Aktualności (nie tylko) fizyczne

W artykule z 13 kwietnia br., opublikowanym w *Physical Review Letters* [1], autorzy donoszą o przeprowadzeniu pierwszego pełnego rachunku za pomocą komputera kwantowego, rachunku polegającego na „wprowadzeniu danych początkowych do komputera kwantowego, wykonaniu obliczeń wymagających mniej kroków niż w przypadku zwykłego komputera oraz odczytaniu wyników". Choć to osiągnięcie było od pewnego czasu oczekiwane, może stanowić przełom tak w informatyce, jak i w doświadczalnym badaniu podstaw mechaniki kwantowej.

Czym różni się komputer kwantowy od zwykłego? Złośliwi (pesymiści) powiedzieliby, że tego pierwszego po prostu nie ma (i nie będzie). Optymiści twierdzą, że wcześniej czy później powstanie, bo jego teoretycznie udowodnione możliwości przekraczają zdolność obliczeniową klasycznego komputera wykorzystującego cały krzem obserwowalnego Wszechświata. Ale o co chodzi z tą „kwantowością"? Przecież współczesne komputery wykorzystują układy scalone zawierające tranzystory, których działanie opiera się właśnie na mechanice kwantowej. Tak, ale operacje wykonywane przez mikroprocesor można równie dobrze przeprowadzić za pomocą przekładania kamyczków, tylko że miliard (bilion?) razy wolniej. Dlatego bardziej skomplikowanych problemów numerycznych nie da się rozwiązać w „rozsądnym czasie" przy wykorzystaniu otoczaków. Istnieją jednak takie problemy, z którymi nawet dowolnie szybkie „Quintylionium®" sobie nie poradzi w rozsądnym czasie (np. krótszym od wieku Wszechświata). Klasycznym przykładem może być rozkład dużych liczb na czynniki pierwsze. Za efektywny uznaje się algorytm, którego liczba kroków rośnie co najwyżej wielomianowo z liczbą informacji wejściowych. Dla rozkładu liczby na czynniki pierwsze taki algorytm nie istnieje. Liczba kroków rośnie co najmniej wykładniczo z długością rozkładanej liczby. Zainteresowanie komputerami kwantowymi wyraźnie wzrosło właśnie po tym, jak Peter Shor odkrył taki algorytm dla komputera kwantowego [4].

Zwykły komputer wykonuje operacje na rejestrach bitowych. Np. rejestr dwubitowy może znajdować się w jednym z czterech stanów: 00, 01, 10 i 11. Za jego pomocą można zaadresować czteroelementową bazę danych. Załóżmy, że pod jednym z adresów kryje się logiczna jedynka, a pod pozostałymi logiczne zera. Aby dowiedzieć się, gdzie ukrywa się jedynka, należy wykonać średnio $(1+2+3+3)/4 = 9/4$ sprawdzeń. Idea komputera kwantowego polega na używaniu rejestrów opartych na tzw. qubitach (ang. qubit = quantum bit). Różnica polega na tym, że qubit może być dowolną superpozycją swoich stanów bazowych, zamiast przyjmować tylko dwie dyskretne wartości. Rejestr N qubitów jest więc superpozycją 2^N stanów opisywanych za pomocą 2^N amplitud (liczb zespolonych). Operacja na takim rejestrze jest wykonywana jednocześnie na wszystkich 2^N liczbach. W naszym przykładzie, jak wykazał Lov Grover [4], do znalezienia poszukiwanej jedynki wystarczy tylko jedno sprawdzenie. Ogólnie, dla N elementowej bazy danych liczba kroków algorytmu Grovera jest rzędu $\sqrt{N}$, podczas gdy zwykły komputer potrzebuje ich rzędu N. Dla dużych N różnica byłaby więc ogromna. Sercem algorytmu jest powtarzana elementarna operacja (opisana na poziomie popularnym np. w [4,5]), w wyniku której amplituda odpowiadająca poszukiwanej pozycji bazy danych wzrasta w każdym kroku o około $1/\sqrt{N}$. Po około $\sqrt{N}$ krokach będzie więc bliska jedności. Sprawdzenie zawartości rejestru w tym momencie pozwala na niemal pewne uzyskanie poszukiwanej informacji. Algorytm ten może być stosowany do bardzo szerokiej klasy problemów, w których odpowiedź łatwo jest sprawdzić, ale trudno znaleźć. Jeden z uznanych ekspertów w tej dziedzinie, John Preskill, stwierdził [6], że „jeżeli komputery kwantowe będą za 100 lat w użyciu, to przypuszczalnie działać będą według algorytmu Grovera lub czegoś podobnego".

Skoro komputery kwantowe są tak dobre, to dlaczego ich nie ma? Okazuje się, że praktyczna implementacja takich pomysłów natrafia na olbrzymie trudności eksperymentalne. Pojedynczym qubitem może być dowolny układ kwantowy o dwóch stanach bazowych, np. spin jądra atomowego. Problem polega na tym, że w trakcie wykonywania obliczeń z rejestru składającego się z qubitów nie powinna wypłynąć żadna informacja! Ostatnio okazało się wprawdzie możliwe poprawianie „kwantowych błędów" (zob. np. przegląd [7]), ale i tak szczególna podatność układów kwantowych na zaburzenia spędza sen z powiek konstruktorom układów doświadczalnych, mających działać jako komputery kwantowe.

Jak zaznaczyłem na początku dzisiejszych aktualności, udało się właśnie zbudować pierwszy „pełny" komputer kwantowy [1]. Jako rejestru kwantowego użyto roztworu chloroformu $CHCl_3$. Pojemność rejestru wynosiła 2 qubity odpowiadające spinom atomów wodoru i węgla ^{13}C, przy czym rolę rejestru spełniała nie pojedyncza cząsteczka, ale (niekoherentny) zespół wszystkich par ^1H–^{13}C. Operacje na rejestrze wykonywane były przy użyciu techniki jądrowego rezonansu magnetycznego. Za pomocą takiego komputera przeprowadzono doświadczalny test algorytmu Grovera. Warto dodać, że całe urządzenie mieści się na biurku. Po jego popularny opis odsyłam do [2]. Technika ta ma szansę rozszerzenia do rejestrów kilku-, a nawet kilkunasto-qubitowych już w najbliższej przyszłości. Jak długo jednak trzeba będzie poczekać na kwantowy komputer z prawdziwego zdarzenia, posiadający rejestr o pojemności przynajmniej kiloqubitów? Myślę, że nie tak długo, zwłaszcza jeżeli czytelnicy *Delty* nie poprzestaną na czekaniu...

Piotr ZALEWSKI

[1] I. L. Chuang, N. Gershenfeld, M. Kubiniec *Phys. Rev. Lett.* **80** (1998) 3408.
[2] G. Taubes, *Science* **275** (1998) 307.
[3] P. W. Shor, in Proc. of the 34th Ann. IEEE Symp. on Found. of Comp. Sci., 1994, 116–123.
[4] L. K. Grover, *Phys. Rev. Lett.* **79** (1997) 325.
[5] G. P. Collins, *Physics Today*, October 1997, 19.
[6] J. Preskill, quant-ph/970532.
[7] J. Preskill, quant-ph/970531.