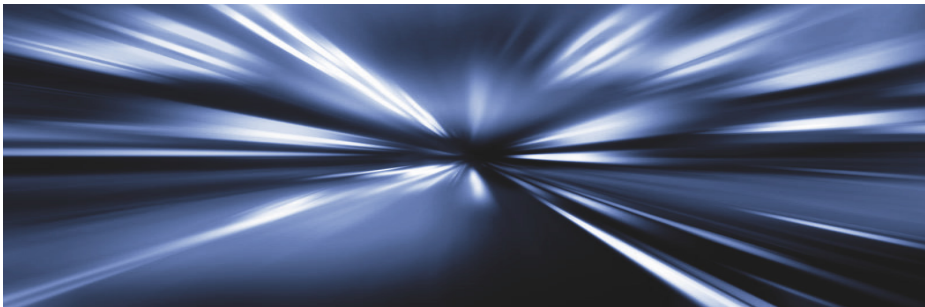



# Paradygmaty i języki programowania

## Smak obliczeń kwantowych

UMCS Lublin

5 czerwiec, 2014. w-15



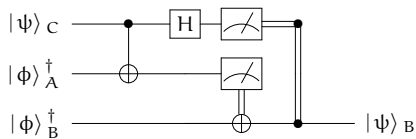
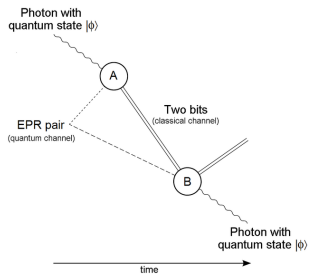
 ETH-researchers cannot “beam” objects or humans of flesh and blood through space yet, a feat sometimes alluded to in science fiction movies. They managed, however, to teleport information from A to B – for the first time in an electronic circuit, similar to a computer chip.

*ETH news. Sierpień, 2014.*

Artykuł:


*Deterministic quantum teleportation with feed-forward in a solid state system.* L. Steffen, Y. Salathe, M. Oppliger, P. Kurpiers, M. Baur, C. Lang, C. Eichler, G. Puebla-Hellmann, A. Fedorov and A. Wallraff. *Nature* **500**, 319–322 (15 August 2013) doi:10.1038/nature12422 <http://www.nature.com/nature/journal/v500/n7462/full/nature12422.html>

# Teleportacja



$$G = (H \otimes I)C_n .$$

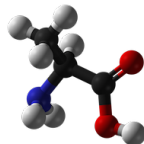
## Teleportacja – streszczenie

ngineered macroscopic quantum systems based on superconducting electronic circuits are attractive for experimentally exploring diverse questions in quantum information science<sup>1,2,3</sup>. At the current state of the art, **quantum bits (qubits) are fabricated, initialized, controlled, read out and coupled to each other** in simple circuits. This enables the realization of basic logic gates<sup>4</sup>, the creation of complex entangled states<sup>5,6</sup> and the demonstration of algorithms<sup>7</sup> or error correction<sup>8</sup>. Using different variants of low-noise parametric amplifiers<sup>9</sup>, dispersive quantum non-demolition single-shot readout of single-qubit states with high fidelity has enabled continuous<sup>10</sup> and discrete<sup>11</sup> feedback control of single qubits. Here **we realize full deterministic quantum teleportation** with feed-forward in a chip-based superconducting circuit architecture<sup>12,13,14</sup>. We use a set of two parametric amplifiers for both joint two-qubit and individual qubit single-shot readout, combined with flexible real-time digital electronics. Our device uses a crossed quantum bus technology that allows us to create complex networks with arbitrary connecting topology in a planar architecture. The deterministic teleportation process succeeds with order unit probability for any input state, as we prepare maximally entangled two-qubit states as a resource and distinguish all Bell states in a single two-qubit measurement with high efficiency and high fidelity. We teleport quantum states between two macroscopic systems **separated by 6mm at a rate of  $10^4 \text{ s}^{-1}$** , exceeding other reported implementations. The low transmission loss of superconducting waveguides is likely to enable the range of this and other schemes to be extended to significantly larger distances, enabling tests of non-locality and the realization of elements for quantum communication at microwave frequencies. The demonstrated feed-forward may also find application in error correction schemes.

# Co to są obliczenia kwantowe?

Wykorzystanie zjawisk mikroświata opisywanych mechaniką kwantową do obliczeń ... teoria istnieje już 90 lat! Główne wysiłki:

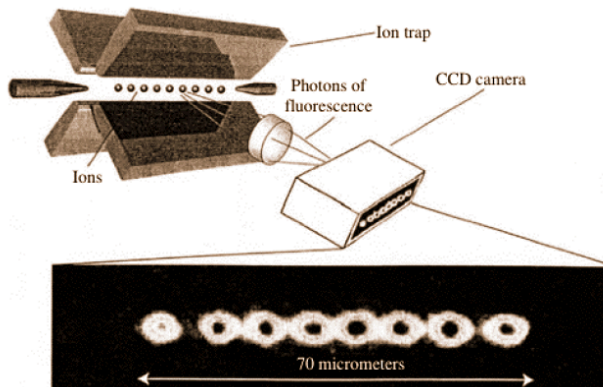
- Budowa urządzeń
- Projektowanie algorytmów



# Plan

1. Czy potrzebujemy komputerów kwantowych?
2. Bit i qubit
3. Algebra
4. Mechanika kwantowa w pigułce
5. Model obliczeń kwantowych
6. Bramki logiczne
7. Algorytmy
  - Algorytm Deutsch
  - Inne algorytmy
8. Informacja kwantowa
  - Teleportacja
9. Literatura
10. Realizacje fizyczne
11. Algorytm Grovera

## Jonowy komputer kwantowy



Komputer kwantowy. N-jonów. (Aspect, Grangier (2004)).

## Po co są komputery kwantowe?

- Świat działa wg. mechaniki kwantowej (MK)
- Urządzenia są coraz mniejsze; upakowanie (patrz prawa Moora)
- W mikroświecie obowiązują prawa fizyki kwantowej
- Wykorzystanie MK może pozwolić na wykonanie klasycznie niemożliwych obliczeń



Komputer klasyczny oparty jest na pracy układów dwustanowych:

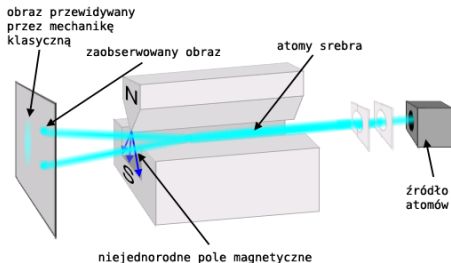
$$0 \leftrightarrow 1$$

Układ o dwóch stabilnych stanach dyskretnych z możliwością kontroli przejść między nimi może być elementem komputera klasycznego.

Realizacja: Kondensator naładowany – 1, nienaładowany – 0.

Realizacja: cząstka ze spinem w polu magnetycznym, atom o dwóch stanach.

Doświadczenie Sterna-Gerlacha (atomy srebra w polu magnetycznym)



$$E = -\mu \cdot \mathbf{B}.$$

$\mu$  – moment magnetyczny atomu,  $\mathbf{B}$  – indukcja magnetyczna.

## Qubity

Układy dwustanowe, wg. mechaniki kwantowej, mogą istnieć jako **superpozycja** stanów czystych (bazowych).

Bit kwantowy (qubit) jest postaci

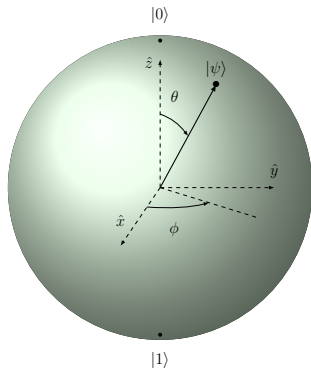
$$\alpha|0\rangle + \beta|1\rangle$$

gdzie  $\alpha$  i  $\beta$  – **amplitudy prawdopodobieństwa**. – liczby zespolone

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

Przykład:

$$|x\rangle = 1/\sqrt{2}(|0\rangle + |1\rangle)$$



Sfera Blocha

$$\alpha|0\rangle + \beta|1\rangle = e^{-i\phi/2} \cos \frac{\theta}{2} |0\rangle + e^{i\phi} \sin \frac{\theta}{2} |1\rangle$$

## Pomiar

Wykonanie pomiaru na qubicie daje stan  $|0\rangle$  z prawdopodobieństwem  $|\alpha|^2$  i stan  $|1\rangle$  z prawdopodobieństwem  $|\beta|^2$ .

Po pomiarze...

układ znajduje się w stanie zmierzonym: następny pomiar da stan zmierzony (kolaps stanu do stanu zmierzonego).



## Pomiar

Stany  $\alpha|0\rangle + \beta|1\rangle$  i  $\alpha|0\rangle - \beta|1\rangle$  są różne.

Prawdopodobieństwa pomiarów w obu przypadkach są jednakowe!

Ewolucja obu stanów jest różna.

Qubit  $\alpha|0\rangle + \beta|1\rangle$  możemy reprezentować wektorem w przestrzeni  $\mathbb{C}$ . Wektor

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

interpretujemy jako

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Wektorami bazowymi są:  $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$  i  $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$  ( $|\cdot\rangle$  – ket-Diraca). Jest to tzw. baza obliczeniowa.

## Splątanie stanów – entanglement

Układ złożony, np. z 4 qubitów (4-qubit)

$$a_0|0000\rangle + a_1|0001\rangle + \dots + a_{15}|1111\rangle$$

lub ogólniej

$$\sum_{i=0}^{2^n-1} a_i |i_2\rangle, \quad \sum |a_i|^2 = 1.$$

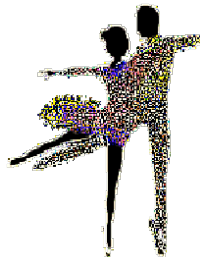
( $i_2$  = liczba binarna)

W wielu przypadkach taki stan można zapisać w postaci “iloczynu” stanów pojedynczych qubitów, np.

$$1/2(|00\rangle - |01\rangle - |10\rangle + |11\rangle) = 1/\sqrt{2}(|0\rangle + |1\rangle) \otimes 1/\sqrt{2}(|0\rangle - |1\rangle).$$

## Splątanie stanów – entanglement

Splątanie ...



Rozpatrzmy stany

$$|a\rangle = 1/\sqrt{2}(|00\rangle + |01\rangle) \quad \text{oraz} \quad |b\rangle = 1/\sqrt{2}(|00\rangle + |11\rangle).$$

Jeśli dokonamy pomiaru pierwszego qubitu w stanie  $|a\rangle$  zobaczymy  $|0\rangle$  z prawdopodobieństwem 1 i stan się nie zmieni.

W drugim przypadku, pomiar da  $|0\rangle$  lub  $|1\rangle$  z równym prawdopodobieństwem. Znamy też drugi qubit. Jest to tzw. stan EPR (Einsteina-Podolskiego-Rosena).





Qubity – wektory z abstrakcyjnej przestrzeni rozpiętej nad ciałem  $\mathbb{C}$  – algebra przestrzeni zespolonych.

Iloczyn tensorowy przestrzeni.

Operator liniowy

$$\hat{\mathcal{A}}(\alpha|0\rangle + \beta|1\rangle) = \alpha(\hat{\mathcal{A}}|0\rangle) + \beta(\hat{\mathcal{A}}|1\rangle)$$

działający w przestrzeni z bazą  $e_i$  reprezentowany jest macierzą o elementach  $A_{ij}$ :

$$\hat{\mathcal{A}}|e_i\rangle = \sum_k A_{ki}|e_k\rangle.$$

Obrót wektorów  $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$  i  $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$  o  $45^\circ$  realizuje macierz

$$\begin{pmatrix} 1/\sqrt{2} & -1/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2} \end{pmatrix}$$

Wynikiem jej działania są wektory:

$$\begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix} \text{ oraz } \begin{pmatrix} -1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix}.$$

## Iloczyn skalarny – wewnętrzny

Ogólnie, dla przestrzeni  $V$ , iloczyn wektorów  $\langle u \| v \rangle$  jest odwzorowaniem:  $V \times V \rightarrow C$ .

### Własności

- $\langle u \| \alpha v + \beta w \rangle = \alpha \langle u \| v \rangle + \beta \langle u \| w \rangle$
- $\langle u \| v \rangle = \langle v \| u \rangle^*$
- $\langle v \| v \rangle \geq 0$ ;  $\langle v \| v \rangle \in \mathbb{R}$ ;  $\langle v \| v \rangle \leftrightarrow v = 0$ .

## Iloczyn skalarny – wewnętrzny

$u, v \in \mathbb{C}^2$  z bazą  $|i\rangle$ :

$$u = \sum_i u_i |i\rangle,$$

$$v = \sum_i v_i |i\rangle$$

$$\langle u | v \rangle = \sum_i u_i^* v_i$$

## Inne pojęcia

Norma:  $|u| = \sqrt{\langle u || u \rangle}$

Wektor jednostkowy:  $|u| = 1$ .

Ortogonalność:  $\langle u || v \rangle = 0$  dla  $u \neq v$ .

Przestrzeń Hilberta = przestrzeń z iloczynem skalarnym.

Operator rzutowy:  $\hat{P}^2 = \hat{P}$ ; Jeśli  $u$  jest jednostkowy to  $\hat{P} = |v\rangle \langle v|$  jest operatorem rzutowania.

Każdy operator liniowy można zapisać w postaci:

$$\hat{A} = \sum_i A_{ij} |i\rangle \langle j|.$$

## Operatory unitarne, Hermitowskie, itp.

Operator sprzężony  $\hat{\mathcal{A}}^\dagger$  z operatorem  $\hat{\mathcal{A}}$ :

$$\langle \mathbf{u} | \hat{\mathcal{A}} \mathbf{v} \rangle = \langle \hat{\mathcal{A}}^\dagger \mathbf{u} | \mathbf{v} \rangle .$$

Reprezentacja macierzowa:  $A^\dagger = (A^*)^\top$ .

Przykład.

$$\begin{pmatrix} 1 & 1+i \\ 1 & 1-i \end{pmatrix}^\dagger = \begin{pmatrix} 1 & 1 \\ 1-i & 1+i \end{pmatrix} .$$

Operator Hermitowski:  $\hat{\mathcal{A}}^\dagger = \hat{\mathcal{A}}$ .

## Operatory unitarne

Operator liniowy unitarny:  $\hat{\mathcal{A}}\hat{\mathcal{A}}^\dagger = \hat{\mathcal{A}}^\dagger\hat{\mathcal{A}}$ .  
lub:  $\hat{\mathcal{A}}^\dagger = \hat{\mathcal{A}}^{-1}$  – odwrotny.

Ważna własność:  $\langle \hat{\mathcal{A}}u \parallel v \rangle = \langle \hat{\mathcal{A}}u \parallel v \rangle$ .

Przykład: Macierze Pauliego.

$$\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_x = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

$$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

## Iloczyn tensorowy

$u \in U, v \in V$ , gdzie  $U, V$  – przestrzenie wektorowe.

$|uv\rangle \in U \otimes V$ :

- $|(u + u')v\rangle = |vu\rangle + |vu'\rangle$
- $|u(v + v')\rangle = |uv\rangle + |uv'\rangle$
- $a|uv\rangle = |(au)v\rangle = |u(av)\rangle$

Dla operatorów liniowych  $\hat{A}: U \rightarrow U$  i  $\hat{B}: V \rightarrow V$  definiujemy operator  $\hat{A} \otimes \hat{B}: U \otimes V \rightarrow U \otimes V$ :

$$\hat{A} \otimes \hat{B}|uv\rangle = |Au, Bv\rangle .$$



## Iloczyn tensorowy

Macierz operatora  $\hat{A} \otimes \hat{B}$ :

$$\begin{pmatrix} A_{11}B & A_{12}B & \dots & A_{1m} \\ A_{21}B & A_{22}B & \dots & A_{2m} \\ \dots & \dots & \dots & \dots \\ A_{n1}B & A_{n2}B & \dots & A_{nm} \end{pmatrix}$$

Przykład.

$$\sigma_x \otimes \sigma_y = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & i \\ 0 & 0 & -i & 0 \\ 0 & -i & 0 & 0 \\ i & 0 & 0 & 0 \end{pmatrix}.$$

- 1 Fizyczny stan układu  $\leftrightarrow$  stan w przestrzeni Hilberta
- 2 Ewolucja układu

$$i\hbar \frac{\partial |\psi\rangle}{\partial t} = \hat{H}|\psi\rangle$$

lub

$$|\psi(t)\rangle = U(t)|\psi(0)\rangle, \quad U(t) = e^{-i\hat{H}t/\hbar}$$

$U(t)$  – unitarny operator ewolucji kwantowej układu w czasie; zależy od hermitowskiego Hamiltonianu  $\hat{H}$

- 3 Postulat pomiaru: Pomiar wtrąca układ w stan zmierzony. Prawdopodobieństwo pomiaru  $p_o$  obserwabli  $\hat{O}$ :

$$p_o = \langle \psi | \hat{O}^\dagger \hat{O} | \psi \rangle, \quad \sum p_o = 1.$$

$P$  jest operacją nieunitarną. Pomiar prawdopodobieństwa znalezienia układu w stanach *obliczeniowych*  $|i\rangle$  realizowany jest przez operacje rzutowe  $\hat{P}_i$ .

Pomiar prawdopodobieństwa znalezienia układu w stanach *obliczeniowych*  $|i\rangle$ , w przypadku jednego qubitu, realizowany jest przez operacje rzutowe  $\hat{P}_i = |i\rangle\langle i|$ ,  $i = 0, 1$ .

$$p_0 = (\alpha^* \langle 0| + \beta^* \langle 1|) P_0^\dagger P_0 (\alpha|0\rangle + \alpha|1\rangle) = |\alpha|^2$$

$$p_1 = (\alpha^* \langle 0| + \beta^* \langle 1|) P_1^\dagger P_1 (\alpha|0\rangle + \alpha|1\rangle) = |\beta|^2$$

## Modele obliczeń

Schemat obliczeń kwantowych:

$$\hat{O} = \hat{O}_1 \hat{O}_2 \dots \hat{O}_n$$

gdzie  $\hat{O}_k$  jest operacją na układzie qubitów.

Obliczenia  $\hat{O}$  są unitarne.

Pomiarów *wielkości obliczonych* dokonuje się po obliczeniach unitarnych.

Założenie: Operacje  $\hat{O}_i$  realizują fizycy!

# Dekoherencja

Wrogiem obliczeń kwantowych jest

## DEKOHERENCJA

Dekoherencja jest to rozpad stanów splątanych powodowany oddziaływaniem z otoczeniem, które jest tym większe im większy jest komputer – większa jest liczba qubitów.

Czasy rozpadu, w zależności od realizacji układu fizycznego (komputera) są zazwyczaj bardzo krótkie. Ilość operacji, które w tym czasie można wykonać zależy od średniego czasu przeprowadzania jednej operacji. Obecnie, szacuje się, że liczba operacji na sekundę (fropy) wynosić może nawet do  $10^{13}$  w przypadku komputera NMR.<sup>1</sup>

Komputery, które zrealizowano (małe) pracują z szybkością tysięcy operacji na sekundę.

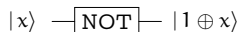
---

<sup>1</sup>Nuclear Magnetic Resonance.

## Bramki klasyczne

Komputer **klasyczny** zbudowany jest z bramek logicznych, przetwarzających bity.

Np. bramki AND;  $x \text{ AND } y = x \wedge y = xy$  oraz NOT:

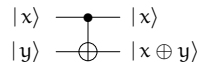
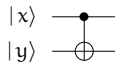


# Bramki kwantowe

Bramki kwantowe mają taką samą liczbę wejść i wyjść – unitarność ewolucji – odwracalność obliczeń.

Przykład. **cNOT** (2 qubity).







$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$



$$\begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix} \rightarrow \begin{pmatrix} a_1 \\ a_2 \\ a_4 \\ a_3 \end{pmatrix}$$

# Bramki kwantowe







## PODSTAWOWE (1 qubit)

Hadamarda		$1/\sqrt{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
Pauliego- $\sigma_x$		$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
Pauliego- $\sigma_y$		$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$
Pauliego- $\sigma_z$		$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
Fazowa		$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$
$\pi/8$		$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$

Więcej qubitów – iloczyny tensorowe.



## Elementy obwodów kwantowych – słowniczek

Symbol	Znaczenie
	<i>drut kwantowy</i> , qubit
	symbol qubitu kontrolnego
	bramka kwantowa B
	bit klasyczny
	Pomiar na qubicie
	unitarne obliczenia funkcji f, 3 qubity

## Bramki kwantowe

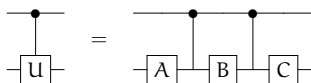
Przykład. Uogólnienie cNOT:  $cU$  (controlled  $U$ ). Kontrolowane  $U$ .

$$cU = \begin{pmatrix} I & 0 \\ 0 & U \end{pmatrix}, \quad I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Jeśli  $x = 0$  to  $y$  się nie zmienia; jeśli  $x = 1$ ,  $cU$  modyfikuje  $y$ :  $|y\rangle \rightarrow |Uy\rangle$ .

$U$  można utworzyć wychodząc z cNOT. Wystarczy znaleźć operatory  $A, B, C$  takie, że

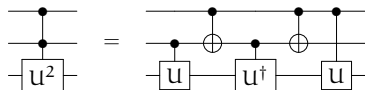
$$CBA = I, \quad C\sigma_x B\sigma_x A = U.$$



# Bramki kwantowe

Przykład. Bramka Toffoliego

$$u = \sqrt{\sigma_x} = \frac{1}{1+i} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}$$



## Algorytm Deutsch

Rozpatrzmy operację odwracalną (2 qubity) ( $\oplus \rightarrow +$  modulo 2):

$$U_f(x, y) = (x, y \oplus f(x)).$$

Jest to operacja obliczania funkcji  $f(x)$ . Dla  $y = 0$

$$(x, 0) \xrightarrow{U_f} (x, f(x)).$$

$U_f$  jest unitarna. (Sprawdzić  $U_f^2 = 1$ )

Działanie H (operacja Hadamarda) na pierwszy qubit ( $x$ ) i kolejne działanie  $U_f$  daje:

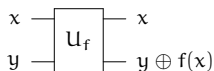
$$|\psi\rangle = U_f |H0\rangle \otimes |0\rangle = U_f \frac{1}{\sqrt{2}} (|0\rangle \otimes |0\rangle + |1\rangle \otimes |0\rangle) = \frac{1}{\sqrt{2}} (|0\rangle \otimes f(0)\rangle + |1\rangle \otimes f(1)\rangle).$$

Wyliczone zostały jednocześnie  $f(0)$  i  $f(1)$ !

$$(x, y) \xrightarrow{U_f} (x, y \oplus f(x)).$$

Unitarność  $U_f$ :

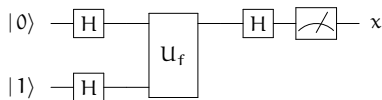
$$(x, y \otimes f(x)) \xrightarrow{U_f} (x, [y \oplus f(x)] \oplus f(x)) = (x, y)$$



Jednoczesne obliczanie  $f(0)$  i  $f(1)$ .

## Algorytm Deutsch

(tzn. czy  $f(0) = f(1)$ , czy też  $f(0) \neq f(1)$ ?)



$$|\psi\rangle = (H|0\rangle) \otimes (H|1\rangle) = \overset{\uparrow}{|\psi\rangle} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \overset{\uparrow}{|\phi\rangle} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{2} \left( \sum_{x=0}^1 |x\rangle \right) \otimes (|0\rangle - |1\rangle)$$

Po zastosowaniu  $U_f$ :

1  $f(x) = 0$ :  $(|0\rangle - |1\rangle) \xrightarrow{U_f} +(|0\rangle - |1\rangle)$

2  $f(x) = 1$ :  $(|0\rangle - |1\rangle) \xrightarrow{U_f} -(|0\rangle - |1\rangle)$

Czyli

$$(|0\rangle - |1\rangle) \xrightarrow{U_f} (-1)^{f(x)} (|0\rangle - |1\rangle).$$

## Algorytm Deutsch

Wiemy, że

$$|\psi\rangle = 1/2 \left( \sum_{x=0}^1 |x\rangle \right) (\otimes |0\rangle - |1\rangle),$$

czyli

$$U_f |\psi\rangle = 1/2 \left( \sum_{x=0}^1 (-1)^{f(x)} |x\rangle \right) \otimes (|0\rangle - |1\rangle).$$

Wynik dla rejestru wejścia:

$$|x\rangle \xrightarrow{U_f} (-1)^{f(x)} |x\rangle.$$

Po obliczeniu stan qubitu jest więc

$$|\phi\rangle = 1/2 \left( (-1)^{f(0)} |0\rangle + (-1)^{f(1)} |1\rangle \right).$$

Przed pomiarem zastosujemy do  $\phi$  operację H (Hadamarda):

$$\begin{aligned} H|\phi\rangle &= \frac{1}{2} \left[ (-1)^{f(0)}(|0\rangle + |1\rangle) + (-1)^{f(1)}(|0\rangle - |1\rangle) \right] \\ &= \frac{1}{2} \left[ (-1)^{f(0)} + (-1)^{f(1)} \right] |0\rangle + \frac{1}{2} \left[ (-1)^{f(0)} - (-1)^{f(1)} \right] |1\rangle . \end{aligned}$$

Jeśli zmierzony qubit ma wartość zero to  $f(0) = f(1)$ .

jeśli wartość zmierzona to jeden, wówczas  $f(0) \neq f(1)$ .

Prowadzi do tego JEDNO obliczenie wszystkich wartości  $f$  jednocześnie.



## Algorytm Grovera

- **Algorytm Grovera** Dotyczy przeszukiwania. Dla  $N$  elementów czas klasycznych obliczeń  $T \sim N/2$ . Czas algorytmu kwantowego:  $T \sim \sqrt{N}$  !
- **Algorytm szybkiej transformacji Fouriera** Niech  $x \in \mathbb{N}$ ,  $x_0 \leq x \leq 2^n - 1$  i niech  $|x\rangle$  będzie wektorem w bazie obliczeniowej

$$|x\rangle = |x_{n-1} \cdots x_1 x_0\rangle, \quad x_i = 0 \text{ lub } 1.$$

Transformata Fouriera jest zdefiniowana jako

$$\langle y | U_{FT} | x \rangle = (U_{FT})_{xy} = \frac{1}{2^{n/2}} e^{2i\pi xy/2^n}.$$

Algorytm FT dotyczy tej transformacji. Wykorzystywany jest w algorytmie Shora faktoryzacji liczb.

- **Algorytm Shora** Klasyczny algorytm Rivesta-Shamira-Adlemana (RSA) służy do szyfrowania i deszyfrowania dokumentów. Polega na ... Algorytm Shora jest algorytmem faktoryzacji liczb - rozkładu na czynniki pierwsze. Jeśli wypali ... nie ma RSA!

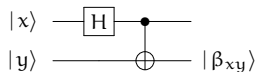
# Informacja kwantowa

- Teleportacja
- Entropia (Shannon vs. von Neumann)
- Kwantowa korekcja błędów
- Kryptografia kwantowa
- ...

# Stany Bella

$$|q_1\rangle \otimes |q_2\rangle$$

We	Wy	-
$ 00\rangle$	$( 00\rangle +  11\rangle)/\sqrt{2}$	$ \beta_{00}\rangle$
$ 01\rangle$	$( 01\rangle +  10\rangle)/\sqrt{2}$	$ \beta_{01}\rangle$
$ 10\rangle$	$( 00\rangle -  11\rangle)/\sqrt{2}$	$ \beta_{10}\rangle$
$ 11\rangle$	$( 01\rangle -  10\rangle)/\sqrt{2}$	$ \beta_{11}\rangle$



Obwód realizujący splątane stany Bella.

## Teleportacja

Załóżmy, że Alicja chce przesłać Bolkowi informację o spinie stanu  $|\phi\rangle_A$  cząstki A.

$$|\phi\rangle_A = \lambda|0_A\rangle + \mu|1_A\rangle,$$

który nie jest *a priori* znany, bez przesłanie samej cząstki. Nie może zmierzyć spinu bo nie zna bazy, w której przygotowano stan i pomiar wtrąciłby cząstkę w inny stan.

Transfer informacji polega na użyciu dodatkowej pary cząstek B i C, w stanie splątanym, z których jedną posiada Alicja, a drugą Bolek. Cząstki te są np. w stanie Bella

$$|\psi_{AB}\rangle = \frac{1}{\sqrt{2}}(|0_B0_C\rangle + |1_B1_C\rangle).$$

Początkowy stan wszystkich cząstek

$$|\phi_{ABC}\rangle = |\phi_A\rangle \otimes |\psi_{BC}\rangle = \frac{\lambda}{\sqrt{2}}|0_A\rangle(|0_B0_C\rangle + |1_B1_C\rangle) + \frac{\mu}{\sqrt{2}}|1_A\rangle(|0_B0_C\rangle + |1_B1_C\rangle).$$

# Teleportacja

(z przeniesienia)

$$|\Phi_{ABC}\rangle = \frac{\lambda}{\sqrt{2}}|0_A\rangle(|0_B0_C\rangle + |1_B1_C\rangle) + \frac{\mu}{\sqrt{2}}|1_A\rangle(|0_B0_C\rangle + |1_B1_C\rangle).$$

Alicja stosuje operację cNOT do qubitów A i B, otrzymując

$$|\Phi'_{ABC}\rangle = \frac{\lambda}{\sqrt{2}}|0_A\rangle(|0_B0_C\rangle + |1_B1_C\rangle) + \frac{\mu}{\sqrt{2}}|1_A\rangle(|1_B0_C\rangle + |0_B1_C\rangle)$$

i następnie H. Wynik końcowy:

$$\begin{aligned} |\Phi''_{ABC}\rangle &= \frac{1}{2}|0_A0_B\rangle(\lambda|0_C\rangle + \mu|1_C\rangle) \\ &\quad + \frac{1}{2}|0_A1_B\rangle(\mu|0_C\rangle + \lambda|1_C\rangle) \\ &\quad + \frac{1}{2}|1_A0_B\rangle(\lambda|0_C\rangle - \mu|1_C\rangle) \\ &\quad + \frac{1}{2}|1_A1_B\rangle(-\mu|0_C\rangle + \lambda|1_C\rangle). \end{aligned}$$

# Teleportacja

(z przeniesienia)

$$\begin{aligned} |\phi''_{ABC}\rangle &= \frac{1}{2} |0_A 0_B\rangle (\lambda |0_C\rangle + \mu |1_C\rangle) \\ &\quad + \frac{1}{2} |0_A 1_B\rangle (\mu |0_C\rangle + \lambda |1_C\rangle) \\ &\quad + \frac{1}{2} |1_A 0_B\rangle (\lambda |0_C\rangle - \mu |1_C\rangle) \\ &\quad + \frac{1}{2} |1_A 1_B\rangle (-\mu |0_C\rangle + \lambda |1_C\rangle). \end{aligned}$$

Alicja mierzy następnie pierwsze dwa qubity w bazie  $\{|0\rangle, |1\rangle\}$ . Wysyła do Bolka (kanałem klasycznym) informacje o tym co ma zrobić:

- 00: OK!
- 01: (**XC**) – rotacja qubitu C o  $\pi$  wokół  $Ox$ .
- 10: (**ZC**) – rotacja o  $\pi$  wokół  $Oz$ .
- 11: (**YC**) – rotacja o  $\pi$  wokół  $Oy$ .

## Teleportacja, uwagi

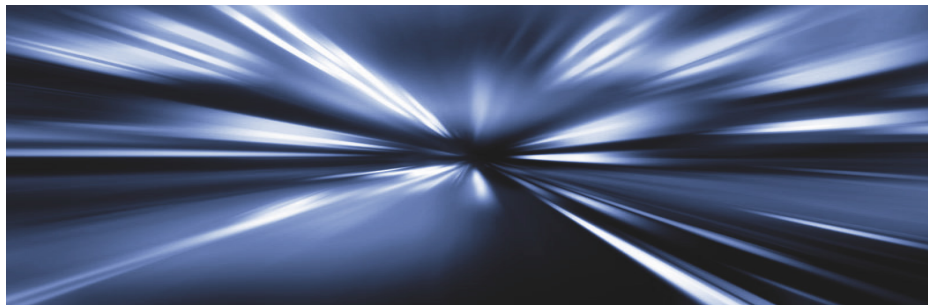
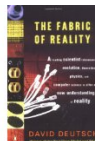
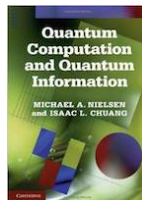
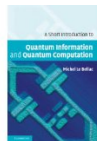
- Współczynniki  $\lambda$  i  $\mu$  nie są nigdy mierzone i stan  $|\phi_A\rangle$  jest niszczone przy pomiarze. Nie ma więc sprzeczności z twierdzeniem o nieklonowaniu.
- Bolek dowiaduje się o stanie cząstki C po tym jak Alicja prześle mu (klasycznie) informacje o pomiarach. Szybkość transmisji nie przekracza więc prędkości sygnałów świetlnych.
- Teleportacja nigdy nie dotyczy transportu materii.

## Podsumowanie

- Dowiedzieliśmy się kilku podstawowych rzeczy o obliczeniach kwantowych.



- Penrose, R. (2006) Droga do rzeczywistości. Prószyński i S-ka.
- Milburn, G.J. (2000) Procesor Feynmana. CiS, Warszawa.
- Deutsch, D. (1997) The fabric of reality. Penguin Books Ltd.
- Le Bellac, M. (2006) Quantum information and quantum computation. Cambridge Uni. Press. JEST WYDANIE POLSKIE.
- Nielsen, M.A. and Chuang, I.L. (2010). Quantum Computation and Quantum Information. 2nd ed. Cambridge University Press.
- Mermin, N.D. (2007). Quantum Computer Science. CUP.
- Kitaev, A.Y., Shen, A.H. and Vyalıy, M.N. (2002). Classical and Quantum Computation. AMS.
- Preskill: <http://www.theory.caltech.edu/people/preskill/ph229/#lecture>



## Realizacje fizyczne

The devices imagined up to now include the following (this list is not exhaustive) :

- a photonic quantum computer based on the nonlinear Kerr effect;
- optical resonant cavities;
- microwave resonant cavities;
- ion traps;
- nuclear magnetic resonance;
- superconducting circuits with Josephson junctions;
- quantum dots;
- atoms of a Bose-Einstein condensate trapped in an optical lattice.

# Realizacje fizyczne. Komputer NMR

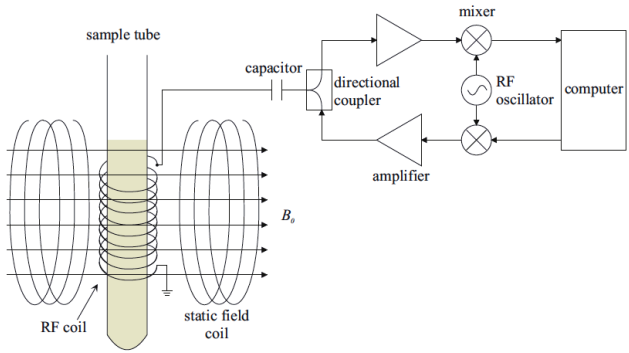
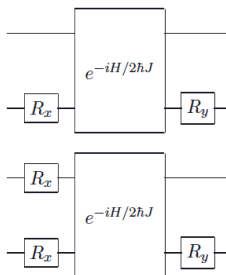


Figure 7.16. Schematic diagram of an NMR apparatus.

*Nielsen, Chuang*

## NMR: Obwody kwantowe



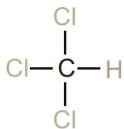
Quantum circuits implemented with NMR. In these circuits,  $R_x$  and  $R_y$  denote single qubit gates which perform  $90^\circ$  rotations about  $\hat{x}$  and  $\hat{y}$ , implemented with RF pulses about 10 microseconds long, and the two qubit box with  $e^{-iH/2\hbar J}$  is a free evolution period of time  $1/2J \approx 2.3$  milliseconds.

(top) Controlled-NOT circuit.

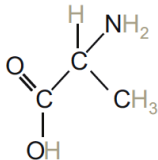
(bottom) Circuit for creating the Bell state  $(|00\rangle - |11\rangle)/\sqrt{2}$ .

(Nielsen, Chuang)

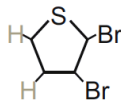
# NMR: Molekuły



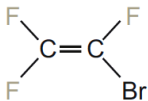
(a)



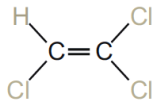
(b)



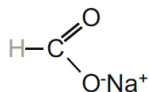
(c)



(d)



(e)



(f)

## Molekuły...

Figure 7.21. A selection of simple molecules which have been used to demonstrate various quantum computation and quantum information tasks with NMR. (a) Chloroform: two qubits, proton and carbon, have been used to implement the Deutsch–Jozsa algorithm, and a two qubit quantum search. (b) Alanine: three qubits, composed of the carbon backbone, have been used to demonstrate error-correction. Note how the three carbon nuclei have distinguishable frequencies because their surrounding chemical environments are different (for example, the electronegativity of the oxygen causes it to draw much of the nearby electrons away from the neighboring carbon). (c) 2,3-dibromothiophene: two qubits, composed of the two protons, have been used to simulate four levels of a truncated simple harmonic oscillator. Here, the two protons are at different distances from the sulphur atom, and thus have distinguishable frequencies. (d) Trifluorobromoethylene: three qubits, the three fluorines, have been used to demonstrate logical labeling and the creation of a  $(|000\rangle + |111\rangle)/\sqrt{2}$  superposition state. (e) Trichloroethylene: three qubits, the proton and two carbons, were used to demonstrate teleportation, with the proton's state being teleported to the rightmost carbon. (f) Sodium formate: two qubits, proton and carbon, used to demonstrate the two qubit quantum error detection code. In this molecule, the sodium radical is used to tune the T2 times of the two qubits to be nearly equal, by changing the ambient temperature to modify its exchange rate with the solvent.

*(Nielsen, Chuang)*

## Quantum computers: physical realization

- There are four basic requirements for implementation of quantum computation: (1) Representation of qubits, (2) Controllable unitary evolution, (3) Preparation of initial qubit states, and (4) Measurement of final qubit states.
- Single photons can serve as good qubits, using  $|01\rangle$  and  $|10\rangle$  as logical 0 and 1, but conventional nonlinear optical materials which are sufficiently strong to allow single photons to interact inevitably absorb or scatter the photons.
- Cavity-QED is a technique by which single atoms can be made to interact strongly with single photons. It provides a mechanism for using an atom to mediate interactions between single photons.
- Trapped ions can be cooled to the extent that their electronic and nuclear spin states can be controlled by applying laser pulses. By coupling spin states through center-of-mass phonons, logic gates between different ions can be performed.
- Nuclear spins are nearly ideal qubits, and single molecules would be nearly ideal quantum computers if their spin states could only be controlled and measured. Nuclear magnetic resonance makes this possible using large ensembles of molecules at room temperature, but at the expense of signal loss due to an inefficient preparation procedure.

*(Nielsen, Chuang)*



## Algorytm Grovera. Wyszukiwanie w tablicy.

Dane są umieszczone na  $n$  qubitach.

Definiujemy funkcję  $f(x)$ ,  $x = \{0, 1, \dots, 2^n - 1\}$  taką, że  $f(x) = 0$  jeśli  $x \neq y$  i  $f(x) = 1$  dla  $x = y$  jest rozwiązaniem, czyli  $f(x) = \delta_{xy}$ . (Założenia.  $y$  jest unikatowe.) Definiujemy operator

$$O|x\rangle = (-1)^{f(x)}|x\rangle.$$

Jak w algorytmie Deutcha dodatkowy qubit nie jest splątany z pozostałymi po wyroczni. Operator Grovera jest

$$G = H^{\otimes n} X H^{\otimes n} O = H^{\otimes n} (2|0\rangle\langle 0| - I) H^{\otimes n}$$

gdzie

$$X|x\rangle = -(-1)^{\delta_{x0}} = (2|0\rangle\langle 0| - I)|x\rangle$$

Dla uproszczenia zapisu zdefiniujemy wektor

$$|\Psi\rangle = H^{\otimes n}|0^{\otimes n}\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle.$$

Biorąc pod uwagę, że

$$H^{\otimes n}(2|0\rangle\langle 0| - I) = 2H^{\otimes n}|0\rangle\langle 0|H^{\otimes n} - I = 2|\Psi\rangle\langle\Psi| - I$$

mamy

$$G = (2|\Psi\rangle\langle\Psi| - I)O.$$

## Algorytm Grovera

Interpretacja G: Operator obrotu w płaszczyźnie.

Jeśli

$$|\alpha\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \neq y} |x\rangle$$

( $N = 2^n$ ) to

$$|\Psi\rangle = \sqrt{1 - \frac{1}{N}} |\alpha\rangle + \sqrt{\frac{1}{N}} |y\rangle .$$

Można to zapisać w postaci

$$|\Psi\rangle = \cos \frac{\theta}{2} |\alpha\rangle + \sin \frac{\theta}{2} |y\rangle$$

gdzie  $\cos(\theta/2) = \sqrt{1 - 1/N}$ .

Działania wyroczeni:

$$O(\lambda|\alpha\rangle + \mu|y\rangle) = \lambda|\alpha\rangle - \mu|y\rangle .$$

Operator  $(2|\Psi\rangle\langle\Psi| - I)$  wykonuje odbicie. Jeśli  $\langle\Psi|\Phi\rangle = 0$  to

$$(2|\Psi\rangle\langle\Psi| - I)(\lambda|\alpha\rangle + \mu|y\rangle) = (\lambda|\alpha\rangle - \mu|y\rangle) .$$

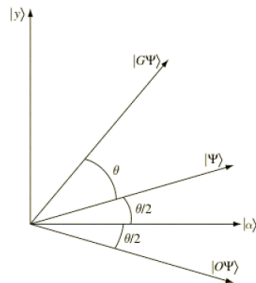
## Algorytm Grovera

Iloczyn dwu odbić jest obrotem. Rysunek obok pokazuje, że kąt zawarty między  $|\alpha\rangle$ , a  $G|\Psi\rangle$  jest równy  $3\theta/2$ .

Wynik po  $k$  iteracjach:

$$G^k|\Psi\rangle = \cos \frac{(2k+1)\theta}{2}|\alpha\rangle + \sin \frac{(2k+1)\theta}{2}|\gamma\rangle .$$

Wynik przybliży się do  $|\gamma\rangle$ .



Schemat rotacji i odbicia w algorytmie Grovera.

## Algorytm Grovera

Po  $k$  iteracjach

$$G^k|\Psi\rangle = \cos \frac{(2k+1)\theta}{2}|\alpha\rangle + \sin \frac{(2k+1)\theta}{2}|\gamma\rangle.$$

Wynik przybliża się do  $|\gamma\rangle$ . Optymalną wartość  $k = k_0$  wyznacza się z warunku

$$0 = \cos \frac{(2k+1)\theta}{2} = \cos k\theta \cos \frac{\theta}{2} - \sin k\theta \sin \frac{\theta}{2}$$

i dalej

$$0 = \sqrt{1-1/N} \cos k\theta - \sqrt{1/N} \sin k\theta.$$

Stąd  $\tan k\theta = \sqrt{N-1}$  lub  $\cos k\theta = 1/\sqrt{N}$ . Czyli

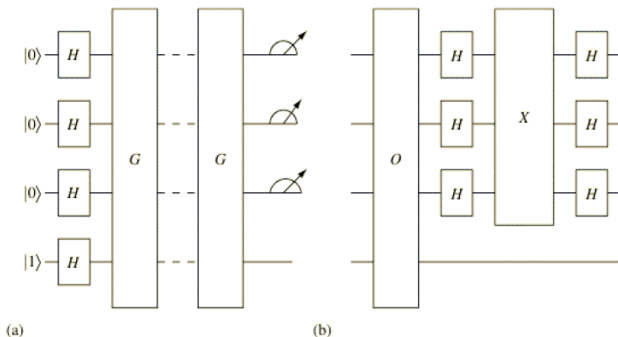
$$k_0 = \left[ \frac{1}{\theta} \cos^{-1} \sqrt{\frac{1}{N}} \right] + 1,$$

gdzie  $[x]$  oznacza część całkowitą z  $x$ . Dla  $N \gg 1$  mamy  $\theta \approx 2/\sqrt{N}$  lub

$$k_0 \approx \frac{\sqrt{N}}{2} \cos^{-1} \sqrt{\frac{1}{N}} \approx \frac{\pi\sqrt{N}}{4}$$

WYSTARCZY więc zastosować wyroczenie  $\approx \sqrt{N}$  razy by mieć szansę otrzymania wyniku.

# Algorytm Grovera



(a) Obwód logiczny algorytmu Grovera. (b) Obwód  $G$ . Wyrocznia  $O$  działa wg. prawa  $O|x\rangle = (-1)^{f(x)}|x\rangle$ , a działanie  $X$  dane jest przez  $X|x\rangle = -(-1)^{\delta_{x0}}$ .

## Grover's Wiki

Bardzo dobry tekst dotyczący algorytmu Grovera:

[https://en.wikipedia.org/wiki/Grover%27s\\_algorithm](https://en.wikipedia.org/wiki/Grover%27s_algorithm)