Obliczenia inspirowane Naturą

Wykład 12 - Algorytmy i protokoły kwantowe

Jarosław Miszczak

IITiS PAN Gliwice

19/05/2016

Na poprzednim wykładzie

1. Motywacja rozwoju informatyki kwantowej.
2. Stany kwantowe.
3. Notacja Diraca.
4. Obwody kwantowe.

1. Obliczenia odwracalne
   - Zasada Landauera
   - Obwody odwracalne
2. Algorytmy kwantowe
   - Algorytm Deutscha-Jozsy
   - Algorytm Grovera
3. Protokoły kwantowe
   - Teleportacja
   - Gęste kodowanie

Zasada Landauera

- Jeżeli nie dochodzi do wymazywania informacji, to proces obliczeniowy może być zrealizowany w sposób odwracalny termodynamicznie.
- W takim procesie nie jest wydzielane ciepło.

Zasada Landauera

- Rolf Landauer, 1961 – sformułowanie teoretycznego ograniczenia na minimalną energochłonność obliczeń.
- 2012 – pomiar zmiany wydzielania ciepła przy procesie wymazywania informacji. (A. Bérut, A. Arakelyan, A. Petrosyan, S. Ciliberto, R. Dillenschneider, E. Lutz, *Experimental verification of Landauer's principle linking information and thermodynamics*, Nature 483 (7388): 187–190, (2012))

Zasada Landauera

Zasada Landauera

Każdy nieodwracalnej manipulacji informacją o układzie (np. wymazanie bitu) towarzyszy wzrost entropii.

Do wymazania jednego bitu informacji potrzebna jest co najmniej energia $kT \ln 2$. Daje to 2.75×10^{-24} J w temperaturze pokojowej.

Obwody odwracalne

- Charles Bennett, 1973 – uniwersalna maszyna Turinga może być zrealizowana w sposób odwracalny.
  (C. H. Bennett, *Logical reversibility of computation*, IBM Journal of Research and Development, vol. 17, no. 6, pp. 525-532 (1973).)

Obwody odwracalne

Przykłady bramek uniwersalnych dla klasycznych obliczeń

- Bramka Fredkina (kontrolowany SWAP)
- Bramka Toffoliego (podwójnie kontrlowany NOT)

Bramki te są **trójbitowe**.

CNOT

W przypadku obliczeń kwantowych do konstrukcji zbioru zupełnego wystarczy dwukubitwa bramka CNOT.

Obwody odwracalne

RESEARCH ARTICLE

QUANTUM MECHANICS

A quantum Fredkin gate

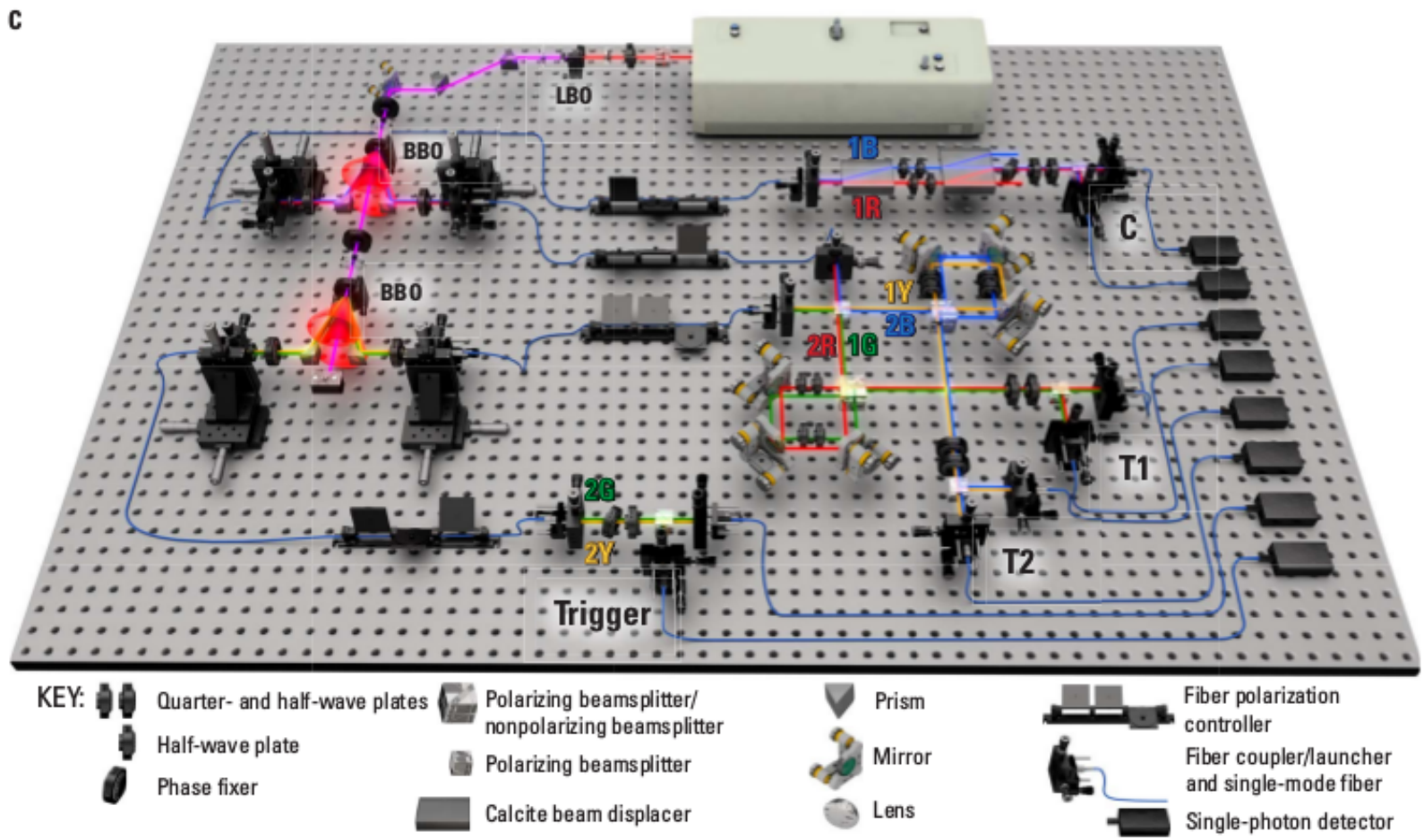
Raj B. Patel,[1]* Joseph Ho,[1] Franck Ferreyrol,[1,2] Timothy C. Ralph,[3] Geoff J. Pryde[1]*

10.1126/sciadv.1501531

Minimizing the resources required to build logic gates into useful processing circuits is key to realizing quantum computers. Although the salient features of a quantum computer have been shown in proof-of-principle experiments, difficulties in scaling quantum systems have made more complex operations intractable. This is exemplified in the classical Fredkin (controlled-SWAP) gate for which, despite theoretical proposals, no quantum analog has been realized. By adding control to the SWAP unitary, we use photonic qubit logic to demonstrate the first quantum Fredkin gate, which promises many applications in quantum information and measurement. We implement example algorithms and generate the highest-fidelity three-photon Greenberger-Horne-Zeilinger states to date. The technique we use allows one to add a control operation to a black-box unitary, something that is impossible in the standard circuit model. Our experiment represents the first use of this technique to control a two-qubit operation and paves the way for larger controlled circuits to be realized efficiently.

(R.B. Patel, J. Ho, F. Ferreyrol, T.C. Ralph and G.J. Pryde, *A quantum Fredkin gate*, Science Advances, 25 Mar 2016, Vol. 2, no. 3, e1501531)

Obwody odwracalne



(R.B. Patel, J. Ho, F. Ferreyrol, T.C. Ralph and G.J. Pryde, *A quantum Fredkin gate*, Science Advances, 25 Mar 2016, Vol. 2, no. 3, e1501531)

Obwody odwracalne

- Obliczenia kwantowe są odwracalne.
- Obliczenia odwracalne są ważne w innych zastosowaniach, m.in. w programowaniu współbieżnym, bazach danych, programowaniu robotów (http://revcomp.eu/)

- Algorytmy kwantowe są tworzone tak, aby wykorzystać superpozycję stanów do obliczania wartość funkcji.
- Dla danej funkcji f, zakładamy, że U_f – bramkę kwantową realizującą f na bazie przestrzeni stanów – można wykonać *efektywnie* na komputerze kwantowym,

$$U_f|x\rangle = |f(x)\rangle.$$

- Aby bramka U_f była unitarna, f musi być odwracalna.
- Jeżeli f jest nieodwracalna, to zawsze możemy zachować jej argument,

$$U_f|x\rangle|y\rangle = |x\rangle|f(x) \oplus y\rangle$$

Kwantowa równoległość

Bramka U_f może działać na kombinacje liniowe stanów bazowych.

Algorytm Deutscha-Jozsy

- Celem algorytmu Deutscha-Jozsy jest wykazanie, że algorytmy kwantowe są w pewnych przypadkach *lepsze* od algorytmów klasycznych.
- Problem Deutsch-Jozsy jest zaprojektowany tak, żeby być trudnym do wykonania na maszynie klasycznej.
- Złożoność algorytmu jest mierzona liczbą wywołań bramki kwantowej odpowiadającej funkcji.

Algorytm Deutscha-Jozsy

Sformułowanie problemu dla najprostszego przypadku:

- Dana jest funkcja $f : \{0, 1\} \mapsto \{0, 1\}$.
- Określ czy f jest stała.

Algorytm Deutscha-Jozsy

- Klasycznie żeby określić czy funkcja jest stała musimy znać obie wartości.
- Kwantowo możemy obliczyć obie wartości *jednocześnie* korzystając z superpozycji.

Algorytm Deutscha-Jozsy

Kroki algorytmu

1. Przygotuj stan $|0\rangle|1\rangle$.
2. Wykonaj bramkę $H \otimes H$.
3. Wykonaj bramkę U_f.
4. Wykonaj bramkę $H \otimes \mathbb{I}$.

Algorytm Deutscha-Jozsy

Co lepiej jest rozpisać na tablicy...

Algorytm Deutscha-Jozsy

Wykonanie kroków 1-3 algorytmu daje stan

$$\frac{1}{2}(-1)^{f(0)}(|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle)(|0\rangle - |1\rangle)$$

lub równoważnie

$$\frac{1}{\sqrt{2}}(|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle) \otimes \frac{(-1)^{f(0)}}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Algorytm Deutscha-Jozsy

Po ostatnim kroku otrzymujemy stan

$$\frac{1}{2}\left(1+(-1)^{f(0)\otimes f(1)}\right)|0\rangle + \frac{1}{2}\left(1-(-1)^{f(0)\otimes f(1)}\right)|1\rangle$$

Algorytm Deutscha-Jozsy

- Algorytm jest deterministyczny – po jednym wykonaniu algorytmu znamy odpowiedź.
- Klasyczny algorytm deterministyczny wymaga *dwóch* wywołań funkcji f.

Algorytm Deutscha-Jozsy

Control parameters for the quantum Deutsch algorithm

ŁUKASZ PAWELA

Institute of Theoretical and Applied Informatics
Polish Academy of Sciences
Bałtycka 5, 44-100 Gliwice, Poland

Received 2 November 2011, Revised 21 November 2011, Accepted 5 December 2011

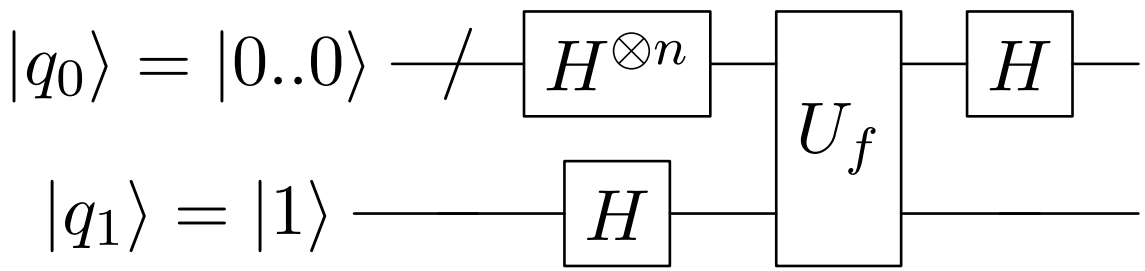
Abstract: An example of two-qubit scenario for finding an optimal control parameters on a spin chain to implement the quantum Deutsch algorithm is provided. Two cases are studied in this paper: two-qubit and three-qubit systems. The latter case is used to study the impact of interaction with an environment on the outcome of the algorithm.

(Ł. Pawela, *Control parameters for the quantum Deutsch algorithm*, Theoretical and Applied Informatics, Vol. 23, no. 3-4, pp. 193-200 (2011))

Algorytm Deutscha-Jozsy

- Algorytm Deutsch-Jozsy może być uogólniony na funkcje $f : \{0,1\}^n \mapsto \{0,1\}$.
- W tym wypadku możliwe jest rozróżnienie między funkcjami *stałymi* i *zbalansowanymi*.
- Klasyczny algorytm wymaga $2^{n-1} + 1$ wywołań funkcji.
- Algorytm kwantowy wymaga *jednego* wywołania U_f.

Algorytm Deutscha-Jozsy



Algorytm Grovera

- Algorytm Grovera pozwala na wyszukanie elementu w zbiorze.
- Wykorzystuje on superpozycję do zapisania informacji o przeszukiwanym zbiorze.
- Algorytm Grovera jest probabilistyczny.

Algorytm Grovera

Postawienie problemu.

- Załóżmy, że dysponujemy zbiorem N elementów, z których jeden spełnia pewien warunek.
- Przyjmujemy, że istnieje funkcja f, która przyjmuje wartość 1 tylko na tym elemencie.
- Do konstrukcji algorytmu kwantowego potrzebujemy operacji unitarnej, która odpowiada tej funkcji, U_ω,

$$U_f|\omega\rangle = -|\omega\rangle$$

dla $x^\star$ spełniającego nasz warunek oraz

$$U_f|x\rangle = |x\rangle$$

dla $x \neq \omega$.

Algorytm Grovera

Kroki algorytmu

- Przygotuj superpozycję $|s\rangle$ wszystkich wyszukiwanych stanów.
- Zastosuj operator U_ω.
- Zastosuj operator $U_s = 2|s\rangle\langle s| - \mathbb{I}$
- Powtórz dwa poprzednie kroki około $\frac{\pi}{4}\sqrt{N}$ razy.

Algorytm Grovera

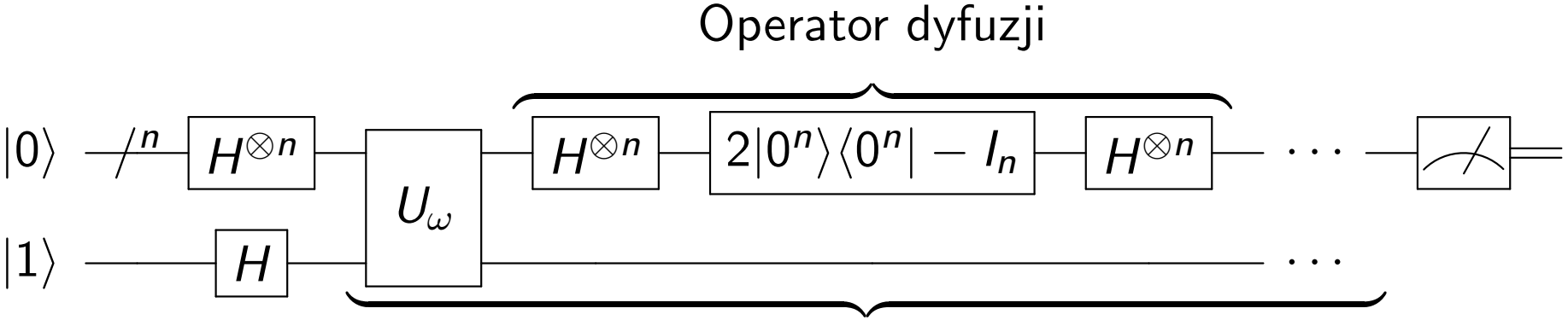
Zobaczmy jak to działa dla jednej iteracji...

Algorytm Grovera

- Proporcja (a właściwie amplituda) stanu $|\omega\rangle$ wzrasta po pierwszej iteracji do $\frac{2}{\sqrt{N}}$.
- Dla $N = 4$ wystarczy jedna iteracja.

Algorytm Grovera

Obwód dla N elementów zapisanych na n qubitach.



Algorytm Grovera

- Algorytm Grover można uogólnić dla kilku zaznaczonych elementów.
- Ponieważ prawdopodobieństwo uzyskania dobrej odpowiedzi rośnie z każdym krokiem, można rozważyć kiedy warto przerwać algorytm.

- Protokoły kwantowe są budowane do *kodowania* i *przesyłania* informacji.
- Oprócz superpozycji stanów, ważna jest tu również możliwość operowania na układach złożonych.

Teleportacja

Transporter działający na status klasy Galaxy, 2364

Teleportacja

- Teleportacja pozwala na przesłanie stanu kwantowego poprzez wysłanie dwóch bitów.
- Układ, którego stan jest teleportowany, jest niszczony w wyniku działania procedury teleportacji.

Teleportacja służy do przesyłania **stanu** układu.

Teleportacja

- Teleportacja polega przesłaniu stanu między dwoma punktami – lub osobami, np. Alicją i Bobem.
- Zakładamy, że Alicja chce przekazać Bobowi (nieznany) stan $|\psi\rangle_c = a|0\rangle + b|1\rangle$.
- Protokół wymaga, żeby Alicja i Bob dysponowali stanem *splątanym*.

$$|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B)$$

$$|\Phi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B - |1\rangle_A \otimes |1\rangle_B)$$

$$|\Psi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B + |1\rangle_A \otimes |0\rangle_B)$$

$$|\Psi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B)$$

Teleportacja

Przyjmijmy, że Alicja i Bob współdzielą stan

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Zatem stan całego układu to

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \otimes (\alpha|0\rangle_B + \beta|1\rangle_B)$$

Teleportacja

Stan całości można zapisać jako

$$\begin{aligned}|\Phi^+\rangle_{AB} \otimes |\psi\rangle_C = \quad & \frac{1}{2}|\Phi^+\rangle_{AC} \otimes (\alpha|0\rangle_B + \beta|1\rangle_B) \\ & + \frac{1}{2}|\Phi^-\rangle_{AC} \otimes (\alpha|0\rangle_B - \beta|1\rangle_B) \\ & + \frac{1}{2}|\Psi^+\rangle_{AC} \otimes (\beta|0\rangle_B + \alpha|1\rangle_B) \\ & + \frac{1}{2}|\Psi^-\rangle_{AC} \otimes (\beta|0\rangle_B - \alpha|1\rangle_B)\end{aligned}$$

Teleportacja

- Do zakończenia protokołu Alicja musi wysłać Bobowi informację o stanie jej podukładu.
- Możliwych stanów jest 2^2, czyli potrzebne są dwa bity.
- W zależności od otrzymanych danych, Bob wykonuje jedną z operacji.
  - $|\Phi^-\rangle \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
  - $|\Psi^-\rangle \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
  - $|\Psi^+\rangle \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

Gęste kodowanie

- Protokół gęstego kodowania to odwrotność teleportacji.
- Przesyłając jeden qubit możemy zakodować dwa bity informacji.