

Komputer kwantowy Google'a – przełom czy PR?

*Instytut Fizyki Teoretycznej, Wydział Fizyki, Uniwersytet Warszawski

Rafał DEMKOWICZ-DOBRZAŃSKI*

Komputerom kwantowym poświęciliśmy cały numer Δ_{12} , którego redaktorem prowadzącym był Tomasz Kazana.

Obliczenia kwantowe wykorzystują ideę superpozycji kwantowej, która pozwala na przygotowanie układów kwantowych w „wielu stanach jednocześnie”, w celu uzyskania nieosiągalnego na komputerach klasycznych zrównoleglenia obliczeń i rozwiązania bardzo trudnych problemów matematycznych w czasie nieosiągalnym dla tradycyjnych urządzeń liczących. Przykładem obliczeń prostych dla komputerów kwantowych, a trudnych dla klasycznych, jest rozkład liczby na czynniki pierwsze. Trudność tego problemu jest kluczowa dla bezpieczeństwa ogromnej większości zaszyfrowanej komunikacji internetowej.

Ostatnio docierały do nas informacje o nowym sukcesie Google'a w związku z przeprowadzeniem obliczeń na komputerze kwantowym, które najlepszemu superkomputerowi klasycznemu zajęłyby 10 000 lat, na co IBM odpowiedział „wcale nie”! Na ile jest to PR, a na ile faktyczny przełom?

1. Na pewno jest to bardzo duże osiągnięcie. Grupie z Google'a udało się zbudować urządzenie pracujące na 53 kubitach, ale co najważniejsze kubitach bardzo dobrej jakości, gdzie pojedyncze bramki kwantowe są wykonywane z bardzo niewielkimi błędami, poniżej 0,5%. Na przykład DWAVE postawił na liczbę kubitów (nawet 4096), nie dbając o ich jakość. Jednak takie myślenie wprowadziło sporo zamieszania i wątpliwości, czy w ogóle to, co robi DWAVE, można nazwać obliczeniami kwantowymi.

W przypadku urządzenia Google'a nie ma wątpliwości: jest to topowe na świecie urządzenie, które wykonuje obliczenia kwantowe.

2. Należy przy tym zaznaczyć, że mimo iż poziom błędów poniżej 0,5% wydaje się niski, nie jest on niestety wystarczająco niski, żeby urządzenie spełniało wymogi tzw. *fault-tolerance* – które oznaczają, że przy danej jakości komponentów można efektywnie zmniejszać błędy poprzez rozbudowywanie obwodów i implementacje tzw. kwantowych kodów korekcji błędów. Do tego niestety wciąż brakuje około 1–2 rzędów wielkości zmniejszenia błędów.

3. Z tego powodu na razie nie ma możliwości przeprowadzenia żadnych praktycznych obliczeń na tego typu urządzeniach. Tym samym Google obniżył sobie poprzeczkę, nie starając się przeprowadzić praktycznego obliczenia, a jedynie jakiegokolwiek obliczenie, które byłoby trudne klasycznie. Z tego powodu zdecydowali się na zadanie: niech komputer klasyczny spróbuje generować liczby losowe zadane rozkładem prawdopodobieństwa zdeterminowanym przez wyjścia pewnego kwantowego obwodu logicznego wygenerowanego poprzez losowo wybierane bramki kwantowe. Jeśli zgodzić się z takim wyzwaniem, to faktycznie wydaje się, że w tym sensie osiągnięto swój cel.

4. Dzień po ogłoszeniu wyników IBM wysunął kontrargument, że w zasadzie to, co zrobił Google, można zasymulować na superkomputerze Summit (klasyczny komputer opracowany przez IBM), i to wcale nie w 10 000 lat, ale w 2 dni. I to też wydaje się prawdą. Google nie docenił tym razem dostępnej ogromnej pamięci w urządzeniu Summit, która de facto pozwala zapisać wiernie wektor stanu 53 kubitów (ponieważ 2^{53} wciąż jest mniejsze niż 250 petabajtów, którymi dysponuje Summit). Ale nawet jeśli kontrargument IBM jest słuszny, to faktem jest, że gdyby tylko dodano 3–4 kubity do urządzenia kwantowego, to już taka szybka symulacja nie byłaby możliwa – chyba że IBM powiększy swój superkomputer o kolejne kilka boisk.

5. Podsumowując, nie należy się spodziewać, że osiągnięcie Google'a spowoduje przełom, dzięki któremu w końcu komputery kwantowe zaczną liczyć coś użytecznego. Do tego potrzeba jeszcze paru skoków technologicznych, tak aby poziom błędów był wystarczająco niski i możliwe było przeprowadzanie poważniejszych obliczeń na większej liczbie kubitów oraz aby skutecznie implementować kody kwantowej korekcji błędów. Niemniej jest to pewien wyraźny i wcale nie oczywisty krok naprzód.

