Komputery kwantowe

Szymon Pustelny
Student SMP, Instytut Fizyki UJ

Wstęp

Współcześnie coraz głośniej mówi się o ograniczeniach stojących przed rozwojem klasycznych komputerów. Zakrojone na szeroką skalę badania mają na celu zbudowania nowego typu urządzenia, tzw. komputera kwantowego. Niniejsza praca jest próbą przybliżenia problemów związanych z tym zagadnieniem.

W pierwszej części artykułu ukazane będą fizyczne bariery, jakie stoją przed rozwojem klasycznych komputerów. W kolejnej części omówione zostaną podstawy kodowania informacji w obu typach komputerów. W części czwartej omówione będą pokrótce dwa najbardziej znane algorytmy kwantowe: algorytm Grovera, służący do przeszukiwania baz danych, oraz algorytm Shora, pozwalający na faktoryzację wielkich liczb. W podsumowaniu zaprezentowana będzie tabela stanowiąca kompendium wiedzy i stan technicznej realizacji wybranych problemów związanych z komputerami kwantowymi. Na końcu artykułu Czytelnik znajdzie kilka pozycji, które mogą posłużyć jako podstawa dalszego poszerzenia wiedzy na ten temat.

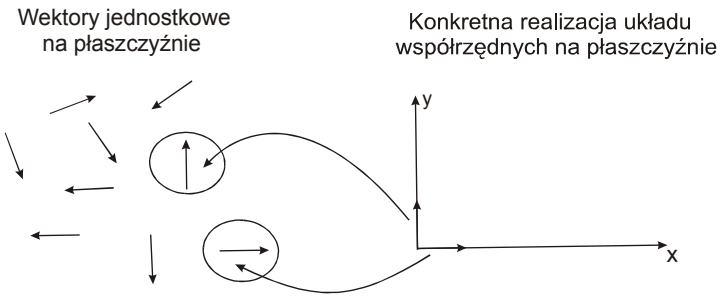
Z roku na rok skraca się czas, jakiego mikroprocesor komputerowy potrzebuje na wykonanie pojedynczego zadania. Zgodnie z prawem Moore'a, co osiemnaście miesięcy podwaja się liczba operacji, które procesor może wykonać w ciągu sekundy. Wydaje się, że jedynym sposobem, w jaki można przyspieszać działanie procesora, jest zwiększanie jego integracji, czyli miniaturyzacja poszczególnych elementów elektronicznych, z których jest on zbudowany. Stosowane współcześnie metody litograficzne pozwalają na wytwarzanie układów scalonych, na których wielkości podstawowych elementów elektronicznych oraz szerokość łączących je ścieżek nie przekraczają jednego mikrometra. Być może w ciągu następnych kilkunastu lat wymiary zintegrowanych na układach scalonych elementów zmaleją do rozmiarów kilku warstw atomowych. Abstrahując od technologicznych problemów związanych z wytwarzaniem tak małych elementów, trzeba zauważyć, że przy takich rozmiarach zaczną one być opisywane w sposób kwantowy, a co za tym idzie – ujawni się w nich probabilistyczna natura mechaniki kwantowej. Różne operacje logiczne, których miliardy wykonywane są każdorazowo przez procesor, przestaną być jednoznaczne, a zaczną podlegać rozkładowi statystycznemu. Przykładowo sumator dodający do siebie dwa bity generować będzie różne wyniki niezależnie od stanu początkowego obu bitów. Innymi słowy, dodając wielokrotnie do siebie pary takich samych liczb przy użyciu tego samego sumatora,

otrzymać możemy różne wyniki. Komputer, w którym wykorzystywano by taki mikroprocesor, bez przerwy generowałby błędy, co uniemożliwiałoby jego działanie.

Fizyczne podstawy funkcjonowania komputerów kwantowych

Mechanika kwantowa, która przez swoją probabilistyczną naturę ogranicza rozwój klasycznych komputerów, jednocześnie otwiera przed nami zupełnie nowe możliwości rozwiązań. Wszystko dzięki jej fundamentalnej własności zwanej *superpozycją*. W 1981 roku Richard Feynman zaproponował wykorzystanie własności superpozycji jako podstawy działania komputerów nowej generacji tzw. komputerów kwantowych.

Aby omówić własność superpozycji, wygodnie jest wykorzystać geometryczny opis mechaniki kwantowej. Z geometrii wiadomo, że na dowolnej płaszczyźnie istnieje nieskończenie wiele par jednostkowych, wzajemnie prostopadłych wektorów. Wybierając jedną z takich par, decydujemy się na konkretną realizację układu współrzędnych na płaszczyźnie, czyli na tzw. *bazę wektorową*. Przypadek ten został zeprezentowany na rysunku 1. Analogicznie można wybrać wektory bazowe w trzech wymiarach, a nawet w przestrzeni o większej liczbie wymiarów. Taka przestrzeń jest *wektorowa*, gdy dowolny wektor może zostać utworzony jako kombinacja liniowa wybranych przez nas wektorów bazowych.



Rys. 1. Utworzenie bazy wektorowej na płaszczyźnie

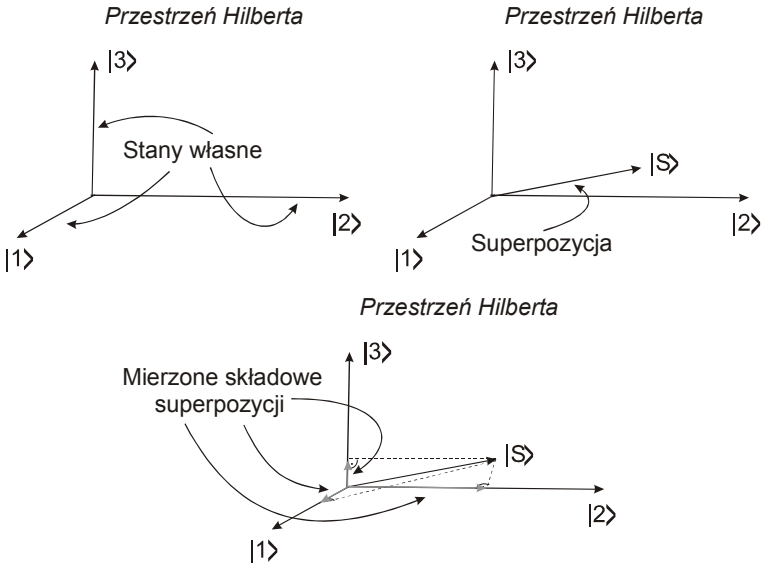
W opisie kwantowym każdy układ fizyczny ma pewne charakterystyczne dla siebie stany energetyczne, zwane *stanami własnymi*. Każdemu takiemu stanowi własnemu można przypisać wektor bazowy w pewnej abstrakcyjnej przestrzeni, która jest *przestrzenią Hilberta*[*]. Liczba wektorów bazowych w tej przestrzeni zależy od tego, ile stanów własnych ma dany układ. Dla najprostszego, nietrywialnego układu fizycznego, czyli układu posiadającego dwa stany własne, przestrzeń

[*] Przestrzeń Hilberta ma ściśle określone własności, których tu nie przytaczamy.

Hilberta jest dwuwymiarowa. Większa liczba stanów charakterystycznych powoduje zwiększenie liczby wektorów bazowych. Ponieważ przestrzeń Hilberta jest przestrzenią wektorową, nic nie stoi na przeszkodzie, aby tworzyć w niej nowe wektory będące kombinacjami liniowymi wektorów bazowych. Jeśli w wyniku kombinacji liniowej wektorów bazowych stworzymy wektor o długości jednostkowej, to będzie on odpowiadał nowemu stanowi fizycznemu układu. Stan ten nosi nazwę *superpozycji stanów własnych*.

Zgodnie z postulatem mechaniki kwantowej, dokonując eksperymentalnego pomiaru stanu układu, nigdy nie uda nam się zaobserwować stanu będącego superpozycją.

Odwołując się do geometrycznej interpretacji mechaniki kwantowej, pomiar stanu układu odpowiada rzutowaniu wektora stanu z przestrzeni Hilberta na jeden z wektorów bazowych. Jeśli układ znajduje się w stanie własnym, to w wyniku pomiaru zmierzymy dokładnie ten stan. Jeśli jednak jest on w stanie superpozycji, to zawsze mierzymy jeden ze stanów własnych, z których ta superpozycja została utworzona. Prawdopodobieństwo zaobserwowania konkretnego stanu własnego zależy od tego, jaki jest jego wkład do mierzonej superpozycji.



Rys. 2. Przestrzeń Hilberta jako geometryczna interpretacja mechaniki kwantowej

Dla zilustrowania powyższych rozważań rozpatrzmy cząstkę o spinie ½, np. elektron. Mechanika kwantowa podpowiada, że przy obranej osi spin elektronu

może mieć tylko dwie orientacje przestrzenne. Nazwijmy je umownie: „do góry", której odpowiada stan |↑> i „na dół" ze stanem |↓>. Te dwa stany są stanami własnymi spinu elektronu, przestrzeń Hilberta jest więc dwuwymiarowa. Oprócz dwóch stanów własnych elektron może istnieć w stanie będącym superpozycją obu stanów

$$|s\rangle = c_{\uparrow}|\uparrow\rangle + c_{\downarrow}|\downarrow\rangle$$

gdzie $c_{\uparrow}$ i $c_{\downarrow}$ są liczbami zespolonymi.

Kierunek spinu elektronu może być w ogólności inny niż „do góry" czy „na dół". Jeśli nawet tak jest, to w wyniku pomiaru spinu i tak elektron ZAWSZE zaobserwujemy w stanie |↑> lub |↓>. Jeśli wielokrotnie powtarzalibyśmy pomiar takiej samej superpozycji, to odpowiednio z prawdopodobieństwem $|c_{\uparrow}|^2$ rejestrowalibyśmy stan |↑>, a z prawdopodobieństwem $|c_{\downarrow}|^2$ stan |↓>, lecz zawsze tylko jeden z nich. Cząstkę obserwujemy w jednym z dwóch stanów, więc pomiędzy prawdopodobieństwami zachodzi relacja

$$|c_{\uparrow}|^2 + |c_{\downarrow}|^2 = 1$$

Warunek ten to nic innego, jak nasze żądanie by stan |s> w przestrzeni Hilberta miał długość jednostkową.

Klasyczne i kwantowe kodowanie informacji

Aby móc „porozumiewać" się z komputerem, niezbędne jest stworzenie swoistego kodu rozumianego przez maszynę. Najprościej można tego dokonać, przypisując każdej informacji wymienianej z komputerem pewną liczbę, którą maszyna zinterpretuje jako żądanie wykonania danej operacji. Pozostaje jednak problem, w jaki sposób przekazać daną liczbę do komputera.

W życiu codziennym przyzwyczajeni jesteśmy do zapisywania liczb w systemie dziesiętnym. Chcąc go wykorzystać w komputerach, musielibyśmy każdej z dziesięciu cyfr tego systemu przypisać dziesięć różnych wartości pewnej wielkości fizycznej. Przykładowo możemy do tego celu wykorzystać dziesięć różnych wartości napięcia. Chcąc uniknąć problemów związanych z niejednoznacznym zdefiniowaniem danej cyfry wartości napięcia, za pomocą których dokonujemy kodowania, muszą się między sobą zdecydowanie różnić. Zakładając, że dwie kolejne liczby musi dzielić taka sama różnica potencjałów, można się łatwo przekonać, że do utworzenia systemu dziesiętnego niezbędne jest zarezerwowanie większego zakresu napięć niż dla systemu zbudowanego z mniejszej liczby cyfr. W szczególności najprościej zbudować system, w którym wykorzystywane będą jedynie dwie wartości napięcia. Doprowadza nas do najwygodniejszego w praktycznej realizacji systemu binarnego.

Systemy binarne wykorzystywane są dziś we wszystkich komputerach. Każda informacja kodowana jest za pomocą ciągu *bitów*. Bit fizycznie reprezentuje jeden z dwóch stanów: zero lub jedynkę. O ile na pojedynczym bicie można zapisać jedynie dwie liczby: 0 lub 1, o tyle ciągi bitów zwane *rejestrami* pozwalają na zapisanie dowolnej liczby. W szczególności ciąg ośmiu bitów, tzw. *bajt*, pozwala na zapisanie liczby od 0 do 255. Te 256 możliwości pozwala na skodyfikowanie wszystkich znaków alfabetu łacińskiego, cyfr arabskich i większości znaków specjalnych, tworząc wykorzystywany w komputerach kod ASCII.

Rozpatrzmy teraz rejestr składający się z trzech bitów. W klasycznym komputerze rejestr ten pozwala na zakodowanie liczby od 0 do 7. Dzięki omówionemu wyżej zjawisku superpozycji na rejestrze kwantowym zbudowanym z trzech *kubitów*, kwantowym odpowiedniku bitów, można JEDNOCZEŚNIE zapisać wszystkie osiem liczb

$$|r\rangle = c_0|0\rangle + c_1|1\rangle + \ldots + c_6|6\rangle + c_7|7\rangle$$

gdzie: $|0\rangle = |0\rangle_1|0\rangle_2|0\rangle_3$, $|1\rangle = |1\rangle_1|0\rangle_2|0\rangle_3$, ... , $|7\rangle = |1\rangle_1|1\rangle_2|1\rangle_3$

Dodanie każdego kolejnego kubitu do rejestru spowoduje podwojenie ilości przechowywanych w nim jednocześnie liczb. Jednakże dokonując pomiaru rejestru zawsze zaobserwujemy stan odpowiadający tylko jednej konkretnej liczbie. Analogicznie jak w przypadku pomiaru spinu elektronu, prawdopodobieństwo, która z wartości zostanie zaobserwowana, zależy od kwadratu modułu współczynników $|c_i|^2$.

Kwantowe algorytmy

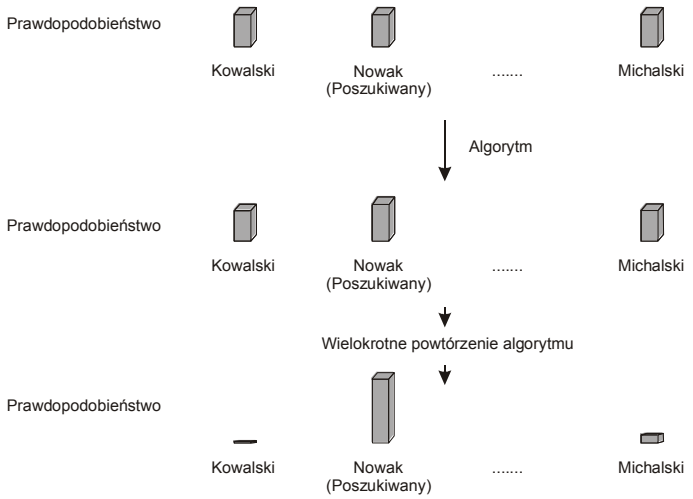
Wykorzystywanie kwantowych rejestrów ma jeszcze jedną ciekawą cechę. Jeśli rejestr kwantowy zbudowany jest z N kubitów, na których możemy zapisać 2^N liczb, to dokonując pewnej operacji na rejestrze przeprowadzamy ją jednocześnie na wszystkich liczbach z rejestru. Dla porównania komputer klasyczny, za pomocą którego chcielibyśmy osiągnąć ten sam skutek, potrzebowałby na to 2^N N-bitowych rejestrów, zaś daną operację musiałby przeprowadzić na każdym rejestrze z osobna. Daje to łącznie 2^N operacji. W pewnych zastosowaniach ta własność algorytmów pracujących w oparciu o rejestry kwantowe jest olbrzymia.

Dla zilustrowania powyższego zagadnienia rozważmy następującą sytuację. W bazie danych policji znajdują się dane osobowe i odciski palców miliona osób. Statystycznie w przypadku klasycznym, chcąc w tej bazie odnaleźć dane osoby, której odciski znaleziono na miejscu przestępstwa, trzeba wykonać pół miliona prób. Średnio po tylu powtórzeniach algorytmu przeszukującego odnajdziemy winowajcę.

Załóżmy teraz, że baza danych zapisana jest w sposób kwantowy oraz że dysponujemy pewnym dodatkowym kwantowym rejestrem, który posłuży nam do

odnalezienia przestępcy. Rejestr ten zawiera tyle samo pozycji co baza, a każda pozycja bazy stanowi jego stan własny. W chwili początkowej rejestr został przygotowany w stanie superpozycji, a każdej osobie, której dane zawarte są w rejestrze, przypisano te same, znalezione na miejscu przestępstwa odciski palców. Na początku więc założono, że każda z osób może być z tym samym prawdopodobieństwem poszukiwanym przestępcą, choć tylko jednej osobie przypisano odpowiednie odciski palców. Algorytm przeszukujący porównuje jednocześnie odciski palców każdej osoby w bazie i w rejestrze. Jeśli dla danej pozycji odciski są identyczne to nieznacznie wzrasta prawdopodobieństwo, że przy pomiarze rejestru otrzymamy właśnie tę pozycję. W przypadku gdy przydzielenie było błędne, prawdopodobieństwo, że przy pomiarze uzyskamy tę pozycję, zmniejsza się. Zmiana prawdopodobieństwa jest na tyle mała, że dopiero wielokrotne powtarzanie algorytmu na tym samym rejestrze porównawczym spowoduje zdecydowany wzrost prawdopodobieństwa znalezienia prawdziwego przestępcy. W rozważanym przez nas przypadku po tysiącu powtórzeniach algorytmu pomiar rejestru porównawczego da prawidłowy wynik z prawdopodobieństwem ½. Kolejnych kilka powtórzeń spowoduje, że prawdopodobieństwo to będzie bliskie jedności.

Warto zauważyć, że przeszukując N-elementową bazę danych metodami klasycznymi, należy wykonać średnio N/2 kroków, by odnaleźć odpowiednią pozycję w bazie. Dla porównania, stosując algorytmy kwantowe, liczba kroków, jaką należy wykonać, jest nieco większa niż $\sqrt{N}$. Zysk płynący z wykorzystania kwantowych algorytmów przeszukujących jest tym większy, im większa jest przeszukiwana baza.



Rys. 3. Zasada działania algorytmu przeszukującego Lova Grovera

Innym przykładem zastosowania komputerów kwantowych jest wykorzystanie ich do wykonywania pewnych operacji matematycznych. Matematycy wierzą, że liczba kroków, którą należy wykonać, aby rozłożyć daną liczbę na liczby pierwsze, zależy eksponencjalnie od ilości tworzących ją cyfr. Zatem wybranie odpowiednio dużej liczby może praktycznie uniemożliwić znalezienie jej dzielników. Z matematycznego punktu widzenia problem szukania dzielników danej liczby może być zastąpiony przez problem szukania okresu pewnej funkcji. W klasycznym przypadku jednak fakt ten nie ma żadnego znaczenia, gdyż liczba kroków potrzebna na rozwiązanie obu problemów jest taka sama. Jednak dzięki niezwykłej efektywności komputerów kwantowych w określaniu okresowości funkcji periodycznych sytuacja ta ulega zmianie. Zastąpienie jednego problemu drugim powoduje, że faktoryzacji będziemy mogli dokonać w znacznie krótszym czasie. Przy użyciu komputerów kwantowych liczba kroków, którą należy wykonać, by znaleźć dzielniki danej liczby, zależy potęgowo, a nie jak wcześniej wykładniczo, od ilości tworzących ją cyfr.

Problem faktoryzacji dużych liczb jest szczególnie ważny, ponieważ stanowi on podstawę działania najpowszechniej obecnie stosowanego algorytmu kryptograficznego. Wielokrotne skrócenie czasu potrzebnego na złamanie klucza kodującego sprawiłoby, że używane m.in. w bankowości metody kryptograficzne przestałyby gwarantować bezpieczeństwo.

Prawdopodobnie jednak omówione wyżej *spekulacje algorytmiczne* nie będą stanowić najważniejszej dziedziny zastosowania komputerów kwantowych. Wspominany już wcześniej Richard Feynman zauważył, że rzeczywiste układy kwantowe charakteryzują się niezwykłą złożonością obliczeniową, gdy chce się je opisywać w sposób klasyczny. Wydaje się więc naturalne, że komputery kwantowe, w które złożoność ta jest wpisana niejako z definicji, staną się bardzo wygodnym narzędziem w *symulacjach układów kwantowych*.

Podsumowanie

Trudno dziś dać jednoznaczną odpowiedź na pytanie, kiedy powstaną komputery kwantowe zdolne przeszukiwać bazy danych czy modelować skomplikowane układy kwantowe. Prototypy pierwszych komputerów zbudowanych z kilku kubitów zostały już skonstruowane w kilku laboratoriach badawczych na świecie. Do końca obecnej dekady powstaną prawdopodobnie komputery zbudowane z dziesięciu kubitów. Problemem jest jednak trwałość takich układów. Dodanie każdego kolejnego kubitu do rejestru powoduje eksponencjalne skrócenie *czasu życia* takiego układu. Innymi słowy, im więcej kubitów buduje dany rejestr, tym krócej istnieje on jako integralna całość.

Zagadnienia związane z komputerami kwantowymi są dziś rozwijane w wielu laboratoriach na całym świecie Głównym celem zakrojonych na szeroką skalę programów badawczych jest zarówno teoretyczne, jak i eksperymentalne opraco-

wanie tego problemu. Z roku na rok zwiększa się liczba konkretnych realizacji komputerów kwantowych, zwiększa się również liczba algorytmów, w oparciu o które miałyby one działać. Powstał nawet pierwszy, prosty język programowania, który ma służyć do oprogramowania komputerów kwantowych. Wszystko po to, byśmy za kilkanaście lat dysponowali nowym, potężnym urządzeniem, którego potencjału nie sposób przecenić.

Zastosowanie	Liczba potrzebnych kubitów	Liczba niezbędnych do wykonania kroków	Status
Symulacje kwantowe	kilka	kilka	teoria niepełna
Proste algorytmy przeszukujące	więcej niż 3 setki	więcej niż 6 setki	zademonstrowane przyszłość
Faktoryzacja			
Uniwersalne komputery kwantowe	więcej niż tysiące	więcej niż tysiąc	przyszłość

Literatura

Książki:
G. J. Milburn, *Procesor Feynmana*, Wydawnictwo CiS, Warszawa (1998)
D. Bouweester, A. Ekert, A. Zeilinger, *The Physics of Quantum Information*, Springer, Berlin (2000)

Czasopisma:
Physics World (Wydanie specjalne), Marzec 1998
L. Jacak, *Postępy fizyki*, **53D**, 72 (2002)

Internet:
www.qubit.org