Komputery kwantowe

Jakub ZIELIŃSKI

Wszyscy wiemy, że wiele problemów nie daje się rozwiązać za pomocą komputera tylko z powodu ich zbyt dużej „złożoności obliczeniowej". Pod tym poważnym stwierdzeniem kryje się prosta i smutna prawda. Nawet najszybsze komputery są zbyt wolne, aby uporać się z niejednym zadaniem. Wiemy też, że nie da się w nieskończoność zwiększać szybkości komputerów. Rozmiary atomów wyznaczają możliwą do wyobrażenia skalę miniaturyzacji. Jako że żaden sygnał nie może rozchodzić się szybciej niż światło w próżni, czas potrzebny na przesłanie informacji między fragmentami procesora też jest ograniczony od dołu. Czy komputer kwantowy może stać się remedium na powyższy problem?

Pierwszy raz z nazwą „komputer kwantowy" zetknąłem się 9 lat temu, na pierwszym roku studiów. Wydała mi się nieco podejrzana. Przecież zasada nieoznaczoności Heisenberga wyklucza dokładne pomiary obiektów kwantowych, powinna więc uniemożliwiać działanie takiego urządzenia. Tak naprawdę to wymienione ograniczenia są, obok gwałtownie rosnącego zużycia energii, główną przeszkodą przy tworzeniu coraz mniejszych i szybszych komputerów „klasycznych". Celowo użyłem cudzysłowu, bowiem w obecnie produkowanych procesorach prawa mechaniki kwantowej odgrywają już znaczącą rolę – tak naprawdę trudno opisać klasycznie działanie pojedynczego tranzystora...

Na czym więc ma polegać owa kwantowość? Na zupełnie odmiennym sposobie przetwarzania informacji. We współczesnych komputerach informacja jest zapamiętywana jako ciąg bitów, czyli zer i jedynek. Obliczenia zatem sprowadzają się do odpowiedniego zamieniania jednych bitów na inne.

W komputerze kwantowym bity są zastąpione przez qubity (quantum bits). Każdy qubit Ψ może być w tak zwanej superpozycji pomiędzy zerem i jedynką. Zapisujemy to w ten sposób:

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle.$$

Jeśli dokonamy pomiaru wartości qubitu, to możemy otrzymać $|0\rangle$ lub $|1\rangle$ z prawdopodobieństwami równymi odpowiednio: $P_0 = |\alpha|^2$ oraz $P_1 = |\beta|^2$. Przykładem tu może być elektron ze spinem skierowanym w górę lub w dół.

Takie uogólnienie bitu można jednak osiągnąć klasycznie. Wystarczy zbudować klasyczny komputer analogowy. Każdy bit będzie przybierał wartości z przedziału $[0, 1]$ i gotowe.

Nie chodzi jednak o operowanie wartościami między 0 i 1, lecz o wykorzystanie praw mechaniki kwantowej, pozwalających na superpozycję stanów jednego lub więcej qubitów.

Zobaczmy, jak to wygląda na przykładzie dwóch qubitów. Najprostsza baza układu dwóch qubitów to oczywiście: $|0\rangle|0\rangle$, $|0\rangle|1\rangle$, $|1\rangle|0\rangle$ oraz $|1\rangle|1\rangle$. Przykładowy stan to pewna kombinacja liniowa wektorów bazy; np.

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle).$$

Pierwszy qubit może być zerem lub jedynką. Obie możliwości są jednakowo prawdopodobne. Drugi tak samo. Wiemy jednak, że zawsze będą miały przeciwne wartości. Zaczyna robić się ciekawie, ale po chwili zastanowienia możemy zaproponować klasyczny odpowiednik tej sytuacji. Weźmy dwie kule: białą i czarną. Włóżmy je, nie patrząc, do dwóch kieszeni. Nie wiemy jednak, gdzie znajduje się któraś z nich, ale wiemy, że kule w kieszeniach są różne.

Aby pokazać różnicę między mechaniką kwantową a klasyczną statystyką, zamienię oznaczenia. Zamiast $|0\rangle$ będę pisał $|\downarrow\rangle$, natomiast $|1\rangle$ zastąpię przez $|\uparrow\rangle$. Wprowadzę również dwa nowe stany, będące superpozycjami powyższych: $|\leftarrow\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle + |\downarrow\rangle)$ oraz $|\rightarrow\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle - |\downarrow\rangle)$. Są to stany spinu skierowanego odpowiednio w lewo i prawo. Prosty rachunek (zachęcam!) pokazuje:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|\downarrow\rangle|\uparrow\rangle - |\uparrow\rangle|\downarrow\rangle) = \frac{1}{\sqrt{2}}(|\leftarrow\rangle|\rightarrow\rangle - |\rightarrow\rangle|\leftarrow\rangle).$$

Wynik jest dość dziwny. Wygląda bowiem na to, że elektrony „nie wiedzą", czy zostały „złożone" z elektronów o spinach góra-dół, czy też lewo-prawo. Co gorsza, my też tego nie wiemy! To tak, jakbyśmy po sprawdzeniu, że kulka z lewej kieszeni jest czerwona, wiedzieli, że ta z prawej jest zielona. Co więcej, moglibyśmy wybrać dowolną parę kolorów dopełniających. Jest tylko jedno ograniczenie: takiego „magicznego" pomiaru możemy dokonać tylko raz. Po pierwszym pomiarze owo połączenie czy też „splątanie" – jak mawiają fizycy – pomiędzy elektronami znika. Każdy z nich ma już określony stan.

Owa przedziwna własność stanów splątanych jest kluczowa – jest tym, co naprawdę odróżnia komputer kwantowy od klasycznego. Aby ją lepiej zrozumieć, musimy najpierw dowiedzieć się, na czym polega pomiar w mechanice kwantowej.

Nie możemy „zapytać", jak skierowany jest spin elektronu. Możemy spytać się jedynie, czy jest skierowany w górę czy w dół. Możemy także wybrać inny pomiar: w lewo czy w prawo albo w przód czy w tył. Ale nie możemy zadać tych pytań naraz. Tego typu zakazy wynikają z zasady nieoznaczoności. Ograniczenie powyższe nie wynika z niedoskonałości przyrządów pomiarowych. Popatrzmy na definicję spinów skierowanych w bok. Widać, że elektron o spinie skierowanym w prawo niejako składa się z elektronów o spinach skierowanych w górę i w dół. Zatem jeśli mamy przyrząd, który rozróżnia elektrony $|\uparrow\rangle$ od $|\downarrow\rangle$, to elektron $|\rightarrow\rangle$ „musi się zdecydować" na jedną

Jakub Zieliński, Instytut Fizyki Teoretycznej, Uniwersytet Warszawski

z tych możliwości. Nie mamy i mieć nie możemy na to wpływu. Każde urządzenie, które wykrywa wszystkie elektrony $|\uparrow\rangle$, musi wykryć co najmniej połowę elektronów $|\rightarrow\rangle$. To, czy wykryje połowę czy więcej, zależy tylko od tego, jak reaguje na elektrony $|\downarrow\rangle$.

Budując algorytmy kwantowe, mamy do dyspozycji dodatkowe stany. Wydawać by się mogło, że z łatwością powinno dać się skonstruować mnóstwo algorytmów znacznie efektywniejszych niż klasyczne. Problemem jest jednak brak możliwości rozróżniania dowolnych stanów. Co z tego, że otrzymamy wspaniały rezultat, jeśli nie będziemy go w stanie odczytać. Dlatego obecnie znamy tak naprawdę tylko dwa algorytmy kwantowe.

Pierwszym jest algorytm Shora. Nie będę tutaj tłumaczył całego algorytmu, gdyż jego opis jest długi i raczej żmudny. Pozwala on rozłożyć liczbę na czynniki pierwsze. Jak wiadomo, jest to kluczowy element łamania tak zwanych szyfrów z kluczem publicznym RSA (używanych powszechnie do szyfrowania informacji w Internecie, np. przez banki). Nie ma wątpliwości, że to jedna z ważniejszych przyczyn zainteresowania informatyką kwantową.

W algorytmie zaproponowanym przez Shora najpierw sprowadza się problem rozłożenia liczby N na czynniki pierwsze do problemu znalezienia okresu pewnej funkcji. Jest ona zadana dla N wartości. Procedura ta jest w pełni klasyczna – pomijam ją tutaj. Po szczegóły odsyłam do oryginalnej pracy [1]. Standardową metodą znajdywania okresu funkcji jest obliczenie jej transformaty Fouriera. W wyniku tej operacji znajdujemy tak zwane widmo. Gdyby funkcja opisywała falę dźwiękową, to dzięki transformacji Fouriera dostalibyśmy informację, jakie tony zawiera dźwięk. Podobnie, dla światła, byłby to rozkład na fale płaskie o określonych częstościach (czyli barwach). Transformacja Fouriera pozwala po prostu wyrazić funkcję przez szereg sinusów i kosinusów o różnych okresach. W wyniku transformacji funkcji, określonej dla N punktów, dostajemy funkcję (również N-punktową), której każdy punkt dostarcza informacji, „ile jest danej częstości".

I tak oto dostajemy wynik – rozkład liczby na czynniki pierwsze. Zaniepokoić powinny nas dwie rzeczy. Po pierwsze, transformatę Fouriera umiemy obliczać klasycznie – gdzie więc jest mechanika kwantowa? Po drugie, czas potrzebny na jej obliczenie jest proporcjonalny do $N \log N$. Widać więc, że jest to fatalny algorytm. Najprostszy pomysł na rozłożenie N to sprawdzać wszystkie liczby od 2 do $\sqrt{N}$.

Rzecz w tym, że transformatę Fouriera można obliczyć bardzo szybko kwantowo. Realizuje to odpowiedni układ „bramek kwantowych", czyli po prostu można wykonać stosowne obliczenia za pomocą manipulacji na spinach elektronów. Jak każde rachunki, można je przeprowadzić na różne sposoby. Jednak niezależnie od tego, jak byśmy się starali, zawsze musimy uwzględnić operacje „splątujące", a więc takie, które z dwóch nieskorelowanych elektronów zrobią splątaną parę. Stanowi to ogromną trudność eksperymentalną.

A jak duży musi być komputer kwantowy, aby poradzić sobie z rozkładem liczby N? Przede wszystkim liczba ta musi zmieścić się w jego „pamięci". Oznacza to, że $N < 2^n$, gdzie n jest właśnie liczbą qubitów. To bardzo ważne, bowiem w wielu przypadkach obowiązuje „zasada zachowania trudności": zwiększenie szybkości algorytmu osiągane jest za cenę większej „pamięciożerności".

Rzeczywiście, transformację Fouriera możemy wykonać bardzo łatwo, kodując funkcję za pomocą fali elektromagnetycznej, a widmo uzyskać natychmiast, przepuszczając światło przez pryzmat lub siatkę dyfrakcyjną. Problemem jest tu jednak ogromna liczba częstości, jakie musielibyśmy rozróżniać. Liczby pierwsze stosowane w kryptografii mają często po kilkaset cyfr. Nie ma najmniejszych szans na rozróżnianie częstości światła z tak ogromną precyzją. W algorytmach klasycznych czas potrzebny na rozłożenie liczby rośnie wykładniczo z liczbą jej cyfr (jej logarytmem). Przy zastosowaniu algorytmu Shora i optyki klasycznej wykładniczo rośnie liczba potrzebnych częstości światła. W algorytmie kwantowym, dzięki splątaniu, czas obliczeń i ilość qubitów rosną potęgowo wraz z logarytmem rozkładanej liczby.

Widać więc, że algorytm Shora to w zasadzie szukanie okresu funkcji. Nie jest to raczej problem fascynujący sam w sobie. Zawdzięcza on swoją popularność temu, że Shor potrafił powiązać ten pozornie czysto akademicki problem z kryptografią. To uczy, że bardzo ryzykowne jest „spisywanie na straty" jakiegoś działu nauki, mówiąc, że „to się do niczego nie przyda".

Na koniec jedna uwaga. Dlaczego upieram się, że komputer kwantowy ma szukać okresu funkcji, a nie po prostu obliczyć transformatę Fouriera? Ten ostatni problem jest ważny w niezliczonych zastosowaniach. Od diagnostyki medycznej, poprzez analizę zdjęć satelitarnych, na symulacjach układów chemicznych kończąc. Otóż komputer kwantowy potrafi obliczyć transformatę Fouriera zawsze, ale wynik możemy odczytać tylko jeśli funkcja jest okresowa. Powód jest prosty: tylko dla funkcji okresowej widmo zawiera niewiele częstości. Jeśli będziemy próbować obliczać transformatę Fouriera z funkcji nieokresowej, to otrzymamy widmo złożone z niezliczonej ilości długości fal. A podczas pomiaru możemy dostać tylko jedną wartość częstości...

Drugim zaproponowanym algorytmem kwantowym [2] jest sposób przeszukania zbioru N-elementowego w poszukiwaniu jednego „dobrego" elementu. W wielu

przypadkach jest tak, że łatwo sprawdzić, czy zaproponowane rozwiązanie jest dobre. Trudno je jednak znaleźć. Często pozostaje nam jedynie sprawdzanie po kolei wszystkich możliwych przypadków. Kłopot zaczyna się, gdy jest ich dużo.

Klasyczny średni czas szukania jednego „dobrego" elementu spośród N jest proporcjonalny do $\frac{N}{2}$. Czas potrzebny dla komputera kwantowego to tylko $\sqrt{N}$.

Wszystkie N sprawdzanych odpowiedzi możemy ponumerować. Od tej pory będziemy sprawdzać, która z N liczb jest „dobra". N liczb zakodujemy za pomocą 2^n qubitów. Pokażę to na prostym przykładzie $N = 4$ ($N_i = \{0, 1, 2, 3\}$):

$$|0\rangle = |00\rangle, \;\; |1\rangle = |01\rangle, \;\; |2\rangle = |10\rangle, \;\; |3\rangle = |11\rangle.$$

Kodowanie jest więc takie, jak w komputerze klasycznym. Następnie tworzymy stan będący superpozycją wszystkich możliwych odpowiedzi:

$$|\Psi\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle).$$

Zwracam uwagę, że jest to stan bardzo silnie splątany. Sprawdzanie, czy dana liczba jest dobra, można zdefiniować jako obliczenie funkcji. Jeśli liczba jest dobra, to funkcja ma wartość 1, a jeśli zła, to -1. Oczywiście, możemy przypisać inne wartości obu odpowiedziom – byleby tylko były różne.

Widać więc, że wszystkie $N - 1$ złych stanów będzie zawsze traktowane tak samo, a inaczej jeden stan dobry. Możemy więc ogólnie zapisać

$$|\Psi\rangle = \sqrt{\frac{1}{N}}(|0\rangle + |1\rangle + \ldots + |N\rangle) =$$

$$= \sqrt{\frac{1}{N}}(\sqrt{N-1}|\text{zły}\rangle + |\text{dobry}\rangle).$$

Jak widać, jeśli zmierzymy, w którym stanie jest układ N qubitów, to z prawdopodobieństwem $\frac{N-1}{N}$ dostaniemy „złą" odpowiedź, a „dobrą" jedynie z prawdopodobieństwem $\frac{1}{N}$. Jest to dość oczywiste – nic jeszcze nie zrobiliśmy i szansa wylosowania stanu o szukanym numerze jest znikoma.

Zwróćmy uwagę, że otrzymany stan jest nieco podobny do pojedynczego spinu. Jeśli przyjmiemy

$$\alpha = \sqrt{\frac{N-1}{N}} \;\; \text{oraz} \;\; \beta = \sqrt{\frac{1}{N}},$$

to otrzymamy:

$$|\Psi| = \alpha|0\rangle + \beta|1\rangle,$$

a więc spin skierowany prawie idealnie do dołu. Spin możemy obrócić o 180 stopni i dostaniemy elektron o spinie skierowanym niemal idealnie do góry. Obrotu pojedynczego spinu można dokonać, np. włączając jednorodne pole magnetyczne lub pole magnetyczne połączone z falą elektromagnetyczną. Jest to technika powszechnie stosowana w obrazowaniu i spektroskopii, opartych na zjawisku rezonansu magnetycznego (zazwyczaj spiny pochodzą tam od jąder, a nie od elektronów – jest to dla nas bez znaczenia. Elektron jest tylko przykładem cząstki ze spinem. Do budowy komputera można użyć innych cząstek).

Oczywiście, w przypadku układu N spinów nie jest tak prosto. Co więcej, problemem jest to, że nie znamy dokładnie stanu $|\Psi\rangle$. Po prostu nie wiemy, co oznacza $|\text{dobry}\rangle$, gdyż to jest nasza niewiadoma. Ale znamy nasz stan z bardzo dobrym przybliżeniem, dlatego też możemy z niezłym przybliżeniem go „obrócić". Zajmuje to $\sqrt{N}$ kroków. Niestety, nie możemy obrócić układu w jednym kroku. Musimy „drobić", bo gdybyśmy „robili zbyt duże kroki", moglibyśmy pójść nieco za daleko. To cena, jaką płacimy za niedokładną znajomość stanu początkowego.

Niestety, pomimo ogromnego wysiłku, nie udało się dotąd zbudować działającego komputera kwantowego i nie wiadomo, czy będzie to kiedykolwiek możliwe. Jak już wspomniałem, nie musimy koniecznie używać elektronów. Próbowano rozmaitych schematów, w tym jądrowego rezonansu magnetycznego.

W tej chwili najbardziej obiecujące wydają się próby z jonami umieszczonymi w pułapce [3, 4]. Można już w sposób kontrolowany umieścić jeden za drugim kilka jonów w próżni. Ich pozycja jest kontrolowana za pomocą odpowiednio uformowanego pola elektromagnetycznego. Co więcej, możliwe jest dokonywanie manipulacji na wybranym jonie oraz ich splątywanie! Niestety, problemem jest tak zwana dekoherencja: po czasach rzędu milisekund w niezwykle przecież delikatny układ wkrada się jakieś zaburzenie. Powoduje to utratę informacji. Nie wiadomo, czy kiedykolwiek uporamy się praktycznie z tym problemem. Wraz ze wzrostem komputera, problem będzie się nasilał. Już jednak zbudowanie układu kilku qubitów i precyzyjna nimi manipulacja pokazuje, jak niesamowity rozwój technik eksperymentalnych nastąpił w ostatnich latach.

Z pewnością komputer kwantowy nie będzie kolejną zabawką stojącą na biurku, lecz urządzeniem służącym do wykonywania najbardziej zaawansowanych obliczeń, umieszczonym w najlepszych światowych laboratoriach. Trzeba jednak pamiętać, że taką samą przyszłość wieszczono klasycznym komputerom...

[1] Peter Shor, *Proceedings 35th Annual Symposium on Foundations of Computer Science*, IEEE Comput. Soc. Press (1994), 124-134.

[2] Lov K. Grover, *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing*, (1996), 212-219.

[3] D. Kielpinski, C.R. Monroe and D.J. Wineland, *Nature* 417, 709-711 (2002).

[4] D. Leibfried et al., *Nature* 422, 412-415 (2003).