

[Akceptuje](#)

W ramach naszej witryny stosujemy pliki cookies w celu świadczenia państwu usług na najwyższym poziomie, w tym w sposób dostosowany do indywidualnych potrzeb. Korzystanie z witryny bez zmiany ustawień dotyczących cookies oznacza, że będą one zamieszczone w Państwa urządzeniu końcowym. Możecie Państwo dokonać w każdym czasie zmiany ustawień dotyczących cookies. Więcej szczegółów w naszej [Polityce Prywatności](#)

[Portal](#) [Informacje](#) [Katalog firm](#) [Praca](#) [Szkolenia](#) [Wydarzenia](#) [Porównania międzylaboratoryjne](#)
[Kontakt](#)



[Laboratoria](#)
[.net](#)
[Innowacje](#)
[Nauka](#)
[Technologie](#)

[Logowanie](#) [Rejestracja](#) [pl](#)

Newsletter

zapisz się



- [Nowe technologie](#)
- [Felieton](#)
- [Tygodnik "Nature"](#)
- [Edukacja](#)
- [Artykuły](#)
- [Przemysł](#)

[Strona główna](#) > [Edukacja](#)

Budowa kwantowego komputera jest niezwykle trudna

Budowa komputerów kwantowych znajduje się na podobnym etapie, jak rozwój komputerów w latach 50-tych XX w, ale w ciągu kilkunastu lat może nastąpić przełom - podkreśla prof. Marek Kuś z Centrum Fizyki Teoretycznej PAN. W przyszłości maszyny takie mogą zupełnie odmienić informatykę, a z nią - inne dziedziny nauki i techniki. Doniesienia o inwestycjach w pracę nad komputerami kwantowymi napływają z różnych stron świata.

Prof. dr hab. Marek Kuś jest pracownikiem Centrum Fizyki Teoretycznej Polskiej Akademii Nauk.

Specjalizuje się w dziedzinie fizyki matematycznej, chaosu kwantowego oraz teorii informacji kwantowej.

PAP: Coraz częściej pojawiają się doniesienia o nowych komputerach kwantowych. Jaki jest faktycznie obecny etap ich rozwoju? Czy można go porównać do któregoś momentu w rozwoju klasycznych komputerów?

Prof. dr hab. Marek Kuś: To, że (technologia - PAP) startuje, nie ulega wątpliwości. Budzi zainteresowanie dużych agencji i instytucji - a ono pojawia się, gdy rzeczywiście istnieją ku temu powody. Jednak obecnie mamy do czynienia z wczesną fazą. Dysponujemy rozbudowaną teorią obliczeń kwantowych, ale nadal do pokonania pozostają bariery technologiczne. Obecną sytuację można porównać do tej, z końca pierwszej połowy XX wieku, kiedy powstawały pierwsze klasyczne komputery. Moc pierwszej takiej maszyny była znikoma w porównaniu do mocy dzisiejszych biurkowych komputerów, choć komputer pomagał w pewnych obliczeniach np. z zakresu fizyki jądrowej. Jeśli chodzi o komputery kwantowe, to według mnie ich obecne możliwości są nawet mniejsze, bo jeszcze nie udało się dzięki nim rozwiązać właściwie żadnego istotnego problemu.

Owszem - można rozwiązywać z ich pomocą niektóre problemy optymalizacyjne. Robi to na przykład komputer D-Wave. Czy są one jednak na tyle złożone, by być zadowolonym z pracy tych komputerów? Uważam, że jeszcze nie. Pierwszy komputer świata - ENIAC, pomagał przy budowie bomby wodorowej. Tymczasem nie mamy jeszcze kwantowych komputerów, które by rozwiązywały naprawdę praktyczne problemy.

PAP: Ile na świecie istnieje komputerów kwantowych?

MK: Takich urządzeń może istnieć kilkadziesiąt. Raczej jednak mówiłbym o procesorach, składających się najwyżej z kilkudziesięciu kwantowych bramek.

PAP: Nadzieje są takie, że komputery kwantowe staną się z czasem niewspółmiernie szybsze od klasycznych. Jak można je porównać do klasycznych maszyn: jak samochód do roweru? Czy to jeszcze zbyt mała różnica?

MK: Będzie ona znacznie większa. Dobrym przykładem jest możliwość złamania przez komputer kwantowy zabezpieczeń kryptograficznych wykorzystujących tzw. algorytm klucza publicznego. Do zaszyfrowania wiadomości używa się s nich dużej liczby będącej iloczynem dwóch liczb pierwszych i ta liczba jest właśnie kluczem publicznym, a do odszyfrowania, czy też załamania kodu potrzebna jest znajomość obu czynników, które stanowią klucz prywatny. Jeśli klucz jest odpowiednio dużą liczbą, a takie używane są w zastosowaniach, to do znalezienia jej czynników, czyli złamania szyfru, przy użyciu wszystkich dostępnych komputerów na Ziemi, wiek Wszechświata okazałby się zbyt krótki. Natomiast uważa się, że komputer kwantowy sobie z tym poradzi bez trudu.

PAP: To znaczy, że wszystkie dzisiejsze szyfry staną się bezużyteczne?

MK: Teoretycznie tak. Dlatego szuka się już nowych, postkwantowych sposobów zabezpieczania przesyłanych informacji. Choć nie ma gwarancji, że również nie zostaną one w jakiś sposób złamane.

PAP: Jednak potencjalne zastosowania komputerów kwantowych z pewnością są szersze. Gdzie jeszcze będzie można je wykorzystać? W tworzeniu różnych symulacji, poszukiwaniach nowych materiałów, projektowaniu przemysłowym, biznesie?

MK: Doskonale nadają się do rozwiązywania problemów optymalizacyjnych. Na przykład do opracowania jak najlepszego systemu połączeń kolejowych, samochodowych czy lotniczych między wieloma miejscami. Będzie je można zresztą wykorzystać we wszystkich dziedzinach, które Pan

wymienił. Tak naprawdę mogą działać na każdym polu, na którym pracują dzisiejsze komputery - tylko dużo szybciej.

PAP: Czy pozwolą wprowadzić na wyższy poziom sztuczną inteligencję?

MK: Jedną z podstaw sztucznej inteligencji jest tzw. uczenie maszynowe i związane z nim rozpoznawanie różnorodnych wzorów - na przykład obrazów, elementów języka czy innych skomplikowanych struktur. W tej metodzie tworzy się sztuczne sieci neuronowe, które samodzielnie się uczą. Znane są już algorytmy, które mogłyby wykonywać takie zadania na komputerach kwantowych z dużo większą prędkością.

PAP: A czy w jakiejś dziedzinie kwantowe komputery będą sobie radziły gorzej, niż obecne?

MK: Tutaj warto powiedzieć, że oprócz sprzętu istotne jest również oprogramowanie. Komputery kwantowe programuje się zupełnie inaczej niż klasyczne. Znanych jest już wiele „kwantowych” algorytmów, ale nie jest tak, że wiemy, jak kwantowo rozwiązać każdy problem, doskonale obsługiwany przez komputery klasyczne. Dla wielu zadań odpowiednie metody trzeba dopiero wymyślić. Niestety nie istnieją konkretne, jasne reguły, jak to robić.

PAP: Jednak, to właśnie z tego, że kwantowe komputery zupełnie inaczej działają, ma wynikać ich ogromna prędkość. Jak można pokrótce wyjaśnić tę zasadę?

MK: W klasycznym komputerze mamy do czynienia z elementami, które mogą być w jednym z dwóch stanów. Na przykład, przez taki element może płynąć prąd lub nie. Dlatego dzisiaj komputery operują na bitach - jednostkach informacji, które mogą mieć wartość 0 lub 1. W przypadku komputerów kwantowych jest zupełnie inaczej. Mechanika kwantowa mówi bowiem, że dany układ może się znajdować w superpozycji różnych stanów. To znaczy, jak gdyby, może przebywać w kilku stanach jednocześnie. Zamiast o bitach, mówi się więc o kubitach (bitach kwantowych). Dzięki tej niezwyklej własności przyjmowania różnych stanów naraz mogą one przetwarzać znacznie więcej informacji. Do tego wraz ze wzrostem ich liczby moc obliczeniowa rośnie wykładniczo. To główna zasada, którą wykorzystuje się na różne sposoby.

PAP: Ile takich kubitów musi zawierać kwantowy procesor, aby mógł rozwiązywać praktyczne problemy?

MK: Naprawdę dużo. Problem polega na tym, że kubity łatwo tracą swoje własności kwantowe, np. przebywanie we wspomnianej superpozycji stanów, m.in. ze względu na oddziaływania z otoczeniem. Jednym ze sposobów jest łączenie tych podstawowych kubitów z innymi kubitami, które - w uproszczeniu mówiąc - stabilizują przechowywaną informację. Jednak na jeden roboczy kubit potrzeba około tysiąca dodatkowych. Tymczasem, aby na przykład pokazać, że $15 = 3 * 5$, potrzeba kilkudziesięciu roboczych kubitów, co w sumie, z dodatkowymi kubitami daje ich kilkadziesiąt tysięcy.

PAP: A ile kubitów mają dzisiejsze procesory?

MK: Dzisiejsze konstrukcje mają ich rzędu 100.

PAP: Problemów jest jednak więcej. Obecne konstrukcje są duże i wymagają utrzymywania procesora w temperaturze bliskiej zera bezwzględnego...

MK: Istnieją różne pomysły realizacji komputerów kwantowych. Nadprzewodzące kubity wymagają ultra-niskich temperatur, podobnie jak oparte na tzw. pułapkowanych jonach czy atomach. Buduje się też jednak procesory kwantowe, oparte na manipulowaniu stanami fotonów o mniejszych

wymaganiach co do temperatury. Pamiętajmy jednak, że pierwsze komputery też były duże. Na razie nie myślimy o budowie kwantowego laptopa, choć i na to może przyjdzie czas. Najpierw chcemy zbudować po prostu dobrze działające komputery kwantowe - niezależnie od tego, jakie będą miały rozmiary.

PAP: Zatem uważa Pan, że kwantowe laptopy czy smartfony mogą się kiedyś pojawić?

MK: Nie umiem tego powiedzieć, ale ludzka pomysłowość wydaje się nieograniczona. Gdybyśmy twórców ENIACA zapytali, czy za kilkadziesiąt lat komputery na biurkach znajdą się komputery nieporównanie szybsze - pewnie by stwierdzili, że to mało prawdopodobne. Sam jestem umiarkowanym optymistą. Uważam, że w ciągu kilkunastu lat doczekamy się jakichś przełomowych dokonań w dziedzinie kwantowej informatyki.

PAP: Jaki udział mogą mieć w tym postępie Polacy? Czy Polska może mieć swój komputer kwantowy?

MK: Wykluczyć tego nie można, ale zbudowanie takiej maszyny jest niezwykle trudne. Jednak Polska ma ogromny wkład w rozwój teorii kwantowej informatyki. Nasz kraj znajduje się pod tym względem w czołówce. Podejmowane są też próby konstruowania kwantowych urządzeń, choć raczej chodzi o układy doświadczalne, na których można sprawdzać różne teorie. Mamy w sumie szereg dużych projektów, w które zaangażowane są liczne krajowe, znane na świecie ośrodki. Bierzymy przy tym udział w różnych międzynarodowych przedsięwzięciach. W naszym instytucie realizujemy kilka projektów związanych z informatyką kwantową. Między innymi kierujemy dużym projektem finansowanym przez Fundację na rzecz Nauki Polskiej we współpracy z Instytutem Informatyki Teoretycznej i Stosowanej PAN w Gliwicach i Uniwersytetem Jagiellońskim. Jego celem jest badanie możliwości i przeszkód w konstruowaniu urządzeń do obliczeń kwantowych przy ograniczeniach, które narzucają nam istniejące obecnie możliwości technologiczne. Zajmujemy się optymalizacją algorytmów kwantowych, ograniczeniem wpływu zaburzeń, problemami korekcji błędów.

Źródło: pap.pl

<http://laboratoria.net/edukacja/31714.html>

Informacje dnia: [W Polsce żyje miasto ludzi uratowanych dzięki przeszczepom szpiku](#) [Popularny lek na tarczycę może mieć związek z zanikiem kości](#) [W ostatnich 60 latach światowa produkcja żywności stale rosła](#) [Sztuczna inteligencja niesie zagrożenia dla rynku pracy](#) [Program naprawczy dla NCBR IChF PAN z grantem KE](#) [W Polsce żyje miasto ludzi uratowanych dzięki przeszczepom szpiku](#) [Popularny lek na tarczycę może mieć związek z zanikiem kości](#) [W ostatnich 60 latach światowa produkcja żywności stale rosła](#) [Sztuczna inteligencja niesie zagrożenia dla rynku pracy](#) [Program naprawczy dla NCBR IChF PAN z grantem KE](#)

Partnerzy