15 Komputery kwantowe

Komputery kwantowe to maszyny obliczeniowe o supermocy, możliwe dzięki dziwacznym prawom fizyki kwantowej. W ciągu kilku minut mogą wykonywać zadania, które na komputerze osobistym trwałyby dłużej niż wiek Wszechświata, i już są dostępne w laboratoriach na całym świecie.

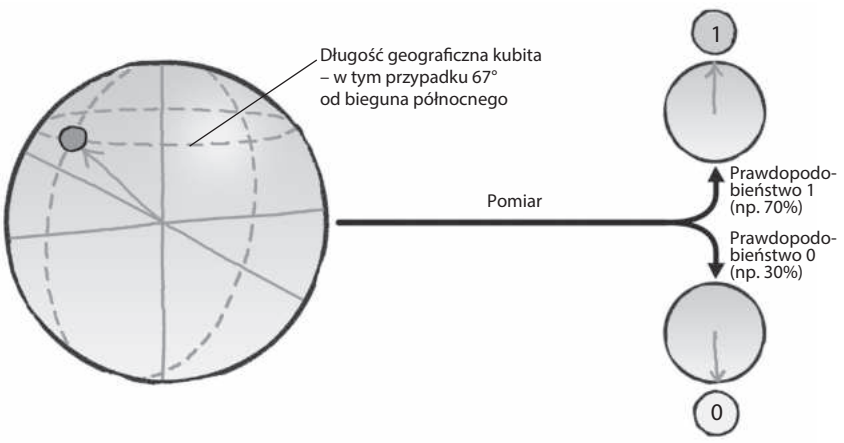
Dzisiejsze komputery działają, przechowując bity informacji (patrz s. 61), wykorzystując stany wł./wył. przełączników elektrycznych zwanych tranzystorami. Ale tranzystory działają zgodnie ze „starymi", klasycznymi prawami fizyki. Na początku XX wieku fizyka klasyczna ustąpiła nowemu podejściu – mechanice kwantowej (patrz s. 39). Podczas gdy fizyka klasyczna pozostaje w pewnych okolicznościach rozsądnym przybliżeniem, szybko stało się jasne, że teoria kwantowa daje prawdziwy obraz rzeczywistości. W roku 1985 brytyjski fizyk teoretyczny David Deutsch zdał sobie sprawę, że obliczenia komputerowe w obecnej postaci są oparte na niewłaściwej fizyce. Zajął się przekształceniem teorii obliczeń do ram kwantowych, co prowadzi do całkiem nowego projektu komputerów – zdecydowanie przewyższających swoich poprzedników.

Hello, kubit W nowym obrazie bity informacji – które klasycznie mogą przyjmować wartości 0 lub 1 – zostają zastąpione przez bity kwantowe, czyli kubity, które jednocześnie mogą być i 0, i 1. Jest to możliwe, gdyż mechanika kwantowa pozwala cząsteczce kwantowej istnieć w mieszaninie wszystkich możliwych stanów do chwili dokonania pomiaru (patrz s. 41). Więc jeśli informacje zapiszemy w świecie kwantowym, to one także będą istniały w mieszance wszystkich możliwych stanów.

Można uważać, że jest to poważny problem dla maszyny obliczeniowej, ale w istocie jest to kluczowa kwestia mocy komputerów kwantowych. Gdy bit informacji przechodzi przez zwykły procesor komputera,

przetwarzane jest tylko 0 lub 1 (zależnie od wartości bitu). Ale gdy przez procesor kwantowy przechodzi kubit, to zarówno 0, jak i 1 są przetwarzane jednocześnie. Jeśli teraz połączymy klasycznie osiem bitów, aby utworzyć bajt, to możemy zapisać dowolną liczbę od 0 do 255. Jeśli nasz komputer kwantowy ma osiem kubitów (czyli kubajt), to może przechować wszystkie te liczby w tym samym czasie i wszystkie jednocześnie przetwarzać w czasie, który klasycznemu komputerowi zabiera przerobienie jednej liczby. Ogólnie biorąc, komputer kwantowy mający n kubitów może przechować i przetwarzać jednocześnie 2^n liczb. Deutsch nazywa to „równoległością kwantową" – węzłem do przetwarzania równoległego na komputerach klasycznych, gdzie kilka procesorów współdziała razem nad zadaniem.

Słowo „równoległy" jest jednak w tym przypadku szczególnie ostre. Deutsch wierzy w interpretację teorii kwantowej jako „wielu światów" – gdzie dziwne zachowanie kwanta, powiedzmy cząsteczki subatomowej, jest powodowane przez interferencję kopii jej samej w równoległym



Fizycy reprezentują stan kubita jako długość geograficzną na kuli, gdzie biegun północny reprezentuje wartość 1, a biegun południowy wartość 0. Wszędzie między biegunami mamy mieszankę tych dwóch wartości, z prawdopodobieństwem 1 lub 0 pomiaru wynikającego ze wzoru trygonometrycznego opartego na długości geograficznej kubita względem bieguna

LINIA CZASU

1985

David Deutsch stworzył podstawy teoretyczne komputerów kwantowych

1994

Peter Shor opracował algorytm kwantowy do rozkładu dużych liczb na czynniki

1998

Uczeni z uniwersytetu w Oxfordzie pokazali pierwszy działający komputer kwantowy

wszechświecie (patrz s. 228). W tym ujęciu komputer kwantowy dosłownie wyprowadza swoją moc ze swoich odpowiedników w sąsiednich Wszechświatach. Nie jest to wcale tak wydumane jak może się wydawać – przechowywanie wszystkich informacji wymaganych do przeprowadzenia pewnych obliczeń kwantowych zabiera więcej klasycznych bitów informacji niż jest atomów w naszym Wszechświecie. W ujęciu Deutscha komputery kwantowe muszą wykorzystywać inne Wszechświaty, bo inaczej nie starczyło by im pamięci do wykonania wszystkich zadań, które już teraz wykonują.

Obliczenia w działaniu W roku 1988 pierwszy działający komputer kwantowy został pokazany przez uczonych na uniwersytecie w Oxfordzie, w Anglii. Miał tylko dwa kubity, ale mógł wykonać prosty algorytm. Od tego czasu nastąpiły znaczące postępy. W sierpniu 2015 roku kanadyjska firma D-Wave Systems wprowadziła swój komputer kwantowy D-Wave 2X do sprzedaży. Ma on 1024 kubity wykonane z nadprzewodzących pętli z metalu niobu. Jedynymi wadami są rozmiary i cena – wymaga on pokoju o powierzchni 10 metrów kwadratowych i kosztuje ponad 15 milionów dolarów. Nie powstrzymało to Google'a od kupienia go i zaprzęgnięcia do pracy przy szkoleniu algorytmów rozpoznawania wzorców, które pozwalają

SZYFROWANIE KWANTOWE

Komputery kwantowe mają ogromny wpływ na bezpieczeństwo narodowe. Nowoczesne systemy szyfrowania – używane do bezpiecznej transmisji wrażliwych komunikatów – polegają na rozkładzie dwóch dużych liczb na ich czynniki. Wysłanie komunikatu wymaga tylko samej liczby (która jest dostępna publicznie), ale odczytanie go wymaga jej czynników (które są piekielnie trudne do obliczenia). To, co nazywamy szyfrowaniem kluczem publicznym przypomina trochę włożenie komunikatu do pudełka z zamkiem zapadkowym – każdy może je zamknąć, ale do jego otwarcia potrzebujemy klucza.

Szyfrowanie kluczem publicznym jest oparte na fakcie, że rozkład na czynniki pierwsze dużych liczb na klasycznym komputerze może trwać dłużej niż czas życia Wszechświata. Zła wiadomość jest taka, że uniwersalny komputer kwantowy może to zrobić w kilka minut.

2011

D-Wave One stał się pierwszym komercyjnym komputerem kwantowym

2012

Powstała firma 1Qbit – pierwsza firma poświęcona oprogramowaniu kwantowemu

2014

Edward Snowden ujawnił, że NSA (amerykańska agencja bezpieczeństwa) rozwija łamanie kodów za pomocą komputerów kwantowych

> **Mechanika kwantowa jest dziwaczna. Nie rozumiem jej. Nie musicie jednak rozumieć natury rzeczy, aby zbudować fajne urządzenia.**
>
> Seth Lloyd

na rozpoznawanie obiektów przez zestaw nagłowny rozszerzonej rzeczywistości Google Glass. Producent samolotów Lockheed Martin też go kupił w celu testowania swojego oprogramowania do lotów.

Niektórzy krytykują produkty D-Wave jako nie do końca kwantowe komputery, i jest w tym sporo racji. Nie są to „uniwersalne komputery kwantowe", gdyż nie można ich programować do wykonywania dowolnych zadań wymaganych przez użytkownika. Zamiast tego D-Wave 2X wykorzystuje proces nazywany kwantowym hartowaniem, gdzie kubity na wejściu po prostu ewoluują do swojej konfiguracji o najmniejszej energii. Można to wykorzystać do rozwiązywania problemów optymalizacyjnych, w których zadaniem jest znalezienie najlepszego możliwego rozwiązania. Optymalizacja ma bardzo wiele zastosowań (np. doradzenie firmie, jak najbardziej efektywnie wydać swoje pieniądze), ale przy dużych problemach zajmuje bardzo dużo czasu. D-Wave twierdzi, że jej komputery mogą rozwiązać problemy optymalizacyjne 600 razy szybciej niż klasyczne maszyny.

Wyluzuj Zbudowanie naprawdę uniwersalnego komputera kwantowego jest trudne ze względu na delikatność bitów kwantowych. W chwili, gdy kubit wchodzi w interakcję z otaczającym go środowiskiem, jego delikatny stan kwantowy zostaje zakłócony i wszelkie obliczenia kwantowe, które mogliśmy przechowywać, zostają utracone. Jest to znane jako dekoherencja (patrz s. 41). Zwykle kubit trwa kilka sekund od chwili powstania, a potem następuje dekoherencja. Uczeni próbują rozszerzyć to, wykorzystując kriogeniczne techniki chłodzenia, aby zredukować szumy cieplne, schładzając kubity do kilku tysięcznych stopnia powyżej zera bezwzględnego.

Komputery kwantowe mają potencjał do zrewolucjonizowania dziedzin, które zależą od siłowego przetwarzania danych, jak finanse, inżynieria i analiza danych. W końcu będą miały możliwość złamania większości dzisiejszych bezpiecznych szyfrów (patrz ramka na s. 71),

co już przyciągnęło uwagę agencji bezpieczeństwa narodowego. Ale jednym z najważniejszych zastosowań będą same badania naukowe, gdzie komputery kwantowe staną się ostatecznym narzędziem do symulacji zachowania układów kwantowych, pogłębiając nasze przyszłe zrozumienie enigmatycznej fizyki świata subatomowego.

TEORIA W PIGUŁCE

Maszyny przetwarzające dane w świecie kwantowym