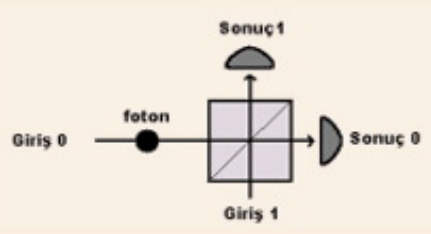
MAKİNELER, MANTIK VE KUANTUM HESAPLAMA

Aziz Kolkıran*

Her ne kadar mantık ve saf matematiğin kavramları doğa kanunlarından bağımsız ve nesnel görünseler de aslında bunların gerçekliği hakkındaki bilgimiz, kuantum fiziğindeki son gelişmelerin ışığında, durumun böyle olmadığını ve tamamen bizim fizik kanunları hakkındaki bilgimize bağlı olduğunu göstermektedir. Özellikle kuantum hesaplama teorisinin bazı deneysel sonuçları, hesaplamanın ve dolaylı olarak matematiksel ispatın fiziksel bir süreç olmaktan bağımsız, tamamen mantıksal bir süreç olduğu görüşünü yavaş yavaş terketmemiz gerektiğinin sinyallerini vermektedir.

Bu yüzyılın ikinci çeyreğinde, bir grup matematikçi, etkili bir şekilde hesap yapabilecek ve çok basit bir çalışma temeline sahip bir takım makinelerden söz etmeye başladılar. Hatta bu makineleri kullanarak matematikteki her teoremin bu makinelere verilecek bir takım işlem basamakları ya da daha genel anlamda algoritmalarla hesaplanabilir bir fonksiyon haline getirilerek ispatlanabileceğini göstermeye çalıştılar. Aslında yaptıkları şey, bugünkü bilgisayar biliminin ve bilgisayarın, kavram olarak gerçekleştirilmesiydi. Bu matematikçilerden Alan Turing, Turing makinaları dediğimiz soyut bir yapıyı önerdi. Bu, fiziksel bir ortamda sağa ve sola hareket eden ve sonlu sayıda iç durumları olan ve bir bant ile iletişim sağlayan basit bir makinedir.Bu makineyle birlikte doğal olarak bir soru ortaya çıktı. Acaba böyle fiziksel bir yapıda, tam olarak, hangi mantık işlemlerini gerçekleştirebiliriz? Aslında, prensipte dahi olsa, ne Turing makinaları ne de etkili işlemler yapabilecek bir takım formel yaklaşımlar bu soruyu cevapsız bırakıyor. Gerçekte bizim ihtiyacımız olan şey Turing makinalarını geliştirip bu işlemleri, teoremlerin ispatlarını etkili bir şekilde kontrol edecek daha genel makinalara uygulamak. Etkili bir şekilde mantıksal operasyonları yapabilen bu mekanik işlemler sayesinde bu makinelerin evrenselliği ve güvenilirliği gösterilebilir. Peki burada fiziksel makinaların bir mantık operasyonun tanımlanmasındaki rolü ne olabilir ya da bu ne demektir? Buna bağlı olarak da fiziğin tutarlılığının ya da etkinliğinin matematiksel bilimlerdeki yeri nedir? Bu makinelerin doğru sonuçları vermedeki güvenilirliği nereden kaynaklanmaktadır? Her şeyden önce hiç kimsenin bu makinaların güvenilirliliğini test edebilecek şekilde olası bütün mantık işlemlerini yapmasına ya da varolan bütün aritmetik işlem kombinasyonlarını uygulamasına gerek yoktur. Çünkü bunu yapmaya kalkarsak o zaman böyle makinaları kullanmamıza gerek kalmayacaktır. Bu makinalara güvenmemizin sebebi, tamamen mantığa dayandırılmadan öte, aynı zamanda onun işleyişinde kullanılan fizik bilgimize de bağlı olmak zorundadır. En azından makinenin işleyişinin tamamen fizik kanunlarına bağlı olduğunu sorgusuz kabul ediyoruz. Bununla beraber bizim hesaplamanın doğasını kavrayışımız fizik teorileri dolayısıyla gerçekleşmektedir. Bu anlamda, aslında Turing'in yaptığı şeye şu perspektiften bakabiliriz: Öyle bir evrensel makine (bilgisayar) yapılabilir ki uygun bir şekilde programlandığında (aynı zamanda gerekli bakım ve enerji sağlandığında) herhangi başka bir fiziksel nesnenin (makina ya da hesaplamayı birebir gerçekleştiren fiziksel bir olay) yapabileceği her türlü hesaplamayı yapsın. Bu şekliyle, bilinen Churh-Turing tezi aslında fiziksel dünya ile ilgili bir tez haline dönüşmüş olur. (Kısaca Church-Turing tezi, orjinal haliyle, şudur: Hesaplanabilir olan herhangi bir fonksiyon bir Turing makinası tarafından da hesaplanabilir).

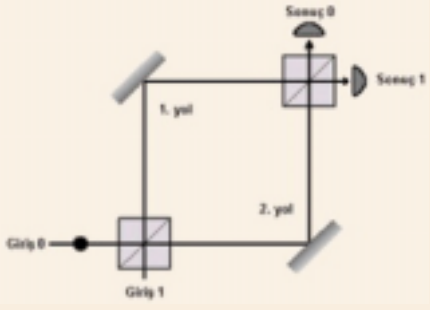


Şimdi kendimize şöyle bir soru soralım: Genel anlamda hesap yapan makinelerin işlem kapasitelerini sınırlayan bir limit var mı? Elbette ki böyle bir limit var ve bu limiti getiren hem fiziksel hem de mantıksal ve matematiksel sınırlar bulmak mümkün. Örneğin birden fazla çift asal sayı bulamayacağınız mantıksal bir kesinliktir; yine herhangi bir işlem süreci sırasında makinenin çalışmasının, termodinamiğin kanunlarına uygun fiziksel süreçlerde gerçekleşme zorunluluğu vardır. Bunun ötesinde örneğin bu mantıksal ve fiziksel limitlerin birarada birbiriyle etkileşerek getirdiği sınırlardan biri de ünlü "durma problemi" (halting problem)'dir. Bu probleme göre, bir makinenin verilen birtakım girdiler (input) sonucunda durup durmayacağına karar verebilecek bir algoritma yoktur. Dolayısıyla, mantıksal açıdan, böyle bir problemi çözebilecek bir makina yapmak, fiziksel yollarla mümkün değildir (en azından bildiğimiz klasik fizik kanunları çerçevesinde böyle bir makina oluşturamayız). Peki, eğer bu problemin üzerine tersten gidersek, yani fizik kanunları ile ilgili teorilerimizi geliştirirsek ya da fiziksel gerçeklikle ilgili bilgilerimizi yeni

fiziksel prensipler dahilinde ilerletirsek bu bize mantık ve matematik ile ilgili varolan sınırlarımızı geliştirmemize ve böylece hesaplanabilirlik üzerindeki sınırların biraz daha genişletilmesine olanak sağlar mı? Bu soru, yeni bir yüzyılın başında, aslında olumlu yönde cevaplanması büyük devrimlere yol açacak, çok önemli bir sorudur ve bizim mantık ve matematikle ilgili bilgilerimizin sadece sorgulamadan kabul ettiğimiz gerçeklerden geldiğini değil de doğrudan gözlem ve deneylerimizle elde ettiğimiz fiziksel prensiplerin katkılarıyla da etkileşip gelişebileceğini gösteren bir kanıt olacaktır. Şimdi bu soruya önemli katkılar sağlayabileceğini düşündüğümüz ve kuantum mekaniğinin keşfinden sonra ortaya çıkan bir fenomenin, kuantum girişiminin, bizim hesaplamanın doğası ile ilgili anlayışımızı nasıl değiştirdiğine bir göz atalım.

Kuantum Girişimi

Bildiğimiz gibi, klasik hesaplamada NOT (DEĞİLLEME) kapısı (NOT gate) 1 ya da 0 olarak gelen bir durumun değilini alarak işlem yapan tek bit'lik bir temel mantık operasyonudur. Bu operasyonu iki defa üstüste uyguladığımız zaman gelen bit durumu ile çıkan bit durumu tamamen birbirine eşit olur. Kuantum hesaplamada kullanılan temel bilgi değerleri ise, genel anlamda, iki duruma sahip bir kuantum parçacığın (ya da sistemin) bu durumlarının toplamı (süperpozisyon) şeklinde ifade edilir (Buna kuantum bit diyoruz). Klasik hesaplamada uygulanan bütün mantık kapıları (NOT, AND(VE), OR(VEYA) gibi) kuantum hesaplamada da aynı mantık kuralları çerçevesinde uygulanabilmektedir. Şimdi fizikçilerin labaratuvarlarda rahatlıkla uygulayabildikleri tek parçacıklı foton girişim deneyini düşünelim. Şekil 1'de görüldüğü gibi her iki durumdan birinde (örneğin 0 durumunda) yarı gümüşlenmiş (yarı geçirgen) ayna üzerine gelen bir foton eşit olasılıklarda sonuç 0 ve sonuç 1 dedektörüne düşmektedir. Aslında kuantum anlamında, burada gerçek bir rasgele davranış yoktur (her ne kadar sonuçlar bize öyle gelse de). Foton her iki dedektöre giden yolu aynı anda almaktadır! Fakat so-



nuçlar dedektörlerde raslantısal bir şekilde eşit olasılıklarla belirir. Bu düzeneğe şekil 2'deki gibi bir ayna daha ekleyelim, yani birinci aynadan çıkan yolları tam yansıtıcı aynalar sayesinde ikinci dedektörde birleştirelim. Klasik fizik anlayışımıza göre, birinci yarı gümüşlenmiş aynadan geçen foton ya birinci yolu ya da ikinci yolu izleyerek ikinci yarı gümüşlenmiş aynaya gelecek ve burada yine hangi yoldan geldiği önemli olmadan ya sonuç 0 ya da sonuç 1 dedektörü üzerine eşit olasılıklarda düşecektir. Ama deneyi yaptığımız zaman sonucun hiç de beklediğimiz gibi raslantısal olmadığını ve giriş 0 durumunda giren parçacığın her zaman sonuç 1 dedektöründe gözlendiğini, hiçbir zaman sonuç 0 dedektörüne düşmediğini görürüz.

Şekil 1: Tek parçacıklı kuantum karekök-NOT köprüsünün deneysel düzeneği. Burada her iki durumdan birinde giren foton sonuç dedektörlerinde eşit olasılıklarda belirmesine rağmen bu olay fotonun aynadan çıktıktan sonra sadece bir yolu izlediği anlamına gelmez. Aslında foton her iki çıkış yolunu da aynı aynda almaktadır!

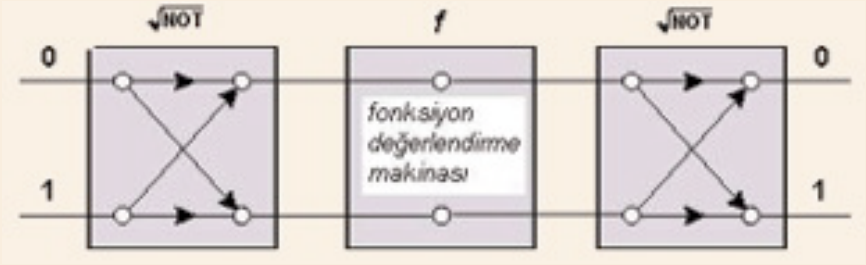
Aynı şekilde giriş 1 durumunda düzeneğe giren parçacık yüzde yüz olasılıkla sonuç 0 dedektörüne düşer. Bunun açıklaması ise, olayın başında da belirtildiği gibi kuantum fiziğinin, aslında fotonun her iki yolu da aynı anda aldığı gerçeğine uygun hesaplamaları yapıldığında, çok iyi bi şekilde anlaşılmaktadır. Bu düzenekte çıkan sonuçlara göre biz çok rahat bir şekilde NOT kapısını şekil 2'deki gibi bir düzenek kurarak kuantum hesaplamada kullanabiliriz. Ama burada aslında, şekilde de çok açık görüldüğü gibi, iki tane birbirine eşdeğer kuantum kapısı kullanılmaktadır, yani bir kuantum mantık kapısı iki defa uygulanmıştır. Bu kapı şekil 1'deki düzenekten başka birşey değildir ve biz bu kapıya bu yüzden karekök-NOT kapısı adını veriyoruz ve böylece klasik hesaplamada olmayan bir mantık kapısı elde etmiş oluyoruz. Buradan hemen şu sonucu çıkarabiliriz: Klasik fizikteki bilgilerimizi kapyasayacak şekilde geliştirdiğimiz yeni bir fiziksel dünya görüşü olan kuantum fiziği, bize mantık ve matematik yapısı içerisine yeni bir mantık operasyonu (karekök-NOT) koymamıza olanak sağlıyor. Bu yeni mantık yapısını tamamen bir takım gözlemler, deneyler ve varsayımlar yaparak kazandığımızı rahatlıkla söyleyebiliriz (çünkü kuantum fiziği de bilimsel bir teoridir ve doğruluğu çeşitli deneyler yapılarak ispatlanmıştır). Bu durumda mantıkçılara artık yeni bir mantıksal operasyon olan karekök-NOT operasyonunu tanımlama hakkını da fizikçiler olarak verebiliriz. Neden mi, çünkü doğada bu operasyon için tanımlanmış bir makinamız var!

Şekil 2: Tek parçacıklı girişim deneyi ya da kuantum NOT kapısını gerçekleştiren deney düzeneği. 0 ya da 1 durumunda giren foton, sonuç dedektörlerinde eşit olasılıklarda belirmektedir. Fakat bu, fotonun girişim ortamına girdikten sonra yollardan sadece birini seçtiği anlamına gelmez. Aslında foton, her iki yoldan da aynı anda geçmektedir (arada gözlenmediği sürece). Burada 0 durumunda giren her foton sonuç 1 dedektöründe ortaya çıkmakta ya da 1 durumunda giren her foton 0 dedektöründe görünmektedir. Bu olay NOT kapısının uygulanmasıdır ve bunu iki tane karekök-NOT köprüsünü ardarda kullanarak gerçeştirmekteyiz.

Kuantum Algoritmaları

Tek parçacıklı kuantum girişim olayında karşımıza çıkan ve klasik olasılık anlayışımızdan farklı bir olasılık yorumuna sahip olan bu durum kuantum mekaniğinin doğasına sahip tüm sistemler için geçerlidir ve dolayısıyla herhangi iyi tanımlanmış iki kuantum durumuna sahip tüm sistemleri kuantum hesaplamada kullanabiliriz. Bu arada aklınızda bu olasılık davranışından dolayı hesaplama sonucunda nasıl olup da yanlış sonuçların çıkmayabileceği sorusu ya da doğru bir hesaplamanın nasıl elde edileceği

konusunda endişeler olabilir. Bunun da yine kuantum fiziğinin kullandığı klasik fizikteki olasılıkların toplanması kuralı değil de olasılık katsayılarının toplanması kuralının getirdiği bir sonuç olan yapıcı girişim (constructive interference) ve yıkıcı girişim (destructive interference) olaylarıyla ortadan kalktığını görebiliriz. Buna göre doğru sonuçlar yapıcı girişim yoluyla ayakta kalırken yanlış olan sonuçlar ise yıkıcı girişim ile ortadan kalkmaktadır.Uygun sayıda girişim yapılarak doğru sonuçların güçlendirilmesi fikri kuantum hesaplamanın en temel prensiplerinden biridir. 1985 yılında David Deutsch'un önerdiği ve bütün ileri düzeydeki kuantum algoritmalarının ana özelliklerini içeren bir algoritma da yine iki karekök-NOT operasyonun arasına sıkıştırılmış bir fonksiyon değerlendirme makinasıyla başarıyla gerçekleştirilmiştir (şekil 3). Bu algoritmada Deutsch, {0,1} kümesinden yine {0,1} kümesine tanımlı bir f fonksiyonunun sabit bir fonksiyon (f(0) ve f(1)'in aynı değeri aldığı durum) mu yoksa birebir bir fonksiyon (f(0) ve f(1)'in farklı değerler aldığı durum) mu olduğunu, bu önerilen makinada sadece fonksiyonun bir defa hesaplanarak belirlenebileceğini göstermiştir. Klasik bir makinada (bir kişisel bilgisayar) bunu gösterebilmek için fonksiyonu iki defa hesaplamaktan başka çare yoktur. Hiçbir klasik algoritma bize, fonksiyonu sadece bir defa hesaplayarak onun sabit mi yoksa birebir mi olduğunu gösteremez. Aslında bütün kuantum hesaplamaların, sadece Deutsch'un kullandığı algoritmanın daha karmaşık bir uygulamasından başka birşey olmadığını göstermek mümkündür. !997 yılında bu algoritma deneysel olarak Nükleer Magnetik Rezonans yöntemi kullanılarak gösterilmiştir. Bu deney sadece iki kuantum bit kullanılarak yapılmıştır. Tabiki daha ileri düzeydeki algoritmalarda daha fazla kuantum bit'e ihtiyaç vardır ve bit sayısı arttıkça da kuantum bilgisayarın işlem yapma hızı ve kapasitesi eksponensiyel olarak artmaktadır ki bu da kuantum hesaplamanın klasik hesaplamaya karşı bir diğer ve en önemli üstünlüklerinden biridir. 1985'ten sonra dikkatler kuantum hesaplamaya çevrilmiş ve 1994'te Peter Shor'un bir sayının asal



Şekil 3: Deutsch'un tek hesaplamada, f fonksiyonun tipini belirleyen kuantum hesaplamasının şematik gösterimi.

çarpanlarını klasik algoritmalara kıyasla çok etkili ve hızlı bir şekilde bulan algoritmasıyla birlikte bu alanda yapılan çalışmalar tam bir patlama noktasına gelmiştir. Şu anda çalışmalar hem deneysel hem de teorik koldan hızla etkili bir sonuca doğru ilerlemektedir. Özellikle Shor'un asal çarpanları bulma algoritmasının bugün çok yaygın bir şekilde, her türlü elektronik şifrelemede kullanılan RSA dediğimiz şifreleme sistemlerini etkili ve uygun sürelerde çözebilmesi, bu alanda yapılan araştırmalara askeri kuruluşların da çok büyük parasal destekler sağlamasına yol açmıştır.

Hesaplamanın Geleceği

Aslında kuantum hesaplama konusundaki ilk tartışmalar Richard Feynman'ın 1981'de MIT (Massachusets Institue of Technology)'de verilen bir konferans sırasında yaptığı konuşmadan sonra başladı. Bu konuşmasında Feynman, kuantum fiziksel bir sistemin bir klasik bilgisayarda klasik olasılık yöntemler kullanılarak etkili bir şekilde simulasyonunun yapılamayacağını gösterdi. Aslında bir güçlük gibi görünen bu fenomenin bize bir fırsat yaratabileceğini ve bu simulasyonun bir kuantum bilgisayarda yapıldığı takdirde bize çok büyük faydalar sağlayabileceği olasılığının kapısını aralamış oldu. Bununla beraber, eğer başka bir kuantum sistemin simulasyonunu yapmak istiyorsak bunun için yeni bir simulator yapmak yerine sistemde küçük değişiklikler yaparak bunu aynı düzenekte yapabileceğimiz fikrini ileri sürdü ve bunu yapan alete de "evrensel kuantum simulatoru" adını verdi. 1985 yılında da Deutsch, böyle bir evrensel kuantum simulatorünün varlığını ispatladı ve herhangi bir kuantum bilgisayaranın yapabileceği bütün hesaplamaları da aynı etkinlikte yapabileceğini gösterdi ve buradan da evrensel kuantum Turing makinaları kavramı ortaya çıktı. Klasik Church-Turing tezi hiçbir zaman ispatlanamadı ama 1985'te kuantum Turing makinalarını kullanan Kuantum Church-Turing tezi, Deutsch tarafından kesin bir şekilde ispatlandı. Bu ispat da yine elimizdeki en iyi teorilerden biri olan kuantum teorisinin hesaplamanın doğasını nasıl etkilediğini ve yeni ve daha güçlü hesaplama modellerinin bu yolla nasıl ortaya çıktığını açık bir şekilde göstermektedir.

Kuantum hesaplamanın, temel seviyede klasik hesaplamadan çok daha üstün özelliklerinin olması ve yeni birtakım fenomenleri doğurması bize matematiksel teoremlerin de ispatında oldukça büyük faydalar sağlamaktadır. Girişim etkileri olmadan klasik yoldan bir matematik teoremin ispatının ancak bir takım önermelerin ve aksiyomların adım adım takip edilmesi sonucunda gerçekleşebileceğini biliyoruz. Ama kuantum etkileri kullanılarak yapılan bir ispatın, artık eski ispat tanımını geride bıraktığını ve bizi ispatın adım adım ulaşılan bir sonuç değil, aslında bir süreç olarak hesaplamanın ta kendisi olduğu görüşüne getirdiğini söyleyebiliriz. Bu yüzden gelecekteki kuantum bilgisayarları teoremlerin ispatını, ne bir insan beyninin ne de başka bir yargı sürecinin adım adım takip edebileceği bir şekilde vermeyecektir. Eğer böyle bir ispata ait adımlar süreci tanımlanabilmiş olsaydı bu adımların yazılacağı kağıt miktarı bütün evreni birkaç defa doldurabilecek miktarda olacaktı!

* ODTÜ Fizik Bölümü

Kaynaklar

D. Deutsch, A. Ekert, R. Lupacchini, Machines, Logic and Quantum Physics

D. Deutsch, Quantum theory, the Church-Turing principle and the universal computer, Proceedings of the Royal Society, A vol. 400 (1985), pp, 339-354

R.P. Feynman, Simulating physics with computers, International Journal of Theoretical physics, vol. 21 (1982), pp. 467-488.

A. Turing, On computable numbers with an application to the Halting Problem, Proceedings of the London Mathematical Society, vol 2. 42(1936-37), pp. 230-265.