POLITYKA - nr 14 (2292) z dnia 07-04-2001; s. 68 Społeczeństwo / Technika

Kwantowe komputery będą prawie tak inteligentne jak my

Koniec inteligentnego idioty

Komputer, choć powszechnie uważany za symbol nowoczesności, jest w istocie prostym liczydłem, tyle że niezwykle rozbudowanym i bardzo szybkim. Prawdziwie inteligentnym urządzeniem będzie dopiero komputer kwantowy, który, wykorzystując fizyczne prawa mikroświata, podoła zadaniom dla obecnych komputerów zupełnie niewykonalnym.

Stanisław Mrówczyński

Moc obliczeniowa nowo wyprodukowanego komputera ulega podwojeniu w ciągu zaledwie 18 miesięcy. Ten niezwykły postęp uzyskuje się bardzo prostymi w istocie metodami. Zwiększa się mianowicie liczbę tranzystorów procesora i układów pamięci komputera. Wymaga to miniaturyzowania tych elementów, ich coraz większego zagęszczania. Nie można powiększać rozmiarów procesora czy układów pamięci, gdyż wydłużałoby to czas potrzebny na przesyłanie sygnałów między poszczególnymi częściami i spowalniało pracę komputera. Jednak miniaturyzowanie i zagęszczanie półprzewodnikowych obwodów nie może odbywać się w nieskończoność. Gdy rozmiary złącz i tranzystorów staną się porównywalne z wielkością atomów, przestaną one działać wedle dobrze poznanych zasad klasycznej fizyki. Kwantowe prawa mikroświata dadzą znać o sobie, wprowadzając fundamentalną przypadkowość w funkcjonowanie całego urządzenia. Osiągnięcie tej granicy miniaturyzacji – co przypuszczalnie nastąpi w ciągu najbliższej dekady – będzie oznaczało kres klasycznych komputerów. Dalszy postęp wymagał będzie wypracowania odmiennych kwantowych zasad działania maszyn liczących, stworzenia zupełnie nowych technologii. Badania zmierzające w tym kierunku tworzą jeden z najszybciej rozwijających się działów fizyki.

Zerojedynki

Myśl o kwantowym komputerze zrodziła się przeszło 20 lat temu. Bodaj jako pierwszy sformułował ją jasno Richard Feynman – jeden z największych fizyków XX wieku. Rozważając możliwość komputerowej symulacji przebiegu różnych zjawisk, Feynman doszedł do wniosku, że klasyczny komputer jest nieprzystosowany do imitowania procesów atomowych. Fundamentalną cechą mikroświata jest występowanie obiektów kwantowych w wielu stanach jednocześnie. Elektron jest jednocześnie cząstką i falą, zaś słynny kot Schrodingera może być żywy i martwy zarazem. W takich sytuacjach mamy do czynienia z superpozycją, czyli złożeniem różnych stanów tego samego obiektu. Dopiero gdy wykonamy odpowiedni pomiar, stan zostanie ustalony – kot okaże się wtedy martwy albo żywy. Wyniki powtarzanych pomiarów nad takim samym układem będą się zmieniały. W jednym doświadczeniu kot będzie żywy, w drugim martwy. Mechanika kwantowa określa jedynie prawdopodobieństwo uzyskania tego czy innego rezultatu.

Jednak owa kwantowa niepewność ma niewiele wspólnego z przypadkowym wynikiem rzutu kostką. Aby uchwycić, na czym polega różnica, rozważmy foton, który na swej drodze do detektora napotyka wiele szyb. Od każdej może się z pewnym prawdopodobieństwem odbić lub przez nią przelecieć. Opisując sytuację klasycznie określilibyśmy, od której szyby foton się odbił, którą pokonał. Kwantowo natomiast foton odbijałby się i przechodził przez kolejne szyby, docierając do detektora wszystkimi możliwymi drogami. Symulacja przebiegu takiego procesu musiałaby uwzględniać jednocześnie każdą z jego potencjalnych historii.

Klasyczny komputer, będący w istocie inteligentnym idiotą, słabo radziłby sobie z takim zadaniem. Umie on bowiem przeprowadzić jedynie najprostsze manipulacje, a i to tylko na zerach i jedynkach. Każda liczba, aby się stała dlań zrozumiała, musi być zamieniona na ciąg zer i jedynek. Wszystkie skomplikowane operacje sprowadzone są do długiego ciągu prostych działań wykonywanych przez tzw. bramki logiczne. Najprostszą jest bramka „Not” – zaprzeczenia, w której mamy tylko jedno wejście i jedno wyjście. Gdy na wejściu pojawia się sygnał, co odpowiada jedynce, bramka reaguje brakiem sygnału, czyli zerem. Gdy zaś na wejściu mamy 0, tzn. brak sygnału, na wyjściu jest sygnał, a więc 1. Bardziej złożona jest bramka „And” – koniunkcji – wyposażona w dwa wejścia i jedno wyjście. Gdy na wejściu mamy dwa razy 1, to na wyjściu też pojawia się 1. W pozostałych przypadkach – 00, 10, 01 – na wyjściu jest 0. Po połączeniu bramki „And” z „Not” powstaje bramka „Nand” – zaprzeczonej koniunkcji, która ma już charakter uniwersalny: z pomocą wielu takich bramek można wykonać dowolne działanie arytmetyczne.

Bit i qubit

Klasyczny komputer operuje bitami. Ta podstawowa jednostka informacji (*binary digit*) przyjmuje wartość 0 lub 1. Nośnikiem kwantowej informacji jest natomiast qubit (*quantum bit*), którego stan jest złożeniem 0 i 1. Qubit może więc reprezentować nie dwie wartości jak bit, lecz nieskończenie wiele. Stany odpowiadające 0 i 1 możemy bowiem zmieszać w dowolnej proporcji. Komputer klasyczny wykonuje obliczenia dla określonych danych wejściowych, natomiast do wejścia kwantowej maszyny możemy wprowadzić dane będące kombinacjami różnych wartości klasycznych. Rachunki zaś będą

wykonywane jednocześnie dla tego całego zestawu danych wejściowych. Właśnie możliwość owego równoległego prowadzenia różnych obliczeń stanowi o ogromnym potencjale kwantowego komputera.

Niestety, nie cały ten potencjał jest do wykorzystania, gdyż odczytując rezultat kwantowych rachunków uzyskamy tylko jeden wynik. Jak pamiętamy kot Schrodingera jest jednocześnie żywy i martwy tylko do momentu przeprowadzenia pomiaru; później jego los się rozstrzyga. Mamy więc paradoksalną sytuację: komputer kwantowy wykonuje jednocześnie wiele obliczeń, możemy jednak odczytać tylko jeden wynik. Może się więc wydawać, że paralelizm działania kwantowego komputera nic nie daje. Tak jednak nie jest! Tyle że pytania, które zadajemy kwantowemu komputerowi, należy formułować inaczej niż dla klasycznego; inaczej też trzeba odczytywać odpowiedzi.

Wyobraźmy sobie, że duży inwestor zamierza wykupić fabrykę samochodów. Ale bank centralny zamierza podnieść stopy oprocentowania kredytów, co może, ale nie musi, wpłynąć na opłacalność przedsięwzięcia. Aby wyjaśnić ten problem, należy przeprowadzić komputerową symulację funkcjonowania fabryki w przypadku zachowanych i podniesionych stóp procentowych. Dla komputera klasycznego oznacza to przeprowadzenie dwukrotnych obliczeń. Komputer kwantowy natomiast radzi sobie z tym zadaniem już w jednym ciągu rachunków, gdyż dane wejściowe mogą uwzględniać jednocześnie obie sytuacje na rynku. Wynik jednak trzeba odczytać inaczej niż w przypadku komputera klasycznego. Pytamy mianowicie nie o to, jaka jest opłacalność zakupu fabryki przy zachowanych i podniesionych stopach, co *de facto* odpowiada dwóm pytaniom, lecz jedynie o to, czy wynik obliczeń dla owych dwóch przypadków jest taki sam czy różny. Komputer kwantowy bez trudu udziela odpowiedzi na takie pytanie. Łatwo się też domyślić, że zysk z kwantowych rachunków jest jeszcze większy, gdy chodzi o rozpatrzenie więcej niż dwóch sytuacji wejściowych.

Na razie na papierze

Wobec ogromnego sukcesu zwykłych komputerów, zagadnienie kwantowych obliczeń długo uchodziło za dziedzinę raczej ezoterycznych rozważań. Sytuacja gwałtownie się zmieniła w 1994 r., gdy Peter Shor wykazał, że z pomocą komputera kwantowego można rozwiązać problem zdawałoby się nierozwiązywalny. Chodzi mianowicie o rozkład dużej liczby na czynniki pierwsze. Jak wiadomo każdą liczbę można przedstawić jako iloczyn liczb pierwszych, czyli takich, które dzielą się tylko przez jeden i samą siebie. Na przykład: 1105 = 5 x 13 x 17. Liczby 5, 13 i 17 są właśnie liczbami pierwszymi. Szukając czynników pierwszych jakiejś liczby komputer sprawdza po prostu, czy liczba ta dzieli się bez reszty przez kolejne liczby pierwsze. Po znalezieniu jednej takiej liczby szuka następnej itd. Musi więc wykonywać bardzo dużo operacji. Dla znalezienia czynników pierwszych liczby 60-cyfrowej wysokiej klasy współczesny komputer potrzebuje ok. 1 sekundy, liczby 100-cyfrowej roku, dla rozłożenia liczby 200-cyfrowej już kilkunastu miliardów lat!

Niemożność znajdowania czynników pierwszych dużych liczb jest powszechnie wykorzystywana do szyfrowania informacji, szczególnie dotyczących operacji bankowych. Poszczególnym liczbom pierwszym przypisuje się określone znaczenie. Wiadomość zapisuje się w postaci ciągu tych liczb, które następnie wymnaża się przez siebie. Zaszyfrowana wiadomość jest jedną wielką liczbą, będącą wynikiem tego mnożenia. Chociaż zasada kodowania jest powszechnie znana, wiadomość jest nie do rozszyfrowania.

Peter Shor wykazał, że komputer kwantowy rozkłada dużą liczbę na czynniki pierwsze w bez porównania mniejszej liczbie kroków niż klasyczny. Złamanie więc opisanego szyfru nie stanowi dlań wielkiego problemu. Odkrycie Shora odmieniło stosunek od obliczeń kwantowych, demonstrując ich ogromne możliwości. Wkrótce przedstawiono i inne zastosowania. Typowym zadaniem komputerowym jest przeszukiwanie baz danych. Klasyczna maszyna sprawdza informację po informacji, aż trafi na pożądaną. Pochłania to zwykle dużo czasu. Lok Grover przedstawił metodę znacznie szybszego kwantowego przeszukiwania baz danych, realizowanego w znacznie mniejszej liczbie kroków. Wielu przypuszcza również, że dopiero komputery kwantowe pozwolą stworzyć sztuczną inteligencję, czyli urządzenie umiejące myśleć.

Komputery kwantowe istnieją dotychczas jedynie na papierze. Opracowano zasady ich funkcjonowania, przygotowano oprogramowanie, brakuje natomiast fizycznego urządzenia. Mówiąc językiem informatyków: jest *software*, nie ma *hardware*. Trwają jednak bardzo intensywne prace doświadczalne nad zbudowaniem bramki logicznej zdolnej operować qubitami. Udowodniono, że pojedyncze atomy uwięzione w pułapce mogą sterowane laserem wykonywać proste działania logiczne. Największe jednak nadzieje wiąże się obecnie z wykorzystaniem w tym celu jądrowego rezonansu magnetycznego. Niezwykły rozwój technologii w ostatnich dziesięcioleciach każe przypuszczać, że zbudowanie kwantowego komputera w ten czy inny sposób jest kwestią bliskiej przyszłości. Czeka nas wtedy druga informatyczna rewolucja.

Autor jest fizykiem, pracuje w Instytucie Problemów Jądrowych w Warszawie oraz w Akademii Świętokrzyskiej w Kielcach.