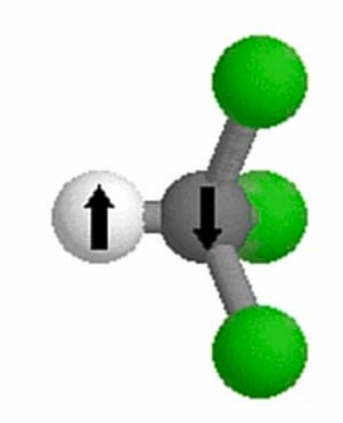
Quantum Computing

Yasin KAPLAN - kaplan@intrakets.com.tr

Günümüzde bilgisayar teknolojisi, insan beyni dışında, bizlere, hesaplama yeteneği kazandırmıştır. Bilgisayarlar, bir insandan çok daha hızlı bir şekilde hesaplama yapabildikleri gibi, bir insanın aynı anda aklında tutabileceğinden daha fazla bilgiyi depolayabilmekte ve bunlara hızlı bir şekilde erişilebilmesine olanak sağlamaktadırlar. İlkel bilgisayarlar mekanik bir mimariye sahipti. Bunlar daha sonra röleler, vakum tüpleri, transistorlar ve nihayet entegre devrelerle değiştirildiler. Her geçen gün bütünleştirilmiş devrelerdeki eleman sayısı artmakta, gelişen litografi teknikleri sayesinde bu devrelerdeki transistor boyları küçülmektedir. Intel Pentium 4 işlemcilerinde 42 milyon adet transistor bulunmaktadır. Bu sayı iki yıla yakın bir periyotta katlanarak artmaktadır. Intel bir on yıl daha bu şekilde gelişimin devam edeceğini tahmin etmektedir.

Bu gelişim yakın bir gelecekte mikroelektronik elemanların birkaç atomdan oluşan modelleri karşımıza çıkaracaktır. Bu boyutta, atomik ölçekte, fiziğin klasik kuralları değil, Quantum fiziğinin kuralları geçerli olmaktadır. Mikroelektronik devre elemanları arasındaki sınırlardan elektronlar atlama yaparak mikroişlemcilerin, görevlerini yerine getiremez hale gelmelerine sebep olacaktır. Ancak bu aşamaya gelinmeden önce klasik bilgisayar mantığında çalışacak ancak Quantum fiziğinin kullanılacağı bilgisayarlar inşa edilebilecektir *(Nanoteknoloji)*. Ancak bu tür bilgisayarlar Quantum algoritmaları yerine klasik bilgisayarlarda işletilebilen algoritmaları kullanacaklardır. Quantum sistemleri gerçek "Quantum Bilgisayarları" inşa edilebildiğinde asıl avantajı sağlayacaktır. Quantum teknolojisi çok daha fazla bitin aynı anda işlenmesine olanak tanıyacak, bilgi işleme teknolojisini temelinden değiştirecektir.



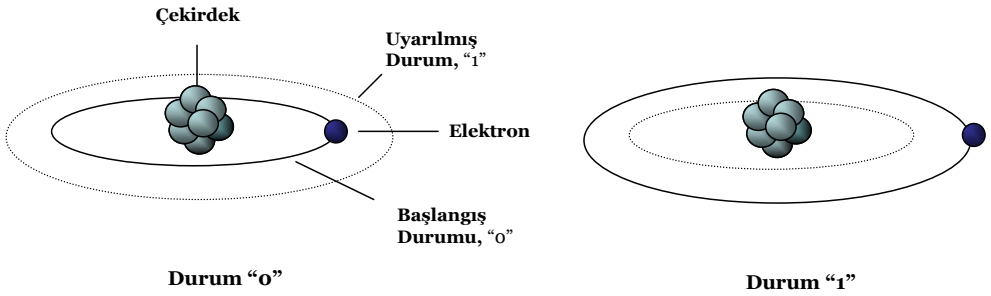
İzotopik olarak etiketlenmiş Kloroform içindeki ^{1}H ve ^{13}C çekirdeği küçük mıknatıslar gibi davranarak, harici bir magnetik alan ile etkileşebilmektedir. Nükleer dönüşler Quantum üstkonumlarında *(Superposition)* bilgi saklayabilmekte ve bunu işleyebilmektedirler. Yeşil renkli klor çekirdekleri ihmal edilebilir. Alan ile hizalı dönüşler mantıksal "1", karşı olanlar ise "0" olarak etiketlenirler. Bu çalışma şekli NMR *(Nuclear Magnetic Resonance)* Quantum bilgisayarının temel prensibini oluşturur.

Ancak atomik boyutta çözülmesi gereken birçok problem bulunmaktadır. Fiziksel olarak bir Quantum bilgisayarının nasıl inşa edileceği bir yana, ana problemlerden biri bir Quantum register'ından *(Yazmaç)*, var olan tutarlı enerji seviyesini değiştirmeden nasıl okuma yazma yapılacağıdır. Bu Quantum fiziğinin çözmek için uğraştığı en önemli problemlerden biridir, fakat ondan önce çözülmesi gereken problem normal koşullarda bir Quantum sisteminde bitleri *(Qubit, Quantum Bit)* modellemek için kullanılan Quantum parçacıklarının tutarlı enerji seviyelerinde tutulabilmesini sağlayacak pratik bir yöntemin bulunmasıdır. Üzerinde durulması gereken başka bir konu ise atomik seviyede, qubit'in çevresel şartlardan etkilenmemesi için nasıl izole edileceğidir.

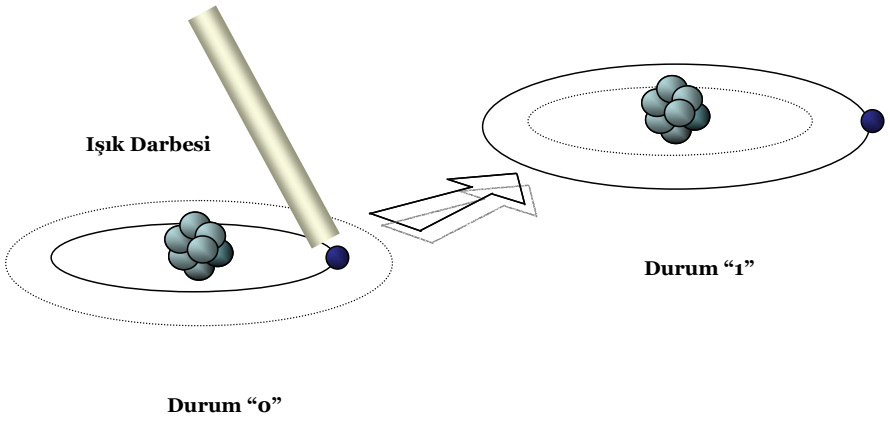
Bilim adamlarına karamsarlığa düşüren ve çözülmesi gereken bu kadar problem olmasına rağmen, bu problemler çözüldüğü takdirde, Quantum bilgisayarları, klasik bilgisayarlarla yapılması mümkün görünmeyen birçok hesaplamayı yapabileceklerdir. Karamsarlığa düşmeyen birçok bilim adamı Quantum bilgisayarları ile işletilebilecek algoritmalar üzerinde çalışmaktadırlar. Ayrıca Quantum pozisyonları bozulmadan, hataya bağışık sistemler için öngörülmüş modellerde bulunmaktadır.

Quantum Mantıksal Kapıları

Bir Quantum sisteminde, iki ayrık ve yeterince farklı enerji seviyesi bir qubit'i modellemek için uygun bir adaydır. Şimdiye kadar yapılan deneylerde Rubidyum *(ENS)* ve Berilyum *(NIST)* atomları qubit'leri modellemek için kullanılmışlardır. Atomlarda, çekirdek etrafında dönen elektronların enerji seviyeleri ayrıktır *(Quantalar)*. Bu seviyelerden herhangi ikisi, mantıksal "0" ve "1" olarak etiketlenip kullanılabilirler. Bu enerji seviyeleri atomdaki elektronların değişik uyarılma durumlarına karşılık gelirler.



Bu iki mantıksal seviyenin nasıl denetim altına alınabileceğini görebilmek için, tek bir elektronu olan ideal bir atomu ele alalım. Elektron'un "0" ve "1" *(Uyarılmış)* olarak tanımlanmış iki ayrı enerji seviyesi olsun.



Atomun başlangıçta "0" durumunda olduğunu ve mantıksal DEĞİL *(NOT)* işlemini gerçekleştirmek istediğimizi varsayalım. DEĞİL işlemi mevcut mantıksal değerin ters değerini elde etmemizi sağlar; 0 iken 1, 1 iken 0 değerini verir. Bu işlem atomlar ile kolaylıkla gerçekleştirilebilir. Uygun şiddet, süre ve dalgaboyunda bir ışık darbesi ile *(Dalgaboyu mutlaka iki enerji seviyesi arasındaki enerji seviyesi farkına karşılık gelmelidir)* bir elektronun enerji seviyesini değiştirmek mümkündür. Bizim durumumuzda "0" durumunda olan elektron, ışık darbesinden enerji soğurarak kendini "1" durumuna geçirecektir. Eğer elektron "1" durumunda olsaydı bu ışık darbesinin etkisi de tersi olacaktı.

Mantıksal DEĞİL işlemi, yukarıda anlatıldığı gibi tümüyle klasik ifadelerle anlatılabilir. Ancak klasik benzerlerinden çok daha farklı olan Quantum mantıksal işlemlerini gerçekleştirmek mümkündür. Örneğin mantıksal DEĞİL işlemini gerçekleştirmek için gerekli sürenin yarısı kadar bir süre uygulanacak ışık darbesi ile iki mantıksal seviye arasında yarım bir geçiş sağlanır. Bu ne anlama gelmektedir? Bu durum özetle, uyarılma yarım gerçekleştiğinden elektronun ne "0" ne de "1" durumunda olması demektir. Elektron arada bir yerde, bağdaşık bir Quantum pozisyonunda yer alacaktır. Başka bir yarım darbe uygulandığında DEĞİL işlemi tamamlanacaktır. Bu tür bir yarım darbe ile gerçekleştirilen Quantum işlemi DEĞİL işleminin karekökü olarak anılır. Bu yaklaşım yeni tür hesaplamaların gerçekleştirilmesine olanak tanımaktadır. Birden fazla qubit kullanılarak çok daha karmaşık işlemlerin yürütülmesi mümkündür.

Quantum Bilgisayarları

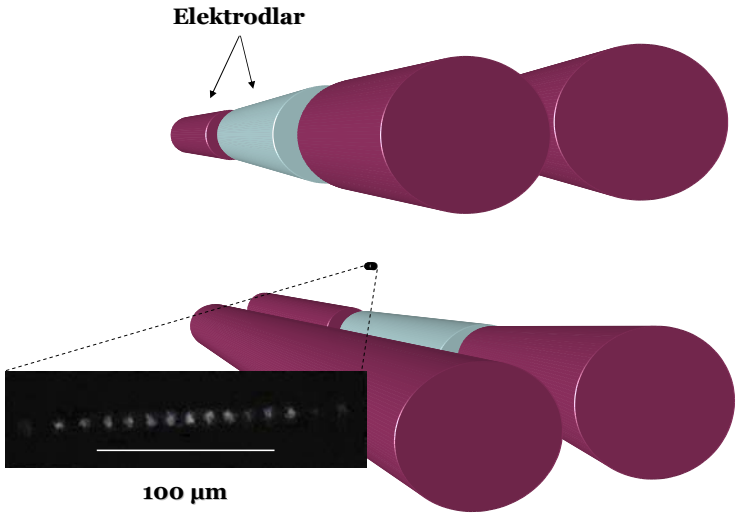
Quantum bilgisayarlarını klasik eşleniklerinden ayıran farklılığı vurgulamak için önce bit kavramına eğilmek gerekir. Fiziksel bakış açısından bir bit mantıksal iki durumdan birini *(Evet-Hayır, Doğru-Yanlış veya basitçe 0-1)* ifade etmek için hazırlanabilen bir fiziksel sistemdir. Örneğin günümüzün sayısal bilgisayarlarında bir kondansatörün levhaları arasındaki gerilim bir bitlik bilgiye karşılık gelir; yüklü bir kondansatör, bit değeri "1"e karşılık gelirken yüklü olmayan bir kondansatör ise mantıksal "0"a karşılık gelmektedir. Bir bitlik bilgi ayrıca ışığın farklı iki polarizasyonu veya bir atomun iki elektronik durumu kullanılarak da kodlanabilir. Ancak, bir atom fiziksel sistem olarak seçilirse atomun iki ayrık elektronik durumu dışında, atom, iki ayrık durumun bağdaşık *(Coherent)* bir üst konumunda da *(Superposition)* bulunabilir. Bu atomun hem "1" ve hem de "0" durumunda olması demektir. Bu durumun başka bir fiziksel sistemde karşılığı yoktur; bu durum tümüyle Quantum fiziğine has bir fenomendir.

Üç fiziksel bitten oluşan bir yazmacı ele alalım. Bu tür bir klasik yazmaç, bir anda, bu üç bitin karşılık gelebileceği sekiz sayıdan birini depolayabilir *(000, 001, 010, ..., 111)*. Ancak üç qubit'ten oluşan bir Quantum yazmacı herhangi bir anda bir Quantum üst pozisyonunda bu sekiz sayının tümünü depolayabilir.

Bir qubit aynı anda hem "0" ve hem de "1" değerlerini alabildiğinden bu şaşırtıcı bir sonuç değildir. Eğer bu yazmacı oluşturan qubit sayısı artırılırsa, depolama kapasitesi de üstsel olarak artacaktır. Örneğin dört qubit 16, beş tanesi ise 32 farklı sayıyı depolayabilecektir. Genel olarak L adet qubit 2^L adet sayıyı aynı anda depolayabilir. Bir yazmaç değişik sayıların üst konumunda hazırlandıktan sonra üzerinde işlem gerçekleştirilebilir. Örneğin, eğer qubit'ler atomlar ise, uygun bir şekilde ayarlanmış lazer darbeleri atomların elektronik durumlarını etkileyecek ve kodlanmış sayıların başlangıçtaki üst konumlarını başka üst konumlara kaydıracaktır. Her sayının bu tür bir kayma ile etkilenmesi tek parça bir Quantum donanımı ile geniş hacimli bir paralel işleme yeteneği sağlayacaktır. Bu başka bir değişle L adet qubit'in bağdaşık üst konumlarında kodlanmış 2^L adet girdi sayısı üzerinde tek adımda aynı matematiksel işlemi gerçekleştirilebilmesi demektir. Aynı işlemin klasik bir bilgisayarda gerçekleştirilebilmesi için aynı matematiksel işlemin tek işlemci ile

2^L kez veya 2^L adet farklı işlemci üzerinde paralel olarak işletilmesi gerekir. Özetle bir Quantum bilgisayarı zaman ve bellek gibi kaynakların kullanımında müthiş bir tasarruf sağlamaktadır.

Gelecekte bir Quantum bilgisayarındaki yazmaçlar aşağıdaki iyon tuzağına benzeyebilir:



Yukarıdaki şekilde doğrusal iyon tuzağı gösterilmektedir. Bu model ikili olarak gruplandırılmış dört paralel çubuktan oluşmaktadır. Kesikli çubuklara DC gerilim uygulanırken, tek parça halindeki çubuklara alternatif gerilim uygulanır. Eksenel sabitleme için kesikli çubukların dış kısmına pozitif, iç kısımlarına sıfır veya pozitif bir gerilim uygulanır. Tuzaktaki iyonlar Kalsiyum veya Berilyum'un vakumda *(~5x10^{-11} mbar)* ısıtılması *(~800˚C)* ve gaz halindeki Kalsiyum veya Berilyumun elektron bombardımanına tutulması elde edilir.

Tuzaktaki tüm iyonlar, aynı yüke sahiptirler ve birbirlerini itmektedirler. Bu iyonların herhangi birinin hareketi bu elektrostatik itme ile, fonon olarak bilinen çeşitli kolektif hareketleri indükleyerek, tuzaktaki diğer iyonlara iletilmektedir. Tuzakta rezonans halindeki bir iyon, söz konusu iyona bir lazer darbesi doğrultularak yavaşlatılabilir *(Soğutulabilir!)*. Uygun güçte ve dalgaboyundaki bir lazer darbesi rezonans halindeki iyonun bir foton yayınlayarak yavaşlamasına sebep olur. Her iyon, iyonlar arası mesafe uyarımı sağlayan lazerin dalga boyundan çok daha geniş olduğundan, ayrı olarak adreslenebilir. Lazer ışığı ve fononlar ile Quantum bilgisayarlarında kullanılabilecek mantıksal etiketleme sağlanabilmektedir. Bu tür Quantum mantıksal kapıları Avrupa *(Ecole Normale Supérieure)* ve ABD'deki *(NIST)* araştırma grupları tarafından şu sıralarda uygulanmaktadırlar. Quantum bilgisayarlarında kullanılabilecek NMR *(Nuclear Magnetic Resonance)* teknikleri de tartışılmaktadır.

Quantum Bilgisayarlarında Çarpanlara Ayırma

Bir tamsayıyı, *N*, bölenlerine ayırmanın en basit yolu, *N*'nin karekökünden daha küçük bir sayı olan *p* gibi bir sayıya bölüp kalanı kontrol etmektir. Eğer kalan "0" ise *p*'nin bölen olduğu sonucuna varılır ve işlem sona erer. Ancak bu yöntem son derece verimsizdir; Saniyede 10^{10} değişik *p*'yi deneyebilen bir bilgisayar *(Bu şimdiye kadar yapılmış en hızlı bilgisayarın gerçekleştirebileceği bir işlem değildir...)*, 60 basamaklı bir sayının çarpanlarının bulabilmek için, evrenin yaşından daha uzun bir süreye ihtiyaç duyacaktır.

Quantum bilgisayarları bu basit bölme yöntemi yerine, verimli bir çarpanlara ayırma işlemi için biraz daha farklı bir yöntem kullanırlar. Aslında bir sayının çarpanlara ayrılması bir fonksiyonun

periyodunun belirlenmesi problemi ile ilişkilendirilebilir. Bu yöntemin nasıl çalıştığını anlatmak için N=15'in asal çarpanlarını bulmak istediğimizi varsayalım. Bunun için N'ten küçük olan örneğin a=7 alalım ve f(x)=7^x mod 15 fonksiyonunu tanımlayalım. Bu fonksiyon 7'nin tamsayı olan x üssünü alır ve 15'e bölündüğündeki kalanını verir. Örneğin eğer x=3 ise f(3)=13 olacaktır zira 7^3=343=15x22+13'tür. Matematiksel olarak f(x)'in periyodik olduğu ve, fonksiyonun periyodu olan r'nin 15'in çarpanları ile ilişkilendirilebileceği gösterilebilir. x=0, 1, 2, 3, 4, 5, 6, ... değerleri için f(x)'in sonuçları 1, 7, 4, 13, 1, 7, 4, ... olacak ve periyod 4 olarak belirlenecektir. Bu bilgi ile N'nin çarpanlarını hesaplamak için N'nin ve $a^{r/2}$ +/-1'nin en büyük ortak bölenini hesaplamak yeterli olacaktır. Örneğimizde 15 ve $7^{4/2}$+1=50 *(veya 74/2-1=48)*'nin en büyük ortak böleni 5 *(veya 3)* olacak, bunlar da 15'in çarpanları olacaktır.

Açıktır ki klasik bilgisayarlar bu yöntemi verimli olarak işletemezler; f(x)'in periyodunu bulmak için f(x)'i birçok kez çözmek gerekir. Aslında yukarıda bahsi geçen çarpan bulma yönteminde olduğu kadar adımın, f(x)'in periyodunun bulunması için işletilmesi gerekir. Bir Quantum bilgisayarı kullanıldığında ise durum çok farklı olacaktır; bir Quantum register'ı 0, 1, 2, 3, 4, ... değerlerini temsil edecek şekilde kurulursa bir adımda f (1), f(2), f(3), f(4), ... değerlerini hesaplamak mümkündür. Başka bir adımda ise kolaylıkla fonksiyonun periyodu hesaplanabilir *(Quantum Fourier Dönüşümü)*.

Peter Shore *(Bell Labs)* 1994'de Quantum sistemi ile çarpanlara ayırma yöntemini tartışan makalesini yayınladığında, Quantum bilgisayarı kavramı insanlar için daha çok şey ifade eder hale gelmiştir. Günümüzde klasik bilgisayarların işlem gücü artmasına karşın halen, klasik bilgisayarlarla çözemeyeceğimiz problemler bulunmaktadır. Quantum bilgisayarları tabiatı ve evreni daha iyi anlayıp modellememize olanak tanıyacak karmaşık hesapların yapılmasında bize yardımcı olacaklardır.

Kaynaklar

1. Centre for Quantum Computation, http://www.qubit.org/
2. IBM, http://www.research.ibm.com/quantuminfo/
3. QC Research Centre - University of Melbourne, Avustralya, http://www.ph.unimelb.edu.au/src
4. SACKETT, C. A., Quantum Information Experiments With Trapped Ions: Status and Prospects, Quantum Information and Computation, Vol. 1, No. 2, (2001), 57-80