

studium informatykę

na kierunku zamawianym



Podstawy obliczeń kwantowych

Jarosław Mischczak
IITiS PAN, Gliwice

20-22.02.2015



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

Wprowadzenie

Motywacje

Motywacja techniczna

Motywacja fizyczna

Motywacja kryptograficzna

Obliczenia kwantowe

Stany kwantowe

Układy złożone

Splątanie

Programowanie kwantowe

Obwody kwantowe

Programy kwantowe

Motywacja techniczna

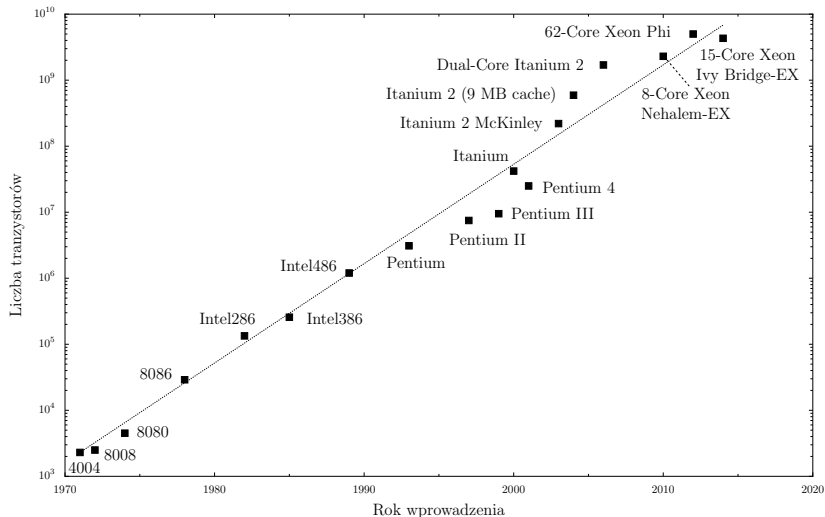
- ▶ Prawo Moore'a

Moc obliczeniowa podwaja się co dwa lata dzięki zwiększeniu gęstości tranzystorów.

- ▶ Prawo Wirtha-Gatesa

Wzrost mocy obliczeniowej jest kompensowany wzrostem złożoności oprogramowania.

Motywacja techniczna



(Dane: http://en.wikipedia.org/wiki/Transistor_count)

Motywacja techniczna



(Źródło: http://en.wikipedia.org/wiki/Moore's_law)

Motywacja techniczna



(Źródło: <http://en.memory-alpha.org/>)

Motywacja techniczna

- ▶ Zgodnie z informacjami w odcinku 9 drugiego sezonu serialu *Star Trek: The Next Generation* komandor porucznik Data dysponował mocą obliczeniową 60 teraflopów. W roku 1989, kiedy był emitowany ten odcinek, był zatem 60 000 szybszy od najszybszego superkomputera (wówczas Cray Y-MP pracujący z częstotliwością 167 MHz z wydajnością do 333 megaflopów).
- ▶ Obecnie najszybszy superkomputer świata (Tianhe-2 o mocy 34 petaflopów) jest 500 razy szybszy niż Data.

Motywacja fizyczna

- ▶ Czy maszyna Turinga może wykonać symulacje układów kwantowych efektywnie?
- ▶ Czy stan układu kwantowego może być wykorzystany do przechowywania (i przesyłania) dowolnie dużej ilości informacji?

Motywacja fizyczna

- ▶ A. Holevo (1973): do zakodowania w stanie kwantowym n bitów potrzebnych jest $2^n - 1$ liczb zespolonych.
- ▶ R.P. Poplavskiĭ (1975): niewykonalność symulacji obliczeń kwantowych na komputerach klasycznych.
- ▶ R.S. Ingarden (1976): uogólnienie teorii informacji Shanona na układy kwantowe.
- ▶ R.P. Feynmann (1981): *Nature isn't classical dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem because it doesn't look so easy.*

Motywacja kryptograficzna

- ▶ W mechanice kwantowej pomiar powoduje, że system ulega zniszczeniu. Czy może być to wykorzystane do zabezpieczenia danych?

Motywacja kryptograficzna

- ▶ S.J. Wiesner (1970): niepodrabialne pieniądze – podstawa zakazu klonowania i kryptografii kwantowej.

Stany kwantowe

Zasada "zerowego" kwantowania

Przyjmijmy, że $0 \mapsto \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ oraz $1 \mapsto \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

Notacja Diraca

$$|0\rangle \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Ponieważ $|0\rangle$ i $|1\rangle$ to wektory, więc kwantowy bit może być w stanie

$$x_0|0\rangle + x_1|1\rangle, \quad x_0, x_1 \in \mathbb{C},$$

np. $\frac{1}{2}|0\rangle + \frac{i}{2}|1\rangle$.

Zatem "zerowa" zasada kwantowania przyjmuje postać

$$\{0, 1\} + | \rangle \mapsto \text{span}\{|0\rangle, |1\rangle\}.$$

Układy złożone

Zasada "zerowego" kwantowania dla układów złożonych

Jeżeli $(b_0, b_1) \in \{0, 1\} \times \{0, 1\}$ to przyjmujemy
 $(b_0, b_1) \mapsto |b_0\rangle \otimes |b_1\rangle$.

W przypadku dwóch bitów kwantowych, dozwolone stany to stany bazowe

$$|00\rangle \equiv |0\rangle \otimes |0\rangle, \quad |01\rangle \equiv |0\rangle \otimes |1\rangle, \quad |10\rangle \equiv |1\rangle \otimes |0\rangle, \quad |11\rangle \equiv |1\rangle \otimes |1\rangle$$

oraz ich dowolne kombinacje $x_{00}|00\rangle + x_{01}|01\rangle + x_{10}|10\rangle + x_{11}|11\rangle$.

Splątanie

Najważniejszym zasobem dostępnym w kwantowej teorii informacji jest splątanie.

Rozkład Schmidta

Macierz współczynników rozkładu w bazie

$$\begin{pmatrix} x_{00} & x_{01} \\ x_{10} & x_{11} \end{pmatrix}$$

można zdiagnozować unitarnie.

Stan jest splątany jeżeli po diagonalizacji macierz ma dwa elementy niezerowe, np.

$$\frac{1}{\sqrt{2}}(|10\rangle + |01\rangle).$$

Obwody kwantowe

Zasada "zerowego" kwantowania operacji

Dla zadanej operacji, kwantowym odpowiednikiem jest takie przekształcenie wektorów, które działa odpowiednio na bazie $\{|0\rangle, |1\rangle\}$.

Przykładowo dla operacji negacji kwantowy odpowiednik to

$$Not = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Możliwe jest natomiast wprowadzenie operacji, które nie mają odpowiedników klasycznych, np. operacja Hadamarda

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

która wprowadza superpozycję 0 i 1.

Obwody kwantowe

Kolejny nieklasyczny przykład to *pierwiastek kwadratowy z negacji* $\sqrt{Not}$, który spełnia własność

$$\sqrt{Not}\sqrt{Not}|x\rangle = Not|x\rangle$$

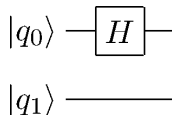
dla dowolnego wejścia $|x\rangle$.

Oczywiście nic nie stoi na przeszkodzie, żeby zdefiniować pierwiastek dowolnego stopnia z dowolnej macierzy.

Programy kwantowe

Programowanie to mnożenie macierzy

Najprostszym sposobem pisania programów kwantowych są *obwody kwantowe*.



Każda linia reprezentuje rejestr (system) kwantowy, a operacje są reprezentowane przez bloki.

Programy kwantowe

Programowanie to mnożenie macierzy

Program 1: Ustaw płaską superpozycję

W notacji Diraca

$$H|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

lub w postaci macierzowej

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

Programy kwantowe

Programowanie to mnożenie macierzy

Ale można to zrobić prościej korzystając z kwantowego języka programowania (<http://tph.tuwien.ac.at/~oemer/qcl.html>)

```
qcl> qureg x[2]
```

```
qcl> H(x[0])
```

```
[2/64] 0.70711 |0> + 0.70711 |1>
```

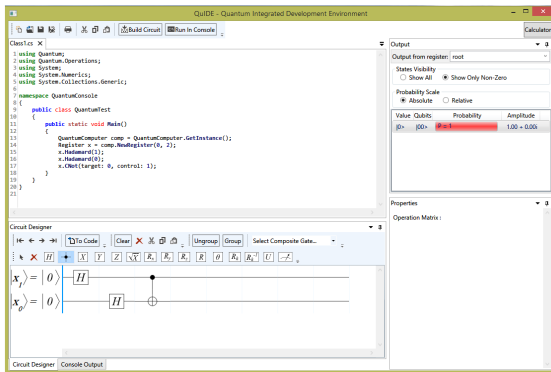
```
qcl> H(x[1])
```

```
[2/64] 0.5 |0> + 0.5 |1> + 0.5 |2> + 0.5 |3>
```

Programy kwantowe

Programowanie to mnożenie macierzy

Albo wykorzystując środowisko graficzne



(QUIDE, Joanna Patrzyk, Kraków 2014, <http://www.quide.eu/>)

Dziękuję za uwagę!
<https://www.iitis.pl/~miszczak>



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego