



**GAZİ ÜNİVERSİTESİ**  
**MÜHENDİSLİK FAKÜLTESİ**  
**BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

**SAİD BERK 21118080070**

**BM311 – BİLGİSAYAR MİMARİSİ**  
**ÖDEV-3**

## İçindekiler

<b>Giriş .....</b>	<b>2</b>
Kuantum Mekanikinin Temelleri.....	2
Kuantum Hesaplamanın Temelleri.....	2
Kuantum Durumlarını Kontrol Etme .....	2
Geleneksel Bilgisayar ile Farkları .....	3
Kuantum Turing Makinesi ve Church – Turing Hipotezi .....	4
Kuantum Paralel Hesaplamanın Tanımı ve Önemi .....	4
<b>Kuantum Mekanik ve Kuantum Bilgisayarlar.....</b>	<b>4</b>
Süperpozisyon ve Dolanıklık (Entanglement).....	4
Süper Pozisyon .....	5
Klasik Korelasyon.....	5
Kuantum Dolanıklık.....	5
Kuantum Bitleri (Qubits) ve Kuantum Kapıları .....	5
Dirac Notasyonu .....	5
Foton Polarizasyonu ile Kübitleri Anlamak.....	6
Kuantum Kapıları .....	7
Tekli Kuantum Kapıları.....	8
Kuantum Not Kapısı.....	8
Z Kapısı .....	8
Hadamard Kapısı.....	8
Çoklu Kuantum Kapıları.....	9
CNOT Kapısı .....	9
Kuantum Devreleri ve Kuantum Algoritmaları .....	10
Kuantum Devreleri .....	10
Klasik Devrelerin Kuantum Devrelerinde Gerçeklenmesi .....	11
Kuantum Algoritmalar .....	12
Shor'un Algoritması .....	12
Grover'in Algoritması.....	12
<b>Kuantum Paralel Hesaplamanın Temelleri .....</b>	<b>12</b>
Kuantum Paralelizminin Matematiksel Temelleri .....	12
Kuantum Paralel Hesaplamanın Klasik Hesaplamadan Farkı .....	13
<b>Kuantum Paralel Hesaplamanın Sınırlamaları Zorlukları ve Potansiyeli .....</b>	<b>13</b>
Kuantum Hata Düzeltme ve Dekoherans.....	13
Kuantum Bilgisayarların Ölçeklenebilirliği .....	14

Kuantum Bilgisayarların Fiziksel Ortamda Gerçeklenmesi .....	14
Kuantum Paralel Hesaplamanın Potansiyel Etkileri .....	15
Kuantum Paralel Hesaplamanın Kriptografi ve Siber Güvenliğe Etkileri .....	15
Kuantum Paralel Hesaplamanın Finansal Modellemeler ve Risk Analizine Etkileri.....	15
Kuantum Paralel Hesaplamanın Makine Öğrenmesi ve Yapay Zekaya Etkileri .....	15
<b>Sonuç</b> .....	<b>15</b>
Araştırma Özeti & Kuantum Paralel Hesaplamanın Önemi ve Sonuçları .....	15
<b>Referanslar</b> .....	<b>16</b>

## Giriş

Kuantum bilgisayarlar, 1980 sonlarında ortaya çıkmaya başlamış, geleneksel mantık ve elektrik alan kullanılarak hesaplama yerine maddenin atom altı tabiatı kullanılarak hesaplama işlemlerinin gerçekleştirilebileceğini öneren teknolojidir. Temel amaçları, klasik bilgisayarların çözmekte zorlandığı veya çok uzun süre aldığı karmaşık hesaplama problemlerini daha hızlı ve verimli bir şekilde çözmektir

### Kuantum Mekaniğinin Temelleri

Kuantum teorisi, insanları en çok etkileyen teorilerden birisi olarak tarihe geçmiştir. 1900'li yılların ilk çeyreğinde ortaya atılan ve temelleri keşfedilen kuantum mekanikleri 1970'lere kadar yalnızca doğayı açıklamak için kullanılan bir teori olarak bilinmiştir. (Nielsen & Chuang, 2010)

Klasik mekanikler sezgisel olarak anlaşılabilir, nesneler insanların tahmin edeceği şekilde hareket ederler. Klasik mekanikleri sezgisel olarak yapan yönü, insanlar ve hayvanlar tarafından her gün hayatta kalmak için kullanılmasıdır. (Susskind & Friedman, 2014)

Kuantum mekanikleri, klasik mekaniklerin açıklayamadığı durumlar (Morötesi kıyamet vs.) araştırılırken keşfedilmiş, doğanın atom altı davranışlarını açıklayan, matematiksel bir çerçevedir. (Nielsen & Chuang, 2010, p. 2)

Kuantum hesaplama teorisi kuantum mekaniği üzerine kurulduğu için kuantum mekaniğinden bağımsız düşünülemez.

### Kuantum Hesaplamanın Temelleri

1970'lerden sonra, öncü isimlerin emekleriyle yalnızca tabiatın gözlemlenebilir bir parçası değil, manipüle edilebilir bir araç olarak kullanılabileceği anlaşılmış durumdadır. Kuantum mekaniklerinin, yalnızca doğada keşfedilebilir bir olgu olmasının yanı sıra tasarlanabilir bir sistem olduğu da kabul edilmektedir (Nielsen & Chaung 2010). Bu kabul; fizik, bilgisayar bilimleri ve bilgi kuramı alanlarıyla aynı anda kesişen pek çok soru ortaya çıkartmıştır.

*“Kuantum hesaplama ve kuantum bilgisi, kuantum mekanik sistemler kullanılarak yapılabilecek bilgi işleme görevlerini çalışma alanıdır.”* (Nielsen & Chuang, 2010, p. 1)

Kuantum hesaplama ve kuantum bilgi kuramlarının hedeflerinden birisinin de kuantum mekanikleri konusunda insanların sezgilerini güçlendirmek ve mekaniklerin öngörülerini insan zihni için daha anlaşılır kılmaktır. (Nielsen & Chuang, 2010, p. 2)

### Kuantum Durumlarını Kontrol Etme

Kuantum hesaplama hedefinin başarılması için kilometre taşlarından birisi olan kuantum durumlarına doğrudan erişim ve manipülasyon, kuantum bilginin kopyalanması işlemleri üzerine çalışmalar devam etmektedir. Bu çabaya *“Tekil Kuantum Sistemler Üzerinde Tam Kontrol”* başlığı verilmiştir (Nielsen & Chuang, 2010, p. 3) . Süper iletken üretimi aşamalarında ve parçacık hızlandırıcılarda kısmi kontrol sağlanmış olsa da hesaplama

yapabilmek için yeterli değildir ve *kısmi kontrol* olarak değerlendirilebilir. Kuantum durumlarını kontrol etmek maksatlı “*Atom Tuzağı*” gibi yöntemler geliştirilmiştir.

### Geleneksel Bilgisayarlar ile Farkları

Geleneksel bilgisayarlar, klasik fizik yasalarını manipüle ederek çalışan, *Evrensel Turing Makinaları* kullanarak tanımlanabilir (Nielsen & Chuang, 2010, p. 3). Kuantum bilgisayarları da klasik bilgisayarlar ile aynı paradigmayı takip eder ve algoritmik olarak çalışır.

Teoride, herhangi bir klasik bilgisayar kuantum bilgisayarını simüle edebilir (yaptığı her işlemi gerçekleştirebilir). Fakat, pratikte bu mümkün değildir. Bu imkansızlığın başlıca sebebi, çeşitli görevler için klasik zamanların gerçekçi olmayan zamana ihtiyaç duymasıdır. Kuantum bilgisayarların geleneksel bilgisayara en göze çarpan avantajı, kuantum bilgisayarların hızıdır (Nielsen & Chuang, 2010, p.5)

Bu bilgiler ışığında, kabiliyetleri açısından yapabilecekleri arasında fark bulunmayan iki tasarım yönetimini birbirinden ayıran asıl özelliğin algoritmayı tamamlamak için ihtiyaç duydukları zaman, bir başka deyişle bilgisayarların hızı yorumu yapılabilir.

### Kuantum Turing Makinesi ve Church – Turing Hipotezi

“(Bir algoritma kullanarak) hesaplanılabilir bütün fonksiyonlar, *Evrensel Turing Makinesi* kullanılarak hesaplanabilir.” İfadesi, Church – Turing Hipotezi olarak bilinir (Church, 1936). Bu hipoteze ek olarak “*Her sonlu bir şekilde gerçekleştirilebilir fiziksel sistem, sonlu araçlarla çalışan evrensel bir model hesaplama makinesi tarafından mükemmel bir şekilde simüle edilebilir.*” Church – Turing Prensibi ile desteklenir. (Deutsch, 1985). Church – Turing prensibine uyan durumlara Güçlü Fiziksel Form denmektedir (Deutsch, 1985).

Klasik Evrensel Turing Makinesi, Güçlü Fiziksel Form’u desteklememesi Kuantum Turing Makinasını oluşturmak için motivasyonlardan birini oluşturur (Deutsch, 1985). Bütün sonlu fiziksel sistemleri mükemmel şekilde simüle edebilen, gerçekleştirilebilir Kuantum Turing Makinesi ( $Q$ ) ideal kapalı (0 Kelvin Sıcaklığında) Ortamlarda gerçekleştirilebilir. (Deutsch, 1985).

Klasik Turing Makinesi gibi Kuantum Turing Makinesi ( $Q$ ) de iki ana bileşenden oluşur: sonlu bir işlemci ve sadece sonlu bir parçası kullanılan sonsuz bir bant. Hesaplama sabit bir  $T$  zamanında yapılır ve her adımda işlemci hafızanın belirli bir kısmında işlem yaparken hafızanın diğer kısımları değişmeden kalır.

Kuantum sistemleri, süperpozisyon gibi kuantum özellikleri nedeniyle sonsuz sayıda olası duruma sahiptir. Bu durumlar, Hilbert Uzayı’ndaki bir vektörle temsil edilebilir.

$$|\Psi(t)\rangle \in H$$

Burada  $H$  Kuantum bilgisayarın durum uzayıdır.

Sonsuz olasılıklara rağmen, herhangi bir anda kuantum bilgisayar sadece sonlu sayıda kubit manipüle eder. Her hesaplama adımında, belirli ve sonlu bir kubit grubuna işlemler uygulanır. Bu sonluluk, matematiksel olarak ifade edilişi:

$$|\psi(nT)\rangle = \mathbf{U}^n |\psi(0)\rangle \quad (n \in \mathbb{Z}^+)$$

n sayısının Pozitif Tam Sayılar kümesinin elemanı olması, sonlu sayıda uniter işlem (kübitlere uygulanacak işlem) olduğunu temsil etmektedir.

Bu işlemler, sonlu boyutlu matrislerle temsil edilir ve hesaplanabilirler. Bu sonlu işlemleri birçok adım boyunca birleştirerek, herhangi bir kuantum sisteminin evrimini simüle edebilir ve böylece sonsuz durum uzayında gezinmiş oluruz.

Böylece kuantum durumlarındaki sonsuz olasılıklara rağmen, her bir hesaplama adımındaki gerçek işlem sadece sonlu ve yönetilebilir bir bilgi miktarını içerir. (Deutsch, 1985, Title 2. Quantum Computers)

### Kuantum Paralel Hesaplamanın Tanımı ve Önemi

Kuantum paralel hesaplama, kuantum bilgisayarların süperpozisyon ilkesini kullanarak aynı anda birden fazla hesaplama yolunu eşzamanlı olarak gerçekleştirebilme yeteneğini ifade eder. Bu, bir kuantum bitinin (kübit) aynı anda hem "0" hem de "1" durumunda bulunabilmesi sayesinde mümkün olur. Süperpozisyon ve dolanıklık gibi kuantum mekanik prensipleri, kuantum bilgisayarların klasik bilgisayarlara kıyasla belirli problemleri çok daha hızlı çözebilmesini sağlar. Kuantum paralelizm, kuantum algoritmalarının temelini oluşturur ve işlem gücünü büyük ölçüde artırır. (Markidis, 2024)

Kuantum bilgisayarı,  $|\Psi_{out}\rangle$  vektörü (output vektörü) için üretilmiş bütün  $C$  stringlerini encode etme (içine veri gömme) yeteneğine sahiptir. Başka bir deyişle,  $2^N$  klasik yolu aynı anda izleyebilir. Bu da birden fazla hesaplama sonucunu tek bir kuantum hesaplama adımıyla encode edebilir. Kuantum bilgisayarın bu yeteneğine "*Kuantum Paralelliği*" denir.  $f(0)$  ve  $f(1)$  için  $\{0,1\} \rightarrow \{0,1\}$  yönlendirmesi aynı anda gerçekleşir.  $\{0,1\} \rightarrow \{0,1\}$  iki fonksiyon için de çıktı durumu bilgileridir. (Djordjevic, 2022, Chapter 5.1 Quantum Parallelism)

Kuantum paralel hesaplama uygulamaları; Kriptografi ve Siber Güvenlik, Optimizasyon Problemleri, Simülasyon ve Modelleme, Yapay Zeka ve Makine Öğrenimi alanlarında kritik öneme sahiptirler. Yukarıdaki başlıklarda tartıştığımız üzere ilgili uygulamaların geçerli bir zaman diliminde gerçekleşmesi için Kuantum Paralel Hesaplama yöntemlerine ihtiyaç duyulur. (Markidis, 2024)

## Kuantum Mekanik ve Kuantum Bilgisayarlar

### Süperpozisyon ve Dolanıklık (Entanglement)

Sistemlerin daha büyük sistemler oluşturmak için birleşmesi, fiziğin araştırma ve uygulama alanlarındandır. (Susskind & Friedman, 2014) Atomlar da kendi başlarına birer kuantum sistemi olan nükleonlar ve elektronlardan oluştuğu gerçeği göz önüne alındığında, birleşmenin kurallarının önemli olduğu göz önünde bulundurulmalıdır.

## Süperpozisyon

Süperpozisyon, kuantum mekaniğinin temel ilkelerinden biridir ve kuantum bilgisayarların klasik bilgisayarlardan farklı çalışmasını sağlayan en önemli özelliklerden biridir. Klasik bilgisayarlarda bilgi, 0 ve 1 gibi belirli durumlarda saklanır. Ancak kuantum bilgisayarlarda, süperpozisyon sayesinde bir sistem aynı anda birden fazla durumu temsil edebilir. Bu, kuantum bilgisayarların aynı anda birçok olasılığı işleyebilmesine olanak tanır (Nielsen & Chaung, 2010)

Kuantum mekaniğinde, bir sistemin durumu bir durum vektörü ile ifade edilir. Bu durum vektörü, sistemin olası tüm durumlarının bir kombinasyonu olabilir. Süperpozisyon, bir kuantum sisteminin bu olası durumların bir karışımında bulunabilmesi anlamına gelir. Örneğin, bir kuantum sisteminin durumu şu şekilde ifade edilebilir:

$$|\psi\rangle = c_1 |A\rangle + c_2 |B\rangle$$

$|A\rangle$  ve  $|B\rangle$  sistemin olası durumlarını temsil eder.  $c_1$  ve  $c_2$  ise olasılık genliklerini temsil etmektedir.  $|c_1|^2 + |c_2|^2 = 1$  durumu her koşulda geçerlidir (Griffiths, 2018).

## Klasik Korelasyon

Korelasyon, iki veya daha fazla değişkenin birlikte nasıl değişim gösterdiğini inceleyen istatistiksel bir ölçümdür. Korelasyon katsayısı ( $r$ ) korelasyon derecesini gösterir ve  $[-1, +1]$  arasında konumlanır.  $r = 0$  ise korelasyon yoktur,  $r = 1$  ise pozitif mükemmel korelasyon vardır ve  $r = -1$  ise negatif mükemmel korelasyon vardır kabulü yapılabilir. (Mukaka, 2012)

## Kuantum Dolanıklık

Kuantum dolanıklık, iki veya daha fazla kuantum sisteminin durumlarının birbirleriyle bağlantılı olduğu özel bir kuantum durumudur (Einstein, Podolsky & Rosen, 1935). Dolanık parçacıklar birbirinden ne kadar uzakta olursa olsun, birinin durumu ölçüldüğünde diğerinin durumu anında belirlenir.

## Kuantum Bitleri (Qubits) ve Kuantum Kapıları

### Kuantum Bitleri (Qubits)

Bit, klasik hesaplama ve klasik bilgi kuramının temel konseptidir. Kuantum hesaplama ve kuantum bilgi kuramı ise *Kuantum Bit* veya kısaca *Qubit* adını verdiğimiz analog bir konsept üzerine inşa edilmiştir. (Nielsen & Chuang, 2010)

Qubitler, belirlenmiş çeşitli özelliklere sahip matematiksel obje olarak tanımlanabilir. Qubitler'in fiziksel dünyada bir karşılığı bulunur. Fakat, işlem kolaylığı açısından çoğunlukla soyut matematiksel bir nesne olarak kabul edilir.

### Dirac Notasyonu

Klasik bitler 0 veya 1 olarak sembolize edilirler, Qubitler ise Dirac Notasyonu kullanarak sembol haline getirilirler.  $|0\rangle$  ve  $|1\rangle$  olarak durumları sembolize edilir.  $|0\rangle$  ve  $|1\rangle$

Qubitlerin baz durumlarıdır. Kuantum enerji seviyelerini temsil eder ve Hilbert Uzayı içerisinde birbirlerine göre Ortogonal (Dik) konumda bulunurlar.

$ 0\rangle$	$\begin{bmatrix} 1 \\ 0 \end{bmatrix}$
$ 1\rangle$	$\begin{bmatrix} 0 \\ 1 \end{bmatrix}$

Matrisleriyle temsil edilirler. (Sakurai & Napolitano, 2017).

Gerçek dünyada bir varlığın durumu net olarak anlaşılabilir. Örneğin bir madeni para ya yazı durumundadır ya da tura. Bu durumun aksine, kuantum mekaniklerinde bir qubit  $|0\rangle$  &  $|1\rangle$  arasında gözlem yapılanaya dek sürekli olarak değişen bir durumda bulunabilir. Gözlemlendiği esnada yalnızca 1 ve 0 değerini alabileceği vurgulanmıştır.

Örnek olarak, Qubit

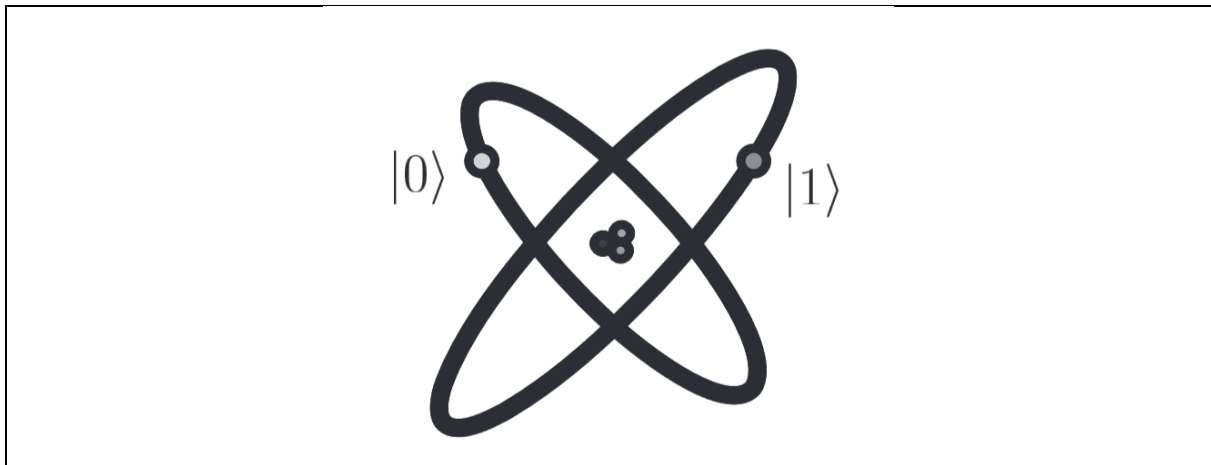
$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

Durumunda olabilir. Bu durum, gözlemlendiğinde %50 oranla 0, %50 oranla 1 sonucu vereceğini göstermektedir. Tuhaf yapılarına karşın, qubitler gerçeklerdir ve doğada bulunurlar. Bu durum deneylerle ispatlanmıştır. (Nielsen & Chuang, 2010)

Qubitlerin gerçekleşmesi hakkında daha net bir fikir sahibi olunması için gerçek hayattaki bazı gerçekleşmeleri incelemek faydalı olabilir.

### Foton Polarizasyonu ile Qubitleri Anlamak

Işık parçacıkları olan fotonların iki farklı polarizasyonu vardır, bunlar düzgün manyetik alandaki nükleer spinlerinin hızı olarak da düşünülebilir. Bir atomdaki elektronlar, düşük enerji seviyesinde (merkeze yakın konum)  $|0\rangle$  (ground) ve yüksek enerji seviyesinde  $|1\rangle$  (excited) olarak iki durumda bulunabilir. Atoma ışık tutulduğunda elektronlarını  $|0\rangle$  seviyesinden  $|1\rangle$  seviyesine yükseltmek doğru koşullar altında mümkündür. Eğer atom  $|1\rangle$  seviyesine ulaşmadan verdiğimiz ışık miktarını azaltırsak *arada bir enerji değerinde* kalır.



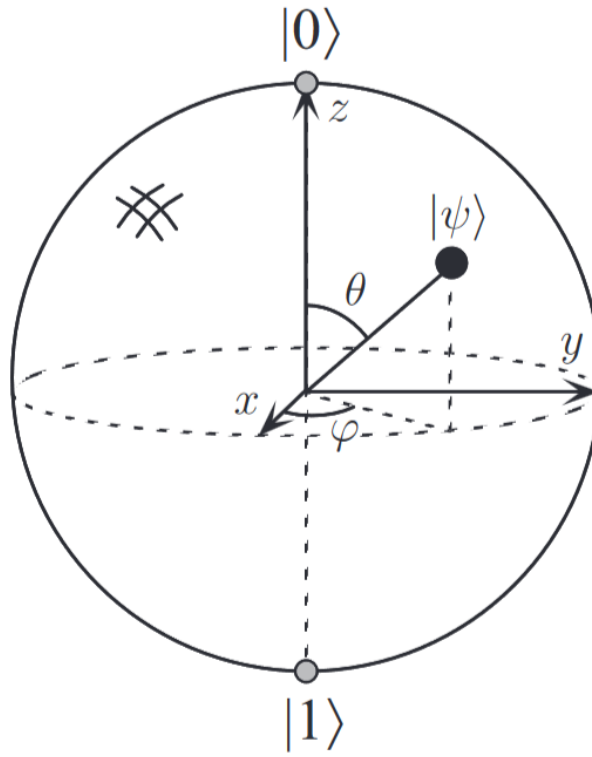


Figür 1. Qubitlerin, atomdaki iki elektronik seviyeyle temsili

$|\psi\rangle$  Sembolü, süperpozisyon vektörüdür. Bir kuantum sisteminin durumunu temsil eder.  $|0\rangle$  ve  $|1\rangle$  durumlarının bir süperpozisyonudur.

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

Süper pozisyonun matematiksel notasyonu



Figür 2. Bloch Gösterimi ile birim çemberde süperpozisyonun geometrik temsili.

Bu gösterimden yola çıkarak bir qubitte sonsuz bilgi saklanabileceği fikrine ulaşılabilir. Bu bağlamda, bütün Shakespeare eserleri bir qubitte tutulabilir yorumu yapılabilir fakat doğru bir mantık olmaz. Qubit gözlemlendiğinde, yalnızca 0 ya da 1 değerini dönecektir ve ölçüm, içinde tuttuğu bilgiyi değiştirir. Böylece gözlemlenmezken tutulan bilgi gözlem esnasında yok olur. (Nielsen & Chuang, 2010)

### Kuantum Kapıları

Kuantum durumundaki değişimler, kuantum hesaplama dili kullanılarak tanımlanabilir. Klasik bilgisayarlar elektrik kabloları ve silikon mantık kapıları içerikleri ile oluşturulurken Quantum devreleri, kablolar ve temel kuantum kapıları kullanarak kuantum bilgisini taşır ve manipüle eder. (Nielsen & Chuang, 2010)

## Tekli Kuantum Kapıları

### Kuantum Not Kapısı

Kuantum not kapıları, klasik not kapılarından farklı olarak, gözlemciye Qubit'in süperpozisyonu hakkında bilgi vermez. Lineer olarak çalışırlar ve deterministiklerdir.

$a | 0 \rangle + b | 1 \rangle$  işlemini  $b | 0 \rangle + a | 1 \rangle$ 'ya dönüştürürler, bir diğer deyişle olasılık katsayılarının yerlerini değiştirirler.

$X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} \alpha \\ \beta \end{bmatrix}$	$X \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix}$
Kuantum Not Kapısı (X)'in Matris Gösterimi	Katsayıların Vektör Gösterimi	Matris Çarpımı ile Vektörün Yer Değiştirmesi

Kuantum kapısının tek kısıtlaması, kapının matris gösteriminin birim matris olması zorunluluğudur. Bu sebepten, herhangi bir birim matris, bir kuantum kapısı olabilir. (Nielsen & Chuang, 2010)

### Z Kapısı

$| 0 \rangle$  katsayısına dokunmaz,  $| 1 \rangle$  katsayısının işaretini değiştir  $-| 1 \rangle$

$Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Z Kapısının Matris Gösterimi

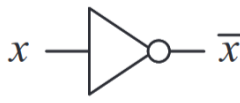
### Hadamard Kapısı

$| 0 \rangle$  durumunu  $| 0 \rangle$  ve  $| 1 \rangle$  arasındaki orta noktaya taşır (enerji seviyesini  $| 1 \rangle$ 'in yarısına kadar artırır)

$| 1 \rangle$  durumunu  $| 0 \rangle$  ve  $| 1 \rangle$  arasındaki orta noktaya taşır (enerji seviyesini  $| 1 \rangle$ 'in yarısına kadar azaltır)

$H \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Hadamard Kapısının Matris Gösterimi

Karekök Not Kapısı olarak da bilinir.

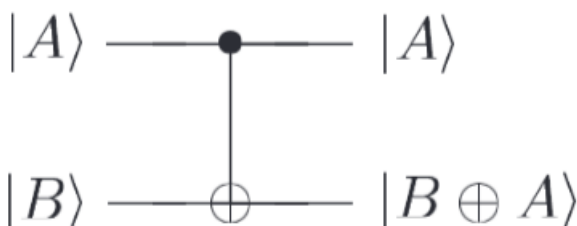
	<table><tr><td><math>\alpha  0\rangle + \beta  1\rangle</math></td><td><math>\xrightarrow{X}</math></td><td><math>\beta  0\rangle + \alpha  1\rangle</math></td></tr><tr><td><math>\alpha  0\rangle + \beta  1\rangle</math></td><td><math>\xrightarrow{Z}</math></td><td><math>\alpha  0\rangle - \beta  1\rangle</math></td></tr><tr><td><math>\alpha  0\rangle + \beta  1\rangle</math></td><td><math>\xrightarrow{H}</math></td><td><math>\alpha \frac{ 0\rangle+ 1\rangle}{\sqrt{2}} + \beta \frac{ 0\rangle- 1\rangle}{\sqrt{2}}</math></td></tr></table>	$\alpha  0\rangle + \beta  1\rangle$	$\xrightarrow{X}$	$\beta  0\rangle + \alpha  1\rangle$	$\alpha  0\rangle + \beta  1\rangle$	$\xrightarrow{Z}$	$\alpha  0\rangle - \beta  1\rangle$	$\alpha  0\rangle + \beta  1\rangle$	$\xrightarrow{H}$	$\alpha \frac{ 0\rangle+ 1\rangle}{\sqrt{2}} + \beta \frac{ 0\rangle- 1\rangle}{\sqrt{2}}$
$\alpha  0\rangle + \beta  1\rangle$	$\xrightarrow{X}$	$\beta  0\rangle + \alpha  1\rangle$								
$\alpha  0\rangle + \beta  1\rangle$	$\xrightarrow{Z}$	$\alpha  0\rangle - \beta  1\rangle$								
$\alpha  0\rangle + \beta  1\rangle$	$\xrightarrow{H}$	$\alpha \frac{ 0\rangle+ 1\rangle}{\sqrt{2}} + \beta \frac{ 0\rangle- 1\rangle}{\sqrt{2}}$								
Figür 4. Klasik Not Kapısı ve Bilinen Kuantum Kapılarının Yan Yana Karşılaştırılması										

Teoride sonsuz sayıda birim matris olacağından sonsuz adet tekli qubit kapısı olduğu varsayımı yanlış değildir. Fakat, gerçek hayatta karşılığı yoktur. (Nielsen & Chuang, 2010)

### Çoklu Kuantum Kapıları

#### Controlled Not (CNOT) Kapısı

İki adet qubiti input olarak kabul eden kapı (kontrol qubiti ve hedef qubit) eğer kontrol qubit'in değeri 0 ise target qubit değerini değiştirmez. Eğer kontrol qubitinin değeri 1 ise hedef qubitinin değeri takla attırılır. (0 -> 1 ya da 1->0) (Nielsen & Chuang, 2010). Kapı, çalışma mantığı olarak T Flip Flop'a benzetilebilir

<p>controlled-NOT</p> 	$U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
CNOT Kapısının Şematik Gösterimi	CNOT Kapısının Matris Gösterimi

$ 00\rangle \rightarrow  00\rangle;  01\rangle \rightarrow  01\rangle;  10\rangle \rightarrow  11\rangle;  11\rangle \rightarrow  10\rangle$
CNOT Kapısının Çalışma Prensipleri

*CNOT Kapısının asıl kullanım amacı, qubitler arasında dolanıklık oluşturmaktır.*

## Kuantum Devreleri ve Algoritmaları

### Kuantum Devreleri

Kuantum devrelerinde kullanılan çizgiler, kabloları temsil etmektedir fakat bu kablolar fiziksel kablolar olarak düşünülmemelidir. Işığın uzayzamanda izleyeceği yol gibi soyut ve zaman boyutunda yapılacak hareketlerin vektörel gösterimi olabilir.

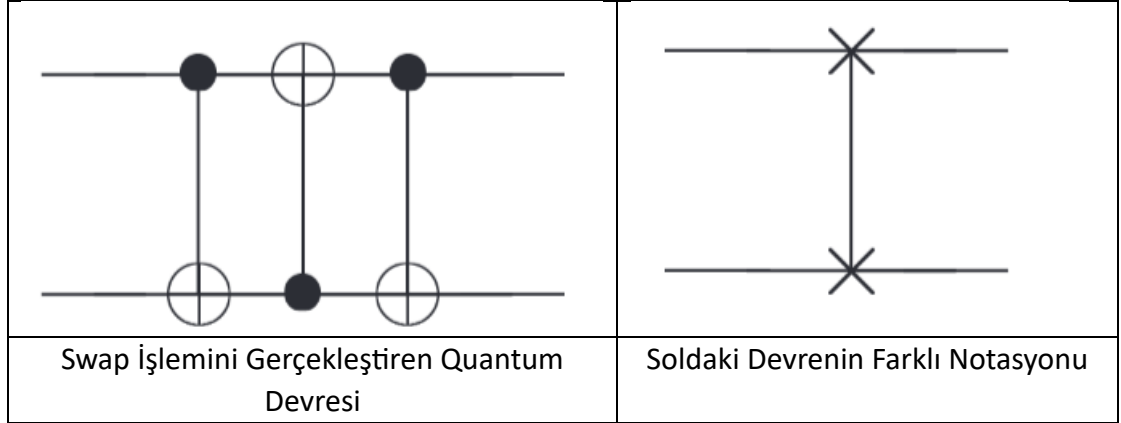
Kuantum devrelerini anlamak için bir örnek işlemden gitmek faydalı olacaktır.

$$\begin{aligned}
 |a, b\rangle &\longrightarrow |a, a \oplus b\rangle \\
 &\longrightarrow |a \oplus (a \oplus b), a \oplus b\rangle = |b, a \oplus b\rangle \\
 &\longrightarrow |b, (a \oplus b) \oplus b\rangle = |b, a\rangle,
 \end{aligned}$$

Kuantum swap işlemi

Kuantum swap işlemi, iki input qubit'in enerji seviyelerini birbirlerinininkile değiştirir. Bu işlem için:

1. a ve b CNOT kapısına girmeli.
2. Sonuç, a ile tekrar CNOT kapısına girmeli.
3. 2. Aşamada bulunan değer, (a CNOT b) işlemi ile CNOT kapısına girmeli.
4. Swap işlemi tamamlandı. (Nielsen & Chuang, 2010)



### Klasik Devrelerin Kuantum Devrelerinde Gerçeklenmesi

Kuantum devreler üzerinde klasik devreler gerçekleştirilebilir, bir başka deyişle klasik devrelerde yapılabilen bütün işlemler kuantum devreler üzerinde de yapılabilir.

Klasik devrelerdeki kapıların terslenemez özelliğe sahip olması (Yarı iletken tabiatı sebebiyle) ve Kuantum devrelerdeki bütün kapıların terslenebilir özelliğe sahip olması (birim matris

temsili) sebebiyle Kuantum devreler doğrudan klasik devreler gibi kullanılamaz. (Nielsen & Chuang, 2010)

Herhangi bir klasik devre, mantığı değişmeksizin bütün elemanları terslenebilir bileşenlerle değiştirilerek tekrar bir eş devreye dönüştürülebilir. Bu dönüşümde Toffoli kapısı kullanılır.

Toffoli kapısı, kendisi terslenebilir kapılardan oluşmasına karşın, terslenemez bir yapı oluşturur.

Inputs			Outputs		
$a$	$b$	$c$	$a'$	$b'$	$c'$
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

Toffoli kapısı kullanılarak kuantum devre üzerinde NAND kapısı gibi davranan bir bileşen taklit edilir. NAND kapısı evrensel bir kapı olduğundan, bütün devreler NAND kapısıyla dolayısıyla da Toffoli kapısıyla gerçekleştirilebilir. Toffoli kapısının kendisi klasik devre bileşeni olarak kabul edilmesine karşın, Kuantum devrelerde de oluşturulabilir. (Nielsen & Chuang, 2010) Çalışma şekli, özetle,  $a$  ve  $b$ 'nin ikisi de 1 olmadığı sürece  $c$ 'nin durumunun değişmeyeceği olarak ifade edilebilir.

Toffoli kapısı sayesinde, Kuantum devreler klasik devrelerin yapabildiği her görevi yapabilir duruma gelmiştir.

## Kuantum Algoritmalar

### 1. Shor'un Algoritması

Shor'un algoritması, asimptotik olarak klasik algoritmalara göre üstel bir hızlanma sağlayarak asal çarpanlara ayırma problemini çözen bir kuantum algoritmasıdır. Bu algoritma, özellikle modern kriptografi sistemlerinin (örneğin **RSA**) güvenliğini tehdit eden en önemli kuantum algoritmalarından biridir.

#### Problemin Tanımı

Verilen bir  $N$  sayısını asal çarpanlarına ayırmak. Örneğin,  $N = 15$  için  $15 = 3 \times 5$

### Probleme Klasik Yaklaşım

1. Rastgele bir  $\alpha$  sayısı seçilir.
2. Eğer  $\text{ebob}(\alpha, N) \neq 1$  bu durumda  $\alpha$  ve  $N$  zaten ortak bir bölene sahiptir. Eğer 1'e eşit olsaydı aralarında asal olmuş olacaktı.

### Probleme Kuantum Yaklaşımı

$$f(x) = a^x \% N$$

fonksiyonun periyodu aranır. Bu, kuantum bilgisayarın süperpozisyon ve Fourier dönüşümü işlemleriyle yapılır.  $O((\log N)^3)$  zaman karmaşıklığına sahiptir. (Nielsen & Chuang, 2010)

### 2. Grover'in Algoritması

Grover'in algoritması, bir veri tabanında arama yapma problemini çözmek için geliştirilmiş bir kuantum algoritmasıdır. Klasik algoritmalara kıyasla karekök hızlanması sağlar.

### Problemin Tanımı

Verilen bir veri tabanı (veya bir fonksiyon) içinde belirli bir öğeyi bulmak.

### Probleme Kuantum Yaklaşımı

1. Kuantum bilgisayar, tüm olası durumların süperpozisyonunu oluşturur. Bu,  $N$  öğenin eşit olasılıkla temsil edildiği bir kuantum durumu yaratır.
2. Bir "oracle" fonksiyonu, hedef öğeyi işaretler. Bu işlem, hedef öğenin fazını ters çevirir.
3. Hedef öğenin olasılığını artırmak için kuantum girişim kullanılır. Bu işlem, hedef öğenin olasılığını artırırken diğer öğelerin olasılığını azaltır.

Grover'in algoritması, klasik algoritmaların  $O(N)$  karmaşıklığına kıyasla kuantum bilgisayarda  $O(\sqrt{N})$  karmaşıklığa sahiptir. Bu, büyük veri tabanlarında gözle görülür bir performans farkı sağlar. (Nielsen & Chuang, 2010)

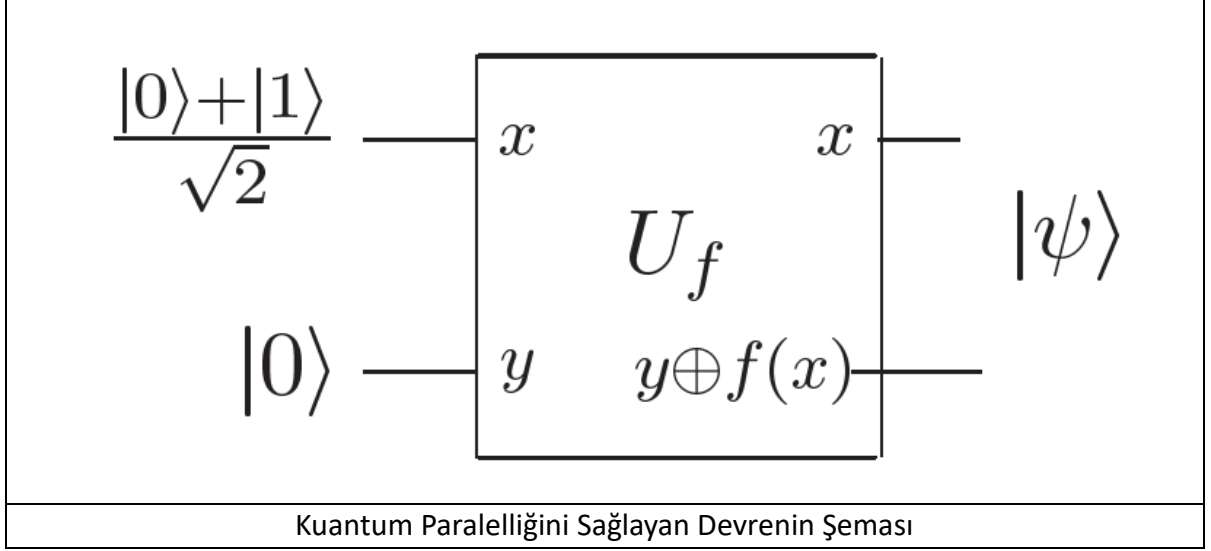
### Kuantum Paralel Hesaplamanın Temelleri

Kuantum paralelliği, kuantum algoritmalarını oluşturan esas özelliklerdendir. Kuantum paralelliği, ilgili  $f(x)$ 'in pek çok farklı  $x$  değerleri için aynı anda hesap yapabilmesidir

### Kuantum Paralelizminin Matematiksel Temelleri

$f(x) : \{0, 1\} \rightarrow \{0, 1\}$  denklemini ele alalım. Bu probleme yaklaşımın uygun yolu şu şekilde verilebilir:

- 2 qubit'li  $|x, y\rangle$  yapısına sahip başlangıç koşulu oluşturulur.
- Doğru bir kuantum devresiyle  $|x, y \oplus f(x)\rangle$  durumuna geçiş sağlanır.
- $f(x)$  ve  $f(y)$ 'nin eş zamanlı hesaplanması sağlanmış olur.
- $x = 0, y = 1$  için Kuantum Paralelliği:



- X inputu,  $|0\rangle$  'ın Hadamard Kapısı'ndan geçirilmesiyle elde edilebilir.

$$\frac{|0, f(0)\rangle + |1, f(1)\rangle}{\sqrt{2}}$$

F Uniter İşlemi Uygulandığında Elde Edilen Sonucun Matematiksel Gösterimi

Algoritmanın bu durumda olması hesaplayıcı için istenen bir durumdur. İçinde hem  $|f(0)\rangle$  hem de  $|f(1)\rangle$ 'in bilgisini barındırır. Bu işlem aynı zamanda gerçekleştiği için Kuantum Paralelliği sağlanmış olur. (Nielsen & Chuang, 2010)

#### Kuantum Paralelizminin Klasik Paralelizmden Farkı

Klasik paralelizmde, paralelizm sağlanmak için aynı görev birden fazla devreye aynı anda verilir, kuantum paralelizminde tek bir devre birden fazla  $x$  değeri için aynı anda hesaplama yapar. (Nielsen & Chuang, 2010)

#### Kuantum Paralel Hesaplamanın Sınırları, Zorlukları ve Potansiyeli

Kuantum bilgisayarların matematiksel teoriden gerçek dünyaya gerçekleştirmesi karmaşık bir mühendislik problemidir. Çeşitli zorluklar ve sınırlar ortaya çıkartır.

#### Kuantum Hata Düzeltme ve Dekoherans

Hangi fiziksel sistemler kuantum bilişim için uygundur sorusunun cevabını bulmak için anlaşılması gereken asıl konsept, Kuantum Gürültüsü veya bir başka deyişle Dekoherans'tır.

Dekoherans, bir kuantum sisteminin çevresiyle etkileşimi sonucu kuantum süperpozisyon durumlarının bozulmasıdır (Schlosshauer, 2005).

Her ne kadar kağıt üzerinde mükemmel çalışan bir sistem çizmek mümkün olsa da bir kuantum hesaplayıcıda pek çok kaynaktan oluşan gürültü ve hata oluşur. Örnek vermek gerekirse:

Atomun iki farklı seviyesinde temsil edilen bir kübiti ışık kullanarak manipüle edilmesi istendiğinde iki farklı seviye dışında başka seviyelere taşan bir temsil mümkün olur ve hesaplar bozulur.

Bu durum, gürültü işleme olarak da bilinir. (Nielsen & Chuang, 2010)

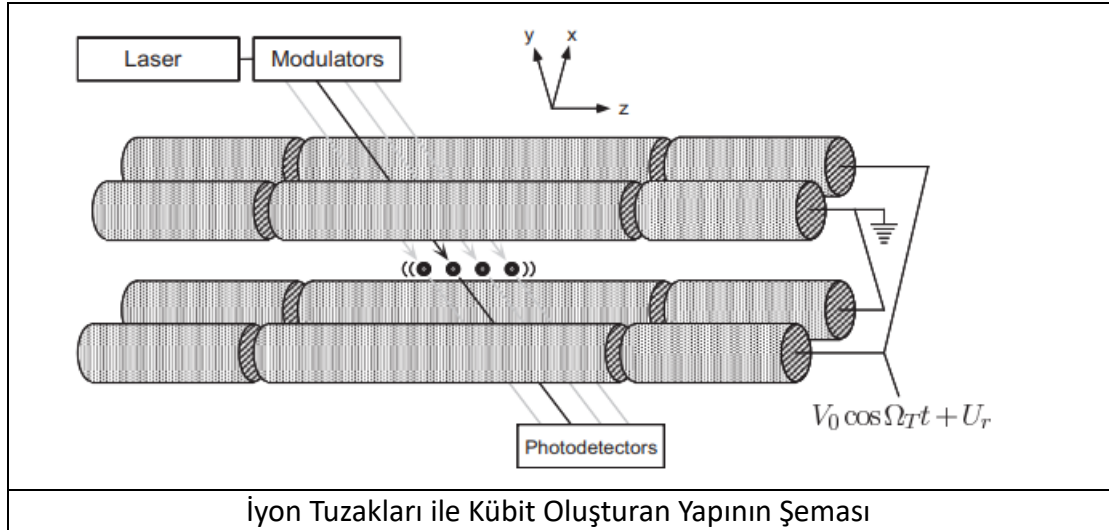
### Kuantum Bilgisayarların Ölçeklenebilirliği

Kuantum bilgisayarlar, kuantum mekaniğinin süperpozisyon ve dolanıklık gibi özelliklerini kullanarak belirli hesaplamaları klasik bilgisayarlardan daha hızlı gerçekleştirebilir (Nielsen ve Chuang, 2010). Ancak, laboratuvar ölçeğinde gerçekleştirilen kuantum sistemleri, pratik uygulamalar için yeterli değildir ve bu teknolojinin ölçeklendirilmesi gerekmektedir (Preskill, 2018).

Ölçeklenebilirlik, bir sistemin boyut ve kapasitesinin artırılmasıyla performansının orantılı olarak artmasıdır (Ladd ve diğerleri, 2010). Kuantum bilgisayarlarda, kubit sayısının artırılmasıyla birlikte sistemin işlevselliğinin korunması ve hata oranlarının kabul edilebilir seviyelerde tutulması elde edilmek istenen asıl durumdur.

### Kuantum Bilgisayarların Fiziksel Ortamda Gerçeklenmesi

- **Süperiletken Kubitler:** Süperiletken devreler, düşük sıcaklıklarda çalıştırılarak kubitler oluşturulabilir (Clarke ve Wilhelm, 2008). Google ve IBM gibi şirketler, bu teknoloji ile 50'den fazla kubitte oluşan sistemler geliştirmişlerdir (Arute ve diğerleri, 2019).
- **İyon Tuzakları:** Yakalanmış iyonlar, lazerlerle kontrol edilerek kubit olarak kullanılabilir (Blatt ve Wineland, 2008). Bu sistemler yüksek koherens sürelerine sahiptir ancak ölçeklendirilmesi zordur.





## Kuantum Paralel Hesaplamanın Potansiyel Etkileri

### Kuantum Paralel Hesaplamanın Kriptografi ve Siber Güvenliğe Etkileri

Kuantum bilgisayarlar, RSA ve ECC gibi günümüzün kriptografik algoritmalarını kırmak için kullanılabilir (Shor, 1994). Shor'un algoritması, büyük sayıların çarpanlarına ayrılmasını üstel bir hızlanma ile gerçekleştirir, bu da mevcut güvenlik protokollerini tehdit eder. Bu nedenle, post-kuantum kriptografi alanında yeni algoritmalar geliştirilmesi gerekmektedir (Bernstein, 2009).

### Kuantum Paralel Hesaplamanın Finansal Modellemeler ve Risk Analizine Etkileri

Finansal piyasaların karmaşık doğası, hızlı ve etkin hesaplama yöntemlerine ihtiyaç duyar. Kuantum hesaplama, portföy optimizasyonu ve risk analizi gibi alanlarda önemli katkılar sağlayabilir (Orús ve diğerleri, 2019).

### Kuantum Paralel Hesaplamanın Makine Öğrenmesi ve Yapay Zekaya Etkileri

Kuantum bilgisayarlar, belirli makine öğrenmesi algoritmalarının hızlandırılmasında kullanılabilir (Biamonte ve diğerleri, 2017). Kuantum destekli öğrenme algoritmaları, büyük veri kümelerinin işlenmesini ve desen tanımayı kolaylaştırabilir.

## Sonuç

### Araştırma Özeti & Kuantum Paralel Hesaplamanın Önemi ve Sonuçları

Kuantum bilgisayarları, doğadaki deterministik olmayan parçacıkları hesaplama amaçları güderek manipüle etmek için çok başarılı bir teknoloji. Olasılıklı tabiatı sayesinde aynı anda farklı durumlarda bulunabiliyor ve bu deterministik olmayan yapısı sayesinde aynı problemin farklı noktaları ek bir donanım gereksinimine ihtiyaç duymadan hesaplanabiliyor. Durum katsayıları üzerinde yapılan değişiklikler ile de kuantum devreler üzerinde klasik devrelerde gerçekleştirilebilen bütün işlemler simüle edilebiliyor.

Bu araştırma, bilgisayar kavramına bakış açımı fazlasıyla genişletti ve abaküse neden bilgisayar dediğimizi daha iyi anlamamı sağladı. Doğada bulunan ve manipüle edilebilen her parçacığın bilgi saklama ve bilgi işleme için kullanılabileceğini fark etmek beni yalnızca klasik bilgisayarlar perspektifinden oluşan dar vizyondan çıkardı ve bilgi teorisi ile hesaplama teorisini daha iyi özümsememi sağladı. Kuantum evrenin dezavantaj gibi gözüken sezgilerden uzak doğasını tam olarak anlamamış olsak bile ondan faydalanabileceğimiz konusunda da beni ikna etmiş oldu.

Kuantum paralelizminin klasik paralelizme göre çok daha az kaynak gerektirdiğini ve daha tutarlı bir süre içinde hesaplamalarını tamamlayabildiğini anlamamı sağladı. Kuantum paralelizmini gerçeklerken çok kübitli sistemlerde oluşabilecek hataları görmemi sağladı.

Faydaları olduğu kadar zararları ve tehditleri hakkında fikir sahibi olmama da yol açtı. Kuantum bilgisayarlarının muhteşem paralellik yeteneğinin medeniyetimizin sıkı sıkıya bağlı olduğu Kriptoloji & Güvenlik protokolleri için nasıl büyük bir tehdit olduğunu, aynı anda birden fazla veriyi işleme yetenekleri sayesinde Makine öğrenimi ve Yapay zeka konusunda bizi Yapay Genel Zeka (AGI) hedefine daha da yaklaştırabilecek bir hesaplama teknolojisi olduğunu fark etmeme ortam sağlamış oldu.

## REFERANSLAR

1. **Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., ... & Martinis, J. M.** (2019). *Quantum supremacy using a programmable superconducting processor*. *Nature*, 574(7779), 505-510.
2. **Bell, J. S.** (1964). "On the Einstein Podolsky Rosen Paradox". *Physics Physique Физика*, 1(3), 195-200.
3. **Bernstein, D. J.** (2009). Introduction to post-quantum cryptography. In *Post-Quantum Cryptography* (pp. 1-14). Springer.
4. **Biamonte, J., Wittek, P., Pancotti, N., Rebentrost, P., Wiebe, N., & Lloyd, S.** (2017). *Quantum machine learning*. *Nature*, 549(7671), 195-202.
5. **Blatt, R., & Wineland, D.** (2008). Entangled states of trapped atomic ions. *Nature*, 453(7198), 1008-1015.
6. **Church, A.** (1936). An unsolvable problem of elementary number theory. *American Journal of Mathematics*, 58(2), 345–363. <https://doi.org/10.2307/2371045>
7. **Clarke, J., & Wilhelm, F. K.** (2008). Superconducting quantum bits. *Nature*, 453(7198), 1031-1042.
8. **Deutsch, D.** (1985). Quantum theory, the Church-Turing principle and the universal quantum computer. *Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences*, 400(1818), 97–117. <https://doi.org/10.1098/rspa.1985.0070>
9. **Djordjevic, I. B.** (2022). *Quantum communication, quantum networks, and quantum sensing*. Academic Press. <https://doi.org/10.1016/C2019-0-05028-5>
10. **Griffiths, D. J.** (2018). *Introduction to Quantum Mechanics*. Cambridge University Press.
11. **Ladd, T. D., Jelezko, F., Laflamme, R., Nakamura, Y., Monroe, C., & O'Brien, J. L.** (2010). Quantum computers. *Nature*, 464(7285), 45-53.
12. **Markidis, S.** (2024). What is quantum parallelism, anyhow? *arXiv:2405.07222*. <https://doi.org/10.48550/arXiv.2405.07222>
13. **Mukaka, M. M.** (2012). "A guide to appropriate use of correlation coefficient in medical research". *Malawi Medical Journal*, 24(3), 69-71.
14. **Nielsen, M. A., & Chuang, I. L.** (2010). *Quantum computation and quantum information*. Cambridge University Press.
15. **Orús, R., Mugel, S., & Lizaso, E.** (2019). Quantum computing for finance: Overview and prospects. *Reviews in Physics*, 4, 100028.
16. **Preskill, J.** (2018). Quantum computing in the NISQ era and beyond. *Quantum*, 2, 79.
17. **Sakurai, J. J., & Napolitano, J.** (2017). *Modern Quantum Mechanics*. Cambridge University Press.
18. **Schlosshauer, M.** (2005). Decoherence, the measurement problem, and interpretations of quantum mechanics. *Reviews of Modern Physics*, 76(4), 1267.
19. **Shor, P. W.** (1994). Algorithms for quantum computation: discrete logarithms and factoring. *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, 124-134.

20. **Susskind, L., & Friedman, A.** (2014). *Quantum mechanics: The theoretical minimum*. Basic Books.