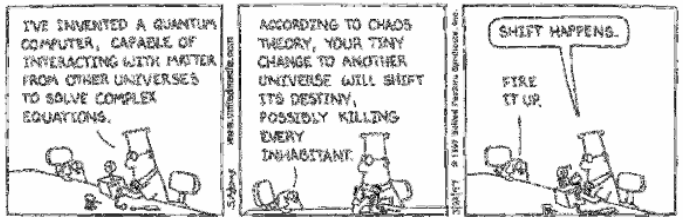
Quantum Computer I (QC)

Jacek Szczytko, Wydział Fizyki UW

1. Komputery kwantowe
   a. Logika bramek
   b. Kwantowe algorytmy
   c. Jak zbudować taki komputer?



Jacek.Szczytko@fuw.edu.pl

"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 1/2 tons"

Popular Mechanics, March 1949

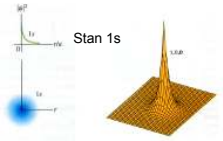
Jacek.Szczytko@fuw.edu.pl

Zapis skrócony

DYGRESJA

Stan pojedynczej cząstki:

Np.: funkcja falowa atomu wodoru



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

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

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

$$\Phi_m(\phi) = Ce^{im\phi}$$

Liczby kwantowe!

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

Jacek.Szczytko@fuw.edu.pl

Zapis skrócony

DYGRESJA

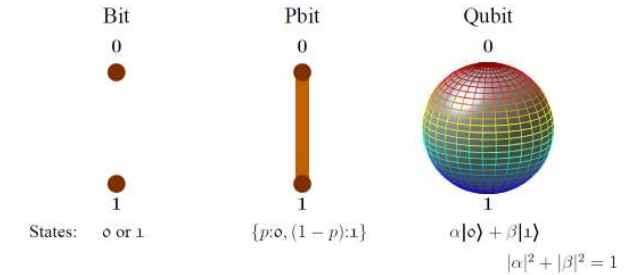
(czyli tak naprawdę)

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

Reprezentacja położeniowa

Zapis skrócony

Bity, P-bity, Q-bity



Jacek.Szczytko@fuw.edu.pl

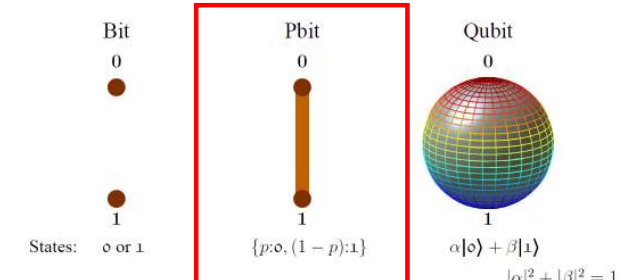
> ***Introduction to Quantum Information Processing***
> E. Knill, R. Laflamme, H. Barnum, D. Dalvit, J. Dziarmaga,
> J. Gubernatis, L. Gurvits, G. Ortiz, L. Viola and W. H. Zurek
> ▌

Bity, P-bity, Q-bity

Jacek.Szczytko@fuw.edu.pl

> komputery (maszyny Turinga)
> standardowe programy
> ▌

Bity, P-bity, Q-bity



Jacek.Szczytko@fuw.edu.pl

> „logika rozmyta”
> metody obliczeniowe typu Monte Carlo
> algorytmy genetyczne
> metody optymalizacji ▌

Bity, P-bity, Q-bity

Jacek.Szczytko@fuw.edu.pl

> komputery kwantowe
> algorytmy kwantowe
> ▌

Bity, P-bity, Q-bity

Kwantowym odpowiednikiem klasycznego bitu jest dowolny układ dwustanowy:

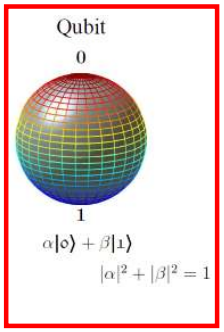
dwa poziomy atomu $\{|g\rangle, |e\rangle\}$ np. $g = 1s$, $e = 2s$

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.

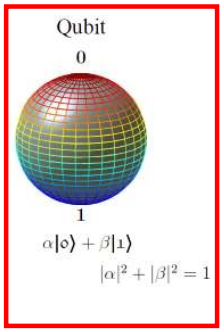


Dwa stany układu, które mozemy nazwac $|0\rangle$ i $|1\rangle$ przez analogie do klasycznego bitu, {0, 1}, tworza baze standardowa albo obliczeniowa — $\{|0\rangle, |1\rangle\}$

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

Bity, P-bity, Q-bity

Obliczenia kwantowe bazują na dwóch własnościach świata kwantowego:
1. splątaniu kwantowym (kodowanie)
2. interferencji stanów (obliczenia)



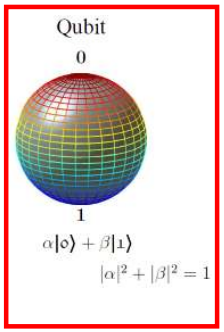
Bity, P-bity, Q-bity

$$|\text{kubit}\rangle = |\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$\alpha, \beta \in \mathbb{C} \qquad \underbrace{|\alpha|^2 + |\beta|^2}_{} = 1$$

ponieważ α i β zespolone – równanie sfery

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



$$(a_x, a_y, a_z) = (\sin\theta\cos\varphi, \sin\theta\sin\varphi, \cos\theta)$$

$$|a_x|^2 + |a_y|^2 + |a_z|^2 = 1$$

Bity, P-bity, Q-bity

$$|\text{kubit}\rangle = |\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$\alpha, \beta \in \mathbb{C} \qquad \underbrace{|\alpha|^2 + |\beta|^2}_{} = 1$$

ponieważ α i β zespolone – równanie sfery

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

$$(a_x, a_y, a_z) = (\sin\theta\cos\varphi, \sin\theta\sin\varphi, \cos\theta)$$

$$|a_x|^2 + |a_y|^2 + |a_z|^2 = 1$$

$|\Psi\rangle = |0\rangle$

$|\Psi\rangle = |1\rangle$

$|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

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

$|\Psi\rangle = \frac{1}{\sqrt{5}}(|0\rangle - 2|1\rangle)$

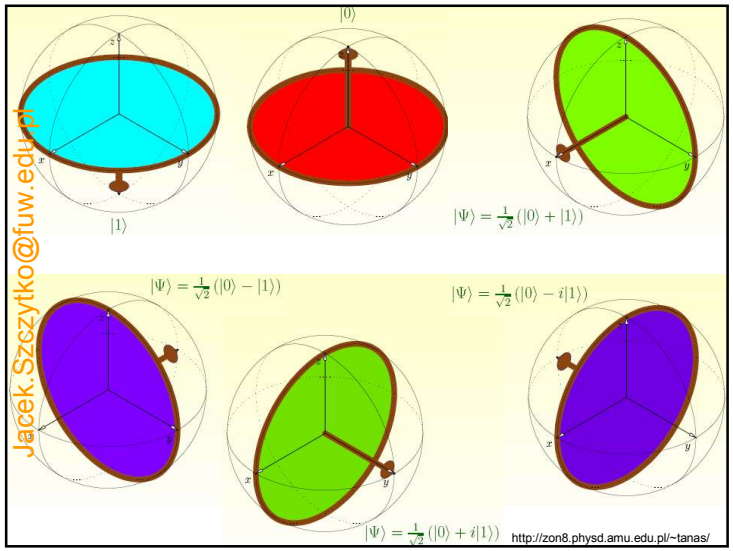
$|\Psi\rangle = \frac{1}{5}(3|0\rangle - 4|1\rangle)$

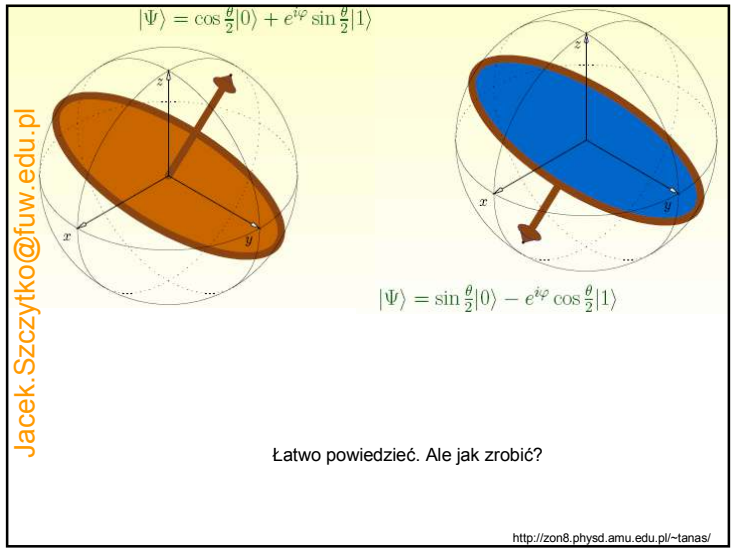
$|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$

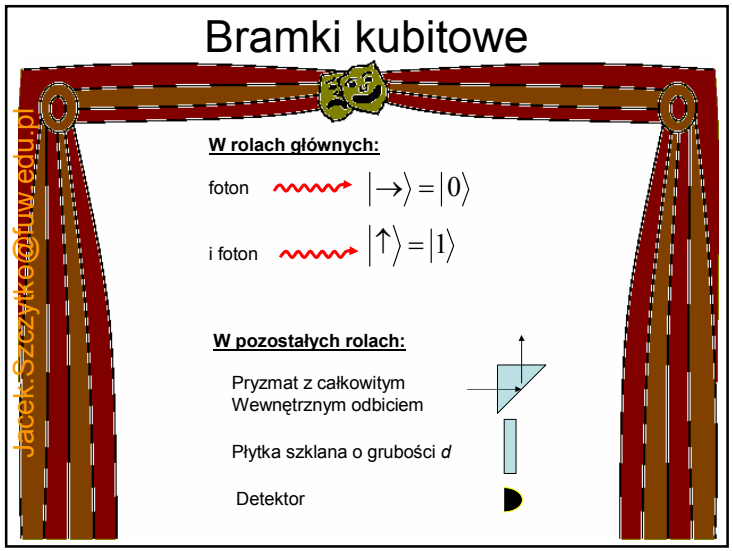
$|\Psi\rangle = \frac{1}{5}(4|0\rangle - 3i|1\rangle)$

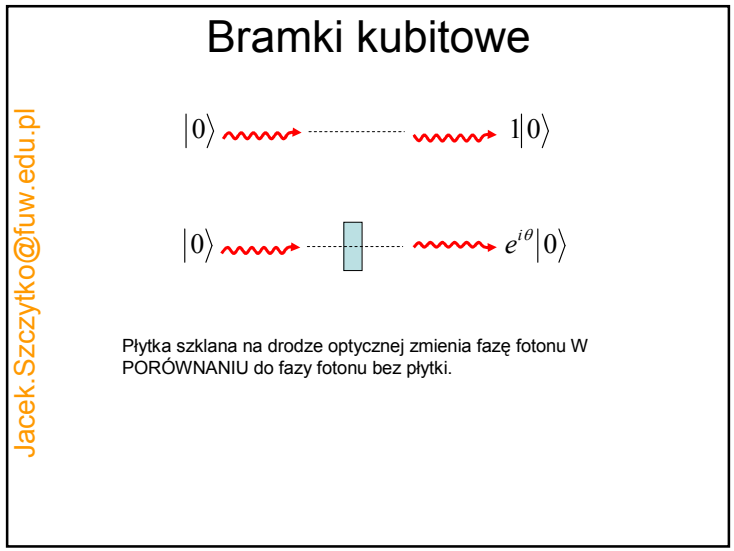
$|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\varphi}|1\rangle)$

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

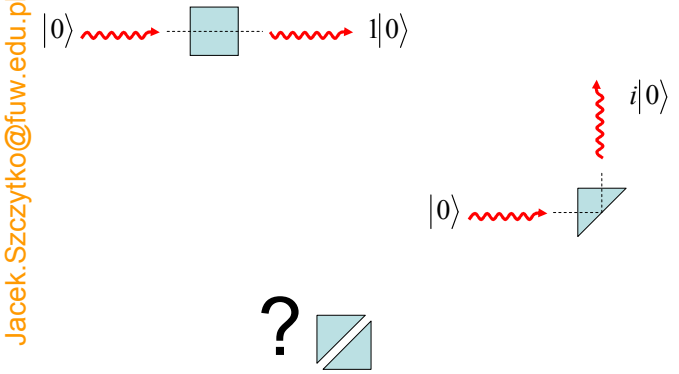

$|0\rangle$
$|1\rangle$
$|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
$|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
$|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$
$|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$
http://zon8.physd.amu.edu.pl/~tanas/
Jacek.Szczytko@fuw.edu.pl


$|\Psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$
$|\Psi\rangle = \sin\frac{\theta}{2}|0\rangle - e^{i\varphi}\cos\frac{\theta}{2}|1\rangle$
Łatwo powiedzieć. Ale jak zrobić?
http://zon8.physd.amu.edu.pl/~tanas/
Jacek.Szczytko@fuw.edu.pl

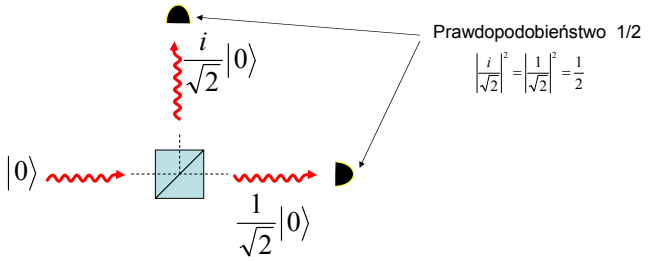

Bramki kubitowe
W rolach głównych:
foton $|\rightarrow\rangle = |0\rangle$
i foton $|\uparrow\rangle = |1\rangle$
W pozostałych rolach:
Pryzmat z całkowitym Wewnętrznym odbiciem
Płytka szklana o grubości *d*
Detektor
Jacek.Szczytko@fuw.edu.pl


Bramki kubitowe
$|0\rangle$
$1|0\rangle$
$|0\rangle$
$e^{i\theta}|0\rangle$
Płytka szklana na drodze optycznej zmienia fazę fotonu W PORÓWNANIU do fazy fotonu bez płytki.
Jacek.Szczytko@fuw.edu.pl

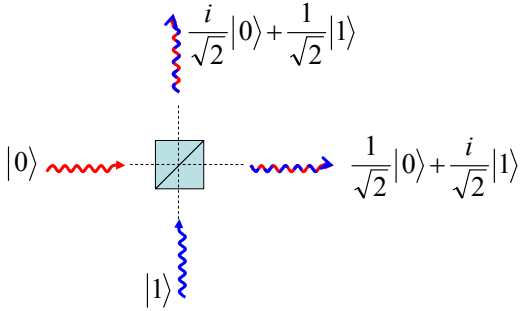
Bramki kubitowe



Bramki kubitowe



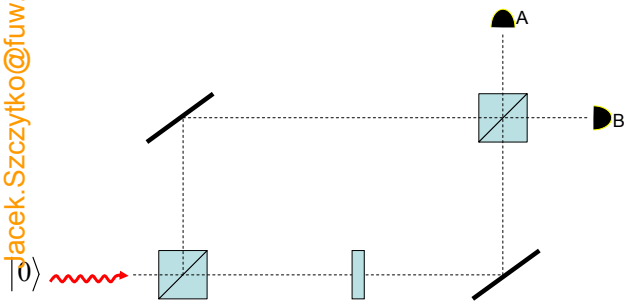
Bramki kubitowe



Umiemy zmieszać stany!

Bramki kubitowe

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

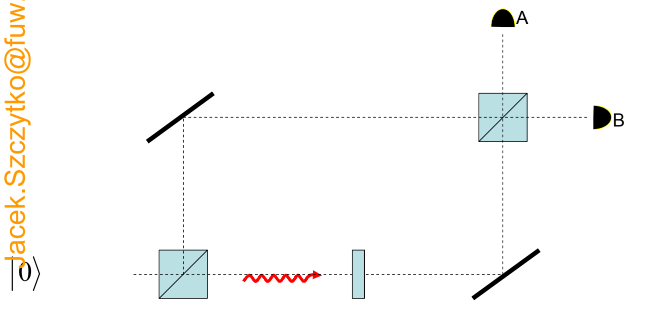


Interferometr Macha-Zendera

Bramki kubitowe

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

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

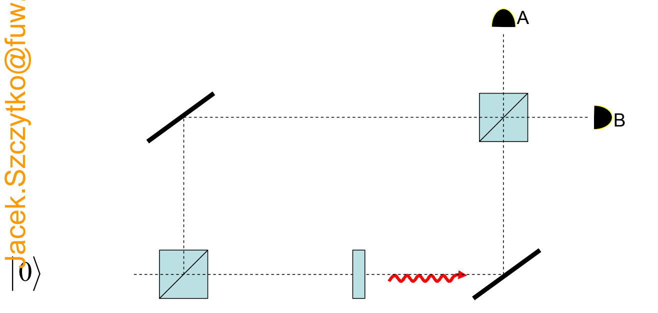


Interferometr Macha-Zendera

Bramki kubitowe

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

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

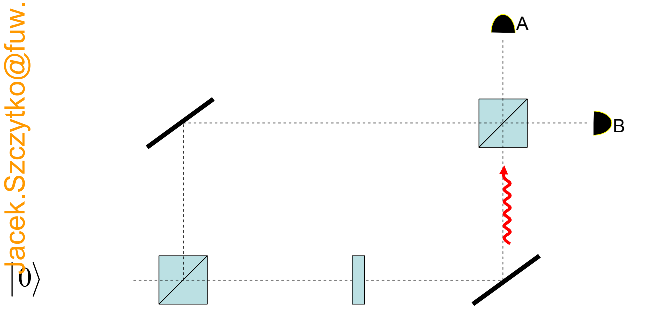


Interferometr Macha-Zendera

Bramki kubitowe

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

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

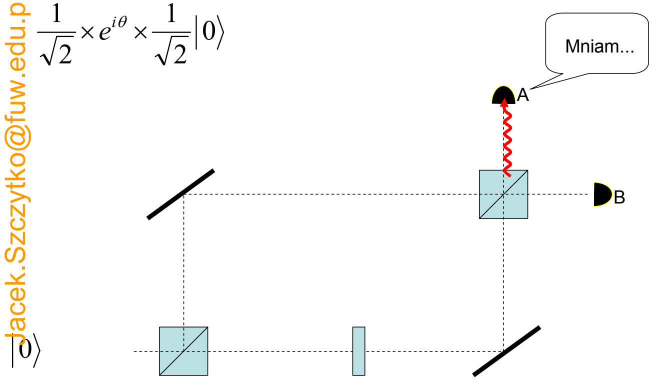


Interferometr Macha-Zendera

Bramki kubitowe

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

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

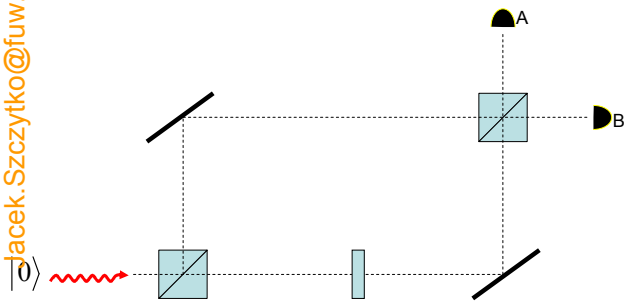


Interferometr Macha-Zendera

Bramki kubitowe

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

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

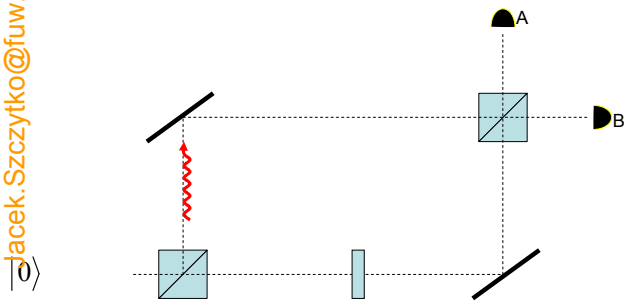


Interferometr Macha-Zendera

Bramki kubitowe

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

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

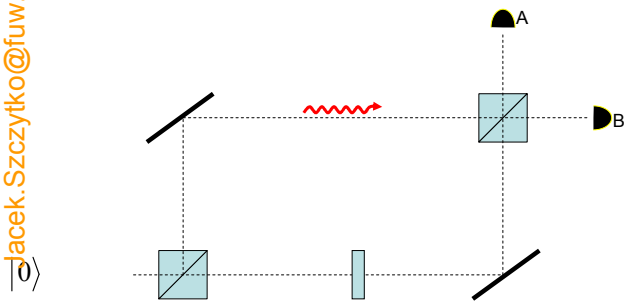


Interferometr Macha-Zendera

Bramki kubitowe

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

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

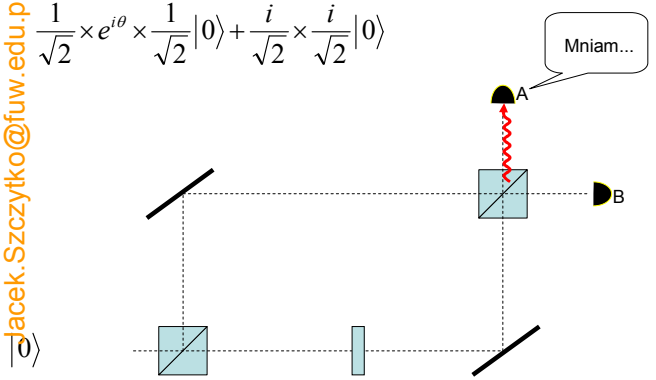


Interferometr Macha-Zendera

Bramki kubitowe

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

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

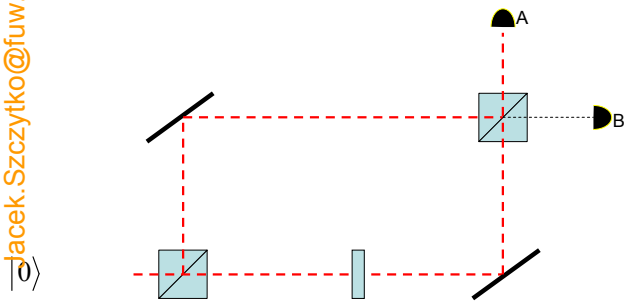


Interferometr Macha-Zendera

Bramki kubitowe

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

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



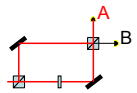
Interferometr Macha-Zendera

Bramki kubitowe

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

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

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

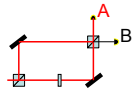


Bramki kubitowe

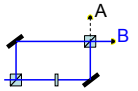
Jakie jest prawdopodobieństwo, że foton znajdzie się w detektorze A?

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

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



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

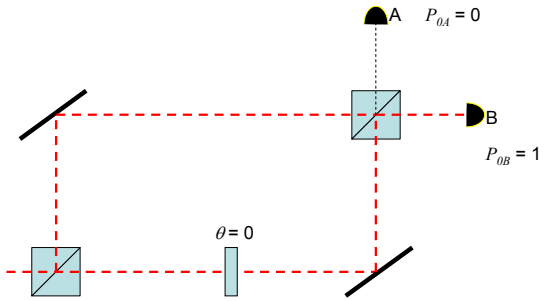


Dla $\theta=0$ mamy $P_{0A}=0$ i $P_{0B}=1$, a więc foton NIGDY nie trafi do detektora A, tylko na pewno trafi do B! Oczywiście dla $\theta=180^o$ jest odwrotnie!

Dygresja: pomiar BEZ oddziaływania

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

Foton interferuje SAM ZE SOBĄ!

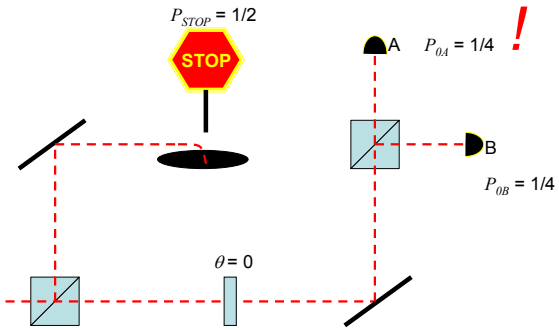


Interferometr Macha-Zendera

Dygresja: pomiar BEZ oddziaływania

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

Jacek.Szczytko@fuw.edu.pl

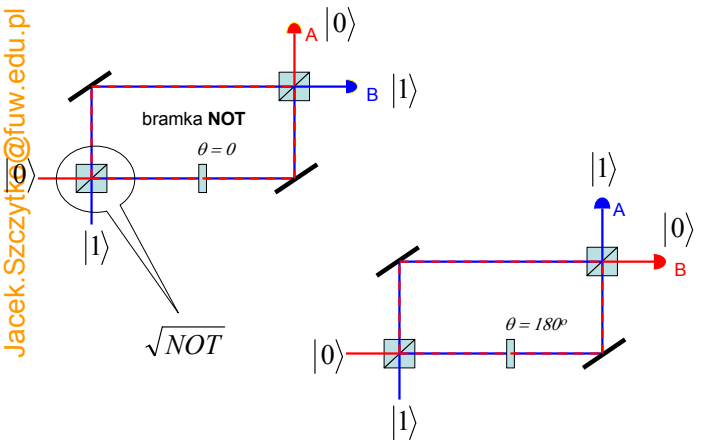


Interferometr Macha-Zendera

Bramki kubitowe

W zależności od fazy θ możemy otrzymać wynik:

Jacek.Szczytko@fuw.edu.pl

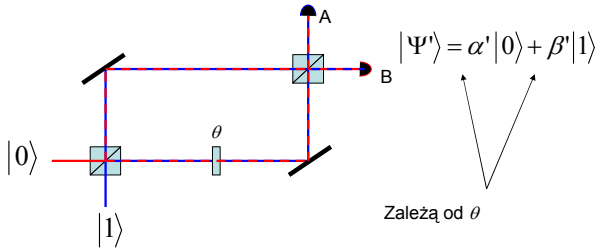


Bramki kubitowe

Jacek.Szczytko@fuw.edu.pl

Ogólnie

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



Matematycznie:

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

przekształcenie unitarne

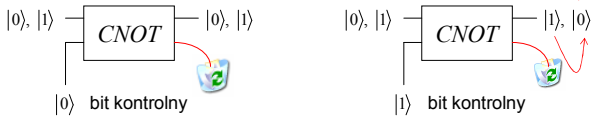
Bramki kubitowe

Jacek.Szczytko@fuw.edu.pl

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

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

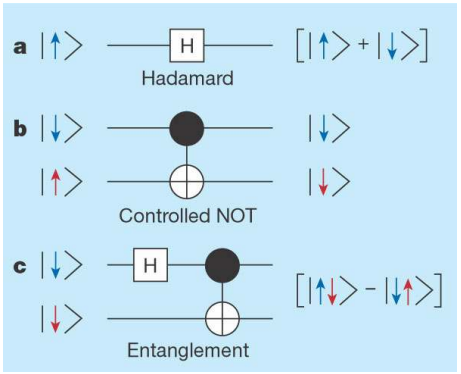
Bramki kwantowe muszą być odwracalne!



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

Bramki kubitowe

Jacek.Szczytko@fuw.edu.pl

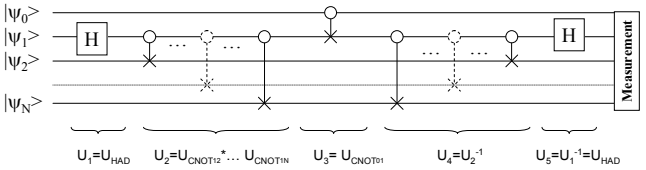


Quantum computing: The qubit duet
Gianni Blatter
Nature 421, 796-797 (20 February 2003)

Bramki kubitowe

Jacek.Szczytko@fuw.edu.pl

Program:



Różne pomysły

Jacek.Szczytko@fuw.edu.pl

…

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

Za tydzień!

Kwantowe procedury:

Jacek.Szczytko@fuw.edu.pl

Komputer klasyczny: $T_n(m)=p$

p = wynik

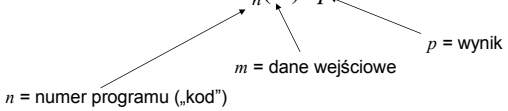
m = dane wejściowe

n = numer programu („kod”)

n = 00101110101101001001000111101101110101 1...
m = 01010010101010101111111100000000000000000...
p = 01010010101010101111111010000000000000000...

Kwantowe procedury:

Komputer klasyczny: $T_n(m)=p$

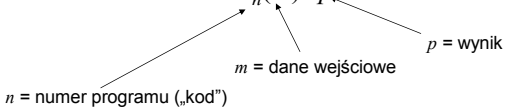


n = 00101110101101001001000111101101110101 1...
m = tak samo, ale zamiast bitów mamy kubity Ψ
p = 01010010101010101111110100000000000000...

Kwantowe procedury:

Jacek.Szczytko@fuw.edu.pl

Komputer klasyczny: $T_n(m)=p$



n = 00101110101101001001000111101101110101 1...
m = tak samo, ale zamiast bitów mamy kubity Ψ
p = 01010010101010101111110100000000000000...

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

Kwantowe procedury:

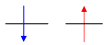
Jak zbudować rejestr z kubitów?

Jacek.Szczytko@fuw.edu.pl

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

Jeden kubit:

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

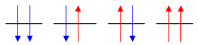


rejestr: $|\Psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$

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

Dla dwóch kubitów:

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

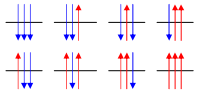


rejestr: $|\Psi\rangle = \alpha_{00}|0\rangle|0\rangle + \alpha_{01}|0\rangle|1\rangle + \alpha_{10}|1\rangle|0\rangle + \alpha_{11}|1\rangle|1\rangle$

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

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

itd..

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

Kwantowe procedury:

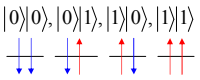
Jak zbudować rejestr z kubitów?

Jacek.Szczytko@fuw.edu.pl

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

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

Dla dwóch kubitów baza obliczeń:



Na przykład:

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

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

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

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

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

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**.

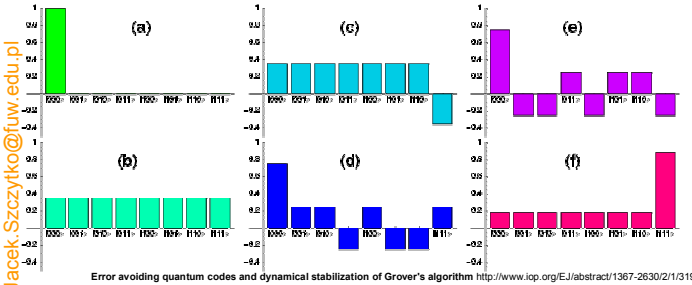
Pewne algorytmy będą działały szybciej na komputerze kwantowym.

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 intereferencji. Faza składników superpozycji kwantowej jest przygotowywana w ten sposób, aby najbardziej prawdopodobny wynik pomiaru odpowiadał interesującemu nas wynikowi.



Error avoiding quantum codes and dynamical stabilization of Grover's algorithm http://www.iop.org/EJ/abstract/1367-2630/2/1/319

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!

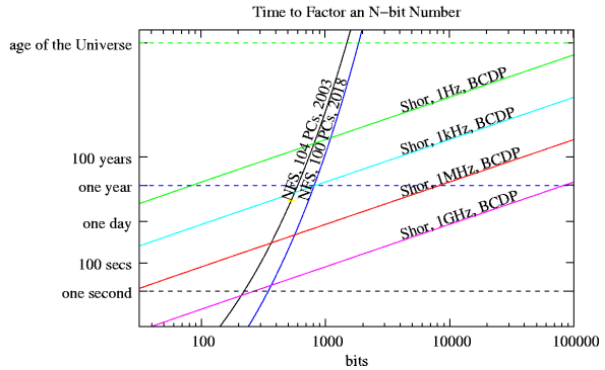
- W 1994 r. RSA 129 został złamany na 1600 stacjach roboczych w ciagu 8 miesiecy
- Algorytm kwantowy Petera Shora wymaga czasu $\sim (\ln N)^{2+\varepsilon}$

Komputer kwantowy, który faktoryzowałby liczbe 130 cyfrowa w ciagu miesiaca, sfaktoryzowałby liczbe 400 cyfrowa w czasie krótszym niz 3 lata

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

Algorytm Shora

Factoring Larger Numbers



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

Algorytm Shora

Jacek.Szczytko@fuw.edu.pl

Peter Shor

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

Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*

Peter W. Shor†

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 by 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, Abelian groups, quantum computation, foundations of quantum mechanics, spin systems, Fourier transforms

AMS subject classifications: 81P10, 11Y05, 68Q15, 81Q15

*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.

†AT&T Research, Room 2D-149, 600 Mountain Ave., Murray Hill, NJ 07974.

Algorytm Shora

Jacek.Szczytko@fuw.edu.pl

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

Kwantowa faktoryzacja

Chcemy sfaktoryzowac liczbe N, N = 15. Wybieramy liczbe losowa $1 < X < N - 1$ wzglednie pierwsza z N, tzn. taka, ze 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 operacje $B = X^A \bmod N$, wykorzystujac kwantowy paralelizm i wyniki umieszczamy w rejestrze B. Komputer kwantowy wykonuje taka operacje 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

• Zauwazamy, ze wyniki w rejestrze B sa okresowe z okresem r = 4

Komputer kwantowy potrafi szybko znajdowac okres funkcji!

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

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

15/3 = 5

15/5 = 3

Jacek.Szczytko@fuw.edu.pl

Algorytm Shora

Jacek.Szczytko@fuw.edu.pl

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

Kwantowa faktoryzacja

Chcemy sfaktoryzowac liczbe N, N = 15. Wybieramy liczbe losowa $1 < X < N - 1$ wzglednie pierwsza z N, tzn. taka, ze 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 operacje $B = X^A \bmod N$, wykorzystujac kwantowy paralelizm i wyniki umieszczamy w rejestrze B. Komputer kwantowy wykonuje taka operacje w jednym kroku!

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

• Zauwazamy, ze wyniki w rejestrze B sa okresowe z okresem r = 4

Komputer kwantowy potrafi szybko znajdowac okres funkcji!

Algorytm Shora

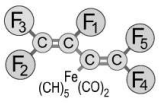
Jacek.Szczytko@fuw.edu.pl

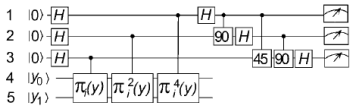
VOLUME 85, NUMBER 25 PHYSICAL REVIEW LETTERS 18 DECEMBER 2000

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

Lieven M.K. Vandersypen,[1,2,*] Matthias Steffen,[1,2] Gregory Breyta,[2]
Costantino S. Yannoni,[2] Richard Cleve,[3] and Isaac L. Chuang[2]
[1]*Solid State and Photonics Laboratory, Stanford University, Stanford, California 94305-4075*
[2]*IBM Almaden Research Center, San Jose, California 95120*
[3]*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

Algorytmy kwantowe

Jacek.Szczytko@fuw.edu.pl

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

Poważny problem

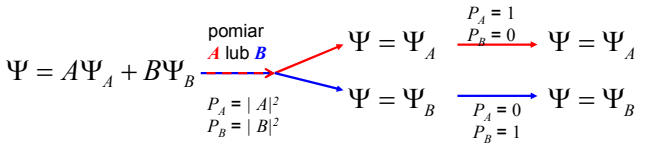
Jacek.Szczytko@fuw.edu.pl

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

Poważny problem

Jacek.Szczytko@fuw.edu.pl

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*)



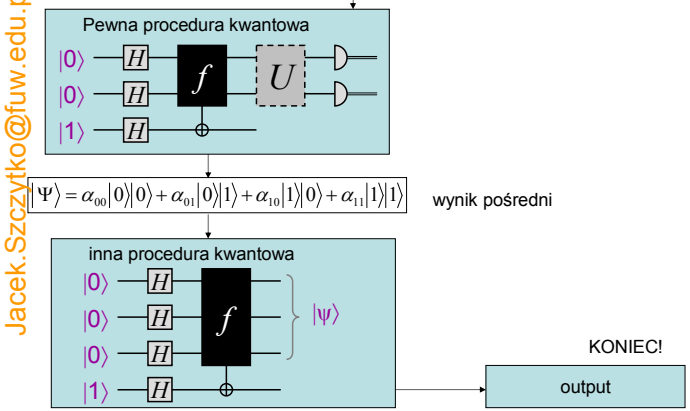
Zakaz klonowania sprawia, że nie można się dowiedzieć wartości każdej ze składowych A lub B z osobna.

„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 Ψ



Jacek.Szczytko@fuw.edu.pl

Poważny problem

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

input Ψ

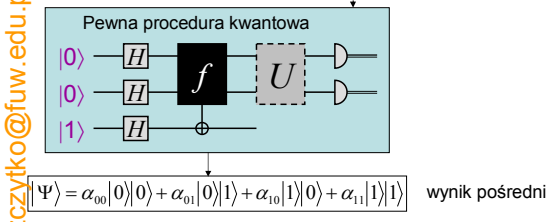
Tym razem z dekoherencją

Jacek.Szczytko@fuw.edu.pl

Poważny problem

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

input Ψ

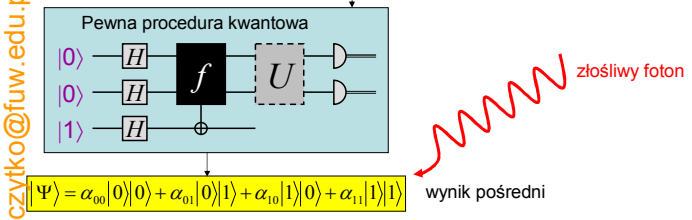


Jacek.Szczytko@fuw.edu.pl

Poważny problem

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

input Ψ

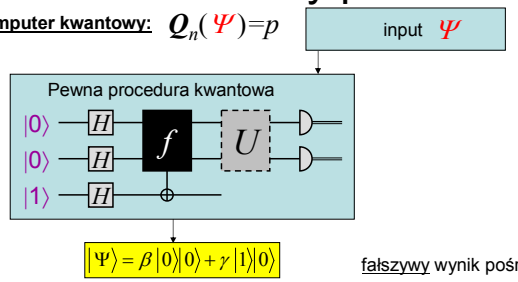


Jacek.Szczytko@fuw.edu.pl

Poważny problem

Jacek.Szczytko@fuw.edu.pl

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

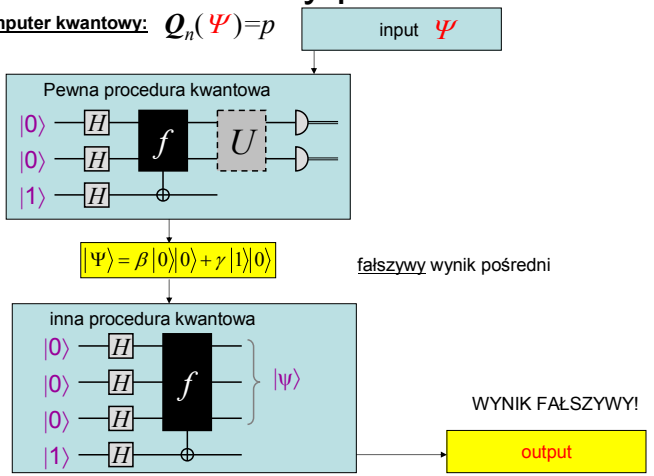


fałszywy wynik pośredni

Poważny problem

Jacek.Szczytko@fuw.edu.pl

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



fałszywy wynik pośredni

WYNIK FAŁSZYWY!

Poważny problem

Jacek.Szczytko@fuw.edu.pl

Rozwiązania:

1. Procedury kwantowej korekcji błędów

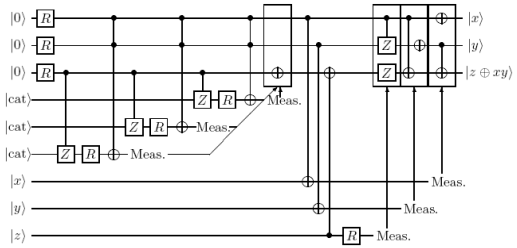


Figure 12: The fault-tolerant Toffoli gate. Each line represents a block of 7 qubits, and the gates are implemented transversally. For each measurement, the arrow points to the set of gates that is to be applied if the measurement outcome is 1; no action is taken if the outcome is 0.

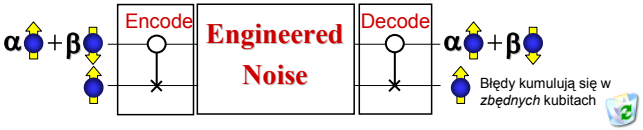
J. Preskill quant-ph/9705031

Poważny problem

Jacek.Szczytko@fuw.edu.pl

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

Nowe podejścia

Jacek.Szczytko@fuw.edu.pl

ELSEVIER

Available online at www.sciencedirect.com
SCIENCE DIRECT®

Theoretical Computer Science 320 (2004) 15–33

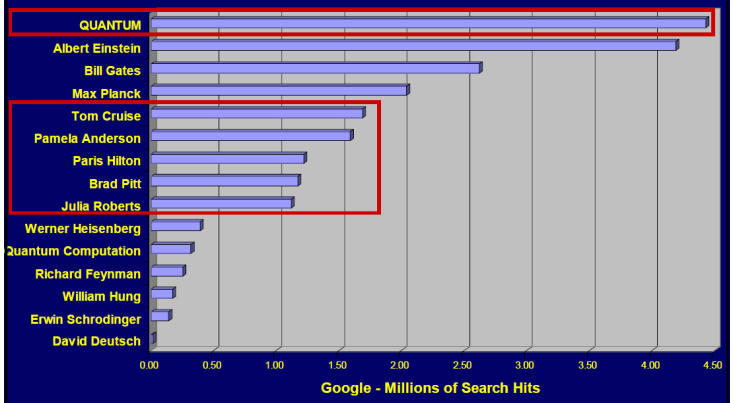
Theoretical Computer Science
www.elsevier.com/locate/tcs

Quantum computing without entanglement☆

Eli Biham[a], Gilles Brassard[b], Dan Kenigsberg[a], Tal Mor[a]

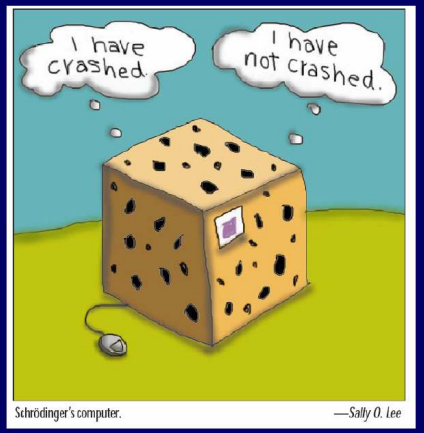
[a]*Computer Science Department, Technion, Haifa 32000, Israel*
[b]*Département d'informatique et de recherche opérationnelle, Université de Montréal, Montréal, Qué., Canada, H3C 3J7*

Quantum is Sexy



http://www.mitstanfordberkeleynano.org/events_past/0406%20-%20QC/Richard%20Gordon.pdf

Qwindows 2098



W przyszłym tygodniu

Komputery kwantowe

Jacek.Szczytko@fuw.edu.pl

Świat Nauki 08.1998

HARDWARE