Scientia PAUperum

Zasada działania kwantowego komputera

W roku 1982 Richard Feynman pokazał potencjalne możliwości hipotetycznej kwantowej maszyny obliczeniowej. Ta pionierska idea dała początek informatyce bazującej na algorytmach kwantowych.

Do opisu układu fizycznego w teorii kwantowej używamy pojęcia *stanu kwantowego*. Jest to narzędzie matematyczne – wektor o jednostkowej długości żyjący w przestrzeni Hilberta – pozwalające obliczać prawdopodobieństwo uzyskania wyniku danego pomiaru. Niezwykłe możliwości kwantowego przetwarzania informacji wynikają z dwóch własności.

Po pierwsze wektory można dodawać, więc dowolne złożenie dwóch stanów, zwane ich *superpozycją*, też jest pełnoprawnym stanem kwantowym. W informatyce klasycznej operujemy jedynie na zerach i jedynkach, a mechanika kwantowa dopuszcza całą gamę przypadków pośrednich: słynny kot Schrödingera może być trochę żywy, a trochę martwy.

Druga ważna cecha teorii objawia się przy badaniu układów złożonych: do opisu dwóch cząstek odpowiadające im przestrzenie Hilberta należy *pomnożyć* w specjalny sposób. Przykładowo, jeśli stan cząstki *A* opisujemy wektorem o trzech składowych, a stan cząstki *B* wektorem o czterech składowych, to układ złożony *AB* trzeba przedstawić wektorem z dwunastoma składowymi. Dla układów składających się z *n* cząstek wymiar przestrzeni rośnie wykładniczo z liczbą *n*. Sprawia to pewne kłopoty obliczeniowe, ale też dostępna przestrzeń stanów – scena, na której rozgrywa się akcja zaprojektowana przez autora kwantowego algorytmu – jest znacznie większa niż ta dostępna dla klasycznego informatyka.

Podstawową jednostką informacji jest bit (*binary unit*), przyjmujący wartość zero lub jeden. W klasycznym komputerze obliczenia realizuje się, wykonując algorytm, który można przedstawić jako złożenie elementarnych operacji wykonanych na poszczególnych bitach. Takie operacje nazywamy bramkami. Najprostszą bramką klasyczną jest operacja negacji, czyli zamiany zer w jedynkę i na odwrót. Bramka AND jest operacją dwubitową, która daje 1 na wyjściu, gdy oba bity na wejściu są równe 1.

Komputer kwantowy operuje na kubitach (*quantum bit*), znajdujących się w dowolnej superpozycji stanów 0 i 1, przekształcanych za pomocą bramek kwantowych. Podobnie jak w przypadku klasycznym, nawet bardzo skomplikowany algorytm kwantowy da się skonstruować, składając wiele kopii kilku wybranych bramek uniwersalnych, stosowanych w odpowiedniej kolejności.

Niektóre bramki, przykładowo bramki AND działające na rozłącznych parach bitów, można wykonać w tym samym czasie. Jednoczesną realizację zaplanowanej liczby bramek nazywamy krokiem algorytmu. Długość algorytmu to liczba takich kroków. Zestawiając algorytm klasyczny i kwantowy, porównuje się liczby kroków niezbędne do wykonania danego zadania przy równej liczbie danych wejściowych, zapisanych odpowiednio w bitach i kubitach.

Fizycznym nośnikiem informacji może być przykładowo polaryzacja fotonu (kwantu światła) lub stan pojedynczego atomu. Po realizacji algorytmu wykonywany jest pomiar, który dla każdego kubitu daje odpowiedź binarną: foton ma polaryzację poziomą lub pionową, a atom znajduje się w stanie podstawowym lub wzbudzonym. Teoria kwantowa ma charakter *probabilistyczny*, więc przeważnie cały eksperyment należy wykonać wielokrotnie, aby odczytać statystykę wyników.

Za pioniera obliczeń kwantowych uznać można Davida Deutscha, który w roku 1985 przedstawił pierwszy algorytm kwantowy, a swą ideę rozwinął w roku 1992 z Richardem Jozsą. Jego algorytm pozwalał sprawdzić własności pewnych funkcji w mniejszej liczbie kroków niż algorytm klasyczny. Nie był on specjalnie użyteczny w praktyce, ale – pośrednio – zainspirował Petera Shora do opracowania algorytmu efektywnie rozkładającego liczby naturalne na czynniki pierwsze (1994), a Lova Grovera do znalezienia algorytmu szybko przeszukującego nieuporządkowaną bazę danych (1996). Wynik Shora zrewolucjonizował całą kryptografię: gdyby udało się skonstruować uniwersalny komputer bezbłędnie działający na 1000 kubitach, można by złamać powszechnie używane metody kryptograficzne, także te aktualnie stosowane w bankach.

Dlaczego kwantowy komputer mógłby pewne zadania wykonać szybciej? Odpowiedź leży w kwantowej superpozycji, dzięki której współistnieją różne niezrealizowane możliwości, niczym potencjalności z filozofii Arystotelesa. Pozwala to − w dość niezwykły sposób − wykonywać równolegle niektóre operacje na informacji kwantowej zawartej w kubitach. Pracując z dwoma kubitami, można wytworzyć superpozycję1 czterech stanów: 00, 01, 10 oraz 11. Procesor n-kubitowy pozwala uzyskać jeden stan kodujący 2^n liczb naturalnych, więc przy 100 kubitach liczba składników takiego stanu ma 30 cyfr. W olbrzymim uproszczeniu, zamiast klasycznie sprawdzać po kolei, czy dana liczba naturalna jest dzielnikiem rozkładanej liczby, w kwantowym algorytmie Shora analizowany jest stan superpozycji bardzo wielu liczb naturalnych. Ponieważ każdy krok algorytmu działa równocześnie na wszystkie liczby wchodzące w skład tej superpozycji, można równolegle uzyskać informację o wszystkich razem, przyspieszając w ten sposób identyfikację tych, które ze znacznym prawdopodobieństwem są poszukiwanymi dzielnikami.

Teoretyczne możliwości obliczeniowe komputera kwantowego rosną wykładniczo z liczbą dostępnych kubitów, co uwidacznia różnicę w porównaniu z obliczeniami prowadzonymi równolegle na kilku procesorach komputera klasycznego.

Po prawie czterech dekadach intensywnych badań koncepcję kwantowego komputera uznać można za obiecującą i dojrzałą: w tym czasie zbadano podstawy przetwarzania informacji kwantowej oraz opracowano liczne algorytmy kwantowe. Dlaczego w takim razie nadal używamy komputerów klasycznych, a komputery kwantowe wciąż znajdują się w stadium bardzo wczesnego rozwoju? Problemy praktycznego wykorzystania pomysłu Feynmana przedstawimy w kolejnym numerze PAUzy.

PAWEŁ HORODECKI
UG/PG

KAROL ŻYCZKOWSKI
UJ/ PAN

PAUza Akademicka – www.pauza.krakow.pl – **tygodnik Polskiej Akademii Umiejętności i środowiska naukowego.**

Rada Redakcyjna: Magdalena Bajer, Andrzej Białas, Janusz Limon, Ewa Lipska, Stanisław Rodziński, Piotr Sztompka, Marta Wyka, Jakub Zakrzewski.

Redakcja: Andrzej Białas – redaktor naczelny; Andrzej Borowski, Andrzej M. Kobos, Piotr Malecki, Marian Nowy – redaktorzy; Adam Korpak, Krzysztof Skórczewski – grafika; Ryszard Otręba – „Galeria PAUzy"; Anna Michalewicz – dyrektor administracyjny; Witold Brzoskowski, Monika Mentel – fotoskład; Wydawnictwo PAU – konsultacje.

Adres do korespondencji: Polska Akademia Umiejętności, 31–016 Kraków, ul. Sławkowska 17; e-mail: pauza@pau.krakow.pl

Oczekujemy na artykuły do 6 000 znaków (ze spacjami) i ilustracje w formacie JPEG o rozdzielczości 300 dpi.