DOI: 10.24425/academiaPAN.2024.150034

prof. Artur Ekert
Polski fizyk teoretyk, absolwent Uniwersytetu Jagiellońskiego i Uniwersytetu Oksfordzkiego, profesor fizyki kwantowej w Mathematical Institute Uniwersytetu Oksfordzkiego oraz profesor honorowy Lee Kong Chian (Lee Kong Chian Centennial Professor) Narodowego Uniwersytetu Singapuru. Jego zainteresowania naukowe obejmują dziedzinę przetwarzania informacji w systemach kwantowo-mechanicznych ze szczególnym uwzględnieniem kryptografii i obliczeń kwantowych. Laureat wielu wyróżnień i nagród, m.in. Medalu Maxwella, Medalu Huygensa, Nagrody Kartezjusza, Nagrody Milnera.
artur.ekert@maths.ox.ac.uk

W KRAINIE KUBITÓW

Komputery kwantowe mogą rozwiązywać zadania, w których klasyczne komputery się nie sprawdzą. To zasługa mechaniki kwantowej – mówi **prof. Artur Ekert** z Mathematical Institute Uniwersytetu Oksfordzkiego oraz Narodowego Uniwersytetu Singapuru.

Jeszcze kilka lat temu ośrodki naukowe prześcigały się w posiadaniu coraz szybszych superkomputerów. Obecnie coraz częściej czytamy wiadomości o komputerach kwantowych. Czy to nawiązanie do fizyki kwantowej jest uzasadnione, czy to tylko chwyt marketingowy?

ARTUR EKERT: Superkomputery klasyczne i komputery kwantowe to zupełnie co innego. Cofnijmy się do czasów, gdy ludzie zaczęli myśleć o automatyzacji obliczeń. Twórcy teorii, twórcy informatyki, *computer science*, tacy jak Alan Turing, potrafili wydobyć esencję fizyki, którą znali. Każda informacja ma nośnik. Nie ma informacji w sensie abstrakcyjnym, informacja jest zawsze zakodowana w jakiejś postaci. Czy to jest elektron, fala akustyczna, prąd, czy kondensator, który jest naładowany lub nienaładowany – to zawsze jest to jakiś stan obiektu fizycznego. Nie ma informacji bez reprezentacji fizycznej. Z informacją możemy zrobić różne rzeczy, to zależy tylko od praw fizyki, dlatego że one dyktują, w jaki sposób możemy przetwarzać stan fizyczny z jednego w drugi. A stan fizyczny reprezentuje informacje, co oznacza, że obliczenia to nic innego jak proces fizyczny. Nie znamy obliczenia, które nie jest procesem fizycznym.

Czyli poznanie praw przyrody rządzących mikroświatem mechaniki kwantowej coś zmieniło?

Jeśli w fizyce są odkrywane nowe rzeczy, to automatycznie powstaje możliwość przetwarzania informacji w inny sposób. Te nowo odkryte zjawiska można użyć do przetwarzania informacji. Przez długi czas, do początku XX wieku, fizyka klasyczna była dziedziną nauki, którą znaliśmy, rozumieliśmy, zawsze była w tle wszystkich maszyn obliczeniowych, które powstały. Komputer Babbage'a i późniejsze elektromechaniczne maszyny obliczeniowe bazowały na klasycznej fizyce. I na podstawie tego wyodrębniono abstrakcyjną teorię informacji – informatykę. Takie maszyny ludzie znali, takimi maszynami byli również ludzie, którzy wykonywali obliczenia. Wraz z mechaniką kwantową odkryto nowe zjawiska, które przyniosły nowości wcześniej nieznane. Te świeżo okiełznane zjawiska można używać do przetwarzania informacji.

Czy bit przestał być bitem?

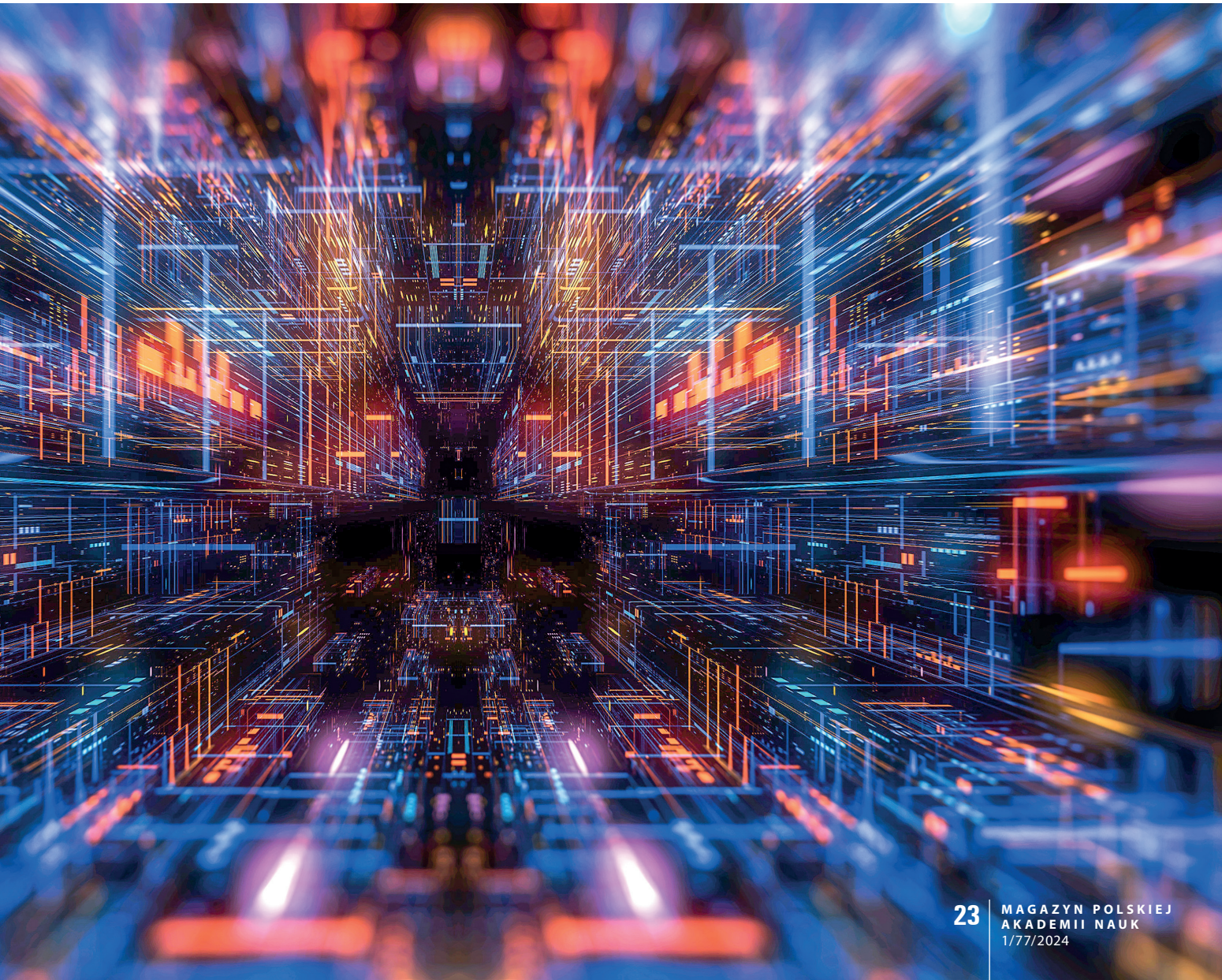
Dawny, klasyczny bit z punktu widzenia fizyka to był każdy układ fizyczny, który można było umiejscowić

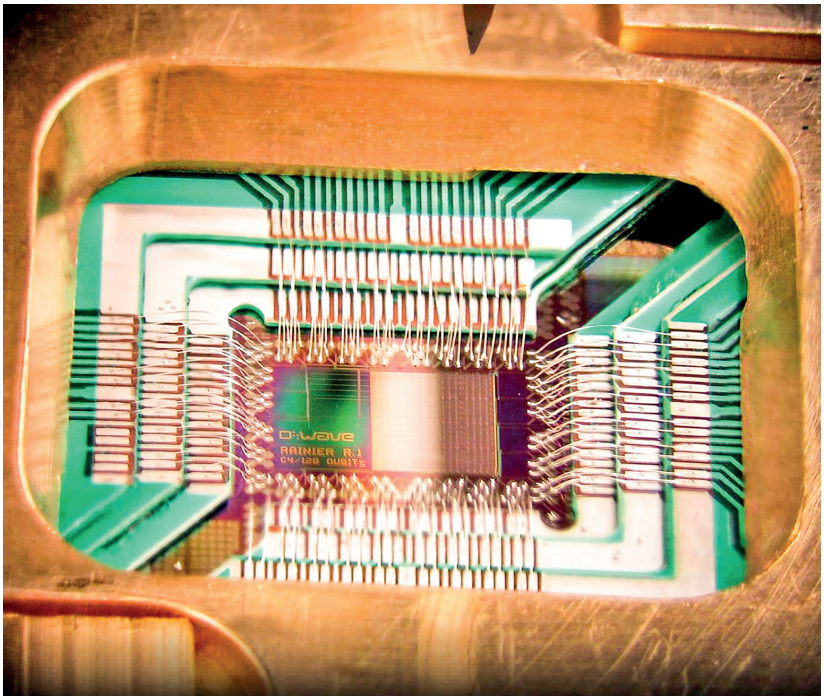
QUARDIA/SHUTTERSTOCK.COM

w dwóch stanach, którym się nadawało oznaczenie „zero" czy „jeden". I jakakolwiek to była technologia klasyczna, to był proces fizyczny, który pozwalał zmienić wartość bitu „zero" na „jeden" i z powrotem. Połączenie kilka bitów z sobą pozwala tworzyć bramki logiczne, np. prosta operacja zmiany bitu – tzw. *Bit-Flip*, czyli zmiany bitu z „zera" na „jeden" i z „jeden" na „zero" – to jest operacja logiczna NOT. Są bramki logiczne typu koniunkcja AND i alternatywa OR itd. Są to więc podstawowe operacje. Kolejnym etapem zamieniającym procesy obliczeniowe jest fizyka kwantowa. Według niej układ fizyczny możemy umiejscowić w różnych stanach: „zero" i „jeden", a także w pośrednich. Jest to układ dwustanowy w tym sensie, że dokonując jakiegokolwiek pomiaru na tym obiekcie, zawsze widoczne jest albo „zero" albo „jeden" – nic więcej. Doświadczenie mówią, że gdzieś tam w tle jest tych stanów znacznie więcej, ponieważ można je przetwarzać. W związku z tym, kubit różni się od bitu tym, że w odróżnieniu od klasycznego bitu, który istnieje tylko w stanie „zero" lub „jeden", bit kwantowy może być przygotowany w wielu innych stanach, które następnie można wykorzystać do procesów obliczeniowych.

Czyli fizyka jest wszędzie, nawet w informatyce. Mamy więc pomysł na hardware. Czy udało się to już skonstruować i to działa?

Jeszcze nie, ale to jest oczywiście bardzo dobre pytanie. Informatyka kwantowa zaczęła się rozwijać w sposób nietypowy dlatego, że najpierw poszły badania teoretyczne. Ludzie zauważyli, że rzeczywiście można robić coś innego, że gdy zaprzęgnie się mechanikę kwantową do obliczeń, to obliczenia kwantowe mają dużo zalet. Szczególnie przydatna jest teoria złożoności obliczeniowej (ang. *computational complexity*). Okazuje się, że fizycy najczęściej interesują się, czy jakieś zjawisko może zaistnieć, czy nie. Zasady określają, że pewne zjawiska są niemożliwe, np. dlatego że przeczyłyby zasadzie zachowania energii czy zachowania pędu. A zatem pewne procesy fizyczne są jak gdyby niemożliwe, bo przeczyłyby znanym





HTTPS://PL.WIKIPEDIA.ORG/WIKI/KOMPUTER_KWANTOWY#/MEDIA/PLIK: DWAVE_128CHIP.JPG

Układ skonstruowany przez D-Wave Systems, zawierający 128 kubitów zrealizowanych za pomocą nadprzewodników

nam zasadom, a inne nie. Więc podstawowe pytanie stawiane przez fizyków brzmi: „Czy coś jest możliwe, czy nie? ". Informatycy stawiają podobne pytanie, lecz dotyczące obliczeń: „Czy coś jest do obliczenia, czy nie? " i „Czy algorytmy do obliczeń są wydajne, efektywne? "

Co to znaczy, że algorytm jest efektywny?

Otóż są pewne algorytmy, które mówią nam, jak coś zrobić, ale gdy staramy się rozwiązać ten problem, to na wejściu mamy coraz więcej danych. Dobrym przykładem jest proces rozłożenia jakieś liczby na czynniki pierwsze. Im większa liczba, tym jej rozkład na czynniki pierwsze zajmuje komputerowi coraz więcej czasu, wymaga też użycia coraz więcej pamięci. Matematycy zastanawiali się, jak to będzie się kalkulowało z wielkością liczby, czy rozłożenie na czynniki pierwsze dwa razy większej liczby trwa dwa razy dłużej. Jeśli ten czas i zużycie pamięci jest wielomianową funkcją liczby bitów liczby rozkładanej, czy to znaczy, że algorytm jest efektywny. Ale jeśli jest to funkcja wykładnicza, to taki algorytm jest nieefektywny, niewydajny. Zauważono, że algorytm mnożenia dwóch liczb przez siebie jest wydajny, a czas, w jakim komputer wykona mnożenie, dość wolno skaluje się z liczbą bitów czynników, czyli z wielkością obu liczb. Im większe liczby mnożymy, tym obliczenie trwa dłużej, ale nie wiele dłużej. Wiemy z matematyki, że każdą liczbę złożoną można rozłożyć na czynniki pierwsze, np. 15 to jest 3 razy 5. To jest tzw. *factoring problem*. Okazuje, że algorytm, zgodnie z którym zwykły komputer ma przeprowadzić ten proces odwrotny, nie jest wydajny. Czas rozkładu liczby na czynniki pierwsze rośnie wykładniczo z liczbą bitów rozkładanej liczby. Rozłożenie bardzo dużej liczby na czynniki pierwsze wymaga bardzo dużo czasu pracy komputera. A jest to bardzo ważny problem matematyczny. Można oczywiście zbudować nowy, wydajniejszy komputer, który ma zegar i jest ileś tam razy szybszy, np. milion razy, niż wcześniejszy. Rozłożenie tej liczby potrwa milion razy krócej, ale ten algorytm, który jest niewydajny na wolnym komputerze, na szybkim będzie tak samo niewydajny. Wykładniczy wzrost czasu trwania obliczeń będzie nadal wzrostem wykładniczym.

Czy komputery kwantowe mogą dokonać jakiegoś przełomu?

Postęp technologiczny jako taki nie daje nam możliwości zmiany klasyfikacji algorytmu. Do tego trzeba stworzyć nowe prawo lub nowy algorytm. Okazuje się, że do rozwiązywania pewnych problemów nie znamy jeszcze wydajnego algorytmu klasycznego, ale mamy wydajne algorytmy kwantowe. Jeśli tylko mielibyśmy komputer kwantowy, to te algorytmy na nim będą. Siła komputerów kwantowych polega na tym, że fizyka kwantowa daje większy i szerszy zestaw instrukcji oraz można ich użyć do programowania. Co więcej, pewne instrukcje, które odzwierciedlają procesy fizyczne, mają sens tylko dla komputerów kwantowych. Używając tych dodatkowych instrukcji, możemy stworzyć nowe, jeszcze wydajniejsze algorytmy.

Klasyczne komputery często są używane do wykonywania obliczeń w dziedzinie fizyki czy chemii. Czy to nie polega na odpowiednim zaprogramowaniu komputera?

Nie, to nie to samo. Klasyczne komputery mogą to symulować, ale wcale nie poprawia to wydajności, szybkości obliczeń. Ludzie zaczęli już badać sporo problemów, których rozwiązanie mogą przynieść komputery kwantowe.

Czyli jest pomysł na oprogramowanie, software, a co ze sprzętem, hardware?

Sądzę, że jesteśmy w tej chwili na wczesnym etapie. Potrafimy zbudować zestaw kilku bramek logicznych i kubitów w różnych technologiach. Czy to będą pułapki jonowe, czy nadprzewodniki. Udało się połączyć je z sobą i zrobić kilka instrukcji. Wykazano, że można to robić, ale droga do takiego komputera kwantowego, w którym widzielibyśmy w całej krasie i okazałości nadzwyczajne rzeczy, właśnie taką wręcz wykładniczą różnicę w wydajności, jest jeszcze długa. Mamy bramki logiczne, potrafimy je łączyć, sprawdzać pewne podstawowe rzeczy, ale do superwydajnych komputerów kwantowych jeszcze nam daleko. Ale na pewno z każdym dniem coraz bliżej.

Rozmawiał **Witold Zawadzki**

Chcesz wiedzieć więcej?

Kaku M., *Kwantowa dominacja. Jak komputery kwantowe odmienią nasz świat*, Warszawa 2023.

Fernández-Vidal S., Miralles F., *Śniadanie z cząstkami, czyli jak ugryźć fizykę kwantową*, Kraków 2023.

Johnson G., *Na skróty przez czas. Czy nadchodzi era komputerów kwantowych?*, Warszawa 2005.