Cwiczenia13

9 maja 2011
17:04

1. Kw. trans Fouriera z el. bramek kwantowych

$$|j\rangle \longrightarrow \frac{1}{\sqrt{N}} \sum_k e^{\frac{2\pi i jk}{N}} |k\rangle =$$

$\begin{cases} i,j = 0,\dots N-1 \\ N = 2^m \end{cases}$ $\quad |j\rangle = |j_{m-1}\rangle \otimes \dots \otimes |j_0\rangle \qquad |k\rangle = |k_{m-1}\rangle \otimes \dots \otimes |k_0\rangle$

$$\frac{1}{\sqrt{N}} \sum_{k_0,\dots k_{m-1}} e^{2\pi i j \cdot \sum_{r=0}^{m-1} k_r 2^r \cdot \frac{1}{2^m}} |k_{m-1}\rangle \otimes \dots |k_0\rangle =$$

$$= \frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i j \cdot \frac{2^{m-1}}{2^m}} |1\rangle\right) \frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i j \frac{2^{m-2}}{2^m}} |1\rangle\right) \dots \frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i j \frac{1}{2^m}} |1\rangle\right)$$

$$= \frac{1}{2^{\frac{m}{2}}} \left(|0\rangle + \underbrace{e^{2\pi i \cdot j \cdot \frac{1}{2}}}_{e^{2\pi i j_0 \cdot 2^{-1}}} |1\rangle\right) \cdot \frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i (j_1 \cdot 2^{-1} + j_0 \cdot 2^{-2})} |1\rangle\right) \cdot$$

$$\cdot \dots \cdot \frac{1}{\sqrt{2}} \cdot \left(|0\rangle + e^{2\pi i \left(j_{m-1} \cdot 2^{-1} + \dots + j_0 \cdot 2^{-m}\right)} |1\rangle\right)$$

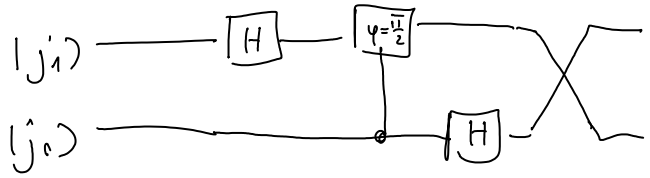
Odpowiednie bity j odpowiadają za wykonanie fcz
w kolejnych qubitach. Musimy pokombinować
z bramkami H ; controlled phase

- 1 qubit $\quad |j\rangle \to \frac{1}{\sqrt{2}} \left(|0\rangle + e^{i\pi j_0} |1\rangle\right)$

$|j_0\rangle$ — H —

- 2 qubity

$$|j\rangle \to \frac{1}{\sqrt{2}} \cdot \left(|0\rangle + e^{i\pi j_0} |1\rangle\right) \otimes \frac{1}{\sqrt{2}} \left(|0\rangle + e^{i\pi \left(j_1 + \frac{1}{2} j_0\right)} |1\rangle\right)$$



$$|j_1\rangle|j_0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}} \cdot \left(|0\rangle + e^{i\pi j_1} |1\rangle\right) |j_0\rangle \xrightarrow{\varphi=\frac{\pi}{2}}$$

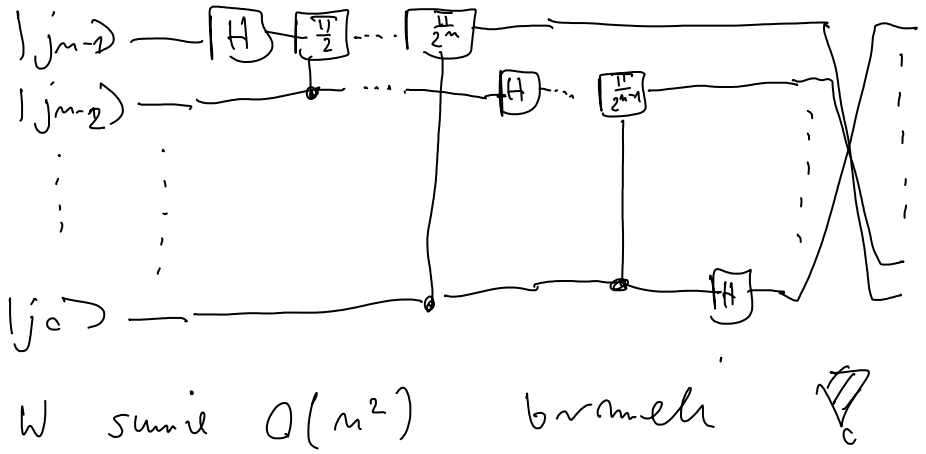
$$\to \frac{1}{\sqrt{2}} \cdot \left(|0\rangle + e^{i\pi j_1 + i\frac{\pi}{2} j_0} |1\rangle\right) |j_0\rangle \xrightarrow{H}$$

$$\to \frac{1}{\sqrt{2}} \left(|0\rangle + e^{i\pi \left(j_1 + \frac{j_0}{2}\right)} |1\rangle\right) \frac{1}{\sqrt{2}} \left(|0\rangle + e^{i\pi j_0} |1\rangle\right) \xrightarrow{SC}$$

$$\to \frac{1}{2} \left(|0\rangle + e^{i\pi j_0} |1\rangle\right) \left(|0\rangle + e^{i\pi \left(j_1 + \frac{j_0}{2}\right)} |1\rangle\right)$$

$$\rightarrow \frac{1}{\sqrt{2}}\left(|0\rangle + e^{\frac{2\pi i}{2}\cdot 1}|1\rangle\right)\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\left(j_1 + \frac{j_0}{2}\right)}|1\rangle\right)$$

- N qubitów



W sumie $O(n^2)$ bramek

2. GCD(x,y) – Algorytm Euklidesa

$y = a_1 x + b_1 \qquad b_1 < x$

$x = a_2 \cdot b_1 + b_2$

$b_1 = a_3 \cdot b_2 + b_3$

$\vdots$

$b_{n-1} = a_{n+1} b_n + b_{n+1}$

$b_n = a_n \cdot b_{n+1}$

Wracając widzimy że b_{n+1} jest największym dzielnikiem x, y.

(maksymalnie n kroków dla liczby n bitowej
Każdy krok: n^2 operacji – dzielenie dwóch liczb n bitowych.)

3. Przykład alg. Shora dla $N = 15$.

- losujemy liczbę < 15, np. 8
- $GCD(15, 8) = 1$
- szukamy $8^r \bmod 15 = 1$

$r = 4$

$8^4 = 4096 = 1 \bmod 15$

$(8^2 - 1)$, $(8^2 + 1)$

" "

63 65

$GCD(63, 15) = 3$ $GCD(65, 15) = 5$

ok.