STUDIA INFORMATICA 2002
Volume 23 Number 2A (48)

Sławomir BUGAJSKI, Jarosław A. MISZCZAK
Instytut Informatyki Teoretycznej i Stosowanej PAN
Uniwersytet Śląski, Instytut Fizyki
Zbigniew MOTYKA
Główny Instytut Górnictwa, Katowice

SYMULACJE OPTYCZNE OBLICZEŃ KWANTOWYCH[1]

Streszczenie. W artykule zaprezentowane są podstawy obliczeń kwantowych. Odpowiedniość pomiędzy macierzami unitarnymi a ciągami elementów optycznych pozwala na zademonstrowanie kilku prostych kwantowych bramek logicznych. Przedstawiona jest symulacja optyczna algorytmu Grovera szybkiego wyszukiwania.

OPTICAL SIMULATIONS OF QUANTUM COMPUTING

Summary. The fundamentals of quantum computation are presented. Correspondence between unitary matrices and sequences of optical elements permits to demonstrate some simple quantum logic gates. Optical simulation of the Grover algorithm for fast searching is presented.

1. Obliczenia kwantowe

Ewolucja układu kwantowego może być opisana w języku operatorów unitarnych działających na przestrzeni Hilberta. Operator U nazywamy unitarnym, jeżeli jest on liniowym, bijektywnym odwzorowaniem zachowującym długość każdego wektora. Stan układu opisany jest przez wektor $|\Psi(t)\rangle$ w przestrzeni Hilberta $\mathcal{H}$ nad ciałem liczb zespolonych.

$$|\Psi(t)\rangle = \sum_{x\in\{0,1\}^m} \alpha_x(t)|x_1 \ldots x_m\rangle \tag{1}$$

[1] Praca wykonana w ramach projektu KBN nr 7 T11C 017 21.

Tutaj wymiar przestrzeni Hilberta $\dim\mathcal{H}=2^m$, stan $|\Psi(t)\rangle$ jest kombinacją liniową iloczynów tensorowych wektorów (stanów) bazowych w przestrzeniach reprezentujących podukłady. Przyjęliśmy, iż $\mathcal{H}$ jest iloczynem tensorowym m przestrzeni 2-wymiarowych. Takie składowe przestrzenie odpowiadają układom o dwóch stopniach swobody. Wybrane w nich wektory bazy – oznaczane zwykle przez $|0\rangle$ i $|1\rangle$ – odpowiadają klasycznym wartościom logicznym 0 i 1, natomiast wszystkie kombinacje liniowe nie mają swoich klasycznych odpowiedników.

Jeśli stan początkowy układu jest $|\Psi(0)\rangle$, a ewolucja opisana jest przez operator $U(t)$, wówczas

$$|\Psi(t)\rangle = U(t)|\Psi(0)\rangle \tag{2}$$

Komputer kwantowy to wyspecjalizowany układ kwantowy. Praktyczna definicja może brzmieć następująco: *komputer kwantowy to system fizyczny, którego ewolucja jest unitarna.* Nasze zadanie polega jedynie na wejściu w odpowiednią interakcję z takim układem. Problem w tym, że świat nie ewoluuje w sposób unitarny i trudno jest zmusić pewną jego część, by poddała się takiej ewolucji. Z drugiej strony naszym celem jest zwykle wykonanie jakiegoś określonego zadania (np. znalezienia rozkładu liczby całkowitej na czynniki pierwsze) i w związku z tym ewolucja układu musi być podporządkowana osiągnięciu tego celu. Dlatego też musimy zrozumieć efekty kluczowe dla obliczeń kwantowych i nauczyć się wykorzystywać je w konstrukcji algorytmów kwantowych.

Obliczenia wykonywane przez komputer kwantowy mogą być przedstawione za pomocą ciągu macierzy unitarnych. Model taki – znany jako obwód kwantowy (ang. *quantum gate array*) – został zaproponowany przez Deutscha w [1]. Program dla takiego obwodu jest wbudowany w jego strukturę. W zależności od tego, co chcemy obliczyć, musimy użyć różnych obwodów. Możliwe jest również zabudowanie programowalnych obwodów kwantowych [2], które wykonywałyby obliczenia (operacje na danych) w zależności od programu (zawartości pewnych rejestrów kwantowych).

Obwody kwantowe pozwalają nam na analizę struktury algorytmów kwantowych – odgrywają one rolę podobną do schematów blokowych przy analizie algorytmów klasycznych. Każdy algorytm kwantowy może być rozłożony na sekwencje operacji elementarnych – kwantowych bramek logicznych.

2. Elementarne bramki kwantowe

Kwantowe bramki logiczne spełniają taką samą role w teorii obliczeń kwantowych jak klasyczne bramki w informatyce klasycznej. Najciekawsze są jednak różnice.

Ponieważ ewolucja układu kwantowego jest unitarna, możemy zawsze ją odwrócić. Jeżeli macierz U jest unitarna, to spełnia ona relacje $U^+U = UU^+ = 1$, czyli możemy wyliczyć macierz (operator) do niej odwrotną $U^{-1} = U^+$. Operator U^+ opisuje ewolucję wstecz. Analogicznie do wzoru (2) możemy zapisać

$$|\Psi(0)\rangle = U^+(t)|\Psi(t)\rangle \tag{3}$$

Zatem kwantowe bramki logiczne są odwracalne i obliczenia kwantowe są odwracalne.

Jak pokazano w [3], każdy zbiór bramek kwantowych zawierający wszystkie bramki jednoqubitowe oraz dwuqubitową operację XOR przeprowadzającą (x, y) w $(x, x \oplus y)$ jest wystarczający do konstrukcji wszystkich operacji unitarnych na dowolnej liczbie qubitów. Okazuje się, iż niemal każda dwuqubitowa lub n-qubitowa bramka kwantowa jest uniwersalna dla obliczeń kwantowych [4], [5]. Zatem wybór uniwersalnego zestawu bramek kwantowych jest o wiele szerszy niż w przypadku klasycznym.

Istnieje nieskończenie wiele bramek kwantowych działających na jednym qubicie, podczas gdy są tylko dwie bramki logiczne działające na jednym bicie. Najprostszą bramką jest operator jednostkowy. Nie powoduje on żadnej zmiany stanów układu kwantowego, ale okazuje się, iż odgrywa on ważną rolę dla układów wieloqubitowych [6]. Odpowiednikiem klasycznej bramki NOT jest operator

$$U_{NOT} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{4}$$

Jego działanie na układzie jednoqubitowym sprowadza się do zamiany stanów bazowych $\{|0\rangle, |1\rangle\}$ układu. Wszystkie pozostałe bramki kwantowe przeprowadzają te wektory w ich kombinacje.

Bramka Hadamarda ma w tej bazie postać

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{5}$$

Transformuje ona wektory bazowe w następujący sposób

$$H|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right), \qquad H|1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) \tag{6}$$

Bramka ta jest transformacją Fouriera na grupie Z_2 [7] i odgrywa kluczową rolę w wielu algorytmach kwantowych. Okazuje się, że szybkie wykonywanie transformaty Fouriera stanowi jedną z najważniejszych cech komputerów kwantowych.

Kolejną ważną operacją kwantową jest bramka $\sqrt{\text{NOT}}$. Spełnia ona warunek $\sqrt{\text{NOT}}\sqrt{\text{NOT}} = \text{NOT}$. W standardowej bazie reprezentuje ją macierz

$$U_{\sqrt{\text{NOT}}} = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \tag{7}$$

Kwantowa bramka zmiany fazy (ang. *quantum phase shift gate*) ma postać

$$U_{\text{Ph}}(\phi) = \frac{1}{\sqrt{2}} \begin{pmatrix} e^{i\phi} & 0 \\ 0 & e^{i\phi} \end{pmatrix} \tag{8}$$

Jej działanie polega na przemnożeniu stanu przez czynnik fazowy $e^{i\phi}$.

Ponieważ wiele cech wyróżniających algorytmy kwantowe ma swoje źródło w działaniach na kwantowych układach złożonych, konieczne się staje wprowadzenie operacji działających na większej liczbie qubitów. W szczególności bramki dwuqubitowe pozwalają nam na skonstruowanie dowolnej operacji n-qubitowej.

Bramka CNOT (kontrolowana bramka NOT) jest reprezentowana w bazie kanonicznej $\{|00\rangle,|01\rangle,|10\rangle,|11\rangle\}$ przez macierz

$$U_{\text{CNOT}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{9}$$

Jeżeli qubit pierwszego podukładu jest w stanie $|1\rangle$, CNOT dokonuje operacji NOT na drugim podukładzie, a jeżeli pierwszy podukład znajduje się w stanie $|0\rangle$, CNOT pozostawia drugi podukład w niezmienionym stanie. Zatem stan drugiego qubitu (ang. *target qubit*) jest kontrolowany przez stan pierwszego qubitu (ang. *controlled qubit*).

Bramka CNOT może wpływać także na stan qubitu kontrolnego – jest to jedna z cech odróżniających ją od bramek klasycznych. Pozwala ona na wprowadzenie nowych efektów do obwodów kwantowych.

3. Elementy optyczne jako bramki kwantowe

Można pokazać, iż każda operacja unitarna na przestrzeni skończenie wymiarowej może być laboratoryjnie odtworzona za pomocą standardowych elementów optycznych [8], [9] – luster, lustrer półprzepuszczalnych oraz płytek opóźniających. Ta odpowiedniość pozwala na demonstrację (symulację) działania kwantowych bramek logicznych. Jeżeli znamy postać algorytmu kwantowego, to możemy przedstawić go w postaci tablicy bramek kwantowych, którą możemy symulować za pomocą optyki liniowej. Procedura ta jest podobna do procesu translacji z jednego języka na inny – tutaj tłumaczymy z języka operacji unitarnych na język elementów optycznych.

Qubity są reprezentowane poprzez zmienną określającą, którą drogę w układzie optycznym wybierze foton. Do wyboru są dwie możliwości – ścieżka góra-dół i ścieżka lewo-prawo. Mówimy, że foton jest w jednym z tych modów przestrzennych (ang. *spatial mode*).

Dodatkowym stopniem swobody, jaki możemy wykorzystać, jest polaryzacja fali. W ten sposób zyskujemy dodatkowy qubit oraz zmniejszamy rozmiary aparatury. Zwiększa się jednak równocześnie złożoność apartaury.

4. Algorytm Grovera i jego implementacja

Wzorując się na pracy [10] przedstawimy tutaj realizację optyczną algorytmu Grovera szybkiego wyszukiwania w bazie danych. Szczegółową prezentację samego algorytmu można znaleźć w pracach [11] i [12]. Rozpatrzymy przypadek wyszukiwania w bazie danych złożonej z czterech elementów i przedstawimy symulację optyczną.

Przypuśćmy, że mamy zbiór N nieposortowanych elementów (np. liczb całkowitych) i tylko jeden z nich spełnia określony warunek[2] (np. jest to liczba pierwsza). Naszym zadaniem jest znaleźć ten wyróżniony element. Klasyczny algorytm musi sprawdzić $O(N)$ elementów, aby odszukać zaznaczony. Algorytm Grovera rozwiązuje zadanie wykonując średnio $\frac{\pi}{8}\sqrt{N}$ sprawdzeń. W przypadku $N=4$ wystarczy jedna iteracja, aby można było uzyskać odpowiedź.

Rozpatrzmy układ stanowiący optyczną implementację algorytmu Grovera dla $n=2$ bitów, z których jeden reprezentowany jest przez polaryzację, a drugi przez mod przestrzenny (rys.1). Na początek na każdym z dwóch bitów oddzielnie realizowana jest transformacja Hadamarda H mająca na celu przygotowanie superpozycji wszystkich czterech elementów bazy:

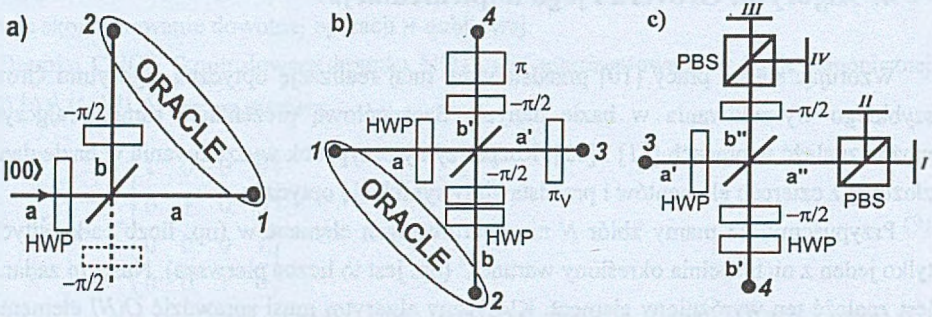
$$H \otimes H|00\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \tag{10}$$

Pierwsza cyfra w każdym wektorze stanu oznacza mod przestrzenny (0 – w prawo, 1 – do góry), a druga polaryzację (0 – pozioma, 1 – pionowa). Dla ułatwienia pominiemy stuprocentowe zwierciadła kierujące, gdyż możemy przyjąć, że nie zmieniają one symetrii układu (odbicie układu z rys.1b względem osi symetrii, wyznaczonej przez centralny dzielnik wiązki, pozwala na sklejenie wszystkich trzech rysunków poprzez umieszczenie luster kierujących w punktach oznaczonych tą samą cyfrą, odpowiednio 1, 2, 3 lub 4). Możemy

[2] Algorytm Grovera może być uogólniony na przypadek, gdy więcej niż jeden element spełnia zadany warunek.

zatem przyjąć, że foton poruszający się pomiędzy pierwszym dzielnikiem wiązki z rys.1a i drugim z rys.1b nie zmienia swego stanu (także modu przestrzennego) pomimo konieczności odbicia go zarówno po drodze a, jak i b przez zwierciadła kierujące pod kątem prostym w kierunku drugiego z dzielników wiązki. Podobnie rzecz się ma z przejściem od rys.1b) do rys.1c), gdzie kolejne dwa lustra kierujące oznaczone zostały numerami 3 i 4.

Fizycznie powyższej operacji na bicie polaryzacji dokonuje półfalówka ustawiona pod kątem 22,5° w stosunku do płaszczyzny poziomej, co powoduje skręcenie płaszczyzny polaryzacji fotonu z poziomej do 45°, w taki sposób, że z równym prawdopodobieństwem może on przejść przez filtr polaryzacyjny ustawiony poziomo, jak i pionowo.



Rys. 1. Kolejne etapy optycznej implementacji algorytmu Grovera dla n=2 bitów, z których jeden reprezentowany jest przez polaryzację, a drugi przez mod przestrzenny: a) przygotowanie superpozycji stanów; b) przesunięcie w fazie o π dla wszystkich elementów poza pierwszym; c) końcowe transformacje H z odczytem na detektorach I-IV bezpośrednio za polaryzacyjnymi dzielnikami wiązki (PBS). Wszystkie półfalówki (HWP) są ustawione pod kątem 22,5°

Fig. 1. The sequential stages of an optical implementation of Grover's algorithm for n=2 bits, one of which is represented by polarisation and the other by the spatial mode: a) the preparation of the superposition of states; b) π – phase shift for all but the first elements; c) the final H transformations with the readouts at the detectors I-IV immediately after PBSs. All the HWPs are at 22.5°

Układ oznaczony przez **ORACLE** zaznacza jeden z elementów bazy, wprowadzając przesunięcie fazy o π, a tym samym powodując zmianę znaku danego elementu, pozostałe pozostawiając bez zmian. Dla naszych celów wystarczy przyjąć, że układ ten stanowi półfalówka umieszczana czy to na drodze a, czy też na drodze b, która zależnie od swojej orientacji wprowadza przesunięcie fazy dla fotonu o polaryzacji pionowej albo poziomej. Jeśli, dla przykładu, za pomocą półfalówki umieszczonej na drodze b zaznaczony zostaje trzeci element, układ w superpozycji (10) przechodzi do stanu $\frac{1}{2}(|00\rangle+|01\rangle-|10\rangle+|11\rangle)$.

Następnie wykonywana jest powtórna transformacja H na każdym bicie. Dla bitu polaryzacji realizowane jest to za pomocą dwóch oddzielnych półfalówek umieszczonych odpowiednio na drodze a i b. Bit przestrzenny poddawany jest tej transformacji poprzez rekombinację obu dróg na kolejnym lustrze półprzepuszczalnym wraz ze związanymi z nim płytkami opóźniającymi dokonującymi przesunięcia w fazie o $-\frac{\pi}{2}$ (rys.1b).

Z kolei wprowadzane jest przesunięcie fazowe π do wszystkich poza pierwszym elementem bazy. Uzyskujemy to poprzez użycie płytki wykonanej ze szkła niedwójłomnego i powodującej przesunięcie fazy o π, umieszczonej na drodze b' (co odpowiada prostemu wydłużeniu drogi optycznej b' o $\frac{\lambda}{2}$) oraz przez umieszczenie półfalówki oznaczonej π_v na drodze a', z szybką osią zorientowaną poziomo. Poziomo spolaryzowany foton przechodzi przez nią bez zmiany polaryzacji, a polaryzacja spolaryzowanego pionowo ulega obrotowi o kąt π.

Następnie na każdym bicie realizowana jest transformacja H poprzez kolejne dwie płytki półfalowe i trzecie lustro półprzepuszczalne (rys.1c).

Trzy ostatnie omówione operacje dokonują transferu części (w tym wypadku praktycznie całości) amplitudy z elementów nie wyróżnionych do elementu zaznaczonego przez układ ORACLE. Na koniec każdy z możliwych rezultatów sprawdzany jest przez 4 detektory umieszczone za dwoma polaryzacyjnymi kostkami światłodzielącymi (rys.1c). W naszym przykładzie (przy zaznaczeniu trzeciego elementu układem Oracle) niemal wszystkie odczyty uzyskiwane są na detektorze *III*, co potwierdza skuteczność implementacji algorytmu Grovera.

5. Perspektywy

Ze względu na wykładniczy wzrost komplikacji aparatury wykorzystywanej przy symulacjach optycznych komputerów kwantowych nie jest możliwe stosowanie tej techniki do symulowania układów operujących na dużej ilości danych (qubitów). Złożoność „komputerów optycznych" opartych na optyce liniowej stoi też w sprzeczności z jednym z założeń teorii informatyki kwantowej. Postulat ten wymaga, by dla uzyskania wykładniczych efektów obliczeniowych wykorzystywać liniowy wzrost zasobów energetycznych.

Jest to jednakże interesująca propozycja obrazowania efektów kwantowych kryjących się w algorytmach kwantowych. Jej znaczenie praktyczne polega na laboratoryjnym sprawdzeniu działania algorytmów kwantowych oraz na demonstracji w skali makroskopowej pewnych

typowo kwantowych cech obliczeń kwantowych (splątania, teleportacji itp.). Istnieje również możliwość stosowania optycznych realizacji bramek kwantowych w układach automatyki.

LITERATURA

1. Deutsch D.: Quantum Computational Networks. Proc. Soc. Roy. Lond. Vol. A 425, 73 (1989).
2. Nielsen M. A., Chuang I. L.: Programmable quantum gate arrays. http://xxx.lanl.gov/abs/quant-ph/9703032.
3. Barenco A., Bennet C. H., Cleve R., DiVicenzo D. P., Margolus N., Shor P., Sleator T., Smolin J., Weinfurter H.: Elementary gates for Quantum Computation. Phys. Rev. A Vol. 52, 3457 (1995), http://xxx.lanl.gov/abs/quant-ph/9503016.
4. Barenco A.: A Universal Two-Bit Gate for Quantum Computation. Proc. Soc. Roy. Lond. http://xxx.lanl.gov/abs/quant-ph/9505016.
5. Lloyd S.: Almost any Quantum Logic Gate is Universal. Phys. Rev. Lett. Vol. 75, 346 (1995).
6. Jozsa R.: Quantum Effects in Algorithms, http:// xxx.lanl.gov /abs/quant-ph/9805086
7. Cerf N. J., Adami C., Kwiat P. G.: Optical Simulations of Quantum Logic, Phys. Rev. A 57, R1477 (1998).
8. Adami C., Cerf N. J.: Quantum Computation with Linear Optics, Lecture Notes in Computer Science, (Springer-Verlag, 1998), in press. (Special issue for 1st NASA Workshop on Quantum Computation and Quantum Communication QCQC 98). http://xxx.lanl.gov/abs/quant-ph/9806048
9. Yurke B.,McCall S. L., Klauder J. R.: SU(2) and SU(1,1) interferometers, Phys. Rev. A Vol. 36, 4033 (1986)
10. Kwiat P.G., Mitchell J.R., Schwindt P.D.D., White A.G.: Grover's search algorithm: an optical approach, A.G. White, J. Mod. Optics Vol. 47, 257 (2000).
11. http://xxx.lanl.gov/abs/quant-ph/9905086
12. Grover L. K.: Quantum Mechanics Helps in Searching for a Needle in a Haystack, Phys. Rev. Lett. Vol. 79, 325, (1997), http://xxx.lanl.gov/abs/quant-ph/9706033
13. Jozsa R.: Searching in Grover's Search Algorithm, http://xxx.lanl.gov/abs/quant-ph/9701021

Recenzent: Prof. dr hab. inż. Jerzy Klamka

Wpłynęło do Redakcji 18 marca 2002 r.

Abstract

Article presents fundamental concepts of quantum information processing. Some basic quantum logic gates commonly used in quantum algorithms are introduces. Also rules of construction of these gates with standard optical elements are presented. One of the quantum algorithms – Grover's search algorithm – is discussed and its simulation is presented. We also present outcomes of experiment – proposed by Kwiat *et. al* in [10] – with set-up for database searching.

Although optical elements allow simulating some simple quantum gates, complexity of the apparatus seems to limit the applicability of this technique.