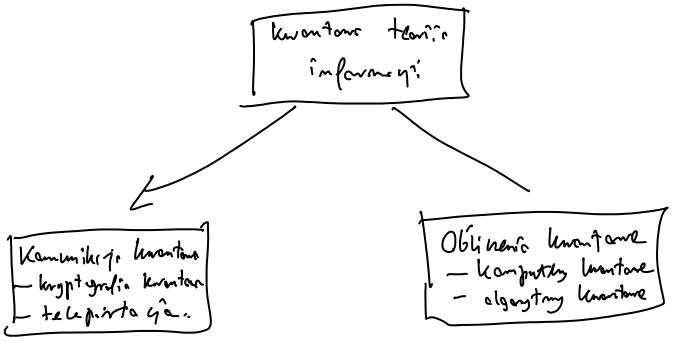
Wyklad12

3 maja 2011
10:47

Obliczenia kwantowe

1. Wstęp

Kwantowa teoria informacji - przetwarzanie informacji kwantowej z praw fizyki kwantowej, operowanie na pojedynczych układach kwantowych, atomach, fotonach



Dotychczas mówiliśmy jedynie o komunikacji kwantowej
Czas zacząć mówić o obliczeniach.

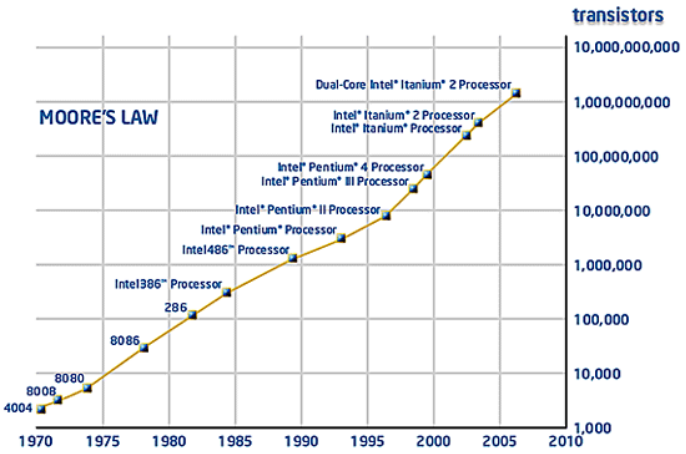
Obecne komputery też wykorzystują prawa fizyki kwantowej:
struktura półprzewodników, tranzystory, momenty magnetyczne atomów (spiny)

Ale ....

- 1 bit danych na dysku twardym: ($d \approx 0{,}5\,nm$)
  $250\,mm \times 250\,mm \times 25\,mm \approx 12{,}5$ mln atomów

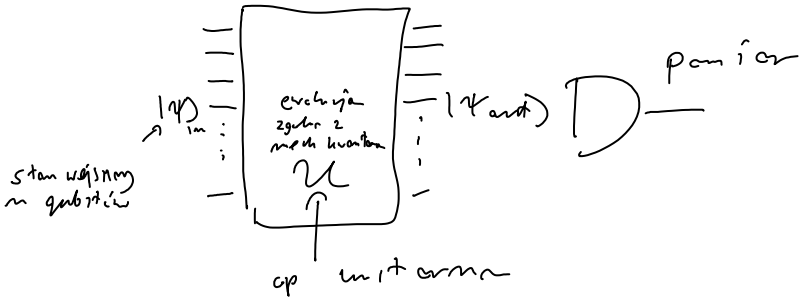
- 1 tranzystor w CPU
  $50\,nm \times 50\,nm \times 25\,nm \approx 500$ tys atomów

Wciąż dużo. Nie jesteśmy na etapie żeby używać pojedynczych atomów do obliczeń i wykorzystać pełne możliwości fizyki kwantowej
Kiedyś zejdziemy do poziomu 1 atomu.



Rozmiar tranzystorów zmniejsza się dwa razy co 2 lata
Będzie różnie ostatecznie około 2030-2050 ?
Nawet jeśli to nastąpi nie oznacza to, że mamy
już komputer kwantowy.
Musimy umieć używać kwantowej superpozycji
tak aby móc wykorzystać potencjał mech. kwantowej

2. Idea



- Klasyczne komputery budujemy zazwyczaj z pewnych elementarnych bramek: NOT, AND, OR, XOR ...
Widzimy, że np. klasyczny układ logiczny można zbudować z bramki NAND .

- W klasycznych komputerach zazwyczaj używamy bramek nieodwracalnych (dlaczego można rozumieć intuicyjnie) a, b → a XOR b — nie da się odtworzyć wejścia z bitu wyjściowego

- Można by używać w klasycznych obliczeniach bramek odwracalnych, wystarczy np.

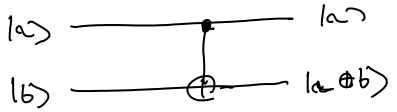
Kosztem komplikacji obwodów zajmiemy się tego nie robić. Pamiętajmy jednak, że linia w zasadzie jest odwracalna. Nieodwracalność bierze się z tego, że po prostu ignorujemy jakieś stopnie swobody

- Myśląc o komputerach kwantowych mamy operacje unitarne - które są odwracalne. Możemy oczywiście też zrobić nieodwracalne np. śledząc po pomiarze z wyjściowych qubitów, ale te zazwyczaj mieszają kwantowe superpozycje, więc nadają się mniej. Ograniczamy się więc do operacji unitarnych.

Chcemy znaleźć elementarne bramki.
z których można złożyć dowolną op. U.
Bramki te muszą być odwracalne.

- Bramka CNOT

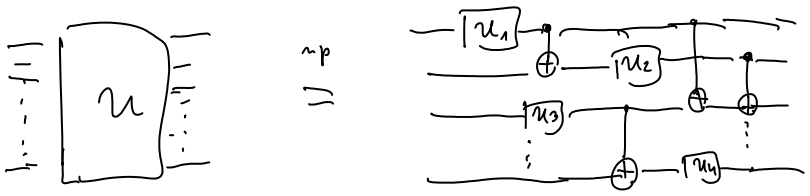
$|0\rangle|0\rangle \to |0\rangle|0\rangle$
$|0\rangle|1\rangle \to |0\rangle|1\rangle$
$|1\rangle|0\rangle \to |1\rangle|1\rangle$
$|1\rangle|1\rangle \to |1\rangle|0\rangle$



$$U_{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

w bazie $|00\rangle, |01\rangle, |10\rangle, |11\rangle$.
Myśląc klasycznie to jest też odwracalny XOR

<u>Fakt</u> Każda wielokubitowa U może być przedstawiona za pomocą jednokubitowych op. unitarnych i bramki CNOT



W praktyce potrzebujemy wielu bramek jednokubitowych (o wiele obszerniejszy Zbiór) można np. wybrać:

— H — bramka Hadamarda $H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ $\{ H^2 H = I$

— φ — operacja fazowa φ (bramka fazowa) $U_\varphi = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{bmatrix}$ ($\varphi = \frac{\pi}{2}$ ćwierć fali)

3. Kwantowy Paralelizm - dlaczego komputer kwantowy ma szanse liczyć szybciej, ?

Idea: $f: \{0,1\} \to \{0,1\}$ jedno bitowa funkcja $f(0), f(1)$

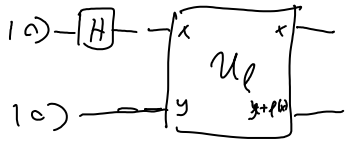
Wyobraźmy sobie że każdą funkcję f w bramce kwantowej U_f

$|x\rangle|y\rangle \xrightarrow{U_f} |x\rangle|y \oplus f(x)\rangle$

$|x\rangle$ qubit z argumentem funkcji; $|y\rangle$ qubit z wynikiem funkcji; $f(x)$ dodawanie mod 2

U_f: $|0\rangle|0\rangle \to |0\rangle|0 \oplus f(0)\rangle$; $|0\rangle|1\rangle \to |0\rangle|1 \oplus f(0)\rangle$; $|1\rangle|0\rangle \to |1\rangle|0 \oplus f(1)\rangle$; $|1\rangle|1\rangle \to |1\rangle|1 \oplus f(1)\rangle$

jest to op. unitarna



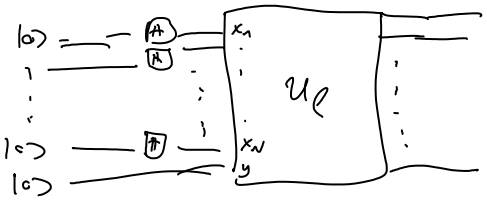
$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|f(0)\rangle + |1\rangle|f(1)\rangle\right)$

$|0\rangle|0\rangle \xrightarrow{H\otimes I} \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle+|1\rangle|0\rangle) \xrightarrow{U_f} \frac{1}{\sqrt{2}}\cdot\left(|0\rangle|f(0)\rangle + |1\rangle|f(1)\rangle\right)$

Uzyliśmy tylko raz obliczenia f a mamy stan $|\psi\rangle$ w którym policzone jest f zarówno dla $f(0)$ i $f(1)$.
„Liczy równolegle" $f(0)$ i $f(1)$ dzięki temu, że wykonaliśmy superpozycję.

Ogólniej: $f: \{0,1\}^N \to \{0,1\}$ funkcja na N bitach

$|x_1, \dots, x_N, y\rangle \xrightarrow{U_f} |x_1 \dots x_N, y \oplus f(x_1, \dots, x_N)\rangle$



$|0\rangle^{\otimes N}|0\rangle \xrightarrow{H^{\otimes N}\otimes I} \left(\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\right)^{\otimes N} \otimes |0\rangle =$

$= \frac{1}{\sqrt{2^N}}\left(|0\rangle\cdots|0\rangle + |0\rangle\cdots|1\rangle + \dots + |1\rangle\cdots|1\rangle\right)\otimes|0\rangle \xrightarrow{U_f}$

wszystkie liczby N bitowe

$= \frac{1}{\sqrt{2^N}}\cdot\left(|0\rangle\cdots|0\rangle\otimes|f(0,\dots,0)\rangle + |0\rangle\cdots|1\rangle\otimes|f(0,\dots,1)\rangle + \dots + |1\rangle\cdots|1\rangle\otimes|f(1,\dots,1)\rangle\right)$

Policzyliśmy N jednym obliczeniem wartości funkcji f dla

„Policzliśmy" w jednym obliczeniu wartości funkcji f dla wszystkich 2^N możliwych danych wejściowych.
Nadzieja na wyjątkowo przyspieszenie obliczeń ?
Ale nie tak szybko - nie istnieje pamięć pozwalająca jednocześnie odczytać wszystkie wartości f. Mamy w bramce $|0,\dots,0\rangle, \dots, |1,\dots,1\rangle$. Stąd znikąd się nam nie pojawi z zasady superpozycji i pomysłu tylko jedna wartość f ....

Ale może są problemy w których takie obliczenie wszystkich f jest elementem pośrednim a nie końcowym odczytujemy jakąś funkcję tych f i wystarczy jedno pomiar dający pożądany wynik.

Algorytm Deutscha

Najprostszy i całkowicie niepraktyczny ale ciekawy dydaktycznie
Rozważmy funkcję $f: \{0,1\} \to \{0,1\}$.
Pytamy się czy funkcja jest zrównoważona ?
Klasycznie funkcję musimy policzyć 2 razy.
A jeśli mamy pudełko kwantowe wystarczy raz

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

$$\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle) \xrightarrow{U_f} \frac{1}{2}\Big(|0\rangle\big(|f(0)\rangle - |1\oplus f(0)\rangle\big) + |1\rangle\big(|f(1)\rangle - |1\oplus f(1)\rangle\big)\Big) =$$

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

$$= \frac{1}{2}\Big((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\Big)(|0\rangle-|1\rangle) \xrightarrow{H\otimes I}$$

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

$$= \cdot\Big(\frac{1}{2}\underbrace{\big[(-1)^{f(0)} + (-1)^{f(1)}\big]}_{\text{1 - 1 stała, 0 - 1 zrównoważ.}}|0\rangle + \frac{1}{2}\underbrace{\big[(-1)^{f(0)} - (-1)^{f(1)}\big]}_{\text{1 - 1 zrównoważ., 0 - 0 stała}}|1\rangle\Big)\otimes\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$$

0 - f. zrównoważona   a - f stała

Mierzymy pierwszy qubit pętli wynik $|0\rangle \Rightarrow$ f. stała
$|1\rangle \Rightarrow$ f zrównoważona

Dzięki temu że policzyliśmy jednocześnie dla obu wartości wejściowych wystarczyło tylko raz użyć pudełka.