MAREK SAWERWAIN • JOANNA WIŚNIEWSKA

INFORMATYKA KWANTOWA

WYBRANE OBWODY I ALGORYTMY

PWN

INFORMATYKA KWANTOWA

MAREK SAWERWAIN • JOANNA WIŚNIEWSKA

INFORMATYKA KWANTOWA

WYBRANE OBWODY I ALGORYTMY

PWN

Projekt okładki **Grzegorz Laskowski**

Ilustracja na okładkę **Shutterstock/Mopic**

Wydawca **Łukasz Łopuszański**

Redaktor prowadzący **Jolanta Kowalczuk**

Produkcja **Mariola Grzywacka**

Skład i łamanie **FixPoint**

Publikacja dofinansowana przez Uniwersytet Zielonogórski
i Wojskową Akademię Techniczną

ISBN 978-83-01-18366-0

Wydanie I
Warszawa 2015

Wydawnictwo Naukowe PWN SA
02-460 Warszawa, ul. Gottlieba Daimlera 2
tel. 22 69 54 321; faks 22 69 54 288
infolinia 801 33 33 88
e-mail: pwn@pwn.com.pl; www.pwn.pl

Druk i oprawa: OSDW Azymut Sp. z o.o.

Spis treści

Wstęp

Informatyka kwantowa to nowa dziedzina informatyki, która dynamicznie się rozwija szczególnie na poziomie teoretycznym. Także na poziomie technologicznym są notowane kolejne niezwykle zaawansowane osiągnięcia. Nie będzie nadużyciem napisanie, iż ten dział informatyki dosłownie rozwija się na naszych oczach.

Choć poziom rozwoju sprzętowych rozwiązań dla komputerów kwantowych nadal nie jest satysfakcjonujący (krótko mówiąc, nie możemy jeszcze kupić komputera kwantowego do domu), dotychczas opracowane algorytmy kwantowe oraz protokoły komunikacji oparte na prawach fizyki kwantowej jednoznacznie pokazały możliwości, jakie tkwią w kwantowym modelu przetwarzania informacji.

Istotnym celem jest także popularyzacja informatyki kwantowej, szczególnie iż jest to dziedzina odwołująca się do dość zaawansowanych pojęć z matematyki oraz fizyki. I właśnie popularyzacja stanowi główny powód napisania tej książki.

Informatyka kwantowa, jak się obecnie sądzi, dostarcza nie tylko nowych algorytmów, ale także oferuje większą moc obliczeniową niż moc obliczeniowa obecnie dostępnych rozwiązań informatycznych.

Pierwsze[1)] maszyny obliczeniowe, które pojawiły się w latach czterdziestych XX w., miały, co naturalne, zastosowania czysto wojskowe. Były stosowane m.in. do łamania szyfru tworzonego za pomocą niemieckiej maszyny szyfrującej Enigma. Nie inaczej jest dzisiaj, choć oprócz utajnionych zastosowań wojskowych, również cywilne zastosowania wymagają wielkich, czy wręcz ogromnych nakładów obliczeniowych. Nie sposób wymienić obszarów wymagających dużych mocy obliczeniowych, choć warto wspomnieć takie zagadnienia jak prognozowanie pogody, badanie struktur molekularnych, co jest szczególnie ważne w kontekście nowych

[1)] Za pierwszy komputer zwykło się uważać maszynę ENIAC, konstruowaną w latach 1943–1945. Jednakże powstały też inne maszyny, jak Z1 oraz Z3, opracowane przez Konrada Zuse, oraz maszyny Colossus oraz ABC zbudowane w Anglii.

materiałów oraz w przypadku nowych lekarstw. Również zadania projektowania, symulacje inżynierskie (np. zderzenia samochodów), także i komputerowa grafika, animacja oraz symulacje stosowane w kinematografii, wymagają użycia systemów komputerowych o bardzo dużej wydajności.

Wymienione zastosowania wykorzystują praktycznie taką samą technologię przetwarzania danych. Technologia ta wykorzystuje fakt, iż bardzo często zadanie główne można podzielić na mniejsze problemy/zadania i wykorzystując wiele jednostek obliczeniowych, pojedynczych procesorów i stacji roboczych połączonych siecią, można rozwiązywać mniejsze zadania w sposób równoległy. W ten sposób uzyskuje się bardzo istotne skrócenie czasu potrzebnego do przeprowadzenia niezbędnych obliczeń. Wspólnym elementem takiego podejścia jest model obliczeniowy. We wszystkich współczesnych rozwiązaniach stosowane jest podejście oparte na tzw. maszynie von Neumanna, która została zaprojektowana w latach czterdziestych XX w. Obecnie poziom doskonałości technologii jest daleko wyższy, jednakże podstawowy model maszyny obliczeniowej, tj. procesor z pamięcią, rejestrami oraz instrukcjami, nadal pozostaje niezmieniony.

W 2015 r., kiedy pisane są te słowa, możemy mówić o powszechności obliczeń równoległych. Większość nowo powstałych programów, czy ogólnie aplikacji, wykorzystuje fakt, iż w większości nowych komputerów użytkowników domowych dostępne są co najmniej dwa rdzenie obliczeniowe. Również urządzenia mobilne, takie jak telefony czy tablety, mają procesory o wielu rdzeniach obliczeniowych. Równoległe przetwarzanie obecne jest również we wszystkich kartach graficznych zarówno dla urządzeń stacjonarnych, jak komputerów czy konsoli do gier, ale także i dla urządzeń mobilnych. Nawet większość modeli kart graficznych średniego segmentu oferuje obecnie wydajność obliczeniową na poziomie 500–1000 gflopsów (miliardy zmiennoprzecinkowych operacji na sekundę) w przypadku stosowania liczb zmiennoprzecinkowych pojedynczej precyzji. Tym czasem wydajność przetwarzania konwencjonalnych procesorów w operacjach na liczbach zmiennoprzecinkowych wynosi około wartości 50–100 gflopsów.

Podstawowy model von Neumanna oraz równoległy schemat przetwarzania danych, w którym wykorzystuje się wiele jednostek obliczeniowych, współdzielą te same podstawowe prawa logiki i algebry Boola. Zasadnicze pytanie, które można postawić w tym kontekście, brzmi następująco, czy możliwe jest wprowadzenie innych modeli obliczeniowych, które charakteryzować się będą znaczącym przyspieszeniem względem obecnie stosowanych rozwiązań sprzętowo-programowych.

Obecnie (2015 r.) wyróżnić można dwa modele przetwarzania informacji. Pierwszy to model oparty na zagadnieniu sekwencjonowania DNA. Drugi zaś jest oparty na teorii kwantowej. W obu przypadkach należy podkreślić, iż są to modele, w których przetwarzanie informacji odbywa się na poziomie fizycznym. Wykorzystywane są podstawowe procesy oraz prawa rządzące w Naturze. W tym kontekście o modelu klasycznym trzeba mówić, iż jest to model abstrakcyjny, gdyż

informacja jest zapisywana za pomocą dwóch sztucznie wyróżnionych stanów, pełniących funkcją zera lub jedynki albo fałszu lub prawdy.

Uważa się, iż nowe modele obliczeniowe przyniosą możliwość rozwiązania problemów wymagających dużych nakładów obliczeniowych. Dotyczy to problemów NP-zupełnych, dla których obecnie znane rozwiązania stosowane na maszynach klasycznych działają w czasie wykładniczym. Nowe modele dają nadzieję, iż będzie można tego typu problemy rozwiązywać w czasie wielomianowym, przy czym oczekuje się, iż będzie to wielomian niskiego stopnia. Jest to szczególnie ważne, gdyż pełne rozwiązanie tylko jednego problemu NP-zupełnego w czasie wielomianowym pozwala także na rozwiązanie wszystkich pozostałych problemów przynależących do grupy problemów NP-zupełnych. Przykładem jest algorytm dla modelu opartego na sekwencjonowaniu DNA, który oferuje rozwiązanie problemu skierowanej ścieżki Hamiltona [2], a także problemu spełnialności funkcji boolowskich [13] oraz systemu odpowiedniości Posta [57] w czasie $O(n)$.

W przypadku modelu kwantowego można również wskazać rozwiązania zadań dla których, jak wykazano, daje się uzyskać znaczące przyspieszenie. Podstawowym przykładem jest algorytm Shora odnoszący się do faktoryzacji liczb całkowitych. Złożoność obliczeniowa tego algorytmu wynosi $O(\mathfrak{L}(n)^3)$, gdzie funkcja $\mathfrak{L}(\cdot)$ wyznacza liczbę cyfr, które są niezbędne do pełnego zapisu faktoryzowanej liczby. Trzeba jednak pamiętać, że algorytm Shora jest algorytmem probabilistycznym. Jednokrotne wykonanie algorytmu nie musi skutkować otrzymaniem poprawnego rozwiązania. W ogólności liczba powtórzeń algorytmu Shora jest ograniczona przez wielkość $O(\log \mathfrak{L}(n))$. Funkcja logarytmiczna potwierdza, że nadal jest to jednak algorytm o złożoności wielomianowej, gdyż powtarzamy logarytmiczną liczbę razy zadanie o rozmiarze wielomianowym. Najlepsze, powszechnie znane algorytmy klasyczne oferują złożoność podwykładniczą.

Próbując tłumaczyć potrzebę wprowadzania nowego kwantowego modelu obliczeniowego, warto przywołać wypowiedź Richarda P. Feynmana, który zwrócił uwagę na fakt, iż współczesne mu komputery[2)] nie oferują dostatecznej mocy

[2)] W 2015 r. stwierdzenie to nadal jest jak najbardziej prawdziwe, gdyż po niemal czterdziestu latach rozwoju technologii informatycznej (od wystąpienia Richarda P. Feynmana) maszyny cyfrowe nadal nie oferują dostatecznej mocy obliczeniowej. Naturalnie, moc ta jest bez porównania większa niż w latach osiemdziesiątych XX w., szczególnie jeśli porównamy wydajność pierwszego superkomputera słynnej firmy Cray. W 1976 r. maszyna ta oferowała moc obliczeniową na poziomie 80 mflops (mflops – milion operacji zmiennoprzecinkowych na sekundę, zazwyczaj są to operacje o podwójnej precyzji). Wielkość ta w stosunkowo krótkim czasie została zwiększona do ok. 136 mflops. Dodatkowo, możliwe było osiągnięcie wartości nawet 250 mflops przy właściwie napisanym programie. Wydajność ówczesnych systemów szybko była poprawiana, bo już w 1982 r. maszyna Cray X-MP oferowała wydajność 800 mflops. Natomiast pierwszą maszynę o wydajności na poziomie 1,9 gflops, Cray-2, pokazano w 1985 r. (dla porównania dzisiejsze procesory do zastosowań domowych oferują wydajność do ok. 50–75 gflops). Procesory w urządzeniach mobilnych również oferują wydajność do ok. 5 gflops, czyli można powiedzieć, iż przysłowiowy telefon komórkowy

obliczeniowej, aby przeprowadzić symulację złożonych procesów fizycznych (ze szczególnym uwzględnieniem procesów kwantowych). W tym miejscu zacytujemy fragment oryginalnej wypowiedzi:

> Can physics be simulated by a universal computer? [...] the physical world is quantum mechanical, and therefore the proper problem is the simulation of quantum physics [...] the full description of quantum mechanics for a large system with R particles [...] has too many variables, it *can not be simulated* with a normal computer with a number of elements proportional to R [...] but it can be simulated with] quantum computer elements. [...] Can a quantum system be probabilistically simulated by a classical (probabilistic, I'd assume) universal computer? [...] If you take the computer to be the classical kind I've described so far [...] the answer is certainly, No!

W tłumaczeniu wykonanym przez autorów książki brzmi ono następująco:

> Czy można symulować fizykę za pomocą (uniwersalnego) komputera? [...] otaczający nas świat jest opisany za pomocą praw mechaniki kwantowej, toteż właściwa byłaby symulacja fizyki kwantowej [...] pełny kwantowo-mechaniczny opis dla dużego systemu o R-cząstkach [...] ma zbyt wiele zmiennych, które *nie mogą być symulowane* za pomocą komputera przy zastosowaniu liczby elementów proporcjonalnej do R [...] ale mogą być symulowane za pomocą komputera kwantowego. [...] Czy można symulować system kwantowy probabilistycznie za pomocą klasycznego (lub probabilistycznego) komputera? [...] Jeśli posługujemy się komputerem, który jest klasyczną maszyną opisaną przeze mnie jak dotychczas [...], odpowiedź jest jasna, Nie!

Fundamentalnym problemem pojawiającym się w przypadku obliczeń kwantowych, a także fizyki kwantowej jest liczba zmiennych, które podlegają przetwarzaniu. W przypadku systemów kwantowych liczba tych zmiennych rośnie wykładniczo. Sytuację pogarsza też fakt, iż w ogólności dodanie nowego elementu do układu podwaja ilość informacji, jaką należy przetworzyć. Dodatkowo, zjawisko splątania kwantowo-mechanicznego skutkuje dalszym zwiększeniem potrzebnej mocy oraz zasobów obliczeniowych podczas symulacji na klasycznym komputerze (w skrócie powoduje ono, iż niezbędne staje się zapamiętanie całości stanu opisującego dany system fizyczny). Pomijamy naturalnie w tym miejscu szczegóły oraz przypadki szczególne, ale stanu splątanego nie można przedstawić w postaci iloczynu tensorowego stanów poszczególnych mniejszych podukładów.

---

to superkomputer z lat osiemdziesiątych XX w. Należy też nadmienić, że wydajność numeryczna lepszych kart graficznych w 2015 r. sięga nawet 4 tflops (teraflops), choć dla liczb o pojedynczej precyzji.

Zarówno na początku lat osiemdziesiątych XX w., jak i dzisiaj w 2015 r., dostępne systemy informatyczne, pomimo ciągłego postępu technologicznego, nie oferują dostatecznej mocy obliczeniowej, by przetwarzać wykładnicze ilości informacji w krótkim czasie. Richard P. Feymann w swej wypowiedzi zwrócił uwagę na bardzo istotne zagadnienie. Aby poznać własności układów opisywanych za pomocą mechaniki kwantowej, najlepiej byłoby symulować ich zachowanie za pomocą systemów kwantowych. Rozwiązania klasyczne, ze względu na ograniczoną moc obliczeniową, nie są wstanie uporać się z tym zadaniem. Innymi słowy, komputer kwantowy nie jest nam potrzebny, aby rozwiązywać problemy klasyczne, choć perspektywa rozwiązywania w czasie wielomianowym problemów NP-zupełnych będzie stanowić rewolucję i krok milowy dla informatyki, lecz główne zadanie dla komputera kwantowego to symulacje różnego typu układów kwantowo-mechanicznych.

Bezpośrednie stosowanie modelu obliczeniowego do projektowania algorytmów czy programów na poziomie języka logiki zarówno w przypadku klasycznych modeli, jak i na poziomie kwantowych superpozycji, jest trudnym i zazwyczaj bardzo żmudnym zadaniem. Dlatego wydaje się niezbędne opracowanie nowych abstrakcyjnych pojęć pozwalających na eksplorację głównych cech danego modelu obliczeniowego, w naszym przypadku modelu kwantowego. Dzisiejszy dynamiczny rozwój informatyki, w tym w szczególności języków programowania, dotyczy przede wszystkim modelu klasycznego. Dla nowych modeli obliczeniowych opracowano kilka różnych sposobów zapisu algorytmów oraz programów, jednakże nadal bardzo popularnym podejściem jest tworzenie obwodów kwantowych na wzór klasycznych obwodów logicznych. Takie podejście nie jest może najwygodniejszym rozwiązaniem, jednakże pozwala na łatwiejsze przeniesienie obwodu kwantowego do etapu jego fizycznej realizacji.

Eksperymenty fizyczne w przypadku obliczeń kwantowych niestety nie wyszły jeszcze poza laboratoria. Dlatego pojawia się konieczność korzystania ze środowiska symulującego nowe modele obliczeniowe za pomocą klasycznych metod obliczeniowych. W ogólności w przypadku korzystania z klasycznych środowisk obliczeniowych model kwantowy wymaga ogromnych, a nieco precyzyjniej, wykładniczych zasobów pamięci i czasu obliczeniowego. Potencjalne środowiska obliczeń kwantowych mogą przechowywać wykładnicze ilości informacji klasycznej, używając tylko liniowej ilości zasobów kwantowych. Dlatego, jak już zostało to już podkreślone, klasyczne maszyny obliczeniowe nie pozwalają na wielkoskalowe symulacje obliczeń kwantowych. Są pewne odstępstwa, np. tzw. obwody CHP. Jednak w ogólności, nie możemy ze względu na ograniczone zasoby maszyn klasycznych przeprowadzać pełnej symulacji maszyny kwantowej zawierającej np.: kilka tysięcy kubitów (kubit – jednostka informacji kwantowej). Niemniej, proces symulacji małych układów kwantowych jest jak najbardziej możliwy i pozwala na eksplorację wszystkich aspektów kwantowego modelu obliczeniowego.

Organizacja książki

Książka ta to pozycja z pogranicza trzech obszarów: informatyki, fizyki oraz matematyki. Naturalnie polecamy, aby czytać ją po kolei, od pierwszego do ostatniego rozdziału. Jednakże, jak wiele innych pozycji dotyczących informatyki czy też książki z obszaru matematyki lub fizyki, zawarty materiał można czytać w wybranej przez siebie kolejności. Szczególnie początkującemu Czytelnikowi sugerujemy jednak lekturę pierwszych podrozdziałów, które prezentują wybrane zagadnienia matematyczne stanowiące bazę pojęć i definicji niezbędnych, aby lepiej zrozumieć podstawy informatyki kwantowej, która jak można wierzyć, będzie technologią przyszłości i dostarczy nam zupełnie nowe technologie obliczeniowe.

Informatyka kwantowa, albo inaczej obliczenia kwantowe, to obecnie dziedzina o charakterze mocno matematycznym, dlatego szczególnie początkujące osoby zachęcamy do lektury rozdziału pierwszego, w którym znajdują się podstawowe pojęcia odnoszące się do liczb zespolonych, przestrzeni wektorowej oraz operacji na wektorach i macierzach, a ogólnie do algebry liniowej. Wymienione tam pojęcia pozwolą już swobodnie testować obwody kwantowe, bowiem weryfikacja np. protokołu teleportacji kwantowej wykonywana na przysłowiowej kartce z zeszytu sprowadza się do mnożenia wektora przez macierz. Istotne pojęcie to również iloczyn tensorowy, jednakże ograniczamy się tylko do najbardziej podstawowych definicji.

W rozdziale pierwszym opisujemy także podstawy notacji Diraca, która szeroko jest stosowana w fizyce kwantowej, a także w dziedzinie obliczeń kwantowych. Ważny jest także podrozdział 1.5, gdzie prezentujemy pojęcia związane z operatorami. Prezentacja zagadnień z algebry liniowej jest ograniczona do najważniejszych dla nas pojęć, dlatego Czytelników, którzy chcieliby pogłębić swoją wiedzę w tym zakresie, zachęcamy do sięgnięcia po dedykowane pozycje z tej dziedziny matematyki.

Charakter wprowadzenia ma także rozdział drugi, w którym przedstawiamy podstawowe pojęcia informatyki kwantowej. Określamy podstawową jednostkę kwantową, tj. kubit, oraz konstrukcję rejestru kwantowego. Określamy także dodatkowe operacje, które wykonuje się w trakcie analizy rejestru kwantowego, tj. ślad częściowy oraz częściową transpozycję.

Sporo miejsca zajmuje omówienie rodzaju operacji wykonywanych na rejestrze kwantowym, tj. operacji unitarnych oraz pomiarów. Wskazujemy także operacje, których nie można wykonać w ramach informatyki kwantowej, oraz własność splątania, która jak się wydaje, jest fundamentalna dla obliczeń kwantowych i stanowi np. główną własność wykorzystywaną w realizacji protokołu teleportacji kwantowej.