda çalışma yapılmaktadır. Kuantum bilgisayarlar yapımıyla ilgili çalışmaların yanında **kuantum programlama dilleri** (örneğin Microsoft'un geliştirdiği **Liquid**, birçok araştırmacının geliştirdiği **quipper**, **QDil** vb.), **kuantum internet** (Amerika askeri projeler DARPA) kapsamındaki geliştirilmiş internet ağı yaklaşık 10 yıldır kullanılmaktadır, benzer bir internet ağı Japonya'nın Tokyo şehrinde mevcuttur. Yine benzer bir internet ağı Avusturya Viyana şehrinde, yine benzer bir internet ağı Almanya'da mevcut olup Çin ve İsrail gibi ülkeler bu tür internet ağlarını geliştirmiş durumdadır. Kuantum kriptoloji de kullanılan **kuantum anahtar dağıtım aletleri** (Amerika, Kanada, Avusturya, Almanya gibi bir çok ülke tarafından üretilmiş olup bazıları da satışa sunulmuştur.), **kuantum wifi**, **kuantum çip** alanlarında da çeşitli gelişmeler olmaktadır.

**Not 3.** Yukarıda bahsedilen kuantum bilgisayar alanındaki gelişmelerin yanında tıp, uzay, sanayi, uçak teknolojileri, telefon teknolojileri gibi bir çok alanda gelişmeler olmaktadır. Bu da insanlık tarihinde sanayi devrimi gibi devrim niteliğinde olacak olan kuantum teknoloji devriminin geldiğinin bir habercisidir.

**Not 4.** Bir çok laboratuvarda farklı yöntemlerle kuantum bilgisayarlar gerçekleştirilmiş olsa da şuanda NASA, Google, CIA ve Martin Locked Silah Sanayi'nin kaullandığı ticari amaçlı D Wave firması tarafından satılan kuantum bilgisayarı mevcuttur. Bu bilgisayar klasik bir bilgisayar tarafından kontrol edilen bir bilgisayar ve son olarak piyasaya sürülen 1012 qubitlik kuantum bilgisayarı $2^{1012}$ işlemi aynı anda yapabilme kapasitesine sahiptir.

Google ve NASA 2013 yılında kendi bilgisayarlarını geliştirmede ve bu alanda çeşitli çaışmalara öncülük etmek amacıyla yaklaşık 20000 kişinin çalıştığı bir laboratuvar kurmuşlardır. Bu laboratuvarlarda kuantum bilgisayarlarla ve kuantum teknoloji ile ilgili çeşitli çalışmalar yürütülmektedir.

**Tanım 2. (Uzay Kavramı):** Olayların içinde meydana geldiği ve olayları ifade etmemize yarayan ve aynı zamanda doğadaki 4 temel etkileşim (zayıf etkileşim, güçlü etkileşim, elektromanyetik etkileşim ve gravitasyonel etkileşim) sonucu farklılaşan durumların sonucu meydana gelen koordinat sitemidir. Bu uzayın koordinat sitemi yukarıdaki etkileşimler bağlamında şekillenmektedir. Örneğin büyük ölçekteki yapılar (gravitasyonel etkileşimin kontolü altında) Riemann Geometrisi ile incelenir. Bu geometri eğrilikli bir geometridir. Daha küçük ölçekteki yapılar Oklid Geometrisi ile incelenir. Molekül, foton ve atomların hareketlerinin gerçekleştiği uzayda Kompleks Uzaydan Hilbert Uzayı (Koordinat Sistemi)dır. Kuantum Bilgisayarlarda molekül, atom ve atomaltı parçacıkların davranışları da Kompleks Uzayda olduğundan Komleks Uzayı inceleme bu bağlamda faydalı olacaktır.

# Bölüm 2

# Kompleks Uzay

Bilindiği gibi olaylar bir ortamda meydana gelmektedir. Bir ortamda meydana gelen herhangi bir olayı anlamak için o olayın gerçekleştiği ortamın iyi bilinmesi gerekir. Bu da ortamın belli ölçülerde tanımlanmasına bağlıdır. Genelde ortamlar koordinat sistemi ile ifade edilir. Olaylarda bu koordinat sistemine göre belirlenir. Örneğin reel uzayda bir olay x, y ve z koordinat sisteminde incelenirken atom ve moleküllerin gerçekleştiği uzay olan kompleks uzayda bir olay kompleks koordinat süsteminde incelenir. Binaların temelleri olduğu gibi uzaylarında temelleribulunmaktadır. Uzayların temellerine bazlar denilmektedir. Örneğin, reel uzayda herhangi bir yönlü büyüklük (vektör) uzayın bazları cinsinde aşağıdaki şekilde ifade edilir.

$$\vec{x} = x_1\vec{i} + x_2\vec{j} + x_3\vec{k}$$

Burada $\vec{i}, \vec{j}, \vec{k}$ vektörleri baz vektörleridir.

Benzer şekilde komleks uzayda bir vektör reel kısmına ilave olarak sanal kısmı da içermektedir. Kompleks uzayda bir vektör,

$$z = a + ib$$

şeklinde ifade edilir. Burada $a$ reel kısım, $b$ sanal (imajiner) kısım $i^2 = -1$ olacak şekilde; komleks sayıyı ifade etmektedir.

## 2.1 Kompleks Düzlem ve Kutupsal Gösterimi

Kompleks düzlem oluşturulurken

$$x = \mathrm{Re}\,|z|$$

$$y = \mathrm{Im}\,|z|$$

uzunlukları seçilerek düzlemden bu noktalara karşılık gelen $z$ kompleks sayıyı göstermektedir. Bu da aşağıdaki şekilde ifade edilir.

**Şekil 1**

$$r^2 = |z|^2 = z^2 + y^2 \qquad \tan\theta = \tfrac{y}{x} \qquad \arctan\left(\tfrac{y}{x}\right) = \underbrace{\theta}_{faz}$$

$$\begin{aligned} r &= |z| = \sqrt{x^2+y^2} \\ x &= r\cos\theta \\ y &= r\sin\theta \end{aligned}$$

**Tanım 3. (Faz):** Herhangi birşeyi incelemek onu küçük parçalara ayırarak yapılır. Bu küçük değişimlere faz denir. (İki boyutluda)

$$\begin{aligned} z = \quad x + iy &= r\cos\theta \mp ir\sin\theta \\ &= \underbrace{r(\cos\theta \mp i\sin\theta)}_{\substack{\text{kutupsal karşılığı} \\ \text{faz uzayı karşılığı}}} \end{aligned}$$

$\sin\theta$ ve $\cos\theta$ nın Taylor Açılımı yapılırsa

$$\begin{aligned} f(\theta) &= \sin\theta \\ \sin\theta &= \theta - \tfrac{\theta^3}{3!} + \tfrac{\theta^5}{5!} - \tfrac{\theta^7}{7!} + \cdots \\ f(\theta) &= \cos\theta \\ \cos\theta &= 1 - \tfrac{\theta^2}{2!} + \tfrac{\theta^4}{4!} - \tfrac{\theta^6}{6!} + \cdots \end{aligned}$$

şeklinde olacaktır. Bu ifadeler $z = x \mp iy = r(\cos\theta \mp i\sin\theta)$ da yerine yazılırsa ve $i^2 = -1$, $i^3 = -i$, $i^4 = 1$ kompleks sayıları da kullanılırsa

$$z \quad = x \mp iy \quad = r(\cos\theta \mp i\sin\theta) = \underbrace{r(1 + i\theta + \frac{i\theta^2}{2!} + \frac{i\theta^3}{3!} + \frac{i\theta^4}{4!} + \cdots)}_{\substack{e^{i\theta}\text{'nın Taylor Açılımı} \\ \theta=0 \text{ daki Macloren Serisi}}}$$

$z = z \mp iy = re^{i\theta}$

Bu durum kompleks sayılarda kuvvet alma, karakök alma, çarpma ve bölme işlemlerinde büyük kolaylık sağlamaktadır. Bunun sebei ise olaylarım gerçekleştiği faz uzayında olaylara birebir tanık olma anlamındadır.

**Örnek 1.** $\left.\begin{aligned} z_1 &= r_1.e^{i\theta_1} \\ z_2 &= r_2.e^{i\theta_2} \end{aligned}\right\}$ **a)** $z_1.z_2 = ?$ **b)** $\frac{z_1}{z_2} = ?$

**a)**
$$\begin{aligned} z_1.z_2 = r_1.e^{i\theta_1}.r_2.e^{i\theta_2} &= r_1.r_2.e^{i(\theta_1+\theta_2)} \\ &= r_1.r_2(\cos(\theta_1+\theta_2) + i\sin(\theta_1+\theta_2)) \end{aligned}$$

**b)** $\frac{z_1}{z_2} = \frac{r_1.e^{i\theta_1}}{r_2.e^{i\theta_2}} = \frac{r_1}{r_2}.e^{i(\theta_1-\theta_2)} = \frac{r_1}{r_2}\cos(\theta_1-\theta_2) + i\sin(\theta_1-\theta_2))$

**Not 5. (De Moivre Kuralı):** De Moivre bilim insanı $\mathbb{C}$ kutupsal gösterimi (faz uzaylarının gösterimlerinin) $\mathbb{C}$'nin kuvvetlerini almada çok önemli kolaylık sağladığını bulmuştur.

**Örnek 2.** $z = r.e^{i\theta} \Rightarrow z^n = r^n.e^{niQ}$

Burada $nQ$ değeri $(-\pi, \pi)$ aralğının dışına çıkıyorsa bu durumda $2n$ değeri kadar taşıma atılır. Buaradan yararlanılarak $z^{\frac{1}{n}}$ ifadesini elde etmek için $k \in \mathbb{Z}$ k tane $2\pi$ ifadesi eklenir ve bu durumda $\mathbb{C}$

$$\begin{aligned} z = &\ r(\cos(\theta + 2k\pi)) + i\sin(\theta + 2k\pi) \\ = &\ re^{\theta+2k\pi}, k \in (0, 1, 2, \cdots) \end{aligned}$$

Buna göre $z^{\frac{1}{n}} = \sqrt{r}(\cos\left(\frac{\theta+2k\pi}{n}\right) + i\sin\left(\frac{\theta+2k\pi}{n}\right))$

## 2.2 Kompleks Sayılarda Dört İşlem

### Toplama İşlemi:

İki kompleks sayının toplamı reel ve sanal kısımlarn ayrı ayrı toplamından elde edilir.

**Örnek 3.** $\left.\begin{array}{l} z_1 = x_1 + iy_1 \\ z_2 = x_2 + iy_2 \end{array}\right\}\ z_1 + z_2 = \ (x_1 + x_2) + i(y_1 + y_2)$

### Çıkarma İşlemi:

İki kompleks sayıda çıkarma işlemi reel ve sanal kısımları birbirinden ayrı ayrı çıkarılmasıyla elde edilir.

**Örnek 4.** $\left.\begin{array}{l} z_1 = x_1 + iy_1 \\ z_2 = x_2 + iy_2 \end{array}\right\}\ z_1 - z_2 = \ (x_1 - x_2) + i(y_1 - y_2)$

### Çarpma İşlemi:

İki kompleks sayıda çıkarma işlemi reel ve sanal kısımları birbirinden ayrı ayrı çıkarılmasıyla elde edilir.

**Örnek 5.** $\left.\begin{array}{l} z_1 = x_1 + iy_1 \\ z_2 = x_2 + iy_2 \end{array}\right\}$

$$\begin{aligned} z_1.z_2 &= (x_1 + iy_1) + (x_2 + iy_2) \\ &= x_1x_2 + ix_1y_2 + ix_2y_1 + i^2y_1y_2 \\ &= \underbrace{x_1x_2 - y_1y_2}_{\mathrm{Re}\{z_1.z_2\}} + i\underbrace{(x_1y_2 + x_2y_1)}_{\mathrm{Im}\{z_1.z_2\}} \end{aligned}$$

### Bölme İşlemi:

?????????

## 2.3 Kompleks Sayıların Büyüküğü (Uzunluğu=Normu)

$z = x + iy$ şeklindeki bir sayının uzunluğu

$$|z| = x^2 + y^2$$

şeklindedir.

## 2.4 Kompleks Sayıların Eşleniği

$$z = x + iy \Rightarrow \bar{z} = x - iy = z^*$$
$$|z|^2 = z.\bar{z} = (x + iy)(x - iy) = x^2 + y^2$$

Kompleks sayının neden bir eşleniği vardır? Proton, nötron gibi doğadaki parçacıkların eşleniği vardır ve bu parçacıklar birbirini yok edip pozitif enerji verir. Hiçbir şey yoktan var edilemez. Bu da enerji korunumunu verir.

**Not 6.** Eşlenikliğin varlığı aslında doğada da mevcuttur. Örneğin parçacıklara eşlik eden diğer parçacıkların varlığı.

**Örnek 6.** $z = 1 + i$ nin kutupsal gösterimini bulunuz.

$r^2 = 1^2 + 1^2 = 2 \Rightarrow r = \sqrt{2}$

$$\left.\begin{array}{ll} x = r\cos\theta & \Rightarrow \cos\theta = \frac{1}{\sqrt{2}} \\ x = r\sin\theta & \Rightarrow \sin\theta = \frac{1}{\sqrt{2}} \end{array}\right\} \begin{array}{ll} \tan\theta = 1 & \Rightarrow \theta = \frac{\pi}{4} + 2k\pi \\ k = 0 \text{ için} & \theta = \frac{\pi}{4} \end{array}$$

$$z = r(\cos\theta + i\sin\theta) = \sqrt{2}(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}) = \sqrt{2}(\cos\frac{1}{\sqrt{2}} + i\sin\frac{1}{\sqrt{2}})$$

**Örnek 7.** $\left.\begin{array}{l} z_1 = 2 - 3i \\ z_2 = -5 + i \end{array}\right\}$ **a)** $z_1 + z_2 = ?$ **b)** $z_1 - z_2 = ?$ **c)** $z_1.z_2 = ?$ **d)** $\frac{z_1}{z_2} = ?$

**a)** $z_1 + z_2 = 2 - 3i - 5 + i = 2 - 5 - 3i + i = -3 - 2i$

**b)** $z_1 - z_2 = 2 - 3i - (-5 + i) = 2 + 5 - 3i - i = 7 - 4i$

**c)** $z_1.z_2 = (2 - 3i)(-5 + i) = -10 + 2i + 15i - 3i^2 = -10 + 3 + 17i = -7 + 17i$

**d)** $\frac{z_1}{z_2} = \frac{2-3i}{-5+i} = \frac{(2-3i)(-5+i)}{25+1} = \frac{-10-2i+15i+3i^2}{26} = \frac{-13+13i}{26} = \frac{13(-1+i)}{26} = \frac{-1+i}{2}$

**Örnek 8.** $z^8 = 1$ denklemini çözünüz.

$$1 = 1 \cdot (\cos 2k\pi + i\sin 2k\pi) = 1 \cdot e^{i2k\pi}$$
$$z^8 = 1e^{i2k\pi} \Rightarrow (z^8)^{\frac{1}{8}} = e^{\frac{i2k\pi}{8}}$$
$$z = e^{\frac{ik\pi}{4}}$$

$k = 0$ için $z = 1 \cdot (\cos 0 + i\sin 0) = 1$
$k = 1$ için $z = 1 \cdot (\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}) = \frac{1+i}{\sqrt{2}}$
$k = 2$ için $z = 1 \cdot (\cos\frac{\pi}{2} + i\sin\frac{\pi}{2}) = i$
$k = 3$ için $z = 1 \cdot (\cos\frac{3\pi}{4} + i\sin\frac{3\pi}{4}) = \frac{-1+i}{\sqrt{2}}$
$k = 4$ için $z = 1 \cdot (\cos\pi + i\sin\pi = -1$
$k = 5$ için $z = 1 \cdot (\cos\frac{5\pi}{4} + i\sin\frac{5\pi}{4}) = \frac{-1-i}{\sqrt{2}}$
$k = 6$ için $z = 1 \cdot (\cos\frac{6\pi}{4} + i\sin\frac{6\pi}{4}) = -i$
$k = 7$ için $z = 1 \cdot (\cos\frac{7\pi}{4} + i\sin\frac{7\pi}{4}) = \frac{1-i}{\sqrt{2}}$
$k = 8$ için $z = 1 \cdot (\cos 2\pi + i\sin 2\pi) = 1$ tekrar ettiği için buraya kadar.

## 2.5 Bazı Kompleks Fonksiyonlar

### Kompleks Polinomlar

$z$ kompleks sayı olmak üzere ve $f(z) = c_0 + c_1 z + c_2 z^2 + \cdots c_n z^n$ şeklinde tanımlı ise kompleks polinom

$$f(z) = \frac{P(z)}{Q(z)}, Q(z) \neq 0$$

şeklinde tanımlanır.

### Üstel Kompleks Fonksiyonlar

$$f(z) = e^z = x^{x+iy} = e^x e^{iy} = e^x(\cos y + i \sin y)$$

### Trigonometrik Fonksiyonlar

$$e^{ix} = \cos x + i \sin x$$

$$e^{-ix} = \cos x - i \sin x$$

Bu ifadelerden $\cos x$ ve $\sin x$ çekilirse

$$\cos x = \frac{e^{ix} + e^{-ix}}{2}$$

$$\sin x = \frac{e^{ix} - e^{-ix}}{2i}$$

Benzer şekilde

$$\cos z = \frac{e^{iz} + e^{-iz}}{2}$$

$$\sin z = \frac{e^{iz} - e^{-iz}}{2i}$$

??????????????????

### Logaritmik Fonksiyonlar

$$z = re^{i\theta}$$

$$\theta = \arctan \frac{y}{x}$$

$$\log_e z = \ln r + i\theta$$

# Bölüm 3

# Operatörler (İşlemciler)

Önüne gelen vektör, fonksiyon veya herhangi bir duruma kendi bulunduğu uzayın özellikleri doğrultusunda etki eden tek başlarına anlamları olmayan ancak etki etmeleri sonucu anlam kazanan niceliklere operatör veya işlemci denir.

**Örnek 9.**

- $\frac{d}{dx} \rightarrow$ türev operatörü
- $\int dx \rightarrow$ integral operatörü
- $\nabla = \frac{\partial}{\partial x} + \frac{\partial}{\partial y} + \frac{\partial}{\partial z}$

**Not 7.** Klasik bilgisayarlarda tüm işlemlerde terslenebilirlik yoktur. Fakat kuantum bilgisayarlarda her işlemi terslenebilirliği vardır. Terslenebilirlik çıktıdan girdiyi bilebilmeyi sağlar.

**Not 8.** Klasik bilgisayarlarda olduğu gibi kuantum bilgisayarlarda da tüm işlemler operatörlerle (işlemciler=kapılar) gerçekleştirilmektedir. Kuantum bilgisayarlardaki operatörler kuantum bilgisayarların dayanağı foton, molekül, atom ve atomaltı parçacıklar olduğundan ve bunların davranışları da uzayda olduğundan operatörlerde kompleks uzayda tanımlı operatörlerdir.

## 3.1 Lineer Operatörler (İşlemciler)

Önüne gelen vektör, fonksiyon veya herhangi bir duruma aşağıdaki özelliklere sahip işlemcinin etki etmesi sonucu oluşan niceliklere lineer operatörler denir.

A,B ve C operatörler olmak üzere lineer operatörler aşağıdaki özellikleri sağlarlar.

i. $A = B \Rightarrow A\vec{a} = B\vec{a}$

ii. $(A + B)\vec{a} = A\vec{a} + B\vec{a}$

iii. $(AB)\vec{a} = A(B\vec{a}) = B(A\vec{a})$

iv. $C(A+B) = CA + CB$

v. $A \cdot B \neq B \cdot A$ aradaki fark $[AB] = AB + BA$ kadardır.

## 3.2 Bazı Özel Operatörler

Bilindiği gibi molekül, atom, atom altı parçacıkları davranışlarının meydana geldiği uzaylar kompleks uzaylardır ki bu uzaylardan **dik** olan ve aynı zamanda **biçimsel** özelliğe sahip olan uzayda **Hilbert Uzayıdır**. Molekül, atom ve atom altı parçacıkların davranışları genellikle Hilbert uzayında incelenir. Bu uzayın tercih edilmesinin nedeni dik ve biçimsel olduğu için bu uzayda işlem yapmak daha kolaydır. Bu bağlamda kompleks uzayda tanımlı aşağıdaki bazı operatörler çok önemlidir.

**1) Birim Operatör:** $I$ şeklinde gösterilen bu operatör önüne gelen fonksiyona veya vektörüne etki ettiğinde onu değiştirmeyen operatördür. Yani $I\vec{a} = \vec{a}$ dir.

**2) Ters (Inverse) Operatör:** $A$ operatör olmak üzere $A\vec{a} = \vec{a'}$ işlemini tersine çeviren operatördür ve $A^{-1}$ ile gösterilir. Yani

$$A^{-1}\vec{a'} = \vec{a}$$

Diğer bir değişle

$$A^{-1}(A\vec{a}) = \vec{a} \Rightarrow A^{-1}A = I$$

**Not 9.**

$$(AB)^{-1} = B^{-1}A^{-1}(ABC)^{-1} = C^{-1}B^{-1}A^{-1}$$

**3) Hermitik Operatör ($A^{-1}$):** Eşleniğinin transpozesi kendisine eşit olan operatörlere hermitik operatör denir. Yani

$$A = (A^*)^t \Rightarrow A \text{ hermitiktir.}$$

Bu operatörler çok çok önemli olup birimsel operatörlerin varlığınında bir göstergesidir.

**4) Birimsel (Unitary) Operatör:** Eşleniğin transpozesi kendinin tersine eşit olan veya kendisinin tersi hermitik operatöre eşit olan işlemcilere birimsel operatörler denir. Yani

$$(A^*)^t = A^{-1} = A^t \Rightarrow A \text{ birimsel (unitary) operatördür.}$$

**Not 10.** Birimsel operatörler etki ettiği vektörün veya herhangi bir durumun uzunluğunu değiştirmezmler. Bu özellik sayesinde biçimsel operatörler terslenebilir işlem yapma olanağı sağlarlar.

**Not 11.** Kuantum bilgisayarlarda ölçme dışında kullanılan operatörlerin (işlemcilerin) hemen hemen hepsi birimsel operatörlerdir ki burda kuantum bilgisayarların diğer bilgisayarlardan üstün olan terslenebilir işlemler yapabilme özelliğinin temel sebeplerinden biridir.

Terslenebilme özelliği biçimsel operatörlerden geliyor.

## 3.3 Lineer Operatörlerin Gösterimi

$A$ lineer operatörü $u_j$ baz vektörüne etki edip daha sonra bu etkinin sonucu ile $u_i$ baz vektörünün skaler çarpımını yani $(u_i, Au_j) = A_{ij}$ ile gösterirsek ($i$ satır, $j$ sütun olmak üzere)

$$A_{ij} = \begin{bmatrix} A_{11} & A_{12} & A_{13} & \cdots & A_{1n} \\ A_{21} & A_{22} & A_{23} & \cdots & A_{2n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ A_{m1} & A_{m2} & A_{m3} & \cdots & A_{mn} \end{bmatrix}_{m \times n}$$

şeklinde gösterime matris gösterimi denir.

# Bölüm 4

# Matris ve Matris Cebiri

$$A_{ij} = \begin{bmatrix} A_{11} & A_{12} & A_{13} & \cdots & A_{1n} \\ A_{21} & A_{22} & A_{23} & \cdots & A_{2n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ A_{m1} & A_{m2} & A_{m3} & \cdots & A_{mn} \end{bmatrix}_{m\times n}$$

elemanları ($A_{ij}$) reel, kompleks fonksiyonlar, integral, türev (fonksiyonların değişimi) olabilen ve bulundukları uzayın özelliklerini taşıyan niceliklerin yukarıdaki tablo şeklinde gösterimine matris denir. Bu skalerler, fonksiyonlar, türevler, integraller $u_i$ baz vektörünün $A$ operatörüne $u_j$ baz vektörüne etkisi ile skaler çarpımını ifade eder.

**Not 12.** Bilindiği gibi matrisler aslında tanımlı oldukları uzayın (skalerler, kompleks nicelikler, fonksiyonlar, fonksiyonların değişimi (türev) vb.) özelliklerini taşımaktadır. Uzayın başka bir davranışın veya uzaydaki bilinmeyen hakkında matrisler yardımıyla bilgi edinilir. (örneğin denklem sistemi çözümüyle veya özdeğer problemi yardımıyla)

## 4.1 Matris Cebiri

### Toplama ve Çıkarma

2 matrisin toplanması ve çıkarılması işlemi karşılıklı elemanlar arasında gerçekleştirilir. Yani

$$(A_{ij} \mp B_{ij}) = C_{ij}$$

### Matrislerin Çarpımı

2 matrisin çarpılabilmesi için öncelikle 1. matrisin satır sayısı 2. matrisin sütun sayısına eşit olmalıdır. Bu durumda çarpma işlemi

$$A_{ik} \cdot B_{kj} = C_{ij}$$

şeklinde olur. Diğer bir değişle $A$ matrisinin $i$. satırının her bir elemanı $B$ matrisinin $j$. sütununda karşılık gelen her bir elemanla çarpmlarının toplamı sonuç $i$. satır $j$. sütun olarak elde edilir.

## 4.2 Matrislerle İlgili Bazı Özellikler

**i)** $\alpha$ skaler olmak üzere bir matrisin skalerle çarpımı demek

$$\alpha A_{ij} = (\alpha A)_{ij}$$

yani skalerle matrisin tüm elemanları ile tek tek çarpımıdır.

**ii) Transpoze Matrisi:** Bir matrisin satır ve sütununun yer değiştirmesiyle elde edilen matrise transpoze matris denir.

$$(A_{ij})^T = A_{ji}$$

a) $(A^T)^T = A$

b) $(A + B)^T = A^T + B^T$

c) $(A \cdot B)^T = B^T \cdot A^T$

**iii) Kompleks Eşlenik Matris:** Elemanları Kompleks olan bir $A$ matrisinin tüm elemanlarının eşleniği alınarak elde edilir ve $\bar{A}, A^*$ şeklinde gösterilir.

**iv) Hermitik Eşlenik Matris:** Eşleniğin transpozesi alınarak elde edilen matrise denir ve $A^t$ şeklinde gösterilir.

**v) Hermitik Matris:** Eşleniğin transpozesi alınarak elde edilen matris kendisine eşitse bu matrise hermitik matris denir.

$$(A^*)^T = A^t = A \Rightarrow A \text{ hermitiktir}$$

**vi) Birimsel (Unitary) Matris:** Eşleniğin transpozesi kendinin tersine eşitse bu matrise

birimsel matris denir. Yani

$$(A^*)^T = A^t = A^{-1} \Rightarrow A \text{ birimsel matris}$$

$$A \cdot (A^*)^T = A \cdot A^t = I \Rightarrow A \text{ hermitiktir}$$

**Not 13.** Birimsel Matris olabilmesi için hermitik olmalıdır.

**vii) Simetrik Matris:** Transpozesi kendisine eşit olan matrise simetrik matis denir.

$$(A_{ij})^T = A_{ji} = A_{ij} \Rightarrow A \text{ simetriktir}$$

**viii) Asimetrik Matris:** Transpozesi kendisinin negatif işaretlisine eşitse bu matrise asimetrik matis denir. Yani

$$(A_{ij})^T = A_{ji} = -A_{ij} \Rightarrow A \text{ asimetriktir}$$

**ix) Ortogonal (Dik) Matris:** Transpozesi ile kendisinin çarpımı birim matrisi veriyorsa o matrise ortogonal matis denir. Yani

$$(A_{ij})^T \cdot A_{ij} = I \Rightarrow A \text{ dik}$$

**Örnek 10.** $A = \begin{bmatrix} 1 & 2+3i \\ e^{i\theta} & i \end{bmatrix}$
matrisinin transpozesi ve hermitik eşleniği nedir?

$$A^T = \begin{bmatrix} 1 & e^{i\theta} \\ 2+3i & i \end{bmatrix} \qquad A^* = \begin{bmatrix} 1 & 2-3i \\ e^{-i\theta} & -i \end{bmatrix} \qquad (A^*)^T = A^t = \begin{bmatrix} 1 & e^{-i\theta} \\ 2-3i & i \end{bmatrix}$$

**Örnek 11.** $A = \begin{bmatrix} 1 & 2+3i \\ e^{i\theta} & i \end{bmatrix}$ matrisinin hermitik olup olmadığını gösteriniz.

$$A^* = \begin{bmatrix} 1 & 2-3i \\ e^{-i\theta} & -i \end{bmatrix} \qquad (A^*)^T = \begin{bmatrix} 1 & e^{-i\theta} \\ 2-3i & -i \end{bmatrix}$$

$(A^*)^T = A^t \qquad A^t \stackrel{?}{=} A \qquad \begin{bmatrix} 1 & e^{-i\theta} \\ 2-3i & -i \end{bmatrix} \neq \begin{bmatrix} 1 & 2+3i \\ e^{i\theta} & i \end{bmatrix}$ olduğundan $A$ matrisi hermitik değildir.

**Örnek 12.** $A = \begin{bmatrix} 3 & 2i \\ 2i & 1 \end{bmatrix}$
**a)** $A^T = ?$ **b)** $A^t = ?$
**c)** Hermitik olup olmadığını gösteriniz.
**d)** A nın dik olup olmadığını gösteriniz.

**a)** $A^T = \begin{bmatrix} 3 & 2i \\ 2i & 1 \end{bmatrix}$

**b)** $A^* = \begin{bmatrix} 3 & -2i \\ -2i & 1 \end{bmatrix}$ ve $(A^*)^T = \begin{bmatrix} 3 & -2i \\ -2i & 1 \end{bmatrix} = A^t$

**c)** $A^t \stackrel{?}{=} A$ $\quad \begin{bmatrix} 3 & -2i \\ -2i & 1 \end{bmatrix} \neq \begin{bmatrix} 3 & 2i \\ 2i & 1 \end{bmatrix}$ olduğundan $A$ matrisi hermitik değildir.

**d)** $A^T \cdot A = \begin{bmatrix} 3 & 2i \\ 2i & 1 \end{bmatrix} \cdot \begin{bmatrix} 3 & 2i \\ 2i & 1 \end{bmatrix} = \begin{bmatrix} 5 & 8i \\ 8i & -3 \end{bmatrix} \neq I$ olduğundan $A$ dik matris değildir.

**Örnek 13.** $U = \frac{1}{3}\begin{bmatrix} \frac{1+i}{\sqrt{2}} & 2+2i \\ -2\sqrt{2} & 1 \end{bmatrix}$ matrisinin birimsel matris olup olmadığını gösteriniz.

$U^T = \frac{1}{3}\begin{bmatrix} \frac{1+i}{\sqrt{2}} & -2\sqrt{2} \\ 2+2i & 1 \end{bmatrix}$

$U^* = \frac{1}{3}\begin{bmatrix} \frac{1-i}{\sqrt{2}} & 2-2i \\ -2\sqrt{2} & 1 \end{bmatrix} \qquad (U^*)^T = \frac{1}{3}\begin{bmatrix} \frac{1-i}{\sqrt{2}} & -2\sqrt{2} \\ 2-2i & 1 \end{bmatrix}$

$U \cdot (U^*)^T = \frac{1}{3}\begin{bmatrix} \frac{1+i}{\sqrt{2}} & 2+2i \\ -2\sqrt{2} & 1 \end{bmatrix} \cdot \frac{1}{3}\begin{bmatrix} \frac{1-i}{\sqrt{2}} & -2\sqrt{2} \\ 2-2i & 1 \end{bmatrix} = \frac{1}{9}\begin{bmatrix} 9 & 0 \\ 0 & 9 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$

$A$ birimsel matristir.

**Örnek 14.** $U = \frac{1}{3}\begin{bmatrix} \frac{1+i}{\sqrt{2}} & 2+2i \\ -2\sqrt{2} & 1 \end{bmatrix}$ dik matris olup olmadığını gösteriniz.

$U^T = \frac{1}{3}\begin{bmatrix} \frac{1+i}{\sqrt{2}} & -2\sqrt{2} \\ 2+2i & 1 \end{bmatrix}$

$U^T \cdot U = \frac{1}{3}\begin{bmatrix} \frac{1+i}{\sqrt{2}} & -2\sqrt{2} \\ 2+2i & 1 \end{bmatrix} \cdot \frac{1}{3}\begin{bmatrix} \frac{1+i}{\sqrt{2}} & 2+2i \\ -2\sqrt{2} & 1 \end{bmatrix} = \frac{1}{9}\begin{bmatrix} 2i+8 & \frac{4i}{\sqrt{2}} - 2\sqrt{2} \\ \frac{4i}{\sqrt{2}} - 2\sqrt{2} & 8i+1 \end{bmatrix} \neq I$

olduğundan $U$ dik matris değildir.

**Örnek 15.** $A = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$ dik matris olup olmadığını gösteriniz.

$A^T = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix}$

$A^T \cdot A = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix} \cdot \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$ olduğundan $A$ dik matrisdir.

## 4.3 Determinant, İzi Matrisin Tersi

### Determinant:

Bir matrisin determinantı olabilmesi için öncelikle matrisin kare matris olması gerekir. Bu bağlamda A matrisinin determinant açılımı

$$\det(A) = \sum_{k=1}^{n} (-1)^{k+i} A_{ik} \text{Minör}$$

şeklinde ifade edilir.

$A_{ik}$ A matrisinin $i$. satır $k$. sütun kapatılarak elde edilen $(n-1) \times (n-1)$ tipindeki matrislerdir.

Yukarıdakine göre matris determinantı bulunurken istenilen satır ve sütuna göre açılım sonucu elde edilir.

**Örnek 16.** $A = \begin{bmatrix} 2 & 1 & 5 \\ 4 & 3 & 6 \\ 0 & 2 & 7 \end{bmatrix}$

3. satıra göre

$$\begin{aligned} \det(A) &= 0 \cdot (-1)^{3+1} \cdot \begin{vmatrix} 1 & 5 \\ 3 & 6 \end{vmatrix} + 2 \cdot (-1)^{3+2} \cdot \begin{vmatrix} 2 & 5 \\ 4 & 6 \end{vmatrix} + 7 \cdot (-1)^{3+3} \cdot \begin{vmatrix} 2 & 1 \\ 4 & 3 \end{vmatrix} \\ &= -2 \cdot (12 - 20) + 7 \cdot (6 - 4) \\ &= 16 + 14 \\ &= 30 \end{aligned}$$

### Determinantın Özellikleri

**1)** Determinant hesaplanırken işlem kolaylığı için bol sıfır olan satır veya sütun seçilir.

**2)** Bir matrisin 2 satır veya sütunu yer değiştirilirse determinant işareti değişir.

**3)** 2 satır veya sütunu aynı olan matrislerin determinantı sıfır(0) dır.

**4)** İki matrisin çarpımının determinantı ayrı ayrı determinantları çarpımına eşittir.

**5)** Ortogonal matrislerin determinantı $\mp 1$ dir.

**6)** $3 \times 3$ tipindeki matrisin determinantı Sarus kuralına göre aşağıdaki şekilde bulunur.

**EKSİK**

## İz (Trace):

Bir matrisin köşegen üzerindeki elemanların toplamı o matrisin izini verir ve Tr veya İz ile gösterilir. $n \times n$ kare matrislerin izi

$$\mathrm{Tr}(A) = a_{11} + a_{22} + a_{33} + \cdots + a_{nn} = \sum_{i=1}^{n} a_{ii}$$

## İzin Özellikleri:

**1)** $\mathrm{Tr}(A \cdot B) = \mathrm{Tr}(B \cdot A)$

**2)** $\mathrm{Tr}(A \cdot B \cdot C) = \mathrm{Tr}(C \cdot A \cdot B) = \mathrm{Tr}(B \cdot C \cdot A)$

# Bölüm 5

# Dirac (Bra-Ket=Parantez) Gösterimi

Bilindiği gibi herhangi bir uzayda bir durumu ifade etmek demek o durumun bileşenlerini uzayın bazları cinsinden ifade etmek demektir. Bu bağlamda örneğin $\vec{i}, \vec{j}, \vec{k}$ bazlarına sahip 3 bpyutlu bir uzayda $\vec{x}$ vektörü

$$\vec{x} = x_1\vec{i} + x_2\vec{j} + x_3\vec{k}$$

şeklinde ifade edilir. Burada $x_1$ $\vec{x}$ vektörünün $i$ bazındaki iz düşümü veya buluşma olasılığıdır. Benzer şekilde $x_2$ $\vec{x}$ vektörünün $j$ bazındaki iz düşümü veya buluşma olasılığı. Benzer şekilde $x_3$ $\vec{x}$ vektörünün $k$ bazındaki iz düşümü veya buluşma olasılığı. Benzer şekilde kompleks uzayda herhangi bir durum kompleks uzayın bazları cinsinden ifade edilir. Diğerinden farklı olarak deneylerle de ispatlandığı gibi atom ve moleküller bulundukları yerlerde sabit olmayıp bir titreşim halindedir. Yani molekül ve atomların durumları olasılıksaldır. Bu nedenle kompleks uzayda binary sistem durumu $|x\rangle$ şeklinde gösterilir. Bu durumun duali ise $\langle x|$ şeklinde gösterilir. Burada $\langle x|$, $|x\rangle$' nin eşleniğinin transpozesine eşittir.

$$\langle x| = ((|x\rangle)^*)^T$$

Buradan da anlaşılacağı gibi $|x\rangle$ sütun şeklindeki bileşenleri içerirken $\langle x|$, $|x\rangle$' nin eşleniğinin satır bileşenlerini içerir. Bunların her ikisine birden $\langle x|x\rangle$ denir ve Dirac gösterimi olarak adlandırılır. Buna göre kompleks uzayda $x$ durumu yani $|x\rangle$, $u_1, u_2, u_3$ kompleks uzayı bazları olmak üzere

$$|x\rangle = x_1 |u_1\rangle + x_2 |u_2\rangle + x_3 |u_3\rangle$$

$x_1 |x\rangle$ in $|u_1\rangle$ deki bulunma olasılığı, $x_2 |x\rangle$ in $|u_2\rangle$ deki bulunma olasılığı, $x_3 |x\rangle$ in $|u_3\rangle$ deki bulunma olasılığı.

**Örnek 17.** Neden bilgisayarlarda binary sistem kullanılır?

$$
\begin{aligned}
x_1^2 &= x_1 x_1^* \\
x_2^2 &= x_2 x_2^* \\
x_3^2 &= x_3 x_3^* \\
x_1^2 &\ |x\rangle \text{ in } |u_1\rangle \text{ de bulunma olasılığı sonucu} \\
x_2^2 &\ |x\rangle \text{ in } |u_2\rangle \text{ de bulunma olasılığı sonucu} \\
x_3^2 &\ |x\rangle \text{ in } |u_3\rangle \text{ de bulunma olasılığı sonucu} \\
|x\rangle &= \tfrac{1}{\sqrt{3}} |u_1\rangle + i\sqrt{\tfrac{7}{15}} |u_2\rangle + \tfrac{1}{\sqrt{5}} |u_3\rangle \\
&\ |x\rangle \text{ in } |u_1\rangle \text{ de bulunma olasılığı } \tfrac{1}{3} \\
&\ |x\rangle \text{ in } |u_2\rangle \text{ de bulunma olasılığı } \tfrac{7}{15} \\
&\ |x\rangle \text{ in } |u_3\rangle \text{ de bulunma olasılığı } \tfrac{1}{5}
\end{aligned}
$$

$$x_1^2 + x_2^2 + x_3^2 = 1$$

Yukarıdan da görüldüğü gibi kompleks uzayda bir sistem durumu tam olarak belli değildir. Yani sistemlerin durumunda

$$\Delta x \cdot \Delta p \geq \frac{\hbar}{2} \left( \hbar = \frac{h}{2\pi} = \text{Plank Sabiti} \right)$$

şeklinde belirsizlik vardır. Diğer bir deyişle bir sistemin konum ve hızı aynı anda belirlenemez. Buradaki belirleme $\frac{\hbar}{2}$ belirsizliğindedi ki buna da $\left(\Delta x \cdot \Delta p \geq \frac{\hbar}{2}\right)$ Heisenberg Belirsizlik İlkesi denir.

**Not 14.** Uzaylarda olaylar incelirken uzayların ortonormal (bazların dik ve uzunluklarının 1 olduğu) sistemler göz önüne alınır. Bunun sebebi ortonormal sistemlerde hesap yapmak daha kolay olduğu içindir.

**Örnek 18.** $|u_1\rangle, |u_2\rangle, |u_3\rangle$ bazlarına sahip kompleks uzayda bir sistem durumu

$$|\tau\rangle = \frac{1}{\sqrt{5}} |u_1\rangle - i\sqrt{\frac{7}{15}} |u_2\rangle + \frac{1}{\sqrt{3}} |u_3\rangle$$

ise

**a)** $\langle\tau| = ?$
**b)** $|\tau\rangle$ ' nin $|u_1\rangle$ bazında bulunma olasılığı ?
**c)** $|\tau\rangle$ ' nin $|u_2\rangle$ bazında bulunma olasılığı ?
**d)** $|\tau\rangle$ ' nin $|u_3\rangle$ bazında bulunma olasılığı ?

**a)** $\langle\tau| = ((|\tau\rangle)^*)^T = \frac{1}{\sqrt{5}}((|u_1\rangle)^*)^T + i\sqrt{\frac{7}{15}}((|u_2\rangle)^*)^T + \frac{1}{\sqrt{3}}((|u_3\rangle)^*)^T$
$= \frac{1}{\sqrt{5}}\langle u_1| + i\sqrt{\frac{7}{15}}\langle u_2| + \frac{1}{\sqrt{3}}\langle u_3|$

**b)** $|\tau\rangle$ ' nin $|u_1\rangle$ bazında bulunma olasılığı $\frac{1}{\sqrt{5}}^2 = \frac{1}{5}$

**c)** $|\tau\rangle$ ' nin $|u_2\rangle$ bazında bulunma olasılığı $\left(-i\sqrt{\frac{7}{15}}\right)\left(i\sqrt{\frac{7}{15}}\right) = \frac{7}{15}$

**d)** $|\tau\rangle$ ' nin $|u_3\rangle$ bazında bulunma olasılığı $\frac{1}{\sqrt{3}}^2 = \frac{1}{3}$

## 5.1 Bra-ket Notasyonu ile İlgili Bilgi

**Tanım 4.** (**İç Çarpım:**) Herhangi bir durumun bra-ket'i iç çarpımı olarak adlandırılır. Örneğin $|\psi\rangle$ durumu için iç çarpım $\langle\psi|\psi\rangle$ şeklinde gösterilir. İç çarpım bir sistemin ortonormal (dik ve normlu) durumua getirilmesinde ölçüm sonuçlarının (beklenen değeri) elde edilmesi gibi bir çok işlemde kullanılmaktadır. Eğer bir sistem için

$$\langle\psi|\psi\rangle = 1$$

ise bu sistemlere normlu (uzunluğu 1 olan) sistemler denir. Eğer bir sistemin iç çarpımı 0 ise dik (ortogonal) dir. Yani

$$\langle\psi_1|\psi_2\rangle = 0 \Rightarrow \text{ Dik (Ortogonal) } \Rightarrow |\psi_1\rangle \perp |\psi_2\rangle$$

## 5.2 Ortonormal Sistemin Özellikleri

$|u_1\rangle$, $|u_2\rangle$, $|u_3\rangle$ kompleks uzayın bazları olmak üzere,

**1)** $\langle u_1|u_1\rangle = \langle u_2|u_2\rangle = \langle u_3|u_3\rangle = 1$

**2)** $\langle u_2|u_1\rangle = \langle u_1|u_3\rangle = \langle u_2|u_3\rangle = 1$

**Not 15.** Hilbert Uzayı (Kompleks Uzay) ortonormal uzaydır. Hilbert uzayının bazları birimlidir yani uzunlukları 1'dir aynı zamanda birbirine diktir.

**Örnek 19.** $|\psi\rangle = \frac{1}{\sqrt{5}}|u_1\rangle - i\sqrt{\frac{7}{15}}|u_2\rangle + \frac{1}{\sqrt{3}}|u_3\rangle$ ise $\langle\psi|\psi\rangle = ?$

**Not 16.** Bra-ket alınırken işlemler her bir bileşenin yanında durumların bra-keti oluşturularak yapılır.

$$\begin{aligned}
\langle\psi| = &\ ((|\psi\rangle)^*)^t \\
= &\ = \left(\left(\tfrac{1}{\sqrt{5}}\right)^*\right)^t ((|u_1\rangle)^*)^t + \left(\left(-i\sqrt{\tfrac{7}{15}}\ \right)^*\right)^t ((|u_2\rangle)^*)^t + \left(\left(\tfrac{1}{\sqrt{3}}\right)^*\right)^t ((|u_3\rangle)^*)^t \\
= &\ \tfrac{1}{\sqrt{5}}\langle u_1| + i\sqrt{\tfrac{7}{15}}\langle u_2| + \tfrac{1}{\sqrt{3}}\langle u_3|
\end{aligned}$$

$$\begin{aligned}
\langle\psi|\psi\rangle = &\ \underbrace{\left[\frac{1}{\sqrt{5}}\langle u_1| + i\sqrt{\frac{7}{15}}\langle u_2| + \frac{1}{\sqrt{3}}\langle u_3|\right]}_{\langle\psi|}\underbrace{\left[\frac{1}{\sqrt{5}}|u_1\rangle - i\sqrt{\frac{7}{15}}|u_2\rangle + \frac{1}{\sqrt{3}}|u_3\rangle\right]}_{|\psi\rangle} \\
= &\ \tfrac{1}{5}\langle u_1|u_1\rangle + \tfrac{1}{\sqrt{5}}\left(-i\sqrt{\tfrac{7}{15}}\right)\langle u_1|u_2\rangle + \tfrac{1}{\sqrt{5}}\tfrac{1}{\sqrt{3}}\langle u_1|u_3\rangle + i\sqrt{\tfrac{7}{15}}\tfrac{1}{\sqrt{5}}\langle u_2|u_1\rangle + \tfrac{7}{15}\langle u_2|u_2\rangle \\
+ &\ \left(i\sqrt{\tfrac{7}{15}}\right)\tfrac{1}{\sqrt{3}}\langle u_2|u_3\rangle + \tfrac{1}{\sqrt{3}}\tfrac{1}{\sqrt{5}}\langle u_3|u_1\rangle + \tfrac{1}{\sqrt{3}}\left(-i\sqrt{\tfrac{7}{15}}\right)\langle u_3|u_2\rangle + \tfrac{1}{\sqrt{3}}\tfrac{1}{\sqrt{3}}\langle u_3|u_3\rangle \\
= &\ \tfrac{1}{5} + \tfrac{7}{15} + \tfrac{1}{3} = 1 \Rightarrow \text{ Dik ve normlu ortonormal olduğu için}
\end{aligned}$$

**Not 17.** Sonuçtan da görüldüğü gibi $|\psi\rangle$'nin olma olasılığı 1'dir. Olma olasılığı denildiğinde ket pisi ($|\psi\rangle$) ise bra-ketini alıp bakacağız.

**Örnek 20.** $|\psi\rangle = \alpha|u_1\rangle + \beta|u_2\rangle + \gamma|u_3\rangle$ ve $|u_1\rangle$, $|u_2\rangle$, $|u_3\rangle$ sistemi de ortonormal olduğuna göre $\langle\psi|\psi\rangle = ?$

$$\begin{aligned}
\langle\psi| = &\ (\alpha^*)^t((|u_1\rangle)^*)^t + (\beta^*)^t((|u_2\rangle)^*)^t + (\gamma^*)^t((|u_3\rangle)^*)^t \\
= &\ \alpha^*\langle u_1| + \beta^*\langle u_2| + \gamma^*\langle u_3| \\
\langle\psi|\psi\rangle = &\ [\alpha^*\langle u_1| + \beta^*\langle u_2| + \gamma^*\langle u_3|]\,[\alpha|u_1\rangle + \beta|u_2\rangle + \gamma|u_3\rangle] \\
= &\ \alpha^*\alpha\langle u_1|u_1\rangle + \beta^*\beta\langle u_2|u_2\rangle + \gamma^*\gamma\langle u_3|u_3\rangle \\
= &\ \alpha^2 + \beta^2 + \gamma^2 \\
= &\ 1
\end{aligned}$$

**Tanım 5.** (**İç Çarpım:**) Dış çarpım tek başına anlamı olmayan fakat önüne gelen fonksiyon ya da duruma etki ettiğinde anlam kazanan bir niceliktir yani dış çarpım bir operatördür. Bu bağlamda dış çarpımı herhangi bir durumun keti ile başka bir durumun bra'sı dış çarpım olarak adlandırılır. Örneğin $|\psi\rangle$ ile $|\phi\rangle$ durumlarının dış çarpımı $|\psi\rangle\langle\phi|$ şeklindedir. Öerneğin yukarıdaki dış çarpım $|\psi\rangle$ durumuna ve ya $|\phi\rangle$ durumuna etki ederse o zaman anlam kazanır.

**Örnek 21.** $|\psi\rangle\langle\phi|$ dış çarpım operatörünün

**a)** $|\psi\rangle$ ye etkisini

**b)** $|\phi\rangle$ ye etkisini bulunuz.

**a)** $(|\psi\rangle\langle\phi|)|\psi\rangle = |\psi\rangle \underbrace{(\langle\phi|\psi\rangle)}_{\substack{\text{kompleks}\\ \text{veya}\\ \text{reel nicelik}}}$

**b)** $(|\psi\rangle\langle\phi|)|\phi\rangle = |\psi\rangle \underbrace{(\langle\phi|\phi\rangle)}_{=1}$

herbiriyle ayrı ayrı işlem yapılır ve bra-ket oluşturularak yapılır. Yoğunluk matrisi hesaplanırken dış çarpım kullanılır.

## 5.3 Beklenen Durum (Beklenen Değer)

Bilindiği gibi kuantum mekaniğinde enerji, momentum ve bunun gibi nicelikler gözlenebilen ya da ölçülebilen niceliklerdir. Bir sistemin durumunu anlamak demek sisteme ait ölçülebilen nicelikleri ölçmek demektir. Kuantum mekaniğinde ölçme sonucu ölçüm yapmadan belirlenebilmektedir. Bunar göre ölçüm yapılacak niceliğe karşılık bir operatör karşılık getirilir. Bu operatörün beklenen değeri ki bu da kuantum durumlarındaki tüm değerlerin ortalamasına karşılık gelir ve bu sonuç ölçüm sonucudur. Örneğin $|\psi\rangle$ durumuna karşılık gelen operatör $A$ operatörü olsun. Burada $A$ operatörü enerji, momentum vb. gibi nicelikler olabilir. Bu $A$ operatörünün ölçüm sonucu bu $A$ operatörünün beklenen değerine eşittir. Yani

$$\underbrace{\langle A\rangle}_{\substack{\text{A' nın beklenen}\\ \text{değeri}\\ =\\ \text{ölçüm sonucu}}} = \langle\psi|A|\psi\rangle$$

**Örnek 22.** $|\psi\rangle = \frac{1}{\sqrt{3}}|0\rangle + \sqrt{\frac{2}{3}}|1\rangle$ şeklindeki bir qubitlik bilginin kuantum bilgisayarlarda temel kapılardan biri olan

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

NOT kapısındaki sonucunun ne olduğunu (beklenen değerini) bulunuz.

$$\begin{aligned}
\langle X\rangle &= \langle\psi|X|\psi\rangle \\
X|\psi\rangle &= \tfrac{1}{\sqrt{3}}X|0\rangle + \sqrt{\tfrac{2}{3}}X|1\rangle \\
&= \tfrac{1}{\sqrt{3}}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \sqrt{\tfrac{2}{3}}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} \\
&= \tfrac{1}{\sqrt{3}}\begin{pmatrix} 0 \\ 1 \end{pmatrix} + \sqrt{\tfrac{2}{3}}\begin{pmatrix} 1 \\ 0 \end{pmatrix} \\
&= \tfrac{1}{\sqrt{3}}|1\rangle + \sqrt{\tfrac{2}{3}}|0\rangle
\end{aligned}$$

$$\begin{aligned}
\langle\psi| &= ((|\psi\rangle)^*) + t \\
&= \tfrac{1}{\sqrt{3}}\langle 0| + \sqrt{\tfrac{2}{3}}\langle 1| \\
\langle\psi|X|\psi\rangle &= \left[\tfrac{1}{\sqrt{3}}\langle 0| + \sqrt{\tfrac{2}{3}}\langle 1|\right]\left[\tfrac{1}{\sqrt{3}}|0\rangle + \sqrt{\tfrac{2}{3}}|1\rangle\right] \\
&= \tfrac{1}{3}\langle 0|1\rangle + \tfrac{\sqrt{2}}{3}\langle 0|0\rangle\,\tfrac{\sqrt{2}}{3}\langle 1|1\rangle\,\tfrac{2}{3}\langle 1|0\rangle \\
&= \tfrac{\sqrt{2}}{3} + \tfrac{\sqrt{2}}{3} = \tfrac{2\sqrt{2}}{3}
\end{aligned}$$

## 5.4 Öz Değer Problemi

Sistemlerin öz durumlarının tespit edilmesine öz değer problemi denir ve klasik olarak

$$A\vec{x} = \lambda\vec{x} \Rightarrow (A - \lambda I)\vec{x} = 0 \rightarrow \text{klasik öz değer problemi}$$

ve kuantumsal olarak

$$A|x\rangle = \lambda|x\rangle \Rightarrow (A - \lambda I)|x\rangle = 0 \rightarrow \text{kuantum öz değer problemi}$$

Burada $A$ operatör $\lambda_i$'ler öz değerler (sistemin), her bir $\lambda_i$'ye karşılık gelen $|x_i\rangle$'ler ise öz durumlardır. Bu öz durumlar belli sayıda olabileceği gibi sonsuz sayıda da olabilir.

**Örnek 23.** $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ şeklinde tanımlı bir operatörü göz önüne alarak bir sistemin öz değerleri ve öz durumlarını bulunuz.

$$\begin{aligned}
A|x\rangle &= \lambda|x\rangle \Rightarrow (A - \lambda I)|x\rangle = 0 \quad |x\rangle \neq 0 \text{ olduğu için} \\
A - \lambda I &= 0 \\
\begin{pmatrix} a & b \\ c & d \end{pmatrix} - \lambda\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} - \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} = \begin{pmatrix} a-\lambda & b \\ c & d-\lambda \end{pmatrix}
\end{aligned}$$

$(a-\lambda)(d-\lambda) - bc = 0$ denklemi 2. dereceden bir denklem olduğu için $\lambda_1$ ve $\lambda_2$ diye iki kökü vardır. $\lambda_1$ ve $\lambda_2$ bulunur.

$\lambda_1$ değeri $(A - \lambda I)|x\rangle = 0$ denkleminde yerine yazılırsa $|x_1\rangle$ öz vektörü bulunur. Benzer şekilde $\lambda_2$ değeri yerine yazılırsa $(A - \lambda_2 I)|x_2\rangle = 0$ $|x_2\rangle$ öz vektörü bulunur. Böylece bir sistemin herhangi bir uzayda tanımlı olan operatöre karşılık gelen özdeğer ve öz vektörleri (öz durumları) tespit edilmiş olunur.

**Örnek 24.** $A = \begin{bmatrix} 1 & 0 & 4 \\ 0 & 1 & 2i \\ 4 & -2i & 0 \end{bmatrix}$ şeklindeki operatörün (enerji, momentum, sistemin karakteri vb.) öz değer denklemini kurup, öz değer ve öz vektörlerini (öz durumlarını) bulunuz.

$A|x\rangle = \lambda_i |x\rangle \Rightarrow (A - \lambda_i I)|x\rangle = 0$ ve $|x\rangle \neq 0$ olduğundan

$A - \lambda_i I = 0$

$$\begin{bmatrix} 1 & 0 & 4 \\ 0 & 1 & 2i \\ 4 & -2i & 0 \end{bmatrix} - \lambda_i \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = 0 \Rightarrow \begin{bmatrix} 1 & 0 & 4 \\ 0 & 1 & 2i \\ 4 & -2i & 0 \end{bmatrix} - \begin{bmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix} = 0$$

$$\Rightarrow \begin{bmatrix} 1-\lambda_1 & 0 & 4 \\ 0 & 1-\lambda_2 & 2i \\ 4 & -2i & -\lambda_3 \end{bmatrix} = 0$$

$(1-\lambda)[(1-\lambda)(-\lambda)+4] + 4[4(1-\lambda)] = 0$

$(1-\lambda)((\lambda^2 - \lambda + 4) + 16(1-\lambda) = (1-\lambda)((\lambda^2 - \lambda + 20) = 0$

$(1-\lambda)(\lambda-5)(\lambda+4) = 0 \rightarrow$ öz değer denklemi

$\lambda_1 = 1, \quad \lambda_2 = 5, \quad \lambda_3 = -4 \rightarrow$ öz değerler

$(A - 1I)|x_1\rangle = 0$

$$\Rightarrow \begin{bmatrix} 1-1 & 0 & 4 \\ 0 & 1-1 & 2i \\ 4 & -2i & 0-1 \end{bmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = 0$$

$$\Rightarrow \begin{bmatrix} 0 & 0 & 4 \\ 0 & 0 & 2i \\ 4 & -2i & -1 \end{bmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = 0 \Rightarrow \begin{bmatrix} 4z \\ 2iz \\ 4x - 2iy - z \end{bmatrix} = 0 \Rightarrow \begin{matrix} z=0 \\ 4x=2iy \\ 2=iy \quad x=1 \quad y=-2i \end{matrix}$$

$$|x_1\rangle = \begin{pmatrix} 1 \\ -2i \\ 0 \end{pmatrix} \quad ||x_1\rangle| = \sqrt{5}$$

$$(A-5I)\left|x_2\right\rangle = 0$$

$$\Rightarrow \begin{bmatrix} 1-5 & 0 & 4 \\ 0 & 1-5 & 2i \\ 4 & -2i & 0-5 \end{bmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = 0$$

$$\Rightarrow \begin{bmatrix} -4 & 0 & 4 \\ 0 & -4 & 2i \\ 4 & -2i & -5 \end{bmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = 0 \Rightarrow \begin{bmatrix} -4x+4z \\ -4y+2iz \\ 4x-2iy-5z \end{bmatrix} = 0 \Rightarrow \begin{array}{c} 4x=4z \Rightarrow x=z \\ 4y=2iz \Rightarrow 2y=iz \\ -z-2iy=0 \Rightarrow z=-2iy \end{array}$$

$$y=i \text{ olsa } z=2 \Rightarrow \left|x_2\right\rangle = \begin{pmatrix} 2 \\ i \\ 2 \end{pmatrix} \Rightarrow \left|\left|x_2\right\rangle\right| = \left\langle x_2 | x_2 \right\rangle$$

$$\left\langle x_2\right| = \left(\left(\left|x_2\right\rangle\right)^*\right)^t = \begin{pmatrix} 2 \\ -i \\ 2 \end{pmatrix}^t = \begin{pmatrix} 2 & -i & 2 \end{pmatrix}$$

$$\left\langle x_2 | x_2 \right\rangle = \begin{pmatrix} 2 & -i & 2 \end{pmatrix} \begin{pmatrix} 2 \\ i \\ 2 \end{pmatrix} = 4+1+4 = 9 \Rightarrow \left|\left|x_2\right\rangle\right| = \sqrt{9} = 3$$

$$(A-\lambda_3 I)\left|x_3\right\rangle = 0$$

$$\Rightarrow \begin{bmatrix} 1+4 & 0 & 4 \\ 0 & 1+4 & 2i \\ 4 & -2i & 0+4 \end{bmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = 0$$

$$\Rightarrow \begin{bmatrix} 5 & 0 & 4 \\ 0 & 5 & 2i \\ 4 & -2i & 4 \end{bmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = 0 \Rightarrow \begin{bmatrix} 5x-4z \\ 5y+2iz \\ 4x-2iy+4z \end{bmatrix} = 0 \Rightarrow \begin{array}{c} 5x+4z=0 \Rightarrow z=5k \quad x=-4k \\ 5y+2iz=0 \Rightarrow 5y+10ki=0 \Rightarrow y=-2ki \\ 4x-2iy+4z=0 \Rightarrow k=1 \text{ için} \end{array}$$

$$\left\langle x_2 | x_2 \right\rangle = \begin{pmatrix} -4 & -2i & 5 \end{pmatrix} \Rightarrow \left|\left|x_3\right\rangle\right| = \sqrt{\left\langle x_3 | x_3 \right\rangle} = \sqrt{45} = 3\sqrt{5}$$

$$\left\langle x_3\right| = \left(\left(\left|x_3\right\rangle\right)^*\right)^t = \begin{pmatrix} -4 \\ 2i \\ 5 \end{pmatrix}^t = \begin{pmatrix} 2 & -i & 2 \end{pmatrix}$$

$$\left\langle x_3 | x_3 \right\rangle = \begin{pmatrix} -4 & 2i & 5 \end{pmatrix} \begin{pmatrix} -4 \\ -2i \\ 5 \end{pmatrix} = 16+4+25 = 45 \Rightarrow \left|\left|x_2\right\rangle\right| = \sqrt{9} = 3$$

$$\left|x\right\rangle_{\substack{\text{normlu} \\ \text{öz vektör}}} = \begin{bmatrix} \left|x_1\right\rangle & \left|x_2\right\rangle & \left|x_3\right\rangle \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{5}} & \frac{2}{3} & \frac{-4}{3\sqrt{5}} \\ \frac{-2i}{\sqrt{5}} & \frac{i}{3} & \frac{-2i}{3\sqrt{5}} \\ 0 & \frac{2}{3} & \frac{5}{3\sqrt{5}} \end{bmatrix}$$

$\left|x_i\right\rangle_{\text{normlu}} = \frac{\left|x_i\right\rangle}{\left|\left|x_i\right\rangle\right|}$ ile bulunur.

**Ödev:** Bilindiği gibi birimsel dönüşümlerin veya birimsel operatörlerin öz değerleri reeldir. Bu bağlamda

**a)** $A$ matrisinin hermitik olup olmadığını araştırınız.

**b)** Normlu $|x\rangle$ öz durumlarının birimsel olup olmadığını araştırınız.

**Not 18.** Herhangi bir sistemi anlamak için onun karakteristiğini bilmek gerekir. Çünkü her bir sütun kendine öz karakteristiğe göre davranır. Bu bağlamda bir sistemin karakteristiği öz değer problemiyle belirlenir.

## 5.5 Tensörler

Bilindiği gibi vektörler bir uzaydan başka bir uzaya taşındığında bileşenleri değişmektedir. Yani koordinat dönüşümleri altında bileşenleri değişmektedir. Bu nedenle bilim insanları evrendeki temel kanunların uzayın her yerinde geçerli olabilmesi için bir uzaydan başka bir uzaya geçildiğinde, bileşenleri değişmeyen niceliklere ihtiyaç duyarlar ki bunlar da tensörlerdir.

**Tanım 6. Tensörler:** Bir uzaydan başka bir uzaya geçildiğinde bileşenleri değişmeyen niceliklerdir. 0. dereceden bir tensör skaler ($T^0$), birinci dereceden bir tensör vektörü ($T^a$) ifade ederken ikinci ($T^{ab}$), üçüncü ($T^{abc}$), dördüncü ($T^{abcd}$) ve daha üst dereceden tensörler mevcuttur.

**Not 19.** Kompleks uzayda daha üst boyutlarda uzay elde etmek için tensörel çarpımdan yararlanılır. Örneğin $N_1$ boyutlu $H_1$ kompleks uzayı ile $N_2$ boyutlu $H_2$ kompleks uzayının oluşturduğu yeni uzay $H^{\otimes 2} = H_1 \otimes H_2$ şeklinde gösterilir. Yeni uzayın boyutu ise $N_1 \cdot N_2$'dir.

Benzer şekilde kuantum bilgisayarlarda birden qubit durumları tensörel çarpım ile elde edilir.

### Sütun Vektörlerinin Tensörel Çarpımı

$|\phi\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$ ve $|x\rangle = \begin{pmatrix} c \\ d \end{pmatrix}$ den oluşsun. Buna göre bunların tensörel çapımı

$$|\phi\rangle \otimes |x\rangle = \begin{pmatrix} a \\ b \end{pmatrix}_{2\times 1} \otimes \begin{pmatrix} c \\ d \end{pmatrix}_{2\times 1} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix}_{4\times 1}$$

**Not 20.** Yukarıda görüldüğü gibi tensörel çarpım sonucunda oluşan boyut her iki vektörün bulunduğu uzayın boyutlarının çarpımına eşittir.

**Not 21.** Satırların da tensörel çarpımı yukarıdakine benzer şekilde yapılır.

**Örnek 25.** $|a\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$ ve $|b\rangle = \frac{1}{\sqrt{3}}\begin{pmatrix}\sqrt{2}\\1\end{pmatrix}$ $|a\rangle \otimes |b\rangle = ?$

$$|a\rangle \otimes |b\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix} \otimes \frac{1}{\sqrt{3}}\begin{pmatrix}\sqrt{2}\\1\end{pmatrix} = \frac{1}{\sqrt{6}}\begin{pmatrix}\sqrt{2}\\1\\-\sqrt{2}\\-1\end{pmatrix}$$

## Matrislerin Tensörel Çarpımı

Matrislerin tensörel çarpımı da sütun vektörlerinin çarpımına benzemektedir. Bu bağlamda matrislerin tensörel çarpımı her bir eleman diğer matrisin tüm elemanları ile çarpılarak çarpım sonucu bulunduğu satır ve sütun yazılır.

**Örnek 26.** $A = \begin{bmatrix}a_{11} & a_{12}\\a_{21} & a_{22}\end{bmatrix}$ $B = \begin{bmatrix}b_{11} & b_{12}\\b_{21} & b_{22}\end{bmatrix}$

$$A \otimes B = \begin{bmatrix}a_{11} & a_{12}\\a_{21} & a_{22}\end{bmatrix}_{2\times 2} \otimes \begin{bmatrix}b_{11} & b_{12}\\b_{21} & b_{22}\end{bmatrix}_{2\times 2} = \left[\begin{array}{cc|cc} a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{11} & a_{12}b_{12}\\ a_{11}b_{21} & a_{11}b_{22} & a_{12}b_{21} & a_{12}b_{22}\\ \hline a_{21}b_{11} & a_{21}b_{12} & a_{22}b_{11} & a_{22}b_{12}\\ a_{21}b_{21} & a_{21}b_{22} & a_{22}b_{21} & a_{22}b_{22}\end{array}\right]_{4\times 4}$$

**Örnek 27.** Kuantum bilgisayarlarda temel kapılardan olan ve tek qubite etki eden $X = \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}$ ve $Z = \begin{pmatrix}1 & 0\\0 & -1\end{pmatrix}$ kapılarının tensörel çarpımının sonucunu bulun.

$$X \otimes Z = \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix} \otimes \begin{pmatrix}1 & 0\\0 & -1\end{pmatrix} = \left[\begin{array}{cc|cc} 0 & 0 & 1 & 0\\ 0 & 0 & 0 & -1\\ \hline 1 & 0 & 0 & 0\\ 0 & -1 & 0 & 0\end{array}\right]$$

# Bölüm 6

# Kuantum Bilgisayarlarda Bilginin İfade Edilmesi

Klasik bilgisayarlarda bir bilgi bir bit ile ifade edilirken kuantum bilgisayarlarda en küçük bilgi birimi kuantum bit (qubit) ile ifade edilmektedir. Klasik bilgisayarlardaki 0 ve 1 kuantum bilgisayarlarda durum olarak ifade edilir. bu bağlamda 0'ı $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ ve 1'i $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ ile ifade edilir. Burada $|0\rangle$ ve $|1\rangle$ kuantum bilgisayarlarda temel bazlardır. Bu durumlar kuantum bilgisayarların yapılışına göre farklı fiziksel durumları ifade etmektedir. Örneğin spinler kullanılarak kuantum bilgisayarlar yapılmışsa $|0\rangle \uparrow$ (yukarı spin), $|1\rangle \downarrow$ (aşağı spin) ile gösterilmektedir. Bilindiği gibi molekül veya atomların spinleri yukarı ve aşağı spinlerin her ikisini barındırmaktadır. Eğer kuantum bilgisayarların ışığın polarizasyonundan yararlanarak gerçekleştirilmişse

- $|0\rangle$ polarize olmamış durum veya yatay ışığı
- $|1\rangle$ polarize olmuş durum veya dikey ışığı

ifade etmektedir.

Eğer kuantum bilgisayarları enerji uyarılma durumundan yararlanılarak yapılmışsa

- $|0\rangle$ uyarılmamış enerji düzeyi
- $|1\rangle$ uyarılmış enerji düzeyi

ifade etmektedir.

Yukarıdaki durumlardaki (spin, polarize, uyarılmış enerji) her iki durum ($|0\rangle$ ve $|1\rangle$) aynı anda bulunmaktadır. Bu nedenle klasik bilgisayarlar 0 ve 1'den bir tanesini değerlendirirken kuantum bilgisayarlar 0 ve 1'in ve 0 ve 1'in olası tüm durumlarını aynı anda değerlendirmektedir.

**Not 22.** Farklı iki durumun aynı anda olmasına süperpozisyon durumu denir

Kuantum bilgisayarlardaki süperpozisyonluk durumu yani farklı iki durumun aynı aynda değerlendirilmesi kuantum bilgisayarların klasik bilgisayarlara göre üstün işlem yapabilme kapasitesini ortaya koymaktadır. Örneğin 24 bitlik klasik bilgisayar ile 3 qubitlik kuantum bilgisayarını karşılaştıracak olursak 24 bitlik klasik bilgisayar 3 tane bytedan oluşan adres saklanabilirken kuantum bilgisayarda bu bilgi için 3 qubitlik durum yeterlidir. buna ilave olarak kuantum bilgisayarlar 0 ve 1'in olası tüm durumlarını da aynı anda değerlendirmektedir.

Kuantum bilgisayarlarda bir qubit kuantum bilgisayarların $|0\rangle$ ve $|1\rangle$ temel bazları cinsinden

$$|x\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \rightarrow 1 \text{ qubitlik bilgi}$$

şeklinde ifade edilir. Burada

$$\begin{aligned}
&\alpha : |x\rangle \text{'in } |0\rangle \text{ bazındaki izdüşümü}\\
&\beta : |x\rangle \text{'in } |1\rangle \text{ bazındaki izdüşümü}\\
&\alpha^2 = \alpha\alpha^*\\
&\beta^2 = \beta\beta^*\\
&\alpha^2 + \beta^2 = 1 \text{ Tüm olasılık 1 dir}
\end{aligned}$$

**Not 23.** Kuantum bilgisayarlarda birden fazla qubit durumu bunların tensörel çarpımı ile elde edilir. Örneğin;

$$|x_1\rangle = \alpha_1\,|0\rangle + \beta_1\,|1\rangle$$

$$|x_2\rangle = \alpha_2\,|0\rangle + \beta_2\,|1\rangle$$

şeklindeki 2 qubitlik bir bilgi bunların tensörel çarpımı sonucu aşağıdaki şekilde elde edilir.

$$\begin{aligned}
\underbrace{|x_1\rangle \otimes |x_2\rangle}_{|x\rangle^{\otimes 2}} &= (\alpha_1\,|0\rangle + \beta_1\,|1\rangle) \otimes (\alpha_2\,|0\rangle + \beta_2\,|1\rangle)\\
\text{(2 qubitlik bir gösterim)} &= \alpha_1\alpha_2\,|0\rangle \otimes |0\rangle + \alpha_1\beta_2\,|0\rangle \otimes |1\rangle + \beta_1\alpha_2\,|1\rangle \otimes |0\rangle + \beta_1\beta_2\,|1\rangle \otimes |1\rangle\\
&= \alpha_1\alpha_2\,|00\rangle + \alpha_1\beta_2\,|01\rangle + \beta_1\alpha_2\,|10\rangle + \beta_1\beta_2\,|11\rangle
\end{aligned}$$

Buna göre $n$-qubitlik bilgi

$$|x\rangle^{\otimes n} = \alpha_1\,|00\ldots00\rangle + \alpha_2\,|00\ldots01\rangle + \cdots + \alpha_N\,|11\ldots11\rangle\,(N = 2^n)$$

şeklinde ifade edilir.

$$|00\ldots00\rangle = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}_{n\times 1} \qquad |00\ldots01\rangle = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}_{n\times 1} \qquad |11\ldots11\rangle = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}_{n\times 1}$$

Yukarıda görüldüğü gibi $n$-qubitlik durumda $2^n$ tane olası durum mevcuttur.

**Örnek 28.** Kuantum bilgisayarlarda 4 qubitlik bir bilgiyi tensörel çarpım ile ifade ediniz.

## 6.1 Kuantum Bilgisayarlarda Temel Kapılar (Operatörler=İşlemciler)

Klasik bilgisayarlarda olduğu gibi kuantum bilgisayarlarda da bilgi işleme kapılarla (operatörlerle) yapılmaktadır. Bu bağlamda kuantum bilgisayarlarda temel kapıları 2 grupta toplayabiliriz.

### 6.1.1 Tek Qubite Etki Eden Kapılar

Bu kapıların çoğu Pauli isimli bilim insanının yıllar önce parçacıkların sınıflandırılmasında kullandığı kapılardır.

**Birim Kapı:**

Bilindiği gibi kapılar aynı zamanda operatörler demektir. Bu nedenle önüne gelen duruma etki ederler ve onları kendi özellikleri doğrultusunda değiştirirler. Buna göre birim kapı önüne gelen qubite etki edip onu değiştirmeyen kapıdır ve

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \delta_0$$

şeklinde ifade edilir.

**Örnek 29.** I kapısının tek qubite etkisini bulunuz.

$$\begin{aligned}
|\psi\rangle &= \alpha|0\rangle + \beta|1\rangle \rightarrow \text{ 1 qubitlik bilgi} \\
I|\psi\rangle &= \alpha I|0\rangle + \beta I|1\rangle \quad I \quad |0\rangle \text{ ve } |1\rangle \text{ in önüne gelir çünkü operatör durumlara etki eder.} \\
&= \alpha\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} + \beta\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} \\
&= \alpha\begin{pmatrix}1\\0\end{pmatrix} + \beta\begin{pmatrix}0\\1\end{pmatrix} \\
&= \alpha|0\rangle + \beta|1\rangle \\
&= |\psi\rangle
\end{aligned}$$

**NOT Kapısı (X Kapısı):**

Bu kapı önüne gelen durumların değilini oluşturduğu için buna NOT kapısı denmektedir ve

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

şeklinde gösterilmektedir.

**Örnek 30.** I kapısının tek qubite etkisini bulunuz.

$$\begin{aligned}
X|\psi\rangle &= \alpha X|0\rangle + \beta x|1\rangle \\
&= \alpha\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} + \beta\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} \\
&= \alpha\begin{pmatrix}0\\1+\beta\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} \\
&= \alpha|1\rangle + \beta|0\rangle
\end{aligned}$$

**($\delta_y$)Y Kapısı:**

$$\delta_y = Y = \begin{pmatrix}0 & i\\ 1 & -i\end{pmatrix}$$

**Örnek 31.** Y kapısının tek qubite etkisini bulunuz.

$$\begin{aligned} Y|\psi\rangle &= \alpha Y|0\rangle + \beta Y|1\rangle \\ &= \alpha\begin{pmatrix}0 & i\\ 1 & -i\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} + \beta\begin{pmatrix}0 & i\\ 1 & -i\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} \\ &= \alpha\begin{pmatrix}0\\-i\end{pmatrix} + \beta\begin{pmatrix}i\\0\end{pmatrix} \\ &= -i\alpha\begin{pmatrix}0\\1\end{pmatrix} + i\beta\begin{pmatrix}1\\0\end{pmatrix} \\ &= -i\alpha|1\rangle + i\beta|0\rangle \end{aligned}$$

**($\delta_z$)Z Kapısı:**

Bu kapı faz kapısı olarak ta adlandırılmaktadır ve

$$\delta_z = Z = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$$

şeklinde gösterilir.

**Örnek 32.** Z kapısının tek qubite etkisini bulunuz.

$$\begin{aligned} Z|\psi\rangle &= \alpha Z|0\rangle + \beta Z|1\rangle \\ &= \alpha\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} + \beta\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} \\ &= \alpha\begin{pmatrix}1\\0\end{pmatrix} + \beta\begin{pmatrix}0\\-1\end{pmatrix} \\ &= \alpha|0\rangle - \beta|1\rangle \end{aligned}$$

Bu kapı gelen olarak phase (P)

$$P(\gamma) = \begin{pmatrix}1 & 0\\ 0 & e^{i\gamma}\end{pmatrix}, \quad e^{i\gamma} = \cos\gamma + i\sin\gamma$$

şeklinde ifade edilir.

$$\begin{aligned} \gamma &= \pi \Rightarrow P(\gamma) \quad \text{Z kapısı} \\ \gamma &= \tfrac{\pi}{2} \Rightarrow P(\gamma) \quad \text{S kapısı} \\ \gamma &= \tfrac{\pi}{4} \Rightarrow P(\gamma) \quad \text{T kapısı} \end{aligned}$$

**Döndürme Kapıları:**

Bu kapılar xyz eksenlerinde döndürme işlemi yapan kapılardır ve aşağıdaki şekilde ifade edilirler.

$$\begin{aligned} R_x(\gamma) = &\quad e^{-i\frac{\gamma x}{2}} = \cos\tfrac{\gamma x}{2} I - i \sin\tfrac{\gamma x}{2} \\ \gamma = &\quad e^{-i\frac{\gamma y}{2}} = \cos\tfrac{\gamma y}{2} I - i \sin\tfrac{\gamma y}{2} \\ \gamma = &\quad e^{-i\frac{\gamma z}{2}} = \cos\tfrac{\gamma z}{2} I - i \sin\tfrac{\gamma z}{2} \end{aligned}$$

Bu 3 kapı aşapıdaki şekilde tek kapı olarak ifade edilir.

$$U = e^{ia} R_z(b) R_y(c) R_z(d)$$

**Hadamard Kapısı:**

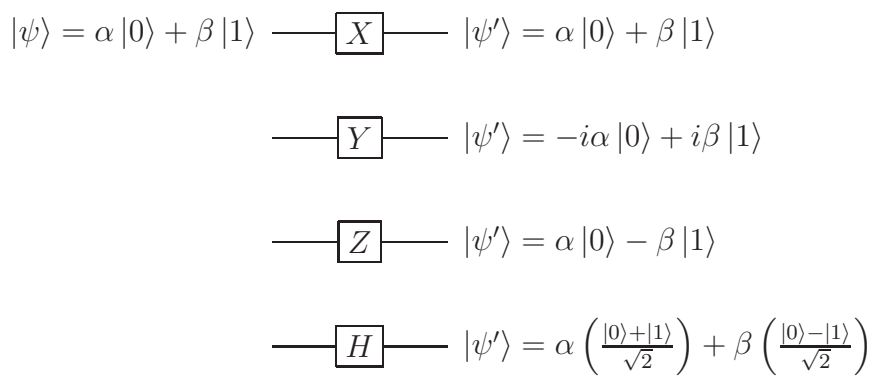
$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

**Örnek 33.** $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$ şeklindeki tek qubite hadamard kapısının etkisini bulunuz.

$$\begin{aligned} H|\psi\rangle = &\quad \alpha H|0\rangle + \beta H|1\rangle \\ = &\quad \alpha \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ = &\quad \alpha \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \tfrac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ -1 \end{pmatrix} \\ = &\quad \alpha \tfrac{1}{\sqrt{2}} (|0\rangle + |1\rangle) + \beta \tfrac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \\ = &\quad \alpha \left( \tfrac{|0\rangle + |1\rangle}{\sqrt{2}} \right) + \beta \left( \tfrac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \end{aligned}$$

**Not 24.** Yukarıdaki örnekten de görüldüğü gibi Hadamard kapısı bir duruma etki ettiğinde o durumu oluşturan 2 alt durum cinsinden süperpozisyon durumuna getirir.

### 6.1.2 Tek Qubitlik Kapıların Devre Diyagramları



**Not 25.** Tek qubitlik kapılar birden fazla qubite de etki ederler bu durumda kapıların tensörel çarpımı oluşturulur. Fakat tensörel çarpım sonucu oluşan matris çok büyük olacağından her bir kapının kendi qubitine etkisi ve böylece birden fazla tek qubitlik kapının birden fazla qubite etkisi bulunmuş olur

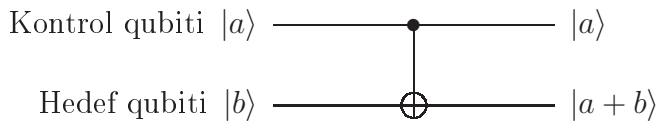
### 6.1.3 İki Qubite Etki Eden Kapılar

**CNOT (Kontrollü NOT Kapısı):**

Bu kapı kontrollü olduğundan ilk girdi qubiti 0 ise 2. qubite etki etmez. İlk girdi qubiti 1 ise 2. qubite etki eder ve değiştirir. Bu kapı

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

şeklinde tanımlanır.




$$CNOT = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10|$$

şeklinde de gösterebiliriz.

**Örnek 34.** $|\psi\rangle^{\otimes 2} = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$ şeklindeki 2. qubite CNOT kapısının etkisini bulunuz.

$$\begin{aligned} CNOT|\psi\rangle^{\otimes 2} &= aCNOT|00\rangle + bCNOT|01\rangle + cCNOT|10\rangle + dCNOT|11\rangle \\ &= a|00\rangle + b|01\rangle + c|11\rangle + d|10\rangle \end{aligned}$$

**Ödev:** Yukarıdaki örneğe CNOT kapısının brak-ket gösterimini (DİRAC) uygulayarak yukarıdaki sonucu elde ediniz.

$$\begin{aligned} |\psi\rangle^{\otimes 2} &= a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle \\ CNOT|\psi\rangle^{\otimes 2} &= aCNOT|00\rangle + bCNOT|01\rangle + cCNOT|10\rangle + dCNOT|11\rangle \\ &= a|00\rangle\langle 00|00\rangle + a|01\rangle\langle 01|00\rangle + a|10\rangle\langle 11|00\rangle + a|11\rangle\langle 10|00\rangle \\ &+ b|00\rangle\langle 00|01\rangle + b|01\rangle\langle 01|01\rangle + b|10\rangle\langle 11|01\rangle + b|11\rangle\langle 10|01\rangle \\ &+ c|00\rangle\langle 00|10\rangle + c|01\rangle\langle 01|10\rangle + c|10\rangle\langle 11|10\rangle + c|11\rangle\langle 10|10\rangle \\ &+ d|00\rangle\langle 00|11\rangle + d|01\rangle\langle 01|11\rangle + d|10\rangle\langle 11|11\rangle + d|11\rangle\langle 10|11\rangle \\ &= a|00\rangle + b|01\rangle + c|11\rangle + d|10\rangle \end{aligned}$$

**CH (Kontrollü Hadamard Kapısı):**

Bu kapı da CNOT kapısına benzer şekilde etki eder yani girdi qubiti 0 ise 2. qubite etki etmez. Girdi qubiti 1 ise 2. qubite hadamard uygulanır ve bu kapı

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

şeklinde tanımlanır.

**Örnek 35.** CH kapısının $|\psi\rangle = a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle$ şeklindeki 2. qubite etkisini bulunuz.

$$\begin{aligned} CH\,|\psi\rangle = &\ aCH\,|00\rangle + bCH\,|01\rangle + cCH\,|10\rangle + dCH\,|11\rangle \\ = &\ a\,|00\rangle + b\,|01\rangle + c\,|1\rangle \otimes \tfrac{|0\rangle+|1\rangle}{\sqrt{2}} + d\,|1\rangle \otimes \tfrac{|0\rangle-|1\rangle}{\sqrt{2}} \\ = &\ a\,|00\rangle + b\,|01\rangle + c\tfrac{|10\rangle+|11\rangle}{\sqrt{2}} + d\tfrac{|10\rangle-|11\rangle}{\sqrt{2}} \end{aligned}$$

# Bölüm 7

# Kuantum Bilgisayarlarda Bilginin Kopyalanamaması (No Cloning Theorem)

Bilindiği gibi kuantum bilgisayarlarda ölçme dışındaki kapıların hepsi birimseldir. Buna göre $u$ operatörü bir qubitlik $|\psi\rangle$ bilginin kopyalayan birimsel operatör olsun. Bu durumda $u$ operatörünün kuantum bilgisayarlardaki temel bazlara ($|0\rangle$ ve $|1\rangle$) etkisi

$$u\,|0\rangle = |00\rangle$$

$$u\,|1\rangle = |11\rangle$$

şeklinde olur.Buna göre $u$'nun bir qubitlik $|\psi\rangle$'ye etkisi

$$\begin{aligned} u\,|\psi\rangle = &\quad \alpha u\,|0\rangle + \beta u\,|1\rangle \\ = &\quad \alpha\,|00\rangle + \beta\,|11\rangle \end{aligned}$$

yukarıdan da görüldüğü gibi $u$ operatörü $|\psi\rangle$'nin tüm olası durumlarını içerecek şekilde kopyasını oluşturamamıştır. Eğer kopyasını oluşturmuş olsaydı elde edilecek bilgi

$$u\,|\psi\rangle = \alpha^2\,|00\rangle + \alpha\beta\,|01\rangle + \beta\alpha\,|10\rangle + \beta^2\,|11\rangle$$

şeklinde olmalıydı.

Yukarıdan da görüldüğü gibi 2 kuantum bilgisayar arasındaki iletişimde araya 3. kişinin girip bilgiyi kopyalaması mümkün gözükmemektedir. Çünkü araya giren kişi ölçüm yapmış olacaktır. Kuantum temelinde ölçüm yapmak demek tüm olası durumların tek bir duruma çökmesi demektir ve bu durumda da ana sistem değişmiş olacaktır. Dolayısıyla ana sistemdeki bilginin tamamını kopyalamak mümkün gözükmemektedir.

# Bölüm 8

# Kuantum Bilgisayarlarda Dolaşıklık (Entanglement)

A ve B gibi 2 sistem düşünelim. Eğer A sisteminin belirli özellikleri B sisteminin bazı özellikleri ile ilişkili ise ve bu ilişki durumu A ve B sistemleri birbirlerinden sonsuz uzaklıkta olsalar bile geçerli ise bu iki sistem dolaşıktır demektir. Bunun anlamı böyle bir iki sistemden herhangi birinde ölçüm yaparak diğerinde hiç ölçüm yapmadan diğeri hakkında bilgi edinmektir. Dolaşıklık bilgisi aslında bilim insanlarının 1930'lu yıllardan veri özellikle Einstein-Podolski-Rosen (EPR) bilim insanlarının yapmış olduğu bilimsel çalışmadan sonra daha bilinir hale gelmiştir.

**Not 26.** Kuantum bilgisayarlarda bu durum kuantum bilgisayarlarda hiç olmayan özellikler kazandırmaktadır. Kuantum bilgisayarların çok çok önemli olmalarının bir sebebi de kuantum bilgisayarlarda dolanık olmayan durumların kapılar yardımıyla (Hadamard ve CNOT) dolanık hale getirilmesinin mümkün olmasıdır ve böylece bir bilgi bir yerden anlık olarak gönderilebilmektedir (teleportasyon) kuantum bilgisayarlarda dolanık olmayan bir bilgi sırasıyla Hadamard ve CNOT kapılarının uygulanmasıyla dolanık hale getirilebilmektedir.

**Örnek 36.** $|\psi\rangle^{\otimes 2} = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$ şeklindeki 2 qubitlik bilgiyi dolanık hale getiriniz.

$$\begin{aligned}
|\psi\rangle^{\otimes 2} &= |\psi_1\rangle \otimes |\psi_2\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle \\
H|\psi\rangle^{\otimes 2} &= aH|00\rangle + bH|01\rangle + cH|10\rangle + dH|11\rangle \\
&= a\left(\tfrac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\otimes|0\rangle + b\left(\tfrac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\otimes|1\rangle + c\left(\tfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\otimes|0\rangle + d\left(\tfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\otimes|1\rangle \\
&= a\left(\tfrac{|00\rangle+|10\rangle}{\sqrt{2}}\right) + b\left(\tfrac{|01\rangle+|11\rangle}{\sqrt{2}}\right) + c\left(\tfrac{|00\rangle-|10\rangle}{\sqrt{2}}\right) + d\left(\tfrac{|01\rangle-|11\rangle}{\sqrt{2}}\right) \rightarrow \text{süperpozisyon durumu} \\
CNOT|\psi\rangle_S^{\otimes 2} &= \tfrac{1}{\sqrt{2}}[a(CNOT|00\rangle + CNOT|10\rangle) + b(CNOT|01\rangle + CNOT|11\rangle) \\
&+ c(CNOT|00\rangle - CNOT|10\rangle) + d(CNOT|01\rangle - CNOT|11\rangle)] \\
|\psi\rangle_D^{\otimes 2} &= \tfrac{1}{\sqrt{2}}[a(|00\rangle + |11\rangle) + b(|01\rangle + |10\rangle) + c(|00\rangle - |11\rangle) + d(|01\rangle - |10\rangle)]
\end{aligned}$$

**Not 27.** Yukarıdaki örneğin sonucunda da görüleceği gibi 2 qubitlik bilginin bir kısmı A kişisi tarafından diğer kısmı ise B kişisi tarafından paylaşılmaktadır. Bu paylaşmadan sonra kişiler arasındaki uzaklık sonsuz da olsa arada hiçbir iletişim kanalı olmamasına rağmen A da yapılan bir değişiklik anlık olarak B de ortaya çıkmaktadır. Bu durumun tersi de geçerlidir. Yani B'de yapılan değişiklik anlık olarak A'da görülmektedir.

**Örnek 37.** Hadamard kapısının birimsel olup olmadığını araştırınız.

$$(H^*)^T = H^{-1} \Rightarrow (H^*)^T = I \text{ ise } H \text{ birimseldir.}$$

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

$$H^* = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad H(H^*)^T = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$H(H^*)^T = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I \text{ olduğundan}$$

$H$ birimseldir.

**Örnek 38.** $X$ kapısının birimsel olup olmadığını araştırınız.

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

$$X^* = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad (X^*)^T = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$X(X^*)^T = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = I \text{ olduğundan } X \text{ birimseldir.}$$

**Not 28.** Birimsel dönüşümler uzunlukları koruyan dönüşümlerdir.

**Örnek 39.** $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ NOT kapısının öz durumlarını (öz vektörlerini bulunuz.)

$$\begin{aligned} X|X\rangle &= \lambda_i |X\rangle \\ (X - \lambda_i I)|X\rangle &= 0 \\ &\Rightarrow \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} - \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} = 0 \\ &\Rightarrow \begin{pmatrix} -\lambda & 1 \\ 1 & -\lambda \end{pmatrix} = 0 \\ &\Rightarrow \lambda^2 - 1 = 0 \\ \lambda &= \mp 1 \\ (X - (1)I)|x_1\rangle &= 0 \\ \left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right] \begin{bmatrix} x \\ y \end{bmatrix} &= 0 \Rightarrow \begin{bmatrix} -1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = 0 \Rightarrow \begin{matrix} -x+y=0 \\ x-y=0 \end{matrix} \Big\} \; x = y \end{aligned}$$

olduğundan keyfi $x = 1$ için $y = 1$ $|x_1\rangle = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ öz vektör

$$\begin{aligned} (X - (-1)I)|x_2\rangle &= 0 \\ \left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} - \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\right] \begin{bmatrix} x \\ y \end{bmatrix} &= 0 \Rightarrow \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = 0 \Rightarrow \begin{matrix} x+y=0 \\ x+y=0 \end{matrix} \Big\} \; x = -y \end{aligned}$$

olduğundan keyfi $x = -1$ için $y = -1$ $|x_2\rangle = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$ öz vektör

$$|x\rangle = (|x_1\rangle\,|x_2\rangle) = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

**Not 29.** Yukarıdaki örnekte görülebileceği gibi NOT kapısını normlu öz vektörleri hadamard kapısına denk gelmektedir.

**Örnek 40.** $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ NOT kapısının $|0\rangle$ daki beklenen değeri $\langle X \rangle$ nedir?

$$\begin{aligned}
\langle X\rangle = &\quad \langle 0|X|0\rangle \\
\langle 0|\left((|0\rangle)^*\right)^T = &\quad \begin{pmatrix}1\\0\end{pmatrix}^T = \begin{pmatrix}1 & 0\end{pmatrix} \\
X|0\rangle = &\quad \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix} \\
\langle 0|X|0\rangle = &\quad \begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} = 0 \rightarrow X \text{ kapısının } |0\rangle\text{'daki ölçüm sonucudur.}
\end{aligned}$$

**Ödev:**

**2)** $X$ kapısının $|1\rangle$'deki beklenen değerini bulunuz.

**2)** Hadamard kapısının $\frac{1}{\sqrt{3}}|0\rangle + \sqrt{\frac{2}{3}}|1\rangle$'deki beklenen değeri bulunuz.

**Örnek 41.** $|01\rangle$'in $|0\rangle$'daki beklenen değeri nedir?

$$\begin{aligned}
&\langle 0|01|0\rangle \\
\langle 0| = &\quad \left((|0\rangle)^*\right)^T = \begin{pmatrix}1 & 0\end{pmatrix} \\
\begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = &\quad \begin{pmatrix}0\\1\\0\\0\end{pmatrix} \\
\begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix}0\\1\\0\\0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} &\quad \text{bu olmaz}
\end{aligned}$$

Beklenen değer ölçülebilen nicekliklere karşılık gelen ölçüm sonucudur. Bir durumun bir durumdaki beklenen değeri olması mümkün değildir.

# Bölüm 9

# Bell Durumları (Bazları)

Herhangi bir sistem iki çift sistemden meydana geliyorsa bu tür sistemlere biparite sistemler denir. İki alt sistemden meydana gelen sistemi olası 4 tane dolaşık durumu (entanglement) vardır ve bu durumlara bell durumları denmektedir. Bunlar aşağıdaki şekilde ifade edilir.

$$|B_{00}\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$$

$$|B_{10}\rangle = \frac{|00\rangle-|11\rangle}{\sqrt{2}}$$

$$|B_{01}\rangle = \frac{|01\rangle+|10\rangle}{\sqrt{2}}$$

$$|B_{11}\rangle = \frac{|01\rangle+|10\rangle}{\sqrt{2}}$$

Bu durumları genel olarak

$$|B_{xy}\rangle = \frac{|0y\rangle + (-1)^x |1\bar{y}\rangle}{\sqrt{2}}$$

şeklinde tanımlanır.

Bunlar dolaşık durumlardır. Bir sistemde dolanıklığı Hadamart ve CNOT uygulayarak buluyoruz.

**Örnek 42.** $|10\rangle$ durumunu dolaşık hale getiriniz.

$$H|10\rangle = H|1\rangle \otimes |0\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}} \otimes |0\rangle$$

$$= \frac{|00\rangle-|10\rangle}{\sqrt{2}}$$

$$CNOT\left(\frac{|00\rangle-|10\rangle}{\sqrt{2}}\right) = \frac{CNOT|00\rangle-CNOT|10\rangle}{\sqrt{2}}$$

$$= \frac{|00\rangle-|11\rangle}{\sqrt{2}}$$

**Örnek 43.** $\underbrace{(H \otimes H)}_{H^{\otimes 2}} |11\rangle$

$$\begin{aligned} H^{\otimes 2} |11\rangle &= H|1\rangle \otimes H|1\rangle \\ &= \tfrac{|0\rangle - |1\rangle}{\sqrt{2}} \otimes \tfrac{|0\rangle - |1\rangle}{\sqrt{2}} \\ &= \tfrac{|00\rangle - |01\rangle - |10\rangle + |11\rangle}{\sqrt{2}} \end{aligned}$$

**Örnek 44.** $H(H|0\rangle) =?$ Hadamart'ın $|0\rangle$'a etkisine Hadamart etkisini bulunuz.

$$\begin{aligned} H|0\rangle &= \tfrac{|0\rangle + |1\rangle}{\sqrt{2}} \\ H\left(\tfrac{|0\rangle + |1\rangle}{\sqrt{2}}\right) &= \tfrac{1}{\sqrt{2}} H|0\rangle + \tfrac{1}{\sqrt{2}} H|1\rangle = \tfrac{1}{\sqrt{2}} \left(\tfrac{|0\rangle + |1\rangle}{\sqrt{2}} + \tfrac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \\ &= \tfrac{1}{2}(2|0\rangle) = |0\rangle \end{aligned}$$

# Bölüm 10

# Sistemlerin Dolaşıklığının Tespiti

## 10.1 Bell Bazları Yardımıyla Dolaşıklık Tespiti

Eğer bir sistem iki alt durumdan meydana geliyorsa bu tür sistemlerin dolaşıklığı Bell bazlarının yardımıyla kolylıkla tespit edilebilmektedir. Bunun için durum

$$|\psi\rangle = \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}$$

şeklinde sütun vektörü şekline getirilir. Eğer

$$\begin{aligned} ad = bc \Leftrightarrow &\quad \text{Sistem dolanık değil} \\ ad \neq bc \Leftrightarrow &\quad \text{Sistem dolaşık} \end{aligned}$$

**Örnek 45.** $|B_{00}\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$ Bell durumunun dolaşık olup olmadığı araştırınız.

$$
\begin{aligned}
|00\rangle = \quad & |0\rangle \otimes |0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\\0\\0\\0\end{pmatrix} \\
|11\rangle = \quad & |1\rangle \otimes |1\rangle = \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\0\\0\\1\end{pmatrix} \\
|B_{00}\rangle = \quad & \tfrac{1}{\sqrt{2}} \left[ \begin{pmatrix}1\\0\\0\\0\end{pmatrix} + \begin{pmatrix}0\\0\\0\\1\end{pmatrix} \right] = \tfrac{1}{\sqrt{2}} \begin{pmatrix}1\\0\\0\\1\end{pmatrix} \begin{matrix}a\\b\\c\\d\end{matrix} \\
\tfrac{1}{\sqrt{2}} \cdot \tfrac{1}{\sqrt{2}} \neq \quad & 0.0 \Rightarrow |B_{00}\rangle \text{ dolaşıktır.}
\end{aligned}
$$

**Ödev:** $|B_{01}\rangle$, $|B_{10}\rangle$, $|B_{11}\rangle$ durumlarının dolaşık olup olmadığını Bell yöntemiyle bulunuz.

## 10.2 Pauli Gösterimi Yardımıyla Dolaşıklık Tespiti

Tek qubitlik bir sistem Pauli gösterimi ile

$$\rho = \frac{1}{2} \sum_{i=0}^{3} c_i \delta_i$$

şeklinde ifade edilir. Burada $\begin{smallmatrix}\delta_i=\text{Pauli Matrislerini}\\ c_i=\text{Pauli Katsayılarını}\end{smallmatrix}$ ifade etmektedir. Burada $c_i$ katsayıları

$$c_i = \mathrm{Tr}(\rho \delta_i)$$

şeklinde ifade edilir. Benzer şekilde 2 qubitlik bir sistemin Pauli gösterimi

$$\rho = \frac{1}{4} \sum_{i=0}^{3} c_{ij} \delta_{ij} \qquad \begin{matrix}\delta_{ij} = \delta_i \otimes \delta_j \\ \delta_i, \delta_j = \text{Pauli Matrisler} \\ c_{ij} = \text{Pauli Katsayılarını}\end{matrix}$$

Benzer şekilde

$$c_{ij} = \mathrm{Tr}(\rho \delta_i \otimes \delta_j)$$

Eğer $|c_{00}| + |c_{11}| + |c_{22}| + |c_{33}| \leq 1$ ise sistem dolaşık değil yani iki alt sistemden oluşan sistem

kendisini oluşturan iki sistemin ayrı ayrı yazılması durumuna sahiptir. Yani sistem ayrılabilir bir sitemdir. Bunun dışındaki durumlarda sistem Dolaşıktır. Yukarıdan da görüldüğü gibi $c_{ij}$ katsayıları elde edilerek sistemlerin dolaşıklığı kolayca anlaşılabilir.

**Not 30.** Tek qubitin dolaşıklığı olmaz.

## Bir Sistemin Yoğunluk Matrisinin Elde Edilmesi:

Herhangi bir sistemin (Kompleks uzaydaki gösterimi $|\psi\rangle$ olur) yoğunluk matrisi

$$\rho = |\psi\rangle\langle\psi|$$

şeklinde durumun dış çarpımı olarak ifade edilir. Yoğunluk matrisi yardımıyla bir sistemin herhangi bir sitem üzerindeki izdüşüm durumu (trace) ve sistemin herhangi bir sistemdeki davranışı yani beklenen değeri kolayca tespit edilebilir. Diğer bir değişle

$$\mathrm{Tr}(\rho) = \sum_j \langle u_j|\rho|u_j\rangle = \sum_j \langle u_j|\psi\rangle\langle\psi|u_j\rangle$$

$$\langle A\rangle = \sum_{i=1}^{n} \langle u_i|\rho_A|u_i\rangle = \mathrm{Tr}\{\rho_A\} \text{ A üzerindeki izdüşümü}$$

**Örnek 46.** $|u_1\rangle$ ve $|u_2\rangle$ ortonormal baz sistemindeki bir durum $|\psi\rangle = \frac{1}{\sqrt{3}}|u_1\rangle + i\sqrt{\frac{2}{3}}|u_2\rangle$ olduğuna göre bu sistemin $\rho$ (yoğunluk matrisi) ve yoğunluk matrisinin izini($\mathrm{Tr}(\rho)$) bulunuz.

$$\begin{aligned}
\mathrm{Tr}(\rho) = &\ |\psi\rangle\langle\psi| \\
\langle\psi| = &\ ((|\psi\rangle)^*)^T = \tfrac{1}{\sqrt{3}}\langle u_1| - i\sqrt{\tfrac{2}{3}}\langle u_2| \\
\rho = &\ \left(\tfrac{1}{\sqrt{3}}|u_1\rangle + i\sqrt{\tfrac{2}{3}}|u_2\rangle\right)\left(\tfrac{1}{\sqrt{3}}\langle u_1| - i\sqrt{\tfrac{2}{3}}\langle u_2|\right) \\
= &\ \tfrac{1}{3}|u_1\rangle\langle u_1| - i\tfrac{\sqrt{2}}{3}|u_1\rangle\langle u_2| + i\tfrac{\sqrt{2}}{3}|u_2\rangle\langle u_1| + \tfrac{2}{3}|u_2\rangle\langle u_2|
\end{aligned}$$

$\mathrm{Tr}(\rho)$ sistemin bulunduğu uzaydaki bazlarındaki beklenen değeri, enerji değeridir. (bazlar üstündeki izdüşümü)

$$\begin{aligned}
\rho = &\ \textstyle\sum_{i=1}^{2}\langle u_i|\rho|u_i\rangle = \langle u_1|\rho|u_1\rangle + \langle u_2|\rho|u_2\rangle \\
= &\ \langle u_1|\left[\tfrac{1}{3}|u_1\rangle\langle u_1| - i\tfrac{\sqrt{2}}{3}|u_1\rangle\langle u_2| + i\tfrac{\sqrt{2}}{3}|u_2\rangle\langle u_1| + \tfrac{2}{3}|u_2\rangle\langle u_2|\right]|u_1\rangle \\
+ &\ \langle u_2|\left[\tfrac{1}{3}|u_1\rangle\langle u_1| - i\tfrac{\sqrt{2}}{3}|u_1\rangle\langle u_2| + i\tfrac{\sqrt{2}}{3}|u_2\rangle\langle u_1| + \tfrac{2}{3}|u_2\rangle\langle u_2|\right]|u_2\rangle \\
= &\ \left[\tfrac{1}{3}\langle u_1| - i\tfrac{\sqrt{2}}{3}\langle u_2|\right]|u_1\rangle + \left[i\tfrac{\sqrt{2}}{3}\langle u_1| + \tfrac{2}{3}\langle u_2|\right]|u_2\rangle \\
= &\ \tfrac{1}{3} + \tfrac{2}{3} = 1
\end{aligned}$$

**Not 31.** Bir matrisin yoğunluk matrisinin karesi yoğunluk matrisine eşitse yani $\rho^2 = \rho$ Diğer bir deyişle yoğunluk matrisinin izi $\mathrm{Tr}(\rho)$ 1 ise bu durumlara saf (pure) durumlar denir.

## 10.3 Schmidt Ayrıştırma Yöntemiyle Dolaşıklık Tespiti

$|a_i\rangle \in H_A$, $|b_i\rangle \in H_B$ ve $|\psi\rangle \in H_A \otimes H_B$ olduğuna göre $|\psi\rangle$ bu iki alt uzayın ortonormal bazları cinsinden

$$|\psi\rangle = \sum_i \lambda_i |a_i\rangle |b_i\rangle$$

şeklinde ifade edilir. Burada $\lambda_i$ =Schmidt Katsayıları'dır ve $\lambda_i \geq 0$ dır.

Yukarıdan da görüldüğü gibi Schmidt katsayıları sistemin 0'dan farklı özdeğerleri toplamına eşittir. Eğer Schmidt katsayıları toplamı 1 ise sistem dolaşık değildir.

$$Sch(\lambda_i) = \sum_i \lambda_i = 1 \Rightarrow \text{ Sistem Dolaşık Değildir.}$$

Yani sistem ayrılabilir bir sistemdir. Diğer bir deyişle sistem iki alt sistemin tensörel çarpımı şeklinde yazılabilir demektir. Eğer Scmidt katsayıları 1'den büyüksebu durumda sistem dolaşıktır.

# Bölüm 11

# Süper Yoğun Kodlama (Super Dense Coding)

Bilindiği gibi kuantum bilgisayarlarda dolaşık olmayan durumlar Hadamard ve CNOT kapısı yardımıyla dolaşık hale getirilebilmektedir. Bu durum yardımıyla iki klasik bit tek bir qubit vasıtasıyla (dolaşık durumu) bir yerden başka bir yere anlık olarak gönderilebilmektedir. Buna da süper yoğun kodlama denir. Süper yoğun kodlama aslında dolaşıklık vasıtasıyla iki klasik bitin tek bir qubit yardımıyla bir yerden başka bir yere anlık olarak teleportasyonudur. Bu durum kuantum kriptografide çok sık kullanılmaktadır.

Süper yoğun kodlama kuantum bilgisayarda aşağıdaki şekilde gerçekleştirilir:

### I. Adım:

Alice Bob'a 2 bitlik bir veriyi göndermek istesin. Öncelikle Alice ve Bob aşağıdaki Bell durumlarından (dolaşık durumlar) birini paylaşmaları gerekir.

$$|B_{00}\rangle = \frac{|0_A0_B\rangle+|1_A1_B\rangle}{\sqrt{2}} \quad |B_{01}\rangle = \frac{|0_A1_B\rangle+|1_A0_B\rangle}{\sqrt{2}}$$

$$|B_{10}\rangle = \frac{|0_A0_B\rangle-|1_A1_B\rangle}{\sqrt{2}} \quad |B_{11}\rangle = \frac{|0_A1_B\rangle-|1_A0_B\rangle}{\sqrt{2}}$$

Örneğin Alice ve Bob $|B_{00}\rangle = \frac{|0_A0_B\rangle+|1_A1_B\rangle}{\sqrt{2}}$ durumunu paylaşsınlar. Alice 00 klasik bitini $|B_{00}\rangle$, 01 klasik bitini $|B_{01}\rangle$, 10 klasik bitini $|B_{10}\rangle$ ve 11 klasik bitini $|B_{11}\rangle$ durumlarına

karşılık getirir ve gönderme işlemi aşağıdaki şekilde gerçekleştirilir.

| Gönderilecek Klasik 2bit | Uygulanması Gereken Kapı | Bob'a Giden |
|---|---|---|
| 00 | $I\left\|B_{00}\right\rangle$ | $\left\|B_{00}\right\rangle$ |
| 01 | $(X\otimes I)\left\|B_{00}\right\rangle$ | $\left\|B_{01}\right\rangle$ |
| 10 | $(Y\otimes I)\left\|B_{00}\right\rangle$ | $\left\|B_{10}\right\rangle$ |
| 11 | $(iY\otimes I)\left\|B_{00}\right\rangle$ | $\left\|B_{11}\right\rangle$ |

**Not 32.** Yukarıdan da görülebileceği gibi Alice ve Bob dolaşık durumu paylaşırken herhangi bir kanal gerekiyorken dolaşıklık paylaşıldıktan sonra klasik bitlerin Bob'a gönderilmesinde arada herhangi bir kurala ihtiyaç yoktur. Bu Alice ve Bob çok uzakta olsalar bile geçerli bir durumdur.

## 11.1 Teleportasyon

Bilinmeyen bir durumu bir yerden başka bir yere anlık olarak gönderilmesidir. Bu durum kuantum bilgisayarda kapılar vasıtasıyla aşağıdaki şekilde gerçekleşir.

### I. Adım:

Öncelikle Alice ve Bob dört Bell durumundan bir tanesini paylaşmaları gerekir. Örneğin Alice ve Bob $\left|B_{00}\right\rangle = \frac{\left|0_A0_B\right\rangle+\left|1_A1_B\right\rangle}{\sqrt{2}}$ durumunu paylaşsınlar. Bu durumda iken Alice ve Bob'a $\left|\psi\right\rangle = \alpha\left|0\right\rangle+\beta\left|1\right\rangle$ şeklindeki bir qubitlik bilgiyi göndermek istesin. Bu 1 qubitlik bilgi aslında her ikisi tarafından bilinmeyen bir durumdur. Çünkü yukarıdan da görüleceği gibi $\alpha$ ve $\beta$'lar bilinmemektedir.

### II. Adım:

Alice'in elinde göndermek istediği qubitle birlikte $\left|\psi\right\rangle$ var bir de $\left|B_{00}\right\rangle$ var.

$$\begin{aligned}\left|\psi\right\rangle\otimes\left(\left|B_{00}\right\rangle\right) = &\ \left|X\right\rangle = \left(\alpha\left|0\right\rangle+\beta\left|1\right\rangle\right)\otimes\left(\tfrac{\left|0_A0_B\right\rangle+\left|1_A1_B\right\rangle}{\sqrt{2}}\right)\\ = &\ \tfrac{\alpha\left|00_A0_B\right\rangle+\alpha\left|01_A1_B\right\rangle+\beta\left|10_A0_B\right\rangle+\beta\left|11_A1_B\right\rangle}{\sqrt{2}}\end{aligned}$$

şeklinde olur. Alice kendi durumuna CNOT kapısı uygular.

$$\begin{aligned}\underbrace{CNOT\left|X\right\rangle}_{\left|X'\right\rangle} = &\ \tfrac{1}{\sqrt{2}}\left[\alpha CNOT\left|00_A0_B\right\rangle+\alpha\left|C\right\rangle NOT01_A1_B+\beta CNOT\left|10_A0_B\right\rangle+\beta CNOT\left|11_A1_B\right\rangle\right]\\ = &\ \tfrac{1}{\sqrt{2}}\left[\alpha\left|00_A0_B\right\rangle+\alpha\left|01_A1_B\right\rangle+\beta\left|11_A0_B\right\rangle+\beta\left|10_A1_B\right\rangle\right]\end{aligned}$$

## III. Adım:

Alice son duruma Hadamard uygular.

$$\begin{aligned}
\underbrace{H\left|X'\right\rangle}_{\left|X''\right\rangle} &= (H\otimes I\otimes I)\left|X'\right\rangle = \left|X''\right\rangle \\
&= \tfrac{1}{\sqrt{2}}\left[\alpha H\left|00_A0_B\right\rangle + \alpha H\left|01_A1_B\right\rangle + \beta H\left|11_A0_B\right\rangle + \beta H\left|10_A1_B\right\rangle\right] \\
&= \tfrac{1}{\sqrt{2}}\left[\alpha\tfrac{\left|0\right\rangle+\left|1\right\rangle}{\sqrt{2}}\otimes\left|0_A0_B\right\rangle + \alpha\tfrac{\left|0\right\rangle+\left|1\right\rangle}{\sqrt{2}}\otimes\left|1_A1_B\right\rangle + \beta\tfrac{\left|0\right\rangle-\left|1\right\rangle}{\sqrt{2}}\otimes\left|1_A0_B\right\rangle + \beta\tfrac{\left|0\right\rangle-\left|1\right\rangle}{\sqrt{2}}\otimes\left|0_A1_B\right\rangle\right] \\
&= \tfrac{1}{\sqrt{2}}\left[\alpha\left|00_A0_B\right\rangle + \alpha\left|10_A0_B\right\rangle + \alpha\left|01_A1_B\right\rangle + \alpha\left|11_A1_B\right\rangle\right. \\
&+ \left.\beta\left|01_A0_B\right\rangle - \beta\left|11_A0_B\right\rangle + \beta\left|00_A1_B\right\rangle - \beta\left|10_A1_B\right\rangle\right] \\
&= \tfrac{1}{2}\left[\underbrace{\left|00\right\rangle}_{Alice}\underbrace{(\alpha\left|0\right\rangle+\beta\left|1\right\rangle)}_{Bob} + \underbrace{\left|10\right\rangle}_{Alice}\underbrace{(\alpha\left|0\right\rangle-\beta\left|1\right\rangle)}_{Bob} + \underbrace{\left|01\right\rangle}_{Alice}\underbrace{(\alpha\left|1\right\rangle+\beta\left|0\right\rangle)}_{Bob} + \underbrace{\left|11\right\rangle}_{Alice}\underbrace{(\alpha\left|1\right\rangle-\beta\left|0\right\rangle)}_{Bob}\right]
\end{aligned}$$

| **Alice'in Ölçüm Sonuçları** | **Bob'un Elindeki Durum** | **Bob'un Uygulaması Gereken Kapı** |
|---|---|---|
| 00 | $\alpha\left\|0\right\rangle+\beta\left\|1\right\rangle$ | $I\left\|B_{00}\right\rangle$ |
| 01 | $\alpha\left\|1\right\rangle+\beta\left\|0\right\rangle$ | $X\left\|B_{00}\right\rangle$ |
| 10 | $\alpha\left\|0\right\rangle-\beta\left\|1\right\rangle$ | $Z\left\|B_{00}\right\rangle$ |
| 11 | $\alpha\left\|1\right\rangle-\beta\left\|0\right\rangle$ | $ZX\left\|B_{00}\right\rangle$ |

**Not 33.** Yukarıda görüleceği gibi Alice ölçüm sonuçlarını herhangi bir iletim kanalından Bob'a söyleyerek Bob da ölçüm sonucuna göre uygun kapı uygulayarak $\left|\psi\right\rangle=\alpha\left|0\right\rangle+\beta\left|1\right\rangle$ bilinmeyen durumunu elde etmiş olur. Dolayısıyla Alice ölçüm yaptığında hiç bir kanal olmadan 1 qubitlik bilgi anlık olarak Bob'a gitmiş olur.

# Bölüm 12

# Kuantum Bilgisayarlarda Ölçme

Bilindiği gibi kuantum bilgisayarlarda bir bilgi 0,1 ve bunların olası tüm durumlarını içerecek şekilde (süper pozisyon durumu) ifade edilmektedir. Kuantum bilgisayarlarda ölçme sistemi bu olası durumlardan muhtemelen olması beklenen durumun elde edilmesi olacağından ölçme işlemi olası durumarın tek bir duruma çökmesidir. Diğer bir deyişle ölçme işlemi sonucunda ana sistemin durumu değişmiş olacaktır. Bu değişim ölçme işlemi ile aynı anda gerçekleşmektedir. Bunun diğer bir sebebi ise kuantum bilgisayarlarda ölçme dışında kullanılan operatörler birimseldir. Bu operatörlerin öz değerleri de ölçüm sonuşlarına karşılık gelen değerler olup reeldir. Bu nedenle ölçüm sonucunda reel bir değer elde edilir. Kuantum bilgisayarlarda diğer işlemlerde olduğu gibi ölçme işlemi de operatör (işlemci=kapı) yardımıyla yapılır ve bu operatör birimsel değildir.

Ölçme işlemi genel olarak aşağıdaki şekilde yapılır.

## 12.1 İzdüşüm Operatörü Yardımıyla Ölçme (Projection)

$P_1, P_2, \cdots, P_n$'ler birbirlerine dik izdüşüm operatörleri olmak üzere bu izdüşüm operatörleri yardımıyla $|\psi\rangle$'nin ölçme olasılığı

$$\Pr(i) = |P_i|\psi\rangle|^2 = \langle\psi|P_i^2|\psi\rangle = \langle\psi|P_i|\psi\rangle$$

şeklinde elde edilir. Ölçüm sonucunda ise sistemin durumu

$$|\psi'\rangle = \frac{P_i|\psi\rangle}{\sqrt{\langle\psi|P_i|\psi\rangle}} \quad \text{Burada } P_i = |u_i\rangle\langle u_i| \text{ 'dir. } (u_i\text{'ler baz vektörleridir.})$$

**Not 34.** Ölçme işlemi aslında ölçmeye karşılık gelen $P_i$ (izdüşüm operatörleri) nin beklenen değerini elde etmektir. Bu da karşılık gelen birimsel operatörün öz değerine denktir.

**Örnek 47.** $|\psi\rangle = \frac{2}{\sqrt{19}}|u_1\rangle + \frac{2}{\sqrt{19}}|u_2\rangle + \frac{1}{\sqrt{19}}|u_3\rangle + \frac{2}{\sqrt{19}}|u_4\rangle + \sqrt{\frac{4}{19}}|u_5\rangle$

**a)** $|u_2\rangle$ durumunda $|\psi\rangle$ nin ölçüm sonucu ve ölçme sonucunda sistemin durumu

**b)** $|u_3\rangle$ durumunda $|\psi\rangle$ nin ölçüm sonucu ve ölçme sonucunda sistemin durumunu bulunuz.

**a)**
$$\left.\begin{array}{ll} P_1 = & |u_1\rangle\langle u_1| \\ P_2 = & |u_2\rangle\langle u_2| \\ P_3 = & |u_3\rangle\langle u_3| \\ P_4 = & |u_4\rangle\langle u_4| \\ P_5 = & |u_5\rangle\langle u_5| \end{array}\right\} \sum_{i=1}^{5} P_i = 1$$

$$P_r(|u_2\rangle) = |\langle u_2|\psi\rangle|^2 = \langle\psi|P_2|\psi\rangle$$

**I. Çözüm:**

$$\begin{array}{rl} P_r(|u_2\rangle) = & |\langle u_2|\psi\rangle|^2 \\ = & \left|\langle u_2| \left(\frac{2}{\sqrt{19}}|u_1\rangle + \frac{2}{\sqrt{19}}|u_2\rangle + \frac{1}{\sqrt{19}}|u_3\rangle + \frac{2}{\sqrt{19}}|u_4\rangle + \sqrt{\frac{4}{19}}|u_5\rangle\right)\right|^2 \\ = & \left|\frac{2}{\sqrt{19}}\langle u_2|u_2\rangle\right|^2 = \frac{4}{19} \end{array}$$

**II. Çözüm:**

$$\begin{array}{rl} P_r(|u_2\rangle) = & \langle\psi|P_2|\psi\rangle \\ P_2|\psi\rangle = & |u_2\rangle\langle u_2| \left(\frac{2}{\sqrt{19}}|u_1\rangle + \frac{2}{\sqrt{19}}|u_2\rangle + \frac{1}{\sqrt{19}}|u_3\rangle + \frac{2}{\sqrt{19}}|u_4\rangle + \sqrt{\frac{4}{19}}|u_5\rangle\right) \\ = & |u_2\rangle \left(\frac{2}{\sqrt{19}}\langle u_2|u_2\rangle\right) \\ = & \frac{2}{\sqrt{19}}|u_2\rangle\langle u_2|u_2\rangle = \frac{2}{\sqrt{19}}|u_2\rangle \end{array}$$

$$\begin{array}{rl} \langle\psi| = & ((|\psi\rangle)^*)^T = \frac{2}{\sqrt{19}}\langle u_1| + \frac{2}{\sqrt{19}}\langle u_2| + \frac{1}{\sqrt{19}}\langle u_3| + \frac{2}{\sqrt{19}}\langle u_4| + \sqrt{\frac{4}{19}}\langle u_5| \\ \langle\psi|P_2|\psi\rangle = & \left(\frac{2}{\sqrt{19}}\langle u_1| + \frac{2}{\sqrt{19}}\langle u_2| + \frac{1}{\sqrt{19}}\langle u_3| + \frac{2}{\sqrt{19}}\langle u_4| + \sqrt{\frac{4}{19}}\langle u_5|\right)\frac{2}{\sqrt{19}}|u_2\rangle \\ = & \frac{4}{19}\langle u_2|u_2\rangle \\ = & \frac{4}{19} \\ |\psi\rangle = & \frac{P_2|\psi\rangle}{\sqrt{\langle\psi|P_2|\psi\rangle}} = \frac{\frac{2}{\sqrt{19}}|u_2\rangle}{\sqrt{\frac{4}{19}}} = |u_2\rangle \end{array}$$

**Örnek 48.** $|\psi\rangle = \frac{\sqrt{3}}{2}|0\rangle - \frac{1}{2}|1\rangle$ şeklindeki bir qubitlik bilginin Y kapısındaki ölçüm sonucunu bulunuz.

**Not 35.** Öncelikle Y kapısına ait izdüşüm operatörlerinin tanımlanabilmesi için Y kapısının öz durumlarını (ortonormal) belirlemek gerekir. Bunun için de Y kapısına ait özdeğer probleminin çözülmesi gerekir. Her bir özdeğere karşılık gelen durumlar Y kapısının öz durumları olur. Bu öz durumlarda ortonormal hale getirilir. Böylece Y kapısına ait öz durumlar yardımıyla ölçüm operatörleri tanımlanmış olur.

$$Y|x\rangle = \lambda_i|x\rangle \Rightarrow \quad (Y-\lambda_i I)|x\rangle = 0 \qquad Y = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}$$

$$\left(\begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} - \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}\right) = 0 \Rightarrow \quad \begin{pmatrix} \lambda & i \\ -i & \lambda \end{pmatrix} = 0 \Rightarrow {}^{\lambda^2-1=0}_{\lambda=\mp 1}$$

$$\lambda_1 = 1 \Rightarrow \quad \begin{pmatrix} -1 & i \\ -i & -1 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = 0 \Rightarrow {}^{-x+iy=0}_{-ix-y=0} \Rightarrow {}^{x=iy}_{y=i \text{ için}}{}_{x=-1} \qquad |u_1\rangle = \begin{pmatrix} -1 \\ i \end{pmatrix}$$

$$||u_1\rangle| = \sqrt{2} \quad |u_1\rangle = \tfrac{|u_1\rangle}{||u_1\rangle|} = \tfrac{1}{\sqrt{2}}\begin{pmatrix} -1 \\ i \end{pmatrix}$$

$$\lambda_2 = -1 \Rightarrow \quad \begin{pmatrix} 1 & i \\ -i & 1 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = 0 \Rightarrow {}^{x+iy=0}_{ix+y=0} \Rightarrow {}^{x=-iy}_{y=i \text{ için}}{}_{x=1} \qquad |u_2\rangle = \begin{pmatrix} 1 \\ i \end{pmatrix}$$

$$||u_2\rangle| = \sqrt{2} \quad |u_2\rangle = \tfrac{|u_2\rangle}{||u_2\rangle|} = \tfrac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ i \end{pmatrix}$$

$$P_1 = \quad |u_1\rangle\langle u_1| = \tfrac{1}{\sqrt{2}}\begin{pmatrix} -1 \\ i \end{pmatrix}\tfrac{1}{\sqrt{2}}\begin{pmatrix} -1 & i \end{pmatrix} = \tfrac{1}{2}\begin{pmatrix} 1+i & i \\ -i & 1 \end{pmatrix} = \tfrac{1}{2}\begin{pmatrix} 1 & i \\ -i & 1 \end{pmatrix}$$

$$P_2 = \quad |u_2\rangle\langle u_2| \tfrac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ i \end{pmatrix}\tfrac{1}{\sqrt{2}}\begin{pmatrix} 1 & -i \end{pmatrix} = \tfrac{1}{2}\begin{pmatrix} 1 & -i \\ i & 1 \end{pmatrix}$$

$$P_r(|u_1\rangle) = \quad |\langle u_1|\psi\rangle|^2 = \langle\psi|P_1|\psi\rangle$$

$$P_1(|\psi\rangle) = \quad \tfrac{1}{2}\begin{pmatrix} 1 & i \\ -i & 1 \end{pmatrix}\left(\tfrac{\sqrt{3}}{2}|0\rangle - \tfrac{1}{2}|1\rangle\right) = \tfrac{1}{2}\begin{pmatrix} 1 & i \\ -i & 1 \end{pmatrix}\left(\tfrac{\sqrt{3}}{2}\begin{pmatrix} 1 \\ 0 \end{pmatrix} - \tfrac{1}{2}\begin{pmatrix} 0 \\ 1 \end{pmatrix}\right)$$

$$= \quad \tfrac{1}{2}\begin{pmatrix} 1 & i \\ -i & 1 \end{pmatrix}\begin{pmatrix} \frac{\sqrt{3}}{2} \\ -\frac{1}{2} \end{pmatrix} = \tfrac{1}{4}\begin{pmatrix} \sqrt{3}-i \\ -i\sqrt{3}-1 \end{pmatrix}$$

$$\langle\psi| = \quad \tfrac{\sqrt{3}}{2}\langle 0| - \tfrac{1}{2}\langle 1|$$

$$\langle\psi|P_1|\psi\rangle = \quad \left(\tfrac{\sqrt{3}}{2}\langle 0| - \tfrac{1}{2}\langle 1|\right)\tfrac{1}{4}\begin{pmatrix} \sqrt{3}-i \\ -i\sqrt{3}-1 \end{pmatrix} = \tfrac{1}{2}(\sqrt{3}-1)\tfrac{1}{4}\begin{pmatrix} \sqrt{3}-i \\ -i\sqrt{3}-1 \end{pmatrix}$$

$$= \quad \tfrac{1}{8}.4 = \tfrac{1}{2}$$

**Ödev:** $P_2$ operatörü yardımıyla diğer sonucu bulunuz.

**Not 36.** Ölçme işlemi $|0\rangle$, $|1\rangle$ bazlarında olduğu gibi X,Y,Z ve aynı zamanda Bell durumlarında da ölçme işlemi olabilir.

**Not 37.** Bilindiği gibi kuantum bilgisayarlarda $|0\rangle$ ve $|1\rangle$ temel bazlardır. Bu bazlara karşılık gelen ölçüm operatörleri ise sırasıyla $P_0 = |0\rangle\langle 0|$, $P_1 = |1\rangle\langle 1|$ şeklindedir. Bu ölçüm operatmrleri qubitlerin birden fazla olması durumunda aşağıdaki şekilde uygulanır. Örneğin 2 qubit

olması durumda

$$\begin{array}{ccccc} P_0 \otimes I & \text{ve} & I \otimes P_1 & & 2 \text{ qubiti için} \\ P_0 \otimes I \otimes I & \text{ve} & I \otimes I \otimes P_1 & & 3 \text{ qubiti için} \\ \vdots & & & & \\ P_0 \otimes I \otimes \cdots \otimes I_{n-1} & \text{ve} & I \otimes I \otimes \cdots \otimes I_{n-1} \otimes P_1 & & \text{n qubiti için} \end{array}$$

**Örnek 49.** $|\psi\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$ durumunun

**a)** $|0\rangle$ ve $|1\rangle$ deki ölçüm sonuçlarını bulunuz.

**b)** Ölçüm sonucunda sistemin durumunu tespit ediniz.

**a)**

$$\begin{aligned} P_r(|0\rangle) &= \langle\psi|P_0|\psi\rangle \qquad P_0 = |0\rangle\langle 0| \\ P_r(|1\rangle) &= \langle\psi|P_1|\psi\rangle \qquad P_0 = |1\rangle\langle 1| \\ (P_0 \otimes I)|\psi\rangle &= |0\rangle\langle 0| \left(\tfrac{|01\rangle - |10\rangle}{\sqrt{2}}\right) = \tfrac{1}{\sqrt{2}}(|0\rangle \otimes \langle 0|0\rangle \otimes |1\rangle - |0\rangle \otimes \langle 0|1\rangle \otimes |0\rangle) \\ &= \tfrac{1}{\sqrt{2}}|01\rangle \\ \langle\psi| &= \tfrac{\langle 01| - \langle 10|}{\sqrt{2}} \\ \langle\psi|P_0|\psi\rangle &= \tfrac{\langle 01| - \langle 10|}{\sqrt{2}} \tfrac{1}{\sqrt{2}}|01\rangle = \tfrac{1}{2}(\langle 0|0\rangle \langle 1|1\rangle - \langle 1|0\rangle \langle 0|1\rangle) \\ &= \tfrac{1}{2} \end{aligned}$$

**b)** $|\psi'\rangle = \frac{(P_0 \otimes I)|\psi\rangle}{\sqrt{\langle\psi|P_0|\psi\rangle}} = \frac{\frac{1}{\sqrt{2}}|01\rangle}{\sqrt{\frac{1}{2}}} = |01\rangle$

**ÖDEV:** $|1\rangle$ bazındakini yap.

**Örnek 50.** $|\psi\rangle = \left(\frac{\sqrt{2}+i}{\sqrt{20}}\right)|000\rangle + \frac{1}{\sqrt{2}}|001\rangle + \frac{1}{\sqrt{10}}|011\rangle + \frac{i}{\sqrt{2}}|111\rangle$

**a)** $P_r(|000\rangle)$ **b)** $P_r(|001\rangle)$ **c)** $P_r(|011\rangle)$ **d)** $P_r(|111\rangle)$ elde etme olasılıklarını bulun.

**a)** $P_r(|000\rangle) = \langle\psi|P_0|\psi\rangle = |\langle 000|\psi\rangle|^2 = \left|\frac{\sqrt{2}+i}{\sqrt{20}}\right|^2 = \frac{3}{20}$

**Eksik**

## 12.2 Genelleştirilmiş Ölçme

$M_m$, $|\psi\rangle$ durumundaki ölçüm (measurement) operatörü olsun. $M$ ölçüm sonucunun elde etme olasılığı $P_r(M) = \langle\psi|M_m^t M_m|\psi\rangle$' dir. Ölçüm sonucunda ise sistemin durumu

$$|\psi'\rangle = \frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^t M_m|\psi\rangle}}$$

şeklindedir. Eğer $|\psi\rangle$ durumunun yoğunluk operatörü $\rho = |\psi\rangle\langle\psi|$ biliyorsak bu durumda $M$ ölçüm sonucunu elde etme olasılığı

$$P_r(M) = \mathrm{Tr}\big(M_m^t M_\rho\big)$$

şeklinde bulunur. Eğer i ölçüm sonunca karşılık gelen izdüşüm operatörü $P_i = |u_i\rangle\langle u_i|$ şeklinde ise bu durumda i tane ölçüm sonucunun elde etme olasılığı

$$P_i = \mathrm{Tr}\big(P_i^t P_i \rho\big) = \mathrm{Tr}(|u_i\rangle\langle u_i|\,\rho) = \langle u_i|\rho|u_i\rangle$$

**Örnek 51.** Herhangi bir sistemin yoğunluk matrisi $\rho = \frac{5}{6}|0\rangle\langle 0| + \frac{1}{6}|0\rangle\langle 1|$ şeklinde verildiğine göre bu sistemin $|0\rangle$ daki ölçülme olasılığını bulunuz.

$$\begin{aligned} P_r(|0\rangle) = &\quad \langle 0|\rho|0\rangle = \langle 0|\left(\tfrac{5}{6}|0\rangle\langle 0| + \tfrac{1}{6}|0\rangle\langle 1|\right)|0\rangle \\ = &\quad \tfrac{5}{6}\langle 0|0\rangle\langle 0|0\rangle + \tfrac{1}{6}\langle 0|0\rangle\langle 1|0\rangle \\ = &\quad \tfrac{5}{6} \end{aligned}$$

# Bölüm 13

# Kuantum Bilgisayar

**Şekil**

$$\rho = \frac{1}{2}\sum_{i=0}^{3} c_i\delta_i \rightarrow \text{ Tek qubitin Pauli Gösterimi } (\delta_i\text{: Pauli Matrisleri})$$

$$\rho = \frac{1}{2^2}\sum_{i,j=0}^{3} c_{ij}\delta_i \otimes \delta_j \rightarrow \text{ İki qubitin Pauli Gösterimi } (\delta_{ij}\text{: Pauli Matrisleri})$$

$$c_i = \mathrm{Tr}(\rho\delta_i) = \langle\delta_i\rangle \text{ ve } c_{ij} = \mathrm{Tr}(\rho\delta_i \otimes \delta_i) = \langle\delta_i\delta_i\rangle$$

$c_{00}$ bir etkisi olmayacağı için alınmıyor.

$$|c_{11}| + |c_{22}| + |c_{33}| \leq 1 \Rightarrow \text{ ayrılabilir (dolaşık değil). Bunun dışındakiler dolaşık.}$$

**Örnek 52.** $\delta = \frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1|$ şeklinde yoğunluk matrisine sahip tek qubitlik durumun Pauli gösterimini elde ediniz.

$c_i$ katsayılarını elde edeceğiz.

$$\rho = \frac{3}{4}\begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}1 & 0\end{pmatrix} + \frac{1}{4}\begin{pmatrix}0\\1\end{pmatrix}\begin{pmatrix}0 & 1\end{pmatrix}$$

$$= \frac{3}{4}\begin{pmatrix}1 & 0\\0 & 0\end{pmatrix} + \frac{1}{4}\begin{pmatrix}0 & 0\\0 & 1\end{pmatrix} = \begin{pmatrix}\frac{3}{4} & 1\\0 & \frac{1}{4}\end{pmatrix}$$

$$c_0 = \mathrm{Tr}(\rho\delta_0) = \mathrm{Tr}\left[\begin{pmatrix}\frac{3}{4} & 1\\0 & \frac{1}{4}\end{pmatrix}\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}\right] = \mathrm{Tr}\begin{pmatrix}\frac{3}{4} & 1\\0 & \frac{1}{4}\end{pmatrix} = \frac{3}{4} + \frac{1}{4} = 1$$

$$c_1 = \mathrm{Tr}(\rho\delta_1) = \mathrm{Tr}\left[\begin{pmatrix}\frac{3}{4} & 1\\ 0 & \frac{1}{4}\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\right] = \mathrm{Tr}\begin{pmatrix}0 & \frac{3}{4}\\ \frac{1}{4} & 0\end{pmatrix} = 0+0=0$$

$$c_2 = \mathrm{Tr}(\rho\delta_2) = \mathrm{Tr}\left[\begin{pmatrix}\frac{3}{4} & 1\\ 0 & \frac{1}{4}\end{pmatrix}\begin{pmatrix}0 & -i\\ i & 0\end{pmatrix}\right] = \mathrm{Tr}\begin{pmatrix}0 & -\frac{3i}{4}\\ \frac{i}{4} & 0\end{pmatrix} = 0+0=0$$

$$c_3 = \mathrm{Tr}(\rho\delta_3) = \mathrm{Tr}\left[\begin{pmatrix}\frac{3}{4} & 1\\ 0 & \frac{1}{4}\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\right] = \mathrm{Tr}\begin{pmatrix}\frac{3}{4} & 1\\ 0 & -\frac{1}{4}\end{pmatrix} = \frac{3}{4}-\frac{1}{4}=\frac{1}{2}$$

$$\rho = \tfrac{1}{2}\textstyle\sum_{i=0}^{3} c_i\delta_i = \tfrac{1}{2}[c_0\delta_0 + c_1\delta_1 + c_2\delta_2 + c_3\delta_3]$$

$$= \tfrac{1}{2}[1I + 0X + 0Y + \tfrac{1}{2}Z]$$

$$= \tfrac{1}{2}[I + \tfrac{1}{2}Z]$$

**Örnek 53.** $H\otimes H\,|00\rangle$ durumunun dolaşık olup olmadığını Pauli gösterimi yardımıyla gösteriniz.

$$H\,|0\rangle \otimes H\,|0\rangle = \tfrac{(|0\rangle+|1\rangle)}{\sqrt{2}} \otimes \tfrac{(|0\rangle+|1\rangle)}{\sqrt{2}}$$

$$= \tfrac{1}{2}[|00\rangle + |01\rangle + |10\rangle + |11\rangle]$$

$$\rho = |\psi\rangle\langle\psi| = \tfrac{1}{2}[|00\rangle + |01\rangle + |10\rangle + |11\rangle]\tfrac{1}{2}[\langle 00| + \langle 01| + \langle 10| + \langle 11|]$$

$$= \tfrac{1}{4}[|00\rangle\langle 00| + |00\rangle\langle 01| + |00\rangle\langle 10| + |00\rangle\langle 11| + |01\rangle\langle 00| + |01\rangle\langle 01|$$

$$+ \ |01\rangle\langle 10| + |01\rangle\langle 11| + |10\rangle\langle 00| + |10\rangle\langle 01| + |10\rangle\langle 10| + |10\rangle\langle 11|$$

$$+ \ |11\rangle\langle 00| + |11\rangle\langle 01| + |11\rangle\langle 10| + |11\rangle\langle 11|]$$

$$\rho = \begin{pmatrix}1 & 1 & 1 & 1\\ 1 & 1 & 1 & 1\\ 1 & 1 & 1 & 1\\ 1 & 1 & 1 & 1\end{pmatrix}$$

$$c_{11} = \mathrm{Tr}(\rho\delta_1\otimes\delta_1) = \mathrm{Tr}(\rho X\otimes X) = \langle X\otimes X\rangle$$

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

$$\mathrm{Tr}(\rho X \otimes X) = \mathrm{Tr}\left[ \tfrac{1}{4} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \right] = \mathrm{Tr}\left[ \tfrac{1}{4} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix} \right]$$

$$= \tfrac{1}{4} + \tfrac{1}{4} + \tfrac{1}{4} + \tfrac{1}{4} = 1$$

$$c_{22} = \mathrm{Tr}(\rho \delta_2 \otimes \delta_2) = \mathrm{Tr}(\rho Y \otimes Y) =$$

$$Y \otimes Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix}$$

$$c_{22} = \mathrm{Tr}(\rho Y \otimes Y) = \mathrm{Tr}\left[ \tfrac{1}{4} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix} \right] = \mathrm{Tr}\left[ \tfrac{1}{4} \begin{pmatrix} -1 & 1 & 1 & -1 \\ -1 & 1 & 1 & -1 \\ -1 & 1 & 1 & -1 \\ -1 & 1 & 1 & -1 \end{pmatrix} \right]$$

$$= -\tfrac{1}{4} + \tfrac{1}{4} + \tfrac{1}{4} - \tfrac{1}{4} = 0$$

$$Z \otimes Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$c_{33} = \mathrm{Tr}(\rho Z \otimes Z) = \mathrm{Tr}\left[ \tfrac{1}{4} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \right] = \mathrm{Tr}\left[ \tfrac{1}{4} \begin{pmatrix} 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \right]$$

$$= \tfrac{1}{4} - \tfrac{1}{4} - \tfrac{1}{4} + \tfrac{1}{4} = 0$$

$$|c_1 1| + |c_2 2| + |c_3 3| \leq 1 \text{ mi bakılır !!!}$$

$1+0+0=1\leq 1$ olduğundan verilen durum Dolaşık değil yani ayrılabilir durum.

**Ödev:** $|B_{00}\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$ durumunu Pauli gösterimi yöntemiyle dolşık olup olmadığına bakınız.

$H_A$ ve $H_B$ Hilbert uzayları olsun.

$|a\rangle$ $|b\rangle$ bazları ortonormal bazlar (Schmidt bazları)

$|\psi\rangle = \sum_i \lambda_i |a_i\rangle |b_i\rangle \rightarrow$ Schmidt ayrıştırma yöntemi

$\lambda_i =$ Schmidt katsayıları

$\lambda_i = \mathrm{Tr}(|\psi\rangle\langle\psi|) \rightarrow$ özdeğerdir $(\lambda_i)$

Schmidt sayıları sıfırdan farklı $\lambda_i$'lerin sayısıdır.

Schmidt sayıları=1 $\Rightarrow$ sistem ayrılabilir yani dolaşık değildir.

Schmidt sayıları $> 1 \Rightarrow$ sistem dolaşıktır.

**Örnek 54.** $|\psi\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$ durumunun dolaşık olup olmadığı schmidt ayrıştırma yöntemiyle bulun.

$$\rho = |\psi\rangle\langle\psi| = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)\frac{1}{2}(\langle 00| + \langle 01| + \langle 10| + \langle 11|)$$

**I. Yol**

$$\begin{aligned}
\rho_A = &\ \mathrm{Tr}_B\,|\psi\rangle\langle\psi| = \langle 0|\psi\rangle\,\langle\psi|0\rangle + \langle 1|\psi\rangle\,\langle\psi|1\rangle \\
= &\ \tfrac{1}{4}(|0\rangle\langle 0| - |0\rangle\langle 1| - |1\rangle\langle 0| + |1\rangle\langle 1|) + \tfrac{1}{4}(|0\rangle\langle 0| - |0\rangle\langle 1| - |1\rangle\langle 0| + |1\rangle\langle 1|) \\
= &\ \tfrac{1}{2}(|0\rangle\langle 0| - |0\rangle\langle 1| - |1\rangle\langle 0| + |1\rangle\langle 1|) \\
\rho_A = &\ \tfrac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}
\end{aligned}$$

**Not 38.** 2 bazımız vardır. Bunların beklenen değerini bularak izini buluruz. Herhangi bir matrisin izini almak demek onun bazlarının izdüşümünü bulmaktır.

**II. Yol**

$$\begin{aligned}
\rho_A = &\ \mathrm{Tr}_B(\tfrac{1}{4}(|0\rangle\langle 0| - |0\rangle\langle 1| - |1\rangle\langle 0| + |1\rangle\langle 1| + \cdots) \\
\rho_A = &\ \langle 0|\psi\rangle\,\langle\psi|0\rangle + \langle 1|\psi\rangle\,\langle\psi|1\rangle
\end{aligned}$$

$$\begin{aligned}
\langle 0|\psi\rangle = &\ \tfrac{1}{2}\left[\langle 0|\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right)\right] \\
= &\ \tfrac{1}{2}\left[\langle 0|0\rangle \otimes |0\rangle + \langle 0|0\rangle \otimes |1\rangle + \langle 0|1\rangle \otimes |0\rangle + \langle 0|1\rangle \otimes |1\rangle\right] \\
= &\ \tfrac{1}{2}(|0\rangle + |1\rangle) = \tfrac{1}{2}\left[\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right] = \tfrac{1}{2}\begin{pmatrix} 1 \\ 1 \end{pmatrix} \\
\langle 1|\psi\rangle = &\ \tfrac{1}{2}(|0\rangle + |1\rangle) = \tfrac{1}{2}\begin{pmatrix} 1 \\ 1 \end{pmatrix}
\end{aligned}$$

$$\begin{aligned}
\langle\psi|0\rangle &= \tfrac{1}{2}\left[(|00\rangle + |01\rangle + |10\rangle + |11\rangle)\,|0\rangle\right] \\
&= \tfrac{1}{2}(\langle 0|\otimes\langle 0|0\rangle + \langle 0|\otimes\langle 1|0\rangle + \langle 1|\otimes\langle 0|0\rangle + \langle 1|\otimes\langle 1|0\rangle) \\
&= \tfrac{1}{2}(\langle 0| + \langle 1|) = \tfrac{1}{2}\begin{pmatrix}1 & 1\end{pmatrix} \\
\langle\psi|1\rangle &= \tfrac{1}{2}(\langle 0| + \langle 1|) = \tfrac{1}{2}\begin{pmatrix}1 & 1\end{pmatrix}
\end{aligned}$$

$$\begin{aligned}
\rho_A &= \tfrac{1}{2}[|0\rangle + |1\rangle]\tfrac{1}{2}[\langle 0| + \langle 1|] + \tfrac{1}{2}[|0\rangle + |1\rangle]\tfrac{1}{2}[\langle 0| + \langle 1|] \\
&= \tfrac{1}{4}[|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| + |1\rangle\langle 1|] + \tfrac{1}{4}[|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| + |1\rangle\langle 1|] \\
&= \tfrac{1}{4}[|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| + |1\rangle\langle 1| + |0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| + |1\rangle\langle 1|] \\
&= \tfrac{1}{2}[|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| + |1\rangle\langle 1|] \\
&= \tfrac{1}{2}\begin{pmatrix}\langle 0|\rho_A|0\rangle & \langle 0|\rho_A|1\rangle \\ \langle 1|\rho_A|0\rangle & \langle 1|\rho_A|1\rangle\end{pmatrix}
\end{aligned}$$

**Not 39.** Bir sisteme ait yoğunluk matrisi verildiğinde yoğunluk matrisinin matris gösterimi aşağıdaki şekilde gösterilir.

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

Bunun anlamı, verilen sistemin kuantum bilgisayar bazlarındaki beklenen değerlerinin matris elemanları şeklinde gösterimidir. Diğer bir değişle $\rho$ yoğunluğuna sahip bir sistemin $|0\rangle$ ve $|1\rangle$ bazlarındaki bulunma olasılığı toplamının matris şeklinde gösterilmesidir.

**Örnek 55.** $|\psi\rangle = \frac{1}{2}(|00\rangle - |01\rangle - |10\rangle + |11\rangle)$ yoğunluk matrisine sahip sistemin dolanıklığı Schmidt ayrıştırma yöntemiyle belirleyiniz.

$$\begin{aligned}
\rho = &\ |\psi\rangle\langle\psi| = \tfrac{1}{2}(|00\rangle - |01\rangle - |10\rangle + |11\rangle)\tfrac{1}{2}(\langle 00| - \langle 01| - \langle 10| + \langle 11|) \\
= &\ \tfrac{1}{4}(|00\rangle\langle 00| - |00\rangle\langle 01| - |00\rangle\langle 10| + |11\rangle\langle 11| \\
- &\ |01\rangle\langle 01| - |01\rangle\langle 01| - |01\rangle\langle 10| + |01\rangle\langle 11| \\
- &\ |10\rangle\langle 00| - |10\rangle\langle 01| - |10\rangle\langle 10| + |10\rangle\langle 11| \\
+ &\ |11\rangle\langle 00| - |11\rangle\langle 01| - |11\rangle\langle 10| + |11\rangle\langle 11|
\end{aligned}$$

Bu sistem üzerinden yukarıdaki sistemin izini almak demek yukarıdaki yoğunluk matrisine sahip sistemin $|0\rangle$ ve $|1\rangle$ bazındaki bulunma olasılığını bulmak demektir.

$$\rho_A = \mathrm{Tr}_B(\rho) = \mathrm{Tr}_B(|\psi\rangle\langle\psi|) = \overbrace{\langle 0|\psi\rangle\,\langle\psi|0\rangle}^{\langle 0|\psi|0\rangle} + \overbrace{\langle 1|\psi\rangle\,\langle\psi|1\rangle}^{\langle 1|\psi|1\rangle}$$

$$\begin{aligned}
\langle 0|\psi\rangle &= \langle 0|\left[\tfrac{1}{2}(|00\rangle - |01\rangle - |10\rangle + |11\rangle)\right] \\
&= \tfrac{1}{2}[\langle 0|0\rangle\otimes|0\rangle - \langle 0|0\rangle\otimes|1\rangle - \langle 0|1\rangle\otimes|0\rangle + \langle 0|1\rangle\otimes|1\rangle] \\
&= \tfrac{1}{2}[|0\rangle - |1\rangle]
\end{aligned}$$

$$\begin{aligned}\langle\psi|0\rangle &= \tfrac{1}{2}[\langle 0| - \langle 1|]\\ \langle 1|\psi\rangle &= \tfrac{1}{2}[-|0\rangle + |1\rangle]\\ \langle\psi|1\rangle &= \tfrac{1}{2}[-\langle 0| + \langle 1|]\end{aligned}$$

**İz Bulma:** Bazların beklenen değerini bulmaktır. Toplam bulunma olasılığını $|0\rangle$ ve $|1\rangle$ için buluyoruz.

$$\begin{aligned}\rho_A &= \langle 0|\psi\rangle\langle\psi|0\rangle + \langle 1|\psi\rangle\langle\psi|1\rangle\\ &= \tfrac{1}{2}[|0\rangle - |1\rangle]\tfrac{1}{2}[\langle 0| - \langle 1|] + \tfrac{1}{2}[-|0\rangle + |1\rangle]\tfrac{1}{2}[-\langle 0| + \langle 1|]\\ &= \tfrac{1}{4}(|0\rangle\langle 0| - |0\rangle\langle 1| - |1\rangle\langle 0| + |1\rangle\langle 1|) + \tfrac{1}{4}(|0\rangle\langle 0| - |0\rangle\langle 1| - |1\rangle\langle 0| + |1\rangle\langle 1|)\\ &= \tfrac{1}{2}(|0\rangle\langle 0| - |0\rangle\langle 1| - |1\rangle\langle 0| + |1\rangle\langle 1|) \rightarrow \text{ 4 tane durum var } 2\times 2 \text{ lik matristir.}\end{aligned}$$

Yukarıdaki ifadenin matris gösterimi aşağıdaki şekilde elde edilir.

$$\rho_A = \frac{1}{2}\begin{pmatrix}\langle 0|\rho_A|0\rangle & \langle 0|\rho_A|1\rangle\\ \langle 1|\rho_A|0\rangle & \langle 1|\rho_A|1\rangle\end{pmatrix}$$

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

Burada bu son bulunan matrisin öz değerleri bulunarak sıfırdan farklı özdeğerlerinin sayısı Schmidt sayısını oluşturacaktır.

$$\begin{aligned}\rho_A|X\rangle &= \lambda|X\rangle\\ (\rho_A|X\rangle - \lambda|X\rangle) &= 0 \Rightarrow (\rho_A - \lambda I)|X\rangle = 0 \quad |0\rangle \neq 0 \text{ olduğundan } \rho_A - \lambda I = 0\\ \rho_A - \lambda I \quad 0 &\Rightarrow \begin{pmatrix}\frac{1}{2} & -\frac{1}{2}\\ -\frac{1}{2} & \frac{1}{2}\end{pmatrix} - \begin{pmatrix}\lambda & 0\\ 0 & \lambda\end{pmatrix} = \begin{pmatrix}\frac{1}{2}-\lambda & -\frac{1}{2}\\ -\frac{1}{2} & \frac{1}{2}-\lambda\end{pmatrix} = 0\\ &\Rightarrow (\tfrac{1}{2}-\lambda)^2 - \tfrac{1}{4} = 0\\ &\Rightarrow \tfrac{1}{4} - \lambda + \lambda^2 - \tfrac{1}{4} = 0\\ &\Rightarrow \lambda^2 - \lambda = 0 \Rightarrow \lambda(\lambda - 1) = 0 \Rightarrow \lambda = 0 \text{ veya } \lambda = 1\end{aligned}$$

Yukarıdan da görüldüğü gibi sistemin 0 dan farklı 1 tane özdeğeri vardır. Bu nedenle Schmidt katsayısı 1 e eşittir ve dolayısıyla sistem dolaşık değildir.

**Ödev:**$|B_{00}\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$ durumunun dolaşık olup olmadığını Schmidt ayrıştırma yöntemiyle bulun.

## 13.1 Dolaşıklık (Fidelity)

Bir qubitlik bir bilginin yoğunluk matrisi fidelity cinsinden

$$\rho = f\,|0\rangle\langle 0| + (1-f)\,|1\rangle\langle 1|$$

şeklinde ifade edilir. Burada $f$, dolaşıklık fidelity'sidir. Örneğin; $\rho = \frac{3}{4}\,|0\rangle\langle 0| + \frac{1}{4}\,|1\rangle\langle 1|$ durumunun dolaşıklık fidelity'si $f = \frac{3}{4}$ dür. $\rho = \frac{1}{4}\,|0\rangle\langle 0| + \frac{3}{4}\,|1\rangle\langle 1|$ sisteminin fidelity'si $f = \frac{1}{4}$ dür. Fidelity dolaşık olma olasılığıdır. Burada $f$'nin başta olmasının sebebi; minumum enerjiyi korumak ister sistem ve temel enerjide kalmak ister.

**Not 40.** Fidelity aslında dolaşıklığın da bir ölçüsüdür. Dolayısıyla bir sistemin fidelity'si ne kadar yüksekse o kadar dolaşık olma durumunda olacaktır. Dolayısıyla yoğunluk matrisini belirlemek demek Bell Durumları, Pauli Gösterimi, Schmidt Ayrıştırma Yöntemindeki gibi sistemlerin dolaşıklığının tespitinde kullanılmaktadır.

# Bölüm 14

# Kuantum Bilgisayarları II

## 14.1 Dolanıklık Takası (Entanglement Swapping)

**Şekil**

Ayşe ile Caner ve Caner ile Burak $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$, $\frac{|00\rangle-|11\rangle}{\sqrt{2}}$, $\frac{|01\rangle+|10\rangle}{\sqrt{2}}$, $\frac{|01\rangle-|10\rangle}{\sqrt{2}}$ Bell durumlarından (Dolanık Durumlar) bir tanesini paylaşsınlar. Böylece A ile Caner ve Caner ile Burak dolanık durumda olmuş olurlar. Aslında bu durum (00, 01, 10, 11 durumlarına) Hadamard ve CNOT kapıları uygulanarak gerçekleştirilebilmektedir. Dolanıklık Takasındaki amaç Ayşe ile Burak arasında dolanıklığı elde etmektir. Bur amaç gerçekleştirilebilmesi için Caner

$$c^1c^2 = \{00, 01, 10, 11\}$$

ölçüm sonuçlarınından bir tanesini kendi qubitlerinde ölçüm yaparak elde eder. Bu durumda Caner, Ayşe ile olan dolanık kısmını Burak'a aktarmış olur. Burak da Caner'in ölçüm sonuçlarına göre değişmiş olan bilgiye kapı uygulayarak Ayşe ile başlangıçta hiç bir dolanıklık olmamasına rağmen dolanıklık takası sayesinde Ayşe ile Burak dolanık hale gelmiş olur. Burada aslında Caner Ayşe ile arasında olan bilginin Ayşe'ye ait kısmını Burak'a teleport etmiş oluyor.

Dolanıklı takasının kuantum devresi ise aşağıdaki şekildedir.

$$\left|\Phi^+\right\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \quad \left|\Phi^-\right\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}} \quad \left|\Phi^+_A\right\rangle = \frac{|0_A0_C\rangle + |1_A1_C\rangle}{\sqrt{2}}$$

**Şekil**

Yukarıdan da görüleceği gibi bu noktalar ses, görüntü, ışık gibi birçok değer olabilmektedir. Faz uzayındaki değerlerin reel uzaydaki karşılıkları ise aşağıdaki şekilde **Ters Fourier**

**Dönüşümü** ile elde edilir.

$$x_j = \underbrace{\frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{-2\Pi i \frac{j.k}{N}}}_{\substack{\text{Ters Fourier Dönüşüm} \\ \text{Operatörü}}} y_k$$

Bunun anlamı ise reel uzaydaki $x_j$ noktalarının faz uzayındaki (üstel uzayı) karşılıkları olan $y_k$ değerlerinin reel uzaydaki karşılıklarının elde edilmesidir. Faz uzayına noktaların taşınması sadece olayın tüm ayrıntılarını incelemek değil aynı zamanda faz uzayında matematiksel işlemler yapmak daha kolaydır. Diğer bir deyişle faz uzayında olayların incelenmesinin kolay olmasının sebebi olayın gerçekleştiği uzaydaki bir tepeden olayın tüm ayrıntılarının gözlenmesine benzemektedir.

**Ödev:**Dolanıklık takasını adım adım 00, 01, 10, 11 ölçümlerine göre gerçekleştirip Burak'ın uygulaması gereken kapıları da açıkça göstererek gerçekleştiriniz.

### 14.1.1 Kuantum Fourier Dönüşümü

Bilindiği gibi klasik uzaydaki noktalar Heisenberg Belirsizlik İlkesinden dolayı ($\Delta x \Delta p \geq \frac{\hbar}{2}, \hbar = \frac{h}{2\pi}$)

- $\Delta x$: konum
- $\Delta P$: momentum
- $h$: planck sabiti

kompleks uzayda (Hilbert uzayında) olasılıksal durumlara yani ket ifadelerine karşılık gelmektedir. Buna göre

$$\underbrace{|0\rangle, |1\rangle, \ldots, |N-1\rangle}_{|j\rangle} \rightarrow |k\rangle$$

qubit durumlarının faz uzayındaki karşılıkları olan $|k\rangle$ ların kuantum Fourier Dönüşüm ile elde edilmesi

$$|k\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{-2\Pi i \frac{j.k}{N}} |j\rangle$$

şeklindedir. Benzer şekilde Faz uzayındaki $|k\rangle$ lardan $|j\rangle$ lerin elde edilmesi ise Ters Kuantum Fourier Dönüşüm ile aşağıdaki şekilde elde edilir.

$$|j\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{-2\Pi i \frac{j.k}{N}} |k\rangle$$

Burada $|k\rangle$ ve $|k\rangle$ ler kuantm bilgisayarlardaki bazlar olan $|0\rangle$ ve $|1\rangle$ cinsinden (binary)(kuantum bilgisayar bazları) qubit ifadeleri denir.

Yukarıdaki Kuantum Fourier Dönüşüm ifadesi aşağıdaki şekilde de matris olarak ifade edilebilir. Örneğin $x_r$ noktalarını Faz uzayındaki $y_k$ noktalarına karşılıklı kuantum Fourier Dönüşümü ile

$$\begin{aligned} y_k = & \frac{1}{\sqrt{N}} \sum_{r=0}^{N-1} e^{-2\Pi i \frac{k.r}{N}} \cdot x_r \\ = & \frac{1}{\sqrt{N}} \left[ e^{-2\Pi i \frac{k.0}{N}} \cdot x_0 + e^{-2\Pi i \frac{k.1}{N}} \cdot x_1 + \cdots + e^{-2\Pi i \frac{k.(n-1)}{N}} \cdot x_{n-1} \right] \end{aligned}$$

$$\begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_{n-1} \end{bmatrix} = \frac{1}{\sqrt{N}} \begin{bmatrix} e^{-2\Pi i \frac{0.0}{N}} & e^{-2\Pi i \frac{0.1}{N}} & \cdots & e^{-2\Pi i \frac{0.(n-1)}{N}} \\ e^{-2\Pi i \frac{1.0}{N}} & e^{-2\Pi i \frac{1.1}{N}} & \cdots & e^{-2\Pi i \frac{1.(n-1)}{N}} \\ \vdots & \vdots & \ddots & \vdots \\ e^{-2\Pi i \frac{(n-1).0}{N}} & e^{-2\Pi i \frac{(n-1).1}{N}} & \cdots & e^{-2\Pi i \frac{(n-1).(n-1)}{N}} \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_{n-1} \end{bmatrix}$$

$$w = e^{\frac{-2\Pi i}{N}},$$

$$\begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_{n-1} \end{bmatrix} = \frac{1}{\sqrt{N}} \begin{bmatrix} w^{00} & w^{01} & \cdots & w^{0(n-1)} \\ w^{10} & w^{11} & \cdots & w^{1(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ w^{(n-1)0} & w^{(n-1)1} & \cdots & w^{(n-1)(n-1)} \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_{n-1} \end{bmatrix}$$

### 14.1.2 İkili (Binary) Gösterim

$j$ tam sayısının ikili (binary) gösterimi aşağıdaki şekildedir.

$$j = j_1 j_2 \cdots j_n = j_1 2^{n-1} + j_2 2^{n-2} + \cdots + j_n 2^0 = \sum_{r=0}^{n-1} 2^r j_{n-r}$$

Yukarıdakine benzer şekilde kesirli ifadelerin ikili (binary) gösterimi

$$0, j_1 j_2 \cdots j_n = j_1 2^{-1} + j_2 2^{-2} + \cdots + j_n 2^{-n} = \sum_{r=0}^{n} j_r 2^{-r}$$

### 14.1.3 Kuantum Bilgisayarlarda Herhangi Bir Keyfi Kuantum Bazının İkili (Binary) Gösterimi

$$|r\rangle = |r_1 r_2 \cdots r_n\rangle = \left|r_1 2^{n-1} + r_2 2^{n-2} + \cdots + r_n 2^0\right\rangle$$

Bu ikili gösterim kullanılarak $|0\rangle$ ve $|1\rangle$ lerden oluşan qubitlerin Kuantum Fourier Dönüşümü aşağıdaki şekildedir.

$$|j_1 j_2 \cdots j_n\rangle \to |k_1 k_2 \cdots k_n\rangle$$

$$|j\rangle = \underbrace{\frac{1}{N}\sum_{k=0}^{N-1} e^{2\Pi i \frac{j.k}{N}}}_{\substack{\text{Kuantum Fourier}\\ \text{Dönüşüm Operatörü}}} |k\rangle\,, \quad N = 2^n$$

$$\begin{aligned}
|j\rangle &= \tfrac{1}{\sqrt{2^n}} \textstyle\sum_{k=0}^{2^n-1} e^{2\Pi i \frac{j.k}{2^n}} |k\rangle \\
&= \tfrac{1}{2^{\frac{n}{2}}} \textstyle\sum_{k=0}^{2^n-1} e^{2\Pi i j \left(\sum_{r=0}^{n-1} \frac{kr}{2^r}\right)} |k\rangle \\
&= \tfrac{1}{2^{\frac{n}{2}}} \textstyle\sum_{k=0}^{2^n-1} \prod_{r=0}^{n-1} e^{2\Pi i j \frac{kr}{2^r}} |k\rangle \\
&= \tfrac{1}{2^{\frac{n}{2}}} \textstyle\sum_{k=0}^{n} \cdots \sum_{k=0}^{1} \prod_{r=0}^{n} e^{2\Pi i j \frac{kr}{2^r}} |k_r\rangle \\
&= \tfrac{1}{2^{\frac{n}{2}}} \textstyle\prod_{r=0}^{n} \sum_{k_r=0}^{1} e^{2\Pi i j \frac{kr}{2^r}} |k_r\rangle \\
&= \tfrac{1}{2^{\frac{n}{2}}} \textstyle\prod_{r=0}^{n} \left(|0\rangle + e^{2\Pi i j \frac{kr}{2^r}} |1\rangle\right) \\
&= \tfrac{1}{2^{\frac{n}{2}}} \left[\left(|0\rangle + e^{2\Pi i j \frac{1}{2}} |1\rangle\right)\left(|0\rangle + e^{2\Pi i j \frac{1}{4}} |1\rangle\right) \ldots \left(|0\rangle + e^{2\Pi i j \frac{1}{2^n}} |1\rangle\right)\right] \\
&= \tfrac{1}{2^{\frac{n}{2}}} \left[\left(|0\rangle + e^{2\Pi i j 0,1} |1\rangle\right)\left(|0\rangle + e^{2\Pi i j 0,01} |1\rangle\right) \ldots \left(|0\rangle + e^{2\Pi i j 0,0\ldots1} |1\rangle\right)\right] \\
&\quad \left[\tfrac{j}{2^n} = 2^n (0, j_1 j_2 \ldots j_n)\right]
\end{aligned}$$

**Açıklama:**

$$\begin{aligned}
\tfrac{j_1 j_2 \ldots j_n}{2^{n-1}} &= \tfrac{2^n (0, j_1 j_2 \ldots j_n)}{2^{n-1}} = j_1 + \tfrac{j_2}{2} + \cdots + \tfrac{j_n}{2^{n-1}} = (j_1 + 0, j_2 \ldots j_n) \\
e^{2\Pi i \frac{j}{2^{n-1}}} &= e^{2\Pi i (j_1 + 0, j_2 \ldots j_n)} = \underbrace{e^{2\Pi i j_1}}_{1} e^{2\Pi i (0, j_2 \ldots j_n)} \\
&= e^{2\Pi i 0, j_2 \ldots j_n}
\end{aligned}$$

$$|j\rangle = \frac{\left(|0\rangle + e^{2\Pi i (0, j_n)} |1\rangle\right) \otimes \left(|0\rangle + e^{2\Pi i (0, j_{n-1} j_n)} |1\rangle\right) \otimes \cdots \otimes \left(|0\rangle + e^{2\Pi i (0, j_1 j_2 \ldots j_n)} |1\rangle\right)}{2^{\frac{n}{2}}}$$

Qubitlerin faz uzaylarındaki karşılıklarını kuantum bilgisayarda elde etmek için Kuantum Fourier Dönüşüm Operatörüne karşılık gelen kuantum kapıları oluşturmak gerekir. Bu da

Hamadamart ve

$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\Pi i}{2^k}} \end{pmatrix} \text{ (Döndürme Kapısı)}$$

kapıları yardımıyla aşağıdaki şekilde elde edilir. Diğre bir değişle Hadamart kapısı yardımıyla bütün qubitler süperpozisyon durumuna getirilir. Yani bütün olası durumları ortaya koymuş olur ve sonra Kontrollü Döndürme Kapıları yardımıyla bütün qubitler faz uzayına taşınmış olur.

Örneğin 3 qubitlik bir durumun Kuantum Fourier Dönüşüm devresi aşağıdaki şekilde ifade edilebilir.

$$|x\rangle = |x_1x_2x_3\rangle = |x_1\rangle \otimes |x_2\rangle \otimes |x_3\rangle$$

**Şekil**

Yukarıdaki devredeki işlemleri yapacak olursak çıktı sonuçlarını aşağıdaki şekilde kolayca elde ederiz.

$$\begin{aligned} H|x_1\rangle &= \tfrac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_1}|1\rangle) \\ &= \tfrac{1}{\sqrt{2}}\textstyle\sum_{y\in\{0,1\}}(-1)^{x,y}|y\rangle \\ &= \tfrac{1}{\sqrt{2}}\textstyle\sum_{y\in\{0,1\}}e^{2\Pi iy(0,x_1)}|y\rangle \\ &= \tfrac{|0\rangle+e^{2\Pi i(0,x_1)}|1\rangle}{\sqrt{2}} \end{aligned}$$

Son durumda kontrollü $R_2$ kapısı uygulanırsa ($x_2$ ile kontrollü)

$$R_2 = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\Pi i}{2^2}} \end{pmatrix}$$

$$R_2\left(\frac{|0\rangle + e^{2\Pi i(0,x_1)}|1\rangle}{\sqrt{2}}\right)\ldots(*)$$

**Açıklama:** $R_2|x_2\rangle$, $|1\rangle$ ise etki edecek $|x_2\rangle$, $|0\rangle$ ise etki etmeyecek.

$$R_2|1\rangle = e^{2\Pi i\frac{x_2}{2^2}}|1\rangle = e^{2\Pi iy(0,0x_2)}|1\rangle$$

Bu ifade $(*)$ da kullanılırsa

$$\frac{(|0\rangle + e^{2\Pi i(0,x_1)}e^{2\Pi i(0,0x_2)}|1\rangle)}{\sqrt{2}} = \frac{|0\rangle + e^{2\Pi i(0,x_1x_2)}|1\rangle}{\sqrt{2}}$$

Son durumda $x_3$ ile kontrollü $R_3$ kapısı uygulanırsa

$$R_3 = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\Pi i}{2^3}} \end{pmatrix}$$

**Açıklama:** $R_3 \left|x_3\right\rangle$; $\left|1\right\rangle$ ise etki eder, $\left|0\right\rangle$ ise etki etmez.

$$R_3 \left|1\right\rangle = e^{2\Pi i \frac{x_3}{2^3}} \left|1\right\rangle = e^{2\Pi i (0,00x_3)} \left|1\right\rangle$$

Bu ifadeyi $R_3 \frac{\left|0\right\rangle + e^{2\Pi i (0,x_1 x_2)} \left|1\right\rangle}{\sqrt{2}}$ ye uygulanırsa

$$= \frac{(\left|0\right\rangle + e^{2\Pi i (0,x_1 x_2)} e^{2\Pi i (0,00x_3)} \left|1\right\rangle)}{\sqrt{2}}$$

$$= \frac{(\left|0\right\rangle + e^{2\Pi i (0,x_1 x_2 x_3)} \left|1\right\rangle)}{\sqrt{2}}$$

**ÖDEV:** $\left|x_2\right\rangle$ ve $\left|x_3\right\rangle$ qubitine Kuantum Fourier Dönüşümünü $\left|x_1\right\rangle$ deki gibi uygulayınız.

Yukarıdaki 3 qubitlik devre aşağıdaki şekilde n qubitlik duruma genelleştirilebilir.

**Şekil**

sonuç sırasıyla yukarıdan aşağı aşağıdaki şekilde çıkar.

$$= \frac{\left|0\right\rangle + e^{2\Pi i (0,x_1 x_2 \ldots x_n)} \left|1\right\rangle}{\sqrt{2}}$$

$$= \frac{\left|0\right\rangle + e^{2\Pi i (0,x_2 x_3 \ldots x_n)} \left|1\right\rangle}{\sqrt{2}}$$

$$= \vdots$$

$$= \frac{\left|0\right\rangle + e^{2\Pi i (0,x_{n-1} x_n)} \left|1\right\rangle}{\sqrt{2}}$$

$$= \frac{\left|0\right\rangle + e^{2\Pi i (0,x_n)} \left|1\right\rangle}{\sqrt{2}}$$

olur.

**Not 41.** Yukarıdaki devreden de görüldüğü gibi ilk qubite bir Hadamard $n-1$ adet $R_k$(faz), 2. qubite 1 Hadamard $n-2$ adet $R_k$(faz), 3. qubite 1 Hadamard $n-3$ adet $R_k$(faz) ve n. qubite 1 Hadamard 0 $R_k$(faz) (hiç uygulanmayacak anlamında) uygulanır. Böylece $n$ adet qubitin faz uzayında 2'li (binary) qubit karşılıkları elde edilmiş olur.

### 14.1.4 Faz Tahmin Algoritması (Ters Kuantum Fourier Dönüşümü)

Bilindiği gibi kuantum bilgisayarlarda kullanılan ölçme dışındaki tüm operatörler birimseldir. $(U^*)^t = U^{-1} \Rightarrow (U^*)^t.U = I \Rightarrow birimsel(unitary)$ Bu nedenle kuantum bilgisayarlarda terslenebilir işlemler gerçekleştirilebilmektedir. Bu bağlamda daha önce kullanılan ikili (binary) işlemlerden yararlanarak 3. qubitlik örnek sonucunda elde edilen sonuçlara Ters Kuantum Fouirer uygulama örneğini aşağıdaki şekilde gerçekleştirilebilir. Dolayısıyla faz tahmininden yararlanılarak faz uzayındaki qubit karşılıklarından Faz Tahmini yardımıyla qubitler elde edilmiş olunur. Bilindiği gibi genel olarak Ters Kuantum Fourier Dönüşümü

$$|x\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{2^n-1} e^{-2\pi i \frac{x.y}{N}} |y\rangle$$

şeklindedir. Buradaki

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{2^n-1} e^{-2\pi i \frac{x.y}{N}}$$

Ters Kuantum Fourier Dönüşüm Operatörünün karşılığı kuantum bilgisayarlar da $R_k^{-n} + H$ operatörleri ile elde edilir. 3. qubit için Ters Kuantum Fourier Dönüşümü (Faz Tahmini) Algoritmasının devresi

**Şekil**

**Açıklama:**

$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^k}} \end{pmatrix}$$

$$R_2 = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^2}} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i(0,01)} \end{pmatrix}$$

$$R_2^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & e^{-2\pi i(0,01)} \end{pmatrix}$$

$|x_1\rangle$ i elde etmek için devreden de görüldüğü gibi ilk önce $R_3^{-1}$ uygulanır. Çıkan sonuca $R_2^{-1}$ uygulanır ve çıkan sonuca da $H$ uygulanarak $|x_1\rangle$ elde edilir.

$\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i(0,x_1x_2x_3)} |1\rangle\right)$ buna $R_3^{-1}$ uygulanacak.

$R_3^{-1} \left[\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i(0,x_1x_2x_3)} |1\rangle\right)\right]$ $R_3^{-1}$ $x_3$ kontrollü olduğu için $x_3$ 1 iken etki eder 0 iken etki etmez.

$$\begin{aligned} \frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i(0,x_1x_2x_3)} R_3^{-1} |1\rangle\right) &= \frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i(0,x_1x_21)} e^{-2\pi i(0,001)} |1\rangle\right) \\ &= \frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i(0,x_1x_2)} |1\rangle\right) \end{aligned}$$

Şimdi bu sonuca $x_2$ kontrollü $R_2^{-1}$ uygulanır. $x_2$ 1 iken etki eder 0 iken etki etmez.

$$\begin{aligned} R_2^{-1}\left[\tfrac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i(0,x_1x_2)}|1\rangle\right)\right] &= \tfrac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i(0,x_1x_2)}R_2^{-1}|1\rangle\right) \\ &= \tfrac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i(0,x_1 1)}e^{-2\pi i(0,01)}|1\rangle\right) \\ &= \tfrac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i(0,x_1)}|1\rangle\right) \end{aligned}$$

Bu sonuca da Hadamard uygulanır.

$$\begin{aligned} H\left[\tfrac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i(0,x_1)}|1\rangle\right)\right] &= \tfrac{1}{\sqrt{2}}\left(H|0\rangle + e^{2\pi i(0,x_1)}H|1\rangle\right) \\ &= \tfrac{1}{\sqrt{2}}\left[\tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) + e^{2\pi i(0,x_1)}\tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right] \\ &= \tfrac{1}{2}\left[(|0\rangle + |1\rangle) + e^{2\pi i(0,x_1)}(|0\rangle - |1\rangle)\right] \\ &= \tfrac{1}{2}\left[|0\rangle + |1\rangle + (-1)^{x_1}(|0\rangle - |1\rangle)\right] \end{aligned}$$

$$\left.\begin{aligned} x_1 = 0 \text{ için sonuç } &= \tfrac{1}{2}\left[|0\rangle + |1\rangle + |0\rangle - |1\rangle\right] = \tfrac{1}{2}2|0\rangle = |0\rangle \\ x_1 = 1 \text{ için sonuç } &= \tfrac{1}{2}\left[|0\rangle + |1\rangle - |0\rangle + |1\rangle\right] = \tfrac{1}{2}2|1\rangle = |1\rangle \end{aligned}\right\} = |x_1\rangle \text{ elde edilir.}$$

**Şekil**

**Not 42.** Kuantum Fourier ve Ters Kuantum Fourier Dönüşümleri cihaz olarak tasarlandığında insanoğlunun bilmedikleri ve görmedikleri hakkında bilgi edinmesine olanaklar sağlanacaktır. Örneğin şu anda kuantum radarlar kullanılarak hayalet uçaklar tespit edilebilmekte, kuantum sensör teknolojisi geliştikçe virüsler ve mikropların görülebilme ve takip edilebilme olanakları ortaya çıkacak. Bunlara ilave olarak tıbbi görüntülemedeki uygulamarı da geliştikçe moleküler ve atomik düzeyde görüntülemeler sayesinde çok çok önceden hastalıklar tespit edilecek ve aynı zamanda beynimizin çalışma prensibi daha ayrıntılı olarak anlaşılabilir düzeye gelecektir.

Yukarıdakilere ilave olarak Kuantum Fourier Dönüşümü kuantum bilgisayarlar alanında özellikle de kuantum kriptolojide çok sık kullanılmaktadır.

**ÖDEV:** Kuantum Fourier Dönüşümü bağlamında qubit gösterimi daha kısa olarak ifade edilip edilemeyeceğini araştırınız.

**ÖDEV:** Kuantum Fourier Dönüşümünü kullanarak $3 + 5 = 8$ olduğunu gösteriniz.

**ÖDEV:** 3 qubitlik Kuantum Fourier Dönüşümü sonucu elde edilen (tensörel çarpımları) duruma Ters Kuantum Fourier Dönüşümü uygulayarak $|x_1\rangle$, $|x_2\rangle$, $|x_3\rangle$ ü elde ediniz.

## 14.2 Deutsch Algoritması

Deutsch Algoritması 1985 yıllarında geliştirilmiş olan ilk kuantum algoritması özelliğini taşımaktadır. Bu algoritmanın ana mantığı fonksiyonların sabit ve ya dengeli olmasının aynı

anda sorgulanmasına dayanmaktadır. Bu da bize kuantum bilgisayarlarda aynı anda 0 ve 1 in tüm olası durumlarının aynı anda değerlendirilmesi durmunu ortaya koymaktadır. Kısaca kuantum bilgisayarlarda aynı anda paralel işlem yapabilmenin olası bir algoritması olduğunu göstermektedir. Deutsch Algoritmasını üstün yapan özelliklerden biri de tek bir girdiden tek bir çıktı elde etmenin tek bir sorguda gerçekleştirilebilmesidir.

**Ek Bilgi:** $x \in 0,1$ olmak üzere öyle fonksiyonlar olabilir ki $x$ üzerine etki edip tek bir çıktı verebilir. Örneğin

**1)** $f(x) = 0,\ f(x) = 1 \Rightarrow f(x)$ sabit fonksiyon

**2)** $f(x) = \begin{cases} 0, & x = 0 \\ 1, & x = 1 \end{cases} \Rightarrow f(x)$ birim fonksiyon

**3)** $f(x) = \begin{cases} 1, & x = 0 \\ 0, & x = 1 \end{cases} \Rightarrow f(x)$ flip fonksiyon

**Not 43.** Birim ve flip fonksiyon her ikisinin özelliğine sahip fonksiyonlara dengeli fonksiyon denir. Çünkü girdilerin yarısı için zır çıktılar verir O nedenle tek bir bitteki fonksiyon ya sabit ya da dengelidir. Deutsch bu ana mantığı kullanarak aşağıdaki birimsel dönüşüm (operatörü) tanımlamıştır ve bu operatörü 2 qubitlik bilgiye etkisi aşağıdaki şekildedir.

$$U_f : U_f \left|xy\right\rangle = \left|x \quad y \oplus f(x)\right\rangle \text{ yani}$$

1. qubit yalnız bırakılıp 2. qubite 1. qubitin argümanı olan fonksiyon eklenir. Burada $x, y \in 0,1$ ve aynı zamanda $|x\rangle$ süperpozisyon durumundadır.

**Not 44.** Bütün algoritmalarda algoritma çalıştırılmadan önce qubitler başlangıç durumuna getirilir. Yani $|0\rangle$ durumuna getirilir. 2. qubit üzerindeki Deutsch Algoritması aşağıdaki şekilde ifade edilir.

**Şekil**

Yukarıdaki devredeki işlemler aşağıdaki şekilde açıkça yazılabilir.

$$\begin{aligned} U_f \left[\tfrac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes |0\rangle\right] &= U_f \left[\tfrac{|00\rangle+|10\rangle}{\sqrt{2}}\right] \\ &= \tfrac{U_f|00\rangle+U_f|10\rangle}{\sqrt{2}} \\ &= \tfrac{|0 \quad 0\oplus f(0)\rangle+|1 \quad 0\oplus f(1)\rangle}{\sqrt{2}} \end{aligned}$$

**Açıklama:**

$$\begin{aligned} 0 \oplus 0 = &\quad 1 \oplus 1 = 0 \\ 0 \oplus 1 = &\quad 1 \oplus 0 = 0 \\ = &\quad \frac{|0 \quad f(0)\rangle + |1 \quad f(1)\rangle}{\sqrt{2}} \end{aligned}$$

Son çıktıdan da görüldüğü gibi $|x\rangle$ in ve f(x) in tüm olası durumları mevcuttur.

$$\frac{1}{\sqrt{2}} U_f |00\rangle + \frac{1}{\sqrt{2}} U_f |10\rangle = \frac{1}{\sqrt{2}} |0 \quad 0 \oplus f(0)\rangle + \frac{1}{\sqrt{2}} |1 \quad 0 \oplus f(1)\rangle$$

Yukarıdan da görüldüğü gibi $U_f$ eş zamanlı olarak süperpozisyon durumundaki 0 ve 1 girdilerini her ikisi içinde $f$ fonksiyonunun değerini hesaplamaktadır. Ölçme işleminden de bilindiği gibi yukarıdaki ifadenin ölçme durumu $\frac{1}{2}$ ihtimalle $|0 \quad 0 \oplus f(0)\rangle$ ve $\frac{1}{2}$ ihtimalle $|1 \quad 0 \oplus f(1)\rangle$ ölçülür. Ölçüm sonucunda da çıktı durumu ya $|f(0)\rangle$ veya $|f(1)\rangle$ olur. Bunun anlamı süperpozisyon durumunda $f(0)$ ve $f(1)$ olur. Bunun anlamı süperposizyon durumunda $f(0)$ ve $f(1)$ aynı anda hesaplanırken ölçüm sonucunda ($|0\rangle$ ve $|1\rangle$ bazlarında) buiki değerden sadece biri elde edilir. Halbuki Deutsch Algoritmasının ana amacı $f(x)$ değerinin sadece birini elde etmek değil $f(0) \oplus f(1)$ in değerlerinin aynı anda belirlenmesidir.

Bu nedenle Deutsch Algoritması aşağıdaki devre ile gerçekleştirilir.

**Şekil**

Deutsch Algoritması bu şekildedir.

$$\begin{aligned} |\psi_0\rangle = &\quad |0\rangle \otimes \tfrac{|0\rangle - |1\rangle}{\sqrt{2}} = \tfrac{1}{\sqrt{2}}(|00\rangle + |01\rangle) \\ |\psi_1\rangle = &\quad H|\psi_0\rangle = H|0\rangle \otimes \left(\tfrac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \\ = &\quad \tfrac{1}{\sqrt{2}}|0\rangle \left(\tfrac{|0\rangle - |1\rangle}{\sqrt{2}}\right) + \tfrac{1}{\sqrt{2}}|1\rangle \left(\tfrac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \\ |\psi_2\rangle = &\quad U_f |\psi_1\rangle \end{aligned}$$

**Açıklama:** $U_f$ nin $|x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$ ye etkisini inceleyelim.

$$\begin{aligned} U_f \left[|x\rangle \left(\tfrac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\right] = &\quad \tfrac{U_f|x\rangle|0\rangle - U_f|x\rangle|1\rangle}{\sqrt{2}} \\ = &\quad \tfrac{|x\rangle|0 \oplus f(x)\rangle - |x\rangle|1 \oplus f(x)\rangle}{\sqrt{2}} \\ = &\quad |x\rangle \left[\tfrac{|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle}{\sqrt{2}}\right] \end{aligned}$$

Son ifade de $f(x)=0$ ve $f(x)=1$ durumlarında

$$\left[\frac{|0\oplus f(x)\rangle - |1\oplus f(x)\rangle}{\sqrt{2}}\right]$$

ifadesini göz önüne alalım.

$$\begin{aligned} f(x)=0 \Rightarrow & \ \tfrac{|0\rangle-|1\rangle}{\sqrt{2}} \\ f(x)=1 \Rightarrow & \ \tfrac{|1\rangle-|0\rangle}{\sqrt{2}} = -\left(\tfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \end{aligned}$$

Bu sonuçlardan da görüldüğü gibi elde edilecek 2 olasılık (-1) çarpanı kadar farklıdır. Buna göre

$$\underbrace{\frac{|0\oplus f(x)\rangle - |1\oplus f(x)\rangle}{\sqrt{2}}}_{U_f \text{ nin etki sonucu}} = (-1)^{f(x)}\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

Buna göre $U_f$ nin $|x\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$ ye etkisi $(-1)^{f(x)}\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$ şeklinde yazılabilir.

Yukarıdaki mantık Deutsch Algoritmasına uygulanırsa

$$\begin{aligned} |\psi_2\rangle = & \ U_f|\psi_1\rangle \\ = & \ U_f\left[\tfrac{1}{\sqrt{2}}|0\rangle\left(\tfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right)+\tfrac{1}{\sqrt{2}}|1\rangle\left(\tfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\right] \\ = & \ \tfrac{1}{\sqrt{2}}U_f|0\rangle\left(\tfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right)+\tfrac{1}{\sqrt{2}}U_f|1\rangle\left(\tfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \\ = & \ \tfrac{1}{\sqrt{2}}(-1)^{f(0)}|0\rangle\left(\tfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right)+\tfrac{1}{\sqrt{2}}(-1)^{f(1)}|1\rangle\left(\tfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \\ = & \ \left[\tfrac{(-1)^{f(0)}|0\rangle+(-1)^{f(1)}|1\rangle}{\sqrt{2}}\right]\left(\tfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \quad (-1)^{f(0)}(-1)^{f(1)}=(-1)^{f(0)\oplus f(1)} \\ = & \ (-1)^{f(0)}\left(\tfrac{|0\rangle+(-1)^{f(0)\oplus f(1)}|1\rangle}{\sqrt{2}}\right)\left(\tfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \end{aligned}$$

Son ifade de $f$ fonksiyonu sabit ise

$$\begin{aligned} f(0)\oplus f(1)=0 \Rightarrow |\psi_2\rangle = & \ (-1)^{f(0)}\left(\tfrac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\left(\tfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \\ |\psi_3\rangle = & \ H|\psi_2\rangle = (-1)^{f(0)}H\left(\tfrac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\left(\tfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \\ = & \ (-1)^{f(0)}|0\rangle\left(\tfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \end{aligned}$$

Yukarıdan da görüldüğü gibi $|0\rangle$ durumunun normunun karesi yani $\left((-1)^{f(0)}\right)^2 = 1$ dir. Bunun anlamı sabit bir fonksiyon için $f(0)\oplus f(1)=0$ olması kesindir.

Eğer $f$ dengeli ise yani $f(0) \oplus f(1) = 1$ ise

$$\begin{aligned} |\psi_2\rangle &= (-1)^{f(0)} \left(\tfrac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \left(\tfrac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \\ |\psi_3\rangle &= H|\psi_2\rangle = (-1)^{f(0)} H \left(\tfrac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \left(\tfrac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \\ &= (-1)^{f(1)} |0\rangle \left(\tfrac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \end{aligned}$$

Yukarıdan da görüldüğü gibi ilk qubit olan $|1\rangle$ durumunun normunun karesi $\left((-1)^{f(0)}\right)^2 = 1$ dir. Bunun anlamı dengeli bir fonksiyon için ilk qubit ölçümünün $f(0) \oplus f(1) = 1$ olması kesindir.

**Not 45.** Sonuç olarak Deutsch Algoritmasının sonunda $f(0) \oplus f(1)$ değerini dolayısıyla fonksiyonun dengeli ya da sabit olduğu belirlenir. Diğer bir değişle fonksiyonun dengeli ya da sabit olduğu aynı anda sağlanarak tek bir çıktı değeri elde edilmiş olur. Bu aslında kuantum bilgisayarlarda aynı ayna paralel işlem yapabilme durumunu diğer bir değişle kuantum bilgisayarların çok daha hızlı çalışabildiğini de göstermektedir. Kuantumsal olarak bakıldığında $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$ durumu $U_f$ operatörünün $(-1)^{f(x)}$ özdeğerli öz durumudur.

Fonksiyona sorgulama yaparak ölçüm sonucu elde edilir. Dengeli ise $|1\rangle$, sabitse $|0\rangle$ dır.

Deutsch Algoritmasından da görülebileceği gibi fonksiyona aynı anda dendeli ya da sabit olup olmadığı sorgusu yapılarak $|0\rangle$ ve $|1\rangle$ ölçüm sonuçları elde edilebilmektedir. Eğer fonksiyon dengeli ise ölçüm sonucu kesinlikle $|1\rangle$ dir. Eğer fonksiyon sabit ise ölçüm sonucu kesinlikle $|0\rangle$ dır.

## 14.3 Deutsch-Jozsa Algoritması

Bu algoritma Deutsch algoritmasının $n$ girdili haline genelleştirilmiştir. Deutsch-jozsa algoritmasının ana mantığı $n$ girdi için çıktı elde edilmesinde fonksiyonun sabit veya dengeli olup olmamasına dayanmaktadır. Deutsch-jazsa algoritmasının devresi aşağıdaki şekildedir.

**Şekil**

$$U_f : U_f |x\rangle |y\rangle \to |x\rangle |y \oplus f(x)\rangle = (-1)^{f(x)} |x\rangle |y\rangle$$

Bu algoritmanın işleyiş adımları ise aşağıdaki şekildedir:

**1)** Girdi qubitlerinin hepsi başlangıç durumuna getirilir. Yani ilk $n$ qubit $|0\rangle$ ve en son olan qubit $|1\rangle$ durumlarına getirilir.

**2)** Her bir qubite $H$ uygulanır. $H^{\otimes n} |0\rangle^{\otimes n}$ ve $H|1\rangle$

**3)** Register a (girdiler) $U_f$ uygulanır.

**4)** İlk $n$ qubite $H$ uygulanır.

**5)** İlk $n$ qubitteki z değeri ölçülür(okunur).

**6)** Eğer ilk $n$ qubitteki $z = 0^n$ ise $f$ sabit. Yani $f(x)$ fonksiyonu sabit ise ilk $n$ qubitin ölçüm sonucu kesinlikle 0 dır. Diğer durumlarda fonksiyon dengelidir. Diğer bir deyişle fonksiyon dengeli ise ilk $n$ qubitteki ölçüm sonuçlarından en az biri 0 dan farklıdır. demektir.

**Not 46.** Deutsch-jozsa algoritmasında fonksiyon sabit veya dengeli olması aynı anda sorgulanmaktadır. Buna kara kutu sorgulaması denmektedir. Deutsch-jozsa algoritması kuantum bilgisayarlarda aynı anda birçok işlemin yapılabildiği yani paralel işlem yapılabildiğini göstermekle birlikle kuantum kriptografide, kuantum saldırılar içinde ve kuantum kara kutu sorgulamarı içinde kullanılmaktadır.

Burada $U_f : U_f |x\rangle |y\rangle \to |x\rangle |y \oplus f(x)\rangle$ ifadesinden de görüleceği gibi kontrollü ikili işlem yapılabilmesi için son qubit $|1\rangle$ olarak eklenmiştir.

Yukarıdaki devrenin ve aynı zamanda Deutsch-jozsa algoritmasının adımları aşağıdaki şekilde açıkca gösterilmiştir.

$$\begin{aligned}
|\psi_0\rangle &= |0\rangle^{\otimes n} \left(\tfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \\
H^{\otimes n}|0\rangle^{\otimes n} &= \left(\tfrac{1}{\sqrt{2}}\right)^n \underbrace{(|0\rangle+|1\rangle)\otimes(|0\rangle+|1\rangle)\otimes\ldots\otimes(|0\rangle+|1\rangle)}_{n \text{ tane}} \\
&= \tfrac{1}{\sqrt{2^n}} \textstyle\sum_{x\in\{0,1\}^n} |x\rangle \\
|\psi_1\rangle &= \tfrac{1}{\sqrt{2^n}} \textstyle\sum_{x\in\{0,1\}^n} |x\rangle \otimes \left(\tfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \\
|\psi_2\rangle &= U_f|\psi_1\rangle = U_f\left[\tfrac{1}{\sqrt{2^n}} \textstyle\sum_{x\in\{0,1\}^n} |x\rangle \otimes \left(\tfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\right] = \tfrac{1}{\sqrt{2^n}} \textstyle\sum_{x\in\{0,1\}^n} (-1)^{f(x)}|x\rangle \left(\tfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right)
\end{aligned}$$

Buradan da görüldüğü gibi $(-1)^{f(x)}$ faz kaymasıyla ilk qubit ilişkilendirilmiş oldu.

**Açıklama:** Hadamardın $|x\rangle$ e etkisi

$$H|x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x|1\rangle) = \frac{1}{\sqrt{2}} \sum_{x\in\{0,1\}} (-1)^{x.z}|z\rangle$$

Tek $H$ için olan bu durum $n$ $H$ lı duruma aşağıdaki şekilde genelleştirilir.

$$\begin{aligned}
H^{\otimes n}|0\rangle &= H^{\otimes n}(|x_1\rangle\otimes|x_2\rangle\otimes\ldots\otimes|x_n\rangle) \\
&= H|x_1\rangle\otimes H|x_2\rangle\otimes\ldots\otimes H|x_n\rangle \\
&= \tfrac{1}{\sqrt{2}}(|0\rangle+(-1)^{x_1}|1\rangle)\otimes\tfrac{1}{\sqrt{2}}(|0\rangle+(-1)^{x_2}|1\rangle)\otimes\ldots\otimes\tfrac{1}{\sqrt{2}}(|0\rangle+(-1)^{x_n}|1\rangle) \\
&= \tfrac{1}{\sqrt{2}}(|0\rangle+(-1)^{x_1z_1}|1\rangle)\otimes\tfrac{1}{\sqrt{2}}(|0\rangle+(-1)^{x_2z_2}|1\rangle)\otimes\ldots\otimes\tfrac{1}{\sqrt{2}}(|0\rangle+(-1)^{x_nz_n}|1\rangle) \\
H^{\otimes n}|0\rangle &= \tfrac{1}{\sqrt{2^n}} \textstyle\sum_{x_i\in\{0,1\}^n} (-1)^{x_1z_1+x_2z_2+\ldots+x_nz_n}|z_1\rangle|z_2\rangle\ldots|z_n\rangle \\
H^{\otimes n}|0\rangle &= \tfrac{1}{\sqrt{2^n}} \textstyle\sum_{x\in\{0,1\}^n} (-1)^{xz}|z\rangle
\end{aligned}$$

Yukarıdaki açıklamalardaki $n$ tane H ın uygulanmasındaki son eşitlik aşağıda kullanılacak olursa

$$\begin{aligned}|\psi_3\rangle = \; & H^{\otimes n}|\psi_2\rangle = \left(\tfrac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}(-1)^{xz}\underbrace{H^{\otimes n}|x\rangle}\right)\otimes\left(\tfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\\ = \; & \left(\tfrac{1}{\sqrt{2^n}}\sum_{x_i\in\{0,1\}^n}(-1)^{f(x)}\tfrac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}(-1)^{xz}|z\rangle\right)\otimes\left(\tfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\\ = \; & \tfrac{1}{2^n}\sum_{x\in\{0,1\}^n}\left(\sum_{x\in\{0,1\}^n}(-1)^{f(x)+xz}|z\rangle\right)\left(\tfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\end{aligned}$$

Bu son durumda $ket0$ ve $|1\rangle$ bazlarında ölçüm yapılır. Bu ölçüm sonucunu açıkça görmek için $|\psi_3\rangle$ durumunun ilk yazmacındaki yani

$$|z\rangle = |0\rangle^{\otimes n}$$

nin toplam genliğini göz önüne alalım. Bu genlikte

$$\frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{f(x)}$$

dir.

Yukarıdakine göre $f$ sabit ise $|z\rangle = |0\rangle^{\otimes n}$ genliği ya $+1$ dir ya da -1 dir. Dolayısıyla tüm ölçüm sonuçları yani n tane $|0\rangle$ ölçülecektir. Eğer $f$ dengeli ise $|z\rangle = |0\rangle^{\otimes n}$ katsayılarının yarısı pozitif yarısı da negatif genlikte olacaktır. Bunlar da birbirini yok eder. Dolayısıyla toplam genlik 0 dır ve sonuç olarak ilk yazmacın hepsinin 0 olması imkansızdır. En az bir tanesi 1 dir.

**Not 47.** Bütün bu işlemler aynı anda gerçekleştirilmektedir.

## 14.4 Shor Algoritması (Asal Çarpanlara Ayırma Algoritması)

**Hatırlatma:** (Çarpanlara Ayırma Problemi)

Asal çarpanlara ayırma problemi çok büyük n tamsayısının asal çarpanlarının bulunmasıdır. Bu da $p$ ve $q$ bilinmeyen 2 asal çarpan olmak üzere $n = p.q$ şeklinde ifade edilir. Burada amaç $p$ ve $q$ bilinmeyen 2 asal çarpanı bulmaktır. Bu sayılar $\mod n$ e göre tam syılardır. Bunun nedeni temel matematik bilgisine göre $R = \{0, 1, 2, \ldots, n-1\}$ kümesinde toplama ve çarpma $\mod n$ e göre kapalıdır. Yani $a, b \in R$ olmak üzere $(a+b) \mod n \in R$ dir. $(a.b) \mod n \in R$ dir. Buna göre $x \geq 0$ ve $a \in R$ olmak üzere $a^* \mod n \in R$ dir.

**Örnek 56.** $a^{183} \mod n$ i bulmak için

$$(183)_{10} = (10110111)_2)$$

Buna göre

$$a^{183} = a^{128}.a^{32}.a^{16}.a^4.a^2.a^1$$

Örneğin $a = 3$ ve $n = 7$ olsun.

$$\begin{aligned} a^2 \mod n &= 9 \mod 7 = 2 \\ a^4 \mod n &= 81 \mod 7 = 4 \end{aligned}$$

Yukarıdan görüldüğü gibi her şeferinde kare uygun şekilde alınacak mod n e göre bulunur. Böylece $a^{183} \mod n$ kolaylıkla hesaplanmış olur.

### 14.4.1 Çarpanlara Ayırma Probleminin İndirgemesi

$n = p.q$ şeklinde asal çarpanlara ayırma problemi $1 < a < n$ için $a \mod n$ nin derecesini (order) bulmaya yani

$$a^r \mod n = 1$$

olan en küçük $r \geq 1$ problemine indirgenebilir. Yani $r$ derecesini bulma problemine indirgenmiş olur. Burda $1, a, a^2, a^3, \ldots \mod n$ listesine bakıldığında periyotuyla $(p < n)$ tekrar ettiği görüşür. $p$. periyidu da $a \mod n$ nin derecesidir. Çünkü $a^k \mod n = a^j \mod n$ dir. $a^{k-j} = 1$ olur. Bunun anlamı p ve q dan birisinin bulunması demektir. Yani öklid algoritmasıyla $gcd(a, n) = OBEB(a, n)$ bulunarak q ve q dan birisi bulunmuş olur.

**Not 48.** Shor çok büyük asal sayılarının çarpanlarını bulma problemini faz uzayında (verilerin kuantum fourier dönüşümü ile taşındığı uzay) periyot bulma problemine dönüştürerek asal çarpanlrı kuantum bilgisayarların aynı anda bir çok işlem yapabilme özelliğini de kullanarak çok kısa sürede bulmayı gerçekleştirmiştir. Bu işlem faz uzayında yapılırken periyot bulma işlemini de faz uzayında öz değer bulma problemine indirgeyerek üstel bir hız kazandırmıştır. Bu algoritmayla kırılması çok uzun yıllar alan şifreler çok kısa sürede kırılabilmektedir.

Yukarıdaki bilgiler ışığında shor alogitması aşağıdaki şekilde çalışır. Shor algoritmasında $n = p.q$ tamsayısı için

$$2n^2 < q < 3n^3$$

olacak şekilde q çarpanı seçilir. Burada $q = 2^1$, $q^2 = q^{1p}$, $q^3 = q^{3p}$, $\ldots$, $q^n = q^{np}$ durumları

göz önüne alınır. Bu durum qubit durumunda aşağıdaki şekilde olur.

$$|xy\rangle = |x\rangle\,|y\rangle$$

durumunda x ve y ler 1 uzunluklu ikili durumlardır. (0 ve 1 lerden oluşuyor) Buna göre sistemin (qubit sisteminin herhangi bir zamandaki durumu)

$$|\psi\rangle = \sum_{x=0}^{q-1}\sum_{y=0}^{q-1} c_{xy}\,|x\rangle\,|y\rangle$$

şekilde olur. Burada

$$\sum_{x,y} |c_{xy}|^2 = 1$$

olur. Bu bilgiler ışığında Shor Algoritması adım adım aşağıdaki şekilde ifade edilir.

**1. Adım** Diğer algoritmalarda olduğu gibi qubitler temel duruma (başlangıç durumuna) getirilir. Sonra ilk yazmaçtaki (register) her qubite H uygulanır. Yani

$$|\psi_2\rangle = H\,|\psi\rangle = \frac{1}{\sqrt{q}}\sum_{x=0}^{q-1}|x\rangle\,|0\rangle$$

**Örnek 57.** $q = 2^2 \Rightarrow l = 2$ yani $|x\rangle$ ve $|y\rangle$ ler 2 uzunluğunda ikililerden oluşmaktadır.

$$H\,|\psi\rangle = \frac{1}{\sqrt{4}}\sum_{x=0}^{3}|x\rangle\,|0\rangle = \frac{1}{2}\left\{\left|\underbrace{00}_{0},00\right\rangle + \left|\underbrace{01}_{1},00\right\rangle + \left|\underbrace{10}_{2},00\right\rangle + \left|\underbrace{11}_{3},00\right\rangle\right\}$$

0,1,2,3 binary döndürdük. virgül koymaya gerek yok.

**2. Adım** 1 ile n arasında bir x sayısı seçilir. Bu işlem $|\psi_2\rangle$ durumuna 4 birimsel dönüşümü uygulanarak aşağıdaki şekilde elde edilir.

$$|x,0\rangle = |x\rangle\,|0\rangle \longrightarrow |x,a^x \mod n\rangle = |x\rangle\,|a^x \mod n\rangle$$

Yani

$$U\,|\psi_2\rangle = U\left(\frac{1}{\sqrt{q}}\sum_{x=0}^{q-1}|x\rangle\,|0\rangle\right) = \frac{1}{\sqrt{q}}\sum_{x=0}^{q-1}|x\rangle\,|a^x \mod n\rangle = |\psi_3\rangle$$

**3. Adım** Sadece 2. yazmaçta ölçüm yapılır. ($a^x \mod n$) Ölçüm sonucunda 2. yazmacın

durumu $|k\rangle$ olur. Bunun anlamı $|k\rangle$ $a \mod n$ in bir kuvvetidir. Burada k belirlenmiştir fakat x belirlenmemiştir.

Ölçüm sonucunda yeni durum

$$|\psi_4\rangle = \frac{1}{\sqrt{m}} \sum_{x \in X} |x, k\rangle$$

olur. Burada x kümesi $a^x \mod n = k$ olan tüm $x < q$ lardan oluşan kümedir. m ise eleman sayısıdır. Dolayısıyla $X$ kümesi

$$X = \{x_a, x_a + r, x_a + 2r, \ldots, x_a + (m-1)r\}$$

$$c = \text{derece} = \text{periyot}$$

Bu bilgiler $|\psi_4\rangle$ te kullanılırsa

$$|\psi_4\rangle = \frac{1}{\sqrt{m}} \sum_{d=0}^{m-1} |x_a + dr, k\rangle$$

**4. Adım** Son durumdaki ilk yazmaca $U_{f=q}$ Ayrık Fourier Döşümü uygulanır.

$$|\psi_5\rangle = \; U_q(|\psi_5\rangle) = \tfrac{1}{\sqrt{qm}} \textstyle\sum_{c=0}^{q-1} \sum_{d=0}^{m-1} U_q |x_a + dr, k\rangle \, |k\rangle$$

$$|\psi_5\rangle = \; \tfrac{1}{\sqrt{qm}} \textstyle\sum_{c=0}^{q-1} \sum_{d=0}^{m-1} e^{2\pi i c\left(\frac{x_a + dr}{q}\right)} |c\rangle \, |k\rangle$$

$$|\psi_5\rangle = \; \tfrac{1}{\sqrt{qm}} \textstyle\sum_{c=0}^{q-1} e^{2\pi i c\left(\frac{x_a}{q}\right)} \left( \sum_{d=0}^{m-1} e^{2\pi i c\left(\frac{dr}{q}\right)} \right) |c\rangle \, |k\rangle \qquad \alpha = e^{2\pi i c\left(\frac{r}{q}\right)}$$

$$|\psi_5\rangle = \; \tfrac{1}{\sqrt{qm}} \textstyle\sum_{c=0}^{q-1} e^{2\pi i c\left(\frac{x_a}{q}\right)} \left( \sum_{d=0}^{m-1} \alpha^d \right) |c\rangle \, |k\rangle$$

**5. Adım** Birinci yazmaçta ($|c\rangle$) öçüm yapılır. $|\psi_5\rangle$ ifadesinde de görülebileceği gibi ölçüm olasılığı

$$\Pr(c) = \left| \sum_{c=0}^{q-1} \frac{e^{2\pi i c\left(\frac{x_a}{q}\right)}}{\sqrt{qm}} . \sum_{d=0}^{m-1} \alpha^d \right|^2$$

**6. Adım** Sürekli kesirlerin yakınsaması sonucu $r_1, 2r_1, 3r_1, \ldots$ den r periyodu veya tekrar sayısı elde edilir ve

$$\left.\begin{array}{rl} \text{ç}_1 = & a^{\frac{r}{2}} + 1 \\ \text{ç}_2 = & a^{\frac{r}{2}} - 1 \end{array}\right\} \text{ den de 2 asal çarpan bulunmuş olur.}$$

**Açıklama: (Sürekli kesirlerin yakınsaması)**

Bilindiği gibi $2n^2 < q < 3n^2$ den $q$ tespit ediliyordu 5. adım sonunda da $c$ bulunduğuna göre buradan da $\frac{c}{a}$ yakınsaması bulunur.

## 14.5 Grover Arama Algoritması

Bu algoritma veritabanından düzensiz verilerin aranmasında kuantum bilgisayarların üstün özelliklerini kullanarak arama gerçekleştiren bir algoritmadır. Bu algoritmanın ana mantığı verileri aranan ve aranmayan şekilde 2 kısımda ayrılması ve arama işlemi esnasında aranan bulunurken arananın genliği arttırılır ve aynı zamanda aranmayanların genlikleri düşürülmesine dayanmaktadır. Bunun sebebi ise olasılık teoreisine göre qubitlerin önündeki genliklerin kareleri toplamının 1 olmasındandır. Yani 1 qubitlik bilgide

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \quad \alpha^2 + \beta^2 = 1 \Rightarrow \alpha^2 = 1 - \beta^2$$

olduğu gibi $\alpha^2$ nin artması demek $\beta^2$ nin azalması demektir. Bu nedenle Grover algoritması klasik algoritmalara göre daha hızlı arama yapan bir algoritmadır. Klasik bir algoritmada arama işlemi $2^n - 1$ işlem gerektirirken Grover algoritmasında arama işlemi $\sqrt{2^n}$ işlem gerektirmektedir.

Örneğin, 5 bitlik bir veri içerisinden aradığımızı bulmak için günümüz bilgisayarlarda $2^5 - 1 = 31$ adım gerekirken kuantum bilgisayarlarda Grover algoritması kullanıldığında $\sqrt{2^5} \cong 6$ adım gerekmektedir.

Yukarıdan da görüldüğü gibi veri sayısı arttığında Grover algoritmasının üstünşüğü kolayca görülmektedir.

Bu algoritmanın işleyişi aşağıdaki şekildedir:

Diğer tüm algoritmalarda olduğu gibi Grover algoritmasında da qubitler başlangıç durumuna ($|0\rangle$) getirilir. Daha sonra n tane $|0\rangle$ durumu süperpozisyon durumuna getirmek için $H$ kapısı uygulanır. Diğer bir deyişle

$$|\psi\rangle = |0\rangle^{\otimes n}$$

$$|\psi\rangle = H^{\otimes n}\,|\psi_1\rangle = H^{\otimes n}\,|0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle \tag{14.1}$$

Bu durum aranan ($|x'\rangle$) ve aranmayanlar ($|x\rangle$) şeklinde 2 gruba ayrılırsa ve aranan durumundan çıkarılırsa

$$|\psi'\rangle = \frac{1}{\sqrt{2^n - 1}} \sum_{\substack{x\in\{0,1\}^{n-1} \\ x\neq x'}} |x\rangle \tag{14.2}$$

Grover yukarıdaki durumlara uygulanacak aşağıdaki şekilde 2 operatör tanımlamıştır.

## 1. Operatör:

$$U_f : U_f |x\rangle = \sum_{x\in\{0,1\}^n} (-1)^{f(x)} |x\rangle = \sum_{x\in\{0,1\}^n} (-1)^{\delta x,x'} |x\rangle$$

Burada

$$\text{Kronecker Deltası} = \delta x, x' = \begin{cases} 1, & x = x' \\ 0, & x \neq x' \end{cases}$$

## 2. Operatör:

$$w = 2 |\psi\rangle\langle\psi| - I$$

Yukarıdaki 2 operatörün birleşimi olan

$$G = WU_f$$

operatörüne Grover tekrarlama operatörü denir. Bu operatörün (G) yaptığı esas işlem arananın genliğini yükseltirken aranmayanların genliğini düşürmektir. Yukarıdaki operatörlerin tanımlarından da görüleceği gibi $U_f$, arananın fazını aranmayana göre değiştirmektedir. W ise bu fazların genliklerini yükseltmektedir. 14.1 denkleminden de görüleceği gibi (aranan ve aranmayanların birlikte olduğu) aranan ve aranmayanların genlikleri eşit olup $(\frac{1}{\sqrt{2^n}})^2$ şeklindedir. Buna göre 14.1 denklemi aranmayanlar 14.2 denklemi de göz önüne alınarak tekrar düzenlenirse

$$|\psi\rangle = \underbrace{\sqrt{\frac{2^n-1}{2^n}} |\psi'\rangle}_{\text{aranmayanlar}} + \underbrace{\frac{1}{2^n} |x'\rangle}_{\text{aranan}} \tag{14.3}$$

$$|x'\rangle = \sqrt{2^n} |\psi\rangle - \sqrt{2^n - 1} |\psi'\rangle \tag{14.4}$$

Yukarıdaki duruma 14.4 denklemine $W$ uygulanırsa

$$\begin{aligned} W |x'\rangle = & \left(2 |\psi\rangle\langle\psi| - I\right) \left(\sqrt{2^n} |\psi\rangle - \sqrt{2^n - 1} |\psi'\rangle\right) \\ = & \; 2\sqrt{2^n} |\psi\rangle \langle\psi|\psi\rangle - 2\sqrt{2^n - 1} |\psi\rangle \langle\psi|\psi'\rangle - \sqrt{2^n} |\psi\rangle + \sqrt{2^n - 1} |\psi'\rangle \end{aligned}$$

$|\psi\rangle$ ve $|\psi'\rangle$ ortonormal olduklarından

$$\begin{aligned}\langle\psi|\psi\rangle &= \langle\psi'|\psi'\rangle = 1\\ \langle\psi'|\psi\rangle &= \langle\psi|\psi'\rangle = 0\\ &= 2\sqrt{2^n}\,|\psi\rangle - \sqrt{2^n}\,|\psi\rangle + \sqrt{2^n-1}\,|\psi'\rangle\end{aligned}$$

$$= \sqrt{2^n}\,|\psi\rangle + \sqrt{2^n-1}\,|\psi'\rangle \tag{14.5}$$

14.5 denklemine benzer olarak $W$ nın $|\psi'\rangle$ üstüne etkisi

$$W|\psi'\rangle = \frac{2\sqrt{2^n-1}}{2^n}|\psi'\rangle + \underbrace{\left(\frac{2}{2^n}-1\right)}_{\cos\theta}|x'\rangle \tag{14.6}$$

veya

$$W|\psi'\rangle = -\left(\frac{2}{2^n}-1\right)|\psi'\rangle + \frac{2\sqrt{2^n-1}}{2^n}|x'\rangle \tag{14.7}$$

**Ödev:** Yukarıdaki eşitlikleri elde ediniz. (6 yı elde et)

$$\frac{2\sqrt{2^n-1}}{2^n} = \sin\theta \text{ dersek } \cos\theta = \frac{\sqrt{2^n-1}}{2^n} \tag{14.8}$$

14.8 denklemi 14.6 ve 14.7 de kullanılırsa

$$W|\psi'\rangle = \sin\theta\,|\psi'\rangle + \cos\theta\,|x'\rangle \tag{14.9}$$

veya

$$W|\psi'\rangle = -\cos\theta\,|\psi'\rangle + \sin\theta\,|x'\rangle \tag{14.10}$$

14.9 ve 14.10 ifadelerine bakıldığında birbirlerinin döndürülmüş hali olduğu görülmektedir. Dolayısıyla $G$ operatörünün $G = WU_f$ $|x'\rangle$ ve $|\psi'\rangle$ e uygulandığında

$$G|x'\rangle = \cos\theta\,|x'\rangle - \sin\theta\,|\psi'\rangle \tag{14.11}$$

$$G|\psi'\rangle = \sin\theta\,|x'\rangle + \cos\theta\,|\psi'\rangle \tag{14.12}$$

elde edilmiş olur. Bu operatörün $|\psi'\rangle$ durumlarını $|x'\rangle$ yani aradığımız duruma döndürdüğü kolayca görülmektedir. Bu işlem m kez tekrarlanırsa 14.11 ve 14.12 denklemi

$$G^m|x'\rangle = \cos m\theta\,|x'\rangle - \sin m\theta\,|\psi'\rangle \tag{14.13}$$

$$G^m|\psi'\rangle = \sin m\theta\,|x'\rangle + \cos m\theta\,|\psi'\rangle \tag{14.14}$$

14.13 ve 14.14 denkleminden görüldüğü gibi $m\theta = \frac{\pi}{2}$ olursa özellikle 14.14 denklemine bakıla-

cak olursa $|\psi'\rangle = |x'\rangle$ olduğu görülür. Diğer bir deyişle Grover operatörü $|\psi'\rangle$ leri aradığımız $|x'\rangle$ ne dönüştürdüğü görülür.

Yukarıdaki özellik küçük açı durumunda değerlendirilirse yani $\frac{2\sqrt{2^n-1}}{2^n} = \sin\theta$ küçük açı yaklaşımında $\frac{2\sqrt{2^n-1}}{2^n} \cong \theta$ olur.

$$m\theta = \frac{\pi}{2} \Rightarrow m = \frac{\pi}{4}\sqrt{2^n} \quad \frac{2\sqrt{2^n-1}}{2^n} \cong \theta$$

Yukarıdan da görüldüğü gibi $|x'\rangle$ nün yani aradığımızı bulmak için $\frac{\pi}{4}\sqrt{2^n}$ adım gerekmektedir. Diğer bir değişle aradığımızı bulmak için $(|x'\rangle)$ $\frac{\pi}{4}\sqrt{2^n}$ kez Grover operatörünü $\left(WU_f = (2\,|\psi\rangle\langle\psi| - I)\sum_{x\in\{0,1\}}(-1)^{\delta x,x'}\,|x\rangle\right)$ uygulamamız gerekir. Aslında yukarıdaki işlemler aradığımızı bulduğumuzda $f(x) = 1$ olması yani başarı durumu. Aradığımızı bulmadığımızda da $f(x) = 0$ yani başarısızlık durumlarının aynı anda elde edilmesidir. Yukarıdaki işlemlerin gerçekleştirilmesinin devresi ise

**Şekil**

**Örnek 58.** 0' dan 20' ye kadar olan bir sayı dizisinden 3 değerini Grover arama algoritması ile bulunuz.

$$\begin{aligned} 3 &\to 2^3 = 8 \Rightarrow n = 3 \text{ qubit ile } 0-7 \text{ arasındakileri gösterebiliriz.} \\ 3 &\to |011\rangle \Rightarrow \underbrace{f(x)}_{|011\rangle} = 1 \text{ diğer durumlarda } f(x) = 0 \Leftarrow 0 : (-1)^{f(x)} = \overset{\text{Oracle}}{\underset{\text{sorgulama}}{}} \\ |\psi\rangle &= \textstyle\sum_{x=0}^{7}\alpha_x\,|x\rangle = \alpha_0\,|000\rangle + \alpha_1\,|001\rangle + \alpha_2\,|010\rangle + \alpha_3\underbrace{|011\rangle}_{\text{aranan}} + \ldots + \alpha_7\,|111\rangle \end{aligned}$$

**Şekil**

$$\begin{aligned} |\psi\rangle &= |000\rangle \\ |\psi\rangle &= H^{\otimes 3}\,|000\rangle = \tfrac{1}{\sqrt{2^3}}\textstyle\sum_{x=0}^{7}|x\rangle \quad = \tfrac{1}{2\sqrt{2}}\,|000\rangle + \tfrac{1}{2\sqrt{2}}\,|001\rangle + \tfrac{1}{2\sqrt{2}}\,|010\rangle + \tfrac{1}{2\sqrt{2}}\,|011\rangle \\ &\qquad\qquad + \tfrac{1}{2\sqrt{2}}\,|100\rangle + \tfrac{1}{2\sqrt{2}}\,|101\rangle + \tfrac{1}{2\sqrt{2}}\,|110\rangle + \tfrac{1}{2\sqrt{2}}\,|111\rangle \end{aligned}$$

**Şekil**

Yukarıdan da görüldüğü gibi tüm durumların ortaya çıkma yani olma olasılıkları eşittir $\left(\left(\frac{1}{2\sqrt{2}}\right)^2\right)$. Aradığımız 3 sayısının $(|011\rangle)$ bulunabilmesi demek önündeki genliğin 1 e yakın veya 1 yapılması demektir. Bu da aynı anda aradıklarımızın genliklerinin düşmesi anlamındadır. Aradığımızın genliğinin 1 yapılması için Grover operatörünün $\left(G = WU_f = 2(|\psi\rangle\langle\psi| - I)(-1)^{f(x)}\,|x\rangle\right.$

kaç kez uygulanması gerektiği $\frac{\pi}{4}\sqrt{2^n}$ =Adım sayısı= $\frac{\pi}{4}\sqrt{2^3} = \frac{\pi}{4}2\sqrt{2} \cong \underbrace{2,2}_{\substack{\text{G operatörleri için} \\ \text{uygulanma sayısı}}}$ 2 adım

**Not 49.** Grover operatöründeki $U_f = O$ (oracle)$= x \longrightarrow (-1)^{f(x)} |x\rangle$ den de görüldüğü gibi faz değişimi oluşturmaktadır. Yani arananın genliğini negatife çevirmektedir.

### 14.5.1 Grover Operatörünün Bir Kez Uygulanması

$$\begin{aligned} G &= W \underbrace{U_f}_{=0} |\psi_2\rangle \\ |\psi_3\rangle \quad U_f |\psi_2\rangle &= |\psi\rangle - \tfrac{2}{2\sqrt{2}} |011\rangle \end{aligned}$$

**Şekil**

$$\begin{aligned} |\psi_4\rangle &= W |\psi_3\rangle \\ &= (2 |\psi\rangle\langle\psi| - I) \left( |\psi\rangle - \tfrac{2}{2\sqrt{2}} |011\rangle \right) \\ &= 2 |\psi\rangle \langle\psi|\psi\rangle - \tfrac{4}{2\sqrt{2}} |\psi\rangle \langle\psi|011\rangle - |\psi\rangle + \tfrac{2}{2\sqrt{2}} |011\rangle \\ &= |\psi\rangle - \tfrac{4}{8} |\psi\rangle + \tfrac{2}{2\sqrt{2}} |011\rangle \\ &= \tfrac{1}{2} |\psi\rangle + \tfrac{2}{2\sqrt{2}} |011\rangle \\ |\psi_4\rangle &= \tfrac{1}{4\sqrt{2}} |000\rangle + \tfrac{1}{4\sqrt{2}} |001\rangle + \tfrac{1}{4\sqrt{2}} |010\rangle + \underbrace{\frac{1}{4\sqrt{2}} |011\rangle} + \ldots + \tfrac{1}{4\sqrt{2}} |111\rangle + \underbrace{\frac{1}{\sqrt{2}} |011\rangle} \\ &= \tfrac{1}{4\sqrt{2}} [|000\rangle + |001\rangle + |010\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle] + \tfrac{5}{4\sqrt{2}} |011\rangle \end{aligned}$$

**Not 50.** Yukardan da görüldüğü gibi arananın genliği aranmayanların genlğine göre 5 kat artmıştır. Bunun anlamı aranmayanların genliklerindeki azalma toplam olasılık 1 olduğundan dolayı arananın genliğine artı olarak etki etmiştir.

**Not 51.** $U_f = 0$ aslında tüm veriler içinde arananı ayıklayan yani arananı tespit eden bir sorgulamadır. Buda gaz farkıyla diğerlerinden ayırt etme ile gerçekleşir. Son duruma ($|\psi_4\rangle$) G operatörü tekrar uygulanırsa yani $G = WU_f$

$$|\psi_5\rangle \quad U_f |\psi_4\rangle = \tfrac{1}{2} \left( |\psi\rangle - \tfrac{6}{2\sqrt{2}} |011\rangle \right)$$

**Şekil**

Son duruma $W$ operatörü uygulanırsa

$$\begin{aligned}
|\psi_6\rangle &= W|\psi_5\rangle = (2|\psi\rangle\langle\psi| - I)\left(\tfrac{|\psi\rangle}{2} - \tfrac{6}{4\sqrt{2}}|011\rangle\right) \\
|\psi_6\rangle &= |\psi\rangle\langle\psi|\psi\rangle - \tfrac{6}{4\sqrt{2}}|\psi\rangle\langle\psi|011\rangle - \tfrac{|\psi\rangle}{2} + \tfrac{6}{4\sqrt{2}}|011\rangle \\
&= \tfrac{|\psi\rangle}{2} - \tfrac{6}{8}|\psi\rangle + \tfrac{6}{4\sqrt{2}}|011\rangle \\
&= -\tfrac{2}{8}|\psi\rangle + \tfrac{6}{4\sqrt{2}}|011\rangle \\
&= -\tfrac{1}{4}|\psi\rangle + \tfrac{6}{4\sqrt{2}}|011\rangle \\
&= -\tfrac{1}{4}(|000\rangle + |001\rangle + |010\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle) - \tfrac{1}{4}|011\rangle + \tfrac{6}{4\sqrt{2}}|011\rangle \\
&= -\tfrac{1}{4}(|000\rangle + |001\rangle + \ldots + |111\rangle) + \left(\tfrac{3}{2\sqrt{2}} - \tfrac{1}{4}\right)|011\rangle
\end{aligned}$$

Bu son durumda $|011\rangle$ ölçümü yapılarak bu ölçüm sonucunda da $\frac{3}{2\sqrt{2}} - \frac{1}{4} = \left(\frac{11}{8\sqrt{2}}\right)^2 \cong 0,95$

## 14.6 Simon Algoritması

Simon algoritmasının ana mantığı Grover algoritmasında olduğu gibi $f : \{0,1\}^n$ n girdi içinde aranan ı bulma işlemini $x = y$ veya $x = y \otimes s$ olduğunda $f(x) = f(y)$ durumuna indirgeyen kara kutu sorgulaması şeklinde yukarıdaki durumu değerlendiren bir s yi bulma problemidir. Klasik bilgisayarlarda bu işlem üstel bir sorguya gerek duyarken Simon algoritması bu sorgulamayı polinomsal zamanda gerçekleştirmektedir. Bu algoritma n girdi içinden aranını bulma durumunun yanında kuantum saldırılar (ataklar) için de kullanılmaktadır. Bu algoritma aynı zamanda periyot bulma algoritması olarak da kullanılmaktadır. Bu algoritmanın işleyişi aşağıdaki şekilde gerçekleşmektedir.

$$O_{f(x)}|x\rangle|y\rangle = |x\rangle|f(x) \otimes y\rangle$$

Yukarıdaki Simon algoritmasının devresinden de görülebileceği gibi n qubitlik durum için Simon algoritması 2 tane n qubitlik başlangıç ($|0\rangle$) durumu ile başlar.

**1)** $|0\rangle^{\otimes n} \otimes |0\rangle^{\otimes n}$

**2)** İlk n qubite $H$ uygulanır.
$H^{\otimes}|0\rangle^{\otimes n} \otimes |0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle|000\rangle$

**3)** 2. duruma Oracle uygulanırsa

$$= \tfrac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n} O|x\rangle|0\rangle = \tfrac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle\overbrace{|f(x)\rangle}^{|f(x)\rangle\otimes 0}$$

**4)** 2. yazmaç ($|f(x)\rangle$'de) ölçüm yapılır. Ölçüm sonucunda birinci yazmaç

$$\frac{1}{\sqrt{2}}|z\rangle + \frac{1}{\sqrt{2}}|z \otimes a\rangle$$

durumuna eşit olur.

Yukarıdan da görüldüğü gibi buradaki asıl amaç a yı yani s yi bulmaktır.

**Hatırlatma:**

$$H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} (-1)^{zy}|y\rangle$$

Yukarıdaki hatırlatma kullanılacak olursa

$$\begin{aligned} H^{\otimes n}\left[\tfrac{1}{\sqrt{2}}|z\rangle + \tfrac{1}{\sqrt{2}}|z\otimes a\rangle\right] &= \tfrac{1}{\sqrt{2}}H^{\otimes n}|z\rangle + \tfrac{1}{\sqrt{2}}H^{\otimes n}|z\otimes a\rangle \\ &= \tfrac{1}{\sqrt{2}}\left\{\tfrac{1}{\sqrt{2^n}}\textstyle\sum_{y\in\{0,1\}^n}(-1)^{zy}|y\rangle + \tfrac{1}{\sqrt{2^n}}\sum_{y\in\{0,1\}^n}(-1)^{(z+a)y}|y\rangle\right\} \\ &= \tfrac{1}{\sqrt{2^{n+1}}}\textstyle\sum_{y\in\{0,1\}^n}\left[(-1)^{zy}+(-1)^{(z+a)y}\right]|y\rangle \\ &= \tfrac{1}{\sqrt{2^{n+1}}}\textstyle\sum_{y\in\{0,1\}^n}\left[(-1)^{zy}+(-1)^{zy+ay}\right]|y\rangle \\ &= \tfrac{1}{\sqrt{2^{n+1}}}\textstyle\sum_{y\in\{0,1\}^n}(-1)^{zy}\left[1+(-1)^{ay}\right]|y\rangle \end{aligned}$$

Buradan da görülebileceği gibi yukarıdaki sistem

$$\begin{aligned} y_1 a &= y_{11}a_1 + y_{12}a_2 + \ldots + y_{1n}a_n = 0 \\ y_2 a &= y_{21}a_1 + y_{22}a_2 + \ldots + y_{2n}a_n = 0 \\ &\vdots \\ y_{n-1} a &= y_{(n-1)1}a_1 + y_{(n-1)2}a_2 + \ldots + y_{(n-1)n}a_n = 0 \end{aligned}$$

şeklinde n-1 adet lineer denklem sistemi elde edilir. Bu denklem sistemi çözülerek a diğer bir deyişle s bulunmuş olur. Yukarıdaki Simon algoritmasını aşağıdaki şekilde adım adım yazabiliriz.

**1)** sayaç $i = 1$ yapılır.

**2)** $\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle|0\rangle$ durumu oluşturulur.

**3)** $U_f$ uygulanarak $\sum_{x\in\{0,1\}^n}|x\rangle|f(x)\rangle$ durumu oluşturulur.

**4)** 2. yazmaçta ölçüm yapılır (Seçimli olabilir).

**5)** İlk $n$ qubit dizisine $H^{\otimes n}$ uygulanır.

**6)** İlk yazmaçta ölçüm yapılır ve ölçüm sonuçları olan $w$ ler saklanır.

**7)** Eğer $i = n + 4$ ise bir sonraki adıma git. Aksi halde $i$ yi arttır ve 2. adıma git.

**8)** $w.s^t = a^t$ den lineer denklem sistemini çöz. $\{s_1, s_2, \ldots, s_n\}$ leri bul.

**9)** $f(0), f(s_1), f(s_2), \ldots, f(s_n)$ leri hesapla ve $s_1, s_2, \ldots, s_n$ leri bul.

**Not 52.** Simon algoritması $n$ girdi değeri içinden istediğimizin bulunmasında kullanıldığı gibi kuantum saldırı (kauntum atak), kuantum saldırılar içinde çok sık kullanılan bir algoritmadır.

Simon Algoritması ile Grover Algoritmasını karşılaştıracak olursak Simon Algoritmasında $n$ girdi için n qubitlik ilave yedek qubite de ihtiyaç varken Grover Algoritmasında böyle bir duruma ihtiyaç yoktur.

**Örnek 59.** $n = 3$ qubitlik durumda $s = a = 110$ durumunu Simon Algoritması ile bulunuz.

$$O_{f(x)} |xy\rangle = |x\rangle \overbrace{|f(x) \oplus y\rangle}^{\substack{z \oplus a \\ z \oplus s}} \quad \text{Bu bağlamda}$$

| $x$ | $f(x)$ |
|---|---|
| 000 | 101 |
| 001 | 010 |
| 010 | 000 |
| 011 | 110 |
| 100 | 000 |
| 101 | 110 |
| 110 | 101 |
| 111 | 010 |

tek bir değer elde edilmiş olur. Bu da aradığımız değere denk gelir.

**Not 53.** Simon Algoritmasında a'nın belirlenmesi için $f$'ye $O(n)$ sorgu gerekirken klasik algoritmalarda bunun için üstel sorguya ihtiyaç duyulmaktadır. Kısacası klasik algoritmalarda (günümüz bilgisayarlarda kullanılan) a'yı bulmak için $f$'ye üstel bir zamanda sorgu gerekirken Simon Algoritmasında aynı iş $O(n)$ adımda gerçekleştirilir. Bu da Simon Algoritmasının klasik algoritmalara göre ne kada hızlı çalıştığını gösterir.

⌜ Neden yedek qubit kullanılmış Simon Algoritmasında?
Oracle fonksiyonu yedek qubit olmadan uygulanamıyor.⌟

# Bölüm 15

# Kuantum Kriptografi (Kuantum Şifreleme)

Klasik şifrelemede güvenli iletişim üretilen anahtar ile gönderilecek mesajın şifrelenerek gönderilmesine dayanmaktadır. Klasik şifrelemede anahtarlar rastgele sayı üreteçleri tarafından oluşturulmaktadır. Klasik güvenli iletişimde mesaj sıfır ve birlerin bir tanesini içerecek biçimde oluşmaktadır. Kuantum şifrelemede ise hem anahtar üretimi hem de mesaj klasiğe göre çok çok farklıdır. Örneğin, anahtar üretimi tamamen kuantumsal yani 0 ile 1 arasındaki tüm olasılıkları içerecek şekilde gerçekleşmektedir. Mesajda 0 ve 1 lerden bir tanesini değil 0 ve 1 lerin aynı anda ve aynı zamanda 0 ve 1 lerin tüm olası durumlarını içerecek şekilde oluşturulmaktadır. Bu nedenle klasiğe göre daha güvenli bir iletişim sağlamaktadır. Diğer bir deyişle klasik şifreleme anahtar oluştururken basit nümerik algoritmaları kullanırken kuantum şifreleme kuantum mekaniksel kurallar çerçevesinde anahtar üretir. Bu anahtar üretimi aynı zamanda kuantum anahtar dağıtımı (Quantum Key Distrubition) olarak da bilinmektedir. Kuantum anahtar dağıtımının gerçekleşmesi için en az iki kişiye gerek vardır. Örneğin Alice ile Bob göz önüne alalım. Bu ikisi arasında iki ietim kanalı kullanılır. Birisi internet, cep telefonu veya ev telefonu gibi klasik kanal şifreli mesaj bu kanal olan kuantum kanaldır. Bu kanalda pratikte fotonun polarizasyonu ile gerçekleştirilir. Örneğin, mevcut fiber optiklerdeki fotonların polarizasyonu gibi. Bu şekildeki bir iletişimde ( kuantum anahtar dağıtımı yardımıyla) araya bir kişinin girip şifreli anahtarları almaya çalışması mümkün değildir. Çünkü araya bir kişinin girebilmesi için ölçüm yapması gerekir. Bu ölçüm sonucunda da ana sitemin durumu değişeceğinden araya giren kişinin anahtarları öğrenmesi mümkün değildir. Örneğin, şifreleme için yapılan bir algoritmayı daha ga güvenli hale getirmek için anahtar paylaşmış süper yoğun kodlama ile gerçekleştirilebilir. Kuantum şifreleme anlamında birade algoritma geliştirilmiştir. Bunlara Benner ve Brassard tarafından 1984 yılında geliştirilen BB84 ve aynı zamanda B92 ve Ekert tarafından geliştirilen E91 algoritmalarını örnek olarak verebiliriz. Bu algoritmaların hepsini şu an gerçekleştiren cihazlar satılmaktadır. Bu cihazların çalışma

prensipleri fotonun polarizasyonuna dayanmaktadır.

## 15.1 BB84 Protokolü

Bu protokol kuantum iletişim alanında ilk geliştirilen kuantum anahtar dağıtım protokolüdür. Bu protokolde kullanılan 3 temel kuantum prensibini aşağıdaki şekilde özetleyebiliriz:

**1)** Kuantumdaki no-cloning teoremi gereği araya giren (örneğin Eve) kişi kuantum durumu kopyalayamayacağından Alice ile Bob arasına girip anahtarı kopyalamayacaktır.

**2)** Ölçme işlemi terslenemezdir. Çünkü ölçme işleminde gerçekleştirilen operatör birimsel değildir. Diğer bir değişle ölçme sonucundan sistemin tüm kuantum durumunu elde etmek mümkün değildir. Diğer bir deyişle ölçme tüm olası durumların tek bir duruma çökmesi demektir. Tek bir durumdan yararlanılarakta tüm durumları elde etmek mümkün değildir.

**3)** Kuantum anahtar dağıtımında bir dizisi oluşturulurken farklı bazlar kullanılır. Bu nedenle verilen bazların birinde ölçme yapıldığında durum tamamen rastgele olan diğer bazlardaki ölçüm sonuçlarına çökecektir. Bu nedenle sistem durumu hakkında bilgi elde edilmesi (araya giren kişi tarafından bilgi edinilmesi) zorlaşmaktadır.

Yukarıdaki durumları (2 ve 3'ü) açıkça görebilmek için sistemin

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \qquad (\text{ Süper pozisyon durumu})$$

durumunda olduğunu kabul edelim. Bu sistemde ölçme $|0\rangle$ ve $|1\rangle$ bazlarında yapılabilir. Bu durumda sistemin ilk orjinal durumu kaybolur.

Örneğin 0 ölçümü yaptığımızı varsayalım. Bu durumda (ölçüm sonucunda) ana sistemin durumu orjinalden çok çok farklıdır. BB84 protokolünde anahtar oluşturmak için

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

şeklindeki 4 temel baz kullanılır. Bu işlem (anahtar oluşturma) aşağıdaki şekilde gerçekleltirilir:

Alice $2n$ qubitlik rastgele bir diziyi oluşturmaya başlar. Her bir qubit $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$ bazlarından birinde oluşturulur. Bu oluşum esnasında

$$0 \longrightarrow |0\rangle \text{ ve } |+\rangle \text{ ile gösterilir.}$$

$$1 \longrightarrow |1\rangle \text{ ve } |-\rangle \text{ ile gösterilir.}$$

Alice bu qubit dizisini kuantum kanal yardımıyla Bob'a gönderir. Bob gönderilen bu qubitlerin her birini ölçer. Bu işlemde $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$ bazlarından birini rastegele seçerek gerçekleştirir.

Yukarıdan da görüleceği gibi $n$ bitlik durum $|0\rangle$ ve $|1\rangle$ bazında oluşurken diğer $n$ bitlik durum $|+\rangle$, $|-\rangle$ bazında oluşacaktır. Sonuçta Alice ve Bob kendi ellerindeki notları karşılaştırır. Bunu karşılaştırırken hangi pozisyonda hangi bazı kullandıklarını birbirine söylerler. Eğer her ikisi farklı baz kullandılar ise bur durumda qubiti iptal ederler sonuç anahtarı ise iptal edilmeyen qubitlerden oluşturulur.

**Not 54.** Klasik güvenlik önlemlerinde araya giren hırsız tespit edilemiyorken kuantumsal iletişimlerde araya giren hırsız Decay State foton ile anlık olarak tespit edilebilmektedir. Bunu gerçekleştiren cihazlar mevcuttur.

## 15.2 B92 Protokolü

Bu protokol BB84 protokolünün geliştirilmiş versiyonudur. Bu protokolün BB84 ten farklı BB84 protokolü dik (ortogonal) baz sistemini kullanırken güvenliği daha da arttırmak için B92 protokolü dik olmayan iki baz sistemini kullanmaktadır. Bu protokolde dik olmayan baz sitemleri $|0'\rangle$ ve $|1'\rangle$ ile gösterilmektedir. Bu protokol aşağıdaki şekilde gerçekleşir.

**1)** Bob rastgele bilgisayar bazlarını veya dik olmayan $|0'\rangle$, $|1'\rangle$ bazlarını seçerek qubitleri ölçer. Yani Bob ölçümünü

$$P_0 = |0\rangle\langle 0|$$

$$P_0' = |0'\rangle\langle 0'|$$

operatörleri ile gerçekleştirilir.

**2)** Bob anahtarı $|1\rangle$ veya $|1'\rangle$ deki ölçüm sonuçlarındaki bir durumlarından oluşturur.

**3)** Bob klasik kanalla sahip olduğu bit pozisyonlarını Alice'e söyler.

Yukarıdaki bilgiler ışığında bu protokolün çalışması aşağıdaki şekildedir.

Örneğin Alice $|0\rangle$ oluştursun ve Bob hesaplama bazlarında ($|0\rangle$ ve $|1\rangle$) $|0\rangle$ ölçer. Eğer Bob $|0'\rangle$ ve $|1'\rangle$ (dik olmayan bazlar) bazlarında ölçüm yaparsa $|1'\rangle$ elde eder.

Eğer Alice $|0'\rangle$ nü oluşturursa Bob hesaplama bazlarında ($|0\rangle$ ve $|1\rangle$) ölçüm yaparak $|0'\rangle$ elde eder. Eğer Bob $|0'\rangle$ ve $|1'\rangle$ (dik olmayan bazlar) bazlarında ölçüm yaparsa $|1\rangle$ elde eder.

**Örnek 60.** Alice aşağıdaki 8 bitlik bir diziyi oluştursun.

$$|0'\rangle\,|0'\rangle\,|0'\rangle\,|0'\rangle\,|0'\rangle\,|0'\rangle\,|0'\rangle\,|0'\rangle = |0'0'0'0'0'0'0'0'\rangle$$

Eğer Bob

$$|0'\rangle\,|0'\rangle\,|0'\rangle\,|0'\rangle\,|0'\rangle\,|0'\rangle\,|0'\rangle\,|0'\rangle$$

leri kullanarak ölçüm yaparsa sonuç

$$|0'\rangle\,\boxed{|1'\rangle}\,|0'\rangle\,|0'\rangle\,\boxed{|1'\rangle}\,\boxed{|1'\rangle}\,\boxed{|1'\rangle}\,|0'\rangle$$

Bob anahtarlar için 2,5,6,7 pozisyonlarını tuttuğunu açıklar.

**Not 55.** BB84 ile B92 protokolü arasındaki en önemli fark BB84'te anahtar Alice tarafından oluşturulurken B92 protokolünde anahtar Bob'un ölçüm sonuçları olan $|1\rangle$ veya $|1'\rangle$ lerden oluşturulur. Anahtar oluşumunda $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$ 4 baz yerine Alice sadece $|0\rangle$ ve $|0'\rangle$ ler şeklindeki 2 baz kullanır.

## 15.3 E91 Protokolü

Bu protokol 1991 yılında Ekert tarafından geliştirilmiş olup dolanık temelli bir protokoldür. Bu protokolde Bell bazları olarak da bilinen 4 tane EPR (Einstein, Podolski, Rosen) bazından (durumundan) biri kullanılır ve bu 4 durumdan birinin bir kısmı Alice'te bir kısmı ise Bob'da olmak üzere ikisi arasında paylaştırılır.

Örneğin Alice ve Bob

$$|B_{00}\rangle = \frac{|0_A 0_B\rangle + |1_A 1_B\rangle}{\sqrt{2}}$$

durumu ile dolanık iseler Alice ve Bob tamamen doğrusal bir ilişkiye sahip ölçüm sonuçları elde edecektir. (Çünkü Alice $|0\rangle$ ölçerse Bob'un elinde $|0\rangle$ olacaktır.)

Örneğin

Alice $|0\rangle$ ölçerse Bob'un ölçüm sonucu da $|0\rangle$ olacaktır.

Alice $|1\rangle$ ölçerse Bob'un ölçüm sonucu da $|1\rangle$ olacaktır.

Eğer Alice ve Bob

$$|B_{01}\rangle = \frac{|0_A 1_B\rangle + |1_A 0_B\rangle}{\sqrt{2}}$$

durumu ile dolanık iseler bu durumda Alice ve Bob'un ölçüm sonuçları tamamen zıt ilişkili olacaktır.

Örneğin

Alice $|0\rangle$ ölçerse Bob'un ölçüm sonucu da $|1\rangle$ olacaktır.

Alice $|1\rangle$ ölçerse Bob'un ölçüm sonucu da $|0\rangle$ olacaktır.

Bu protokolde Alice ve Bob karşılıklı qubitlerini rastgele seçilen bazlarda ölçerler sonra aynı bazlarda ölçüm sonuçlarını birbirlerine söyleyerek ölçüm sonucu anahtar olur. Ölçüm sonuçları tamamen ilişkili veya tamamen ilişkisiz olacağı için araya giren bir kişinin (Evet)

tespit edilmesi çok kolaydır. Bu kuantum atağı düzeltilerek tespit edilebilir.

Tüm kuantum anahtar üretim ve dağıtım sistemlerinde Eve tespiti için yedek foton üretilerek gönderilen fotonların içinde (anahtarı temsil eden) Eve tespiti için gönderilen yedek fotonlarda bulunur.

Örneğin eğer anahtar 20 biten oluşuyorsa Eve bunun 6 bitini biliyorsa sonuç anahtar bu 6 bitin çıkarılmasıyla elde edilen 14 bitlik olacaktır.

**Not 56.** Hem BB84 ve B92 hem de dolanıklık temelli E91 protokollerini gerçekleştiren cihazlar mevcut olup satışa da sunulmuş durumdadır. Bu tür cihazlar Amerika, Japonya, Avusturalya, Avusturya, Almanya, Çin, İngiltere, Fransa, Kanada gibi ülkeler tarafından kullanılmaktadır. Örneğin Japonya'nın Tokyo şehrinde Amerika'nın birçok şehrinde, Avusturya'nın Viyana şehrinde, Kanada'nın birkaç şehrinde bu cihazlar kullanılarak iletişim hatları denenmiş ve gerçekleştirilmiştir. Bu protokoller şuanda ışığın polarizasyonu kullanılarak gerçekleştirilmektedir. Çünkü şuanda dünyadaki mevcut altyapı fiber optik olduğu için ve fiber optik kablolarda da iletişim fotonlar aracılığıyla olduğu için polarizasyon kullanılmaktadır.

Dolanık temelli protoller ile dolanık temelli olmayan protokoller arasındaki en önemli fark dolanık temelli protokollerde dolanıklık paylaşıldıktan sonra hiçbir iletin kanalı (fiber optik kablo, uydu vb.) olmadan iletişimin gerçekleştirilmesidir. Bu da çok önemli bir güvenlik avantajı sunmaktadır. Ekert tarafından geliştirilen dolanıklık temelli E91 protokolü geliştirilerek SARG protokolü geliştirilmiştir.

**Örnek 61.** Alice 8 bitlik aşağıdaki durumları oluştursun.

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

Eğer Bob aşağıdaki sırada rastgele ölçüm yaparsa ellerinde kalan (uyuşmayan bazlar göz ardı edildikten sonra) anahtarı bulunuz.

$$\{|0\rangle\,,|1\rangle\},\{|0\rangle\,,|1\rangle\},\{|\pm\rangle\},\{|\pm\rangle\},|\pm\rangle\,\{|0\rangle\,,|1\rangle\}\,|\pm\rangle\,,|\pm\rangle$$

**Not 57.** Bilindiği gibi kuantum bilgisayarlarda

$$\text{mantıksal } 0 \to |0\rangle \;\text{ ve }\; |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

$$\text{mantıksal } 1 \to |1\rangle \;\text{ ve }\; |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

ile gösterilmektedir.

Buradan

$$|0\rangle = \frac{|+\rangle + |-\rangle}{\sqrt{2}}$$

$$|1\rangle = \frac{|+\rangle - |-\rangle}{\sqrt{2}}$$

olur.

Kolaylık olsun diye Alice ve Bob'un farklı bazlarda kullandıkları bitleri 1'den 8'e kadar numaralandıralım. Bu durumda aşağıdaki tablo oluşturulur.

| | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** |
|---|---|---|---|---|---|---|---|---|
| **Alice'in bitleri** | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 |
| **Alice'in bazları** | $\{\|0\rangle, \|1\rangle\}$ | $\{\|0\rangle, \|1\rangle\}$ | $\|\pm\rangle$ | $\{\|0\rangle, \|1\rangle\}$ | $\{\|0\rangle, \|1\rangle\}$ | $\|\pm\rangle$ | $\|\pm\rangle$ | $\|\pm\rangle$ |
| **Bob'un bazı** | $\{\|0\rangle, \|1\rangle\}$ | $\{\|0\rangle, \|1\rangle\}$ | $\|\pm\rangle$ | $\|\pm\rangle$ | $\|\pm\rangle$ | $\{\|0\rangle, \|1\rangle\}$ | $\|\pm\rangle$ | $\|\pm\rangle$ |
| **Çakışma** | Evet | Evet | Evet | Hayır | Hayır | Hayır | Evet | Evet |
| **Elde kalan** | Evet | Evet | Evet | Hayır | Hayır | Hayır | Evet | Evet |

**Not 58.** Yukarıdan da görüldüğü gibi 4,5 ve 6 durumları çakışma olmadığından (Alice ve Bob'un ölçüm sonuçları) göz ardı edilir. 1,2,3,7,8 durumlarındaki bitler (Alice ve Bob'un ölçüm sonuçları) birbiri ile uyuşmaktadır ve bunlar aşağıdaki anahtarı oluşturur.

$$s = 01001$$

Anahtardan da görüldüğü gibi başlangıçta Alice'in oluşturduğu rastgele bit 8 tane iken oluşan anahtar 5 bitten oluşmaktadır. Bunun sebebi çevresel faktörlerden dolayı hatalar oluşması bu hataları da Alice ile Bob'un kontrol etmesidir. Bunun yanında hatalara çevresel faktörler sebep olabileceği gibi anahtarı kopyalamak için araya giren (Eve) de sebep olabilir. Eğer hata çok fazla ise bu Eve'in varlığını göstermektedir. Bu durumda Alice ve Bob anahtarı iptal ederşer ve tekrar anahtar oluştururlar. Yukarıdaki örnekte 8 bit üzerinde Eve'nin ölçüm yaptığını farz edelim. Buna göre %50 şansla $\{|0\rangle, |1\rangle\}$ ve %50 şansla $|\pm\rangle$ bazlarını seçme durumu mevcuttur.

Örneğin Eve'nin bilgisayar bazlarını sectiğini farz edelim. Bu durumda Eve'in ölçüm sonucu ya $|0\rangle$ ya da $|1\rangle$ olacaktır.

Bu durumda $|0\rangle$ olduğunu farz edelim

$$|0\rangle = \frac{|+\rangle + |-\rangle}{\sqrt{2}}$$

Bob ölçüm yaptığında Alice kendi qubitini $|-\rangle$ durumda hazırlamasına rağmen Eve'nin doğru sonucu görme ihtimali %50'dir. Eğer ilk oluşturulan bir dizisi sayısı arttırılırsa bu durumda

araya giren kişinin (Eve) doğru sonucu yakalama olasılığı çok çok azalacaktır. Bununla beraber kuantum kanaldaki gürültü hatalar oluşturacaktır. Bu hatalar anahtar qubitlerini karşılıklı sabitleştirmekte kullanılmaktadır.

Örneğin; ölçüm sonucu oluşan hata kuantum kanal hatasından büyükse arada mutlaka bir dinleyici vardır. Bu durumda anahtar iptal edilir. Genelde kuantum kanaldaki gürültü eşik değer (threshold) olarak kabul edilmektedir.

**Not 59.** Mevcut anahtar dağılımlarında kuantum kanaldaki gürültü eşik değer olarak göz önüne alınmaktadır. Her kanalın gürültüsü farklı olduğundan bu görüntülerde o kanalı kullanan kullanıcılar tarafından kolayca tespit edildiğinden kanal gürültüsü hata oranlarını karşılaştırmak için eşik değer olarak göz önüne alınmaktadır.

**Not 60.** BB84 ve diğer kuantum anahtar dağıtım protokollerinde araya giren kişi (Eve) tespit etmek Decay State foton durumu başlangıçtaki Alice'in bit stringlerine yerleştirilir ve böylece aradaki kişi tespit edilmiş olunur. Şuandaki bu durum mevcut internet kullanımında mümkün değildir.

Geliştirilen algoritmalarla aynı zmanda atak (saldırılar) da yapılabiliyor. DNS zehirlenmesi klasik bilgisayarlarda en çok yapılan ve önlem alınması zor olan bir saldırıdır. Klasik bilgisayarlarda ayrıca saldıganı tespit etmesi şuan mümkün değildir. Fakat Decay State ile kuantumsal olarak tespit etmek mümkündür.

## 15.4 Deutsch-Jozsa Algoritması ile Nasıl Atak Yapılır?

Deutscj-Jozsa algoritması ya da diğer algoritmalar ile yapılan atağın ana mantığı cihazdaki dolanıklık durumla dolanık hale gelmek yani dolanıklık kullanılarak saldırı planlamaktır.

Cihazdaki dolanıklık ile kendimi nasıl dolanık hale getirebilirim ve bunu kullanarak bilgileri elde edebilirim.

Deutsch-Jozsa algoritmasındaki karakutu sorgulamasında birimsel sorgulama operatörü birinci yazmaç olduğu gibi kalıyor ikinci yazmaca birinci yazmaç argüman alınıp binary toplam yapıyor ($U_f$) karakutu uygulaması yapılıyor.

İlk önce $H$ kapısı uygulanır hepsinde başlangıç durumuna getiriliyor. Deutsch-Jozsa algoritmasında diğer algoritmalarda da olduğu gibi ilk aşamada qubitleri başlangıç durumuna getiriyoruz.

**1)** Girdi qubitlerinin hepsi başlangıç durumuna getirilir. Yani ilk $n$ qubit $|0\rangle$ ve en son olan qubit $|1\rangle$ durumlarına getirilir.

**2)** $n+1$ qubite $H$ uygulanır. Yani $H^{\otimes n}|0\rangle^{\otimes n} H|1\rangle$

**3)** Karakutu sorgulaması

binary toplam $U_f$ uygulanmalı

$U_f : U_f \left|x\right\rangle_A \left|y\right\rangle_B \longrightarrow \left|x\right\rangle_A \left|y \oplus f(x)\right\rangle_B = (-1)^{f(x)} \left|x\right\rangle \left|y\right\rangle$

**4)** İlk $n$ qubite $H$ uygulanır.

$\left|\psi\right\rangle_3 = (-1)^{f(x)+xy} \left|y\right\rangle$

fonksiyon sabtise $|0\rangle$, dengeli ise $|1\rangle$ sonucunu elde ederiz.

**Not 61.** Fonksiyon sabitken sonucun her zaman $|0\rangle$ olması önemli, dengeli iken sonucun her zaman $|1\rangle$ olması önemli.

$$\frac{1}{\sqrt{2^{n+1}}} \sum_{x\in\{0,1\}^n} \left|x\right\rangle_A \left(\left|0\right\rangle_B - \left|1\right\rangle_B\right) \tag{15.1}$$

15.1 eşitliğine $U_f$ uygulayalım

$$\xrightarrow{U_f} \quad \frac{1}{\sqrt{2^{n+1}}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} \left|x\right\rangle_A \left(\left|0\right\rangle_B - \left|1\right\rangle_B\right) \tag{15.2}$$

15.2 eşitliğine ilk n qubite (birinci yazmaç A yazmacına) $H$ uygulanır.

$$\xrightarrow{H^{\otimes n}} \quad \frac{1}{2\sqrt[n]{2}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)\oplus xy} \left|y\right\rangle_A \left(\left|0\right\rangle_B - \left|1\right\rangle_B\right) \tag{15.3}$$

$f$ ise sabit çıktı.

$$(-1)^{f(0)} \left|0\right\rangle_A \left(\left|0\right\rangle_B - \left|1\right\rangle_B\right) \tag{15.4}$$

$f$ dengeli ise $\left|0\right\rangle_A$ yı elde edemeyiz.

15.1 eşitlikte C saldırganı başlangıç durumundaki $\left|0\right\rangle_A$ yı dolanık olanla değiştirirse

$$\frac{1}{\sqrt{2^{n+1}}} \sum_{x\in\{0,1\}^n} \left|x\right\rangle_A \left|x\right\rangle_C \left(\left|0\right\rangle_B - \left|1\right\rangle_B\right) \tag{15.5}$$

Saldırgan A yazmacının $i$. qubiti yer değiştirirse

$$\left|\phi^+\right\rangle_{A_iC_i} = \left(\frac{1}{\sqrt{2}}\right) \left(\left|0\right\rangle_{A_i} \left|0\right\rangle_{C_i} + \left|1\right\rangle_{A_i} \left|1\right\rangle_{C_i}\right) \tag{15.6}$$

Deutsch-Jozsa kullanan kişi ile C dolanık hale geldi. Kişi daha algoritma çalışmaya başlamadan önce onunla dolanık hale geliyor. (irtibat kuruldu)

Yasal kullanıcı 15.5 eşitliğinde $U_f$ yi hem A hem B yazmaçlarına uygular.

$$\xrightarrow{U_f} \quad \frac{1}{\sqrt{2^{n+1}}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} \left|x\right\rangle_A \left|x\right\rangle_C \left(\left|0\right\rangle_B - \left|1\right\rangle_B\right) \tag{15.7}$$

$$\xrightarrow{H_A^{\otimes n}\otimes H_C^{\otimes n}} \quad \frac{1}{2^{\frac{3n}{2}}\sqrt{2}} \sum_{x,y,z\in\{0,1\}^n} (-1)^{f(x)\oplus x(y\oplus z)} |y\rangle_A |z\rangle_C (|0\rangle_B - |1\rangle_B) \tag{15.8}$$

$f$ sabit ise $y = z$

$f$ dengeli ise $y \neq z$

Farklı senaryolar oluşur. Bunlardan

**1. Durum:** Eğer asıl kullanıcı Deutsch-Jazsa algoritmasını kullanmadan önce saldırgan başlangıç qubitlerinden $\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)$ lerin birini kendisindeki dolanıklıkla değiştirdiğini farz edelim. Bu durumda içerdeki birisi (saldırganla işbirliği içindeki) A'nın ölçüm sonuçlarını söylerse bu durumda saldırgan fonksiyon sabit veya dengeli olduğunu öğrenir. Bu durumda asıl kullanıcı yanlış cevap elde eder ve saldırganın saldırdığını fark etmez. Dolanıklık vasıtasıyla ölçüm sonucunu da öğrenebilir.

Bu durumdan kurtulmanın yolu yani saldırganın saldırısını önlemek için algoritmanın başlangıç durumuna getirilmeden önce algoritmanın başlangıç durumuna getirilip getirilmediği kontrol edilir. İkinci olarak da Decay State foton kullanarak arada bir kişi olup olmadığını veya bilgisayarımıza bir kişinin ulaşmayı deneyip denemediği kontrol edilir.

## 15.5 Simon Algoritması ile Nasıl Atak Yapılır?

- $f(x) : x \in \{0,1\}^n$ farklı ve $f$ fonksiyonu birebirdir.
- $s \in \{0,1\}^n$ $s \neq 0$

$f(x) = f(y) \Leftrightarrow x = y \vee x = y \oplus s$ doğrudur. $f$ 1-1 dir.

$x = y$ veya arananlar alt grublara parçalandığından arananlar alt gruplarda olabilir.

Groverdan farkı $n$ veri için $n$ yedek qubit olmasıdır. Groverda arama işlemi yapılırken aynı anda aranmayanlar eleniyordu. Çünkü ana mantığı arananın genliğini yükseltmekti. (Genlikler toplamı yani $\alpha^2 + \beta^2 = 1$)
Bu yüzden Grover Simon'a göre daha avantajlıdır.

$n$ tane lineer denklem sistemi bunların çözümü bize aranan $s$'yi verir. Simon algoritmasında

$$|x\rangle_A |y\rangle_B \xrightarrow{U_f} |x\rangle_A |y \oplus f(x)\rangle_B , \qquad x, y \in \{0,1\}^n \tag{15.9}$$

**1)** $n$ tanesi başlangıç durumuna getiriliyor

$$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle_A |0\rangle_B \tag{15.10}$$

**2)** 15.17 eşitliğine $U_f$ uygulanır.

$$\xrightarrow{U_f} \quad \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle_A |f(x)\rangle_B \tag{15.11}$$

**3)** A yazmacının tüm qubitlerine $H$ uygulanır

$$\xrightarrow{H^{\otimes n}} \quad \frac{1}{2^n} \sum_{x,y\in\{0,1\}^n} (-1)^{xy} |y\rangle_A |f(x)\rangle_B \tag{15.12}$$

$$\begin{array}{lll} k_1.s = 0 & \mod 2 & s \neq 0 \text{ olduğunda ve } f \text{ örten ise} \\ k_2.s = 0 & \mod 2 & \text{denklem sağlanır.} s = 0 \text{ ise } f \text{ birebirdir.} \\ \vdots & & \\ k_m.s = 0 & \mod 2 & \end{array}$$

$s \neq 0$ iken $s$ bulunacak.

Simon algoritması kullanılması durumunda da Deutsch-Jozsa algoritmasında olduğu gibi başlangıçtaki süperpozisyon durumlarından biri veya bir kaçı dolanık olan qubit ile yer değiştirilir. Bu işlem algoritma başlangıç durumuna getirilmeden önce yapılır.

$$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle_A |x\rangle_C |0\rangle_B \tag{15.13}$$

$$\xrightarrow{U_f} \quad \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle_A |x\rangle_C |f(x)\rangle_B \tag{15.14}$$

$$\xrightarrow{H_A^{\otimes n}\otimes H_C^{\otimes n}} \quad \frac{1}{2^{\frac{3n}{2}}} \sum_{x,y,z\in\{0,1\}^n} (-1)^{x(y\oplus z)} |y\rangle_A |z\rangle_C |f(x)\rangle_B \tag{15.15}$$

## 15.6 Grover Algoritması ile Nasıl Atak Yapılır?

Hepsindeki ana mantık algoritmalar çalışmaya başlamadan önce başlangıçtaki qubitler ile dolanık hale gelerek karşı tarafın bilgilerini almak.

Saldırının ana mantığı dolanıklığı kullanarak karşı tarafla ilişki kurup algoritmalar çalışmadan dolanık hale gelip karşı tarafın yapmış olduğu işlemleri aynı anda almak (ve karşı tarafın farklı sonuç elde etmesini sağlamak).

Grover algoritmasında $n$ tane düzensiz veri içinden arananı bulmak. Ölçümde $|0\rangle$ $|1\rangle$ lerden oluşan reel bir dizi elde ederiz. Bu ölçüm sonuçları $\alpha, \beta$ denilen genliklerle çarpılır. Genlikler olma olasılığı. İstediğimin olmasını istiyorsam genliği ile oynarım. Genliklerle faz

uzayında oynanmaz.

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

Faz uzayında bir genliğin durumunu oynamak zordur. Groverda istediğinin genşiğini yükseltme mantığı vardır. Biri yükseltilirken diğeri düşünülür. Çünkü toplamları 1 olmalıdır. $n$ tane veri $2^n$ tane olası durum demektir. Grover operatörü arananın genliğini yükseltirken diğer genliğin düşmesi fazın değişimidir. Qubit sayısı arttığında Grover Algoritması kullanılan makineler saldırı yapmak mümkün değildir. Algoritma başlamadan önce karşı tarafa sızmak için dolanık durumla karşı tarafla ilişkiye geçilmelidir. Saldırgan Grover Algoritmasını çalıştırmadan önce $|0\rangle$ yerine örneğin

$$\frac{1}{2}\sum_{x\in\{0,1\}^2} |x\rangle_A\,|x\rangle_B \tag{15.16}$$

2 qubitlik durumunu oluşturur. Asıl bilgisayar kullanıcısı A yazmacına Grover operatörünü uygular. Sonuçta tüm sistemin durumu

$$|\phi_k\rangle_{AB} = \frac{1}{2}\left[(WR_0W)R_kW\right]_A \sum_{x\in\{0,1\}^2} |x\rangle_A\,|x\rangle_B \tag{15.17}$$

$$\begin{aligned}
|\phi_{00}\rangle_{AB} &= \frac{1}{2}(-\,|00\rangle_A\,|00\rangle_B + |10\rangle_A\,|01\rangle_B + |01\rangle_A\,|10\rangle_B + |11\rangle_A\,|11\rangle_B)\\
|\phi_{01}\rangle_{AB} &= \frac{1}{2}(-\,|00\rangle_A\,|00\rangle_B - |10\rangle_A\,|01\rangle_B + |01\rangle_A\,|10\rangle_B - |11\rangle_A\,|11\rangle_B)\\
|\phi_{10}\rangle_{AB} &= \frac{1}{2}(-\,|00\rangle_A\,|00\rangle_B + |10\rangle_A\,|01\rangle_B - |01\rangle_A\,|10\rangle_B - |11\rangle_A\,|11\rangle_B)\\
|\phi_{11}\rangle_{AB} &= \frac{1}{2}(-\,|00\rangle_A\,|00\rangle_B - |10\rangle_A\,|01\rangle_B - |01\rangle_A\,|10\rangle_B + |11\rangle_A\,|11\rangle_B)
\end{aligned}$$

Yukarıdan da görüleceği gibi 3 olası senaryo mevcuttur.

**1)** Saldırgan $|00\rangle_B$ sonucunu elde ederse bilgisayarı asıl kullanan doğru sonucu elde eder.

**2)** Bilgisayarı asıl kullanan olası 4 sonuçtan birini eşit olasılıkla elde eder.

**3)** Saldırgan görünmeden (hissedilmeden) doğru cevap elde ettiğinde asıl kullanıcı yanlış sonuç elde eder.

15.16 denklemi (durumu) aslında dolanık durumdur. Yani saldırgan algoritma başlamadan önce $|0\rangle$ durumu ile dolanık bir durumu değiştirmiştir.

Asıl kullanıcı Grover Algoritmasını çalıştırdıktan sonra A yazmacındaki sonuçları görecektir. Bu durumda $\frac{1}{4}$ olasılıkla doğru cevabı elde eder. $\frac{3}{4}$ olasılıkla da yanlış cevabı elde eder.

Oracle fonksiyonunu asıl bilgsayar kullanıcısı uyguladığından sonucun doğruluğunu kontrol edebilir. Buna rağmen saldırgan karşıdaki kişinin doğru veya yanlış sonuç elde edip etmediğini öğrenebilir ve sonuçta saldırgan doğru sonucu $\frac{3}{4}$ olasılıkla elde eder. Bu durumda asıl kullanıcı $\frac{1}{4}$ olasılıkla da yanlış sonucu elde eder.

**Not 62.** Grover Algoritması kullanılması durumunda saldırgan ancak ve ancak asıl kullanıcı 1 qubit kullandığında aşarılı olabilir. Qubit sayısı 2 den fazla olduğu durumlarda saldırganın başarılı olması mümkün değildir.

**Örnek 62.** 3 qubit olması durumunda ($n = 3$ olduğunda)

$$m = \left[\frac{1}{2}\left(\frac{1}{\theta}\frac{\pi}{2} - 1\right)\right] \sim \left[\frac{\pi}{4}\sqrt{2^n}\right] \rightarrow \text{ iterasyon sayısı}(m)$$

iterasyon sayısı 2 dir.

$$\sin\theta = \frac{1}{\sqrt{2^n}}, \quad \cos\theta = \sqrt{\frac{2^n - 1}{2^n}}$$

$n = 3$ durumunda $\sin\theta = \frac{1}{\sqrt{8}}$ $\cos\theta = \sqrt{\frac{7}{8}}$ olduğundan $\theta \cong 0.36$ dır.

Asıl kullanıcı Grover operatörünü uyguladıktan sonra

$$|\phi_0\rangle_A = (-1)^m \left[\sin(2m+1)\theta\,|k\rangle_A + \frac{\cos(2m+1)\theta}{\sqrt{2^n - 1}} \sum_{\substack{j\in\{0,1\}^n \\ j\neq k}} |j\rangle_A\right] \tag{15.18}$$

sin ve cos değerleri 15.18 eşitliğinde yerine yazılırsa

$$|\phi_0\rangle_A = (-1)^m \left[\sin 5\theta\,|k\rangle_A + \frac{\cos 5\theta}{\sqrt{7}} \sum_{\substack{j\in\{0,1\}^3 \\ j\neq k}} |j\rangle_A\right]$$

Aynı zamanda

$$\begin{aligned} |\phi_x\rangle_A &= (-1)^{x.k}\frac{\cos(4L+1)\theta}{\sqrt{2^n-1}}\,|k\rangle_A \\ &+ \sin\theta \sum_{\substack{j\in\{0,1\}^n \\ j\neq k}} \left[(-1)^{j.x} - 4(-1)^{x.k}\frac{\sin\theta}{\sqrt{2^n-1}}\sum_{l=0}^{L-1}\cos(4l+3)\theta\right]|j\rangle_A \end{aligned} \tag{15.19}$$

$m = 2L$, $L \geq 1$ dir. 15.19 da kullanılırsa

$$|\phi_x\rangle_A = (-1)^{x.k}\frac{\cos 5\theta}{\sqrt{7}}\,|k\rangle_A + \sin\theta \sum_{\substack{j\in\{0,1\}^3 \\ j\neq k}} \left[(-1)^{x.j} - 4(-1)^{x.k}\frac{\sin\theta}{\sqrt{7}}\cos 3\theta\right]|j\rangle_A \tag{15.20}$$

elde edilir.

Eğer $k = (000)$ ölçüldüğünü düşünelim. Bu durumda

$$|\phi_0\rangle_A = a_0 |0\rangle_A + a_1 \sum_{\substack{j\in\{0,1\}^3 \\ j\neq k}} |j\rangle_A \tag{15.21}$$

$$|\phi_1\rangle_A = a_1 |0\rangle_A + b\,[c_0(|1\rangle_A + |3\rangle_A + |5\rangle_A + |7\rangle_A) + c_1(|2\rangle_A + |4\rangle_A + |6\rangle_A)] \tag{15.22}$$

elde edilir.

Burada $a_0 \cong 0.9723$, $a_1 \cong -0.08839$, $b \cong 0.3536$, $c_0 \cong -1.25$ ve $c_1 \cong 0.75$ dir.

Yukarıdan da görüldüğü gibi saldırgan $|1\rangle_B$ durumunu gözlemlese dahi $|\phi_1\rangle_A$ doğru sonucu göstermeyecektir. Bu nedenle asıl bilgisayar kullanıcısının yanındaki işbirlikçi A'daki (A yazmacı, $|\phi_1\rangle_A$) ölçüm sonucunu söylese dahi saldırgan doğru cevabı (ölçüm sonucunu) tahmin edemeyecektir (Çünkü $|\phi_1\rangle_A$ doğru sonucu göstermiyor).

# Bölüm 16

# Quantum Yürümeler (Quantum Walks)

Bütün algoritmalar kuantum yürümeden yararlanır. Ayrıca kuantum internet dağıtımında kuantum yürüme kullanılmaktadır.

## Rastgele Yürüme

Bir parçacığın bir graf etrafındaki rastgele hareketini tanımlamaktadır. Kuantum yürüme buna benzemekle beraber buradaki parçacık artık kuantumsal parçacıktır.

## Kuantumsal Parçacık

Kendisini oluşturan iki alt durumu da içeren parçacıktır. Her iki durumda da bulunabilen yani yukarı spin aşağı spin hareketlerini aynı anda sergileyebilmesi gibi.

Rastgele yürüme deterministiktir. Yani bir belirsizlik bulunmaktadır.

## 16.1 Bir Grafta Rastgele Yürüme

**Şekil**

- 3 adımda 5 ve ya 6 ya gidilir.
- 5 veya 6 ya erişme olasılığı eşittir.
- 1 de bulunma olasılığı 1 dir.
- 2 veya 3 de de bulunma olasılığı $\frac{1}{2}$
- 4 te bulunma olasılığı 1 dir.

- 5 veya 6 da bulunma olasılığı $\frac{1}{2}$

3 adımda 5 ve ya 6 ya gidilir. 5 veya 6 ya erişme olasılığı eşittir. 1 de bulunma olasılığı 1 dir. 2 veya 3 de de bulunma olasılığı $\frac{1}{2}$. 4 te bulunma olasılığı 1 dir. 5 veya 6 da bulunma olasılığı $\frac{1}{2}$

## 16.2 Bir Grafta Kuantumsal Yürüme

**Şekil**

- 1 e gelme olasılığı 1 dir. Buradaki 1 genliklerin toplamıdır.
- 2 veya 3 e ulaşılabilir. 2 ye olaşma olasığılı $\frac{i}{\sqrt{2}}$, 3 e ukalma olasılığı $\frac{1}{\sqrt{2}}$.
- 4 e ulaşma olasılığı $\frac{i+1}{\sqrt{2}}$
- 3 adımdan sonra hem 5 hem 6 da kesinlikle vardır. İkisinden birinde 1 dir. Bu aynı yerde bulunuyor. Kuantum yürümede 5 veya 6 dan birinde kesin bulunur. Klasik yürümede ise 5 veya 6 da bulunması kesin değildir. Bunun sebebi (kuanym yürümede 5 veya 6 dan birinde kesin olmasının kauntum interference dır). Kuantum interfrence, fotonun aynı anda farklı yerde bulunma durumudur.

**Not 63.** Bütün olası durumlarda toplam olasılık 1 dir.

## 16.3 Kuantum Yürümenin Matematiksel Tanımı

Kuantum yürümeye en güzel örnek para atma olayıdır. Üzerinde hem yazı hem tura vardır. Gelme olasılıkları toplamı 1 dir.

## 16.4 Bir Çizgi Üzerinde Rastgele Yürüme

**Şekil**

Sonsuz bir graf olarak da değerlendirilebilir. Burada bir noktadan sağa ve sola yürüme olasılığı eşittir. İki adım arasındaki uzaklık $n$ adım sonunda $\sqrt{n}$ dir.

## 16.5 Bir Çizgi Üzerinde Kuantumsal Yürüme

Solda ve aynı zamanda pozisyon durum
Sağda ve aynı zamanda pozisyon durum

$$\begin{aligned} |L\rangle &\rightarrow |L\rangle + i\,|R\rangle \\ |R\rangle &\rightarrow i\,|L\rangle + |R\rangle \\ |L\rangle\,|p\rangle &\rightarrow |L\rangle\,|p-1\rangle \\ |R\rangle\,|p\rangle &\rightarrow |R\rangle\,|p+1\rangle \end{aligned}$$

Klasik yürümedeki tüm graf boyundaki dağılımı **Şekil**
Kuantum yürümedeki tüm graf boyundaki dağılım **Şekil**⟶ pic: her iki yerde aynı anda bulunabilme özelliğinden kaynaklanır.
Grafta kuantum yürüme 2 şekilde olur.

- Yönlü grafta
- Yönlü olmayan grafta→ Kuantum yürüme için $d$ tane para yazı ve turanın para kuantum parçacık, foton örneğidir. 2 özelliği vardır. Parayı tek düşününce hem yazı hem tura özelliğine sahiptir.

## 16.6 Yönlü Olmayan Kuantum Yürüme Davranışı

Kuantum yürüme quadratik olarak daha hızlıdır. Bu artış verilen grafta bir köşeye ulaşma zamanının çok kısa olmasını sağlar. Bu durum kuantum algoritmada sonuca daha hızlı ulaşmasını sağlar.

Bazı graflarda kuantum rastgele yürüme üstel olarak daha hızlıdır. "Bu graf hangisidir?" sorusuna yanıt bulabiliriz. Yanıt bulmak için yönlü graflarda kuantum yürümeden bahsedebiliriz.

Yönlü graflarda önemli olan terslenebilir olmasıdır. Bu da yönlendirilmiş graflarda her bir bileşenin birbiri ile bağlantılı olduğunu göstermektedir.

Terslenemez mühendislik için adımlar atılmak isteniyor. Kuantum yürüme bu bağlamda yol göstermektedir.

## 16.7 Terslenebilen ve Terslenemeyen Graflar

Terslenebilen graflarda başlanan noktaya gelinebilir. Klasik yürümede kesin bir belirlilik görülse bile sonuçta olasılıksal bir durumdur. Kuantumsal durumda ise kesinlik vardır.

Kuantum yürüme ile bir merminin hedefe ulaşıp ulaşamamasında %100 hedefe ulaşması için kuantum yürüme kullanılmalı. Kuantum yürümede daha az alt yapı kullanarak daha kısa sürede yapmak istenen gerçekleştirilir. Kuantum yürüme kuantum algoritmalarda da kullanılmaktadır. Kuantum rastgele yürümenin bir alanı da oyundur.