KUANTUM BİLGİSAYARLARI

Dr. Mahir E. Ocak [*TÜBİTAK Bilim ve Teknik Dergisi*

Günümüzde bilgiyi işlemek ve aktarmak için kullanılan makinelerin çalışma ilkeleri klasik mekanikle tam anlamıyla açıklanabilir. Ancak klasik mekanik sadece günlük hayatta aşina olduğumuz makro ölçekte geçerli bir kuramdır, maddeye giderek daha küçük ölçeklerde bakıldığında geçerliliğini yitirdiği görülür. Temel parçacıkların, atomların ve moleküllerin davranışları klasik mekanikle değil kuantum mekaniğiyle açıklanır.

Klasik mekaniğin aksine kuantum mekaniği her ölçekte geçerli bir kuramdır. Mikro ölçekten başlayarak giderek daha büyük ölçekte sistemlerde uygulandığında geçerliliğini yitirmez, makro ölçekte de geçerlidir. Ancak sistem giderek büyüdükçe, sistemin bir bütün olarak davranışları giderek klasik mekanik yasalarıyla daha uyumlu hale gelir. Başka bir deyişle, klasik mekaniğin kuantum mekaniğinin bir limit durumu olduğu söylenebilir. Dolayısıyla çalışma ilkeleri kuantum mekaniğiyle açıklanan makinelerin, bilgiyi işlemede ve aktarmada çalışma ilkeleri klasik mekanikle açıklanan makinelerden çok daha verimli olabileceğini söylemek yanlış olmaz. Bu sebepten dolayı, yıllardır kuantum bilgisayarları geliştirmek için çalışmalar yapılıyor. Bugün gelinen noktada kuantum bilgisayarlarının hâlâ emekleme evresinde olduğu söylenebilir. Ancak hem kuramsal hem de deneysel araştırmalar yoğun bir biçimde devam ediyor. *IBM quantum experience* projesi kapsamında geliştirilmiş 20 kübitlik (kuantum bit) bir kuantum bilgisayarı var ve kuantum bilişim deneylerinde kullanılabiliyor. Hatta IBM yakın gelecekte 50 kübitlik bir kuantum bilgisayarı üretip kullanıma açacağını duyurdu. Ayrıca kuantum bilgisayarları kullanarak belirli soruları çözmek için geliştirilmiş algoritmalar var. Büyük ölçekte (çok sayıda kübit içeren) kuantum bilgisayarları geliştirildiğinde bu algoritmalarla klasik bilgisayarların çözmekte zorlandığı pek çok problemin kolaylıkla çözülebileceği düşünülüyor.

Kuantum Bilgisayarlarının Gerçeğe Dönüştürülmesi

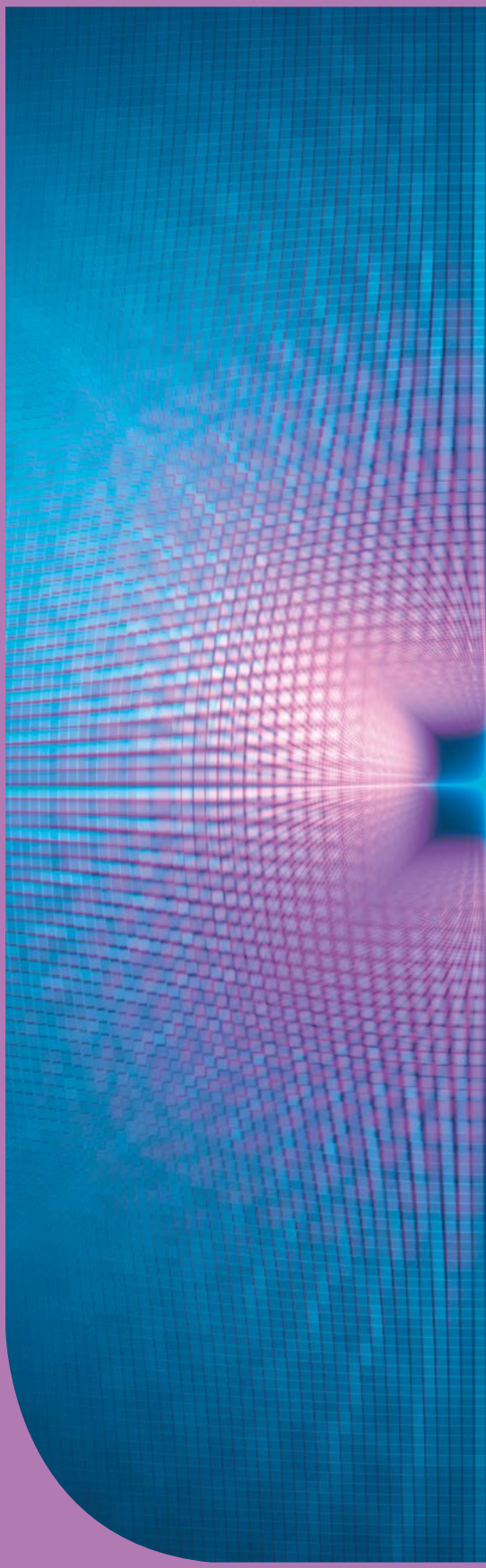
Bir bilgisayarın kuantum mekaniği ilkelerine uygun biçimde çalışıp anlamlı sonuçlar vermesi için sağlaması gereken beş koşul var.

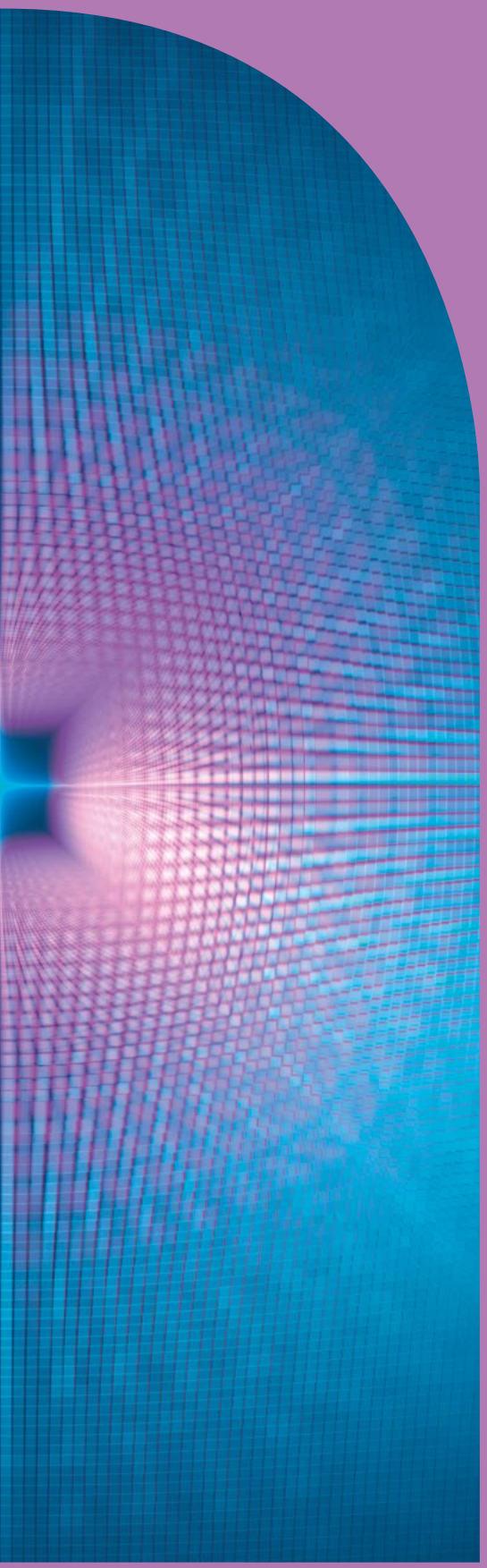
Arzu edilen ölçekte üretilebilecek, iyi karakterize edilmiş kübitler içeren bir fiziksel sistem

Klasik bilgisayarlarda bilgiyi depolamak için kullanılan en küçük birimlere bit denir. Bir bitin sahip olabileceği iki değer vardır: 0 ve 1. Bir bitin herhangi bir andaki değeri ya 0 ya da 1'dir. Kuantum bilgisayarlarındaki bitleri (kübitleri) klasik bilgisayarların bitlerinden ayıran en önemli fark, kübitlerin süperpozisyon durumunda da olabilmeleridir. Bir kübitin sahip olabileceği iki ayrı durumu $|0\rangle$ ve $|1\rangle$ olarak gösterelim. Kübitler de klasik bitler gibi $|0\rangle$ ve $|1\rangle$ durumlarında bulunabilirler. Ancak klasik bitlerin aksine kübitlerin herhangi bir süperpozisyon durumunda bulunması da mümkündür. a ve b iki karmaşık sayı olmak üzere süperpozisyon durumları $a|0\rangle+b|1\rangle$ olarak ifade edilebilir. a'nın ve b'nin sağlaması gereken tek koşul $|a|^2+|b|^2=1$'dir ve bu koşulu sağlayan sonsuz ayrı kombinasyon vardır. Süperpozisyon kuantum mekaniğini klasik mekanikten ayıran en önemli olgulardan biridir. Klasik mekaniğin "iyi çalıştığı" günlük hayatta süperpozisyon durumlarına tanık olmayız. Örneğin bir aracın iki nokta arasında yolculuk etmek için kullanabileceği iki ayrı rota varsa ya birini takip eder ya da diğerini. Mikro dünyadaysa bir parçacığın takip ettiği rotanın, spininin ya da başka bir özelliğinin süperpozisyon durumunda olması mümkündür.

n tane kübit içeren bir kuantum bilgisayarındaki kübitlerin durumu, aynı sayıda bit içeren bir klasik bilgisayardaki bitlerin bulunabilecekleri 2^n ayrı durumun bir süperpozisyonudur. Örneğin iki bitin bulunabileceği $2^2=4$ ayrı durum vardır: 00, 01, 10, 11. İki kübitin genel durumuysa dört ayrı durumun bir süperpozisyonudur: $a|00\rangle+b|01\rangle+c|10\rangle+d|11\rangle$. Kübitlerin durumu genel olarak birbirine "dolanık"tır, yani birbirilerinden bağımsız değildir. *n* tane bit içeren bir klasik bilgisayardaki bitlerin durumunu ifade etmek için *n* tane 0 ya da 1 yeterlidir. *n* tane kübit içeren bir kuantum bilgisayarındaki kübitlerin durumunu ifade etmek içinse 2^n tane karmaşık sayı gerekir.

İki seviyeli herhangi bir sistem, kübit olarak kullanılabilir. Bugüne kadar öne sürülmüş pek çok fikir var ve bugün de bu konu üzerine araştırmalar devam ediyor. Üzerine en çok çalışma yapılan kuantum bilgisayarı türlerinden biri iyon-kapanı kuantum bilgisayarları. Bu bilgisayarlarda, elektrik ve manyetik alanlar yardımıyla belirli hacimlerin içine hapsedilen iyonlar kübit işlevi görür. İyonun en düşük enerji seviyesinde olması $|0\rangle$ durumuna, uyarılmış bir enerji seviyesinde olmasıysa $|1\rangle$ durumuna karşılık gelir. Benzer biçimde fotonların varlığı ya da yokluğu, elektronların varlığı ya da





yokluğu, atomların spinlerinin yukarı ya da aşağı olması, elektronların spinlerinin yukarı ya da aşağı olması da |0> ve |1> durumlarını kodlamak için kullanılabilir.

Bir kübitin bir kuantum bilgisayarı içerisinde tam olarak işlevini yerine getirebilmesi için özelliklerinin çok iyi karakterize edilmiş olması gerekir. Kübitlerin enerji seviyeleri, birbirleriyle ve harici elektrik ve manyetik alanlarla etkileşimleri çok iyi bilinmelidir. Ayrıca kübitin üçüncü, dördüncü, ... seviyeleri varsa, kübitleri kontrol eden mekanizmaların bu seviyelere geçişe imkân vermeyecek şekilde tasarlanması gerekir.

Kübitlerin durumunu bir referans durumuna dönüştürebilmek

Kübitlerin herhangi bir işlemde kullanılmadan önce belirli bir başlangıç durumuna (|0>) getirilebilmeleri gerekir. Ayrıca işlemler sırasında meydana gelebilecek hataları düzeltmek için öne sürülmüş algoritmalar da sürekli olarak |0> durumunda kübitler oluşturulabilmesini gerektirir.

Kübitlerin durumunun referans durumuna dönüştürülmesinde kullanılabilecek çeşitli yöntemler var ve bu yöntemler doğal olarak kübitin türüne göre değişiyor. Örneğin |0> durumu kübitin temel enerji seviyesiyse, kübit doğal olarak enerji yayarak soğuyabilir ve uyarılmış bir enerji seviyesinden temel enerji seviyesine inebilir. Ayrıca kübit üzerinde ölçüm yaparak referans durumuna dönüşmesini sağlamak da mümkündür. Bilginin spin durumlarında kodlandığı kübitler için önerilmiş başka bir yöntemse güçlü manyetik alanlar kullanarak spinlerin manyetik alan yönünde hizalanmasını sağlamak.

Geçitlerin işlem zamanından daha uzun *decoherence* zamanları

Bir kübitin işlevini yerine getirebilmesi için kontrolsüz bir biçimde çevresiyle etkileşmemesi gerekir. Çünkü bu etkileşimler kübitte depolanmış bilginin kaybolmasına neden olur. *Decoherence* olarak adlandırılan bu süreç, kuantum mekaniksel bir sistemin klasik davranışlar göstermeye başlamasına (süperpozisyon durumlarının yok olmasına) sebep olan temel mekanizmadır. Dolayısıyla bir kuantum bilgisayarının bir klasik bilgisayardan daha iyi performans gösterebilmesi için, klasik davranışların ortaya çıkma süresinin (*decoherence* zamanının) yeteri kadar uzun olması gerekir. Ne kadar sürenin yeteri kadar uzun olduğu sadece sistemin özelliklerine değil aynı zamanda kullanılan hata düzeltme algoritmalarına da bağlıdır.

Bir kuantum bilgisayarının yapacağı işlemlerin süresi uzadıkça *decoherence*'ın giderek daha önemli bir sorun haline geleceği düşünülebilir. Ancak doğru değildir. Çünkü geçmişte kuantum bilgi kuramı üzerine yapılan çalışmalar kuantum durumlarında "hata düzeltmesi" yapılabileceğini gösterdi. Kuantum bilgisayarların işleyişi sırasında meydana gelen hataları da düzeltmek mümkündür. *Decoherence* da işlemler sırasında meydana gelen bir tür hata gibi düşünülebileceği için

kuantum hata düzeltme yöntemleri kullanarak *decoherence*'ın sebep olduğu sorunları gidermek mümkündür. Üstelik hata düzeltmesi işlemler devam ederken de yapılabilir.

Detaylı analizler kuantum hesaplamaları için gerekli *decoherence* zamanının bilgisayarın çalışma hızının (tek bir işlemi yapması sırasında geçen zamanın) 10^4-10^5 katı kadar olduğunu gösteriyor. Kuantum sistemleri genel olarak bu kadar uzun *decoherence* zamanlarına sahip değildir. Bu yüzden *decoherence*, bugün hâlâ kuantum bilgisayarı araştırmalarının odakladığı en önemli konuların başında geliyor.

"Evrensel" kuantum geçitleri

Klasik bilgisayarlarda bitler üzerinde mantık işlemleri yapan temel birimlere "mantık geçitleri" denir. Bu geçitler bir ya da iki biti girdi olarak alır ve çıktı olarak bir bit üretir. Bir bilgisayarın işlemesi için gerekli tüm mantık geçitleri, birbirlerinden tamamen bağımsız devre elemanları olabileceği gibi bir ya da birkaç mantık geçidini farklı kombinasyonlarda bir araya getirerek tüm mantık geçitlerini üretmek de mümkündür. Gerekli tüm mantık geçitlerini üretmek için kullanılabilecek mantık geçitlerinin oluşturduğu kümeye "evrensel mantık geçitleri kümesi" denir. Örneğin mantıktaki "ve" işleminin tersini gerçekleştiren NAND geçidi, bir evrensel mantık geçididir. Sadece NAND geçidi kullanılarak üretilen devrelerle "ve", "veya", "ise", "değil" ve tüm diğer mantık işlemlerini yapmak mümkündür.

Kuantum bilgisayarlarında da bitler üzerinde mantık işlemleri yapabilmek için "kuantum mantık geçitlerine" ihtiyaç vardır. Örneğin Hadamard geçidi ve CNOT geçidi bir evrensel kuantum geçitleri kümesi oluşturur. Kübitler üzerinde yapılabilecek tüm mantık işlemlerini bu iki kuantum geçidini kullanarak gerçekleştirmek mümkündür. Hadamard geçidinin temel işlevi süperpozisyon durumunda kübitler oluşturmaktır: $|0\rangle$ durumundaki bir kübiti $(|0\rangle+|1\rangle)/\sqrt{2}$ durumunda bir kübite, $(|1\rangle)$ durumundaki bir kübiti $(|0\rangle-|1\rangle)/\sqrt{2}$ durumundaki bir kübite dönüştürür. Ayrıca bu işlem kendisinin tersidir. Başka bir deyişle bir kübite iki kez uygulandığında kübitin durumu değişmez. CNOT geçidi girdi olarak iki kübit alır. Birinci kübit kontrol kübitidir. İşlem sonunda değeri değişmez. Eğer birinci kübit $|0\rangle$ durumundaysa ikinci kübite bir işlem yapılmaz. Eğer birinci kübit $|1\rangle$ durumundaysa ikinci kübitin değeri değişir. Bu işlem de yine kendisinin tersidir. İki kübite iki kez CNOT işlemi uygulandığında durumları değişmez.

Kuantum bilgisayarları için geliştirilmiş algoritmalar, işlemler dizisi olarak tanımlanır. Bu işlemlerin fiziksel olarak gerçeğe dönüştürülebilmesi için, kübitler üzerinde o işlemleri yapabilecek aletlerin tasarlanması, üretilmesi ve işleyişlerinin arzu edildiği gibi kontrol edilebilmesi gerekir. İşlemlerle ilgili en önemli zorluklardan biri, farklı kübitler arasındaki etkileşimi sağlamaktır. Örneğin iyon-kapanı kuantum bilgisayarlarındaki kübitler arasında doğrudan bir etkileşim yoktur. Bu durum farklı bitlerle sırayla etkileşerek bitler arasındaki etkileşimlere aracılık edecek özel kuantum sistemlerinin varlığını gerektirir.

Kuantum geçitlerinin her zaman mükemmel bir biçimde çalışması mümkün değildir. İşlemler sırasında hatalar meydana gelebilir. Ancak hata düzeltme algoritmalarıyla giderilebilirler. Üstelik bu algoritmalar işlemleri yapmak için kullanılanlardan farklı kuantum geçitleri gerektirmez.

İstenilen kübitler üzerinde istenilen ölçümlerin yapılması

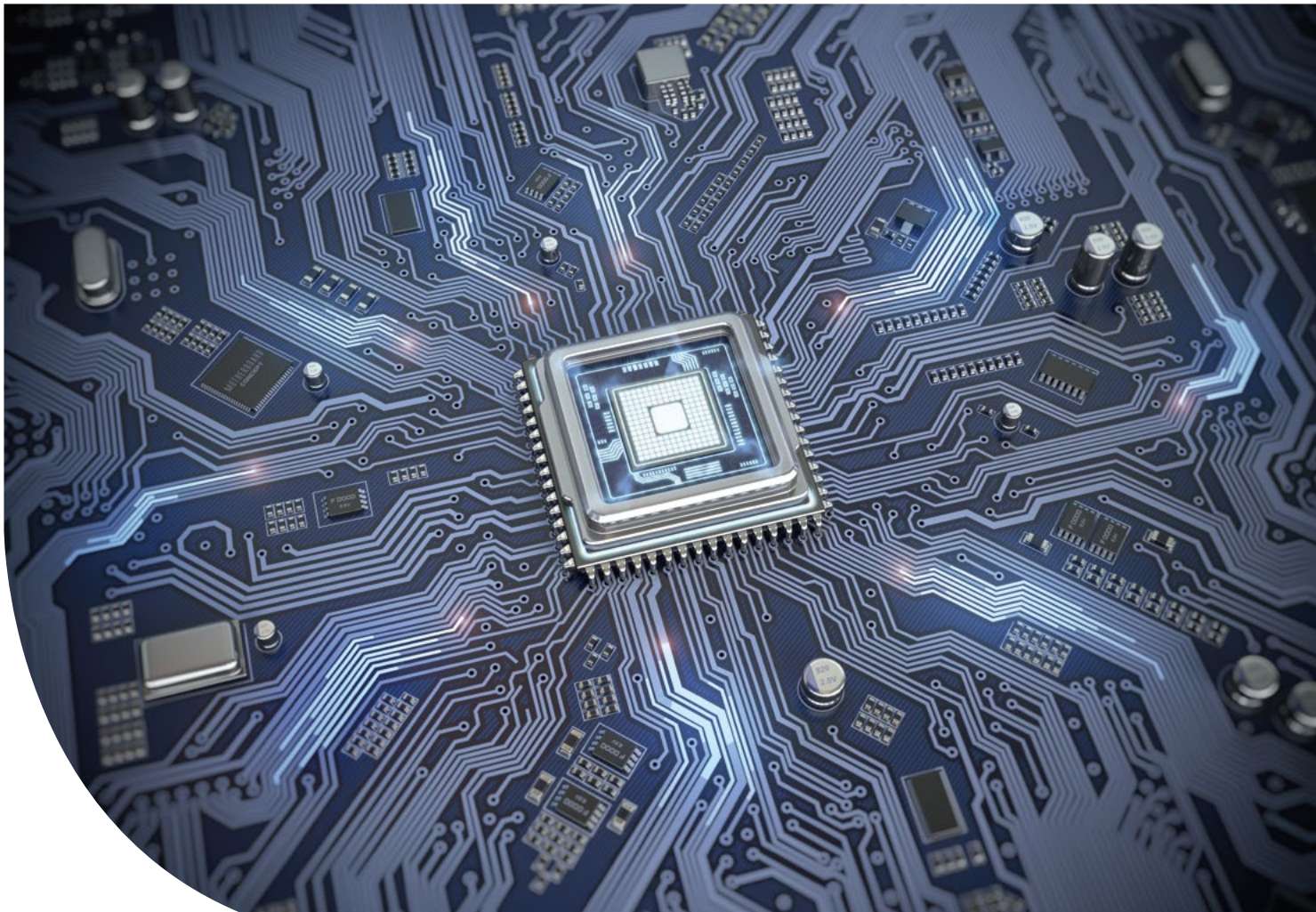
Hesaplamalar yapıldıktan sonra sistemin durumunun belirlenmesi gerekir, dolayısıyla arzu edilen kübitler üzerinde ölçüm yapılabilmelidir. İdeal olarak bir ölçümün %100 verimlilikle yapılması istenir. Gerçek ölçümlerin verimliliğiyse her zaman daha düşüktür. Ancak söz konusu olan kuantum hesaplamaları olduğunda, bu durum genellikle sorun değildir. Ölçümlerin verimliliğinin %90 olduğu durumu ele alalım. Eğer sistemde başka bir kusur yoksa sonuçların güvenilirliği %90 olacaktır. Eğer elde edilen sonuçların güvenilirliğinin daha yüksek olması isteniyorsa arzu edilen seviyeye ulaşana kadar aynı hesap tekrar tekrar yapılabilir. Ayrıca pek çok kuantum algoritması doğru sonucu kesin olarak değil *sadece belirli bir olasılıkla* verdiği için de hesapların tekrar tekrar yapılması gerekebilir.

Kuantum Üstünlüğü

Bir kuantum bilgisayarı bir klasik bilgisayarla karşılaştırıldığında ne ölçüde daha hızlıdır? Bu sorunun cevabı çözülmeye çalışılan sorunun ne olduğuna göre değişir.

Bazı görevler için kuantum bilgisayarları klasik bilgisayarlardan daha hızlı değildir. Örneğin f(x) bir fonksiyon olmak üzere, bu fonksiyonun n. yinelemesini, f(f(...f(x)...)), hesaplamak gibi. Bazı görevler için kuantum bilgisayarları klasik bilgisayarlardan "biraz" daha hızlıdır. Örneğin bir veri tabanına kayıtlı bir verinin yerini belirlemek gibi. Bazı görevler içinse kuantum bilgisayarları klasik bilgisayarlara göre aşırı derecede hızlıdır. Örneğin sayıları çarpanlarına ayırmak gibi. Bu problem özellikle internet güvenliği açısından çok önemlidir. Günümüzde yaygın olarak kullanılan RSA algoritmasıyla hazırlanmış şifreli metinleri çözmenin yolu yüzlerce basamaklı sayıları çarpanlarına ayırmaktan geçer. Klasik bilgisayarlarla bu problemi çözmenin bilinen tek yolu, tüm olasılıkları tek tek denemektir ki günümüzdeki en hızlı bilgisayarlarla bile böyle bir işi başarmak yüzyıllar sürer. Shor algoritması olarak adlandırılan, kuantum bilgisayarları için geliştirilmiş bir algoritmaysa sadece birkaç denemede yüzlerce basamaklı sayıların çarpanlarını bulmaya imkân veriyor.

Günümüzde fizik ve kimyayla ilgili pek çok olgu, kuantum sistemlerinin iyi anlaşılmasına dayanıyor. Ancak bu sistemlerin klasik bilgisayarda verimli bir biçimde benzetiminin yapılması neredeyse imkânsız. Örneğin 10 kübit içeren bir kuantum bilgisayarındaki kübitlerin durumunu klasik bir bilgisayarda depolamak için 2^{10}=1024 tane karmaşık sayının hafızaya kaydedilmesi gerekir. Kübitlerin sayısı 50 ye çıktığındaysa bu sayı 2^{50}=1.125.899.906.842.624'e çıkar ki herhangi bir klasik bilgisayarın kapasitesinin çok üzerindedir. Kuantum bilgisayarlarının en önemli kullanım alanlarından birinin kuantum benzetimleri olacağı düşünülüyor. Örneğin atomların ve moleküllerin sıra dışı koşullar altındaki davranışları ya da nanoteknolojiyle ilgili benzetimler kuantum bilgisayarları yardımıyla kolaylıkla yapılabilir.



Bugün ulaşılan son noktada, henüz kuantum bilgisayarları hiçbir görevi klasik bilgisayarlardan daha hızlı yapamıyor. Ancak Google ve IBM gibi çeşitli firmalar yakın gelecekte, bazı görevleri klasik bilgisayarlardan daha hızlı yapabilen kuantum bilgisayarları geliştirebileceklerini iddia ediyor.

Bugün kuantum bilgisayarı araştırmalarının odaklandığı en önemli konular, çok sayıda kübit içeren bilgisayarlar geliştirmek ve *decoherence*. İşlemlerdeki hata oranları, genel olarak bir işlem sırasında geçen zamanın *decoherence* zamanına oranıdır. Dolayısıyla hata oranının düşük olması için herhangi bir işlemin *decoherence* zamanından çok daha kısa bir süre içinde tamamlanabilmesi gerekir. Eğer hata oranı yeteri kadar düşük olursa, kuantum hata düzeltme algoritmalarını kullanarak *decoherence*'tan kaynaklanan hataları düzeltmek ve *decoherence* zamanından daha uzun süren hesaplamalar yapmak mümkün olur. Ancak hata düzeltmeleri yapmak, işlemler için gerekli kübitlerin sayısının da aşırı derecede artmasına sebep oluyor. Örneğin sayıları çarpanlarına ayırmak için öne sürülmüş Shor algoritmasını ele alalım. Eğer çarpanlarına ayrılacak sayı L tane bitle temsil ediliyorsa, bu sayıyı çarpanlarına ayırmak için gerekli kübitlerin sayısının L ile L^2 arasında olacağı düşünülüyor. İşlemler sırasında hata düzeltmesi yapabilmek içinse bu sayıyı L katına çıkarmak gerekiyor. Örneğin 1000 bitle temsil edilen bir sayıyı Shor algoritmasıyla, kuantum hata düzeltmesi yapmadan, çarpanlarına ayırmak için 10^4 kübite ihtiyaç olduğunu düşünelim. Hata düzeltmesi yapabilmek için kübitlerin sayısının en az 10^7 olması gerekir. Shor algoritması yaklaşık L^2 işlem gerektirir. Dolayısıyla 1000 bitle temsil edilen bir sayının 10^7 bit içeren ve çalışma hızı mikrosaniye zaman ölçeğinde olan bir kuantum bilgisayarıyla çarpanlarına ayrılması sadece saniyeler sürer. Bunu gerçeğe dönüştürmek için gereken şeyse 10^7 kübit içeren bir kuantum bilgisayarı geliştirmek. Günümüzdeki en büyük kuantum bilgisayarı sadece 20 kübit içeriyor. Ancak araştırmacılar tüm hızlarıyla çalışmaya devam ediyor. ■

Kaynak

DiVincenzo, D. P., "The Physical Implementation of Quantum Computation", https://arxiv.org/abs/quant-ph/0002077, 2000.