Wykład monograficzny

Algorytmy Kwantowe

dr Miłosz Michalski

Kwantowa teoria informacji, zwana bardziej popularnie *informatyką kwantową*, jest dzisiaj jedną z najszybciej rozwijających się gałęzi fizyki. Idea kwantowego komputera, którą jako swego rodzaju konceptualną zabawę zaproponował w latach 70-tych Richard Feynman, powróciła na nowo po bez mała 20 latach, w związku z bardzo spektakularnym postępem w zakresie technik laboratoryjnych, przedłużających nasze zdolności manipulacyjne do poziomu pojedynczych obiektów kwantowych. Kwantowy komputer trafił w latach 90-tych na czołówki codziennych gazet i choć w rzeczywistości budowa takiego urządzenia to nadal bardzo odległy, o ile w ogóle możliwy do realizacji cel, nie sposób odmówić informatyce kwantowej sukcesów. Np. w dziedzinie telekomunikacji opracowano całkowicie bezpieczne kwantowe protokoły kryptograficzne do przesyłania poufnych danych. Na rynku działają już firmy oferujące komercyjnie kwantowe maszyny szyfrujące.

Algorytmy kwantowe, wobec niedostępności kwantowego procesora, można dziś co najwyżej symulować klasycznie, niestety gubiąc przy tym ich największy atut — niewiarygodną szybkość działania. Ta wielka moc obliczeniowa przyszłych programowalnych urządzeń kwantowych daje nadzieję na rozwiązanie wielu problemów obliczeniowych, z którymi prawdopodobnie nie poradzą sobie nigdy nawet najlepsze klasyczne superkomputery.

Przykładem jest z pozoru banalne zadanie rozkładu liczby na czynniki pierwsze. Choć metoda rozwiązania jest niemal oczywista, liczba elementarnych operacji potrzebna do rozkładu dużej, powiedzmy 1000-cyfrowej liczby, jest tak wielka, że najszybszym klasycznym procesorom zadanie to zajęłoby miliony lat. Przeciwnie, kwantowy algorytm Shora teoretycznie radzi sobie z faktoryzacją liczb podobnego rzędu w ciągu kliku sekund lub minut. Warto przy tym zauważyć, że bezpieczeństwo powszechnie stosowanych w dzisiejszych sieciach komputerowych algorytmów szyfrujących, protokołów z tzw. „publicznym kluczem", czy też realizacji podpisu elektronicznego (wykorzystujących algorytm RSA) zasadza się właśnie na niemożności szybkiej faktoryzacji liczb. Łamanie takich kodów polega bowiem na rozkładzie wielkiej liczby, pełniącej rolę klucza szyfrującego. Tak więc osiągnięcia informatyki kwantowej z jednej strony — poprzez algorytm Shora — przekreślają skuteczność klasycznej kryptografii, z drugiej zaś oferują zupełnie nowe, niezawodne, kwantowe metody bezpiecznej wymiany poufnych danych.

Warto więc poznać algorytmy kwantowe w oczekiwaniu na pojawienie się na rynku pierwszych kwantowych laptopów.

Wykład rozpocznie się omówieniem podstaw teorii informacji w ujęciu klasycznym i kwantowym, modeli klasycznej złożoności obliczeniowej i porównaniem ich z kwantowymi odpowiednikami. Następnie zajmiemy się „komputerem kwantowym" w ujęciu R. Feynmana (1985) oraz tym jak idee Feynmana mają się do dzisiejszego spojrzenia na kwantowe układy liczące. Główna część wykładu poświęcona będzie „algorytmom kwantowym"

wykorzystującym tzw. kwantową transformację Fouriera — algorytmowi Deutscha-Jozsy, algorytmowi faktoryzacji Shora i algorytmowi Simona. Omówimy również kwantowy algorytm szybkiego wyszukiwania Grovera. Wykład zakończy się przeglądem innych zastosowań kwantowej informatyki — w tym zagadnieniom kryptografii kwantowej, gęstego kodowania i kwantowej korekcji błędów.

Do udziału w wykładzie wystarcza elementarna znajomość podstaw informatyki, rachunku macierzowego i analizy zespolonej oraz podstaw mechaniki kwantowej.

Miłosz Michalski

Literatura

1. M.A. Nielsen, I.L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2000.
2. V. Vedral, *Introduction to Quantum Information Science*, Oxford University Press, 2006.
3. Ph. Kaye, R. Lafamme, M. Mosca, *An Introduction to Quantum Computing*, Oxford University Press, 2007
4. M. Hirvensalo, *Algorytmy Kwantowe*, WSiP, Warszawa, 2004.
5. M. Nakahara, T. Ohmi, *Quantum Computing: From Linear Algebra to Physical Realizations*, CRC Press, 2008.
6. R. Feynman, *Feynman Lectures on Computation*, ed. T. Hey, R.W. Allen, Westview, 1999.
7. T. Hey, *Feynman and Computation: Exploring the Limits of Computers*, Westview, 2002.

Program wykładu

1. Klasyczne modele obliczeń i złożoność obliczeniowa
    a. Maszyny Turinga
    b. Klasyczne układy liczące, zupełne układy bramek
    c. Złożoność obliczeniowa: klasy P i NP
    d. Problemy decyzyjne a problemy obliczeniowe
    e. Obliczenia probabilistyczne, klasa BPP (bounded error probabilistic polynomial time)

    f. Przykład: faktoryzacja liczby
2. Klasyczne obliczenia odwracalne — bramki Fredkina i Toffoliego
3. Qubit
    a. Przestrzeń stanów kwantowych
    b. Reprezentacja stanów na sferze Blocha
    c. Macierze Pauliego jako proste bramki kwantowe
    d. Zupełny układ kwantowych bramek 1-qubitowych
    e. Pomiar stanu qubitu
    f. Twierdzenie o nieklonowaniu
4. Układy qubitów
    a. Stany separowalne i splątane
    b. Miara splątania
    c. Bramki 2-qubitowe C-Not i C-U
    d. Operacje n-qubitowe — kaskadowe konstrukcje sterujące i ich złożoność
    e. Zupełność układu 1-qubitowych bramek kwantowych i C-Not
5. Komputer kwantowy w ujęciu R. Feynmana
6. Splątanie jako zasób obliczeniowy
    a. Teleportacja
    b. Gęste kodowanie
    c. Problem Deutscha-Jozsy
7. Kwantowa transformata Fouriera i estymacja fazy
8. Algorytm faktoryzacji Shora
    a. Klasyczny algorytm RSA — podstawy teorio-liczbowe
    b. Wyznaczanie rzędu elementu w grupie metodami klasycznymi
    c. Zastosowanie kwantowej estymacji fazy do wyznaczania rzędu
    d. Złożoność kwantowego algorytmu Shora
9. Inne zastosowania kwantowej transformaty Fouriera
    a. Określanie okresu funkcji
    b. Dyskretne logarytmy
    c. Problem ukrytej podgrupy jako prototypowy algorytm kwantowy
10. Algorytm wyszukiwania Grovera
11. Kwantowa korekcja błędów

(P. także www.fizyka.umk.pl/~milosz/index.htm)