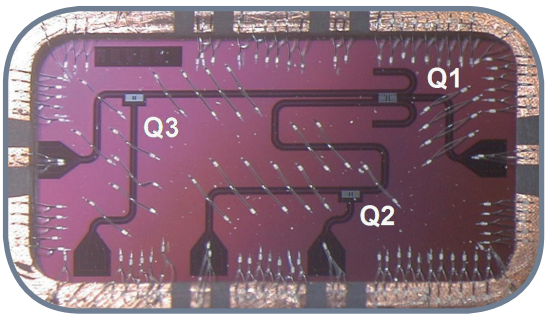
Börteçin Ege

Hacettepe Üniversitesi
Semantik Web Doktora Öğrencisi

Kuantum Mekaniğinden Kuantum Bilgisayarlarına

İnsanlığın uzun süreden beri beklediği kuantum bilgisayarları yolda gibi görünüyor. Süper bilgisayarlara rakip olacağı hatta onları tahtından edeceği iddia edilen bu bilgisayarların yapımının gerçekleştirilmesi için Batı ülkeleri yıllardan beri çok para harcıyor. Her ne kadar bilim insanlarının çözmesi gereken birçok teknik sorun olsa da, son yıllarda elde edilen sonuçlar gerçekten çarpıcı. Başta ABD, Almanya ve Avusturya olmak üzere bu teknolojiyi geliştirmek isteyen ülkeler her geçen gün yavaş ama emin adımlarla hedeflerine doğru yürüyor. Gerek yapısal açıdan gerekse çalışma biçimi açısından bildiğimiz bilgisayarlardan çok farklı olacak bu bilgisayarların yapımının, beraberinde bir devrim getireceği daha şimdiden belli.

Peki, kuantum bilgisayarlarının özellikleri ve onları bu kadar önemli yapan nedir?
Kuantum bilgisayarlarının ne zaman dünya piyasalarına çıkması bekleniyor?
Bir gün hayata geçirildiklerinde bilim dünyasını ve günlük hayatımızı nasıl değiştirecekler?
Gelin, bilim dünyasında gerçekleşecek bir sonraki devrimin anatomisini hep beraber inceleyelim.



Kuantum Mekaniği

Kuantum bilgisayarlarının temeli kuantum mekaniğine dayanır. Kuantum mekaniği 20. yüzyılın başlarında, içinde bulunduğumuz evreni bir süreklilik olarak tanımlayan klasik mekaniğin yetersiz kaldığı durumlarda alternatif açıklamalar üretmek üzere geliştirildi. Örneğin 20. yüzyılın başlarına gelindiğinde klasik mekanik artık ışığın, enerjinin ve atomların yapısını açıklamakta yetersiz kalıyordu. Temelleri tam olarak 1925-1935 yılları arasında Werner Heisenberg, Erwin Schrödinger, Max Born, Pascual Jordan, Wolfgang Pauli, Niels Bohr, Paul Dirac, Friedrich Hund ve John von Neumann gibi bir avuç İngiliz, Alman ve Avusturyalı bilim insanı tarafından atılan kuantum fiziği, sonraki yıllarda başka bilim insanlarının katkısıyla daha da geliştirilerek günümüzün modern teknolojisinin oluşumuna çok önemli katkılarda bulunmuştur. Kuantum mekaniği sayesinde bugün herkesin yakından bildiği lazer, elektron mikroskopu, röntgen cihazı ve atom saati gibi teknolojik araçlar geliştirilmiş ve yarı iletken maddelerin yine kuantum mekaniği sayesinde incelenebilmesiyle günümüzün modern elektroniğinin temelini oluşturan yarıiletkenlik özelliğine sahip modern diyot ve transistörler icat edilerek, en sonunda bugün hepimizin kullandığı bilgisayarlar geliştirilmiştir. Nükleer silahların geliştirilmesinde de hayli önemli bir rolü olan kuantum mekaniğinin günümüzdeki en önemli uygulama alanlarından biri, kuantum bilgisayarları olarak da adlandırılan yeni nesil bir bilgisayarın geliştirilmesidir.

Süperpozisyon İlkesi

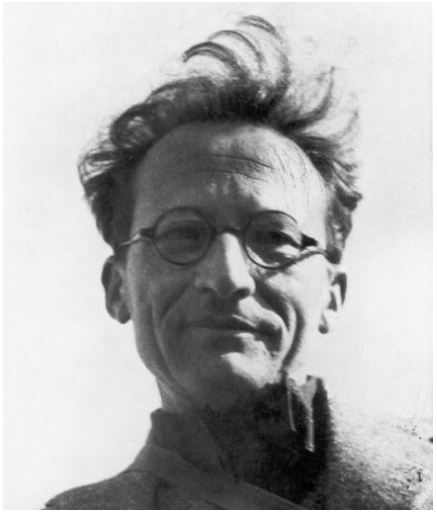
Kuantum mekaniğinin doğrudan uygulandığı nadir alanlardan biri kuantum bilgisayarlarıdır. Kuantum bilgisayarı fikri ilk olarak Amerikalı ünlü fizikçi Richard Feynman tarafından 1980'lerin başında ortaya atıldı. 1981'de Fizik ve Hesaplanabilirlik (*Physics and Computation*) konulu bir seminer veren Feynman, orada kuantum fiziğinin bildiğimiz klasik bilgisayarlarla etkin bir şekilde simüle edilip edilemeyeceği sorusunu ortaya attı. Seminer sonucunda bunun ancak kuantum mekaniği kanunlarına göre çalışan kuantum bilgisayarları aracılığıyla yapılabileceği sonucuna varan Feynman, tarihe kuantum bilgisayarları üzerine çalışmaları tetikleyen kişi olarak geçti. Bu tarihten itibaren tüm dünyada ele alınan kuantum bilgisayarları konusu günümüzde halen en geçerli araştırma alanlarından biridir.

Kuantum bilgisayarları ve bunları oluşturan elektronik devreler klasik mekaniğin kanunlarına değil, kuantum mekaniğinin kanunlarına göre hareket eder. Bu kapsamda birçok önemli kavram var, ancak özellikle biri ön plana çıkıyor: Kuantum Süperpozisyon ilkesi. Günümüzde kullanılan bilgisayarlarda hâkim olan dijital sistemlerde bir bit aynı anda sadece 0 veya 1 değerini alabilirken, kuantum mekaniğinde geçerli olan süperpozisyon ilkesine göre bir kubit aynı anda hem 0 hem de 1 değerini alarak bir nevi belirsizlik durumuna geçebiliyor (bu durum çakışma olarak da adlandırılıyor). Bu özellik kuantum bilgisayarlarının temelini oluşturan ana unsurlardan biri, çünkü bir kuantum bilgisayarı bu sayede bir kubitin (kuantum bit, kısaca kubit) tüm süperpozisyonları ile aynı anda işlem yaparak, süper paralel bir şekilde çalışıyor ve normal bilgisayarlarla çözümü yıllar alacak problemleri çok kısa sürede çözebiliyor. Adından da kolaylıkla anlaşılabileceği kuantum bilgisayarlarında bilgi dijital sistemlerden tanıdığımız bitlerde değil, kuantum bitlerde saklanıyor.

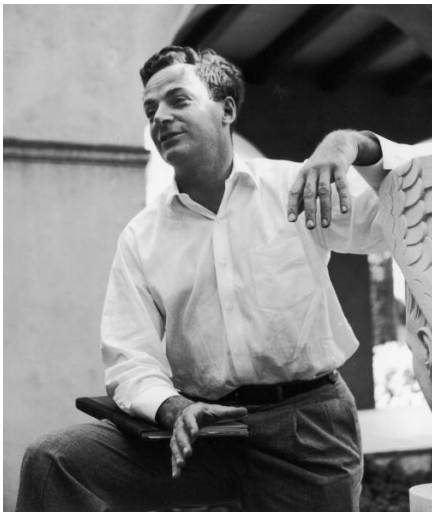
Kuantum Bilgisayarlarının Önündeki En Önemli Engel: Kuantum Bozunumu

Yine dijital dünyamızda geçerli klasik mekanik kurallarından farklı olarak kubitler sıcaklık, elektromanyetik dalgalar gibi nedenlerle kolayca bozunuma uğramaya eğilimli olduklarından, normal şartlar altında güncel bilgilerini dolayısıyla geçerli durumlarını sadece çok kısa süreyle (örneğin saniyenin milyonda biri) koruyabiliyorlar. Bu durum kısaca kuantum bozunumu olarak adlandırılıyor ve araştırmacılar için önemli bir problem teşkil ediyor, çünkü gerek kubitlerdeki bilgilerin okunması gerekse bu bilgileri işleyecek kuantum algoritmalarının çalıştırılarak söz konusu verilerle karmaşık işlemlerin yapılabilmesi için, bu sürenin mümkün olduğunca uzatılması gerekiyor. Bu noktada aynı süperbilgisayarlar alanında olduğu gibi, kuantum bilgisayarlarının geliştirilmesinde de başı çeken IBM tarafından yakın bir zaman önce bir çözüm bulunmuş gibi görünüyor: Süperiletkenlik.

Erwin Schrödinger



Richard Feynman



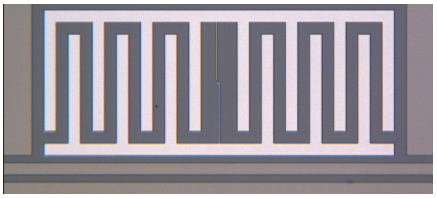
Süperiletkenler

IBM ve Yale Üniversitesi tarafından geliştirilen bu teknik ile kuantum bitleri -273,15 dereceye yani mutlak sıfır noktasına yaklaştırılarak süper iletkenlik durumuna geçiriliyor (mutlak sıfır noktası entropinin minimum olduğu bir maddedeki tüm moleküler hareketlerin durduğunun kabul edildiği noktadır.). IBM'in ve Yale Üniversitesi araştırma görevlilerinin elde ettiği sonuçlara göre süperiletkenlik moduna geçirilen kubitler bir enerjiye sahip olmadığından sıcaklık, elektromanyetik dalgalar gibi dış etkenlerden de hemen hemen hiç etkilenmiyor ve bu nedenle de "bilgiyi" şimdiye kadar olduğundan 2-4 kat daha uzun süre koruyabiliyorlar. Bu yöntemin kullanılması ile IBM mühendisleri tarafından kırılan rekor 100 mikro saniye civarında (yani kubitler geçerli durumlarını 100 mikro saniyeye kadar koruyabiliyor). Yine IBM tarafından bildirildiğine göre bu yöntemin kullanılmasıyla erişilen bu süreler, çeşitli kuantum algoritmalarının söz konusu kubitler üzerinde çalıştırılıp karmaşık işlemler yapılması için gerekli süreyi de kazandırıyor. Bu bilimsel amaçlarla sadece laboratuvarlarda kullanılan kuantum bilgisayarlarından, ticari amaçlı kuantum bilgisayarlarına geçiş için hayli ümit verici bir adım.

Kuantum Algoritmaları

Donanım uzmanları kullanılabilir ilk kuantum bilgisayarını yaratmaya çalışırken, bilgisayar bilimciler ve matematikçiler de doğal olarak boş durmuyor ve 1990'lı yılların başından beri kuantum bilgisayarlarında uygulanabilecek ilk algoritmaları geliştirmeye çalışıyorlar. Bilgilerin bitler yerine kubitlerde saklandığı ve kuantum mekaniğinin geçerli olduğu bu ortamda kuantum algoritmaları, kuantum bitlerinin süperpozisyon özelliğini

kullanarak işlem yapıyor. 1980'li yılların ortalarından günümüze kadar geliştirilmiş sadece bir avuç kuantum algoritması var. Bunlardan en bilinenleri ise Deutsch, Shor ve Grover algoritmaları.



Deutsch Algoritması

1985'te David Deutsch tarafından geliştirilen Deutsch algoritması bilim tarihindeki ilk kuantum algoritması. Sadece tek bir kubit üzerinde işlem yapabilen Deutsch algoritması, günümüzde de klasik algoritmaların sınırlarına dayandığı yerde kuantum algoritmalarının olağanüstü bir işlem hızıyla sonuca ulaşabildiğini kanıtlaması açısından hayli önemli bir yere sahip.

1992'de yine David Deutsch ve Richard Josza tarafından genelleştirilerek sınırsız sayıda (n tane) kubit üzerinde işlem yapabilecek şekilde tekrar formüle edilen ve Deutsch-Jozsa algoritması adını alan Deutsch algoritması, daha sonraki yıllarda geliştirilen Shor ve Grover algoritmaları için gerçek bir ilham kaynağı olmuştur.

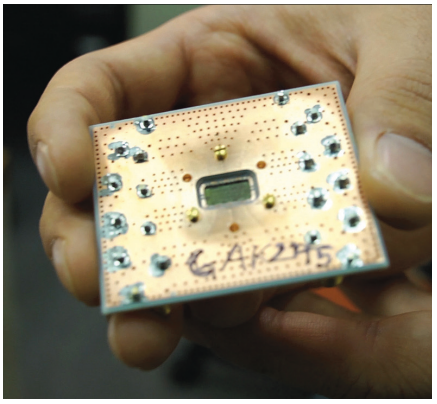
Shor Algoritması

Günümüzde laboratuvarlarda sadece bilimsel amaçlı deneyler için geliştirilen kuantum bilgisayarlarının test edilmesi için özellikle iki kuantum algoritması ön plana çıkıyor: Shor algoritması ve Grover algoritması.

1994'te Amerikalı matematikçi Peter W. Shor tarafından geliştirilen bu algoritma kuantum bilgisayarlarında çok büyük sayıları kolaylıkla faktörlerine ayırabiliyor. Shor algoritmasının bu özelliği kriptoloji açısından çok büyük önem taşıyor, zira günümüzdeki şifreleme mekanizmaları çok büyük sayıların klasik bilgisayarlar tarafından kabul edilir bir zaman dilimi içerisinde faktörlerine ayrılmasının mümkün olmadığı varsayımına dayanarak çalışıyor. Laboratuvar ortamları için geliştirilmiş ve çok az sayıda kubite sahip kuantum bilgisayarlarının bile en büyük sayıları, çok çok kısa sürede faktörlerine ayırabilmesi bugüne kadar bildiğimiz klasik kriptoloji biliminin temellerini şimdiden sarsarak kuantum kriptoloji adlı yeni bir bilim dalının yolunu açıyor.

Grover Algoritması

1996'da Hint asıllı Amerikalı bilgisayar bilimci Lov Grover tarafından geliştirilen Grover algoritması (GSA) çok büyük veri tabanlarında aranan bir bilginin, gerekli sorgulamanın çok detaylı bir şekilde formüle edilmesine gerek kalmadan fakat yine de hızlı bir şekilde bulunmasını sağlıyor. GSA da diğer birçok kuantum algoritması gibi olasılık kuramı tabanlı çalışan bir algoritma, dolayısıyla doğru cevabı bulabilmesi için veriler üzerinde çoğu zaman sadece bir kez değil, birçok defa çalıştırılması gerekiyor. Bu şekilde aynı verileri birçok defa işleyen algoritma, en sonunda doğru olma olasılığı en yüksek cevabı buluyor.



Uygulama Alanları

Kuantum bilgisayarlarının süperpozisyon ilkesinin beraberinde getirdiği süper paralel işlem yapma yeteneğinden ve programlanmalarının hayli zor olmasından dolayı ilk aşamada sadece günümüzün klasik bilgisayarları ve süper bilgisayarlarının yardımıyla çözülemeyen veya son derece uzun sürede çözülebilen özel problemlerin çözümünde kullanılması planlanıyor.

Gelecekte kuantum bilgisayarlarının başlıca uygulama alanları şunlar olacak:

Çok büyük sayıların olağanüstü hızlı bir şekilde faktörlerine ayrılarak, günümüzde hiçbir şekilde kırılamayacağı düşünülen şifreleme mekanizmalarının sadece saniyeler içinde kırılması

Kuantum sistemlerini atom düzeyinde simüle ederek, bu simülasyonlar sonucunda gerçeğe yakın sonuçlar elde edilmesi ve özellikle tıp, ilaç sektörü gibi alanlarda bugüne kadar erişilemeyen bilgilere erişilmesi

Olağanüstü derecede kapsamlı veri tabanlarının çok hızlı bir şekilde sorgulanması

Kuantum bilgisayarları ne zaman gelecek?

Gelişmeler artık dijital sistemlerin günlerinin sayılı olduğunu gösteriyor, fakat kuantum bilgisayarlarının tam anlamıyla hayata geçirilebilmesi için bilim insanlarının önünde daha uzun bir yol olduğu da açık, çünkü kuantum bilgisayarları klasik mekanik kanunlarına göre değil, insanlığın henüz tam bir fikir sahibi olmadığı kuantum mekaniği yasalarına göre çalışıyor. Bu nedenle ilk aşamada bu yasalarla uyumlu çalışacak kuantum mikroişlemcilerin, kuantum belleklerin, kuantum algoritmalarının ve hatta yeni kuantum programlama dillerinin geliştirilmesi gerekiyor. İlk kuantum bilgisayarlarının üretimine odaklanmış firmaların mühendisleri ve bu konuda araştırma yapan diğer bilim insanları önümüzdeki 15-20 yıl içinde ilk kuantum bilgisayarının prototipinin gerçekleştirilmiş ve üretime hazır olacağını belirtiyor.

Kaynaklar
IBM, "IBM Research Advances Device Performance for Quantum Computing", **http://www-03.ibm.com/press/us/en/pressrelease/36901.wss**, 28.02.2012.
Vandersypen, L., Steffen, M., Breyta, G., Yannoni, C., Sherwood, M. ve Chuan, I., "Experimental realization of an order-finding algorithm with an NMR quantum Computer", *Nature*, Sayı 414, s. 883-887, 2001.
Shor W. P., "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer", *SIAM Journal on Computing*, Sayı 26, s. 1484-1509, 1997.
Deutsch, D., "The Church-Turing principle and the universal quantum Computer", *Proceedings of the Royal Society of London*, Sayı 400, s. 97, 1985.
Deutsch D. ve Jozsa, R., "Rapid solutions of problems by quantum Computation", *Proceedings of the Royal Society of London*, Sayı 439, s. 553, 1992.
Grover, L.K., "A fast quantum mechanical algorithm for database search", *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, s. 212-219, 1996.
Shor, W. P., "Algorithms for Quantum Computation: Discrete Logarithms and Factoring", *IEEE Symposium on Foundations of Computer Science*, s. 124-134, 1994.
Bennett, C. H., Bernstein, E., Brassard, G., Vazirani, U.,"The strengths and weaknesses of quantum Computation", *SIAM Journal on Computing*, Sayı 26 (5), s. 1510-1523, 1997.