Informatyka Kwantowa
Sekcja Informatyki Kwantowej – prezentacja

Robert Nowotniak
Wydział FTIMS, Politechnika Łódzka

XV konferencja SIS, 26 października 2007

Streszczenie

Informatyka kwantowa jest dziedziną z pogranicza informatyki i mechaniki kwantowej. W niniejszym referacie zostaną przedstawione podstawowe informacje dotyczące tej dziedziny oraz zainteresowania naukowe *Sekcji Informatyki Kwantowej* – jednej spośród trzech sekcji Koła Naukowego Informatyki na wydziale FTIMS Politechniki Łódzkiej.

Treść referatu

Informatyka kwantowa zajmuje się wykorzystaniem możliwości obliczeniowych układów, podlegających prawom *mechaniki kwantowej*. Od pewnego czasu stało się jasne, iż istnieje pewna klasa problemów, które mogą być rozwiązywane w sposób znacznie bardziej efektywny, dzięki wykorzystaniu możliwości obliczeniowych takich układów. Sztandarowe problemy należące do tej klasy to faktoryzacja liczb oraz przeszukiwanie nieposortowanego zbioru. Oprócz zadań algorytmicznych, rozpatruje się także możliwość wykorzystania układów, podlegających prawom mechaniki kwantowej, m.in. w teorii informacji (protokół teleportacji kwantowej [4], kodowanie supergęste) i w teorii gier [5, 6].

Podstawowymi obiektami w informatyce kwantowej są *kubity* oraz *rejestry kwantowe*. W niniejszym referacie zostaną pominięte kwestie związane z aparatem matematycznym. W sposób formalny zdefiniujmy jedynie, czym jest kubit, podstawowa jednostka informacji kwantowej:

$$|\psi\rangle = \alpha|0\rangle \ + \beta|1\rangle$$

$$\text{gdzie } \alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1$$

Kubit to wektor znormalizowany w dwuwymiarowej, zespolonej przestrzeni Hilberta. Współrzędne takiego wektora określają prawdopodobieństwo otrzymania jednego ze stanów bazowych po wykonaniu odczytu stanu kubitu. Kubity pozwalają zatem przechowywać *superpozycję* stanów bazowych $|0\rangle$ i $|1\rangle$.

Układ wielu kubitów tworzy tzw. *rejestr kwantowy*. Jedną ze szczególnych własności informatyki kwantowej jest fakt, iż wraz z liniowym wzrostem liczby kubitów w rejestrze kwantowym, rośnie w tempie wykładniczym wymiar przestrzeni stanów takiego rejestru.

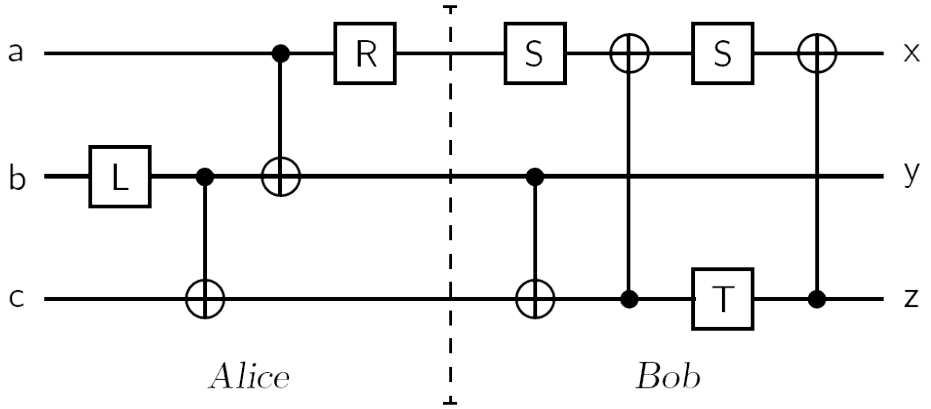
Sekcja Informatyki Kwantowej zajmuje się szczególnie kilkoma zagadnieniami. Pierwszym z nich jest algorytmika kwantowa – to zagadnienie będzie dalej przedstawione bardziej szczegółowo. Zajmujemy się także symulacją obliczeń kwantowych, w szczególności modelem kwantowych bramek logicznych, a także językami programowania kwantowego (jak QCL lub biblioteka libquantum). Potrafimy symulować pracę komputera kwantowego w środowisku do obliczeń numerycznych, jak Matlab lub Python wraz z biblioteką NumPy. Interesujemy się również połączeniem metod sztucznej inteligencji i informatyki kwantowej. Istnieją tutaj dwa podejścia – wykorzystanie metod sztucznej inteligencji w projektowaniu elementów algorytmów kwantowych oraz rozwój metod sztucznej inteligencji, które czerpałyby z możliwości informatyki kwantowej.

Jak dotąd odkryto jedynie kilka przydatnych algorytmów kwantowych. Najpopularniejsze to: algorytm Grovera, algorytm Shora, algorytm Deutscha-Jozsy. Algorytm Grovera pozwala na wyszukiwanie elementu w nieposortowanej bazie danych ze złożonością $O(\sqrt{N})$. Najlepszy klasyczny algorytm realizuje to zadanie ze złożonością $O(N)$. Algorytm Shora pozwala na faktoryzację liczb ze złożonością mniejszą niż wykładnicza — $O(log^3 N)$. Jak dotąd nie został znaleziony algorytm klasyczny o tej własności i przypuszcza się, że taki algorytm nie istnieje. Pozostałe algorytmy kwantowe służą do rozwiązania nieco mniej praktycznych problemów.

Tworzenie algorytmów kwantowych jest zadaniem trudnym z kilku względów. Istnieje bardzo słaba analogia do algorytmów klasycznych, z powodu wykorzystania efektów mechaniki kwantowej. Są to algorytmy probabilistyczne, czyli oparte na prawdopodobieństwie. Podstawowym klasom złożoności, jak P, NP, BPP odpowiadają – w przypadku obliczeń kwantowych – odpowiednio klasy: EQP, NQP oraz BQP. Algorytmy kwantowe wykorzystują

nieintuicyjne własności mechaniki kwantowej, takie jak superpozycja stanów, interferencja amplitud prawdopodobieństwa (będących liczbami zespolonymi), kwantowe splątanie i paralelizm.

Jednym z formalnych modeli obliczeń kwantowych są *układy kwantowych bramek logicznych*. Równoważnym – ale mniej praktycznym – formalnym modelem obliczeń kwantowych jest Kwantowa Maszyna Turinga, którą jak dotąd nie była przedmiotem zainteresowań Sekcji.

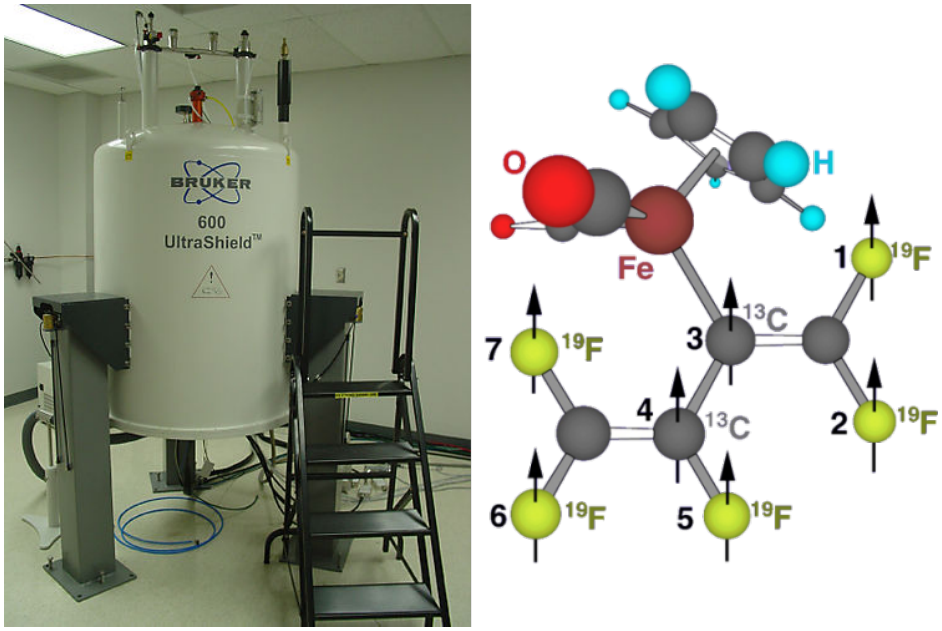


Rysunek 1: Układ kwantowych bramek logicznych

Rysunek 1 przestawia przykładowy schemat kwantowych bramek logicznych. Symulacja działania takiego układu polega na wykonywaniu operacji na macierzach unitarnych, związanych z poszczególnymi bramkami. Podstawową zasadą jest to, że połączenie równoległe bramek odpowiada iloczynowi tensorowemu ich macierzy, natomiast macierz całego układu jest – w tym najprostszym przypadku – iloczynem macierzy poszczególnych etapów obliczeń.

Powyższy przykładowy układ realizuje protokół teleportacji kwantowej, czyli przesłanie nieznanego stanu kubitu z wykorzystaniem splątanej pary w konfiguracji Einsteina-Podolskiego-Rosena [4].

Tak jak to było zaznaczone wcześniej, projektowanie algorytmów kwantowych – a więc tworzenie odpowiednich układów bramek – które wykonywałyby jakąś pożądaną operację, jest zadaniem trudnym z powodu nieintuicyjnych własności mechaniki kwantowej. Okazuje sie jednak, że – w pewnym stopniu – elementy algorytmów kwantowych można projektować automatycznie z wykorzystaniem metod sztucznej inteligencji. Umiejętność symulacji działania bramek kwantowych pozwala na projektowanie takich układów np. za pomocą algorytmów genetycznych lub programowania genetycznego ([8, 9]). O skuteczności takiego podejścia świadczy fakt, iż za pomocą tej metody



Rysunek 2: Magnetyczny rezonans jądrowy

było możliwe znalezienie prostszego układu realizującego protokół teleportacji kwantowej niż równoważny układ zaprojektowany przez człowieka ([7, 4]).

Istnieje obecnie wiele ścieżek, dających nadzieję na fizyczną realizację *skalowalnego*[1] komputera kwantowego. Do jego zbudowania niezbędny jest dowolny układ fizyczny, pozwalający utrzymywać „delikatny" stan *koherencji kwantowej*. Zjawiska fizyczne, oferujące taką własność to m.in.: magnetyczny rezonans jądrowy, stany energetyczne elektronów na powłokach elektronowych, polaryzacja światła, kropki kwantowe, pułapki jonowe.

Dużo badań poświęcono jak dotąd zwłaszcza wykorzystaniu magnetycznego rezonansu jądrowego (ang. *Nuclear Magnetic Resonance*). Rysunek 2 przestawia spektrometr NMR[2], oraz cząsteczkę składającą się z atomów posiadających wewnętrzny moment magnetyczny czyli tzw. spin.

Spiny magnetyczne tej cząsteczki mogą być traktowane jako wektory bazowe w przestrzeni stanów rejestru kwantowego i mogą być ustawiane za pomocą zewnętrznego pola elektromagnetycznego. Natomiast odczyt wyników jest realizowany poprzez badanie widma przy pomocy spektrometru.

[1] trudność stanowią obecnie problemy, pojawiające się wraz z przekraczaniem pewnej – aktualnie niewielkiej – liczby kubitów w rejestrze

[2] podobne urządzenie, Brüker 700, stanowi wyposażenie Instytutu Chemii Organicznej Wydziału Chemicznego Politechniki Łódzkiej

W roku 2001 w laboratoriach IBM, wykorzystując tę technikę, zbudowano pierwszy prymitywny, siedmiokubitowy, komputer kwantowy, który był w stanie wykonywać algorytm Shora.

Literatura

[1] Materiały z referatów na spotkaniach Sekcji Informatyki Kwantowej, 2006–2007

[2] Michael A. Nielsen, Isaac L. Chuang. *Quantum Computation and Quantum Information*, 2000

[3] Mika Hirvensalo. *Algorytmy Kwantowe*, 2004

[4] Gilles Brassard. *Teleportation as a quantum computation*, 1996

[5] Johann Summhammer. *Quantum Cooperation of Two Insects*, 2006

[6] Gleb V. Klimovitch. *How Quantum Entanglement Helps to Coordinate Non-Communicating Players*, 2004

[7] Taro Yabuki, Hitoshi Iba. *Genetic Algorithms for Quantum Circuit Design - Evolving a Simpler Teleportation Circuit*

[8] Gilson A. Giraldi, Renato Portugal, Ricardo N. Thess *Genetic Algorithms and Quantum Computation*

[9] B.I.P. Rubinstein. *Evolving Quantum Circuits using Genetic Programming*

[10] + wiele innych źródeł