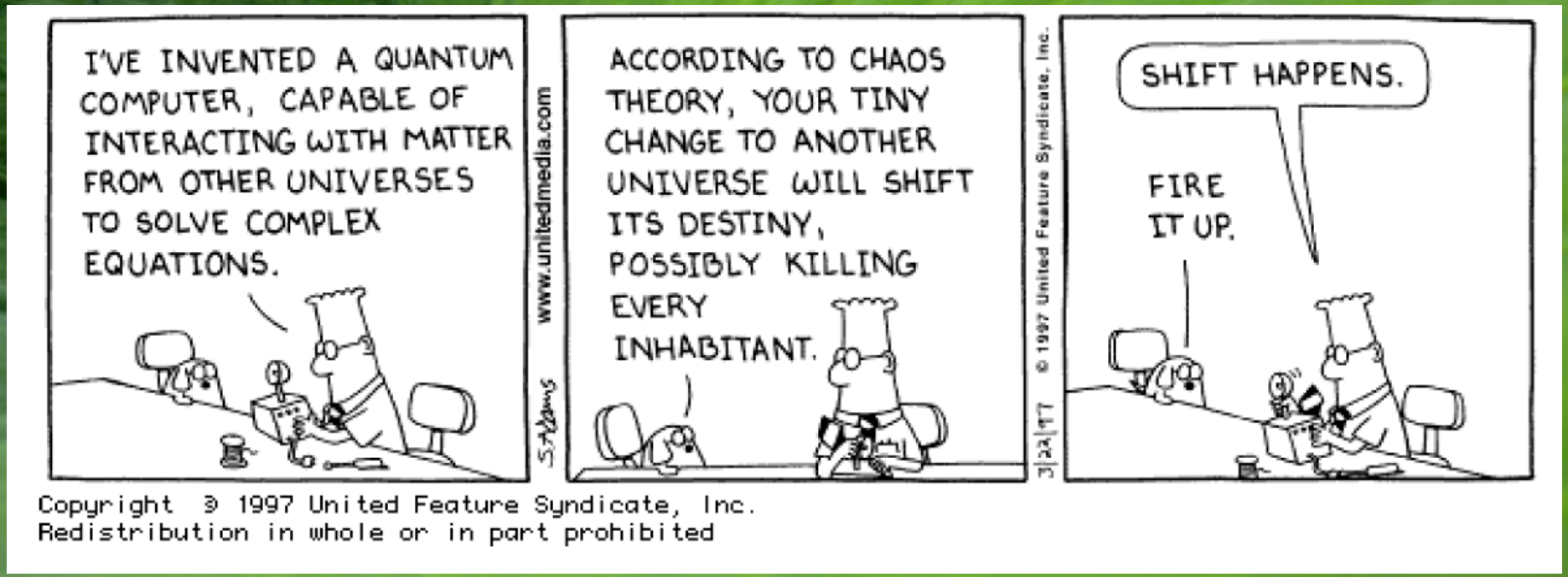
Obliczenia kwantowe



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?

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"

"Komputer kwantowy nigdy nie zadziała" - Onet.pl Wiadomości - 02.12.2006 - Mozilla Firefox

Plik Edycja Widok Przejdź Zakładki Narzędzia Pomoc

http://wiadomosci.onet.pl/1443239,18,1,1,,item.html

Idź

Getting Started Latest Headlines Wiadomości - Gazeta.pl INTERIA.PL - Fakty Tabela NBP Slownik Ang. Slownik Fra. Google Desktop

Internet i komputery

PAP, msu /02.12.2006 19:41

"Komputer kwantowy nigdy nie zadziała"

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

Naukowcy od dawna roztaczają olśniewające 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 wysiłki 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.

« Po wyborach...
Satyryczny komentarz polityczny
rys. Jerzy Krzętowski/Jurek.pl

SONDA

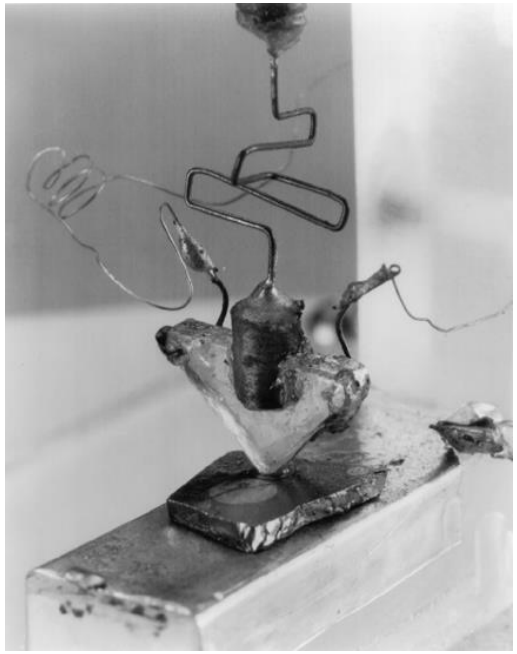
Który minister Twoim zdaniem pracuje najgorzej?

- Andrzej Aumiller
- Ludwik Dorn
- Anna Fotyga
- Grażyna Gęsicka
- Roman Giertych
- Zyta Gilowska
- Przemysław Gosiewski
- Wojciech Jasiński
- Anna Kalata
- Andrzej Lepper

Zakończono

Disabled

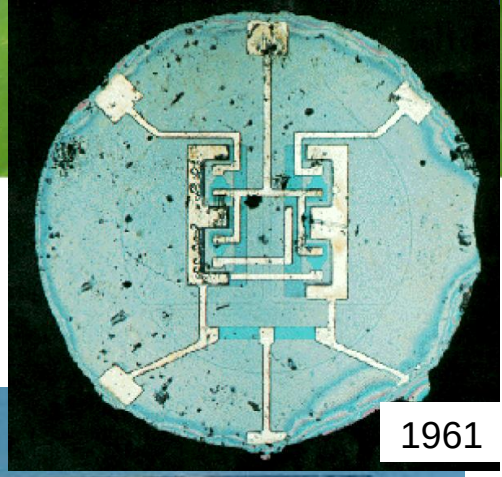
Jak działa tranzystor?

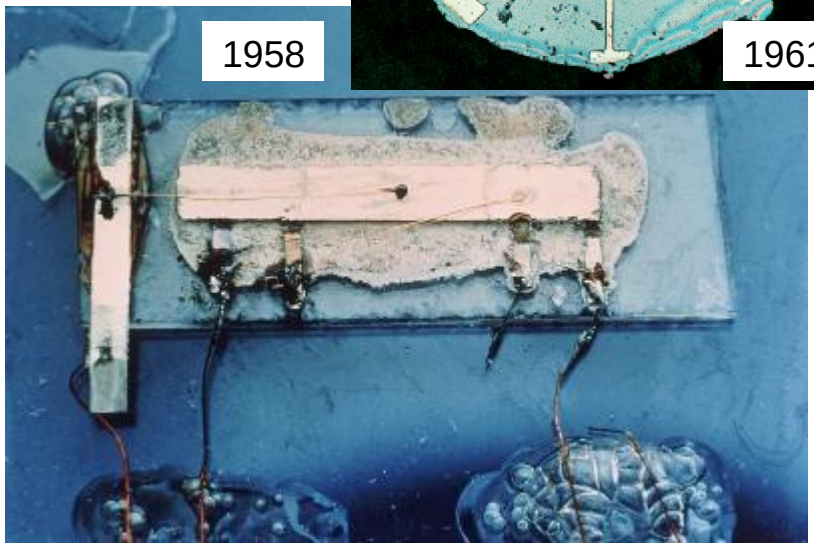


1948 – William Schockley, John Bardeen oraz Walter Brattain z Bell Labs wymyślają tranzystor (Nobel 1956)

Źródło: http://www.facsnet.org/tools/sci_tech/tech/applications/chipsys.php3 http://www.lucent.com/minds/transistor/history.html , http://www.pbs.org/transistor/science/events/pointctrans.html

Trochę historii


1961


1958

1955 Shockley Semiconductor – pierwsza firma w Palo Alto (krzemowej dolinie)
Rok 1956
IBM tworzy pierwszy dysk twardy - RAMAC 350. Jego pojemność to 5MB,natomiast cena - milion dolarów.
W laboratoriach MIT ukończony zostaje pierwszy komputer tranzystorowy.
A. Newell, D. Shaw i F. Simon wynajdują IPL (Information Processing Language - język przetwarzania informacji).

1957 Fairchild Semiconductor – na skutek nieporozumień z Shockleyem odchodzą z firmy: Julius Blank, Victor Grinich, Gordon E. Moore, Robert W. Noyce, Jean Hoerni, Gene Kleiner, Jay Last, Sheldon Roberts **(„zdradziecka 8-ka").**

Ken Olsen i Harlan Anderson zakładają firmę DEC (Digital Equipment Corporation).

Oficjalnie opublikowany zostaje język FORTRAN-1, stworzony przez Johna Backusa i jego współpracowników z IBM. FORTRAN używa zapisu podobnego do tego z algebry. Dlatego też język ten stanie się popularny, szczególnie wśród naukowców i techników.

1958 Pierwszy układ scalony (IC – Integrated Circuit) wykonany przez Jack Kilby na germanie w **Texas Instruments** (2000 Nagroda Nobla z fizyki). Niezależnie Robert Noyce (**Fairchild**) zbudował IC na krzemie.

Źródło: http://www.facsnet.org/tools/sci_tech/tech/applications/chipsys.php3 http://www.lucent.com/minds/transistor/history.html

Obliczenia kwantowe

http://www.gizmag.com/first-electronic-quantum-processor/12125/

Obliczenia kwantowe

Pierwszy komercyjny komputer kwantowy - sprzedany - Mozilla Firefox

Plik Edycja Widok Historia Zakładki Narzędzia Pomoc

Pierwszy komercyjny komputer kwanto...

http://technologie.gazeta.pl/internet/1,104530,9684065,Pierwszy_komercyjny_komputer_kwantowy__sprzedany.html

Gazeta.pl | Technologie | Poczta | Forum | Blogi | Wyborcza.pl

Gazeta.pl Technologie

Szukaj

Program TV | Newsletter

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

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

Polecamy | Aplikacje mobilne | Tablety | Komputer w firmie

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

Volkswagen Aqua - poduszkowiec dla Chin

Czy Samsung D7000 jest idealny? [test]

Janusz A. Urbanowicz | 28.05.2011 15:27

Pierwszy komercyjny komputer kwantowy - sprzedany

Lubię to! 126

Komentuj, dodawaj zdjęcia i znajomych!

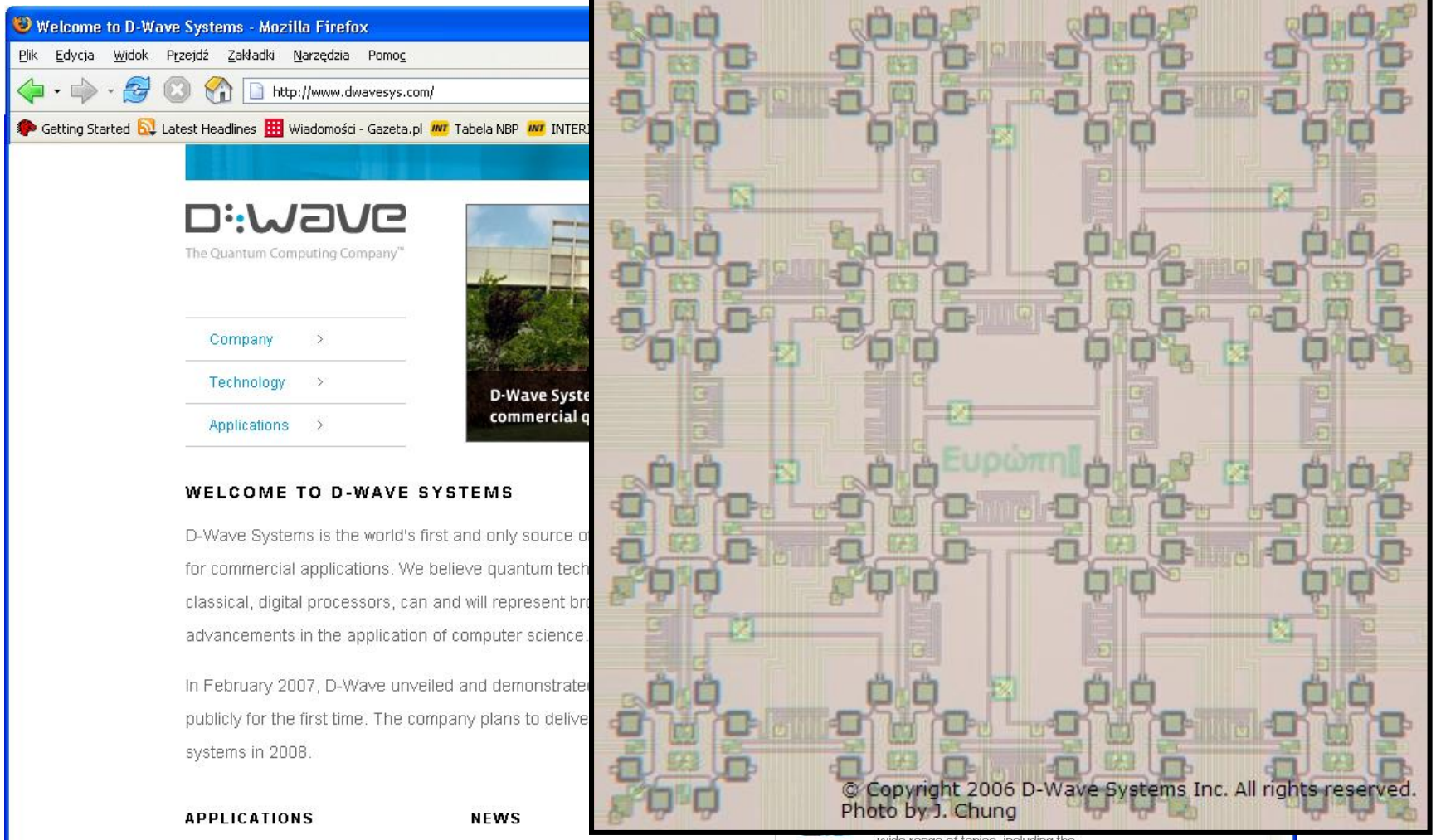
Zaloguj się | Nie masz u nas konta? Zarejestruj się

Najczęściej czytane

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

Quantum Computer II (QC)

HARDWARE



Obliczenia kwantowe

IBM Puts a Quantum Processor in the Cloud

By Rachel Courtland
Posted 4 May 2016 | 4:02 GMT

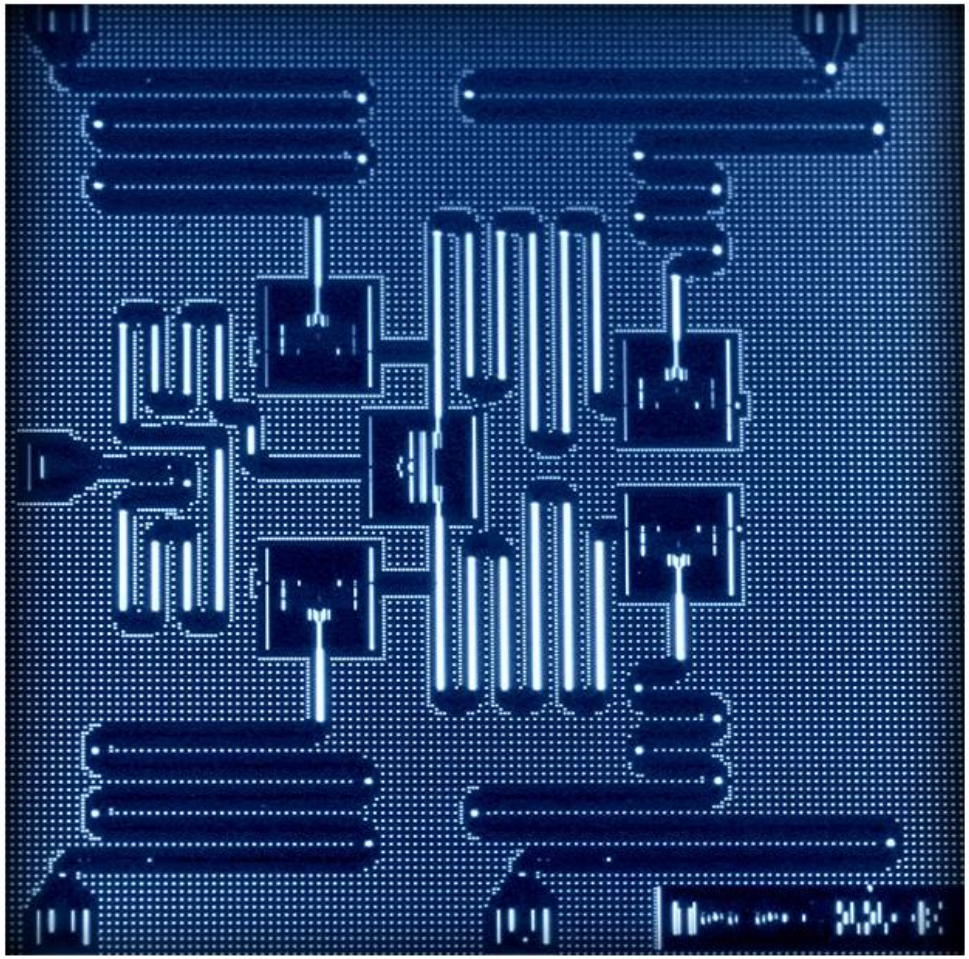


Photo: IBM Research

IBM Puts a Quantum Processor in the Cloud
By Rachel Courtland
Posted 4 May 2016 | 4:02 GMT
Photo: IBM Research

IBM announced today that it is making one of its superconducting quantum processors accessible over the Internet. Those itching to try out such hardware will be able to get hands-on experience through a new quantum computing platform—at least, the experience will be as hands-on as it can be with hardware sealed inside a remote dilution refrigerator and cooled to a fraction of a degree above absolute zero.

With just five qubits, the chip won't let you rapidly factor large numbers in order to break encryption. In fact, a classical simulation of this system takes less time to run, says Jay Gambetta, manager of the Theory of Quantum Computing and Information Group at IBM's Thomas J. Watson Research Center in Yorktown Heights, N.Y.
img
Photo: IBM Research
IBM is offering software that will let people run a five-qubit quantum processor from any computer or mobile device. Proximity to a dilution refrigerator not required.

But the goal of this tool, says Gambetta, "is to get people to start thinking quantum, to start thinking in terms of how a quantum computer works. Most people think quantum is hard or it's spooky or it's different. And yes it's different, but it's actually not hard."

http://spectrum.ieee.org/tech-talk/computing/hardware/ibm-puts-a-quantum-processor-in-the-cloud

CES 2018: IBM przywiózł do Las Vegas 50-kubitowy komputer kwantowy

Wintermute 10 stycznia 2018 5 komentarzy

Kwantowe maszyny przestają być tylko laboratoryjną, futurystyczną osobliwością. Najpierw Intel, a teraz IBM pokazują swoje urządzenia, oparte o tę nowoczesną i zapowiadaną od dawna technologię. Komputer skonstruowany przez IBM potrzebuje do pracy temperatury 10 milikelwinów.

Komputery kwantowe z klasycznymi komputerami łączy tylko jedno – nazwa. Pod względem konstrukcyjnym, zasady działania, architektury czy wreszcie wzornictwa to zupełnie inne urządzenia. Swój 49-kubitowy procesor kwantowy na Consumer Electronics Show pokazał już Intel – pisał o tym Jacek Tomczyk. Teraz IBM demonstruje nie tylko QPU (Quantum Processing Unit), ale cały komputer kwantowy.

CZYTAJ RÓWNIEŻ

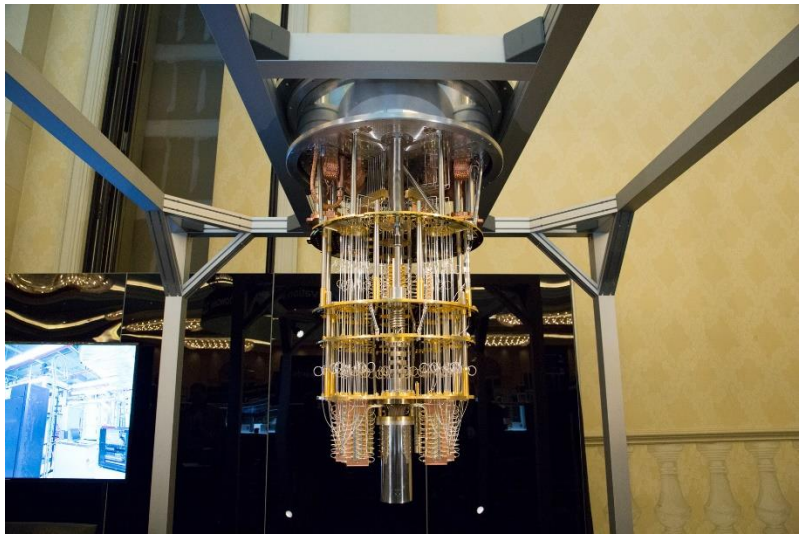
CES 2018: Razer Linda czyli smartfon, który zmienia się w laptopa

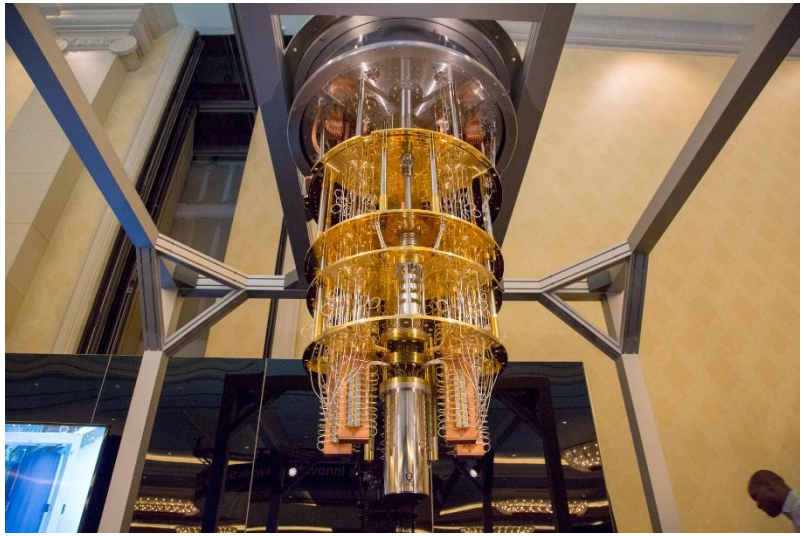
12

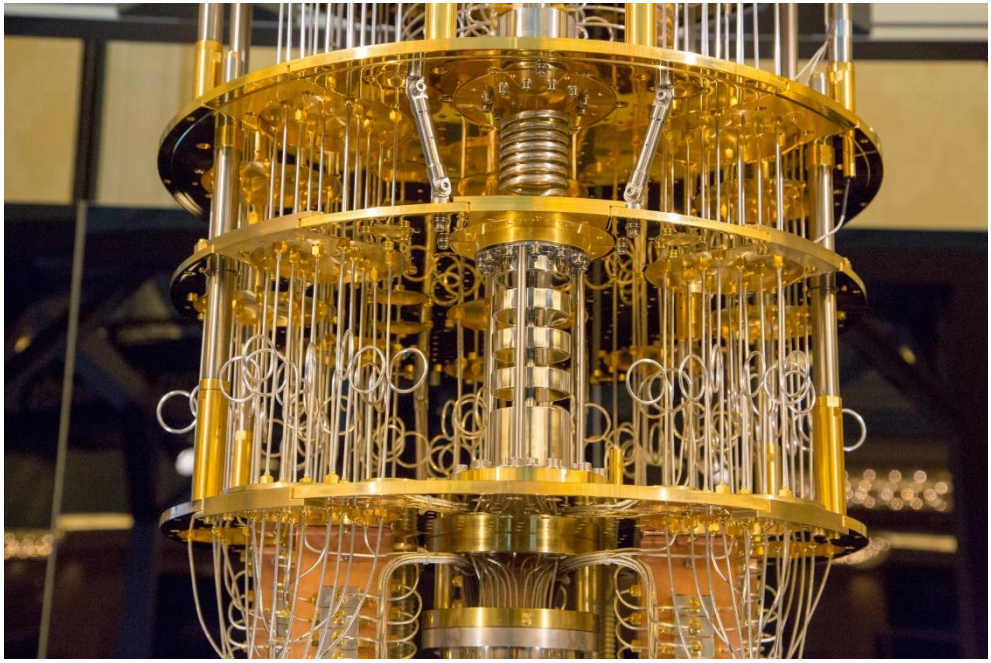
Ewakuacja Apple Store, straż pożarna, policja i karetki – z powodu baterii

http://www.chip.pl/2018/01/ces-2018-ibm-przywiozl-las-vegas-50-kubitowy-komputer-kwantowy/

Obliczenia kwantowe

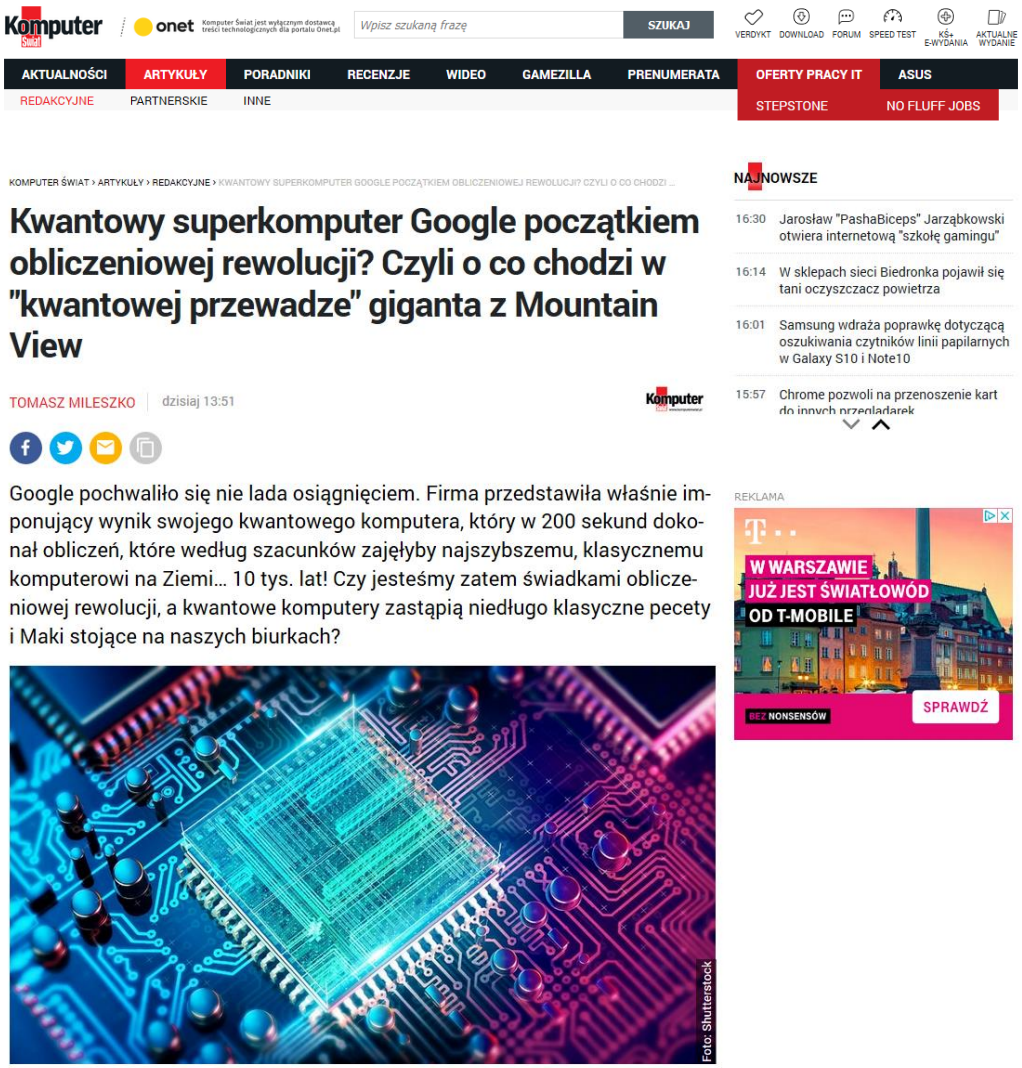






http://www.chip.pl/2018/01/ces-2018-ibm-przywiozl-las-vegas-50-kubitowy-komputer-kwantowy/

Obliczenia kwantowe



Komputer Świat | onet | Wpisz szukaną frazę | SZUKAJ

VERDYKT DOWNLOAD FORUM SPEED TEST KŚ+ E-WYDANIA AKTUALNE WYDANIE

AKTUALNOŚCI ARTYKUŁY PORADNIKI RECENZJE WIDEO GAMEZILLA PRENUMERATA OFERTY PRACY IT ASUS

REDAKCYJNE PARTNERSKIE INNE STEPSTONE NO FLUFF JOBS

KOMPUTER ŚWIAT › ARTYKUŁY › REDAKCYJNE › KWANTOWY SUPERKOMPUTER GOOGLE POCZĄTKIEM OBLICZENIOWEJ REWOLUCJI? CZYLI O CO CHODZI ...

Kwantowy superkomputer Google początkiem obliczeniowej rewolucji? Czyli o co chodzi w "kwantowej przewadze" giganta z Mountain View

TOMASZ MILESZKO | dzisiaj 13:51

Google pochwaliło się nie lada osiągnięciem. Firma przedstawiła właśnie imponujący wynik swojego kwantowego komputera, który w 200 sekund dokonał obliczeń, które według szacunków zajęłyby najszybszemu, klasycznemu komputerowi na Ziemi... 10 tys. lat! Czy jesteśmy zatem świadkami obliczeniowej rewolucji, a kwantowe komputery zastąpią niedługo klasyczne pecety i Maki stojące na naszych biurkach?

Foto: Shutterstock

NAJNOWSZE

16:30 Jarosław "PashaBiceps" Jarząbkowski otwiera internetową "szkołę gamingu"

16:14 W sklepach sieci Biedronka pojawił się tani oczyszczacz powietrza

16:01 Samsung wdraża poprawkę dotyczącą oszukiwania czytników linii papilarnych w Galaxy S10 i Note10

15:57 Chrome pozwoli na przenoszenie kart do innych przeglądarek

REKLAMA

24.10.2019

https://www.komputerswiat.pl/artykuly/redakcyjne/kwantowy-superkomputer-google-poczatkiem-obliczeniowej-rewolucji-czyli-o-co-chodzi-w/937e5r1

Quantum supremacy

Article

Quantum supremacy using a programmable superconducting processor

https://doi.org/10.1038/s41586-019-1666-5

Received: 22 July 2019

Accepted: 20 September 2019

Published online: 23 October 2019

Frank Arute[1], Kunal Arya[1], Ryan Babbush[1], Dave Bacon[1], Joseph C. Bardin[1,2], Rami Barends[1], Rupak Biswas[3], Sergio Boixo[1], Fernando G. S. L. Brandao[1,4], David A. Buell[1], Brian Burkett[1], Yu Chen[1], Zijun Chen[1], Ben Chiaro[5], Roberto Collins[1], William Courtney[1], Andrew Dunsworth[1], Edward Farhi[1], Brooks Foxen[1,5], Austin Fowler[1], Craig Gidney[1], Marissa Giustina[1], Rob Graff[1], Keith Guerin[1], Steve Habegger[1], Matthew P. Harrigan[1], Michael J. Hartmann[1,6], Alan Ho[1], Markus Hoffmann[1], Trent Huang[1], Travis S. Humble[7], Sergei V. Isakov[1], Evan Jeffrey[1], Zhang Jiang[1], Dvir Kafri[1], Kostyantyn Kechedzhi[1], Julian Kelly[1], Paul V. Klimov[1], Sergey Knysh[1], Alexander Korotkov[1,8], Fedor Kostritsa[1], David Landhuis[1], Mike Lindmark[1], Erik Lucero[1], Dmitry Lyakh[9], Salvatore Mandrà[3,10], Jarrod R. McClean[1], Matthew McEwen[5], Anthony Megrant[1], Xiao Mi[1], Kristel Michielsen[11,12], Masoud Mohseni[1], Josh Mutus[1], Ofer Naaman[1], Matthew Neeley[1], Charles Neill[1], Murphy Yuezhen Niu[1], Eric Ostby[1], Andre Petukhov[1], John C. Platt[1], Chris Quintana[1], Eleanor G. Rieffel[3], Pedram Roushan[1], Nicholas C. Rubin[1], Daniel Sank[1], Kevin J. Satzinger[1], Vadim Smelyanskiy[1], Kevin J. Sung[1,13], Matthew D. Trevithick[1], Amit Vainsencher[1], Benjamin Villalonga[1,14], Theodore White[1], Z. Jamie Yao[1], Ping Yeh[1], Adam Zalcman[1], Hartmut Neven[1] & John M. Martinis[1,5*]

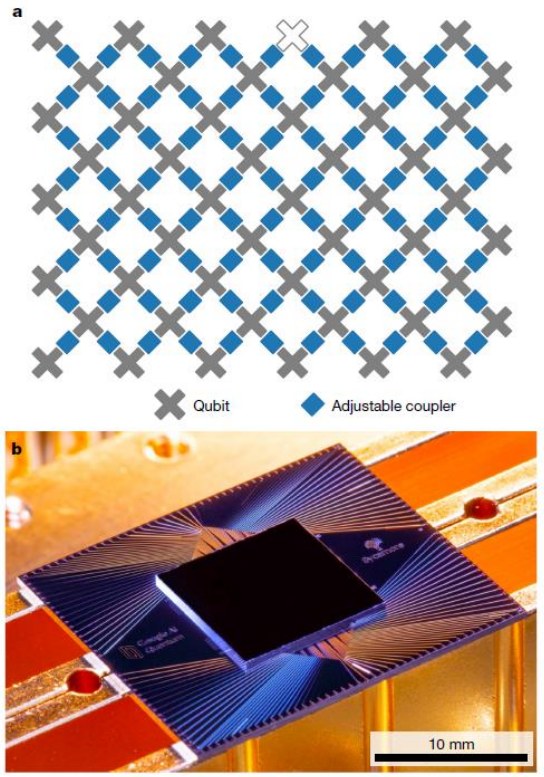


Fig. 1 | The Sycamore processor. a, Layout of processor, showing a rectangular array of 54 qubits (grey), each connected to its four nearest neighbours with couplers (blue). The inoperable qubit is outlined. **b**, Photograph of the Sycamore chip.

Nature **volume 574**, pages505–510 (2019)

Electronic states

LETTER

Nature 549, 242 (2017)

doi:10.1038/nature23879

Hardware-efficient variational quantum eigensolver for small molecules and quantum magnets

Abhinav Kandala[1]*, Antonio Mezzacapo[1]*, Kristan Temme[1], Maika Takita[1], Markus Brink[1], Jerry M. Chow[1] & Jay M. Gambetta[1]

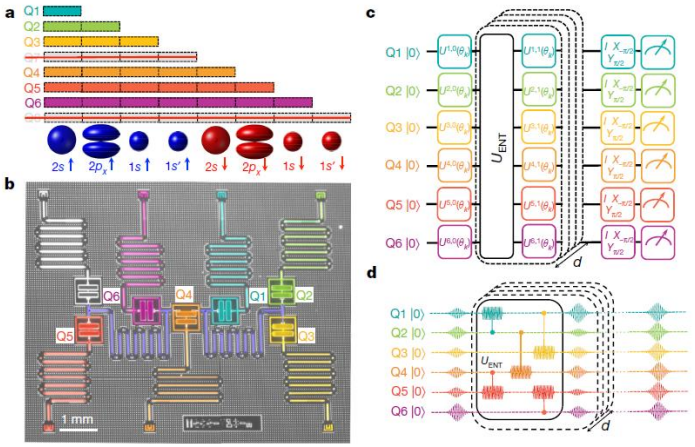


Figure 1 | Quantum chemistry on a superconducting quantum processor. Solving electronic-structure problems on a quantum computer relies on mappings between fermionic and qubit operators. **a**, Parity mapping of eight spin orbitals (drawn in blue and red, not to scale) onto eight qubits, which are then reduced to six qubits owing to fermionic spin and parity symmetries. The length of the bars indicate the parity of the spin orbitals that are encoded in each qubit. **b**, False-coloured optical micrograph of the superconducting quantum processor with seven transmon qubits. These qubits are coupled via two coplanar waveguide resonators (violet) and have individual coplanar waveguide resonators for control and read-out. **c**, Hardware-efficient quantum circuit for trial-state preparation and energy estimation, shown here for six qubits. For each iteration k, the circuit is composed of a sequence of interleaved single-qubit rotations $U^{q,d}(\boldsymbol{\theta}_k)$ and entangling unitary operations U_{ENT} that entangle all of the qubits in the circuit. A final set of post-rotations (I, $X_{-\pi/2}$ or $Y_{\pi/2}$) before the qubits are read out is used to measure the expectation values of the individual Pauli terms in the Hamiltonian and to estimate the energy of the trial state. **d**, An example of the pulse sequence for the preparation of a six-qubit trial state, in which U_{ENT} is implemented as a sequence of two-qubit cross-resonance gates.

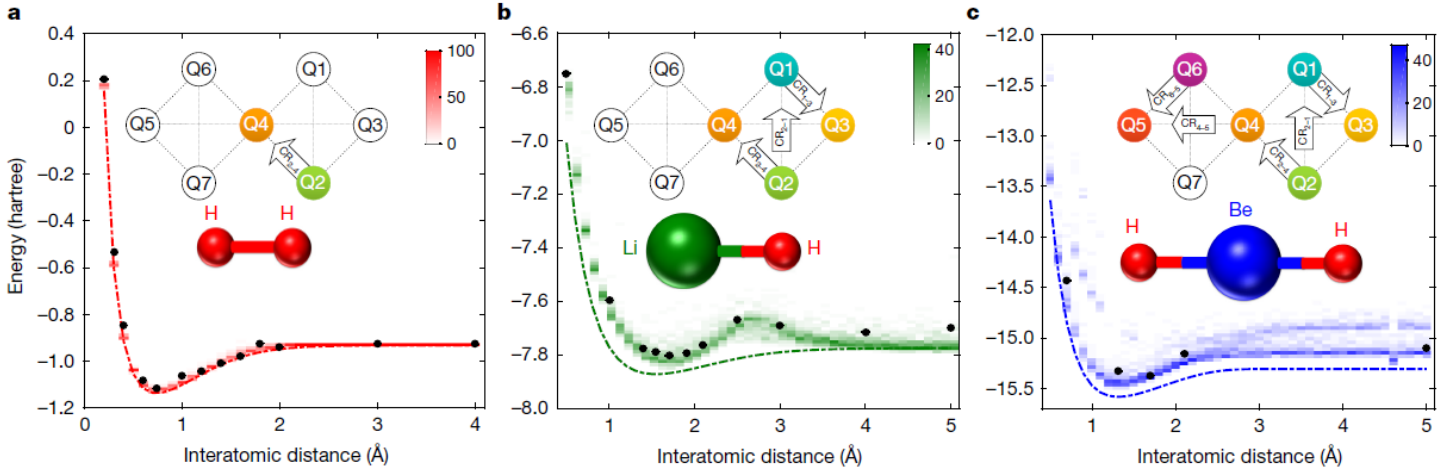


Figure 3 | Application to quantum chemistry. a–c, Experimental results (black filled circles), exact energy surfaces (dotted lines) and density plots (shading; see colour scales) of outcomes from numerical simulations, for several interatomic distances for H_2 (**a**), LiH (**b**) and BeH_2 (**c**). The experimental and numerical results presented are for circuits of depth $d = 1$. The error bars on the experimental data are smaller than the size of the markers. The density plots are obtained from 100 numerical outcomes at each interatomic distance. The top insets in each panel highlight the qubits used for the experiment and the cross-resonance gates (arrows, labelled CR_{c-t}; where 'c' denotes the control qubit and 't' the target qubit) that constitute U_{ENT}. The bottom insets are representations of the molecular geometry (not to scale). For all the three molecules, the deviation of the experimental results from the exact curves is well explained by the stochastic simulations.

Electronic states

PHYSICAL REVIEW X 8, 011021 (2018)

Featured in Physics

Computation of Molecular Spectra on a Quantum Processor with an Error-Resilient Algorithm

J. I. Colless, V. V. Ramasesh, D. Dahlen, M. S. Blok, and M. E. Kimchi-Schwartz‡
Quantum Nanoelectronics Laboratory, Department of Physics, University of California, Berkeley, California 94720, USA; and Center for Quantum Coherent Science, University of California, Berkeley, California 94720, USA

J. R. McClean,† J. Carter, and W. A. de Jong
Computational Research Division, Lawrence Berkeley National Laboratory, Berkeley, California 94720, USA

I. Siddiqi*
Quantum Nanoelectronics Laboratory, Department of Physics, University of California, Berkeley, California 94720, USA; Center for Quantum Coherent Science, University of California, Berkeley, California 94720, USA; and Materials Science Division, Lawrence Berkeley National Laboratory, Berkeley, California 94720, USA

(Received 7 August 2017; published 12 February 2018)

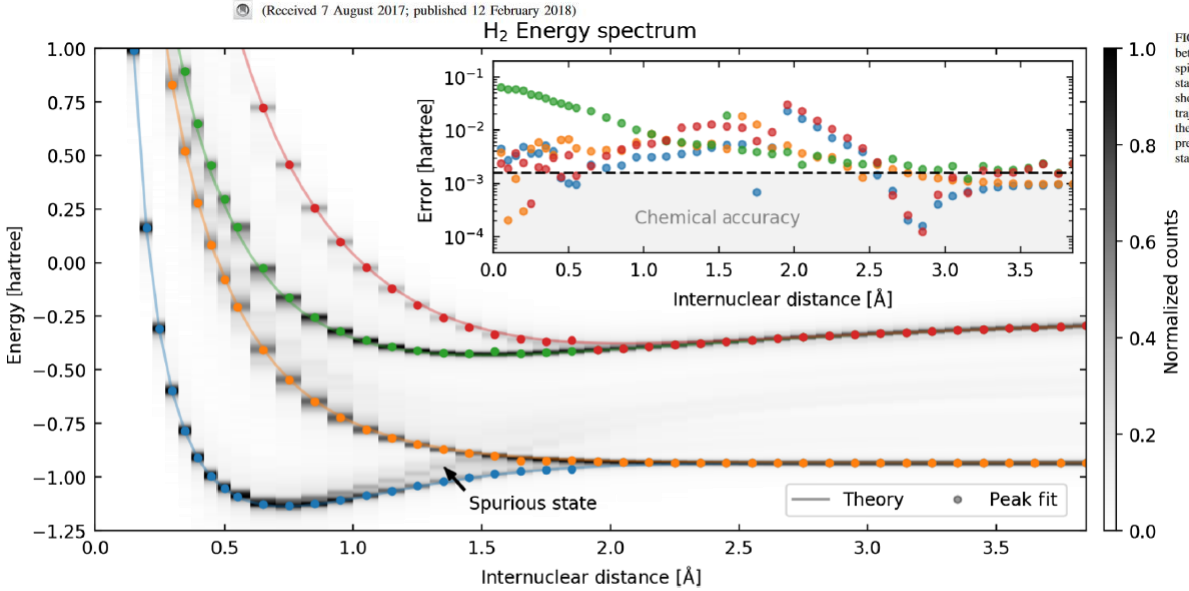


FIG. 3. H_2 energy spectrum as a function of internuclear distance. Swarm particle energies for each bond length are histogrammed after application of a linear-response expansion and Gaussian filter. Energy estimates obtained by a peak finding routine are indicated by dots with theoretically predicted energy levels shown as solid lines. An unphysical spurious state emerges at internuclear distances greater than ~1.2 Å due to uncorrected incoherent errors. Inset shows errors in the estimated ground- and excited-state energies as compared to chemical accuracy (1.6×10^{-3} Ha).

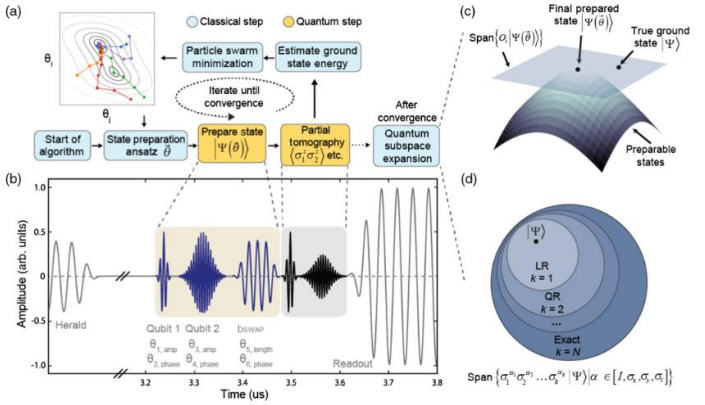


FIG. 1. Description of the variational quantum eigensolver algorithm and associated quantum subspace expansion. (a) Mapping between qubit states and electronic states of the hydrogen molecule in the STO-3G basis. As the molecular Hamiltonian preserves total spin projection, the four states with $s_z = 0$ (dashed box) decouple from the other two. These four are mapped to the four two-qubit basis states. (b) Flow chart outline of the algorithm with classical resources colored in blue and quantum resources colored in yellow. Inset shows a cartoon example of the swarm minimization process with equal-energy contours shown in gray scale and 5 swarm particle trajectories (colored). (c) Cartoon of the QSE protocol; operators from O_i are used to expand about the variational solution provided by the VQE, allowing for the mitigation of incoherent errors that otherwise render the true ground state inaccessible. (d) Typical qubit preparation and measurement sequence consisting of a projective heralding measurement (on which we later postselect so that the qubits start in the state $|00\rangle$), single-qubit and two-qubit pulses, tomography pulses, and finally a projective readout.

Phys. Rev X 8 011021 (2018)

Electronic states

nature COMMUNICATIONS

ARTICLE

https://doi.org/10.1038/s41467-019-10988-2 OPEN

An adaptive variational algorithm for exact molecular simulations on a quantum computer

Harper R. Grimsley[1], Sophia E. Economou[2], Edwin Barnes[2] & Nicholas J. Mayhall[1]

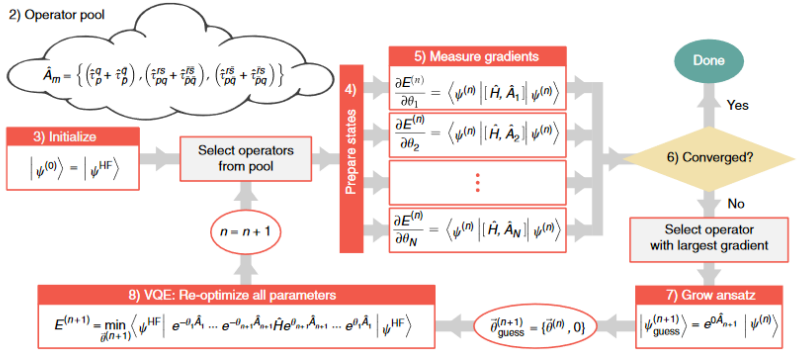


Fig. 1 Schematic depiction of the ADAPT-VQE algorithm described presented. Since step 1 occurs on classical hardware, it is not included in the illustration. $\vec{\theta}^{(n)}$ is the list of ansatz parameters at the *n*th iteration. The number of parameters, $len(\vec{\theta}^{(n)})$, is equal to the number of operators in the ansatz. "Operator Pool" refers to the collection of operators which are used to grow the ansatz one-at-a-time. Each τ^q_p represents a generalized single or double excitation, and these operators are then spin-complemented. The orbital indices refer to spatial orbitals, and the overbar indicates β spin. Orbital indices without overbars have α spin. Note that growing the ansatz does not drain the pool, and so operators can show up multiple times if selected by the algorithm

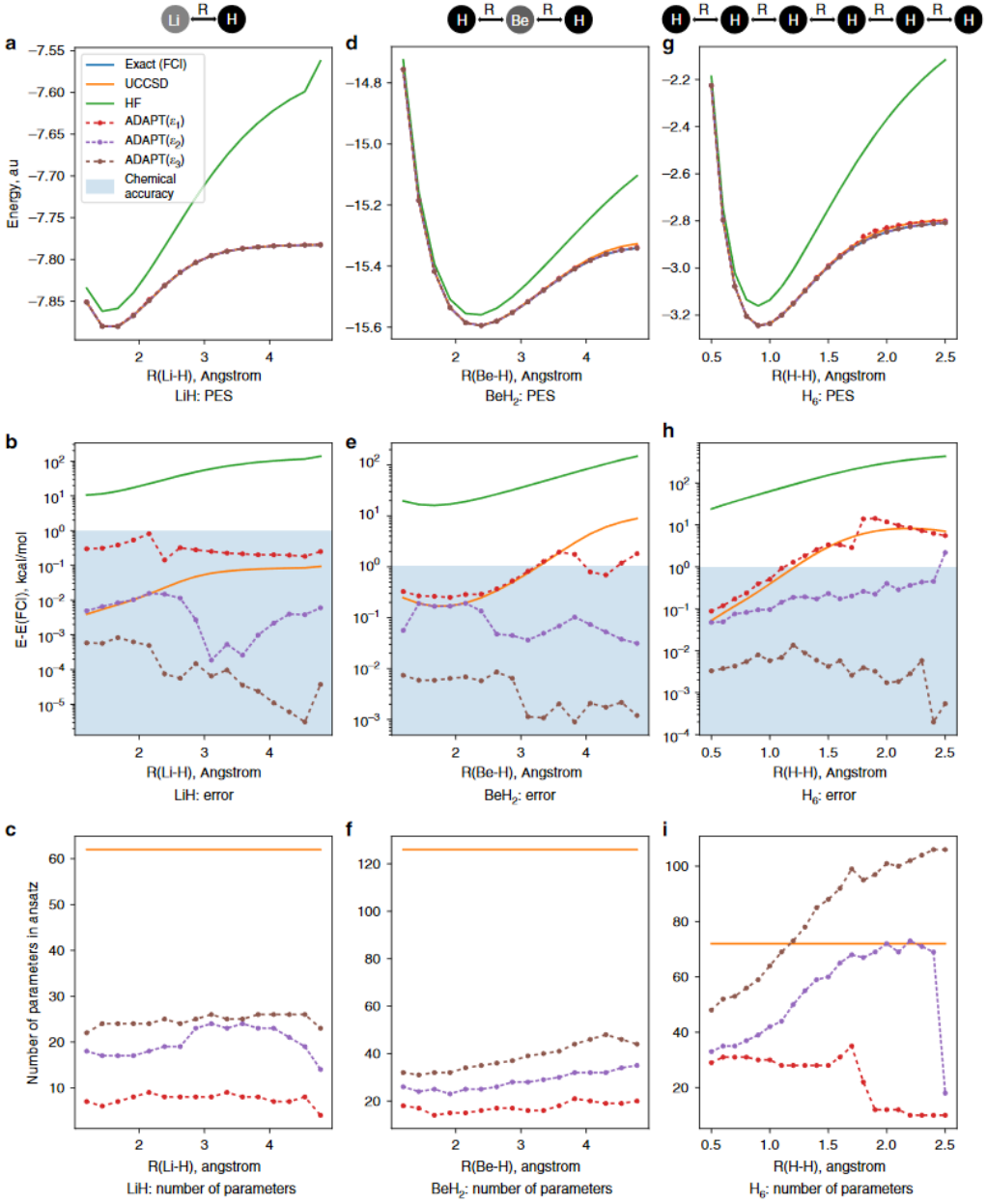


Fig. 2 Dissociation curves for LiH, BeH_2, and H_6. Potential energy as a function of nuclear coordinate, Hartree units (**a**, **d**, **g**). Absolute energy differences from FCI, kcal/mol units (**b**, **e**, **h**). Shaded blue region represents area within "chemical accuracy" as 1 kcal/mol. Number of variational operators in associated ansatz (**c**, **f**, **i**). Notation: ε indicates gradient norm threshold used such that $\varepsilon_m = 10^{-m}$. In all curves, the FCI curve lies directly underneath the ADAPT(ε_3) curve, and so is not visible

Nature Commun. 10, 3007 (2019)

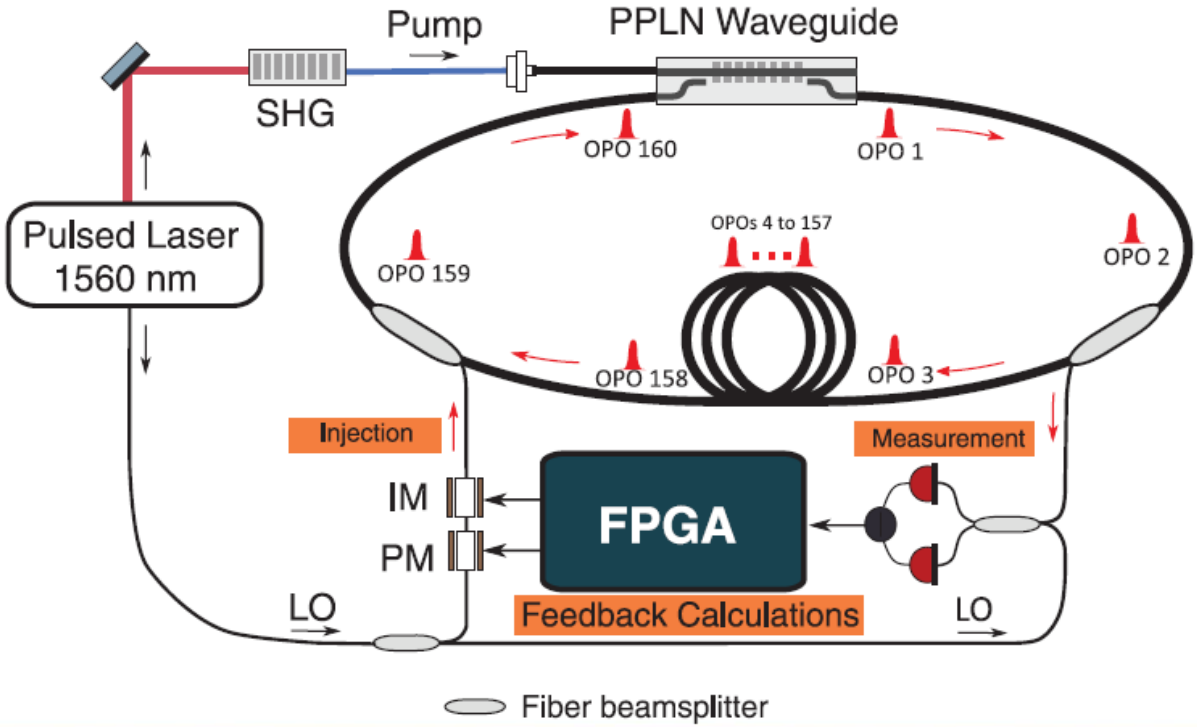
Electronic states

Yoshihisa Yamamoto

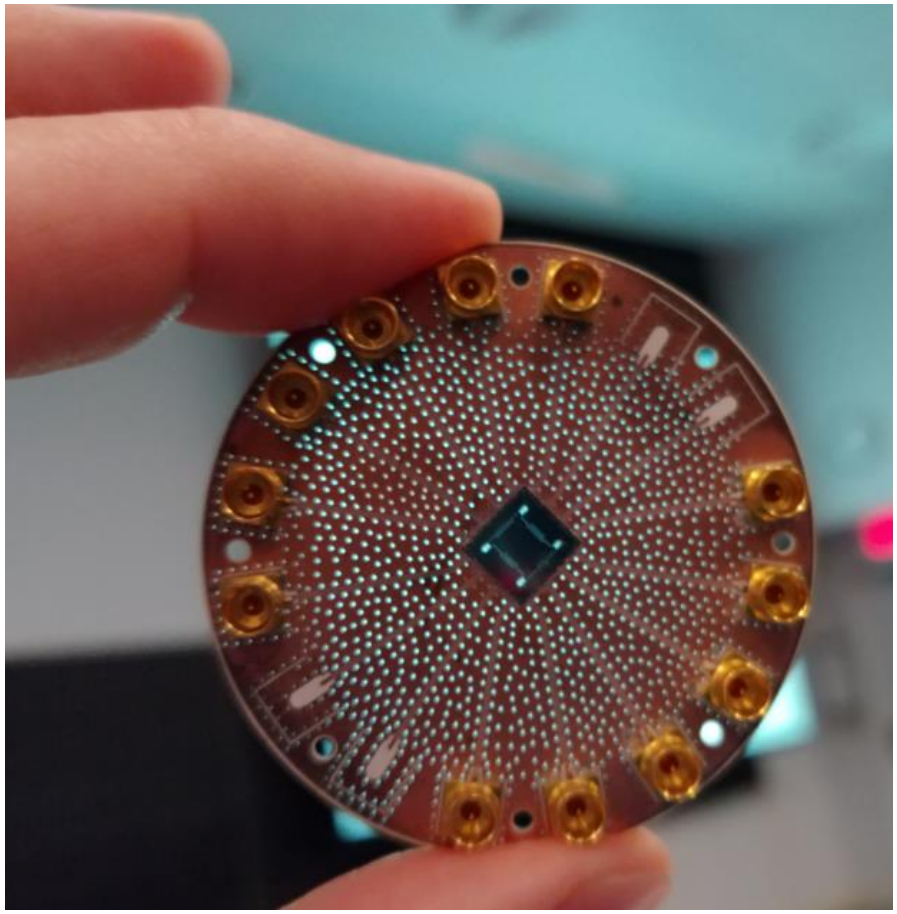
OPTICAL PROCESSING

A fully programmable 100-spin coherent Ising machine with all-to-all connections

Peter L. McMahon,[1,2*†] Alireza Marandi,[1*†] Yoshitaka Haribara,[2,3,4] Ryan Hamerly,[1] Carsten Langrock,[1] Shuhei Tamate,[2] Takahiro Inagaki,[5] Hiroki Takesue,[5] Shoko Utsunomiya,[2] Kazuyuki Aihara,[3,4] Robert L. Byer,[1] M. M. Fejer,[1] Hideo Mabuchi,[1] Yoshihisa Yamamoto[1,6]



Electronic states



Alexandre Blais: *Quantum Computing with Superconducting Circuits*, Montreal 2018

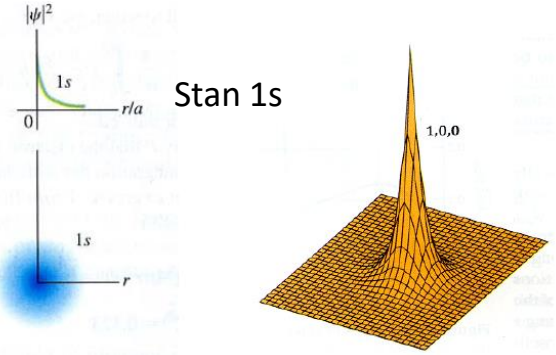
https://www.usherbrooke.ca/iq/en/personne/alexandre-blais/

Zapis skrócony

D Y G R E S J A

Stan pojedynczej cząstki:

Np.: funkcja falowa atomu wodoru



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

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

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

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

Liczby kwantowe!

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

Zapis skrócony

D Y G R E S J A

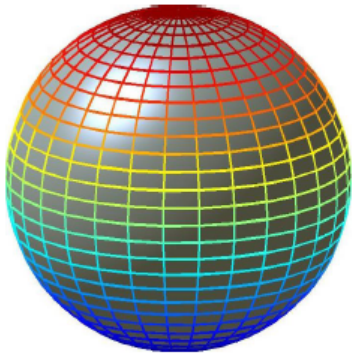
(czyli tak naprawdę)

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

Reprezentacja położeniowa

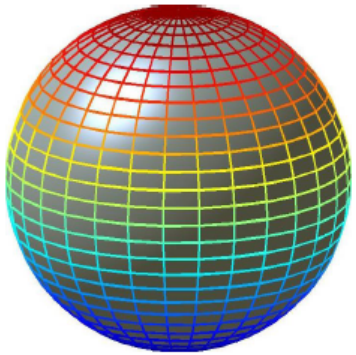
Zapis skrócony

Bity, P-bity, Q-bity

	Bit	Pbit	Qubit
	0	0	0
			
	1	1	1
States:	o or ı	$\{p{:}\mathrm{o}, (1-p){:}\mathrm{ı}\}$	$\alpha\|\mathrm{o}\rangle + \beta\|\mathrm{ı}\rangle$
			$\|\alpha\|^2 + \|\beta\|^2 = 1$

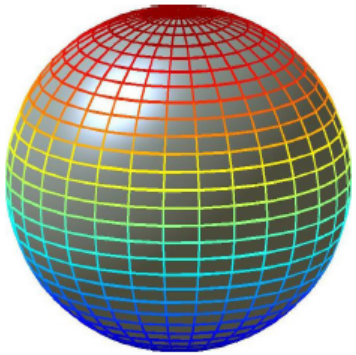
> ***Introduction to Quantum Information Processing***
> E. Knill, R. Laflamme, H. Barnum, D. Dalvit, J. Dziarmaga,
> J. Gubernatis, L. Gurvits, G. Ortiz, L. Viola and W. H. Zurek
> ▌

Bity, P-bity, Q-bity

Bit	Pbit	Qubit
0	0	0
		
1	1	1
States: 0 or 1	$\{p{:}0, (1-p){:}1\}$	$\alpha\|0\rangle + \beta\|1\rangle$
		$\|\alpha\|^2 + \|\beta\|^2 = 1$

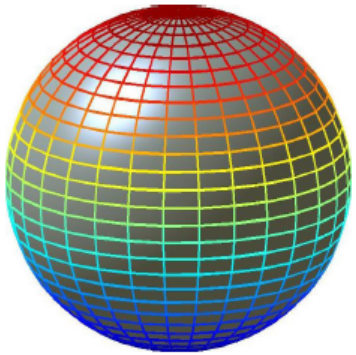
> komputery (maszyny Turinga)
> standardowe programy
> ▌

Bity, P-bity, Q-bity

Bit	Pbit	Qubit
0	0	0
		
1	1	1
States: 0 or 1	$\{p{:}0, (1-p){:}1\}$	$\alpha\|0\rangle + \beta\|1\rangle$
		$\|\alpha\|^2 + \|\beta\|^2 = 1$

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

Bity, P-bity, Q-bity

	Bit	Pbit	Qubit
	0	0	0
			
	1	1	1
States:	o or ı	$\{p$:o, $(1-p)$:ı$\}$	$\alpha\|\text{o}\rangle + \beta\|\text{ı}\rangle$
			$\|\alpha\|^2 + \|\beta\|^2 = 1$

> komputery kwantowe
> algorytmy kwantowe
> ▌

Bity, P-bity, Q-bity

Kwantowym odpowiednikiem klasycznego bitu jest dowolny układ dwustanowy:

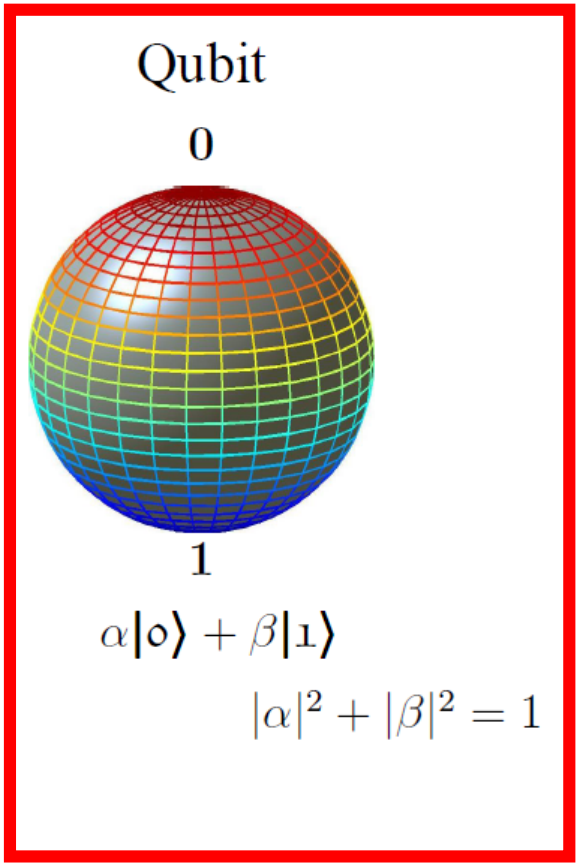
dwa poziomy atomu $\{|g\rangle, |e\rangle\}$ np. $g = 1s$, $e = 2s$

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

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

itp.

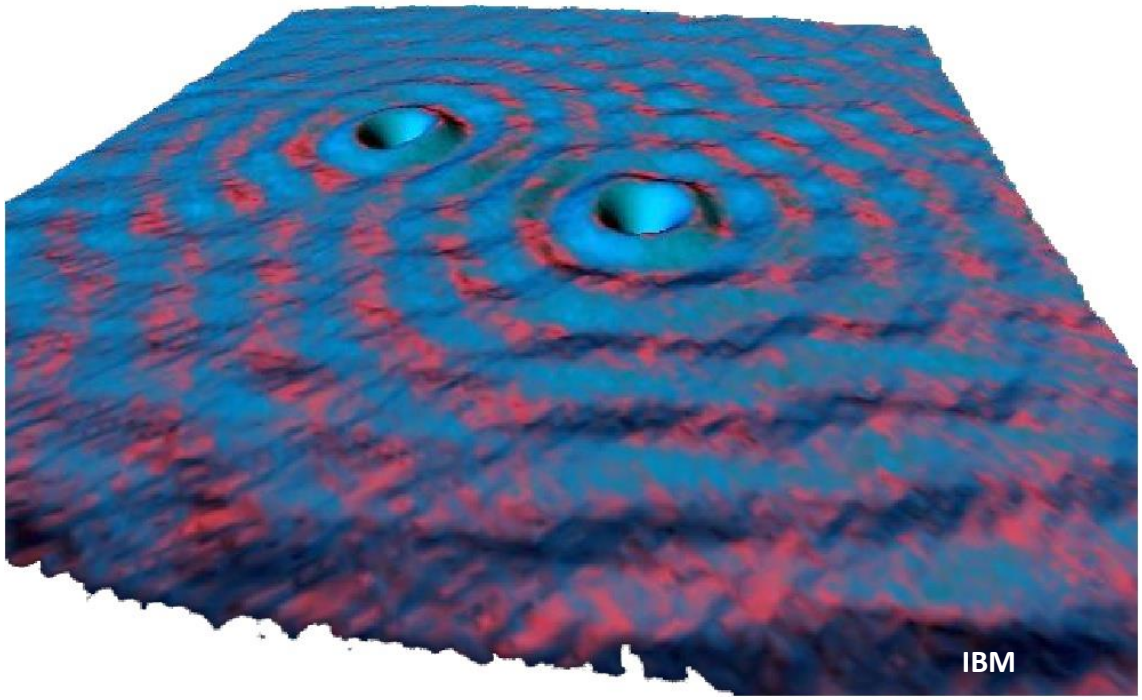
Taki układ to qubit (quantum bit); po polsku kubit.



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

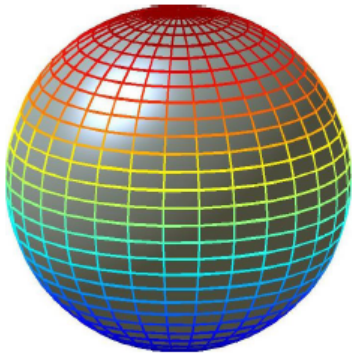
Bity, P-bity, Q-bity

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



Qubit

0



1

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

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

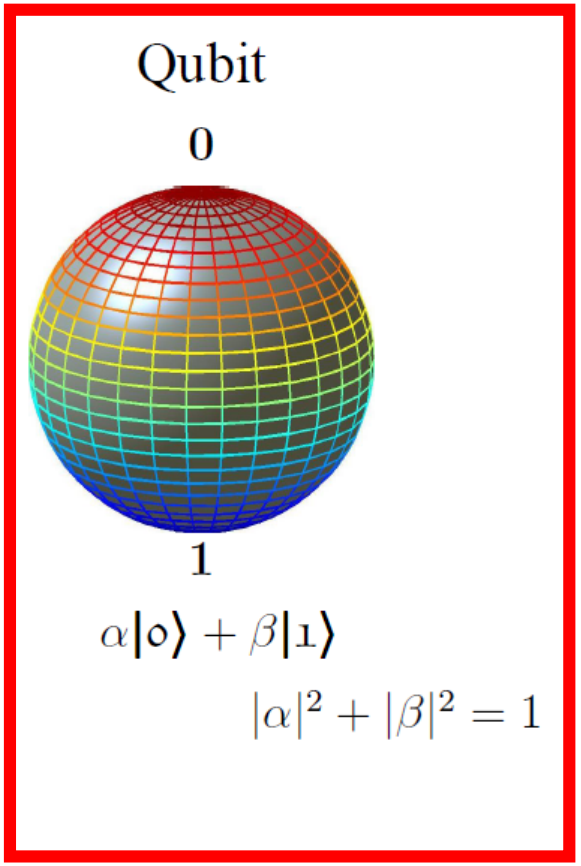
Bity, P-bity, Q-bity

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

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

ponieważ α i β zespolone – równanie sfery

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



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

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

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

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

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

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

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

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

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

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

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

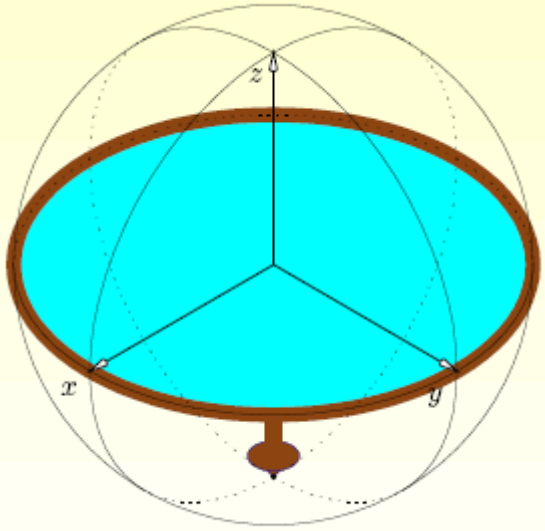
$$|\Psi\rangle = \frac{1}{5}(3|0\rangle - 4|1\rangle)$$

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

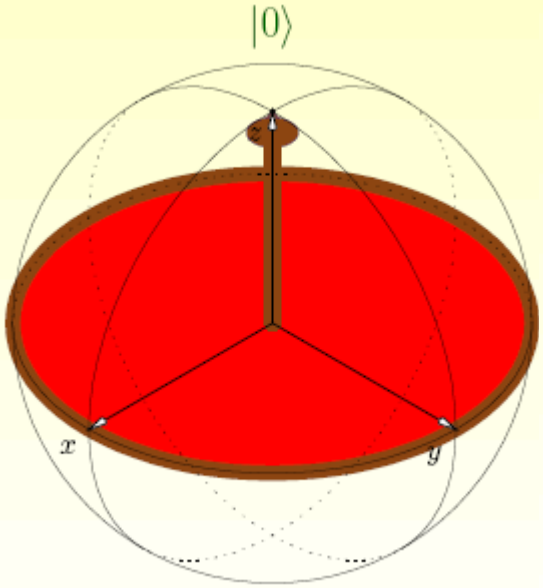
$$|\Psi\rangle = \frac{1}{5}(4|0\rangle - 3i|1\rangle)$$

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

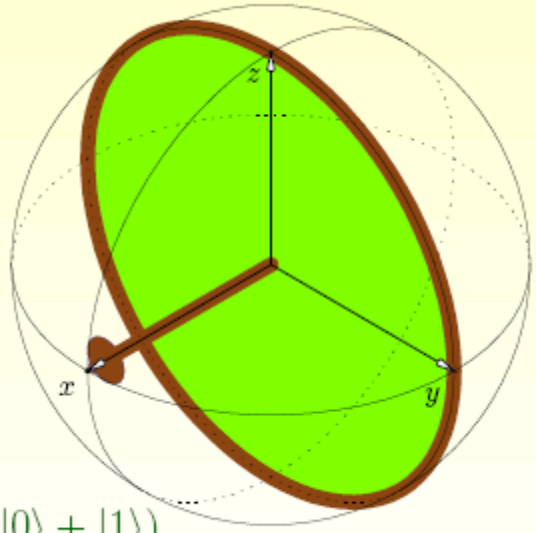
$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(e^{i\theta}|0\rangle + e^{i\varphi}|1\rangle\right)$$



$|1\rangle$

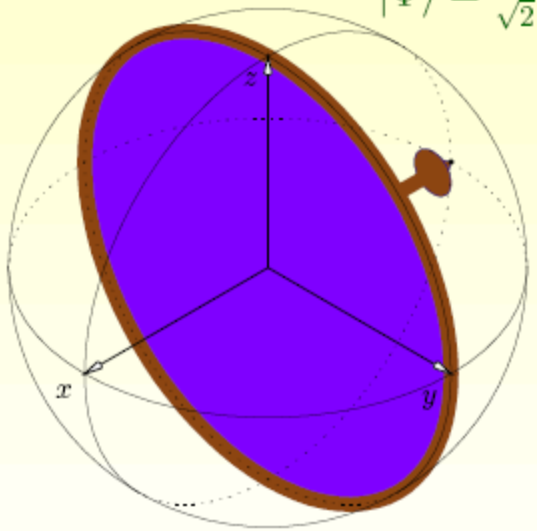


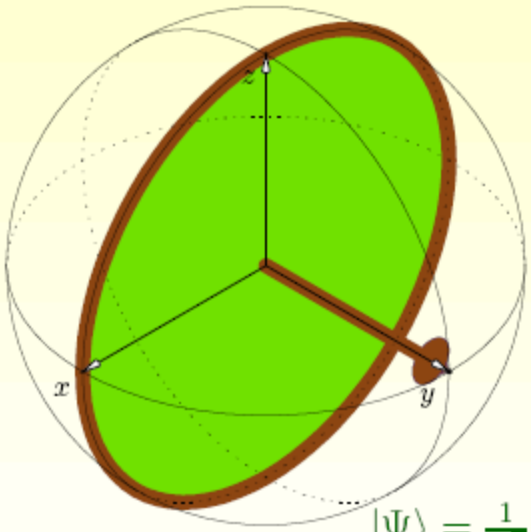
$|0\rangle$



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

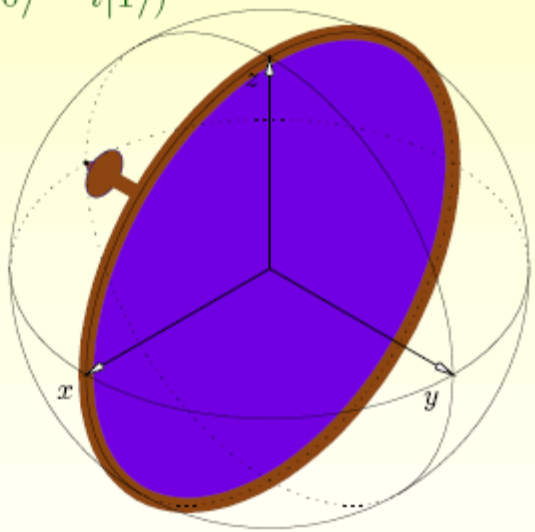
$|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$





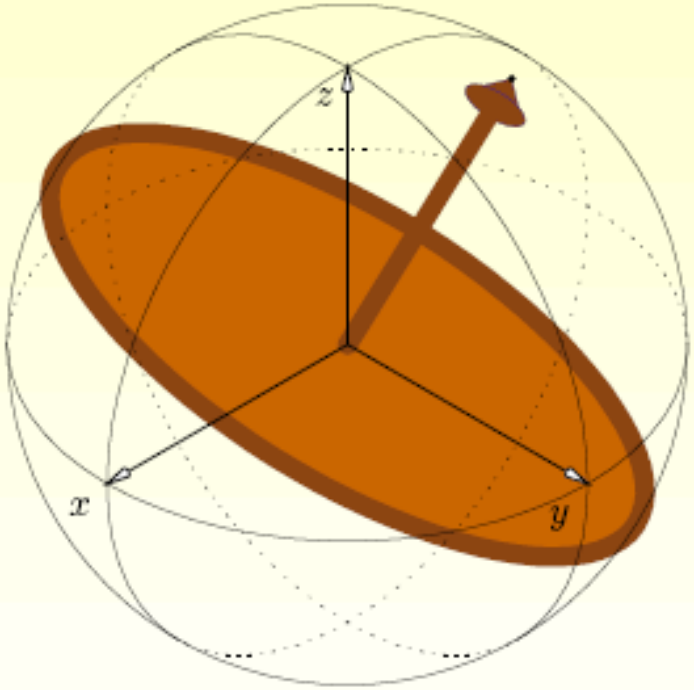
$|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$

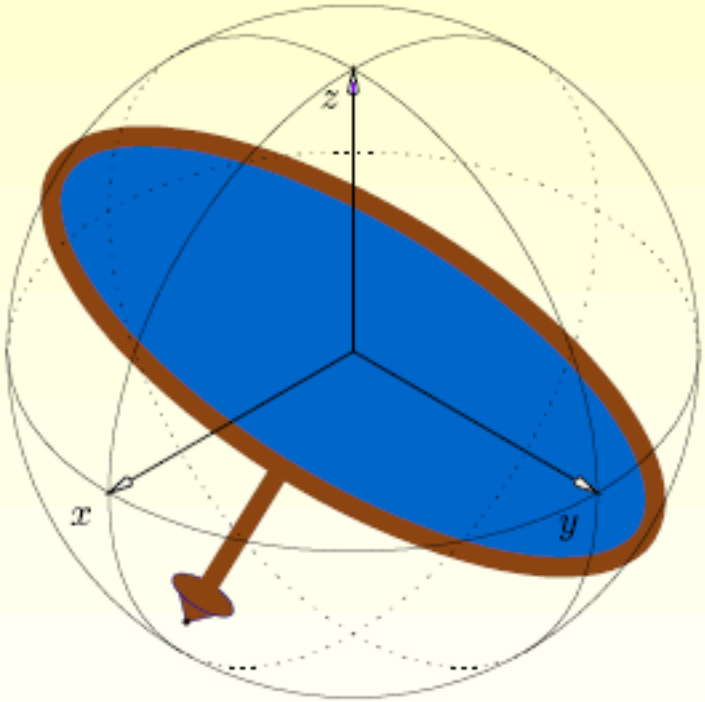
$|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$



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

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





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

Łatwo powiedzieć. Ale jak zrobić?

Bramki kubitowe

W rolach głównych:

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

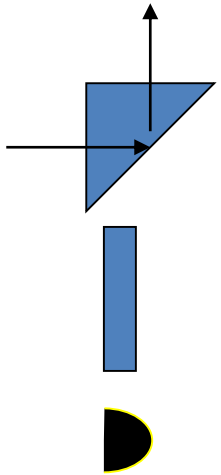
i foton $|\uparrow\rangle = |1\rangle$

W pozostałych rolach:

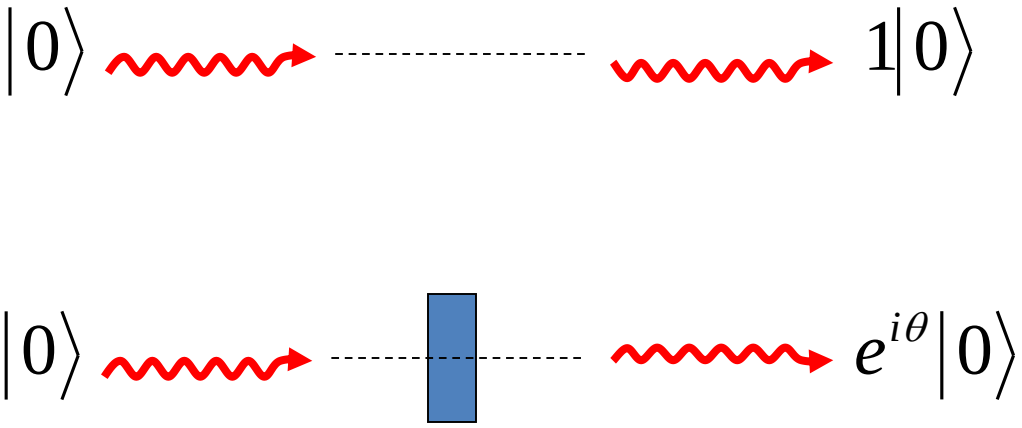
Pryzmat z całkowitym Wewnętrznym odbiciem

Płytka szklana o grubości *d*

Detektor

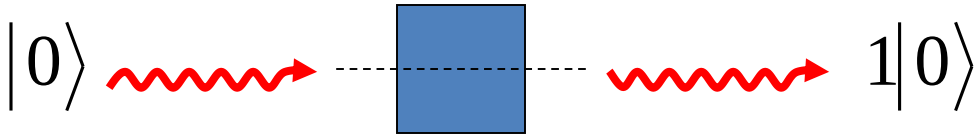


Bramki kubitowe

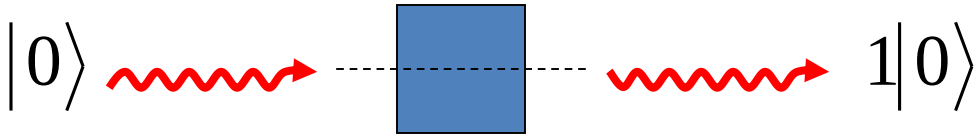


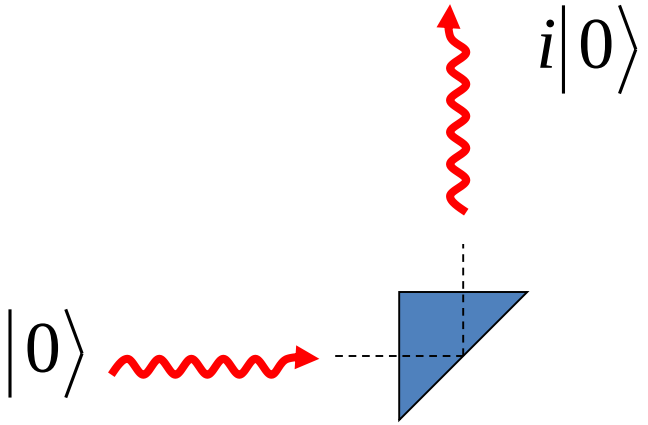
Płytka szklana na drodze optycznej zmienia fazę fotonu W PORÓWNANIU do fazy fotonu bez płytki.

Bramki kubitowe

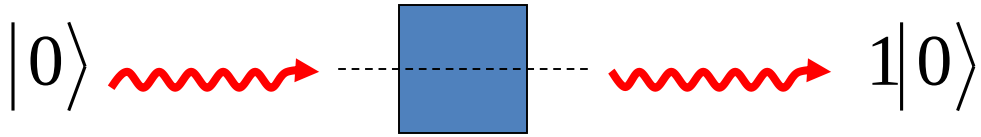


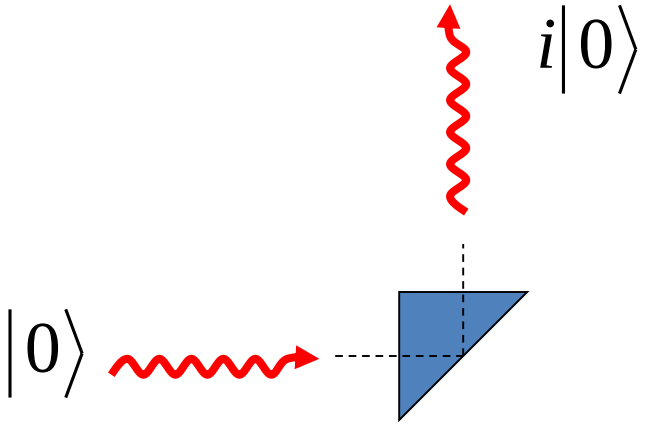
Bramki kubitowe

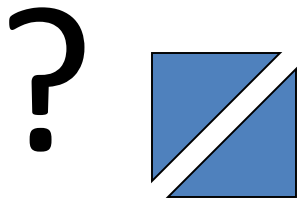




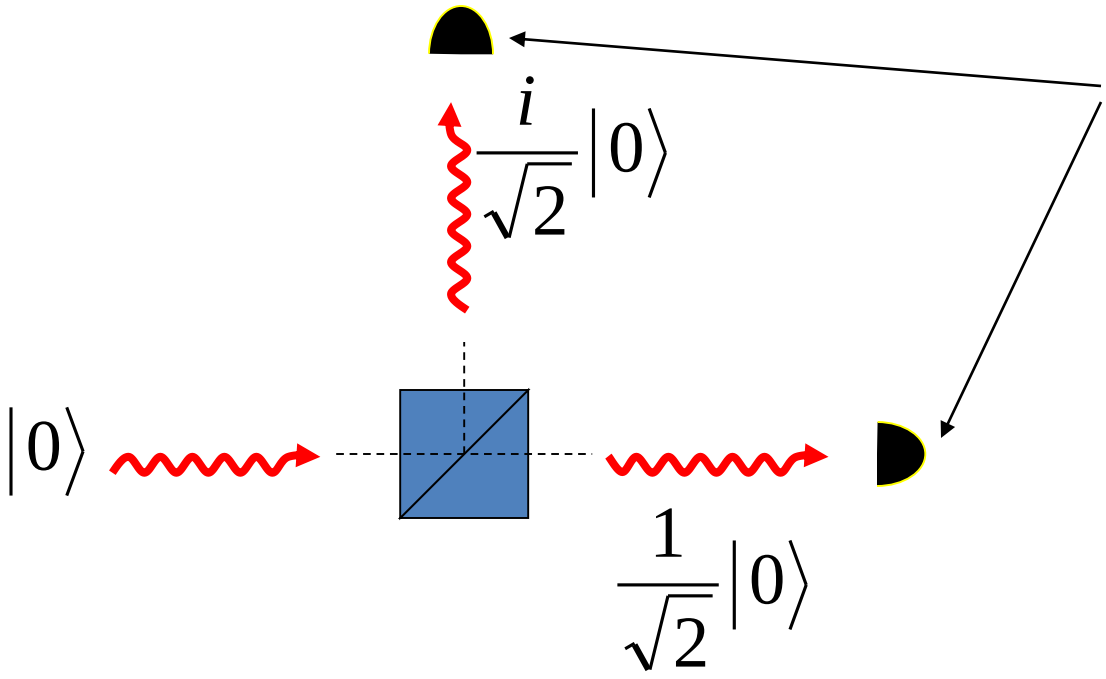
Bramki kubitowe







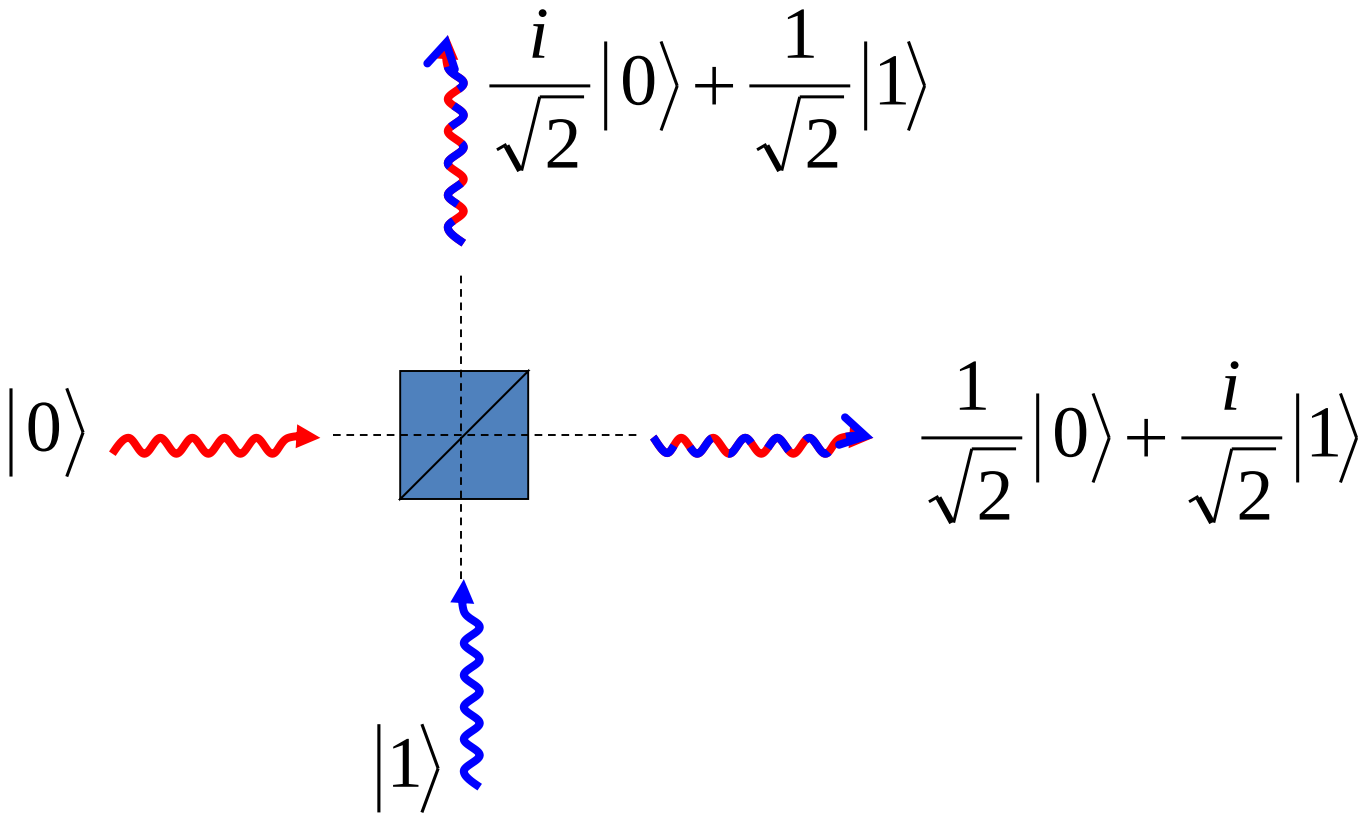
Bramki kubitowe



Prawdopodobieństwo 1/2

$$\left|\frac{i}{\sqrt{2}}\right|^2 = \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}$$

Bramki kubitowe

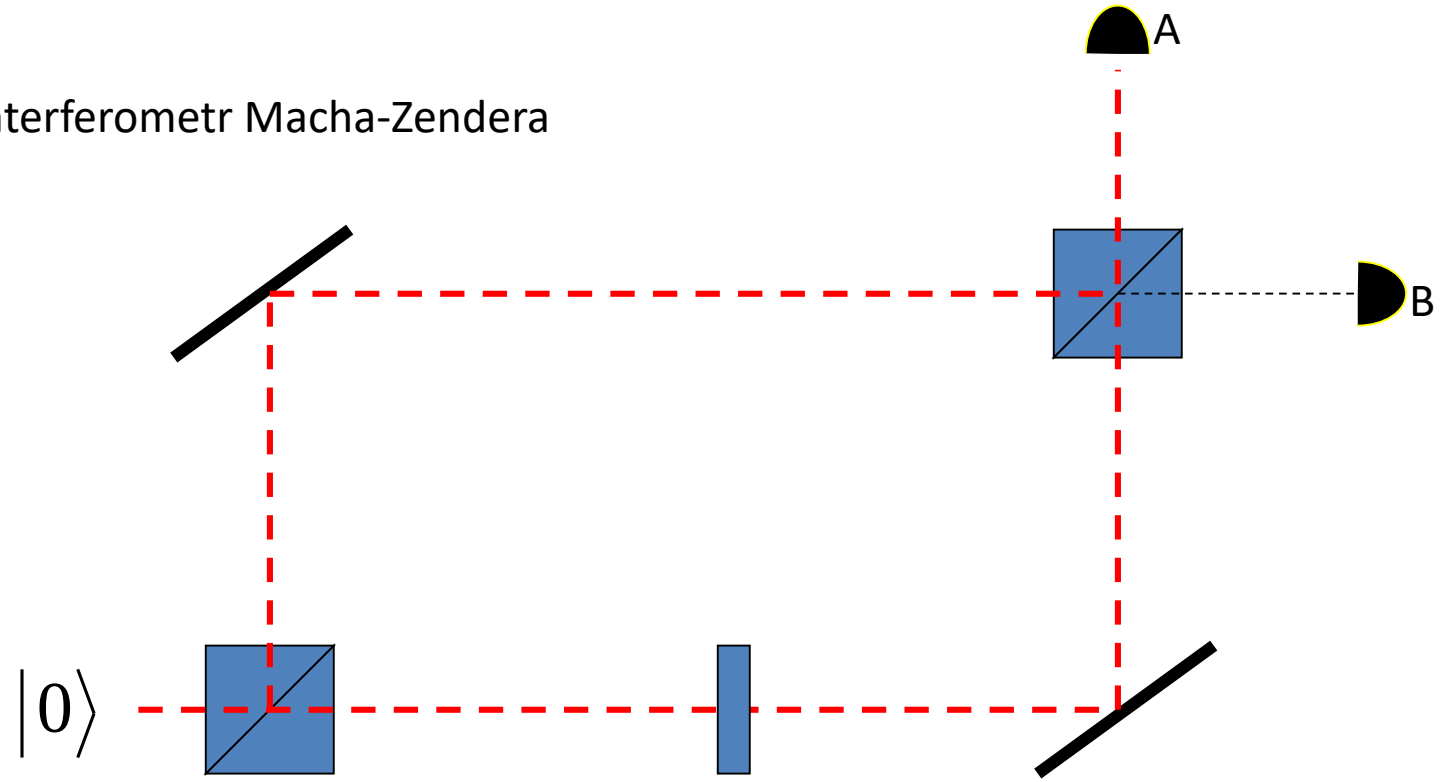


Umiemy zmieszać stany!

Bramki kubitowe

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

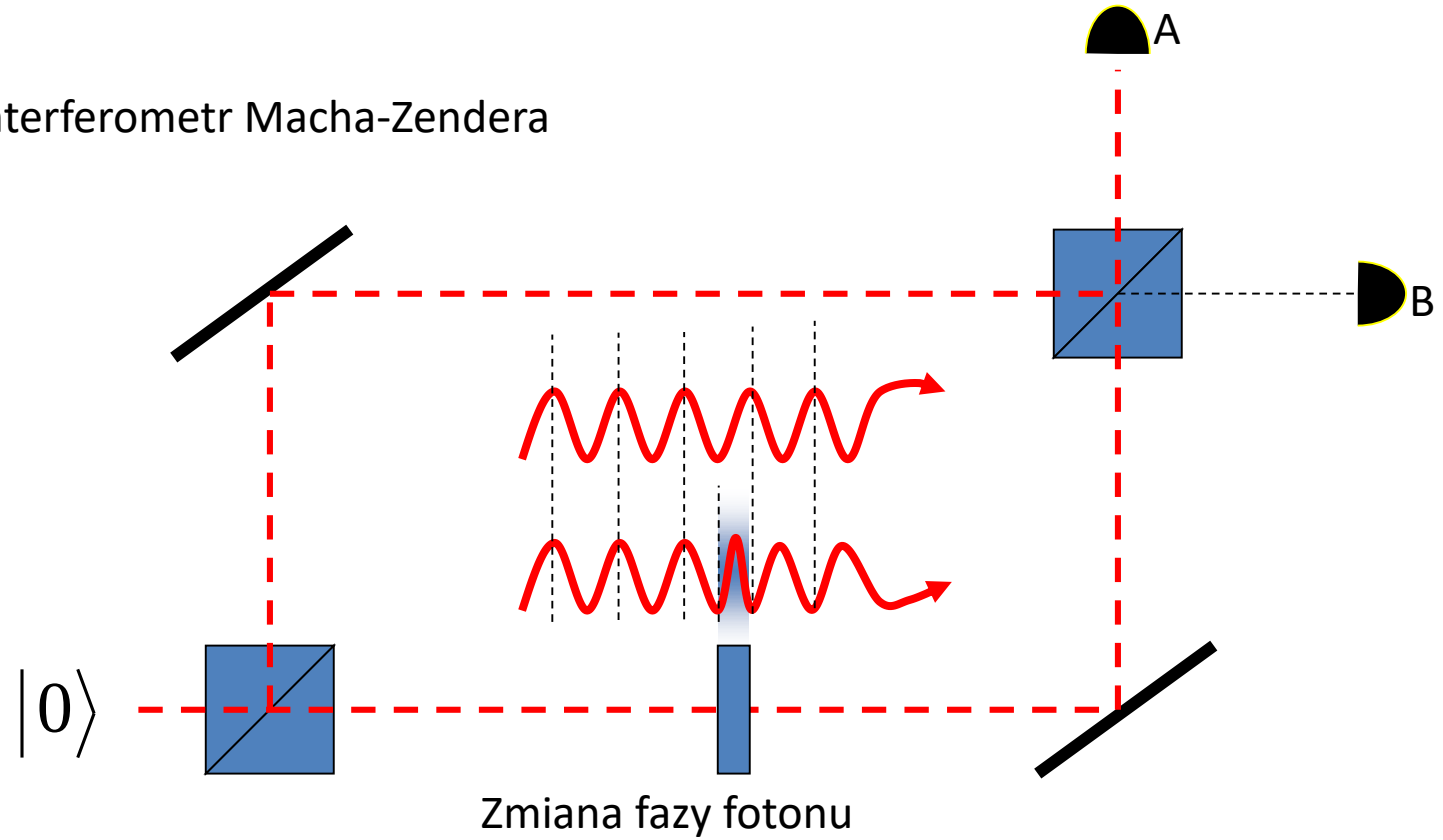
Interferometr Macha-Zendera



Bramki kubitowe

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

Interferometr Macha-Zendera



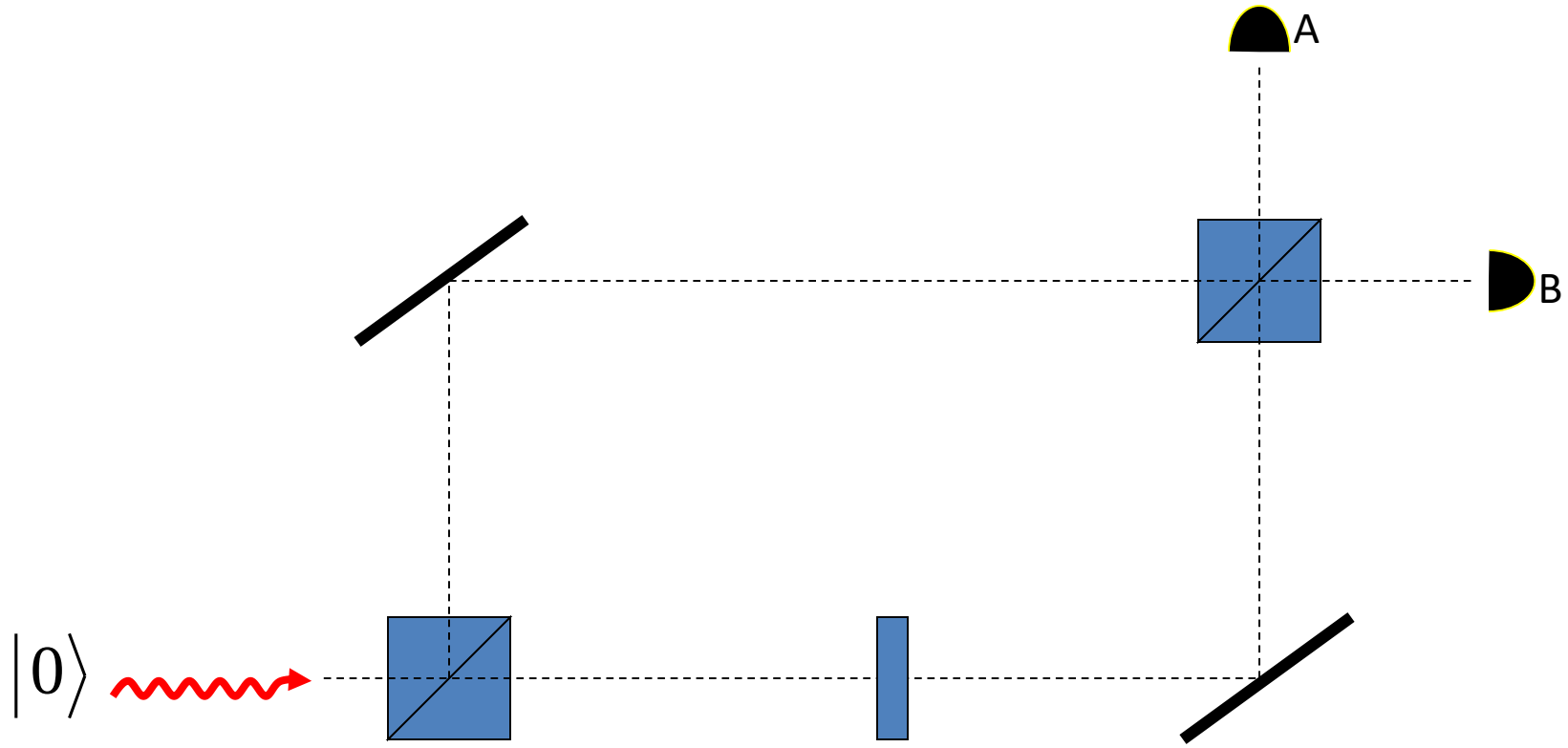
Bramki kubitowe

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

Liczymy!

Bramki kubitowe

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

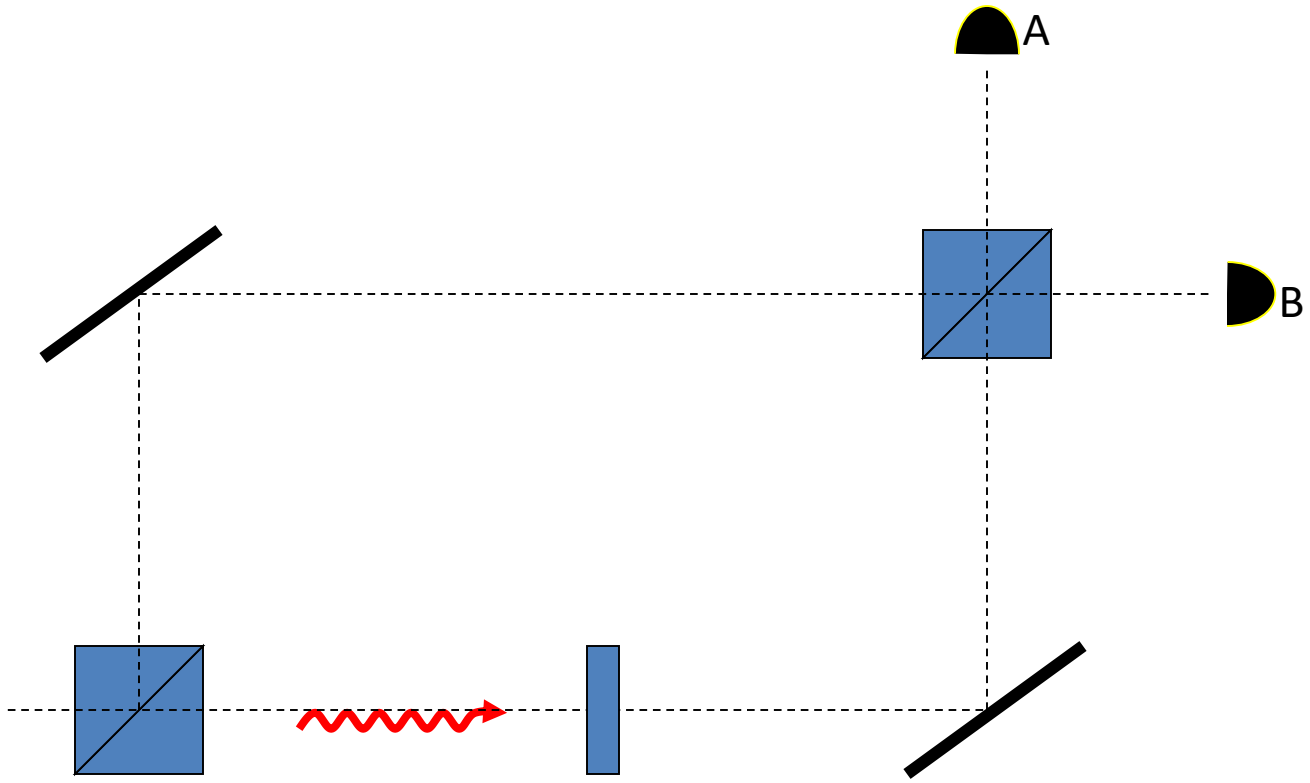


Interferometr Macha-Zendera

Bramki kubitowe

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

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



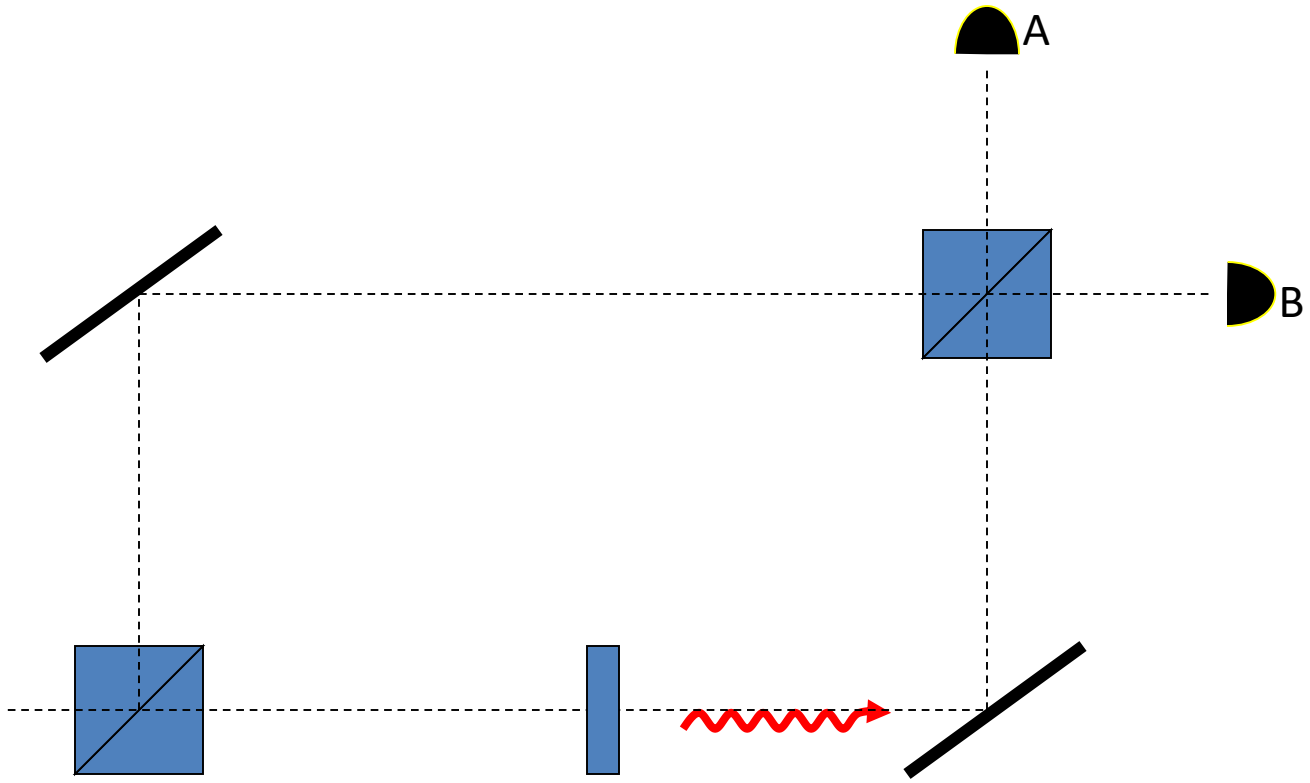
$|0\rangle$

Interferometr Macha-Zendera

Bramki kubitowe

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

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



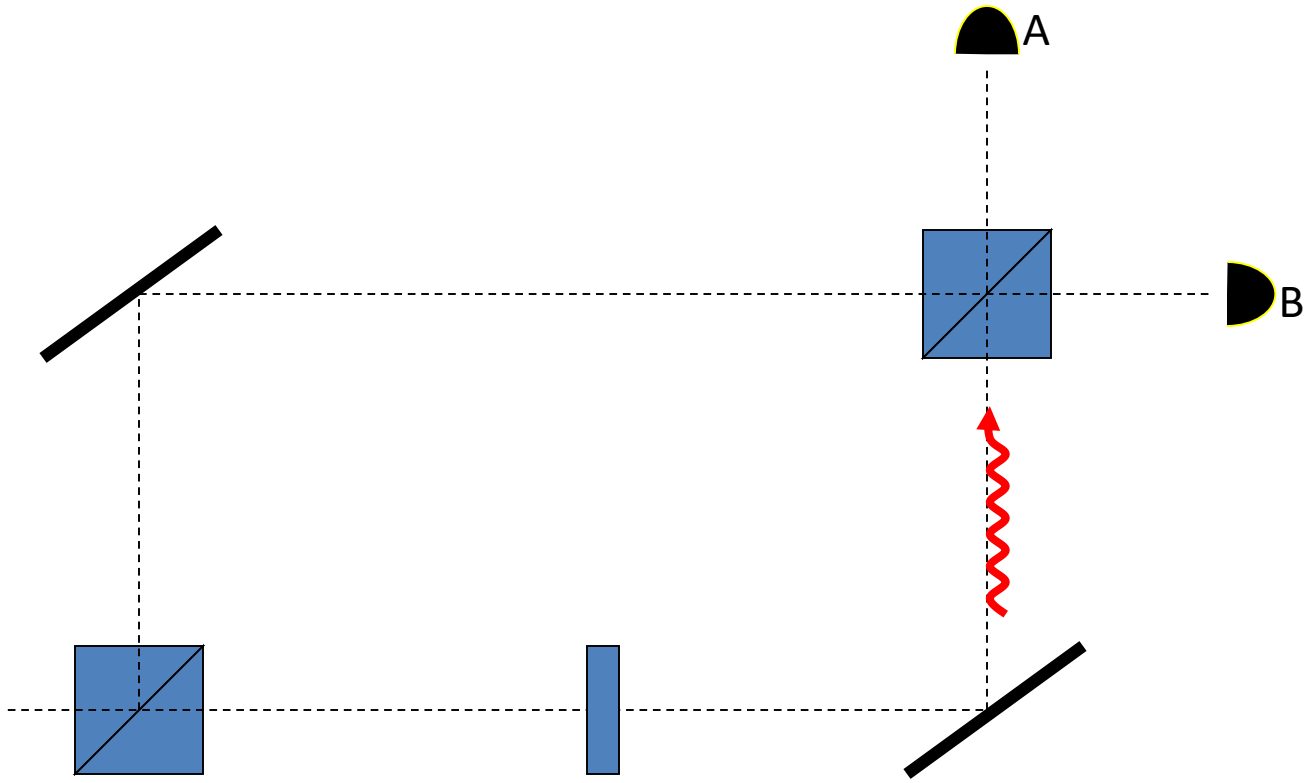
$|0\rangle$

Interferometr Macha-Zendera

Bramki kubitowe

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

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



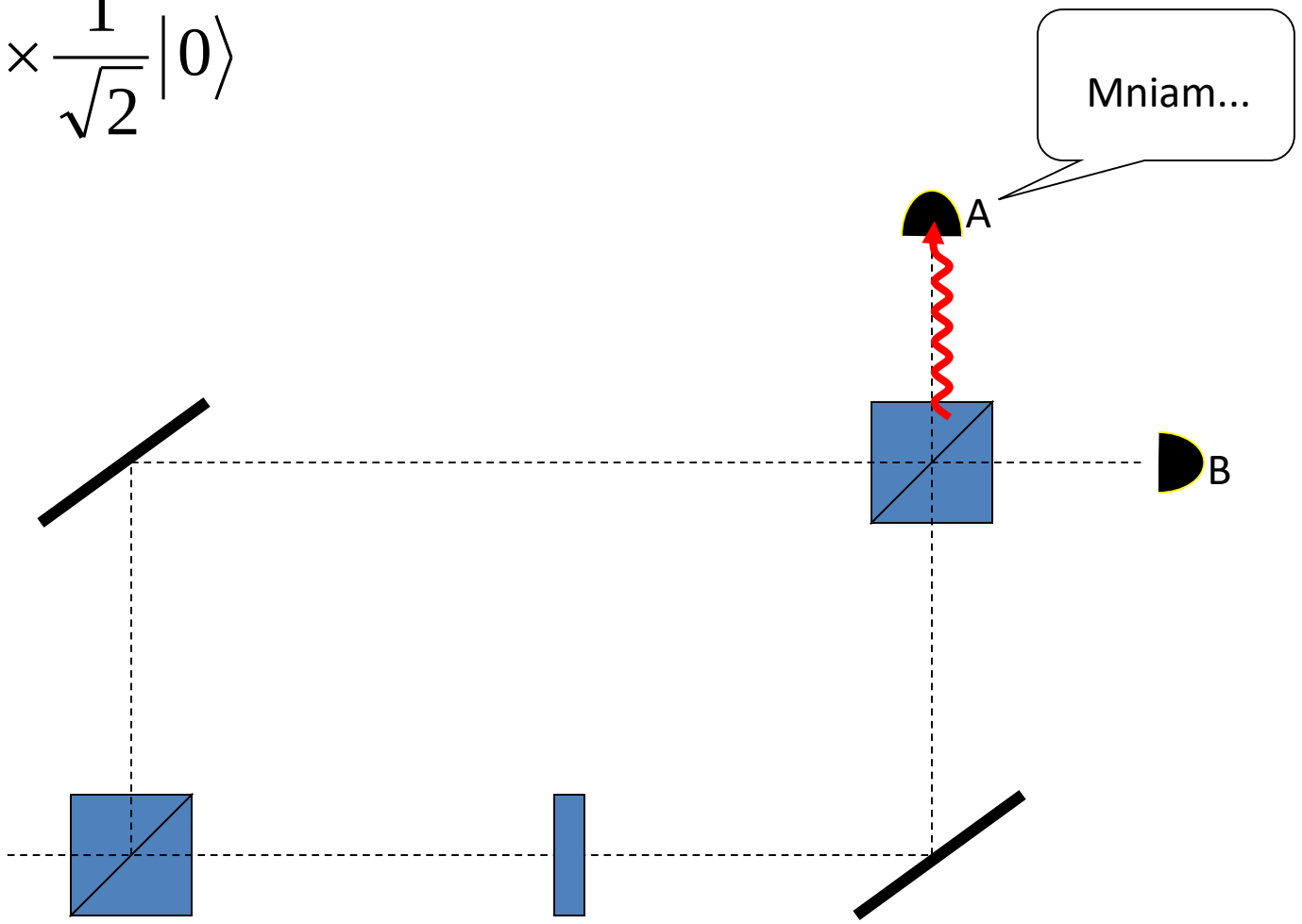
$|0\rangle$

Interferometr Macha-Zendera

Bramki kubitowe

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

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

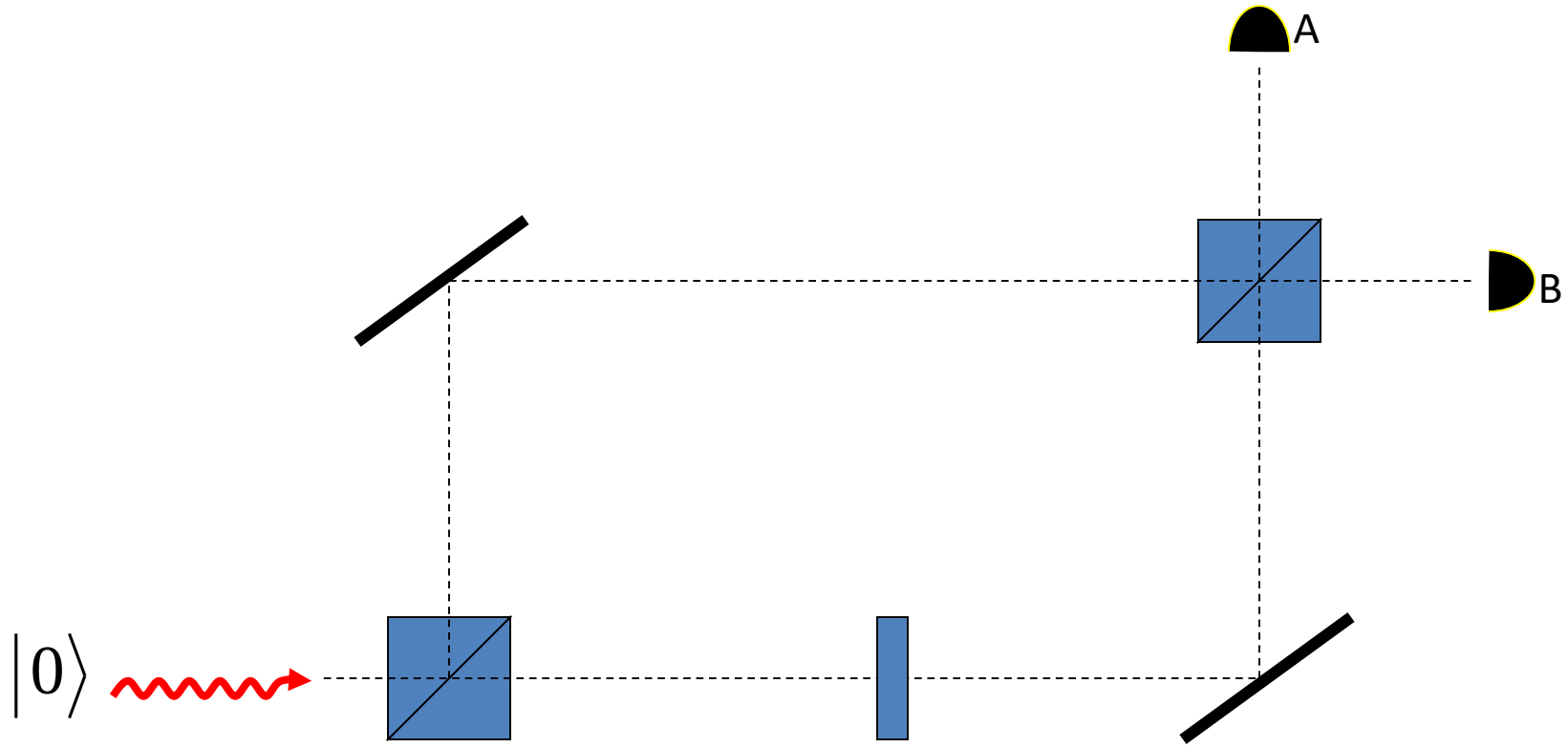


Interferometr Macha-Zendera

Bramki kubitowe

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

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

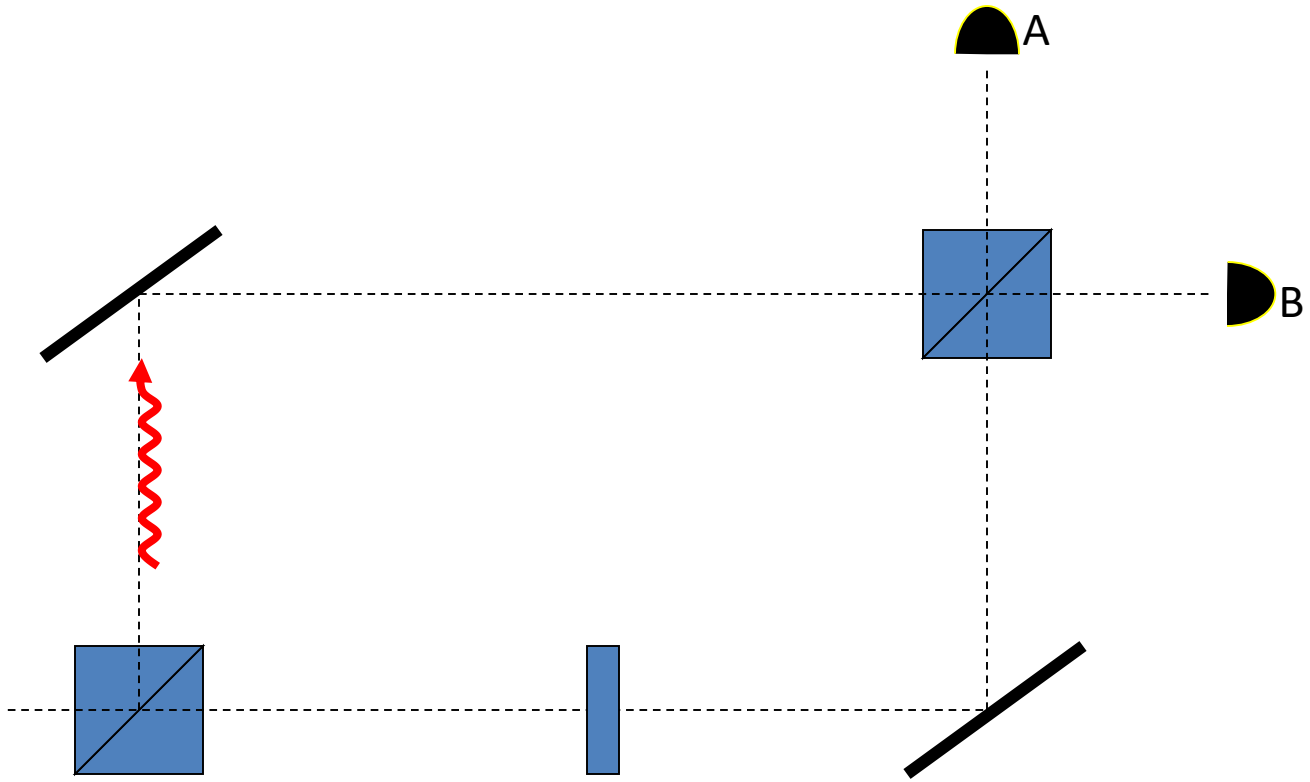


Interferometr Macha-Zendera

Bramki kubitowe

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

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



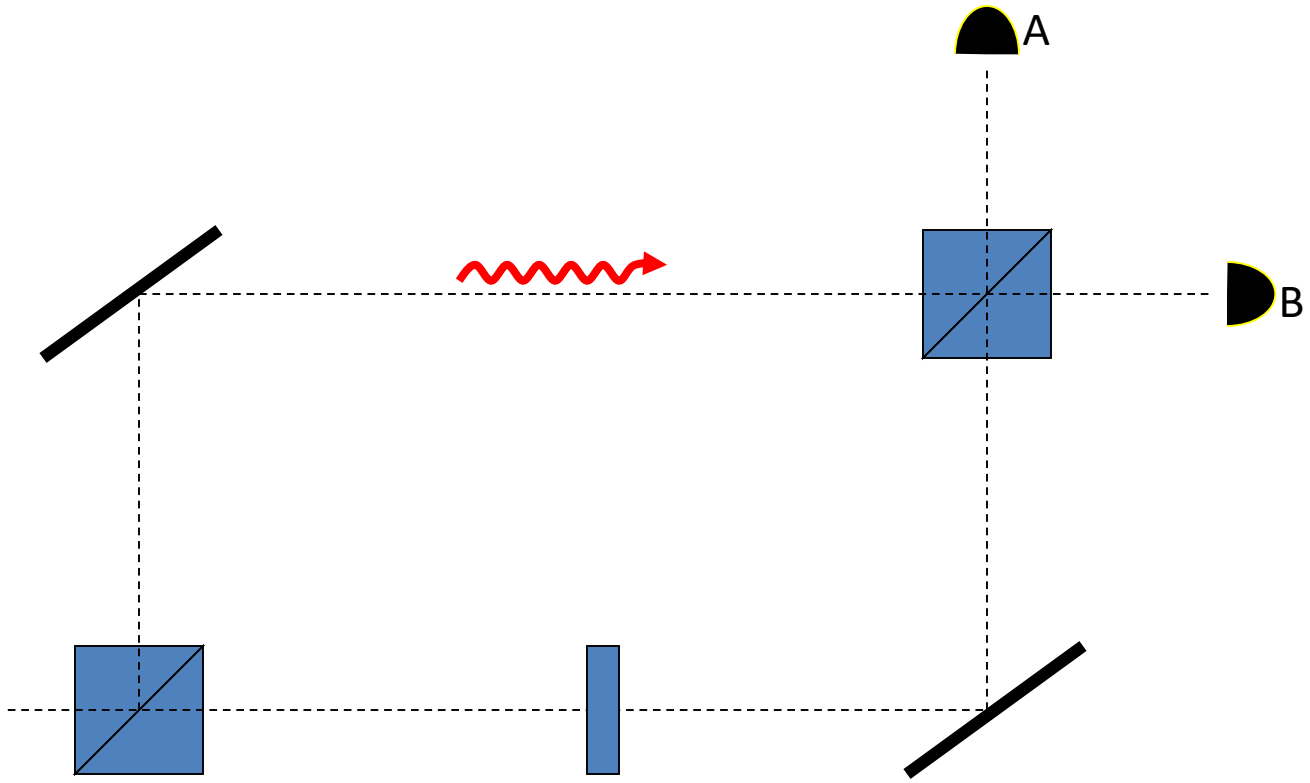
$|0\rangle$

Interferometr Macha-Zendera

Bramki kubitowe

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

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

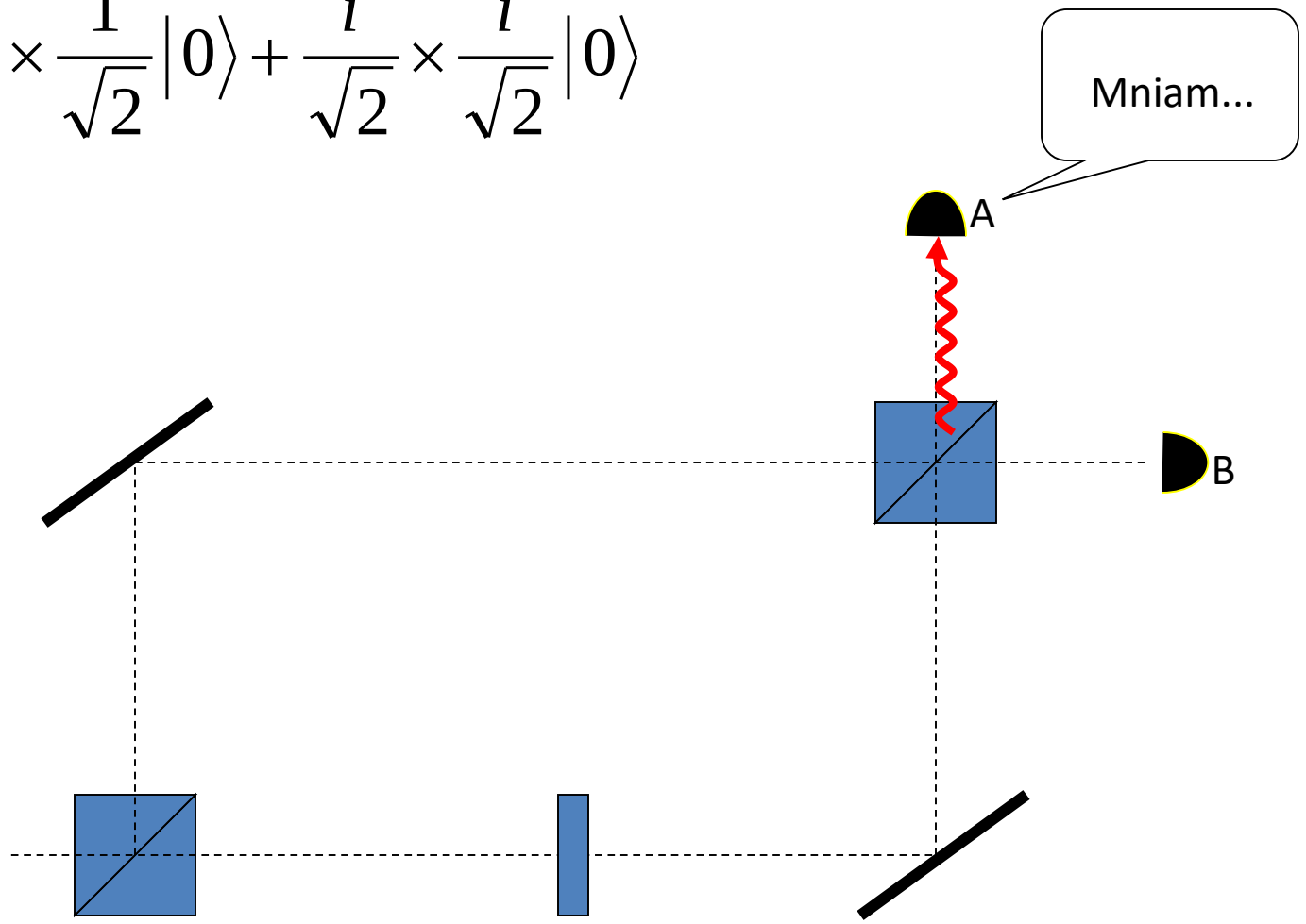


Interferometr Macha-Zendera

Bramki kubitowe

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

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

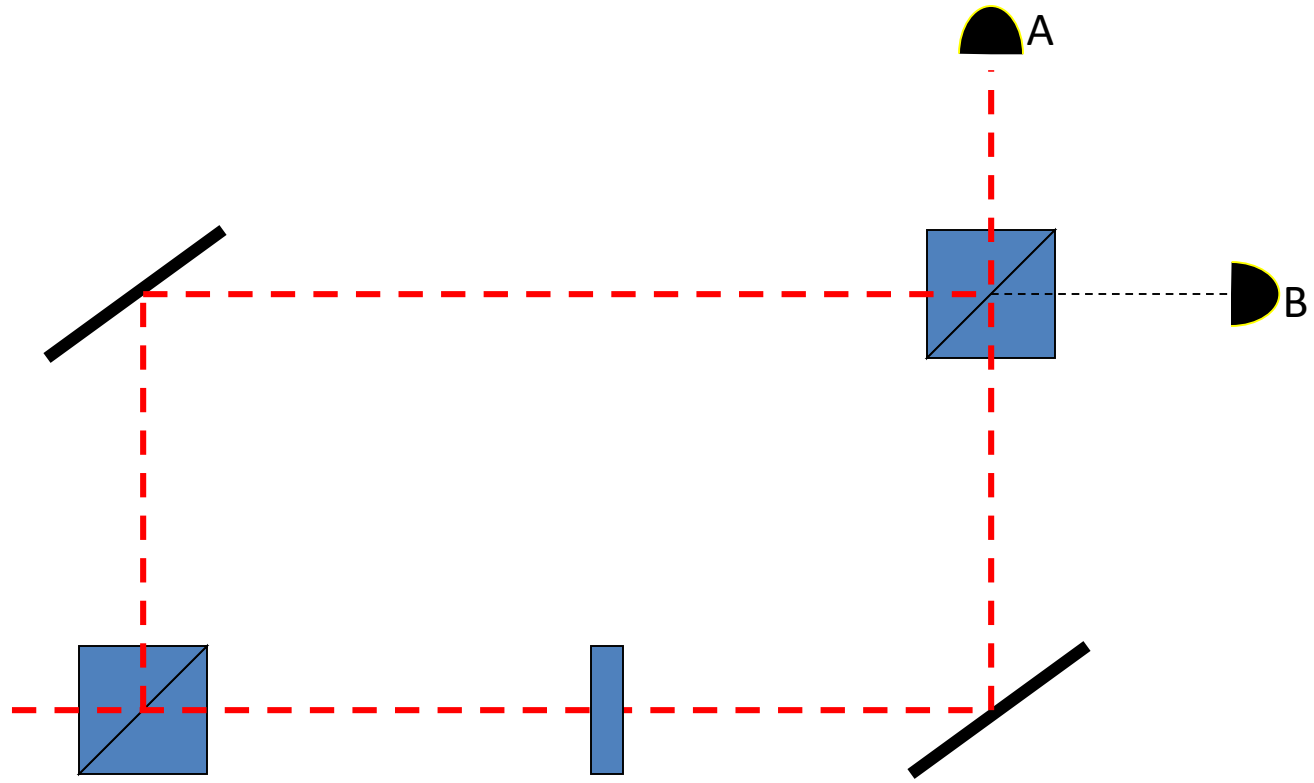


Interferometr Macha-Zendera

Bramki kubitowe

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

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



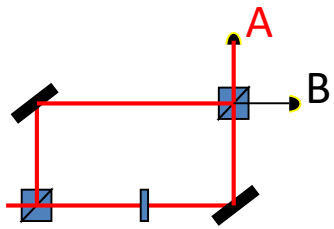
Interferometr Macha-Zendera

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

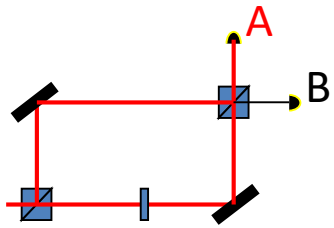


Bramki kubitowe

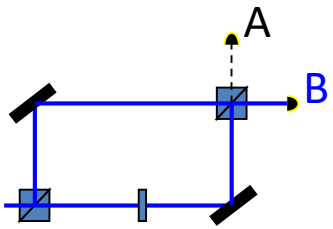
Jakie jest prawdopodobieństwo, że foton znajdzie się w detektorze A?

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

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



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

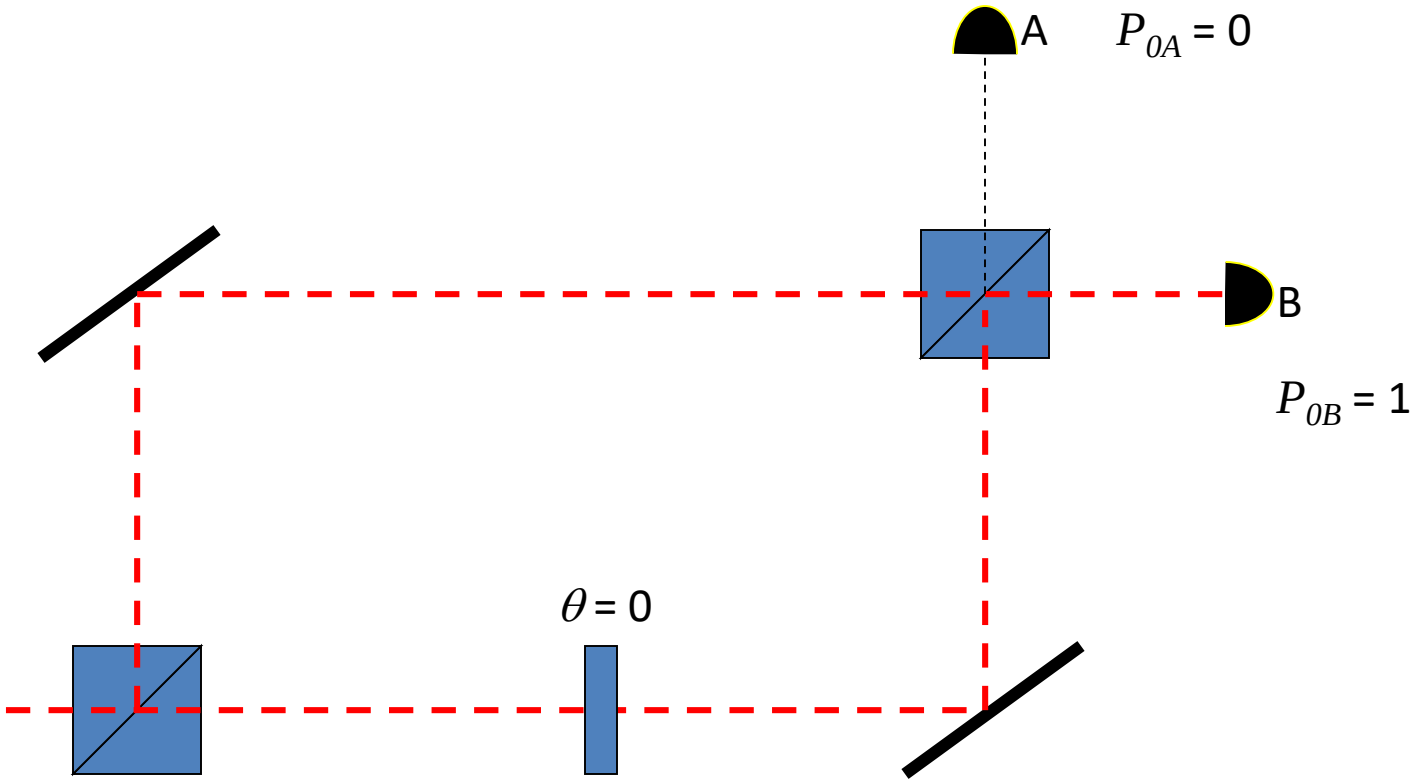


Dla $\theta = 0$ mamy $P_{0A} = 0$ i $P_{0B} = 1$, a więc foton NIGDY nie trafi do detektora A, tylko na pewno trafi do B! Oczywiście dla $\theta = 180^o$ jest odwrotnie!

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!

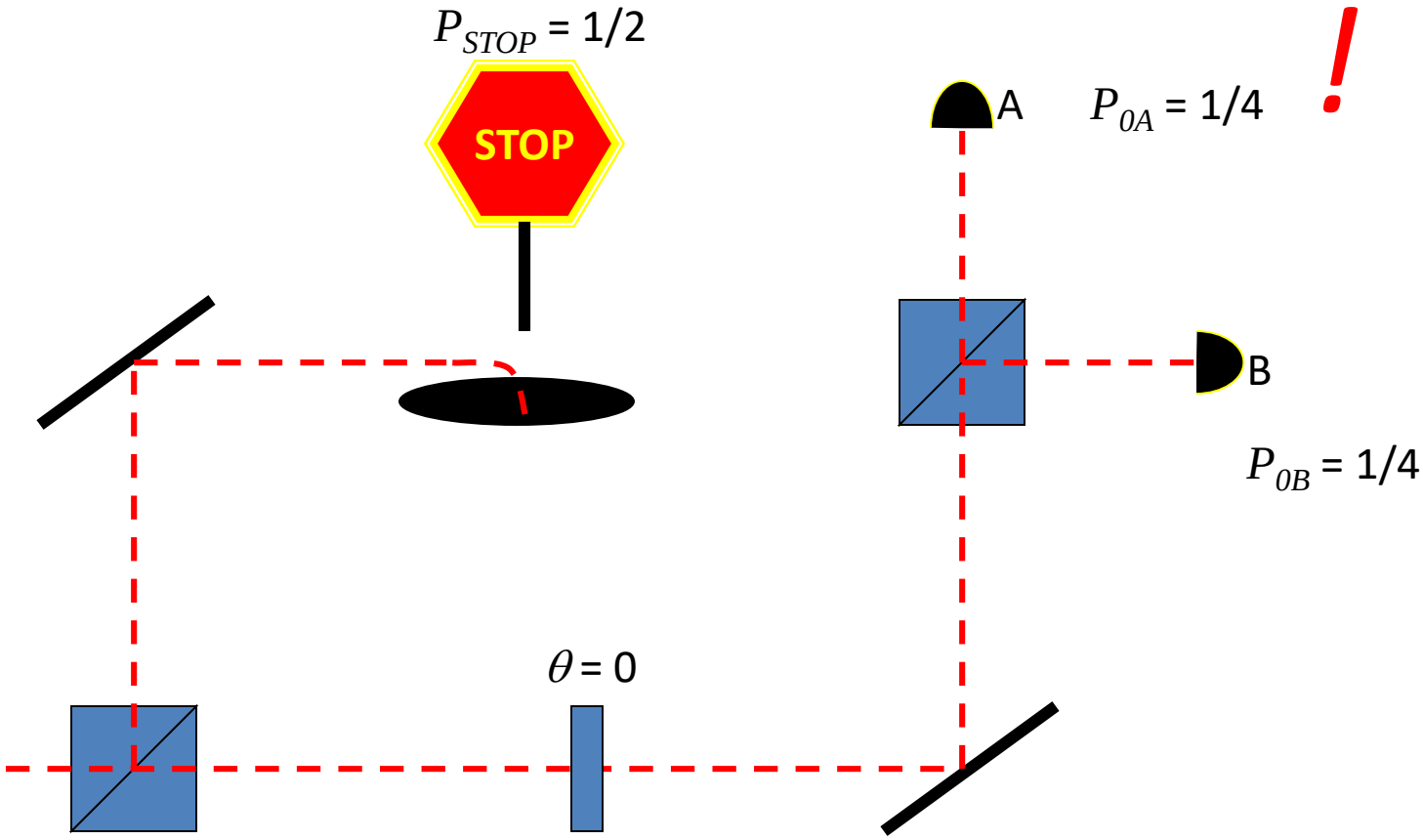
Foton interferuje SAM ZE SOBĄ!



Interferometr Macha-Zendera

Dygresja: pomiar BEZ oddziaływania

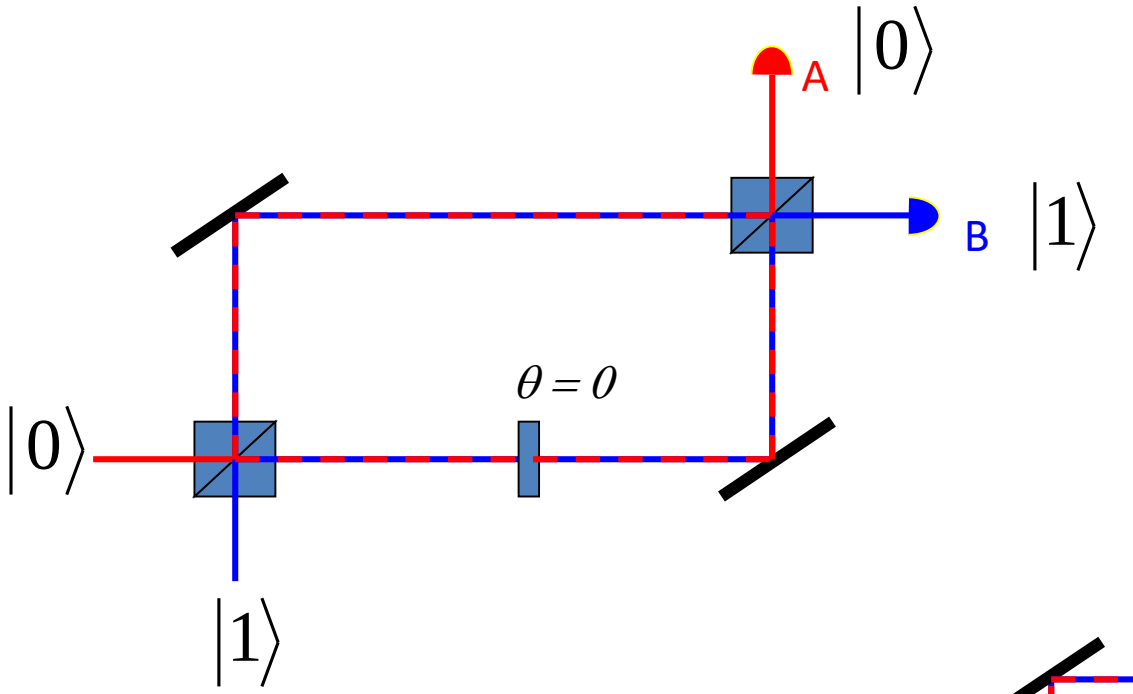
Ale co się stanie gdy na jednej z dróg interferometru stanie przeszkoda?

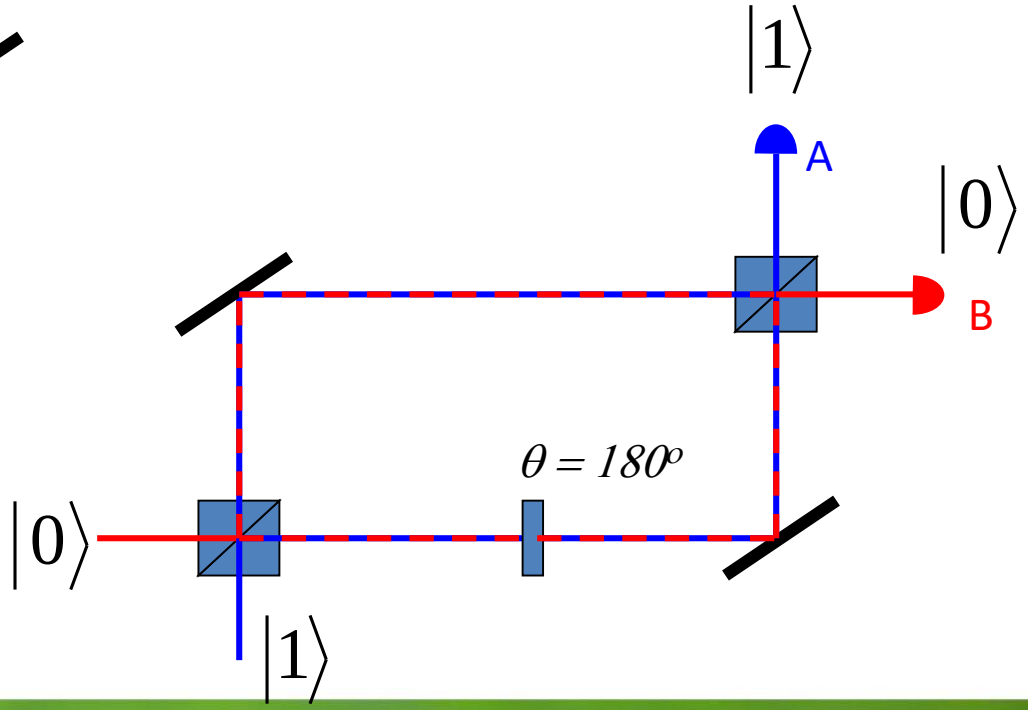


Interferometr Macha-Zendera

Bramki kubitowe

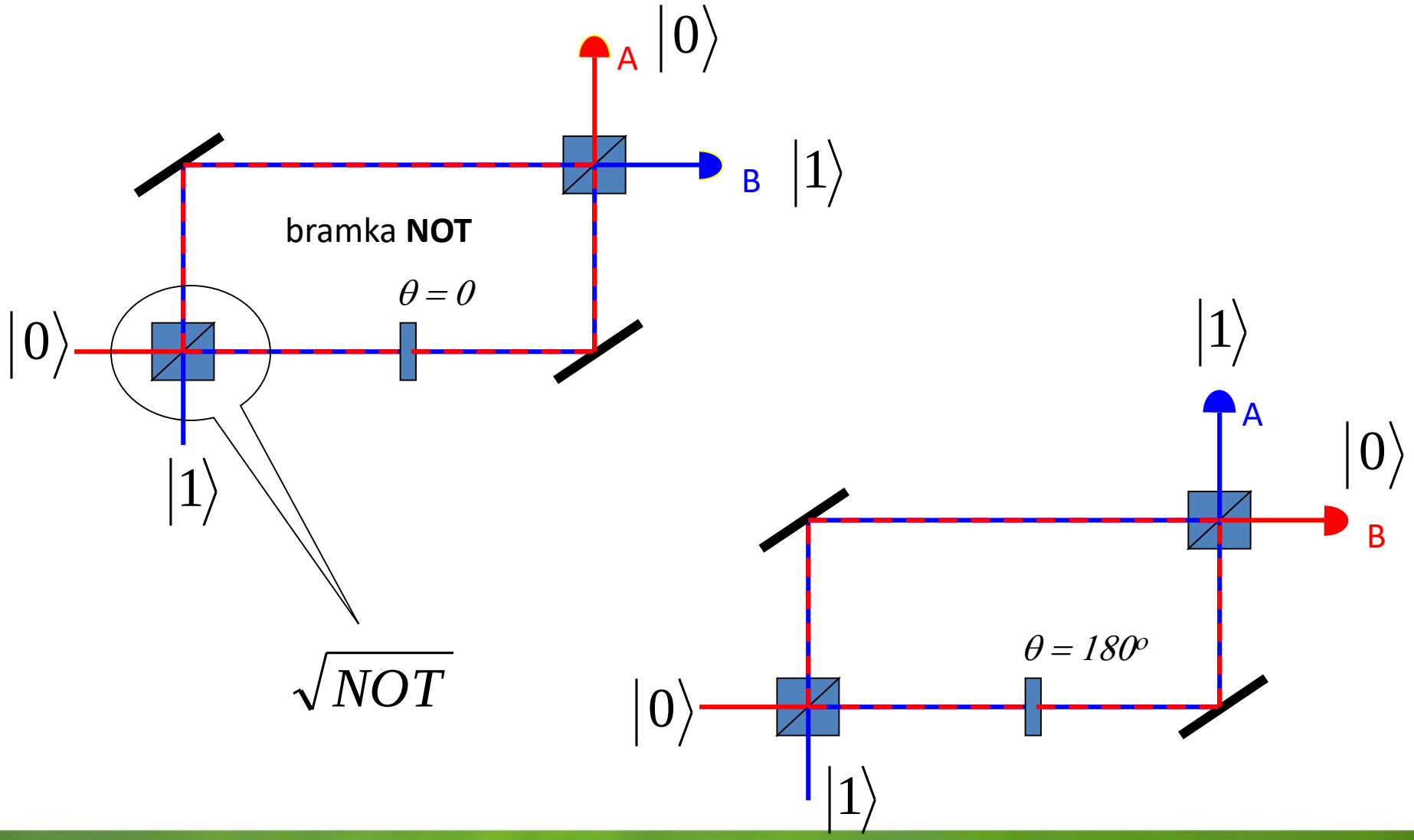
W zależności od fazy θ możemy otrzymać wynik:





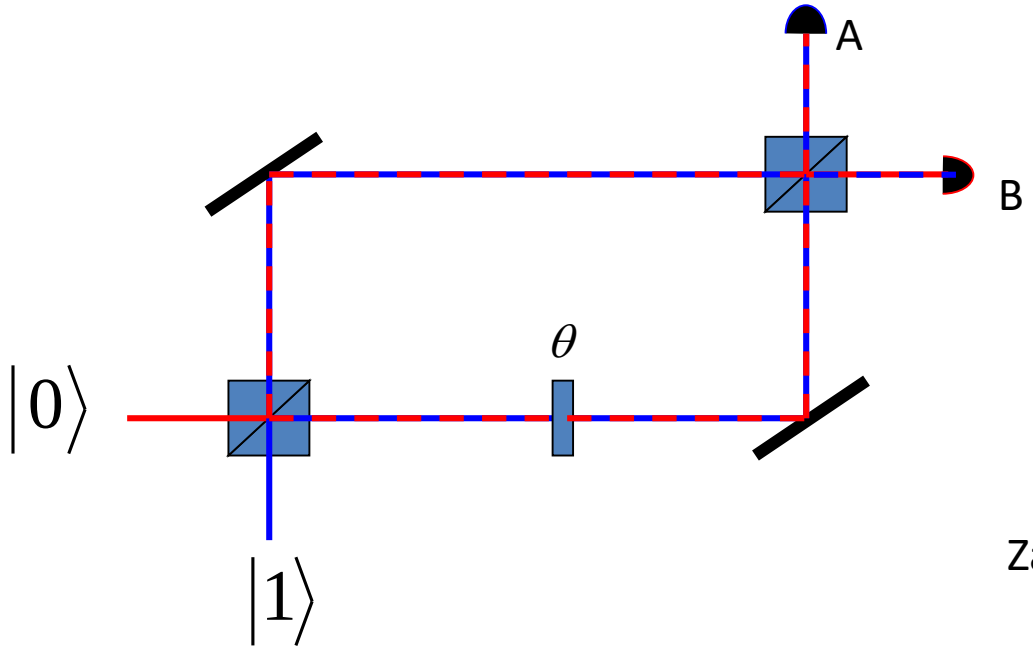
Bramki kubitowe

W zależności od fazy θ możemy otrzymać wynik:



Bramki kubitowe

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



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

Zależą od θ

Matematycznie:

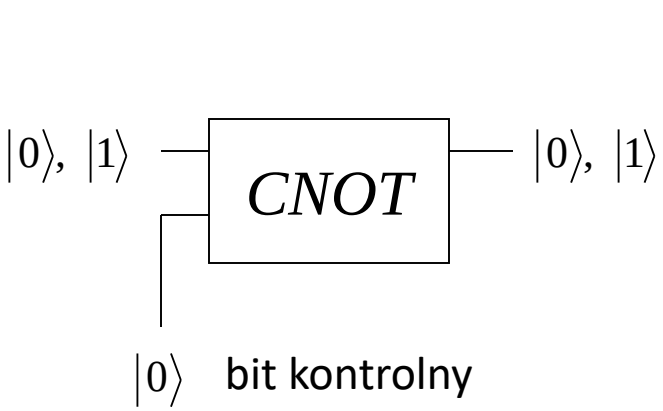
$$\begin{pmatrix} |\Psi\rangle \\ |\Psi'\rangle \end{pmatrix} = \begin{vmatrix} \alpha & \beta \\ \alpha' & \beta' \end{vmatrix} \begin{pmatrix} |0\rangle \\ |1\rangle \end{pmatrix} = \left| U \right| \begin{pmatrix} |0\rangle \\ |1\rangle \end{pmatrix}$$

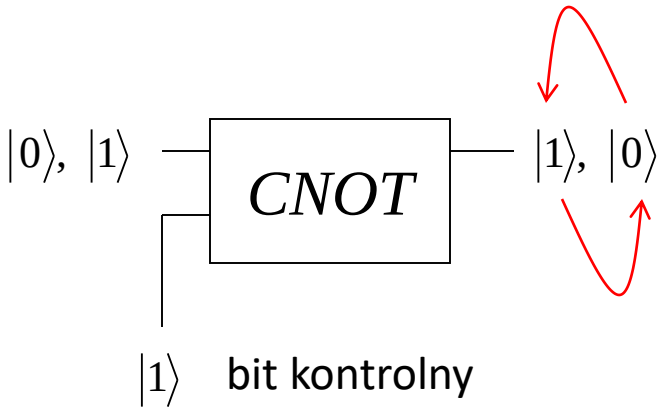
przekształcenie unitarne

Bramki kubitowe

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

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





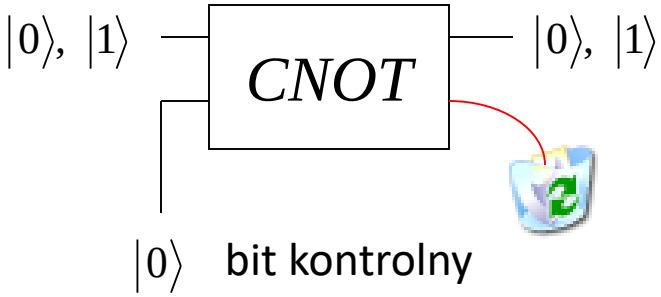
Bramki CNOT są bramkami „uniwersalnymi” – można za ich pomocą zbudować dowolny obwód logiczny.

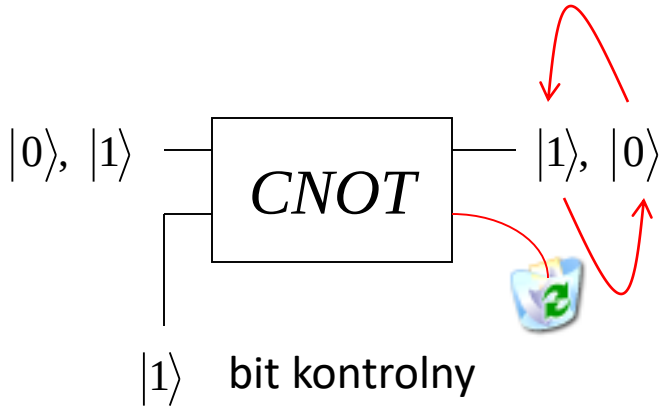
Bramki kubitowe

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

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

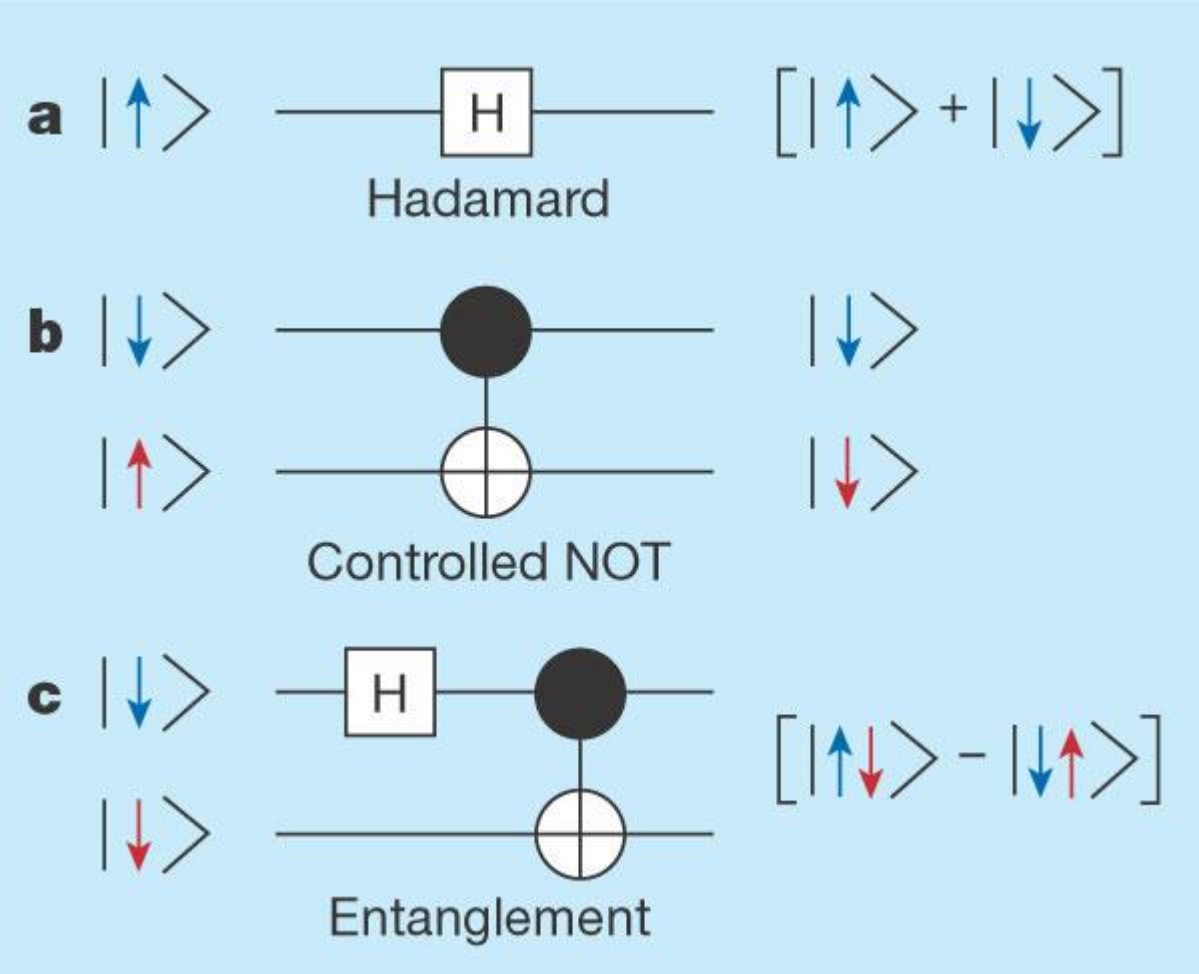
Bramki kwantowe muszą być odwracalne!





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

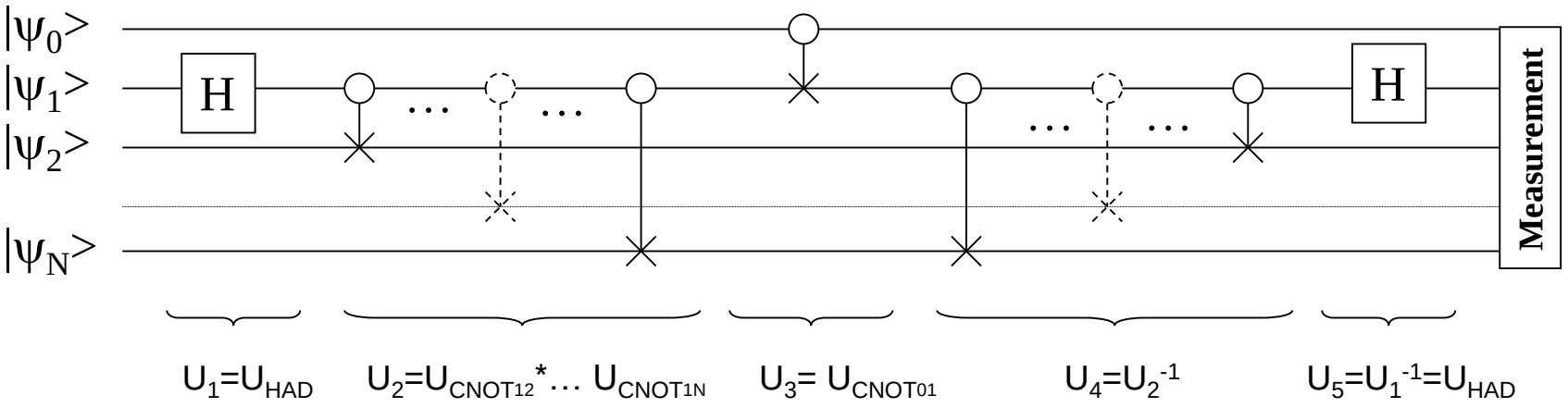
Bramki kubitowe



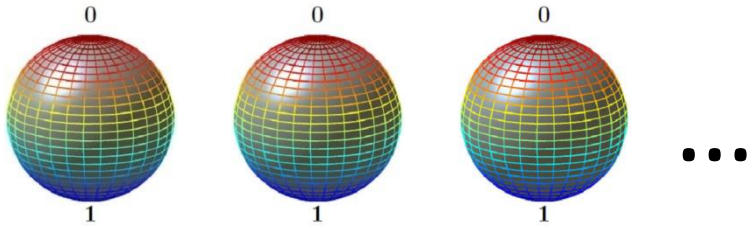
Quantum computing: The qubit duet
Gianni Blatter
Nature 421, 796-797 (20 February 2003)

Bramki kubitowe

Program:



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

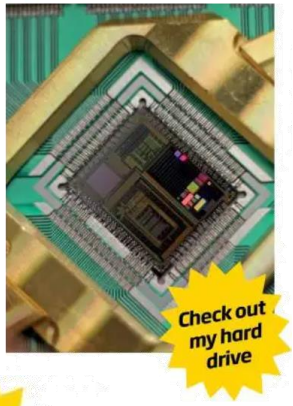
Buyers' guide

Which quantum computer is right for you?

There are many types to choose from. Here's how they compare and our all-important verdict

- Factorisation
- Backward search
- Optimisation
- Quantum simulation

	D-Wave 2	Superconducting qubits	Spin qubits	Trapped ion qubits	Topological qubits	Photonic qubits
Estimated time before useful (years)	1	10	15	10	25	20
Apps	●	● ● ● ●	● ● ● ●	● ● ● ●	● ● ● ●	● ● ● ●
Room temperature operation in future	○	○	●	●	○	●
Error correction	○	●	●	●	●	●
Upgradeability	■■■■■■	■■■■■■■■	■■■■■■	■■■	■■■	■■■■■■
Quantumness	■■	■■■■■	■■■■■	■■■■■	■■■■■	■■■■■
Ease of use	■■	■■■■■	■■■	■■■■■	■	■■■
New Scientist says	👍👍	👍👍👍👍👍	👍👍👍👍	👍👍👍	👍👍	👍👍👍



https://www.newscientist.com/round-up/quantum-buyers-guide/

Kwantowe procedury:

Komputer klasyczny:

$$T_n(m) = p$$

p = wynik

m = dane wejściowe

n = numer programu („kod”)

n = 00101110101101001001000111101101110101 1...
m = 01010010101010101111111000000000000000 0...
p = 01010010101010101111111010000000000000 0...

Kwantowe procedury:

Komputer klasyczny:

$$T_n(m) = p$$

p = wynik

m = dane wejściowe

n = numer programu („kod”)

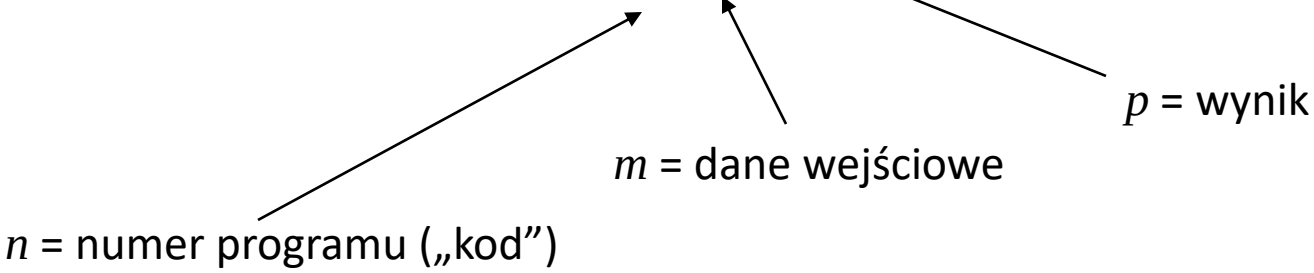
n = 00101110101101001001000111101101110101 1...

m = tak samo, ale zamiast bitów mamy kubity Ψ

p = 01010010101010101111110100000000000000...

Kwantowe procedury:

Komputer klasyczny: $T_n(m)=p$



n = 00101110101101001001000111101101110101 1...

m = tak samo, ale zamiast bitów mamy kubity Ψ

p = 01010010101010101111110100000000000000 0...

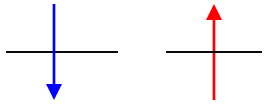
Komputer kwantowy: $Q_n(\Psi)=p$

Kwantowe procedury:

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

Jeden kubit:

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



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

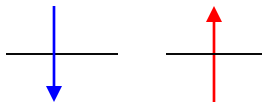
$$\alpha_0^2 + \alpha_1^2 = 1$$

Kwantowe procedury:

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

Jeden kubit:

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

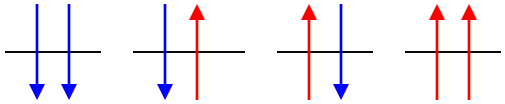


rejestr: $|\Psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$

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

Dla dwóch kubitów:

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



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

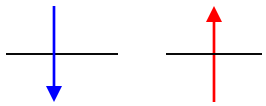
$$\alpha_{00}^2 + \alpha_{01}^2 + \alpha_{10}^2 + \alpha_{11}^2 = 1$$

Kwantowe procedury:

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

Jeden kubit:

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

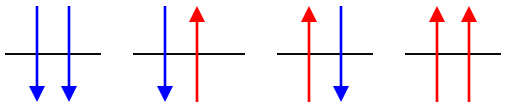


rejestr: $|\Psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$

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

Dla dwóch kubitów:

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

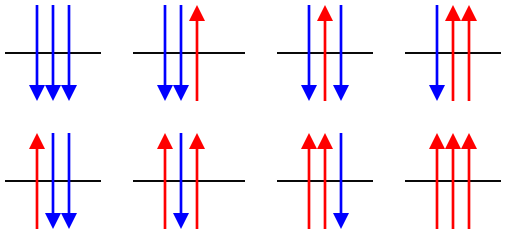


rejestr: $|\Psi\rangle = \alpha_{00}|0\rangle|0\rangle + \alpha_{01}|0\rangle|1\rangle + \alpha_{10}|1\rangle|0\rangle + \alpha_{11}|1\rangle|1\rangle$

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

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:

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

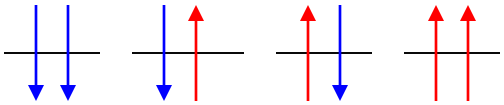
Ogólnie jeden rejestr N-kubitowy może przechować 2^N „klasycznych” liczb!

Kwantowe procedury:

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

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

$|0\rangle|0\rangle, |0\rangle|1\rangle, |1\rangle|0\rangle, |1\rangle|1\rangle$



0 1 2 3

Na przykład: Dla dwóch kubitów baza obliczeń:

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

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

$$|\Psi\rangle = \frac{1}{2}\left(|0\rangle + |1\rangle + |2\rangle + |3\rangle\right)$$ ← 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!

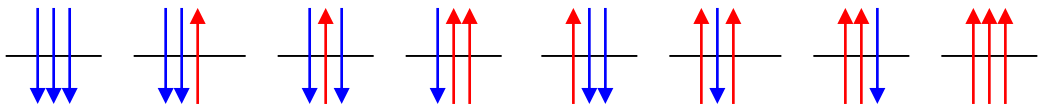
Dla **trzech** kubitów baza obliczeń:

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

$|\uparrow\rangle|\downarrow\rangle|\downarrow\rangle, |\uparrow\rangle|\downarrow\rangle|\uparrow\rangle, |\uparrow\rangle|\uparrow\rangle|\downarrow\rangle, |\uparrow\rangle|\uparrow\rangle|\uparrow\rangle,$

$$|\Psi\rangle = \alpha_{000}|\downarrow\rangle|\downarrow\rangle|\downarrow\rangle + \alpha_{001}|\downarrow\rangle|\downarrow\rangle|\uparrow\rangle + \alpha_{010}|\downarrow\rangle|\uparrow\rangle|\downarrow\rangle + \alpha_{011}|\downarrow\rangle|\uparrow\rangle|\uparrow\rangle +$$
$$+ \alpha_{100}|\uparrow\rangle|\downarrow\rangle|\downarrow\rangle + \alpha_{101}|\uparrow\rangle|\downarrow\rangle|\uparrow\rangle + \alpha_{110}|\uparrow\rangle|\uparrow\rangle|\downarrow\rangle + \alpha_{111}|\uparrow\rangle|\uparrow\rangle|\uparrow\rangle$$

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



0 1 2 3 4 5 6 7

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**.

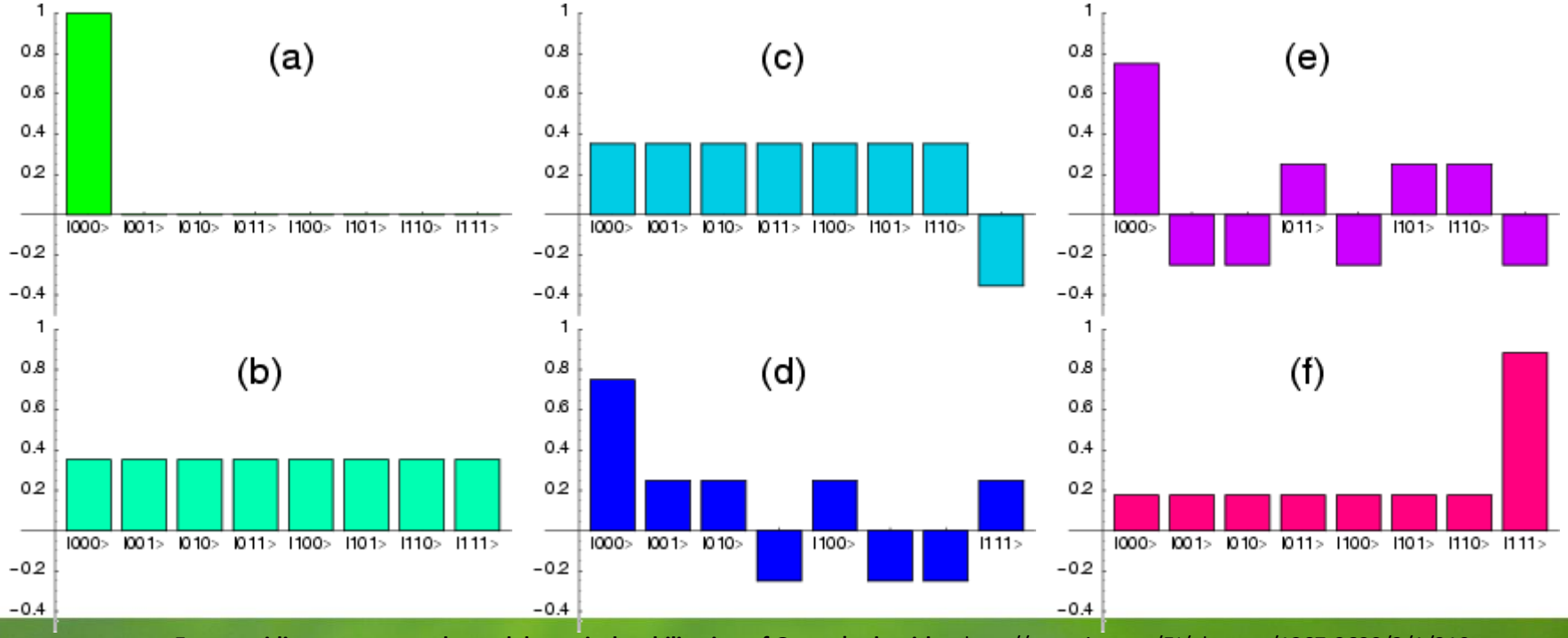
Pewne algorytmy będą działały szybciej na komputerze kwantowym.
Przede wszystkim te wymagające obliczeń równoległych: łamanie kodów, gra w szachy, przeszukiwanie baz danych, symulacje pogody, trzęsień ziemi, wybuchów jądrowych itp.

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 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!

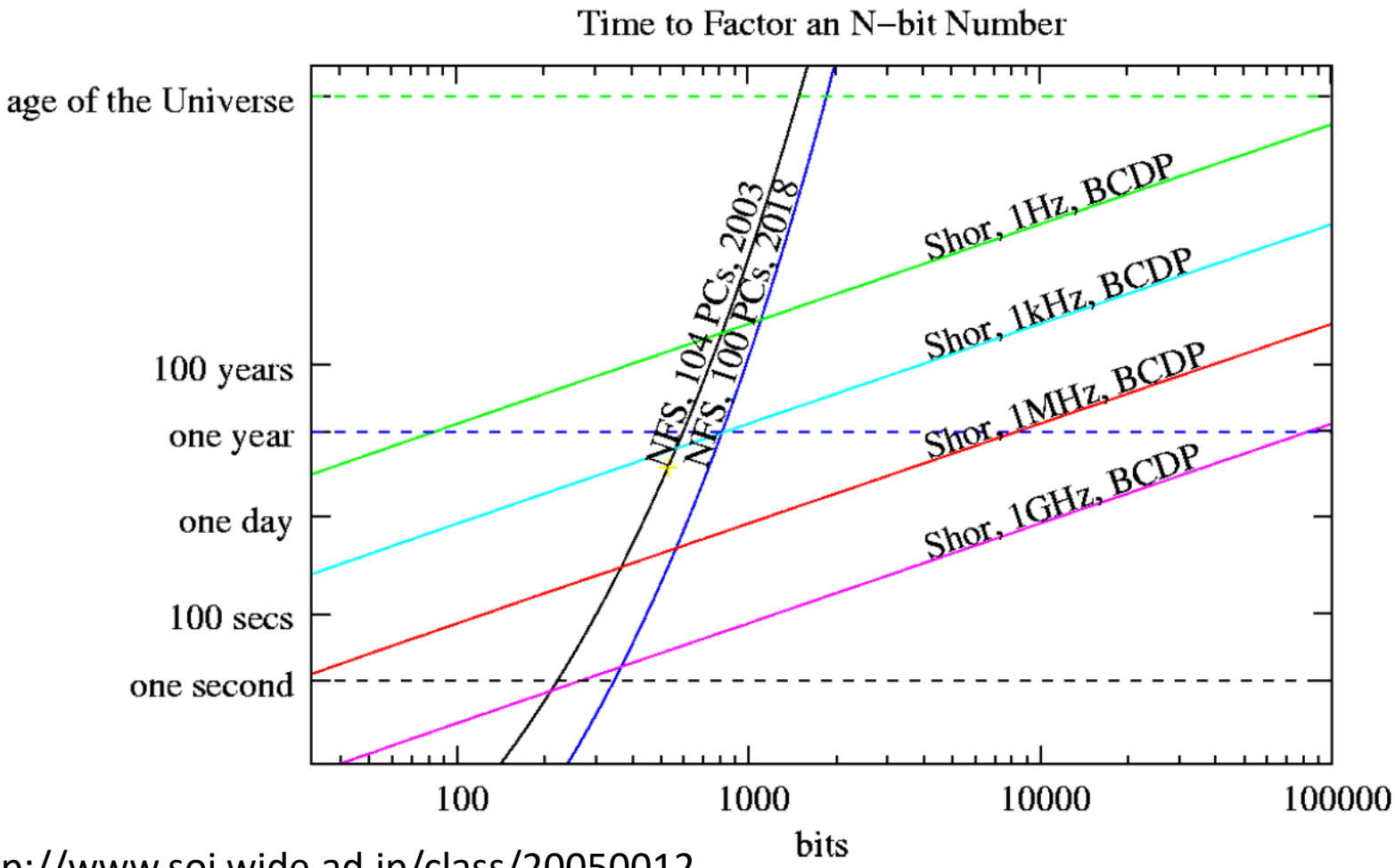
- W 1994 r. RSA 129 został złamany na 1600 stacjach roboczych w ciagu 8 miesiecy
- Algorytm kwantowy Petera Shora wymaga czasu

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

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

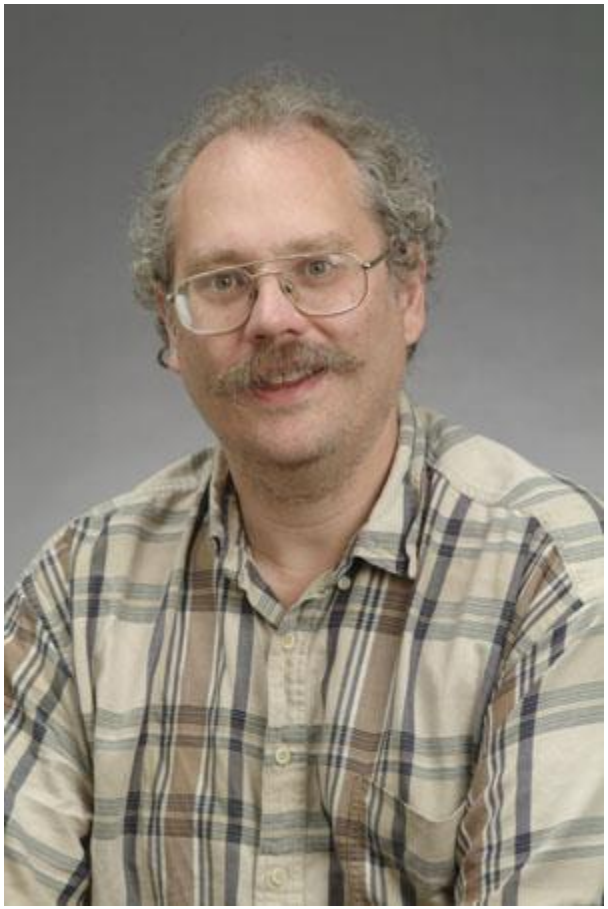
Algorytm Shora

Factoring Larger Numbers



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

Algorytm Shora



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

AMS subject classifications: 81P10, 11Y05, 68Q10, 03D10

*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

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. 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

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. 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 $B = X^A \bmod N$, wykorzystując 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

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. 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 $B = X^A \bmod N$, wykorzystując 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

- Zauważamy, że wyniki w rejestrze B sa okresowe z okresem r = 4

Komputer kwantowy potrafi szybko znajdować 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

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 NWD P i N. W naszym przykładzie $r = 4$ i $P = 2^{4/2} - 1 = 3$ lub $P = 2^{4/2} + 1 = 5$.

$15/3 = 5$

$15/5 = 3$

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 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 $B = X^A \bmod N$, wykorzystując 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

• Zauważamy, ze wyniki w rejestrze B sa okresowe z okresem r = 4
Komputer kwantowy potrafi szybko znajdować okres funkcji!

Algorytm Shora

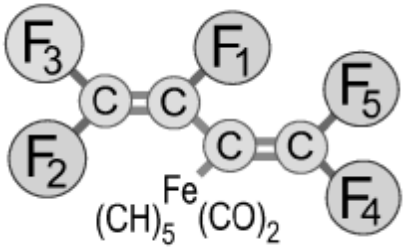
VOLUME 85, NUMBER 25 PHYSICAL REVIEW LETTERS 18 DECEMBER 2000

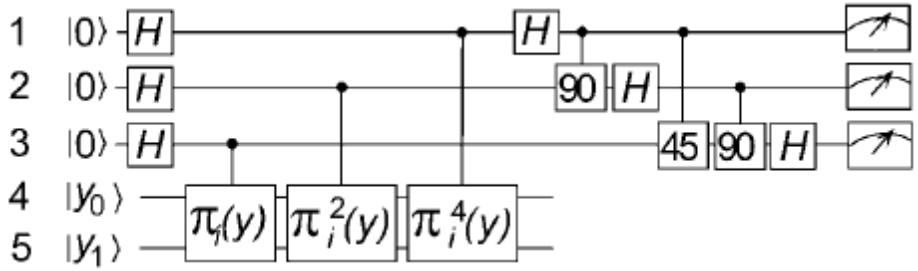
Experimental Realization of an Order-Finding Algorithm with an NMR Quantum Computer

Lieven M. K. Vandersypen,[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.

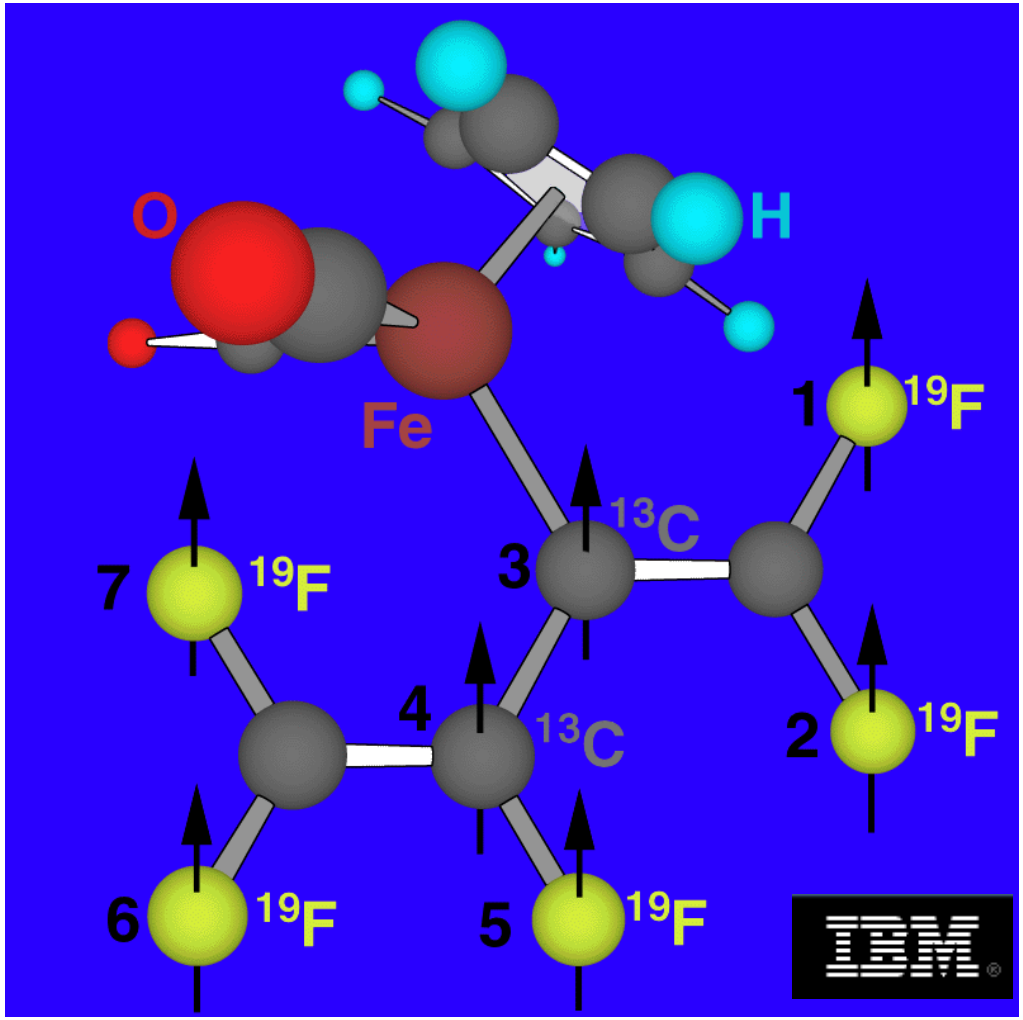


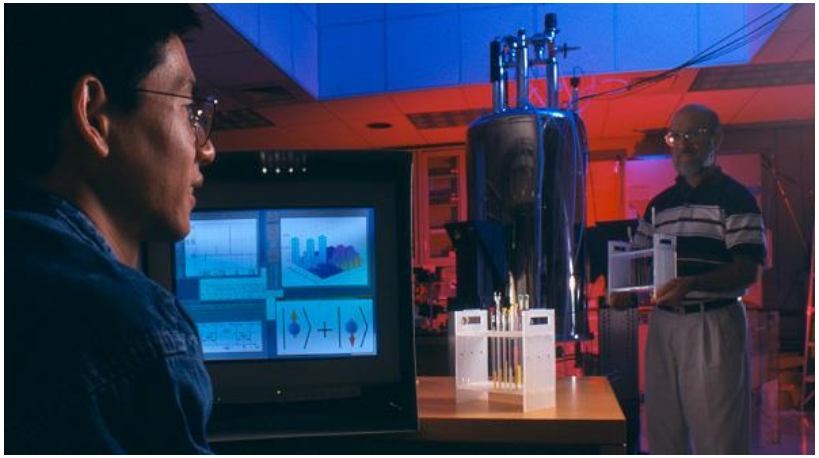


pentafluorobutadienyl cyclopentadienyldicarbonyliron complex

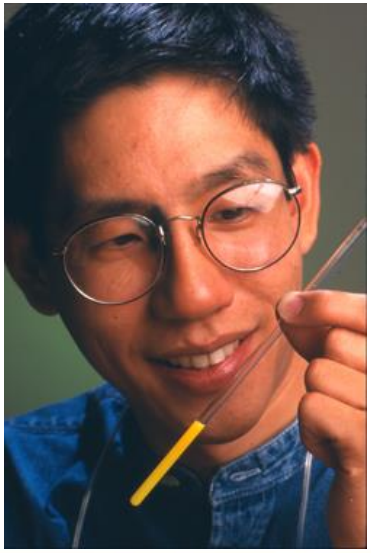
Komputery kwantowe

7 Qubits





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



19.12.2001

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

Algorytmy kwantowe

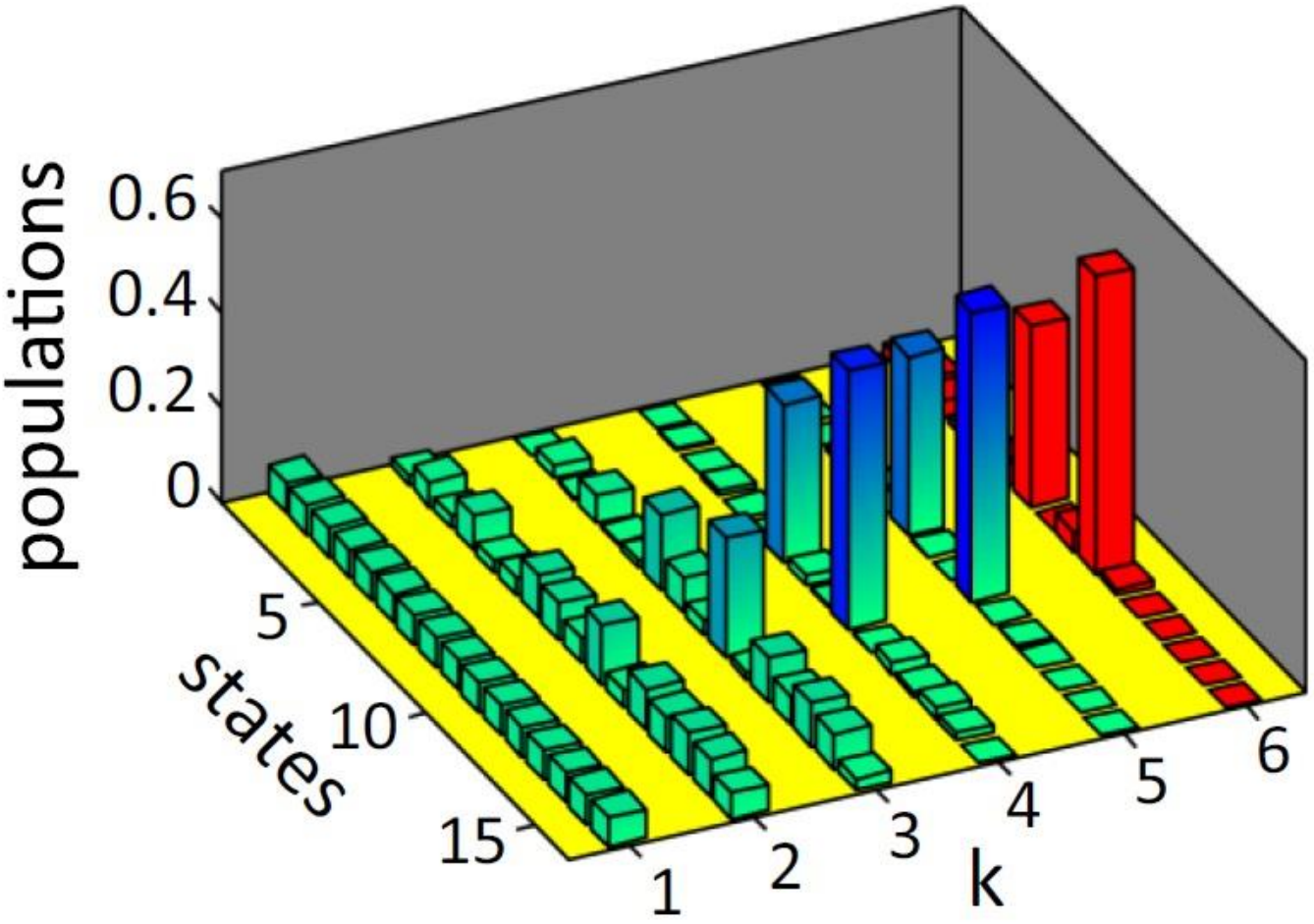
Table 5: *Quantum factorization records*

Number	# of factors	# of qubits needed	Algorithm	Year implemented	Implemented without prior knowledge of solution
15	2	8	Shor	2001 [2]	×
	2	8	Shor	2007 [3]	×
	2	8	Shor	2007 [3]	×
	2	8	Shor	2009 [5]	×
	2	8	Shor	2012 [6]	×
21	2	10	Shor	2012 [7]	×
143	2	4	minimization	2012 [1]	✓
56153	2	4	minimization	2012 [1]	✓
291311	2	6	minimization	not yet	✓
175	3	3	minimization	not yet	✓

http://phys.org/news/2014-11-largest-factored-quantum-device.html

Algorytmy kwantowe

143 is largest number yet to be factored by a quantum algorithm



http://phys.org/news/2012-04-largest-factored-quantum-algorithm.html

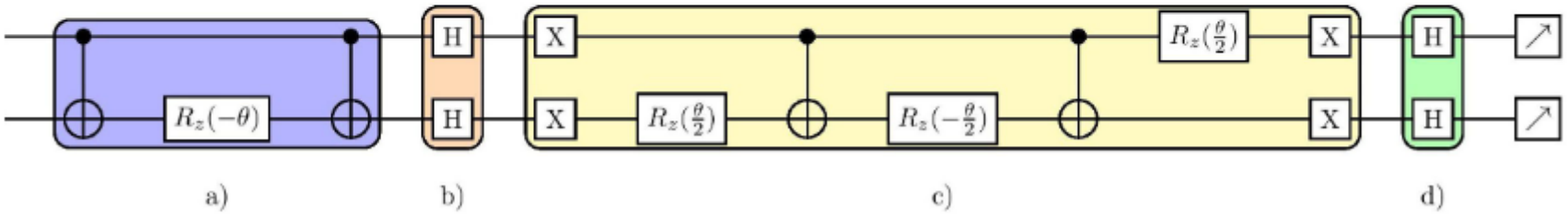
Algorytmy kwantowe

Exact search algorithm to factorize large biprimes and a triprime on IBM quantum computer

Avinash Dash, Deepankar Sarmah, Bikash K. Behera, and Prasanta K. Panigrahi
Department of Physical Sciences, Indian Institute of Science Education and Research Kolkata, Mohanpur, 741246, West Bengal, India

SUPPLEMENTARY INFORMATION: EXACT SEARCH ALGORITHM TO FACTORIZE LARGE BIPRIMES AND A TRIPRIME ON IBM QUANTUM COMPUTER

Circuit used for the factorization of $N = 4088459$



Algorytmy kwantowe

Quantum factorization of 56153 with only 4 qubits

Nikesh S. Dattani,[1,2,*] **Nathaniel Bryans**[3,†]
[1]Quantum Chemistry Laboratory, Kyoto University, 606-8502, Kyoto, Japan, [2]Physical & Theoretical Chemistry Laboratory, Oxford University, OX1 3QZ, Oxford, UK, [3]University of Calgary, T2N 4N1, Calgary, Canada. *dattani.nike@gmail.com, †nbryans1@gmail.com

December 1, 2014

Table 5: *Quantum factorization records*

Number	# of factors	# of qubits needed	Algorithm	Year implemented	Implemented without prior knowledge of solution
15	2	8	Shor	2001 [2]	✗
	2	8	Shor	2007 [3]	✗
	2	8	Shor	2007 [3]	✗
	2	8	Shor	2009 [5]	✗
	2	8	Shor	2012 [6]	✗
21	2	10	Shor	2012 [7]	✗
143	2	4	minimization	2012 [1]	✓
56153	2	4	minimization	2012 [1]	✓
291311	2	6	minimization	not yet	✓
175	3	3	minimization	not yet	✓

Algorytmy kwantowe

Quantum Annealing for Prime Factorization

Shuxian Jiang[1], Keith A. Britt[2], Alexander J. McCaskey[2], Travis S. Humble[*2], and Sabre Kais[†1,3]

[1]Department of Computer Science, Purdue University, West Lafayette, IN 47906
[2]Quantum Computing Institute, Oak Ridge National Laboratory, Oak Ridge, TN 37831
[3]Department of Chemistry, Physics and Birck Nanotechnology Center, Purdue University, West Lafayette, IN 47906

Abstract

We have developed a framework to convert an arbitrary integer factorization problem to an executable Ising model by first writing it as an optimization function and then transforming the k-bit coupling ($k \geq 3$) terms to quadratic terms using ancillary variables. Our resource-efficient method uses $\mathcal{O}(\log^2(N))$ binary variables (qubits) for finding the factors of an integer N. We present how to factorize 15, 143, 59989, and 376289 using 4, 12, 59, and 94 logical qubits, respectively. This method was tested using the D-Wave 2000Q for finding an embedding and determining the prime factors for a given composite number. The method is general and could be used to factor larger integers as the number of available qubits increases.

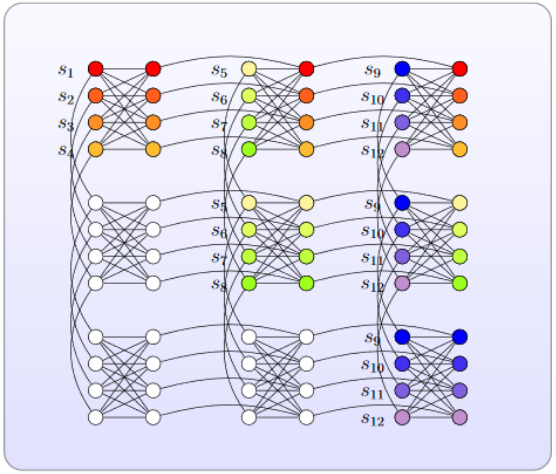
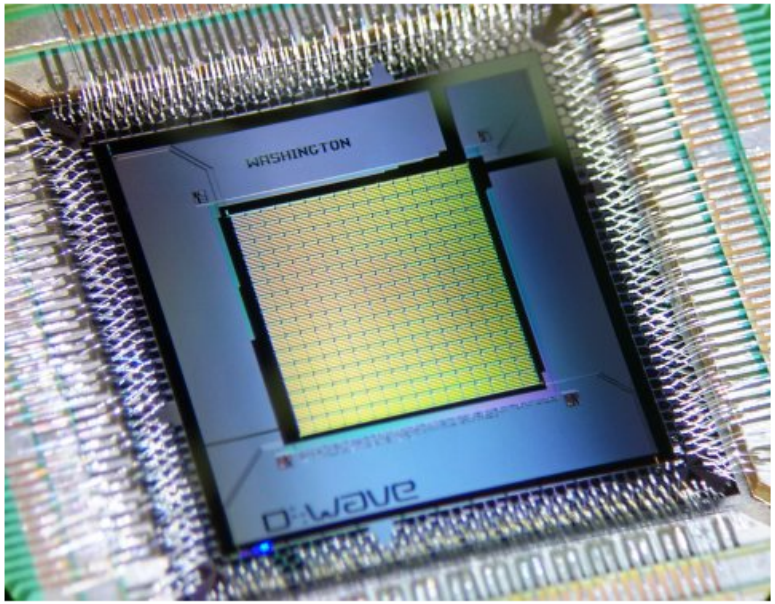


Figure 2: Embedding the factoring instance $N = 143$ to Chimera graph. The nodes with the same color denote the same original qubit, with their connected lines corresponding to strong couplings. The left footnotes refer to which spin the node was embedded.



JUN 22, 2015

D-Wave Systems Breaks the 1000 Qubit Quantum Computing Barrier

New Milestone Will Enable System to Address Larger and More Complex Problems

Palo Alto, CA – June 22, 2015 – D-Wave Systems Inc., the world's first quantum computing company, today announced that it has broken the 1000 qubit barrier, developing a processor about double the size of D-Wave's previous generation and far exceeding the number of qubits ever developed by D-Wave or any other quantum effort. This is a major technological and scientific achievement that will allow significantly more complex computational problems to be solved than was possible on any previous quantum computer.

Poważny problem

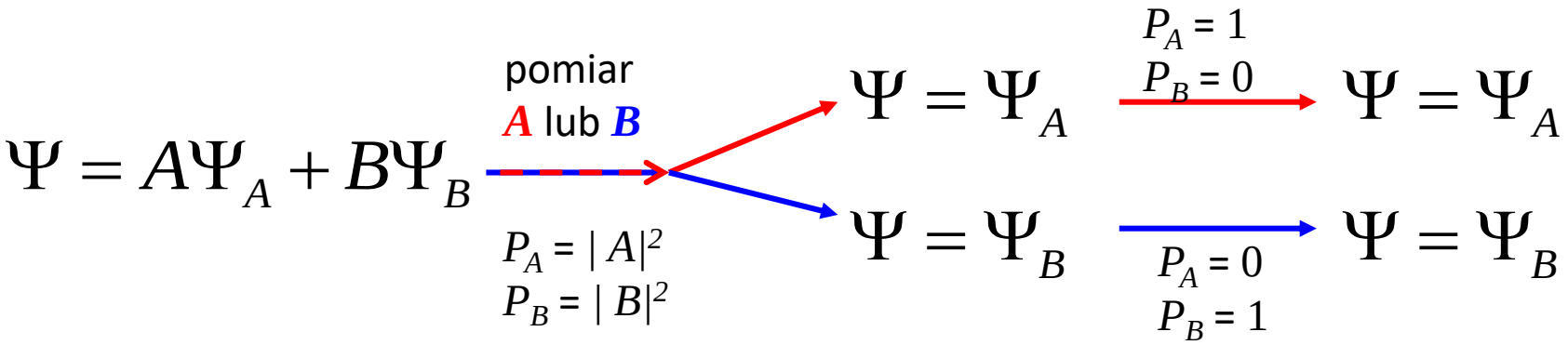
Skoro to takie proste, to dlaczego
to jeszcze nie działa?

Poważny problem

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

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*)



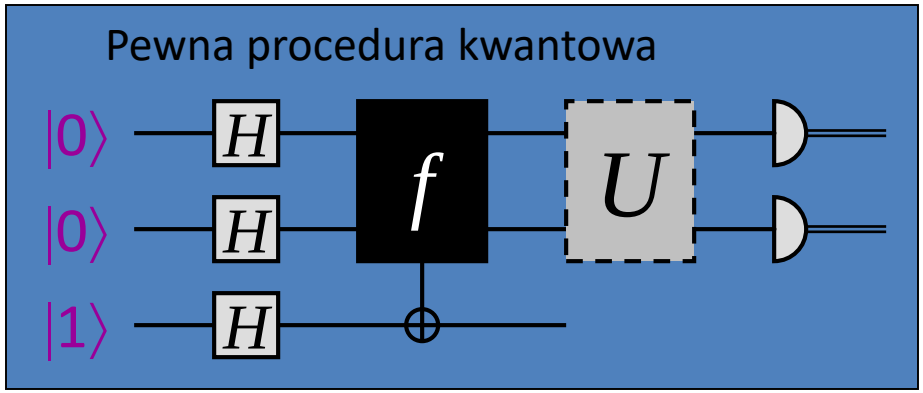
Zakaz klonowania sprawia, że nie można się dowiedzieć wartości każdej ze składowych A lub B z osobna.

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

Poważny problem

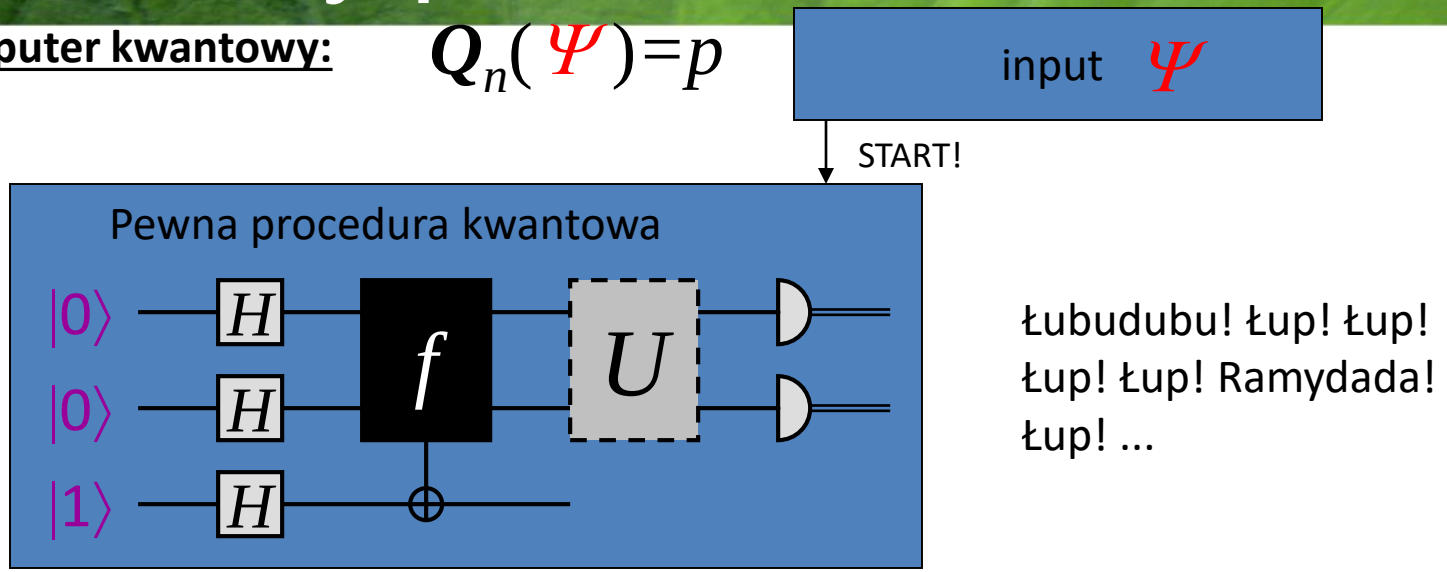
Komputer kwantowy: $Q_n(\Psi)=p$

input Ψ



Poważny problem

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

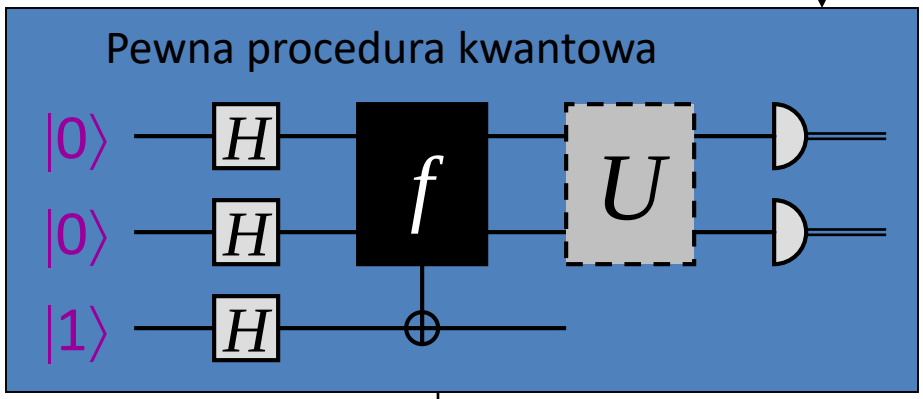


Łubudubu! Łup! Łup!
Łup! Łup! Ramydada!
Łup! ...

Poważny problem

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

input Ψ

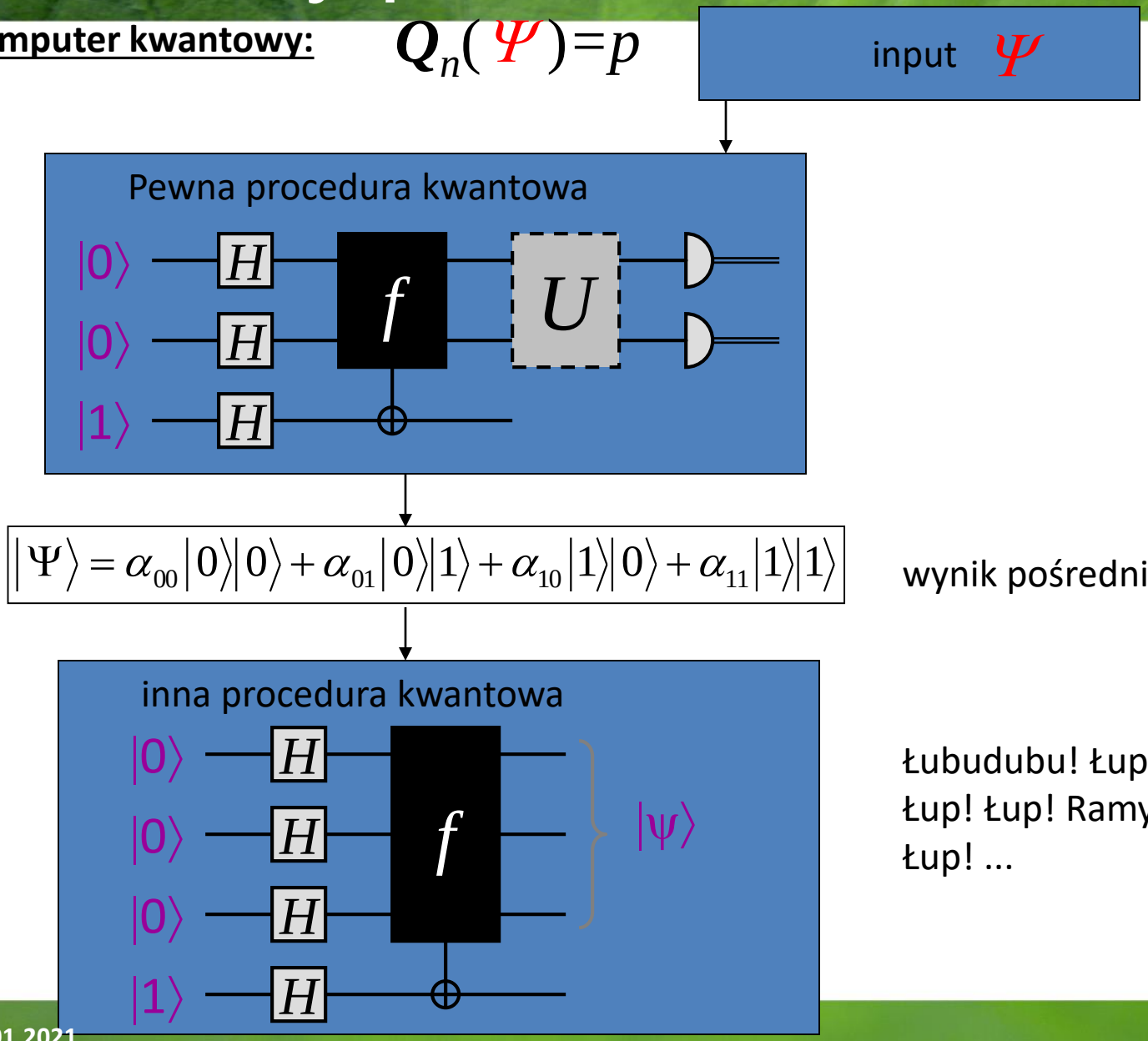


$$|\Psi\rangle = \alpha_{00}|0\rangle|0\rangle + \alpha_{01}|0\rangle|1\rangle + \alpha_{10}|1\rangle|0\rangle + \alpha_{11}|1\rangle|1\rangle$$

wynik pośredni

Poważny problem

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

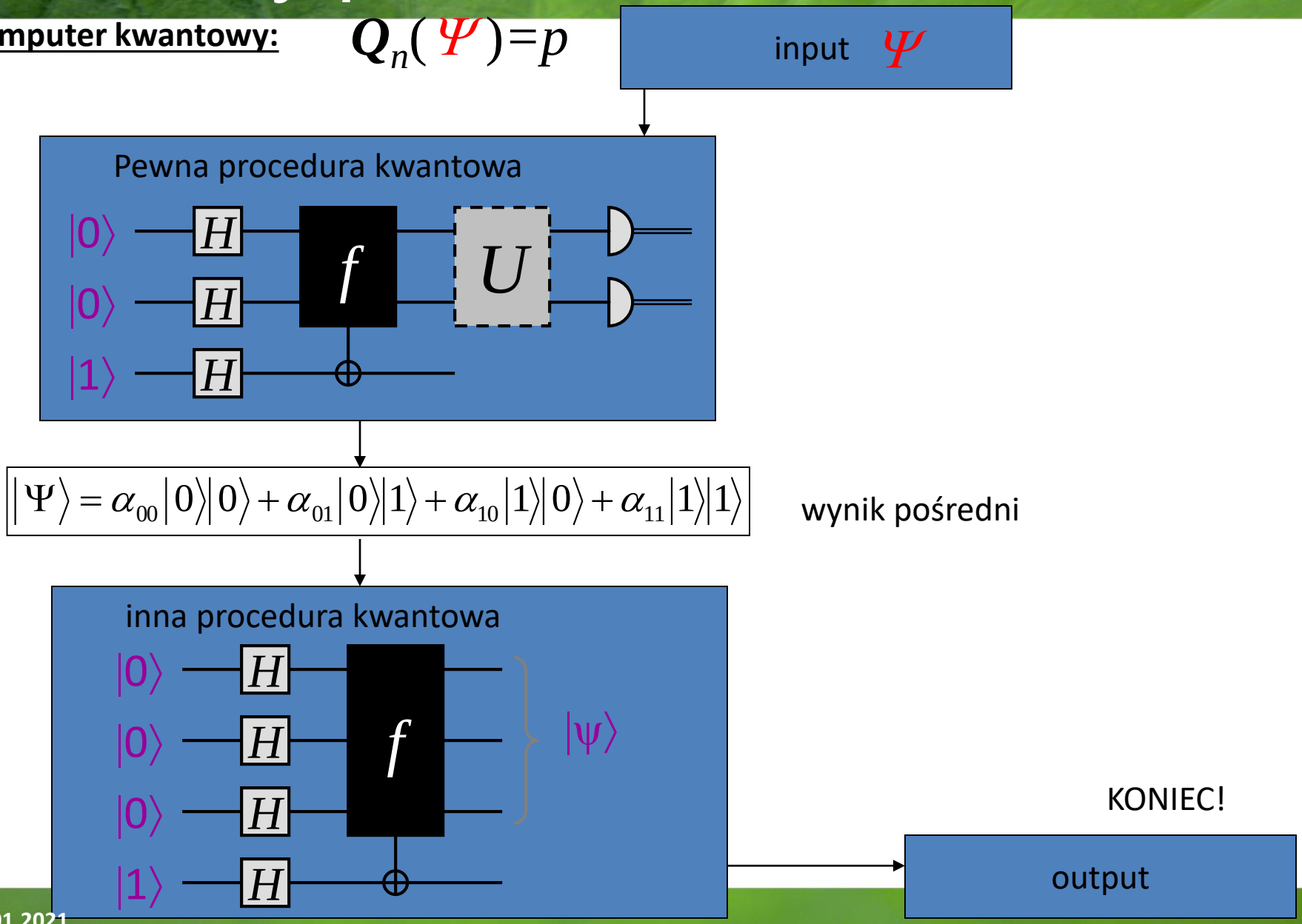


wynik pośredni

Łubudubu! Łup! Łup!
Łup! Łup! Ramydada!
Łup! ...

Poważny problem

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



Poważny problem

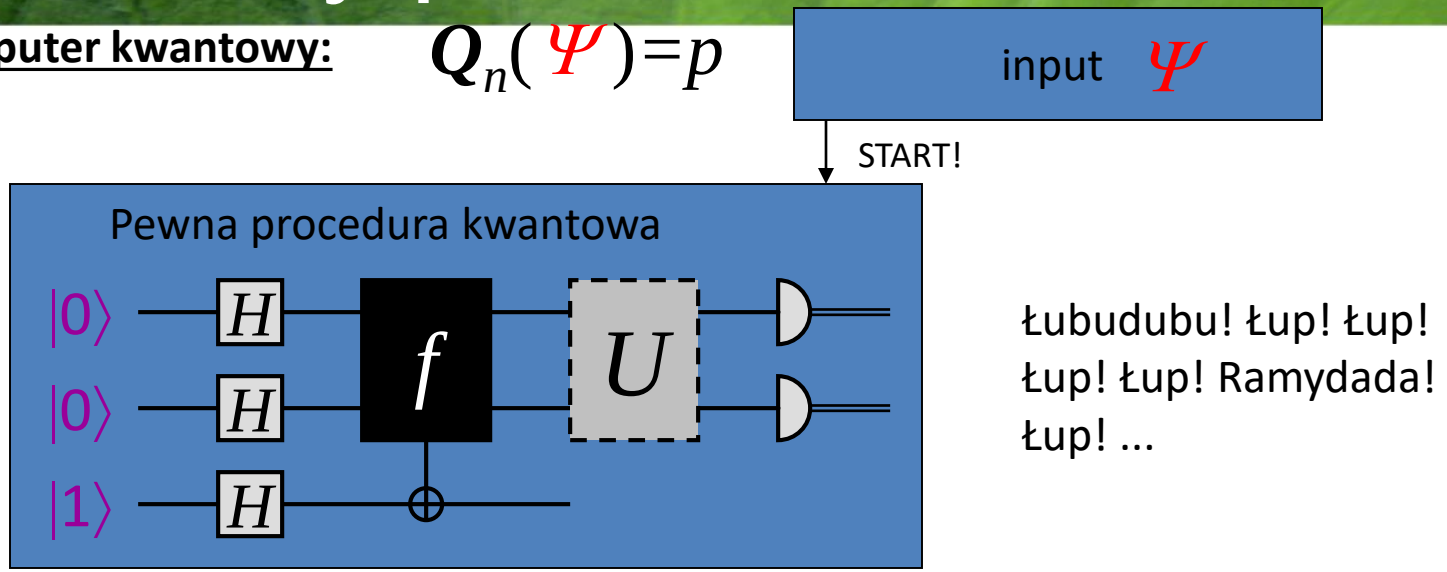
Komputer kwantowy: $Q_n(\Psi)=p$

input Ψ

Tym razem z dekoherencją

Poważny problem

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

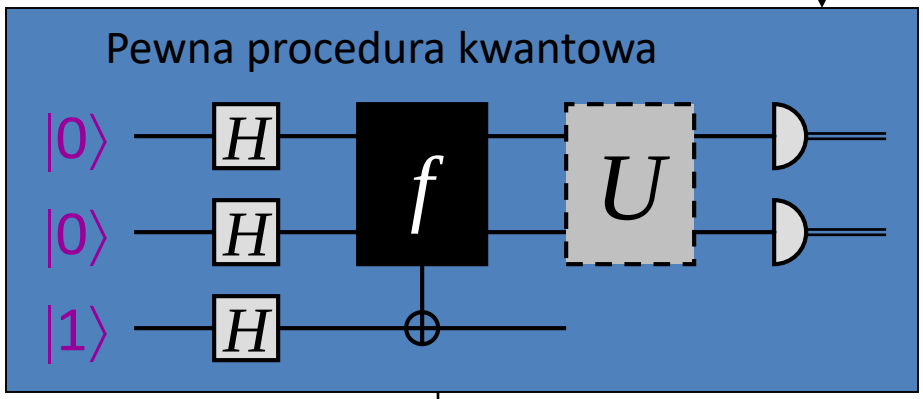


Łubudubu! Łup! Łup!
Łup! Łup! Ramydada!
Łup! ...

Poważny problem

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

input Ψ



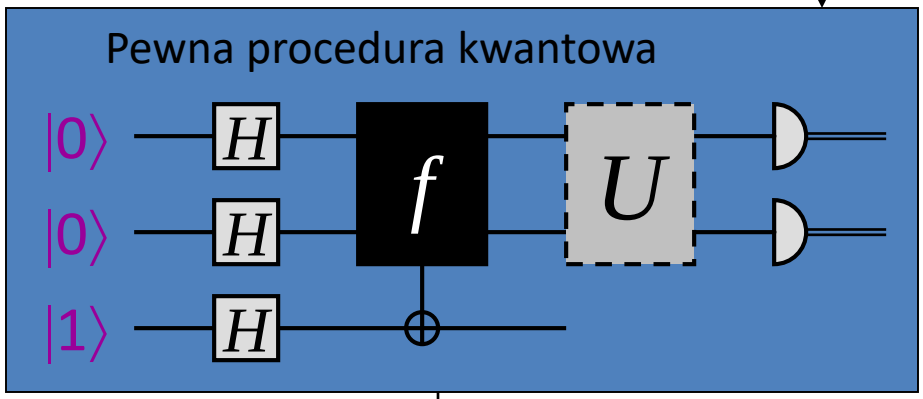
$$|\Psi\rangle = \alpha_{00}|0\rangle|0\rangle + \alpha_{01}|0\rangle|1\rangle + \alpha_{10}|1\rangle|0\rangle + \alpha_{11}|1\rangle|1\rangle$$

wynik pośredni

Poważny problem

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

input Ψ



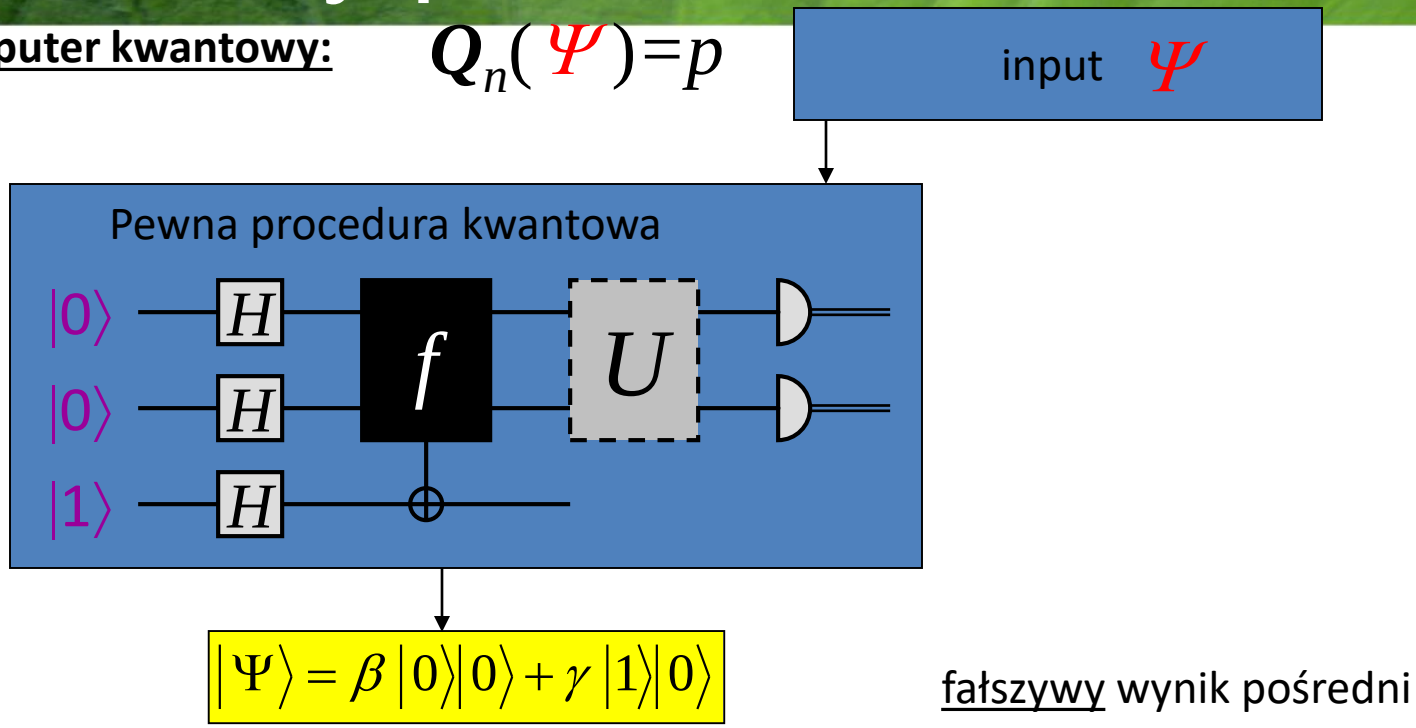
złośliwy foton

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

wynik pośredni

Poważny problem

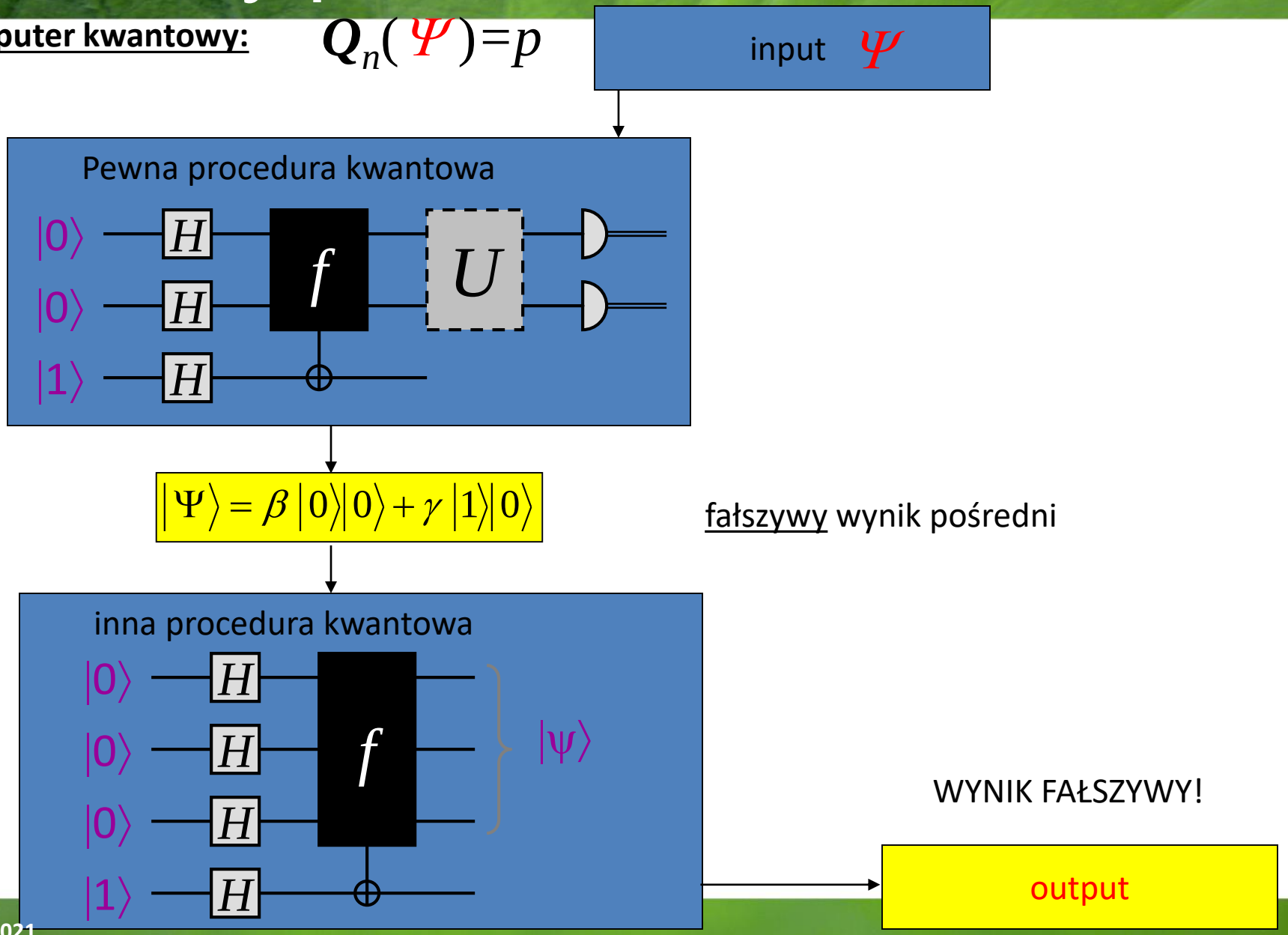
Komputer kwantowy: $Q_n(\Psi)=p$



fałszywy wynik pośredni

Poważny problem

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

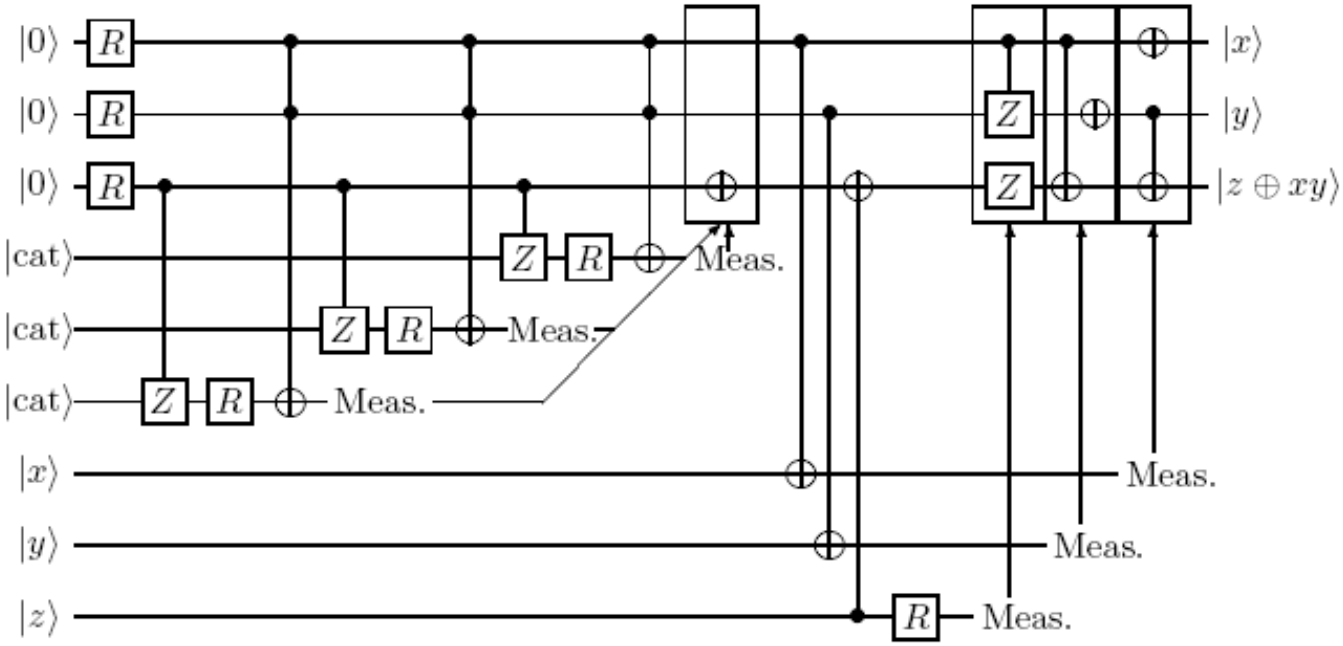


Poważny problem

Rozwiązania:

0 → 000
1 → 111

1. Procedury kwantowej korekcji błędów



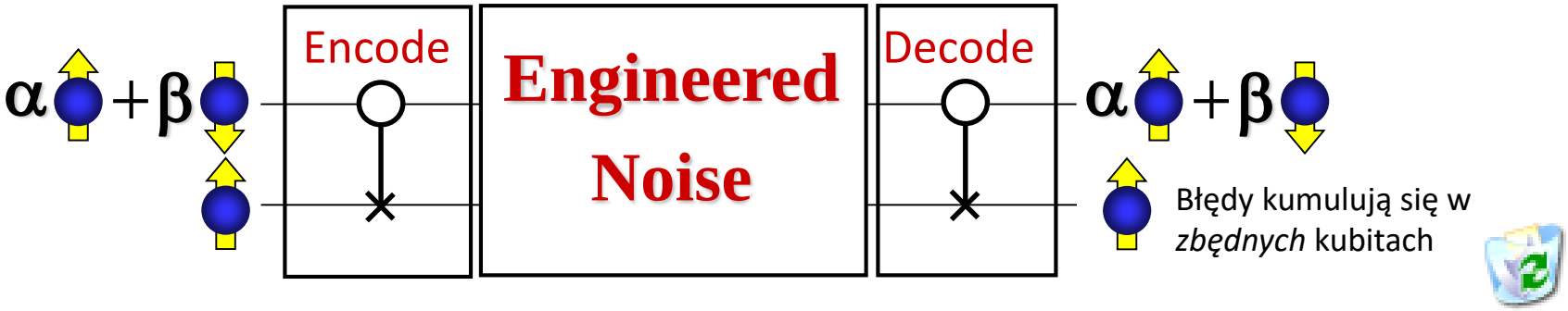
J. Preskill quant-ph/9705031

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

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*

Firefox

Agencja Bezpieczeństwa Narodowego U...

wiadomosci.gazeta.pl/wiadomosci/1,114871,15217697,Agencja_Bezpiec:

zdzisław wilhelmi

Gazeta.pl | Poczta | Radio | Zaloguj się

Gazeta.pl Wiadomości

Lubię to! 101 tys.

Polska | Polityka | Świat | Nauka | Quiz | Rysunki Raczkowskiego | Policyjni | Na żywo | Infoblog | Deser | Zdjęcia

Agencja Bezpieczeństwa Narodowego USA pracuje nad komputerem łamiącym większość zabezpieczeń

Osi, PAP 03.01.2014 10:25

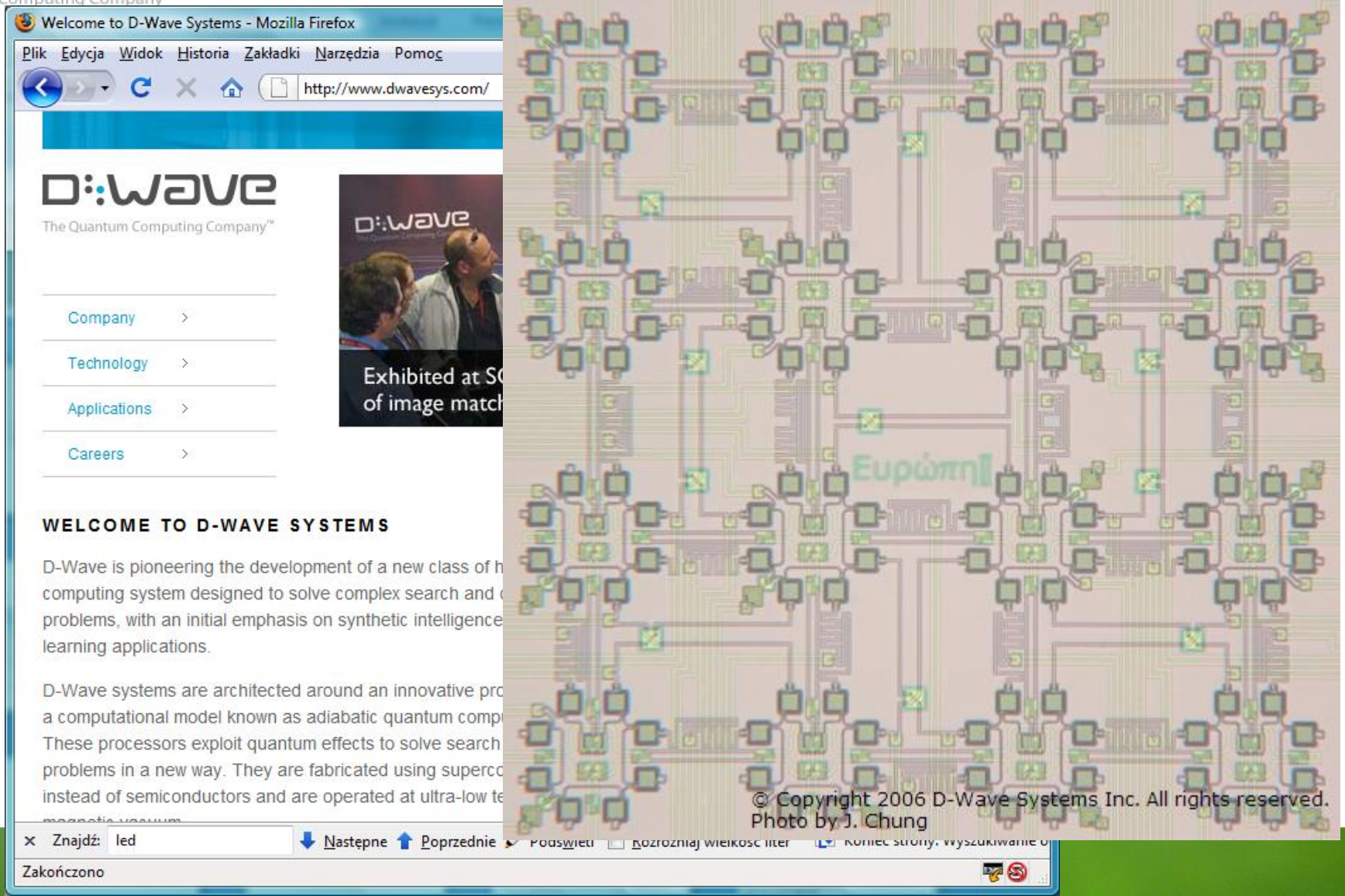
A A A

Najczęściej czytane

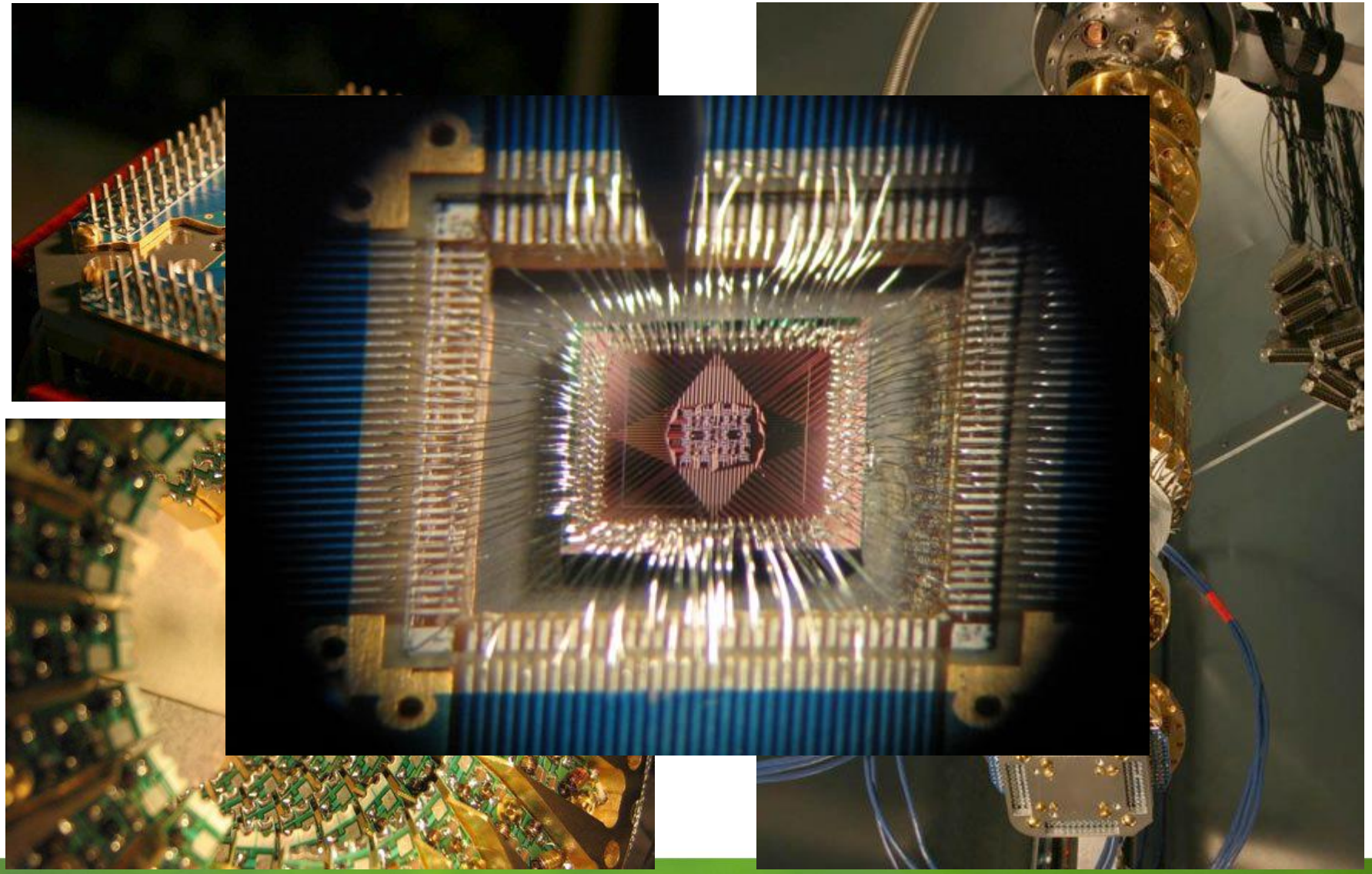
1. Tragedia w Kamieniu Pomorskim. Mężczyzna z zarzutami.
2. ZUS odebrał 2 tys. zł Ewie Wójciak. Na L4 zagrała w
3. 17-letnia Paulina wyszła z domu w sylwestra. Do tej pory nie
4. Zarzut spowodowania katastrofy w ruchu lądowym dla 26-latka,
5. Bili i gwałcili, żeby w ten sposób wymierzyć sprawiedliwość

D:wave

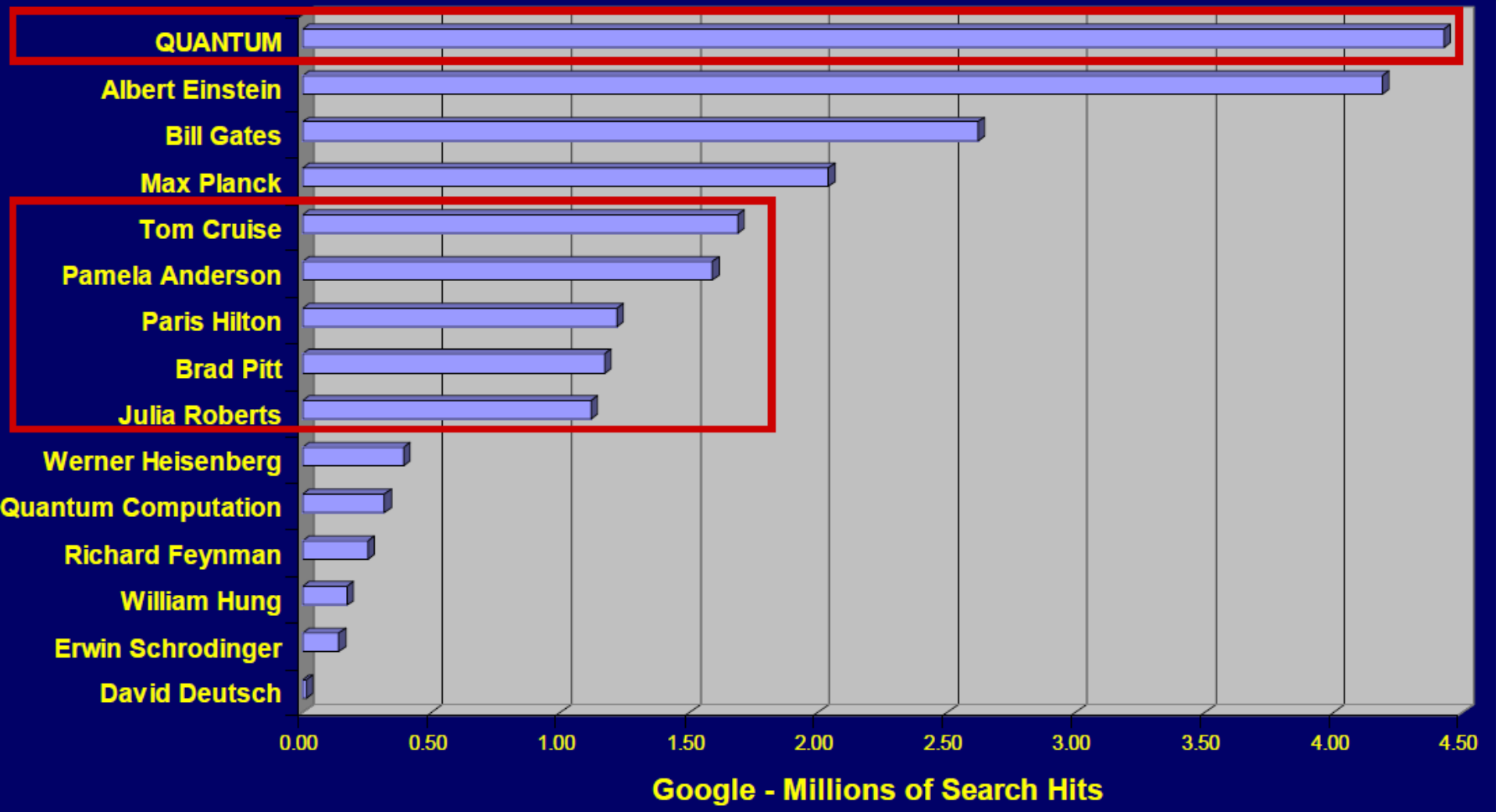
The Quantum Computing Company™



Here’s a view of a 16-qubit processor mounted in its sample holder.



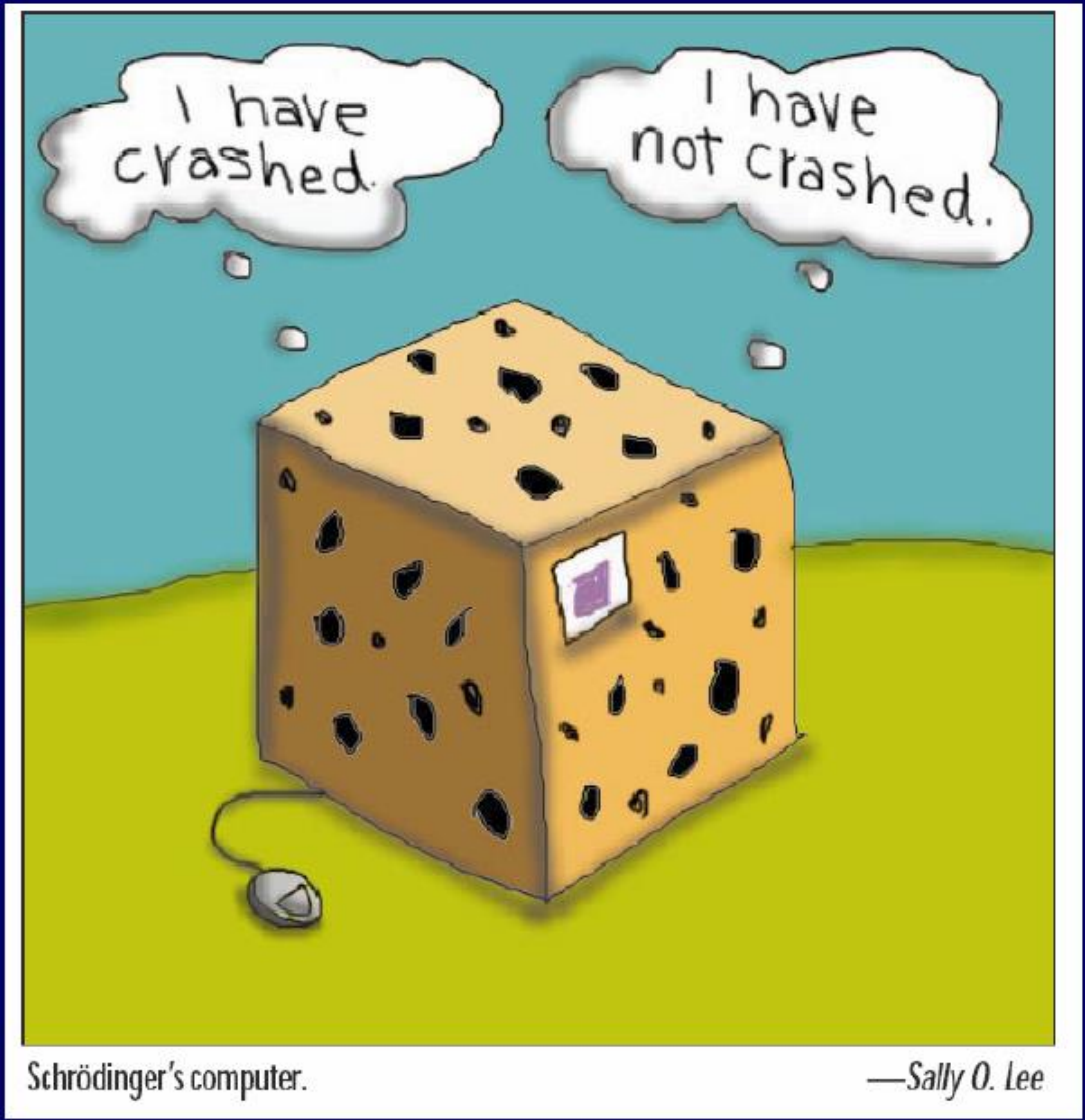
Quantum is Sexy



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

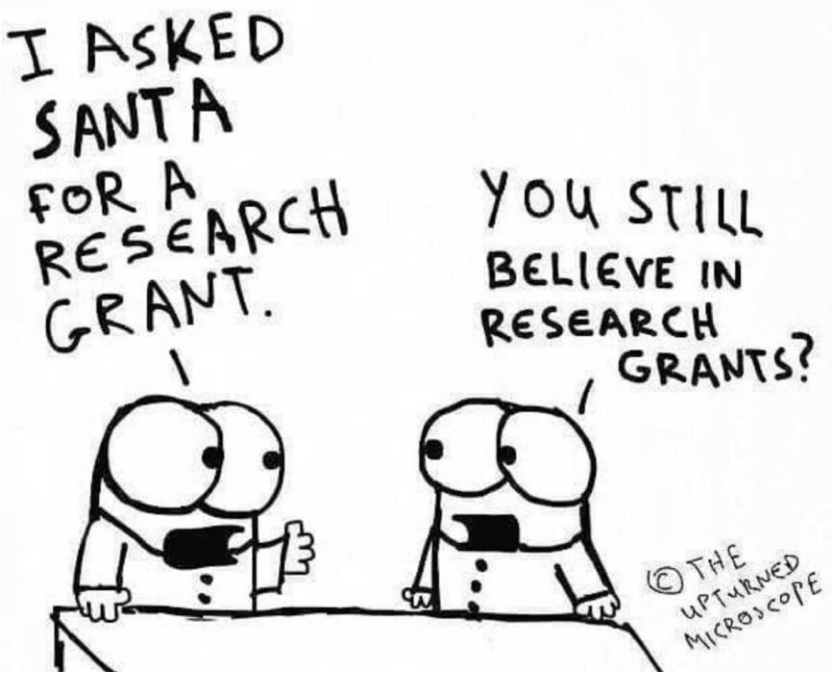
T-Zero Engineering

Qwindows 2098



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

T-Zero Engineering


I ASKED SANTA FOR A RESEARCH GRANT.
YOU STILL BELIEVE IN RESEARCH GRANTS?
©THE UPTURNED MICROSCOPE