Kwantowa rewolucja

Zobacz jak komputery kwantowe zmienią świat

Leon Jeremy

Spis treści

1. Pożegnanie z bitem, powitanie kubitu

Bit – fundament cyfrowego świata

Gdziekolwiek spojrzeć we współczesnym świecie, wszędzie pracują bity. Wiadomość tekstowa wysłana do znajomego, zdjęcie wyświetlone na ekranie telefonu, muzyka płynąca ze słuchawek, film oglądany wieczorem – wszystko to sprowadza się ostatecznie do długich ciągów zer i jedynek. Bit stanowi najmniejszą jednostkę informacji w świecie cyfrowym, a jednocześnie najprostszą z możliwych.

Wyobraźmy sobie zwykły włącznik światła na ścianie. Może znajdować się w jednej z dwóch pozycji: włączonej lub wyłączonej. Nie ma trzeciej opcji, nie ma stanów pośrednich. Światło albo się świeci, albo nie. Właśnie tak działa bit. To przełącznik, który przyjmuje jeden z dwóch stanów, umownie oznaczanych jako 0 i 1. Zero oznacza „wyłączony", jedynka – „włączony". Nic więcej, nic mniej.

Ta prostota może wydawać się rozczarowująca. Trudno uwierzyć, że cała potęga współczesnych komputerów, całe bogactwo internetu, wszystkie cyfrowe cuda technologii opierają się na tak elementarnym fundamencie. A jednak tak właśnie jest. Pojedynczy bit niesie minimalną ilość informacji – odpowiedź na najprostsze możliwe pytanie typu „tak lub nie". Dopiero połączenie ogromnej liczby bitów pozwala zakodować złożone treści. Osiem bitów tworzy bajt, który może reprezentować pojedynczą literę. Miliardy bitów składają się na film w wysokiej rozdzielczości.

Fizycznie bit może przybierać różne formy. W starych komputerach bywał reprezentowany przez kierunek namagnesowania niewielkiego fragmentu taśmy lub dysku. W układach elektronicznych przyjmuje postać napięcia elektrycznego – wyższe napięcie oznacza jedynkę, niższe – zero. W światłowodach bit może być impulsem światła lub jego brakiem. Forma nie ma znaczenia, liczy się tylko to, że zawsze istnieją dokładnie dwa rozróżnialne stany.

Narodziny idei

Zanim bit stał się fundamentem cyfrowej cywilizacji, musiał najpierw zaistnieć jako idea. Stało się to w 1948 roku, gdy młody amerykański matematyk i inżynier Claude Shannon opublikował artykuł zatytułowany „Matematyczna teoria komunikacji". Ten tekst, liczący kilkadziesiąt stron, zmienił sposób rozumienia informacji i położył podwaliny pod całą erę cyfrową.

Shannon pracował wówczas w laboratoriach Bell Telephone Company, gdzie zajmował się problemami przesyłania sygnałów telefonicznych. Zadawał sobie pozornie proste pytania. Czym właściwie jest informacja? Jak ją mierzyć? Ile informacji można przesłać danym kanałem komunikacyjnym? Odpowiedzi, które znalazł, okazały się rewolucyjne.

Przed Shannonem informację traktowano intuicyjnie, jako coś nieokreślonego i trudnego do uchwycenia. On jako pierwszy pokazał, że można ją precyzyjnie zmierzyć i wyrazić liczbowo. Wprowadził pojęcie bitu jako podstawowej jednostki tej miary. Słowo „bit" powstało jako skrót od angielskiego „binary digit", czyli cyfra dwójkowa.

Kluczowa obserwacja Shannona brzmiała następująco: każdą wiadomość można przedstawić jako ciąg odpowiedzi na pytania typu „tak lub nie". Każda taka odpowiedź to jeden bit informacji. Im więcej możliwych wariantów wiadomości, tym więcej bitów potrzeba do jej zakodowania. Rzut monetą daje jeden bit – orzeł lub reszka. Rzut kostką sześcienną wymaga nieco ponad dwóch bitów, bo jest sześć możliwych wyników. Zasada pozostaje ta sama niezależnie od rodzaju przesyłanej treści.

Shannon pokazał również, że istnieją fundamentalne granice szybkości przesyłania informacji przez dowolny kanał komunikacyjny. Granice te zależą od właściwości fizycznych kanału i poziomu szumów, ale nie można ich przekroczyć żadnym sprytnym trikiem. To odkrycie ma

praktyczne znaczenie do dziś – inżynierowie projektujący sieci telekomunikacyjne wciąż odwołują się do twierdzeń Shannona.

Sam Shannon był postacią niezwykłą. Poza pracą naukową konstruował dziwaczne maszyny – żonglujące roboty, urządzenie do przewidywania wyników ruletki, mechaniczną mysz potrafiącą znaleźć wyjście z labiryntu. Jeździł po korytarzach laboratorium na jednokołowym rowerze, czasem żonglując jednocześnie. Ta ekscentryczność nie przeszkadzała mu w tworzeniu teorii, która legła u podstaw całego cyfrowego świata.

Przez kolejne dekady bit pozostawał niezachwiany na swoim miejscu fundamentu informatyki. Komputery stawały się coraz szybsze, mogły przetwarzać coraz więcej bitów na sekundę, ale sama natura bitu nie ulegała zmianie. Zawsze zero albo jeden, włączony albo wyłączony, tak albo nie. Ta binarna logika wydawała się ostateczna i nieprzekraczalna.

Od lamp próżniowych do atomów krzemu

Pierwszym zadaniem konstruktorów komputerów było znalezienie sposobu, by abstrakcyjny bit zamienić w coś namacalnego, w fizyczny obiekt zdolny przechowywać informację. Rozwiązania, które przyjmowano na przestrzeni dekad, różniły się radykalnie pod względem rozmiaru, niezawodności i zużycia energii.

Najwcześniejsze maszyny liczące, budowane w latach czterdziestych dwudziestego wieku, wykorzystywały elektromechaniczne przekaźniki. Przekaźnik to przełącznik sterowany elektromagnesem – gdy płynie przez niego prąd, styki się zamykają, gdy prąd ustaje, styki się otwierają. Jeden przekaźnik mógł reprezentować jeden bit. Przekaźniki pracowały głośno, ich charakterystyczne klikanie wypełniało pomieszczenia pierwszych komputerów. Były też powolne – wykonanie pojedynczego przełączenia zajmowało ułamek sekundy, co ograniczało szybkość obliczeń.

Równolegle rozwijano maszynę z lampami próżniowymi. Lampa próżniowa, zwana też triodą, to szklana bańka z usuniętym powietrzem, wewnątrz której znajdują się elektrody. Przepływ elektronów między elektrodami można kontrolować, przykładając odpowiednie napięcie. W ten sposób lampa działa jak przełącznik, tyle że elektroniczny, bez części ruchomych. Przełączanie następowało znacznie szybciej niż w przekaźnikach.

Komputer ENIAC, uruchomiony w 1945 roku, zawierał około osiemnastu tysięcy lamp próżniowych. Zajmował przestrzeń wielkości sali gimnastycznej i ważył trzydzieści ton. Pobierał tyle energii, że według anegdoty jego włączenie powodowało wahania napięcia w okolicznej sieci elektrycznej. Lampy przepalały się regularnie – średnio co kilka minut jedna wymagała wymiany. Zespół techników pracował bez przerwy, by utrzymać maszynę w ruchu.

Lampy próżniowe wytwarzały ogromne ilości ciepła. Pomieszczenia z komputerami wymagały potężnej klimatyzacji. Same lampy były drogie w produkcji i zawodne. Budowa większych, szybszych komputerów na tej technologii natrafiała na nieprzekraczalne bariery praktyczne.

Przełom nastąpił w 1947 roku, gdy w tych samych laboratoriach Bell, gdzie pracował Shannon, trzej fizycy – William Shockley, John Bardeen i Walter Brattain – skonstruowali pierwszy tranzystor. To niewielkie urządzenie półprzewodnikowe działało jak lampa próżniowa, ale było znacznie mniejsze, tańsze, bardziej niezawodne i zużywało ułamek energii. Za to osiągnięcie twórcy tranzystora otrzymali później Nagrodę Nobla.

Tranzystor działa na pozór prosto. Wykonany jest z materiału półprzewodnikowego, zazwyczaj krzemu. W zależności od przyłożonego napięcia przepuszcza prąd lub go blokuje. Te dwa stany odpowiadają bitowym wartościom jeden i zero. W rzeczywistości fizyka stojąca za działaniem tranzystora jest subtelna i wymaga mechaniki kwantowej do

pełnego zrozumienia, ale z perspektywy użytkownika liczy się efekt końcowy: niezawodny, miniaturowy przełącznik.

Kolejne dekady przyniosły nieustanny postęp w miniaturyzacji. W latach sześćdziesiątych nauczono się umieszczać wiele tranzystorów na jednej płytce krzemu, tworząc układy scalone. Z czasem liczba tranzystorów rosła wykładniczo. Pierwszy komercyjny mikroprocesor, Intel 4004 z 1971 roku, zawierał około dwóch tysięcy tranzystorów. Współczesne procesory mieszczą ich dziesiątki miliardów.

Pojedynczy tranzystor w nowoczesnym procesorze mierzy zaledwie kilka nanometrów. Dla porównania – ludzki włos ma średnicę około osiemdziesięciu tysięcy nanometrów. Na przekroju włosa zmieściłoby się tysiące tranzystorów ułożonych w rzędzie. Ta zdumiewająca miniaturyzacja pozwoliła zmieścić moc obliczeniową dawnych sal komputerowych w urządzeniach noszonych w kieszeni.

Zmniejszanie tranzystorów napotyka jednak granice. Gdy rozmiary zbliżają się do skali pojedynczych atomów, zaczynają się ujawniać dziwne efekty związane z naturą materii w najmniejszych skalach. Elektrony nie zachowują się już jak posłuszne kulki, które można dowolnie kierować. Zaczynają rządzić się innymi prawami.

Od pojedynczego bitu do cyfrowego świata

Pojedynczy bit może powiedzieć tylko „tak" lub „nie", „włączony" lub „wyłączony". To zbyt mało, by zakodować cokolwiek użytecznego. Prawdziwa moc kryje się w łączeniu wielu bitów razem.

Dwa bity dają cztery możliwe kombinacje: 00, 01, 10, 11. Trzy bity to osiem kombinacji. Każdy dodatkowy bit podwaja liczbę możliwości. Osiem bitów, nazwanych bajtem, pozwala zapisać jedną z dwustu pięćdziesięciu sześciu różnych wartości. Wystarczy to, by zakodować pojedynczą literę alfabetu łacińskiego wraz z cyframi i znakami przestankowymi.

Bajt stał się podstawową jednostką praktyczną w informatyce, choć sam w sobie też nie pomieści zbyt wiele. Pojedyncze słowo tekstu zajmuje kilka bajtów. Strona tekstu to kilka tysięcy bajtów, czyli kilka kilobajtów. Kilobajt to tysiąc bajtów, megabajt to milion, gigabajt to miliard.

Te jednostki szybko przekładają się na codzienne doświadczenie. Wiadomość tekstowa wysłana z telefonu zajmuje zazwyczaj mniej niż kilobajt. Zdjęcie wykonane smartfonem może ważyć kilka megabajtów – to miliony bajtów, dziesiątki milionów bitów, wszystkie niezbędne do zapisania informacji o kolorze każdego punktu obrazu. Film w wysokiej rozdzielczości trwający dwie godziny zajmuje kilka gigabajtów, a więc miliardy bajtów, dziesiątki miliardów bitów.

Każdy piksel zdjęcia opisany jest przez wartości liczbowe określające nasycenie barw składowych – czerwonej, zielonej i niebieskiej. Każda z tych wartości zajmuje zwykle jeden bajt. Zdjęcie o rozdzielczości dwunastu megapikseli zawiera dwanaście milionów punktów, każdy opisany trzema bajtami – to daje trzydzieści sześć milionów bajtów surowych danych. Algorytmy kompresji zmniejszają tę liczbę, usuwając powtórzenia i wykorzystując ograniczenia ludzkiego wzroku, ale wciąż pozostają miliony bitów.

Film to sekwencja obrazów wyświetlanych kilkadziesiąt razy na sekundę, uzupełniona ścieżką dźwiękową. Dźwięk także zapisuje się cyfrowo – mikrofon zamienia fale ciśnienia powietrza na sygnał elektryczny, który następnie zostaje zmierzony dziesiątki tysięcy razy na sekundę. Każdy pomiar to liczba wyrażona w bitach. Nawet sekunda muzyki wymaga setek tysięcy bitów.

Dysk twardy w typowym laptopie mieści dziś kilkaset gigabajtów lub kilka terabajtów. Terabajt to tysiąc gigabajtów, bilion bajtów, osiem bilionów bitów. Każdy z tych bitów ma swoją fizyczną reprezentację – mikroskopijny obszar namagnesowany w określonym kierunku lub niewielki ładunek elektryczny uwięziony w komórce pamięci.

Internet przesyła biliony bitów na sekundę w skali globalnej. Każde kliknięcie, każde wyszukiwanie, każdy przesłany plik rozkłada się na strumień zer i jedynek wędrujących przez światłowody i fale radiowe. Serwery rozsiane po całym świecie nieustannie przetwarzają te potoki bitów, wykonując operacje logiczne na niezliczonych przełącznikach.

Tyrania jednoznaczności

Siła bitu jest zarazem jego fundamentalnym ograniczeniem. Każdy bit musi przyjąć konkretny stan – zero albo jeden, nigdy nic pomiędzy. Ta bezwzględna binarność przenika całą klasyczną informatykę i określa sposób, w jaki komputery przetwarzają informację.

Gdy komputer wykonuje obliczenia, każda operacja prowadzi do jednoznacznego wyniku. Dodawanie dwóch liczb daje jedną konkretną sumę. Porównanie dwóch wartości zwraca odpowiedź „większe" albo „mniejsze", ewentualnie „równe". Nie istnieje możliwość odpowiedzi „prawdopodobnie większe" ani „raczej równe". Komputer nie zna odcieni szarości – widzi wyłącznie czerń i biel.

Ta cecha doskonale sprawdza się w wielu zastosowaniach. Księgowość wymaga precyzji – stan konta musi być określony co do grosza. Sterowanie maszynami przemysłowymi nie toleruje niejednoznaczności – zawór jest otwarty lub zamknięty. Bazy danych przechowują fakty, które mają być jednoznacznie prawdziwe lub fałszywe.

Problemy zaczynają się, gdy rzeczywistość nie daje się łatwo wtłoczyć w binarne ramy. Rozpoznawanie twarzy na zdjęciu to zadanie, w którym nie ma prostej odpowiedzi „tak" lub „nie". Obraz może przedstawiać twarz częściowo zasłoniętą, widzianą pod nietypowym kątem, w słabym oświetleniu. Człowiek poradziłby sobie z taką sytuacją intuicyjnie, dostrzegając stopnie podobieństwa i niepewności. Klasyczny komputer musi ostatecznie wydać werdykt – rozpoznano lub nie rozpoznano – nawet gdy sytuacja jest głęboko niejednoznaczna.

Programiści radzą sobie z tym ograniczeniem, wprowadzając prawdopodobieństwa. Zamiast odpowiedzi „to jest kot", program może obliczyć „prawdopodobieństwo, że to kot, wynosi dziewięćdziesiąt trzy procent". Jednak te prawdopodobieństwa same w sobie są zapisane jako ciągi bitów. Wewnętrznie komputer wciąż operuje wyłącznie zerami i jedynkami, symulując płynność i niepewność za pomocą dyskretnych wartości.

Podobne wyzwania pojawiają się przy optymalizacji złożonych problemów. Wyobraźmy sobie zadanie ułożenia planu dostaw dla setek ciężarówek rozwożących towary do tysięcy punktów. Każda możliwa trasa ma określony koszt – zużycie paliwa, czas jazdy, opłaty drogowe. Zadaniem jest znalezienie najtańszego rozwiązania. Problem w tym, że liczba możliwych kombinacji rośnie astronomicznie wraz z liczbą punktów. Klasyczny komputer musi sprawdzać warianty jeden po drugim, każdorazowo dochodząc do jednoznacznej odpowiedzi „ta trasa kosztuje tyle". Nie może jednocześnie eksplorować wielu możliwości, nie może odpowiedzieć „te wszystkie trasy są mniej więcej równoważne".

Pewne problemy matematyczne mają strukturę, która sprawia, że klasyczne podejście bit po bicie staje się beznadziejnie powolne. Rozkład dużej liczby na czynniki pierwsze – operacja kluczowa dla współczesnej kryptografii – wymaga w klasycznym ujęciu sprawdzenia ogromnej liczby potencjalnych dzielników. Każde sprawdzenie to sekwencja operacji na bitach, każda operacja daje jednoznaczny wynik, a następne sprawdzenie może ruszyć dopiero po zakończeniu poprzedniego. Binarny komputer musi cierpliwie przebijać się przez możliwości jedna po drugiej.

Innym przykładem jest symulowanie układów fizycznych złożonych z wielu oddziałujących elementów. Zachowanie pojedynczej cząsteczki można opisać równaniami i obliczyć na komputerze. Zachowanie dwóch oddziałujących cząsteczek wymaga uwzględnienia ich wzajemnego wpływu. Przy trzech cząsteczkach sytuacja się komplikuje, przy dziesięciu staje się trudna, przy stu wymaga potężnych zasobów

obliczeniowych. A przecież prawdziwe układy chemiczne i biologiczne składają się z miliardów miliardów cząsteczek, z których każda wpływa na każdą.

Fundamentalny problem polega na tym, że świat fizyczny nie jest binarny. Cząsteczki nie istnieją w stanach zero-jedynkowych. Elektrony nie zachowują się jak maleńkie przełączniki. Przyroda operuje płynnością i nieoznaczonością, a klasyczny komputer próbuje ją opisać za pomocą narzędzia, które zna tylko skrajności.

Kubit – informacja w stanie zawieszenia

Wyobraźmy sobie monetę wirującą w powietrzu. Dopóki nie upadnie na stół, nie można powiedzieć, czy pokazuje orła czy reszkę. Nie jest ani jednym, ani drugim – a jednocześnie jest w pewnym sensie oboma naraz, gotowa stać się którymkolwiek z nich w momencie upadku.

Ta metafora przybliża ideę kubitu, choć jak każda metafora ma swoje ograniczenia. Kubit to kwantowy odpowiednik bitu, podstawowa jednostka informacji w świecie obliczeń kwantowych. W przeciwieństwie do klasycznego bitu, który zawsze przyjmuje jednoznaczny stan zero albo jeden, kubit może istnieć w czymś znacznie dziwniejszym – w stanie zawieszenia między tymi możliwościami.

Fizycy nazywają ten stan superpozycją. Słowo może brzmieć technicznie, ale opisuje sytuację zaskakująco prostą w swojej istocie: kubit nie musi dokonywać wyboru. Może pozostawać w stanie, który zawiera w sobie zarówno zero, jak i jeden, w różnych proporcjach. Nie chodzi o to, że nie wiemy, w jakim stanie się znajduje, tak jakbyśmy po prostu nie sprawdzili. Kubit naprawdę nie znajduje się ani w stanie zero, ani w stanie jeden – jest w stanie, który nie ma odpowiednika w klasycznym świecie.

To fundamentalna różnica między niewiedzą a nieoznaczonością. Gdy rzucamy zwykłą kostką i zakrywamy ją dłonią, kostka pokazuje konkretną liczbę – po prostu jej nie widzimy. Nasza niewiedza nie zmienia faktu, że wynik już istnieje. Z kubitem jest inaczej. Przed pomiarem kubit rzeczywiście nie ma określonej wartości. Wartość powstaje dopiero w momencie odczytu.

Można pomyśleć o tym jak o pytaniu, które jeszcze nie zostało zadane. Przed zadaniem pytania nie istnieje odpowiedź czekająca gdzieś na odkrycie. To samo pytanie, kontekst i moment jego zadania współtworzą odpowiedź. Kubit przed pomiarem jest jak pytanie wiszące w powietrzu, pełne potencjalnych odpowiedzi, z których żadna nie jest jeszcze wybrana.

Proporcje, w jakich kubit zawiera zero i jeden, można precyzyjnie kontrolować. Kubit może być prawie całkowicie zerem z niewielką domieszką jedynki. Może być niemal jedynką z nikłą domieszką zera. Może być dokładnie po połowie jednym i drugim. Cały zakres możliwości między skrajnościami stoi otworem. To bogactwo stanów pośrednich stanowi jeden z kluczowych zasobów obliczeń kwantowych.

Wirująca moneta

Metafora wirującej monety zasługuje na głębsze rozwinięcie, ponieważ pomaga uchwycić istotę superpozycji lepiej niż abstrakcyjne opisy. Wyobraźmy sobie więc monetę podrzuconą wysoko w powietrze, obracającą się wokół własnej osi dziesiątki razy na sekundę.

W każdym ułamku sekundy moneta ukazuje naprzemiennie obie strony. Gdyby ktoś zapytał, co teraz pokazuje – orła czy reszkę – pytanie nie miałoby sensu. Wirująca moneta nie jest ani jednym, ani drugim, a zarazem jest obiema możliwościami w ruchu, w dynamicznej jedności. Dopiero gdy spadnie na stół i znieruchomieje, jednoznaczna odpowiedź stanie się możliwa.

Kubit w superpozycji przypomina tę wirującą monetę. Zawiera w sobie obie możliwości – zero i jeden – w sposób, który nie pozwala wskazać żadnej z nich jako tej właściwej w danej chwili. Moneta wiruje, kubit trwa w superpozycji. Oba stany są równie realne i równie obecne.

Analogia ma jednak swoje granice. Wirująca moneta jest obiektem klasycznym – gdybyśmy mieli wystarczająco szybką kamerę, moglibyśmy w każdej chwili zobaczyć, która strona akurat zwrócona jest w naszym kierunku. Moneta zawsze pokazuje konkretną stronę, tylko zmienia ją bardzo szybko. Z kubitem jest fundamentalnie inaczej. Nie chodzi o szybkie przeskakiwanie między zerem a jedynką, zbyt szybkie, by je zarejestrować. Kubit naprawdę nie ma w danym momencie określonej wartości. Superpozycja nie jest szybkim migotaniem między stanami – jest czymś głębszym, stanem niemającym odpowiednika w codziennym doświadczeniu.

Inna przydatna analogia odwołuje się do dźwięku. Gdy uderza się w strunę gitary, wibruje ona z pewną podstawową częstotliwością, ale jednocześnie obecne są tony harmoniczne – wielokrotności tej częstotliwości. Dźwięk, który słyszymy, jest złożeniem wszystkich tych wibracji naraz. Struna nie wybiera między tonem podstawowym a harmonicznymi, wydaje je wszystkie jednocześnie, a dopiero nasze ucho i mózg rozkładają to złożenie na składowe.

Kubit w superpozycji przypomina taką wibrującą strunę. Zawiera w sobie różne składowe – odpowiadające zeru i jedynce – które współistnieją, dopóki coś nie wymusi na nich rozdzielenia. Informacja nie jest jeszcze skrystalizowana, pozostaje rozproszona między możliwościami.

Moment decyzji

Stan zawieszenia nie może trwać wiecznie. Gdy nadchodzi moment pomiaru, kubit musi wreszcie odpowiedzieć na pytanie: zero czy jeden? I wtedy dzieje się coś nieodwracalnego.

Superpozycja rozpada się. Wirująca moneta upada na stół. Ze wszystkich współistniejących możliwości pozostaje tylko jedna – konkretna, namacalna, klasyczna wartość. Kubit pokazuje zero albo jeden, nigdy obie wartości naraz. Pomiar kończy stan zawieszenia i wymusza jednoznaczność.

Ten proces nazywany jest kolapsem stanu kwantowego lub redukcją wektora stanu. Nazwy brzmią technicznie, ale opisują coś intuicyjnie zrozumiałego: przejście od wielu możliwości do jednego faktu. Przed pomiarem kubit zawierał różne potencjalne odpowiedzi, po pomiarze zawiera tylko jedną rzeczywistą odpowiedź.

Kluczowe pytanie brzmi: co decyduje o tym, który wynik się pojawi? Jeśli kubit był w superpozycji pół na pół – równe proporcje zera i jedynki – to co sprawia, że po pomiarze zobaczymy akurat zero, a nie jeden? Odpowiedź może rozczarowywać: nic konkretnego nie decyduje. Wynik jest fundamentalnie losowy.

To nie jest losowość wynikająca z niewiedzy, jak przy rzucie klasyczną kostką, gdzie teoretycznie można by obliczyć wynik, znając wszystkie siły działające na kostkę. Losowość kwantowa jest losowością u samych podstaw rzeczywistości. Żadna ukryta przyczyna nie determinuje wyniku, żadna głębsza teoria nie pozwala go przewidzieć z całkowitą pewnością. Proporcje superpozycji określają jedynie prawdopodobieństwa – kubit w stanie bardziej przechylonym ku jedynce częściej pokaże jedynkę przy pomiarze, ale każdy pojedynczy pomiar pozostaje nieprzewidywalny.

To, co można przewidzieć, to rozkład statystyczny. Gdyby przygotować tysiąc identycznych kubitów w tej samej superpozycji i zmierzyć je wszystkie, proporcja zer do jedynek będzie odpowiadać proporcjom w superpozycji. Prawidłowość wyłania się dopiero z powtórzeń, nigdy z pojedynczego zdarzenia.

Po dokonaniu pomiaru kubit nie wraca automatycznie do poprzedniej superpozycji. Informacja o jego wcześniejszym stanie zostaje bezpowrotnie utracona. Nie da się zmierzyć kubitu i potem odtworzyć superpozycji, która przed chwilą istniała. Pomiar nie jest neutralną obserwacją – jest ingerencją, która nieodwracalnie zmienia stan układu.

Paradoks pojemności

W tym miejscu łatwo o nieporozumienie, które warto rozwiać od razu. Skoro kubit może być jednocześnie zerem i jedynką, to czy nie oznacza to, że przechowuje dwa razy więcej informacji niż klasyczny bit? A może jeszcze więcej, skoro możliwe są różne proporcje superpozycji?

Odpowiedź jest przecząca i może wydawać się zaskakująca. Kubit nie przechowuje więcej informacji niż zwykły bit. Gdy nadchodzi moment pomiaru – a pomiar jest jedynym sposobem wydobycia informacji z kubitu – otrzymujemy zawsze tylko jeden wynik: zero albo jeden. Dokładnie tyle samo, ile z klasycznego bitu. Cała bogata struktura superpozycji, wszystkie proporcje i fazy, wszystko to redukuje się do pojedynczej odpowiedzi binarnej.

Przewaga kubitu leży więc gdzie indziej – nie w przechowywaniu informacji, lecz w sposobie jej przetwarzania. To subtelna, ale kluczowa różnica.

Klasyczny komputer wykonuje obliczenia krok po kroku. Jeśli ma sprawdzić dziesięć możliwości, musi przetworzyć każdą z nich osobno, jedną po drugiej. Kubit w superpozycji może natomiast uczestniczyć w obliczeniach, które dotyczą wielu możliwości równocześnie. Superpozycja nie służy magazynowaniu większej ilości danych, lecz równoległemu przetwarzaniu różnych wariantów w tym samym czasie.

Można pomyśleć o tym jak o różnicy między czytaniem dziesięciu książek po kolei a w jakiś sposób przeglądaniem ich wszystkich naraz.

Na końcu i tak można opowiedzieć tylko o jednej – tej, która okaże się najważniejsza – ale proces dochodzenia do wniosku przebiegał inaczej. Kubit nie pozwala wyciągnąć więcej informacji na końcu, pozwala jednak przetworzyć więcej informacji po drodze.

Ta cecha staje się potężna dopiero przy odpowiednim wykorzystaniu. Nie każdy problem obliczeniowy nadaje się do takiego równoległego podejścia. Ale te, które się nadają, mogą zyskać ogromne przyspieszenie – nie dlatego, że kubity przechowują więcej danych, lecz dlatego, że przetwarzają je w fundamentalnie inny sposób.

Kruchość kwantowa

Superpozycja jest stanem niezwykle delikatnym. Kubit w swoim zawieszeniu między zerem a jedynką przypomina akrobatę balansującego na linie – najmniejsze zakłócenie może zakończyć występ przed czasem.

Otoczenie kubitu nieustannie próbuje z nim oddziaływać. Przypadkowe fotony światła, drgania cieplne atomów, błądzące pola elektromagnetyczne – wszystko to może zaburzyć delikatny stan superpozycji. Każde takie oddziaływanie jest formą mimowolnego pomiaru, który wymusza na kubicie przejście do konkretnego stanu klasycznego. Wirująca moneta upada, nim nadszedł na to właściwy moment.

Zjawisko to sprawia, że superpozycja ma charakter ulotny. Nie można kubitu przygotować w odpowiednim stanie, a potem odłożyć na półkę i wrócić do niego za godzinę. Stan kwantowy rozpływa się w ułamkach sekund, czasem w milionowych częściach sekundy. Informacja zakodowana w superpozycji wycieka do otoczenia, rozmywa się, przestaje istnieć jako coś odrębnego i kontrolowalnego.

Ta kruchość nie wynika z niedoskonałości technologii, którą można by kiedyś przezwyciężyć. Jest wpisana w samą naturę zjawisk kwantowych. Im większy i cieplejszy obiekt, tym więcej oddziałuje z otoczeniem i tym

szybciej traci właściwości kwantowe. Dlatego codzienne przedmioty – kamienie, stoły, ludzie – nie wykazują superpozycji, choć zbudowane są z kwantowych cząstek. Skala makroskopowa i nieustanne oddziaływania z otoczeniem niszczą superpozycję, zanim zdążyłaby się ujawnić.

Kubit musi być chroniony przed światem zewnętrznym z niezwykłą starannością. Wymaga izolacji od wszelkich zakłóceń, często ekstremalnie niskich temperatur, próżni, ekranowania elektromagnetycznego. Nawet przy tych wszystkich środkach ostrożności okno czasowe na przeprowadzenie obliczeń pozostaje bardzo krótkie. To wyścig z rozpadem – trzeba zdążyć wykonać operacje, zanim superpozycja zdąży się rozwiać.

Kruchość superpozycji jest jednym z powodów, dla których budowa użytecznych komputerów kwantowych stanowi tak ogromne wyzwanie inżynieryjne. To nie kwestia zminiaturyzowania istniejącej technologii ani po prostu zwiększenia mocy obliczeniowej. To walka z fundamentalnymi właściwościami natury, która zdaje się nie lubić, gdy informacja kwantowa pozostaje zbyt długo w stanie zawieszenia.

Różnice w zapisie i przetwarzaniu danych

Sposób, w jaki komputer rozwiązuje problem, można przyrównać do przeszukiwania labiryntu. Wyobraźmy sobie ogromny labirynt z jednym wejściem i jednym wyjściem, pełen ślepych uliczek i rozwidleń. Zadaniem jest znalezienie drogi prowadzącej na drugą stronę.

Komputer klasyczny podchodzi do tego zadania jak samotny wędrowiec. Wchodzi do labiryntu i na pierwszym rozwidleniu musi wybrać jedną z dróg. Idzie nią, dopóki nie trafi na ścianę lub kolejne rozwidlenie. Gdy utknie, cofa się i próbuje innej ścieżki. Każdą możliwość sprawdza osobno, jedną po drugiej, cierpliwie eliminując ślepe zaułki. Jeśli labirynt

ma tysiąc rozgałęzień, wędrowiec może być zmuszony przejść tysiąc tras, zanim znajdzie właściwą.

Komputer kwantowy działa inaczej. Zamiast pojedynczego wędrowca można sobie wyobrazić chmurę możliwości – jakby wszystkie potencjalne ścieżki były eksplorowane jednocześnie. Na każdym rozwidleniu nie trzeba wybierać jednej drogi, bo superpozycja pozwala podążać wszystkimi naraz. Ścieżki prowadzące donikąd wygaszają się wzajemnie, podczas gdy ścieżki zbliżające się do celu wzmacniają. Z tej chmury możliwości wyłania się ostatecznie odpowiedź – droga przez labirynt.

Oczywiście jest to uproszczenie, ale oddaje istotę różnicy. Klasyczne przetwarzanie jest sekwencyjne – jedna rzecz po drugiej, jak koraliki nawlekane na sznurek. Przetwarzanie kwantowe wykorzystuje równoczesność wpisaną w naturę superpozycji. Nie chodzi o to, że komputer kwantowy jest po prostu szybszy w wykonywaniu tych samych kroków. On wykonuje obliczenie w fundamentalnie inny sposób.

Ta różnica ma konsekwencje praktyczne tylko dla pewnych rodzajów problemów. Istnieją zadania, gdzie sekwencyjne sprawdzanie możliwości jest jedyną rozsądną metodą – i tam komputer klasyczny radzi sobie równie dobrze. Ale istnieją też problemy, gdzie liczba możliwości rośnie tak szybko, że żaden klasyczny komputer nie zdołałby ich wszystkich sprawdzić przed końcem wszechświata. W takich przypadkach zdolność do równoczesnej eksploracji wielu ścieżek staje się decydująca.

Cienie w labiryncie

Warto rozwinąć analogię labiryntu, bo dobrze ilustruje różnicę między klasycznym a kwantowym przetwarzaniem informacji. Wyobraźmy sobie osobę stojącą u wejścia do rozległego labiryntu z latarką w dłoni. Światło latarki oświetla tylko jeden korytarz naraz – ten, który aktualnie

jest eksplorowany. Każde rozwidlenie wymaga decyzji: w lewo czy w prawo? Wybrawszy jedną ścieżkę, trzeba nią podążać, aż okaże się ślepą uliczką lub doprowadzi do celu. Dopiero wtedy można wrócić i spróbować inaczej.

Komputer kwantowy działa tak, jakby zamiast osoby z latarką do labiryntu weszło widmo zdolne rozdzielać się na każdym rozwidleniu. Na pierwszym skrzyżowaniu jeden cień skręca w lewo, drugi w prawo. Na kolejnych rozwidleniach każdy cień dzieli się znowu. Wkrótce labirynt wypełnia się mgiełką rozgałęziających się możliwości, z których każda bada inną trasę w tym samym czasie.

Te cienie nie są od siebie niezależne – interferują ze sobą jak fale na wodzie. Gdy dwie fale spotykają się w tym samym miejscu, mogą się wzmocnić lub wygasić w zależności od tego, czy ich szczyty się nakładają, czy jeden szczyt trafia na dolinę drugiej fali. Podobnie cienie w labiryncie – ścieżki prowadzące do rozwiązania wzmacniają się wzajemnie, podczas gdy ślepe zaułki wygaszają się nawzajem.

Na końcu, gdy przychodzi moment pomiaru, z całej tej chmury możliwości wyłania się jedna konkretna odpowiedź. Jeśli obliczenie zostało dobrze zaprojektowane, będzie to odpowiedź właściwa – droga prowadząca przez labirynt. Sztuczka polega na tym, że wszystkie ślepe uliczki zostały zbadane i odrzucone równocześnie, bez konieczności przechodzenia ich jedna po drugiej.

Granice przewagi

Należy wystrzegać się wrażenia, że komputer kwantowy jest uniwersalnie lepszy od klasycznego. To nieprawda i prowadzi do głębokich nieporozumień.

Wiele codziennych zadań obliczeniowych nie zyskuje nic na podejściu kwantowym. Edycja tekstu, przeglądanie internetu, odtwarzanie muzyki, wyświetlanie grafiki – wszystko to opiera się na operacjach, które klasyczne komputery wykonują doskonale i które nie mają struktury

pozwalającej wykorzystać superpozycję. Wysyłanie cieni wszystkimi korytarzami nie pomaga, gdy zadanie wymaga po prostu przejścia jednym konkretnym korytarzem od początku do końca.

Dodawanie liczb pozostaje dodawaniem liczb. Dwa plus dwa równa się cztery i żadna superpozycja tego nie zmieni ani nie przyspieszy. Podobnie sortowanie listy nazwisk, wyszukiwanie słowa w tekście czy obliczanie podatku – to zadania, gdzie klasyczny komputer radzi sobie świetnie, bo ich struktura nie zawiera elementu masowej równoległości, którą można by wykorzystać.

Co więcej, w wielu przypadkach komputer klasyczny pozostaje nie tylko wystarczający, ale wręcz lepszy. Jest prostszy w obsłudze, tańszy, bardziej niezawodny. Nie wymaga ekstremalnych warunków działania. Jego wyniki są deterministyczne i powtarzalne. Dziesięciolecia rozwoju technologii sprawiły, że klasyczne procesory osiągnęły zadziwiającą wydajność i elastyczność.

Komputer kwantowy błyszczy w specyficznych niszach – tam, gdzie klasyczne podejście napotyka fundamentalne bariery. Problemy optymalizacyjne o ogromnej liczbie możliwych rozwiązań. Symulacje układów kwantowych, gdzie natura problemu sama jest kwantowa. Pewne typy przeszukiwania i rozkładu matematycznego. To nie są marginalne zagadnienia – mają znaczenie w chemii, farmakologii, logistyce, finansach – ale nie stanowią całości informatyki.

Przyszłość obliczeń nie polega zapewne na zastąpieniu klasycznych komputerów kwantowymi. Raczej oba typy maszyn będą współistnieć, każdy stosowany tam, gdzie jego mocne strony przychodzą do głosu. Klasyczne komputery do codziennych zadań, kwantowe do wyspecjalizowanych problemów, których struktura pozwala wykorzystać przewagę superpozycji. Jak śrubokręt i młotek – oba są narzędziami, żadne nie jest uniwersalnie lepsze, każde ma swoje zastosowania.

Pewność i prawdopodobieństwo

Gdy klasyczny komputer kończy obliczenie, wynik jest jednoznaczny i powtarzalny. Zadając to samo pytanie po raz drugi, trzeci czy tysięczny, otrzymuje się identyczną odpowiedź. Dodawanie dwóch i dwóch zawsze da cztery, nigdy cokolwiek innego. Ta determinizm stanowi fundament zaufania do klasycznych maszyn – można polegać na tym, że wynik jest poprawny i nie zmieni się przy ponownym sprawdzeniu.

Komputer kwantowy działa inaczej. Ponieważ superpozycja redukuje się do konkretnego wyniku w sposób probabilistyczny, pojedyncze uruchomienie obliczeń nie musi dać poprawnej odpowiedzi. Może ją dać – i dobrze zaprojektowany algorytm kwantowy sprawia, że prawdopodobieństwo poprawnej odpowiedzi jest wysokie – ale gwarancji nie ma.

Wyobraźmy sobie algorytm kwantowy, który z prawdopodobieństwem dziewięćdziesięciu procent daje prawidłowy wynik. Przy pojedynczym uruchomieniu istnieje dziesięcioprocentowa szansa, że odpowiedź będzie błędna. Aby zyskać pewność, trzeba uruchomić obliczenie wielokrotnie i sprawdzić, która odpowiedź pojawia się najczęściej. Po stu powtórzeniach właściwy wynik powinien dominować w statystyce, pozwalając go zidentyfikować z dużą pewnością.

To podejście może wydawać się marnotrawstwem – po co uruchamiać coś sto razy, skoro klasyczny komputer daje pewną odpowiedź za pierwszym razem? Odpowiedź tkwi w skali trudności problemu. Jeśli klasyczny komputer potrzebowałby tysiąca lat na znalezienie rozwiązania, a kwantowy znajduje je z dziewięćdziesięcioprocentową pewnością w godzinę, to nawet konieczność stu powtórzeń daje sto godzin zamiast tysiąca lat. Przewaga pozostaje przytłaczająca.

Probabilistyczna natura wyników wymaga jednak innego podejścia do weryfikacji. Nie wystarczy uruchomić programu raz i przyjąć wynik za pewnik. Potrzebna jest analiza statystyczna, powtórzenia, ocena

rozkładu odpowiedzi. To dodatkowa warstwa złożoności, nieobecna w klasycznym przetwarzaniu danych.

Niektóre algorytmy kwantowe dają wyniki, które można łatwo zweryfikować klasycznie, nawet jeśli znalezienie ich klasycznie byłoby trudne. To korzystna sytuacja – komputer kwantowy proponuje rozwiązanie, komputer klasyczny sprawdza, czy jest poprawne. Jeśli nie jest, próba się powtarza. Ta hybryda łączy moc eksploracyjną obliczeń kwantowych z niezawodnością klasycznej weryfikacji.