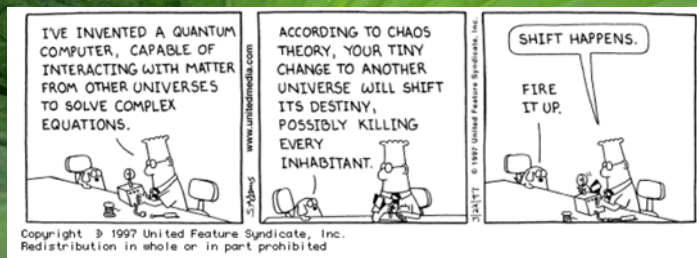


## Obliczenia kwantowe



Copyright © 1997 United Feature Syndicate, Inc.  
Redistribution in whole or in part prohibited

Jacek.Szczytko@fuw.edu.pl

Wydział Fizyki UW

## Obliczenia kwantowe

1. Bity, P-bity, Q-bity
2. Bramki Qbitowe
3. Kwantowe procedury
4. Poważny problem
5. Jak zbudować taki komputer?

**D:WAVE**  
The Quantum Computing Company™



Copyright © 1997 United Feature Syndicate, Inc.  
Redistribution in whole or in part prohibited

2014-01-22

2

## Sprawy bieżące

1. Esej na temat przyszłości – do 10 stycznia!
2. Nowy przedmiot „**Od pomysłu do patentu - Trendy, nowe technologie i zarządzanie innowacjami**” (Jacek Szczytko, Piotr Nieżurawski)– kwalifikacje na podstawie EGZAMINU! 1100-2`TNT (2 i 3 rok FIZ), 3 ECTS

2014-01-22

3

## Obliczenia kwantowe

"Where a calculator on the Eniac is equipped with 18000 vacuum tubes and weighs 30 tons, computers in the future may have only 1000 tubes and weigh only 1/2 tons"

*Popular Mechanics, March 1949*

„Podczas gdy kalkulator Eniac jest wyposażony w 18000 lamp próżniowych i waży 30 ton, przyszłe komputery mogą mieć tylko 1000 lamp i ważyć tylko 1/2 tony"

2014-01-22

4

# Obliczenia kwantowe

**Gazeta.pl Technologie**

Wiadomości | Sport | Biznes | Kultura | Technologie | Moto | Kobieta | Plotki

Wiadomości | Testy | Porady | Telewizory | Mobile | Audio | Internet | Rankingi | Komputer w firmie | Teleinformatyka

Polaciany | Aplikacje mobilne | Tablety | Komputer w firmie

Strata 51: zobacz, nad czym w tajemnicy pracowała armia USA

Volkswagen Aqua - poduszki powietrzne dla Chin

Czy Samsung O7000 jest idealny? [test]

Janusz A. Lipiński | 28.05.2011 | 15:37

## Pierwszy komercyjny komputer kwantowy - sprzedany

Komentuj, dodawaj zdjęcia i znajomych!  
Zaloguj się | logniewo.com?ref=Zaloguj\_sie

Najczęściej czytane

1. 10 najbardziej pożądanych gadżetów lat 80 (i czy ich jeszcze
2. Witamie do Lockheed-Martin okazuje się być robotą
3. Pierwszy komercyjny komputer kwantowy - sprzedany
4. Falester gościny: Empik.com - prawie jak Amazon.com
5. Samsung i Apple: wojna na pozory

2014-01-22

# Obliczenia kwantowe

**Onet Domeny**  
Edukuj w Internecie!

Sprawdź czy Twoja domena jest wolna:  
Super okazja! 50% taniej!

**onet.pl Wiadomości**

W Internecie | Szukaj | Poiszta Onet.pl

Internet i komputery | 02.17.2006 19:43

## "Komputer kwantowy nigdy nie zadziała"

**Komputer kwantowy nigdy nie będzie działał - twierdzi francuski uczyony cytowany przez pismo "New Scientist".**

Naukowcy od dawna rozstrzygają oliniewające wizje komputerów kwantowych, znacznie potężniejszych niż najszybsze z dzisiejszych komputerów. Taka maszyna dokonywałaby obliczeń w oparciu o ewolucję stanów kwantowych, dając wynik niemal natychmiast. Trzeba by jednak stosować bardzo złożone układy.

Choć powstały już pierwsze kwantowe bramki logiczne, istniejące przez ułamek sekundy, zdaniem Michaela Dyakonova z uniwersytetu w Montpellier wysłki w tym kierunku są daremne, ponieważ wraz ze złożonością kwantowego układu pojawia się coraz więcej zakłóceń, a sposoby ich korekty są oparte na błędnych założeniach.

**Impreza skinheadów czy pieśń patriotyczna?**

**PO WYBORACH...**  
Który minister Twoim zdaniem pracuje najlepiej?

- Andrzej Aurniller
- Ludwik Dom
- Anna Fotyga
- Grzegorz Gajda
- Roman Giertych
- Zyła Glowka
- Przemysław Gosiewski
- Wojciech Jasiński
- Anna Kalata
- Andrzej Lepper

2014-01-22

# Quantum Computer II (QC)

**D-WAVE**  
The Quantum Computing Company

**HARDWARE**

WELCOME TO D-WAVE SYSTEMS

D-Wave Systems is the world's first and only source for commercial applications. We believe quantum technology, digital processors, can and will represent to advancements in the application of computer science.

In February 2007, D-Wave unveiled and demonstrated publicly for the first time. The company plans to deliver systems in 2008.

**APPLICATIONS**  
Discover the potential of quantum computers and learn how they can accelerate breakthrough.

**NEWS**  
February 15, 2008  
Fourth First Commercial Quantum Computer Demonstrated  
New System Sets a Breakthrough in

Copyright 2006 D-Wave Systems Inc. All rights reserved. Photo by: G. Chung

2014-01-22

# Obliczenia kwantowe

**First electronic quantum processor points to new era in computing**

By Dario Borghino  
16:32 July 1, 2009 PDT

**Recent popular articles in Electronics**

graphene thinnest material in nature...  
World's thinnest material used to create...

The all-electronic, two-qubit quantum processor engineered by scientists at Yale

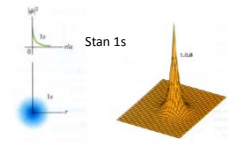
First electronic quantum processor points to new era in computing

2014-01-22

## Zapis skrócony

**DYGRESJA**

**Stan pojedynczej czastki:**  
 Np.: funkcja falowa atomu wodoru



Stan 1s

$$\Psi = R_{n,l}(r)\Theta_{l,m}(\theta)\Phi_m(\phi)$$

$$R_{n,l}(r) = \sqrt{\frac{(n-l+1)!}{2n(n+l)!}} \left(\frac{2Z}{na_0}\right)^{3/2} e^{-\rho/2} \rho^l G_{n-l-1}^{2l+1}(\rho)$$

$$\Theta_{l,m}(\theta) = (-1)^m \sqrt{\frac{2l+1}{2\pi} \frac{(l-m)!}{(l+m)!}} P_l^m(\cos\theta)$$

$$\Phi_m(\phi) = C e^{im\phi}$$

Liczby kwantowe!

$\Psi = R_{n,l}(r)\Theta_{l,m}(\theta)\Phi_m(\phi) = |n, l, m\rangle$

2014-01-22 9

## Zapis skrócony

**DYGRESJA**  
 (czyli tak naprawdę)

$$\Psi_{n,l,m}(\vec{r}, t) = \langle \vec{r} | n, l, m \rangle = |n, l, m\rangle$$

Reprezentacja położeniowa

↗

Zapis skrócony

↖

2014-01-22 10

## Bity, P-bity, Q-bity

<p><b>Bit</b></p> <p>0 ●</p> <p>1 ●</p> <p>States: 0 or 1</p>	<p><b>Pbit</b></p> <p>0 ●</p> <p>1 ●</p> <p>{p:0, (1-p):1}</p>	<p><b>Qubit</b></p> <p>0 ●</p> <p>1 ●</p> <p><math>\alpha 0\rangle + \beta 1\rangle</math></p> <p><math> \alpha ^2 +  \beta ^2 = 1</math></p>
---	--	---

> *Introduction to Quantum Information Processing*  
 > E. Knill, R. Laflamme, H. Barnum, D. Dalvit, J. Dziarmaga,  
 > J. Gubernatis, L. Gurvits, G. Ortiz, L. Viola and W. H. Zurek  
 > |

2014-01 11




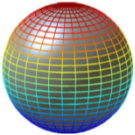
## Bity, P-bity, Q-bity

<p><b>Bit</b></p> <p>0 ●</p> <p>1 ●</p> <p>States: 0 or 1</p>	<p><b>Pbit</b></p> <p>0 ●</p> <p>1 ●</p> <p>{p:0, (1-p):1}</p>	<p><b>Qubit</b></p> <p>0 ●</p> <p>1 ●</p> <p><math>\alpha 0\rangle + \beta 1\rangle</math></p> <p><math> \alpha ^2 +  \beta ^2 = 1</math></p>
---	--	---

> komputery (maszyny Turinga)  
 > standardowe programy  
 > |

2014-01 12




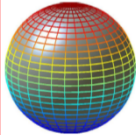
### Bity, P-bity, Q-bity

<p>Bit</p> <p>0</p>  <p>1</p>  <p>States: 0 or 1</p>	<p>Pbit</p> <p>0</p>  <p>1</p> <p>{p:0, (1-p):1}</p>	<p>Qubit</p> <p>0</p>  <p>1</p> <p><math>\alpha 0\rangle + \beta 1\rangle</math>  <math> \alpha ^2 +  \beta ^2 = 1</math></p>
--	---	--

- > „logika rozmyta“
- > metody obliczeniowe typu Monte Carlo
- > algorytmy genetyczne
- > metody optymalizacji

2014-01-13

### Bity, P-bity, Q-bity

<p>Bit</p> <p>0</p>  <p>1</p>  <p>States: 0 or 1</p>	<p>Pbit</p> <p>0</p>  <p>1</p> <p>{p:0, (1-p):1}</p>	<p>Qubit</p> <p>0</p>  <p>1</p> <p><math>\alpha 0\rangle + \beta 1\rangle</math>  <math> \alpha ^2 +  \beta ^2 = 1</math></p>
--	---	--

- > komputery kwantowe
- > algorytmy kwantowe
- > |

2014-01-14

### Bity, P-bity, Q-bity

Kwantowym odpowiednikiem klasycznego bitu jest dowolny układ dwustanowy:

dwa poziomy atom  $\{|g\rangle, |e\rangle\}$  np.  $g = 1s, e = 2s$

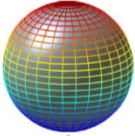
spin elektronu  $\{|\uparrow\rangle, |\downarrow\rangle\}$

foton o dwóch wzajemnie ortogonalnych stanach polaryzacji  $\{|\rightarrow\rangle, |\uparrow\rangle\}$  itp.

Taki układ to qubit (quantum bit); po polsku kubit.

Qubit

0



1

$\alpha|0\rangle + \beta|1\rangle$   
 $|\alpha|^2 + |\beta|^2 = 1$

Dwa stany układu, które możemy nazwać  $|0\rangle$  i  $|1\rangle$  przez analogie do klasycznego bitu,  $\{0, 1\}$ , tworzą bazę standardową albo obliczeniową —  $\{|0\rangle, |1\rangle\}$

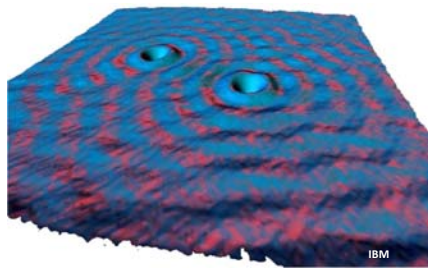
http://zon8.physd.amu.edu.pl/~tanasz/

2014-01-22 15

### Bity, P-bity, Q-bity

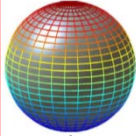
Obliczenia kwantowe bazują na dwóch własnościach światła kwantowego:

1. splątaniu kwantowym (kodowanie)
2. interferencji stanów (obliczenia)



Qubit

0



1

$\alpha|0\rangle + \beta|1\rangle$   
 $|\alpha|^2 + |\beta|^2 = 1$

IBM

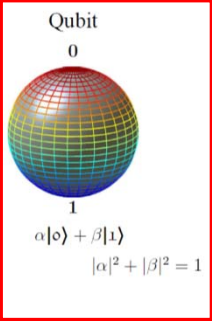
2014-01-22 16

### Bity, P-bity, Q-bity

$|\text{kubit}\rangle = |\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$   
 $\alpha, \beta \in \mathbb{C} \quad |\alpha|^2 + |\beta|^2 = 1$   
 ponieważ  $\alpha$  i  $\beta$  zespolone – równanie sfery

$|\Psi\rangle = e^{i\alpha} \left( \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi} \sin\left(\frac{\theta}{2}\right)|1\rangle \right)$

Qubit



$(a_x, a_y, a_z) = (\sin \theta \cos \varphi, \sin \theta \sin \varphi, \cos \theta)$   
 $|a_x|^2 + |a_y|^2 + |a_z|^2 = 1$

2014-01-22 17

### Bity, P-bity, Q-bity

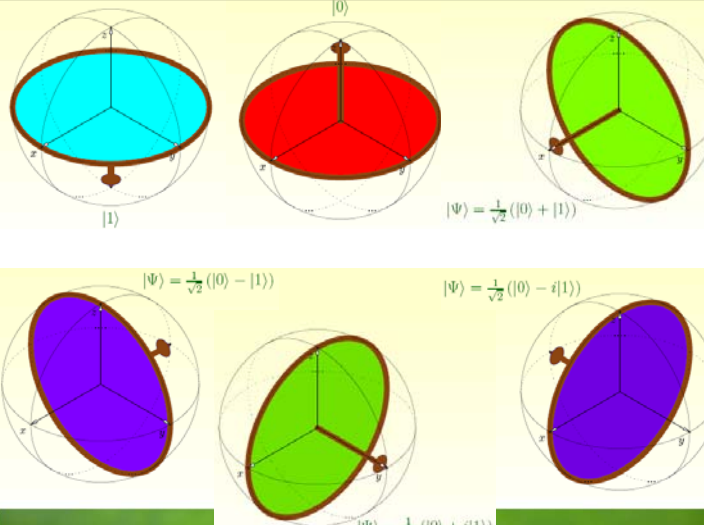
$|\text{kubit}\rangle = |\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$   
 $\alpha, \beta \in \mathbb{C} \quad |\alpha|^2 + |\beta|^2 = 1$   
 ponieważ  $\alpha$  i  $\beta$  zespolone – równanie sfery

$|\Psi\rangle = e^{i\alpha} \left( \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi} \sin\left(\frac{\theta}{2}\right)|1\rangle \right)$

$|\Psi\rangle = |0\rangle$   
 $|\Psi\rangle = |1\rangle$   
 $|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$   
 $|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$   
 $|\Psi\rangle = \frac{1}{\sqrt{5}}(|0\rangle - 2|1\rangle)$   
 $|\Psi\rangle = \frac{1}{5}(3|0\rangle - 4|1\rangle)$   
 $|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$   
 $|\Psi\rangle = \frac{1}{5}(4|0\rangle - 3i|1\rangle)$   
 $|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\varphi}|1\rangle)$   
 $|\Psi\rangle = \frac{1}{\sqrt{2}}(e^{i\theta}|0\rangle + e^{i\varphi}|1\rangle)$

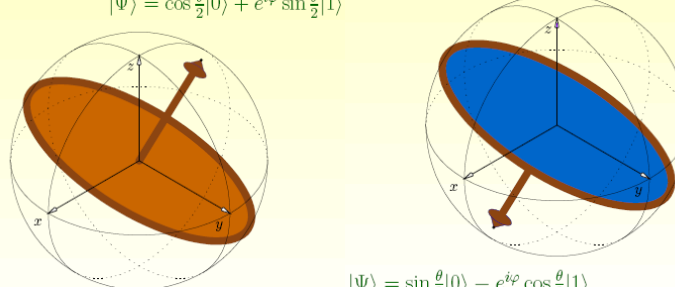
$(a_x, a_y, a_z) = (\sin \theta \cos \varphi, \sin \theta \sin \varphi, \cos \theta)$   
 $|a_x|^2 + |a_y|^2 + |a_z|^2 = 1$

2014-01-22 18



http://zon8.physd.amu.edu.pl/~tanasi/

$|\Psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi} \sin\frac{\theta}{2}|1\rangle$



$|\Psi\rangle = \sin\frac{\theta}{2}|0\rangle - e^{i\varphi} \cos\frac{\theta}{2}|1\rangle$

łatwo powiedzieć. Ale jak zrobić?

http://zon8.physd.amu.edu.pl/~tanasi/

### Bramki kubitowe

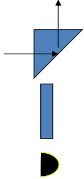
**W rolach głównych:**

foton  $\rightarrow$   $|\rightarrow\rangle = |0\rangle$

i foton  $\uparrow$   $|\uparrow\rangle = |1\rangle$

**W pozostałych rolach:**

- Pryzmat z całkowitym Wewnętrznym odbiciem
- Płytką szklaną o grubości  $d$
- Detektor



2014-01-22 21

### Bramki kubitowe

$|0\rangle \rightarrow \dots \rightarrow |0\rangle$

$|0\rangle \rightarrow \dots \rightarrow e^{i\theta}|0\rangle$

Płytką szklaną na drodze optycznej zmienia fazę fotonu W PORÓWNANIU do fotonu bez płytki.

2014-01-22 22

### Bramki kubitowe

$|0\rangle \rightarrow \dots \rightarrow |0\rangle$

2014-01-22 23

### Bramki kubitowe

$|0\rangle \rightarrow \dots \rightarrow |0\rangle$

$|0\rangle \rightarrow \dots \rightarrow i|0\rangle$

2014-01-22 24

### Bramki kubitowe

$|0\rangle \rightarrow |0\rangle$   
 $|0\rangle \rightarrow i|0\rangle$   
 ?

2014-01-22 25

### Bramki kubitowe

$|0\rangle \rightarrow \frac{i}{\sqrt{2}}|0\rangle$   
 $\frac{1}{\sqrt{2}}|0\rangle$   
 Prawdopodobieństwo  $1/2$   
 $\left|\frac{i}{\sqrt{2}}\right|^2 = \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}$

2014-01-22 26

### Bramki kubitowe

$|0\rangle \rightarrow \frac{i}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$   
 $\frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle$   
 $|1\rangle$

Umiemy zmieszać stany!

2014-01-22 27

### Bramki kubitowe

Jakie jest prawdopodobieństwo, że foton znajdzie się w detektorze A?

Interferometr Macha-Zendera

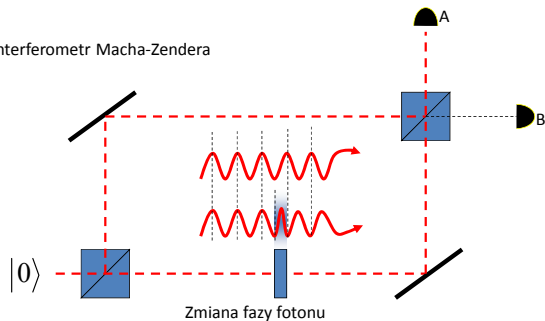
$|0\rangle$   
 A  
 B

2014-01-22 28

## Bramki kubitowe

Jakie jest prawdopodobieństwo, że foton znajdzie się w detektorze A?

Interferometr Macha-Zendera



2014-01-22

29

## Bramki kubitowe

Jakie jest prawdopodobieństwo, że foton znajdzie się w detektorze A?

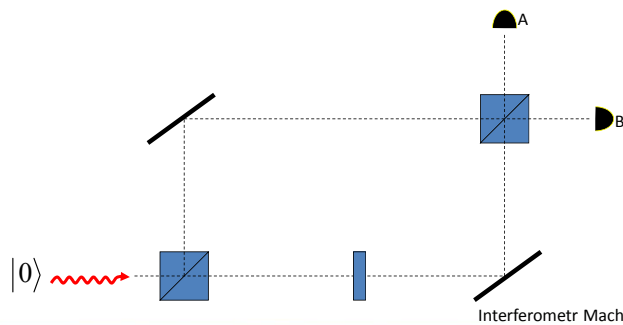
# Liczymy!

2014-01-22

30

## Bramki kubitowe

Jakie jest prawdopodobieństwo, że foton znajdzie się w detektorze A?



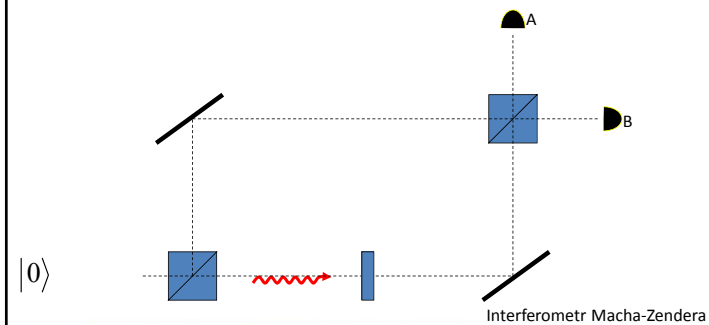
2014-01-22

31

## Bramki kubitowe

Jakie jest prawdopodobieństwo, że foton znajdzie się w detektorze A?

$$\frac{1}{\sqrt{2}}|0\rangle$$



2014-01-22

32



### Bramki kubitowe

Jakie jest prawdopodobieństwo, że foton znajdzie się w detektorze A?

$$\frac{1}{\sqrt{2}} \times e^{i\theta} |0\rangle$$

Interferometr Macha-Zendera

2014-01-22 33

### Bramki kubitowe

Jakie jest prawdopodobieństwo, że foton znajdzie się w detektorze A?

$$\frac{1}{\sqrt{2}} \times e^{i\theta} |0\rangle$$

Interferometr Macha-Zendera

2014-01-22 34

### Bramki kubitowe

Jakie jest prawdopodobieństwo, że foton znajdzie się w detektorze A?

$$\frac{1}{\sqrt{2}} \times e^{i\theta} \times \frac{1}{\sqrt{2}} |0\rangle$$

Mniam...

Interferometr Macha-Zendera

2014-01-22 35

### Bramki kubitowe

Jakie jest prawdopodobieństwo, że foton znajdzie się w detektorze A?

$$\frac{1}{\sqrt{2}} \times e^{i\theta} \times \frac{1}{\sqrt{2}} |0\rangle + \text{druga droga}$$

Interferometr Macha-Zendera

2014-01-22 36

### Bramki kubitowe

Jakie jest prawdopodobieństwo, że foton znajdzie się w detektorze A?

$$\frac{1}{\sqrt{2}} \times e^{i\theta} \times \frac{1}{\sqrt{2}} |0\rangle + \frac{i}{\sqrt{2}} |0\rangle$$

Interferometr Macha-Zendera

2014-01-22 37

### Bramki kubitowe

Jakie jest prawdopodobieństwo, że foton znajdzie się w detektorze A?

$$\frac{1}{\sqrt{2}} \times e^{i\theta} \times \frac{1}{\sqrt{2}} |0\rangle + \frac{i}{\sqrt{2}} |0\rangle$$

Interferometr Macha-Zendera

2014-01-22 38

### Bramki kubitowe

Jakie jest prawdopodobieństwo, że foton znajdzie się w detektorze A?

$$\frac{1}{\sqrt{2}} \times e^{i\theta} \times \frac{1}{\sqrt{2}} |0\rangle + \frac{i}{\sqrt{2}} \times \frac{i}{\sqrt{2}} |0\rangle$$

Interferometr Macha-Zendera

2014-01-22 39

### Bramki kubitowe

Jakie jest prawdopodobieństwo, że foton znajdzie się w detektorze A?

$$\frac{1}{\sqrt{2}} \times e^{i\theta} \times \frac{1}{\sqrt{2}} |0\rangle + \frac{i}{\sqrt{2}} \times \frac{i}{\sqrt{2}} |0\rangle = \frac{1}{2} (e^{i\theta} - 1) |0\rangle$$

Interferometr Macha-Zendera

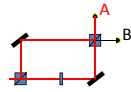
2014-01-22 40

## Bramki kubitowe

Jakie jest prawdopodobieństwo, że foton znajdzie się w detektorze A?

$$\frac{1}{\sqrt{2}} \times e^{i\theta} \times \frac{1}{\sqrt{2}} |0\rangle + \frac{i}{\sqrt{2}} \times \frac{i}{\sqrt{2}} |0\rangle = \frac{1}{2} (e^{i\theta} - 1) |0\rangle$$

Prawdopodobieństwo:  $P_{0,A} = \left| \frac{1}{2} (e^{i\theta} - 1) \right|^2 = \frac{1}{2} (1 - \cos \theta)$



2014-01-22

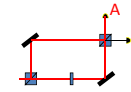
41

## Bramki kubitowe

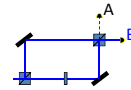
Jakie jest prawdopodobieństwo, że foton znajdzie się w detektorze A?

$$\frac{1}{\sqrt{2}} \times e^{i\theta} \times \frac{1}{\sqrt{2}} |0\rangle + \frac{i}{\sqrt{2}} \times \frac{i}{\sqrt{2}} |0\rangle = \frac{1}{2} (e^{i\theta} - 1) |0\rangle$$

Prawdopodobieństwo:  $P_{0,A} = \left| \frac{1}{2} (e^{i\theta} - 1) \right|^2 = \frac{1}{2} (1 - \cos \theta)$



Analogiczne:  $P_{0,B} = \left| \frac{i}{2} (e^{i\theta} + 1) \right|^2 = \frac{1}{2} (1 + \cos \theta)$



Dla  $\theta = 0$  mamy  $P_{0,A} = 0$  i  $P_{0,B} = 1$ , a więc foton NIGDY nie trafi do detektora A, tylko na pewno trafi do B! Oczywiście dla  $\theta = 180^\circ$  jest odwrotnie!

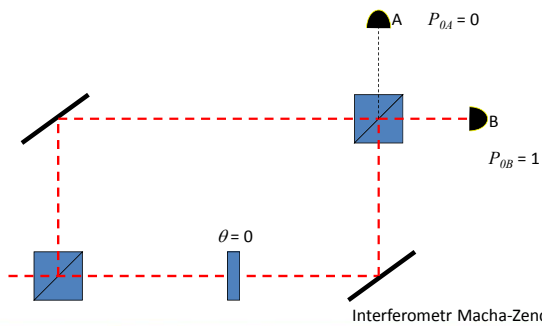
2014-01-22

42

## Dygresja: pomiar BEZ oddziaływania

Dla  $\theta = 0$  mamy  $P_{0,A} = 0$  i  $P_{0,B} = 1$ , a więc foton NIGDY nie trafi do detektora A, tylko na pewno trafi do B!

Foton interferuje SAM ZE SOBĄ!

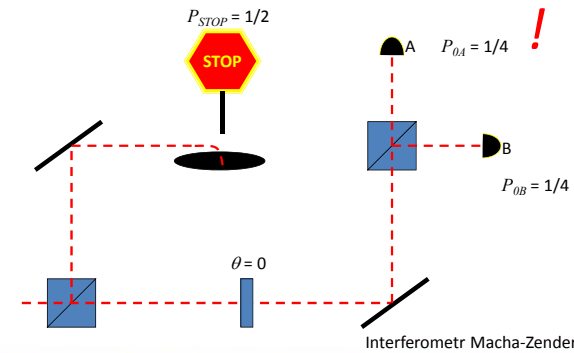


2014-01-22

43

## Dygresja: pomiar BEZ oddziaływania

Ale co się stanie gdy na jednej z dróg interferometru stanie przeszkoda?



2014-01-22

44

### Bramki kubitowe

W zależności od fazy  $\theta$  możemy otrzymać wynik:

2014-01-22 45

### Bramki kubitowe

W zależności od fazy  $\theta$  możemy otrzymać wynik:

2014-01-22 46

### Bramki kubitowe

Ogólnie  $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$

Matematycznie:

$$\begin{pmatrix} |\Psi\rangle \\ |\Psi'\rangle \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \alpha' & \beta' \end{pmatrix} \begin{pmatrix} |0\rangle \\ |1\rangle \end{pmatrix} = U \begin{pmatrix} |0\rangle \\ |1\rangle \end{pmatrix}$$

przeształcenie unitarne

2014-01-22 47

### Bramki kubitowe

$$\sqrt{NOT} = \frac{1}{2} \begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}$$

$$NOT = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} |0\rangle \\ |1\rangle \end{pmatrix} \begin{pmatrix} |1\rangle \\ |0\rangle \end{pmatrix}$$

Bramki CNOT są bramkami „uniwersalnymi” – można za ich pomocą zbudować dowolny obwód logiczny.

2014-01-22 48

### Bramki kubitowe

$$\sqrt{NOT} = \frac{1}{2} \begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}$$

$$NOT = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} |0\rangle \\ |1\rangle \end{pmatrix} = \begin{pmatrix} |1\rangle \\ |0\rangle \end{pmatrix}$$

Bramki kwantowe muszą być odwracalne!

$|0\rangle, |1\rangle$  bit kontrolny  $\rightarrow$   $|0\rangle, |1\rangle$   
 $|0\rangle, |1\rangle$  bit kontrolny  $\rightarrow$   $|1\rangle, |0\rangle$

Bramki CNOT są bramkami „uniwersalnymi” – można za ich pomocą zbudować dowolny obwód logiczny.

2014-01-22 49

### Bramki kubitowe

**a**  $|\uparrow\rangle \xrightarrow{H} [|\uparrow\rangle + |\downarrow\rangle]$   
 Hadamard  
**b**  $|\downarrow\rangle$  control,  $|\uparrow\rangle$  target  $\rightarrow |\downarrow\rangle, |\downarrow\rangle$   
 Controlled NOT  
**c**  $|\downarrow\rangle$  control,  $|\downarrow\rangle$  target  $\rightarrow [|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle]$   
 Entanglement

Quantum computing: The qubit duet  
Gianni Blatter  
Nature 421, 796-797 (20 February 2003)

2014-01-22 50

### Bramki kubitowe

Program:

$U_1 = U_{HAD}$     $U_2 = U_{CNOT12} \dots U_{CNOT1N}$     $U_3 = U_{CNOT1H}$     $U_4 = U_2^{-1}$     $U_5 = U_1^{-1} = U_{HAD}$

2014-01-22 51

### Różne pomysły

1. Kubity ze spinów
2. Kubity z atomów
3. Kubity jądrowe
4. Kubity krzemowe
5. Kubity z kropek
6. Kubity z ekscytonów
7. Kubity nadprzewodzące
8. Kubity świetlne

2014-01-22 52

### Kwantowe procedury:

**Komputer klasyczny:**  $T_n(m) = p$

$n$  = numer programu („kod”)  $m$  = dane wejściowe  $p$  = wynik

$n = 001011101011010010010001111011011101011...$   
 $m = 0101001010101010101111110000000000000000...$   
 $p = 010100101010101010111111010000000000000000...$

2014-01-22 53

### Kwantowe procedury:

**Komputer klasyczny:**  $T_n(m) = p$

$n$  = numer programu („kod”)  $m$  = dane wejściowe  $p$  = wynik

$n = 001011101011010010010001111011011101011...$   
 $m = \text{tak samo, ale zamiast bitów mamy kubity } \Psi$   
 $p = 010100101010101010111111010000000000000000...$

2014-01-22 54

### Kwantowe procedury:

**Komputer klasyczny:**  $T_n(m) = p$

$n$  = numer programu („kod”)  $m$  = dane wejściowe  $p$  = wynik

$n = 001011101011010010010001111011011101011...$   
 $m = \text{tak samo, ale zamiast bitów mamy kubity } \Psi$   
 $p = 010100101010101010111111010000000000000000...$

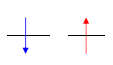
**Komputer kwantowy:**  $Q_n(\Psi) = p$

2014-01-22 55

### Kwantowe procedury:

Jak zbudować rejestr z kubitów?

**Komputer kwantowy:**  $Q_n(\Psi) = p$

Jeden kubit: 

baza:  $|0\rangle, |1\rangle$

rejestr:  $|\Psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$

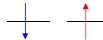
$\alpha_0^2 + \alpha_1^2 = 1$

2014-01-22 56

### Kwantowe procedury: Jak zbudować rejestr z kubitów?

**Komputer kwantowy:**  $Q_n(\Psi)=p$


Jeden kubit:

baza:  $|0\rangle, |1\rangle$  

rejestr:  $|\Psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$

$\alpha_0^2 + \alpha_1^2 = 1$

Dla dwóch kubitów:

baza:  $|0\rangle|0\rangle, |0\rangle|1\rangle, |1\rangle|0\rangle, |1\rangle|1\rangle$  

rejestr:  $|\Psi\rangle = \alpha_{00}|0\rangle|0\rangle + \alpha_{01}|0\rangle|1\rangle + \alpha_{10}|1\rangle|0\rangle + \alpha_{11}|1\rangle|1\rangle$

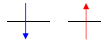
$\alpha_{00}^2 + \alpha_{01}^2 + \alpha_{10}^2 + \alpha_{11}^2 = 1$

2014-01-22 57

### Kwantowe procedury: Jak zbudować rejestr z kubitów?

**Komputer kwantowy:**  $Q_n(\Psi)=p$

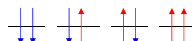
Jeden kubit:

baza:  $|0\rangle, |1\rangle$  

rejestr:  $|\Psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$

$\alpha_0^2 + \alpha_1^2 = 1$

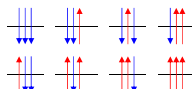
Dla dwóch kubitów:

baza:  $|0\rangle|0\rangle, |0\rangle|1\rangle, |1\rangle|0\rangle, |1\rangle|1\rangle$  

rejestr:  $|\Psi\rangle = \alpha_{00}|0\rangle|0\rangle + \alpha_{01}|0\rangle|1\rangle + \alpha_{10}|1\rangle|0\rangle + \alpha_{11}|1\rangle|1\rangle$

$\alpha_{00}^2 + \alpha_{01}^2 + \alpha_{10}^2 + \alpha_{11}^2 = 1$

Dla trzech kubitów:

baza:  $|0\rangle|0\rangle|0\rangle, |0\rangle|0\rangle|1\rangle, |0\rangle|1\rangle|0\rangle, |0\rangle|1\rangle|1\rangle,$   
 $|1\rangle|0\rangle|0\rangle, |1\rangle|0\rangle|1\rangle, |1\rangle|1\rangle|0\rangle, |1\rangle|1\rangle|1\rangle,$  

rejestr:  $|\Psi\rangle = \alpha_{000}|0\rangle|0\rangle|0\rangle + \alpha_{001}|0\rangle|0\rangle|1\rangle + \alpha_{010}|0\rangle|1\rangle|0\rangle + \dots + \alpha_{111}|1\rangle|1\rangle|1\rangle$

$\alpha_{000}^2 + \alpha_{001}^2 + \alpha_{010}^2 + \dots + \alpha_{111}^2 = 1$

2014-01-22 58

### Kwantowe procedury: Jak zbudować rejestr z kubitów?

**Komputer kwantowy:**  $Q_n(\Psi)=p$

Ogólnie jeden rejestr  $N$ -kubitowy może przechować  $2^N$  „klasycznych” liczb!

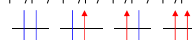
2014-01-22 59

### Kwantowe procedury: Jak zbudować rejestr z kubitów?

**Komputer kwantowy:**  $Q_n(\Psi)=p$

Ogólnie jeden rejestr  $N$ -kubitowy może przechować  $2^N$  „klasycznych” liczb!

Dla dwóch kubitów baza obliczeń:

$|0\rangle|0\rangle, |0\rangle|1\rangle, |1\rangle|0\rangle, |1\rangle|1\rangle$   
  
0 1 2 3

**Na przykład:**

$|\Psi\rangle = |2\rangle$

$|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|3\rangle)$

$|\Psi\rangle = \frac{1}{2}(|0\rangle + |1\rangle + |2\rangle + |3\rangle)$  ← Wszystkie stany jednakowo prawdopodobne (maksymalne splątanie kwantowe)

$|\Psi\rangle = \frac{1}{2}(|0\rangle - |1\rangle + i|2\rangle - |3\rangle)$  ← i tu też wszystkie stany jednakowo prawdopodobne

$|\Psi\rangle = \frac{1}{\sqrt{529}} \left( |0\rangle + \frac{i}{23}|1\rangle + \frac{8}{234323}|2\rangle + \frac{\sqrt{12}}{13123133}|3\rangle \right)$

2014-01-22 60

## Kwantowe procedury: Jak zbudować rejestr z kubitów?

**Komputer kwantowy:**  $Q_n(\Psi)=p$

Ogólnie jeden rejestr  $N$ -kubitowy może przechować  $2^N$  „klasycznych” liczb!

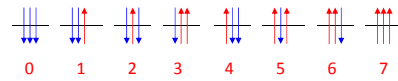
Dla trzech kubitów baza obliczeń:

baza:  $|\downarrow\rangle|\downarrow\rangle|\downarrow\rangle, |\downarrow\rangle|\downarrow\rangle|\uparrow\rangle, |\downarrow\rangle|\uparrow\rangle|\downarrow\rangle, |\downarrow\rangle|\uparrow\rangle|\uparrow\rangle,$   
 $|\uparrow\rangle|\downarrow\rangle|\downarrow\rangle, |\uparrow\rangle|\downarrow\rangle|\uparrow\rangle, |\uparrow\rangle|\uparrow\rangle|\downarrow\rangle, |\uparrow\rangle|\uparrow\rangle|\uparrow\rangle,$

$$|\Psi\rangle = \alpha_{000}|\downarrow\rangle|\downarrow\rangle|\downarrow\rangle + \alpha_{001}|\downarrow\rangle|\downarrow\rangle|\uparrow\rangle + \alpha_{010}|\downarrow\rangle|\uparrow\rangle|\downarrow\rangle + \alpha_{011}|\downarrow\rangle|\uparrow\rangle|\uparrow\rangle +$$

$$+ \alpha_{100}|\uparrow\rangle|\downarrow\rangle|\downarrow\rangle + \alpha_{101}|\uparrow\rangle|\downarrow\rangle|\uparrow\rangle + \alpha_{110}|\uparrow\rangle|\uparrow\rangle|\downarrow\rangle + \alpha_{111}|\uparrow\rangle|\uparrow\rangle|\uparrow\rangle$$

$$\alpha_{000}^2 + \alpha_{001}^2 + \alpha_{010}^2 + \alpha_{011}^2 + \alpha_{100}^2 + \alpha_{101}^2 + \alpha_{110}^2 + \alpha_{111}^2 = 1$$



itd..

## Kwantowe procedury:

**Komputer kwantowy:**  $Q_n(\Psi)=p$

Ogólnie jeden rejestr  $N$ -kubitowy może przechować  $2^N$  „klasycznych” liczb!

Przy  $N=300$  liczba  $2^{300}$  przekracza ilość protonów we Wszechświecie (widzialnym)!

Komputer kwantowy wykonuje operacje na całym rejestrze, czyli na wszystkich  $2^N$  liczbach jednocześnie. Nazywa się to **kwantowym paralelizmem**.

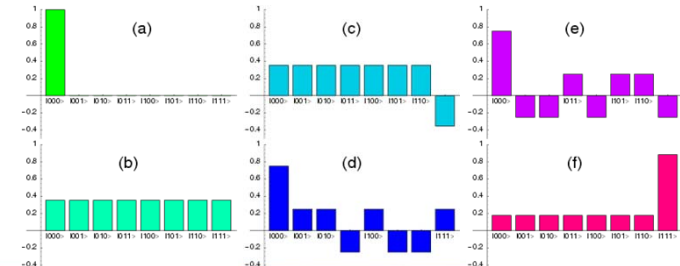
**Pewne algorytmy będą działały szybciej na komputerze kwantowym.**  
 Przede wszystkim te wymagające obliczeń równoległych: łamanie kodów, gra w szachy, przeszukiwanie baz danych, symulacje pogody, trzęsień ziemi, wybuchów jądrowych itp.

Aby móc odczytać wynik końcowy trzeba go jeszcze odseparować od wszystkich możliwych wyników. Wykorzystuje się kwantową interferencję stanów.

## Kwantowe procedury:

**Komputer kwantowy:**  $Q_n(\Psi)=p$

- Program zaczyna się od przygotowania superpozycji wszystkich możliwych danych wejściowych
- Wykonanie programu daje superpozycje wszystkich możliwych wyników (każdy ze składników superpozycji kwantowej działa niezależnie od innych)
- Oddzielenie wyników następuje na skutek kwantowej interferencji. Faza składników superpozycji kwantowej jest przygotowywana w ten sposób, aby najbardziej prawdopodobny wynik pomiaru odpowiadał interesującemu nas wynikowi.



## Kwantowe procedury:

**Komputer kwantowy:**  $Q_n(\Psi)=p$

**Przykład:**

Systemy kryptograficzne z kluczem publicznym wykorzystują fakt, że rozkład dużej liczby na czynniki jest trudny (czasochłonny)

- Najszybszy obecnie algorytm (GNFS – General Number Field Sieve ) wymaga czasu

$$\sim \exp\left[\left(\frac{64}{9}N\right)^{1/3} (\ln N)^{2/3}\right]$$

faktoryzacja liczby 400 cyfrowej wymagałaby  $10^{10}$  lat!

- W 1994 r. RSA 129 został złamany na 1600 stacjach roboczych w ciągu 8 miesięcy
- Algorytm kwantowy Petera Shora wymaga czasu

$$\sim (\ln N)^{2+\epsilon}$$

Komputer kwantowy, który faktoryzowałby liczbę 130 cyfrowa w ciągu miesiąca, sfaktoryzowałby liczbę 400 cyfrowa w czasie krótszym niż 3 lata



# Algorytm Shora

## Factoring Larger Numbers

http://www.soi.wide.ad.jp/class/20050012

2014-01-22 65

# Algorytm Shora

Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer<sup>\*</sup>

Peter W. Shor<sup>1</sup>

Abstract

A digital computer is generally believed to be an efficient universal computing device; that is, it is believed able to simulate any physical computing device with an increase in computation time for at most a polynomial factor. This may not be true when quantum mechanics is taken into consideration. This paper considers factoring integers and finding discrete logarithms, two problems which are generally thought to be hard on a classical computer and which have been used as the basis of several proposed cryptosystems. Efficient randomized algorithms are given for these two problems on a hypothetical quantum computer. These algorithms take a number of steps polynomial in the input size, e.g., the number of digits of the integer to be factored.

Keywords: algebraic number theory, prime factorization, discrete logarithms, Church's thesis, quantum computers, foundations of quantum mechanics, spin systems, Fourier transform

AMS subject classifications: 81P10, 11Y05, 68Q10, 68D10

arXiv:quant-ph/9508027 v2 25 Jan 1996

<sup>\*</sup>A preliminary version of this paper appeared in the Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, Nov. 20-22, 1994, IEEE Computer Society Press, pp. 124-134.

<sup>1</sup>AT&T Research, Room 2D-149, 600 Mountain Ave., Murray Hill, NJ 07974.

Peter Shor  
http://www-math.mit.edu/~shor/

2014-01-22 66

# Algorytm Shora

Prof. Ryszard Tanas <http://zon8.physd.amu.edu.pl/~tanar/>

Kwantowa faktoryzacja

Chcemy sfaktoryzować liczbę  $N$ ,  $N = 15$ . Wybieramy liczbę losową  $1 < X < N - 1$  względnie pierwszą z  $N$ , tzn. taką, że  $\text{NWD}(N, X) = 1$ , powiedzmy  $X = 2$ .

- Przygotowujemy rejestr kwantowy w stanie superpozycji wszystkich liczb od 0 do 15

A	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
---	---	---	---	---	---	---	---	---	---	---	----	----	----	----	----

2014-01-22 67

# Algorytm Shora

Prof. Ryszard Tanas <http://zon8.physd.amu.edu.pl/~tanar/>

Kwantowa faktoryzacja

Chcemy sfaktoryzować liczbę  $N$ ,  $N = 15$ . Wybieramy liczbę losową  $1 < X < N - 1$  względnie pierwszą z  $N$ , tzn. taką, że  $\text{NWD}(N, X) = 1$ , powiedzmy  $X = 2$ .

- Przygotowujemy rejestr kwantowy w stanie superpozycji wszystkich liczb od 0 do 15

A	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
---	---	---	---	---	---	---	---	---	---	---	----	----	----	----	----

• Wykonujemy operację  $B = X^A \text{ mod } N$ , wykorzystując kwantowy paralelizm i wyniki umieszczamy w rejestrze B. Komputer kwantowy wykonuje taką operację w jednym kroku!

	$2^0$	$2^1$	$2^2$	$2^3$	$2^4$	$2^5$	$2^6$	$2^7$	$2^8$	$2^9$	$2^{10}$	$2^{11}$	$2^{12}$	$2^{13}$	$2^{14}$
A	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
B	1	2	4	8	1	2	4	8	1	2	4	8	1	2	4

2014-01-22 68

# Algorytm Shora

Prof. Ryszard Tanas <http://zon8.physd.amu.edu.pl/~tanas/>

Kwantowa faktoryzacja

Chcemy sfaktoryzować liczbę  $N$ ,  $N = 15$ . Wybieramy liczbę losową  $1 < X < N - 1$  względnie pierwszą z  $N$ , tzn. taką, że  $\text{NWD}(N, X) = 1$ , powiedzmy

$X = 2$ .

- Przygotowujemy rejestr kwantowy w stanie superpozycji wszystkich liczb od 0 do 15

A	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
---	---	---	---	---	---	---	---	---	---	---	----	----	----	----	----

- Wykonujemy operację  $B = X^A \text{ mod } N$ , wykorzystując kwantowy paralelizm i wyniki umieszczamy w rejestrze B. Komputer kwantowy wykonuje taką operację w jednym kroku!

A	0	1	2 <sup>2</sup>	2 <sup>3</sup>	2 <sup>4</sup>	2 <sup>5</sup>	2 <sup>6</sup>	2 <sup>7</sup>	2 <sup>8</sup>	2 <sup>9</sup>	2 <sup>10</sup>	2 <sup>11</sup>	2 <sup>12</sup>	2 <sup>13</sup>	2 <sup>14</sup>
B	1	2	4	8	1	2	4	8	1	2	4	8	1	2	4

- Zauważamy, że wyniki w rejestrze B są okresowe z okresem  $r = 4$ . Komputer kwantowy potrafi szybko znajdować okres funkcji!

2014-01-22

69

# Algorytm Shora

A	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
B	1	2	4	8	1	2	4	8	1	2	4	8	1	2	4

Jeśli  $r$  jest nieparzyste, to wybieramy inne  $X$  i zaczynamy procedurę od nowa. Jeśli  $r$  jest parzyste, obliczamy  $P = X^{r/2} - 1$  lub  $P = X^{r/2} + 1$  i sprawdzamy  $\text{NWD}(P, N)$ . W naszym przykładzie  $r = 4$ ;  $P = 2^{4/2} - 1 = 3$  lub  $P = 2^{4/2} + 1 = 5$ .

$$15/3 = 5$$

$$15/5 = 3$$

2014-01-22

70

# Algorytm Shora

Prof. Ryszard Tanas <http://zon8.physd.amu.edu.pl/~tanas/>

Kwantowa faktoryzacja

Chcemy sfaktoryzować liczbę  $N$ ,  $N = 15$ . Wybieramy liczbę losową  $1 < X < N - 1$  względnie pierwszą z  $N$ , tzn. taką, że  $\text{NWD}(N, X) = 1$ , powiedzmy

$X = 7$ .

- Przygotowujemy rejestr kwantowy w stanie superpozycji wszystkich liczb od 0 do 15

A	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
---	---	---	---	---	---	---	---	---	---	---	----	----	----	----	----

- Wykonujemy operację  $B = X^A \text{ mod } N$ , wykorzystując kwantowy paralelizm i wyniki umieszczamy w rejestrze B. Komputer kwantowy wykonuje taką operację w jednym kroku!

A	0	1	2 <sup>7</sup>	2 <sup>8</sup>	2 <sup>9</sup>	2 <sup>10</sup>	2 <sup>11</sup>	2 <sup>12</sup>	2 <sup>13</sup>	2 <sup>14</sup>	
B	1	7	4	13	1	7	4	13	1	7	4

- Zauważamy, że wyniki w rejestrze B są okresowe z okresem  $r = 4$ . Komputer kwantowy potrafi szybko znajdować okres funkcji!

2014-01-22

71

# Algorytm Shora

VOLUME 85, NUMBER 25 PHYSICAL REVIEW LETTERS 18 DECEMBER 2000

## Experimental Realization of an Order-Finding Algorithm with an NMR Quantum Computer

Lieven M.K. Vandersypen,<sup>1,2,\*</sup> Matthias Steffen,<sup>1,2</sup> Gregory Bryce,<sup>2</sup> Costantino S. Yannoni,<sup>2</sup> Richard Cleve,<sup>3</sup> and Isaac L. Chuang<sup>2</sup>

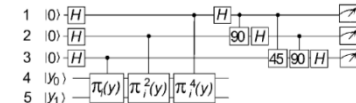
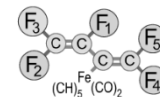
<sup>1</sup>Solid State and Photonics Laboratory, Stanford University, Stanford, California 94305-4075

<sup>2</sup>JBM Almaden Research Center, San Jose, California 95120

<sup>3</sup>Department of Computer Science, University of Calgary, Calgary, Alberta, Canada T2N 1N4

(Received 1 August 2000)

We report the realization of a nuclear magnetic resonance quantum computer which combines the quantum Fourier transform with exponentiated permutations, demonstrating a quantum algorithm for order finding. This algorithm has the same structure as Shor's algorithm and its speedup over classical algorithms scales exponentially. The implementation uses a particularly well-suited five quantum bit molecule and was made possible by a new state initialization procedure and several quantum control techniques.



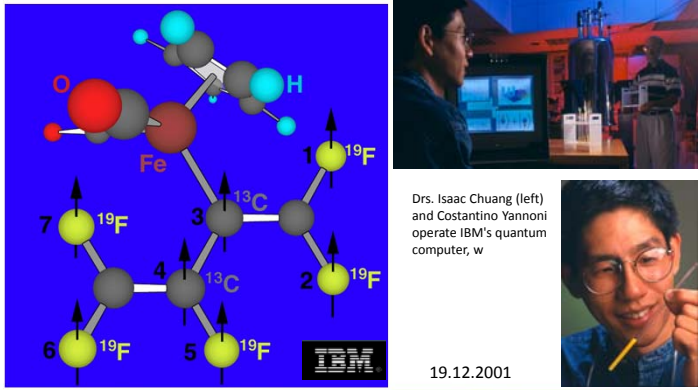
pentafluorobutadienyl cyclopentadienyldicarbonyliron complex

2014-01-22

72

## Komputeru kwantowe

7 Qubits



Drs. Isaac Chuang (left) and Costantino Yannoni operate IBM's quantum computer, w

19.12.2001

2014-01-22 73

## Algorytmy kwantowe

W tej chwili znanych jest mniej więcej 6 znaczących algorytmów kwantowych

- Deutsch-Josza (1992) – funkcja stała lub zrównoważona
- Shor (1994) - Faktoryzacja
- Kitaev (1995) - Faktoryzacja
- Grover (1992) - Przeszukiwanie bazy danych
- Grover (1997) - Szacowanie mediany
- Durr-Hoyer (1996) - Szacowanie minimum

[http://www.if.ufrgs.br/~jgallas/QUBITS/CURSO/brief\\_history.html](http://www.if.ufrgs.br/~jgallas/QUBITS/CURSO/brief_history.html)

2014-01-22 74

## Poważny problem

Skoro to takie proste, to dlaczego to jeszcze nie działa?



2014-01-22 75

## Poważny problem

Skoro to takie proste, to dlaczego to jeszcze nie działa?



**KOHERENCJA\*!**

Słownik Kopalińskiego: \* **koherencja** spoiwość, spójność; zgodność (myśli, sądów; częstotliwości i długości fal). Koherencję można opisać jako stopień korelacji czasowej i przestrzennej między wartościami amplitud.

2014-01-22 76

### Poważny problem

W czasie trwania procedury kwantowej wszystkie procesy MUSZĄ być odwracalne w czasie. W mechanice kwantowej POMIAR jest najczęściej nieodwracalny - w momencie pomiaru „dowiadujemy” się w jakim stanie jest funkcja (tzw. *redukcja f. falowej*)

$$\Psi = A\Psi_A + B\Psi_B$$

pomiar **A** lub **B**  
 $P_A = |A|^2$   
 $P_B = |B|^2$

$\Psi = \Psi_A$      $P_A = 1$   
 $P_B = 0$

$\Psi = \Psi_B$      $P_A = 0$   
 $P_B = 1$

Zakaz klonowania sprawia, że nie można się dowiedzieć wartości każdej ze składowych *A* lub *B* z osobna.

„Pomiarem” może być przypadkowe oddziaływanie z sąsiednim układem, szum (przypadkowa zmiana fazy funkcji falowej), oddziaływanie z aparaturą pomiarową, absorpcja fotonu termicznego itd.

### Poważny problem

**Komputer kwantowy:**  $Q_n(\Psi) = p$     input  $\Psi$

Pewna procedura kwantowa

2014-01-22 78

### Poważny problem

**Komputer kwantowy:**  $Q_n(\Psi) = p$     input  $\Psi$

START!

Pewna procedura kwantowa

łubudubu! łup! łup!  
 łup! łup! Ramydada!  
 łup! ...

2014-01-22 79

### Poważny problem

**Komputer kwantowy:**  $Q_n(\Psi) = p$     input  $\Psi$

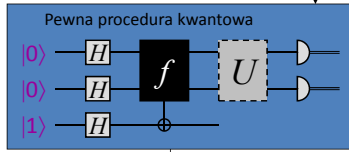
Pewna procedura kwantowa

$|\Psi\rangle = \alpha_{00}|0\rangle|0\rangle + \alpha_{01}|0\rangle|1\rangle + \alpha_{10}|1\rangle|0\rangle + \alpha_{11}|1\rangle|1\rangle$     wynik pośredni

2014-01-22 80

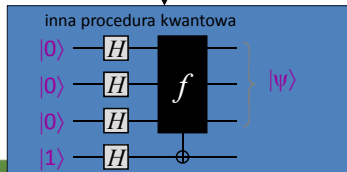
# Poważny problem

Komputer kwantowy:  $Q_n(\Psi) = p$  input  $\Psi$



$$|\Psi\rangle = \alpha_{00}|0\rangle|0\rangle + \alpha_{01}|0\rangle|1\rangle + \alpha_{10}|1\rangle|0\rangle + \alpha_{11}|1\rangle|1\rangle$$

wynik pośredni



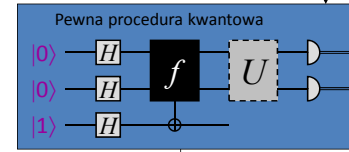
łubudubu! łup! łup!  
łup! łup! Ramydada!  
łup! ...

2014-01-22

81

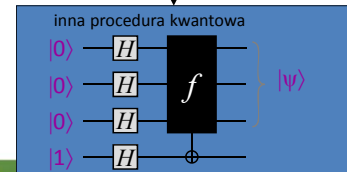
# Poważny problem

Komputer kwantowy:  $Q_n(\Psi) = p$  input  $\Psi$



$$|\Psi\rangle = \alpha_{00}|0\rangle|0\rangle + \alpha_{01}|0\rangle|1\rangle + \alpha_{10}|1\rangle|0\rangle + \alpha_{11}|1\rangle|1\rangle$$

wynik pośredni



KONIEC!

output

2014-01-22

82

# Poważny problem

Komputer kwantowy:  $Q_n(\Psi) = p$  input  $\Psi$

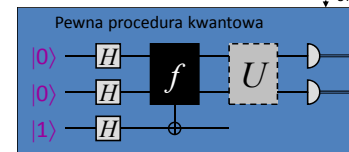
Tym razem z dekoherencją

2014-01-22

83

# Poważny problem

Komputer kwantowy:  $Q_n(\Psi) = p$  input  $\Psi$



łubudubu! łup! łup!  
łup! łup! Ramydada!  
łup! ...

2014-01-22

84

### Poważny problem

Komputer kwantowy:  $Q_n(\Psi)=p$  input  $\Psi$

Pewna procedura kwantowa

$|\Psi\rangle = \alpha_{00}|0\rangle|0\rangle + \alpha_{01}|0\rangle|1\rangle + \alpha_{10}|1\rangle|0\rangle + \alpha_{11}|1\rangle|1\rangle$  wynik pośredni

2014-01-22 85

### Poważny problem

Komputer kwantowy:  $Q_n(\Psi)=p$  input  $\Psi$

Pewna procedura kwantowa

$|\Psi\rangle = \alpha_{00}|0\rangle|0\rangle + \alpha_{01}|0\rangle|1\rangle + \alpha_{10}|1\rangle|0\rangle + \alpha_{11}|1\rangle|1\rangle$  wynik pośredni

złśliwy foton

2014-01-22 86

### Poważny problem

Komputer kwantowy:  $Q_n(\Psi)=p$  input  $\Psi$

Pewna procedura kwantowa

$|\Psi\rangle = \beta|0\rangle|0\rangle + \gamma|1\rangle|0\rangle$  fałszywy wynik pośredni

2014-01-22 87

### Poważny problem

Komputer kwantowy:  $Q_n(\Psi)=p$  input  $\Psi$

Pewna procedura kwantowa

$|\Psi\rangle = \beta|0\rangle|0\rangle + \gamma|1\rangle|0\rangle$  fałszywy wynik pośredni

inna procedura kwantowa

WYNIK FAŁSZYWY!

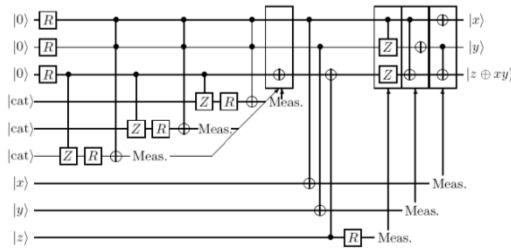
output

2014-01-22 88

# Poważny problem

**Rozwiązania:**  
 0 → 000  
 1 → 111

## 1. Procedury kwantowej korekcji błędów



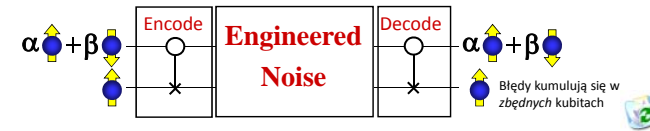
J. Preskill quant-ph/9705031

Figure 12: The fault-tolerant Toffoli gate. Each line represents a block of 7 qubits, and the gates are implemented transversally. For each measurement, the arrow points to the set of gates that is to be applied if the measurement outcome is 1; no action is taken if the outcome is 0.

# Poważny problem

**Rozwiązania:**

## 1. Procedury kwantowej korekcji błędów



2. Na czas działania procedur kwantowych układ należy odizolować od wpływu otoczenia (liczy się tzw. czas koherencji, w którym układ pozostaje spójny).

**Dekoherencja ogranicza rozmiary rejestru kwantowego**

# Poważny problem

**Rozwiązania:**

## Is Fault-Tolerant Quantum Computation Really Possible?

M. I. Dyakonov

*Laboratoire de Physique Théorique et Astroparticules, Université Montpellier II, France*

The so-called "threshold" theorem says that, once the error rate per qubit per gate is below a certain value, indefinitely long quantum computation becomes feasible, even if all of the qubits involved are subject to relaxation processes, and all the manipulations with qubits are not exact. The purpose of this article, intended for physicists, is to outline the ideas of quantum error correction and to take a look at the proposed technical instruction for fault-tolerant quantum computation. It seems that the mathematics behind the threshold theorem is somewhat detached from the physical reality, and that some ideal elements are always present in the construction. This raises serious doubts about the possibility of large scale quantum computations, even as a matter of principle.

**Dekoherencja ogranicza rozmiary rejestru kwantowego**

# Nowe podejścia



Available online at [www.sciencedirect.com](http://www.sciencedirect.com)

SCIENCE @ DIRECT®

Theoretical Computer Science 320 (2004) 15–33

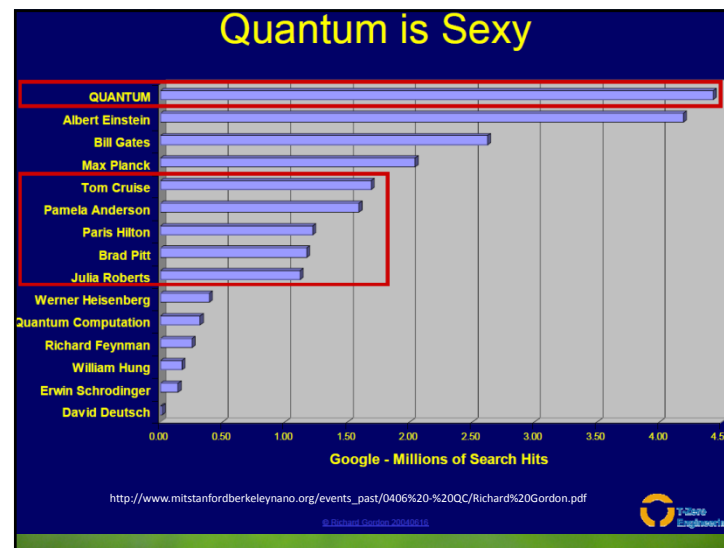
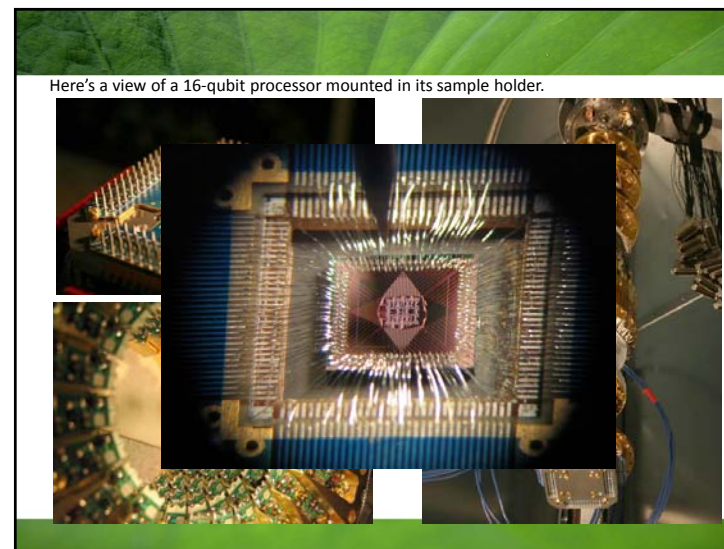
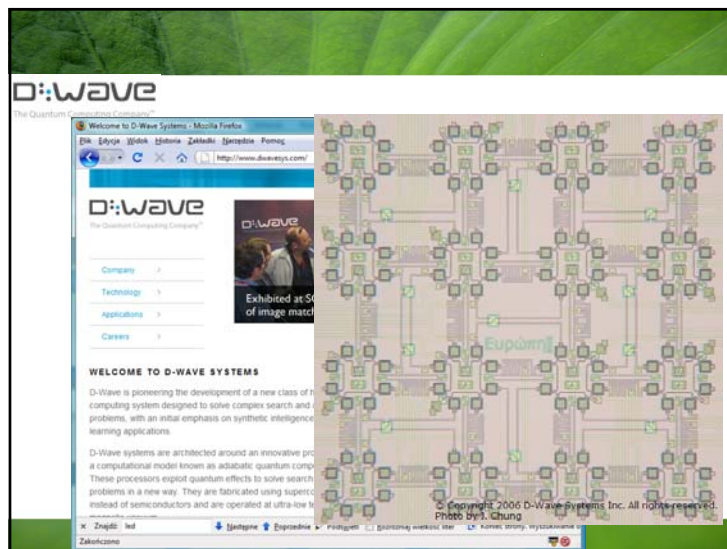
Theoretical  
Computer Science  
[www.elsevier.com/locate/tcs](http://www.elsevier.com/locate/tcs)

## Quantum computing without entanglement<sup>☆</sup>

Eli Biam<sup>a</sup>, Gilles Brassard<sup>b</sup>, Dan Kenigsberg<sup>a</sup>, Tal Mor<sup>a</sup>

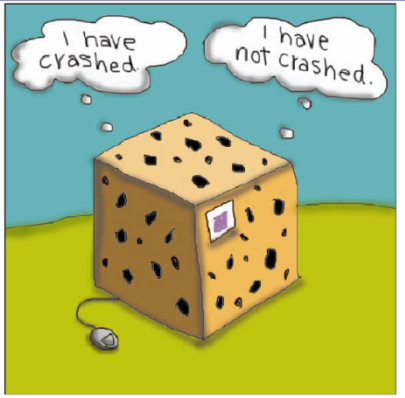
<sup>a</sup>Computer Science Department, Technion, Haifa 32000, Israel

<sup>b</sup>Département d'informatique et de recherche opérationnelle, Université de Montréal, Montréal, Qué., Canada, H3C 3J7





# Qwindows 2098



Schrödinger's computer. —Sally O. Lee

http://www.mit.edu/~stanford/berkeleymano.org/events\_past/04/05/20-%20OC/charles%20Gordon.pdf

© Richard Gordon 2004/05/16

