Jarosław Wódka
Matematyki Informatyki i Mechaniki

Komputery kwantowe jako *disruptive technology*

W ubiegłej dekadzie ciągły wzrost taktowania procesorów poprzestał na granicy około 3GHz. Od tego momentu rozwój jednostek obliczeniowych ukierunkował się na zwiększanie ilości rdzeni CPU. Krok dalej poszła firma nVidia oferując programistom karty graficzne typu CUDA oferujące setki wątków obliczeniowych. Te trendy wymusiły na uczelniach informatycznych zmianę podejścia w nauczaniu programowania. Aby wykorzystać dostępne zasoby obliczeniowe konieczne było położenie większego nacisku na nauczanie programowania w środowisku rozproszonym. Czy taki model programowania zagości w informatyce na wiele dziesięcioleci?

Już teraz model programowania rozproszonego jest zagrożony przez pierwsze, eksperymentalne komputery kwantowe. Najnowsze z nich potrafią wykonać bardzo proste operacje, takie jak faktoryzacja liczby 21. Wielu wierzy, że dalszy rozwój komputerów kwantowych spowoduje, że staną się one w ciągu dwudziestu lat tak popularne, jak dzisiejsze laptopy, a przy tym miliony razy szybsze. To z kolei oznacza dla programistów, że zamiast operować na bitach, będą musieli pracować z kubitami. Natomiast algorytmy rozproszone zostaną wyparte przez algorytmy kwantowe.

Komputery te mają znacznie większy potencjał, niż obecne komputery. Na chwilę obecną są to jeszcze mało wydajne maszyny, jednak jeśli będą podążać prawem Moore'a, w ciągu 20 lat mogą zagościć do naszych domów. Będzie to nie lada gratka dla miłośników gier komputerowych. Większe możliwości obliczeniowe komputerów będą oznaczać bardziej rozbudowane środowisko gry, inteligentniejszych przeciwników oraz bardziej szczegółowy świat gry.

Rozwój komputerów kwantowych będzie miał swój wydźwięk nie tylko w naszym życiu codziennym, ale przede wszystkim technologia ta otworzy nowe możliwości w wielu dziedzinach nauki, np:

- **genetyka**: Obecnie przetwarzanie i analizowanie sekwencji genetycznych to proces wymagający ogromnych nakładów sprzętu komputerowego. Głównym problemem jest ogrom danych do przetworzenia. W przyszłości, takie analizy będzie mógł przeprowadzić jeden komputer kwantowy.

- **rynki finansowe**: Wycena instrumentów finansowych zależy od niezliczonej ilości czynników. Obecne komputery biorą pod uwagę tylko najważniejsze z nich. Komputery kwantowe pozwolą na znacznie dokładniejszą wycenę.

- **medycyna**: Technologia ta ulegnie znacznej miniaturyzacji. Komputery te będzie można obudować w mikro roboty, które będą wszczepiane do organizmu chorego na nowotwór pacjenta, aby zlokalizować i usunąć przyczynę choroby.

Technologia ta niesie dla ludzkości także pewne zagrożenia. Trafnym przykładem jest bezpieczeństwo danych. Większość powszechnie używanych dzisiaj algorytmów szyfrujących opartych jest o trudność faktoryzacji liczb złożonych z iloczynu małej ilości liczb pierwszych. Komputery kwantowe jednak bardzo dobrze radzą sobie z tym problemem. To oznacza, że kanały kryptograficzne, których używamy każdego dnia, aby na przykład zalować się do banku za pośrednictwem komputera, zostaną złamane. Oznacza to ogromne zagrożenie dla bezpieczeństwa i poufności każdego użytkownika Internetu.

Komputery kwantowe są intensywnie rozwijającą się technologią w ostatnich latach. Jeśli rozwój ten dalej będzie postępował, klasyczne komputery zostaną wyparte przez komputery kwantowe. Otworzy to przed ludzkością nowe możliwości, ale stworzy też pewne zagrożenia.