Obliczenia inspirowane Naturą

Wykład 11 - Podstawy obliczeń kwantowych

Jarosław Miszczak

IITiS PAN Gliwice

12/05/2016

Na poprzednim wykładzie

1. Zasada działania mrówek – stygmergia.
2. Algorytm S-ACO.
3. Zastosowania w optymalizacji.

Obliczanie

Jednym z podstawowych (nieformalnych) założeń współczesnej informatyki jest hipoteza Churcha-Turinga, która określa rodzinę funkcji obliczalnych.

Hipoteza Churcha-Turinga

Dowolne rozsądne obliczenia, mogą być wykonane przez maszynę Turinga.

Hipoteza Churcha-Turinga

- nie dotyczy kosztów wykonywanych obliczeń.
- zawiera ona w sobie ukryte założenie, że *rozsądne* obliczenia są wykonywane mechanicznie zgodnie z zasadami fizyki klasycznej.

Obliczanie

- Wszystko wskazuje na to, iż mechanika klasyczne nie jest podstawową teorią opisującą układy fizyczne.
- W chwili obecnej uznaje się, iż taką teorią jest mechanika kwantowa.

Hipoteza Churcha-Turinga-Deutscha

Każdy proces fizyczny może być symulowany przez uniwersalny komputer.

Motywacja techniczna

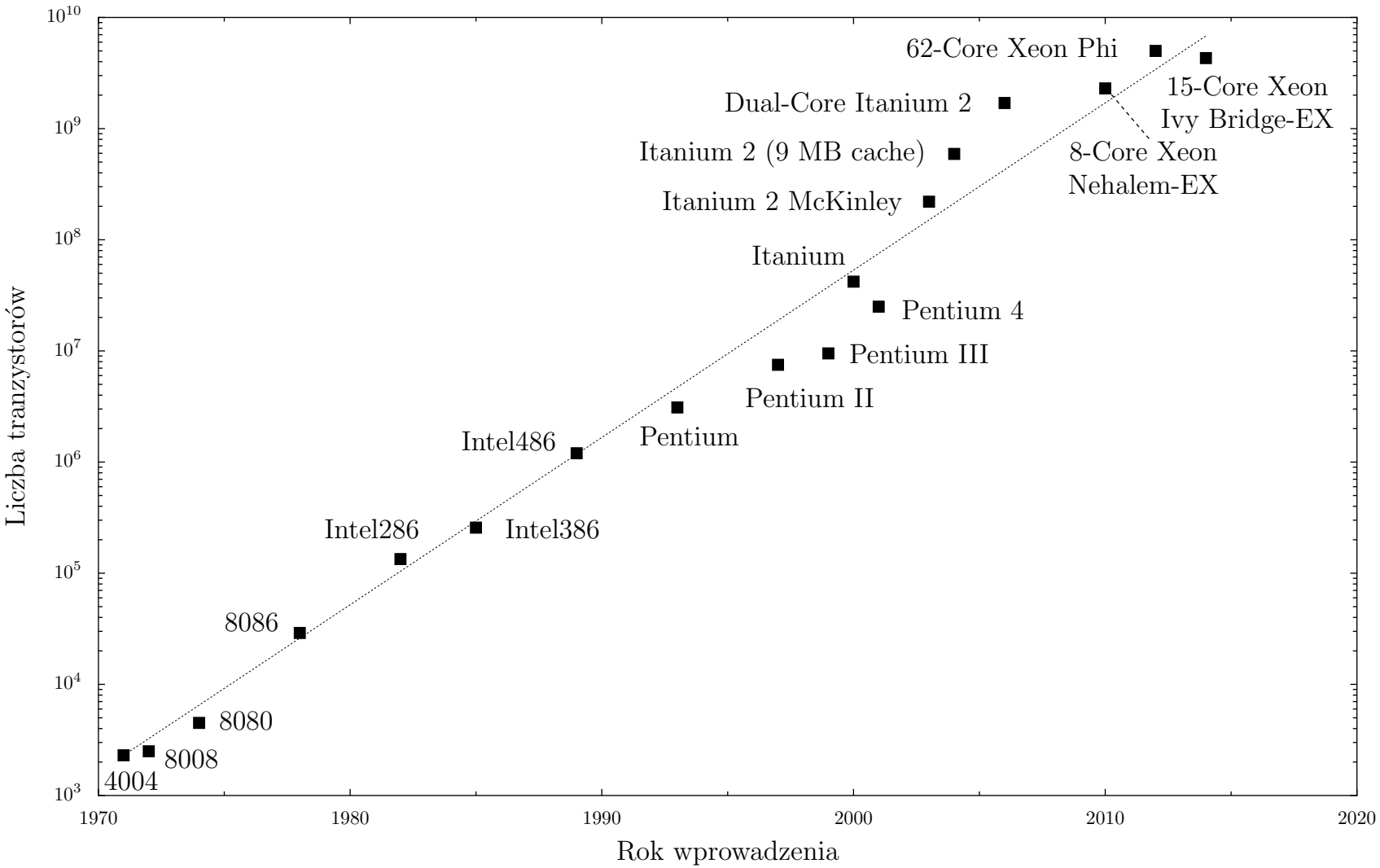
Prawo Moore'a (1965)

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

Osborne Executive (1982) oraz iPhone (2007)

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

Motywacja techniczna

Komandor podporucznik Data, 2366

(Źródło: http://memory-alpha.wikia.com/wiki/Data)

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. (Roman S. Ingarden, *Quantum information theory*, Rep. Math. Phys., Vol. 10, pp. 43-72 (1976))
- 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.* (Richard P. Feynman, *Simulating Physics with Computers*, International Journal of Theoretical Physics, Vol 21, Nos. 6/7, 1982)

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. S.J. Wiesner, *Conjugate Coding*, SIGACT News, Vol. 15, pp. 78-88 (1983).
- A. Ekert (1991): kryptografia kwantowa (Artur Ekert, *Quantum cryptography based on Bell's theorem*. Physical Review Letters, 67: 661–663.)

Stany układu

Liniowość

Pierwszą z zasad przy wprowadzaniu opisu układów w języku mechaniki kwantowej jest **zasada liniowości**. Prowadzi ona do sytuacji w której dwa stany układu kwantowego można dodać i otrzymany w ten sposób obiekt (czyli kombinacja liniowa) jest również poprawnym stanem układu.

Superpozycja stanów

Kombinacje liniowe stanów nazywane są **superpozycjami stanów**.

Stany układu

Aby wykonywać obliczenia ($\equiv$ operować na danych), konieczne jest wprowadzenie reprezentacji danych dostosowanej do modelu obliczeń.

Zasada "zerowego" kwantowania

Przyjmijmy, że $0 \mapsto \binom{1}{0}$ oraz $1 \mapsto \binom{0}{1}$.

Ponieważ $\binom{1}{0}$ i $\binom{0}{1}$ to wektory, więc kwantowy bit może być w stanie

$$x_0 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + x_1 \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad x_0, x_1 \in \mathbb{C},$$

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

Notacja Diraca

Notacja Diraca

$|0\rangle \equiv \binom{1}{0}$, $|1\rangle \equiv \binom{0}{1}$

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

Układy złożone

Druga zasada dotyczy tworzenia układów złożonych.

Tworzenie układów złożonych

Jeżeli układ jest złożony z dwóch podukładów, to jego stan jest opisany przez **iloczyn tensorowy** przestrzeni reprezentujących podukłady.

Układy złożone

Definicja (Iloczyn tensorowy)

Rozważmy przestrzenie wektorowe V, W i X, oraz odwzorowania liniowe postaci $f : V \times W \mapsto X$. Iloczynem tensorowym przestrzeni V i W nazywamy przestrzeń liniową T wraz z odwzorowaniem t, takim, że dowolne odwzorowanie f może być zapisane jako

$$f = g \circ t,$$

gdzie $g : W \mapsto X$.

Powyżej zdefiniowaną przestrzeń T oznacza się jako $V \otimes W$.

Układy złożone

Definicja (Iloczyn Kroneckera)

Dla dwóch macierzy $A \in \mathbb{M}_{k,l}(\mathbb{C})$ *i* $B \in \mathbb{M}_{m,n}(\mathbb{C})$ *ich iloczynem tensorowym jest macierz*

$$A \otimes B = \begin{pmatrix} a_{11}b_{11} & \dots & a_{11}b_{1n} & \dots & a_{1l}b_{11} & \dots & a_{1l}b_{1n} \\ \vdots & \ddots & \vdots & \dots & \vdots & \ddots & \vdots \\ a_{11}b_{m1} & \dots & a_{11}b_{mn} & \dots & a_{1l}b_{m1} & \dots & a_{1l}b_{mn} \\ \vdots & & \vdots & & \vdots & & \vdots \\ a_{k1}b_{11} & \dots & a_{k1}b_{1n} & \dots & a_{kl}b_{11} & \dots & a_{kl}b_{1n} \\ \vdots & \ddots & \vdots & \dots & \vdots & \ddots & \vdots \\ a_{k1}b_{m1} & \dots & a_{k1}b_{mn} & \dots & a_{kl}b_{m1} & \dots & a_{kl}b_{mn} \end{pmatrix}$$

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

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

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 zdiagonalizować unitarnie.

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

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

Obwody kwantowe

Odwracalność

Trzecią zasadą jest **odwracalność operacji** wykonywanych na stanach (czyli ewolucji układu).

Bramki kwantowe

Przekłada się to na opis ewolucji układu za pomocą **macierzy unitarnych**, nazywanych **bramkami kwantowymi**.

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

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

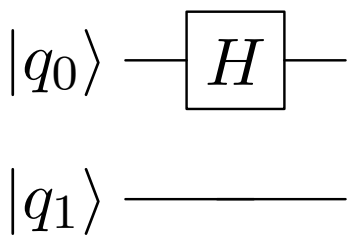
dla dowolnego wejścia $|x\rangle$.

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

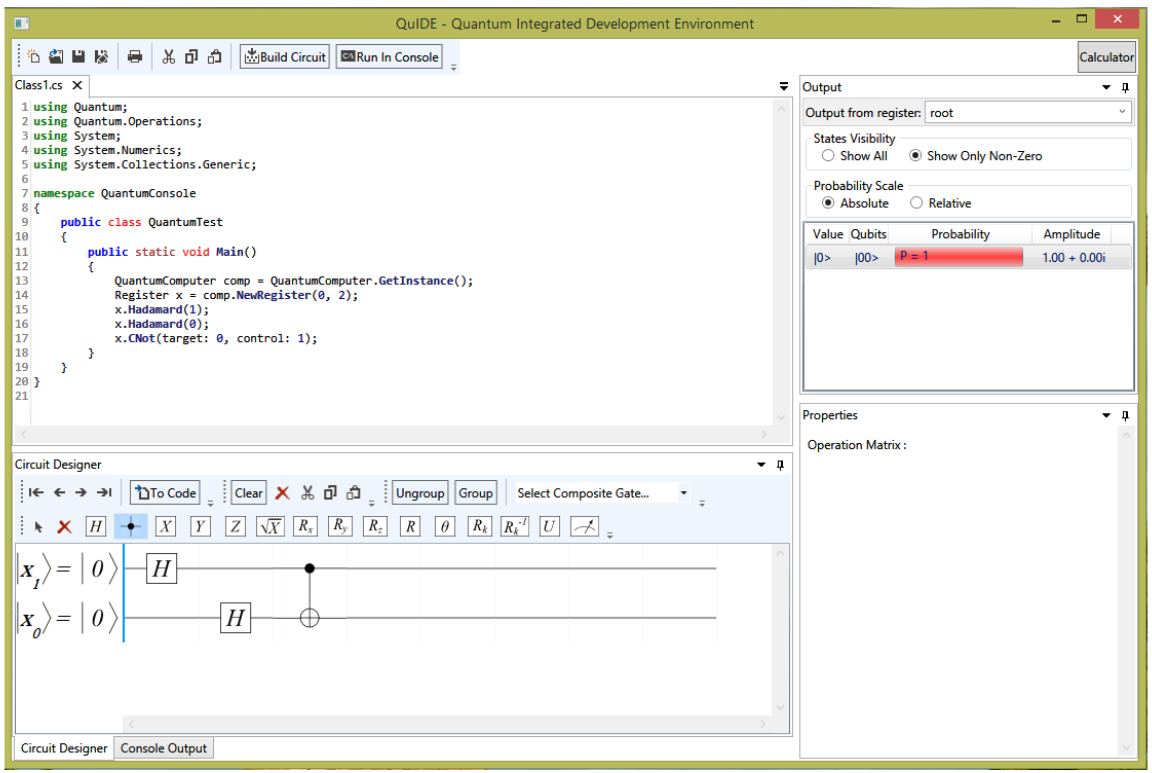
Ale można to zrobić prościej korzystając z kwantowego języka programowania (http://tph.tuwien.ac.at/~oemer/qcl.html)

```
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/)

Kolokwium

Uwaga!

Na następnych zajęciach (19.05) odbędzie się kolokwium z wykładów $\leqslant 11$.