12 - Cwiczenia

9 maja 2011 17:04

1. Kw. trans Fouriera z el. bramek kwantowych

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

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

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

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

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

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

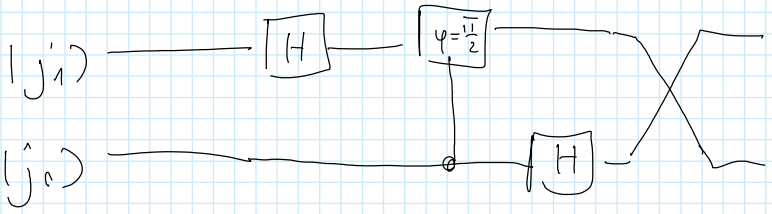
Odpowiednie bity j odpowiadają za mnożenie faz w kolejnych qubitach. Musimy potrafić zbudować 2 bramki H ; controlled phase

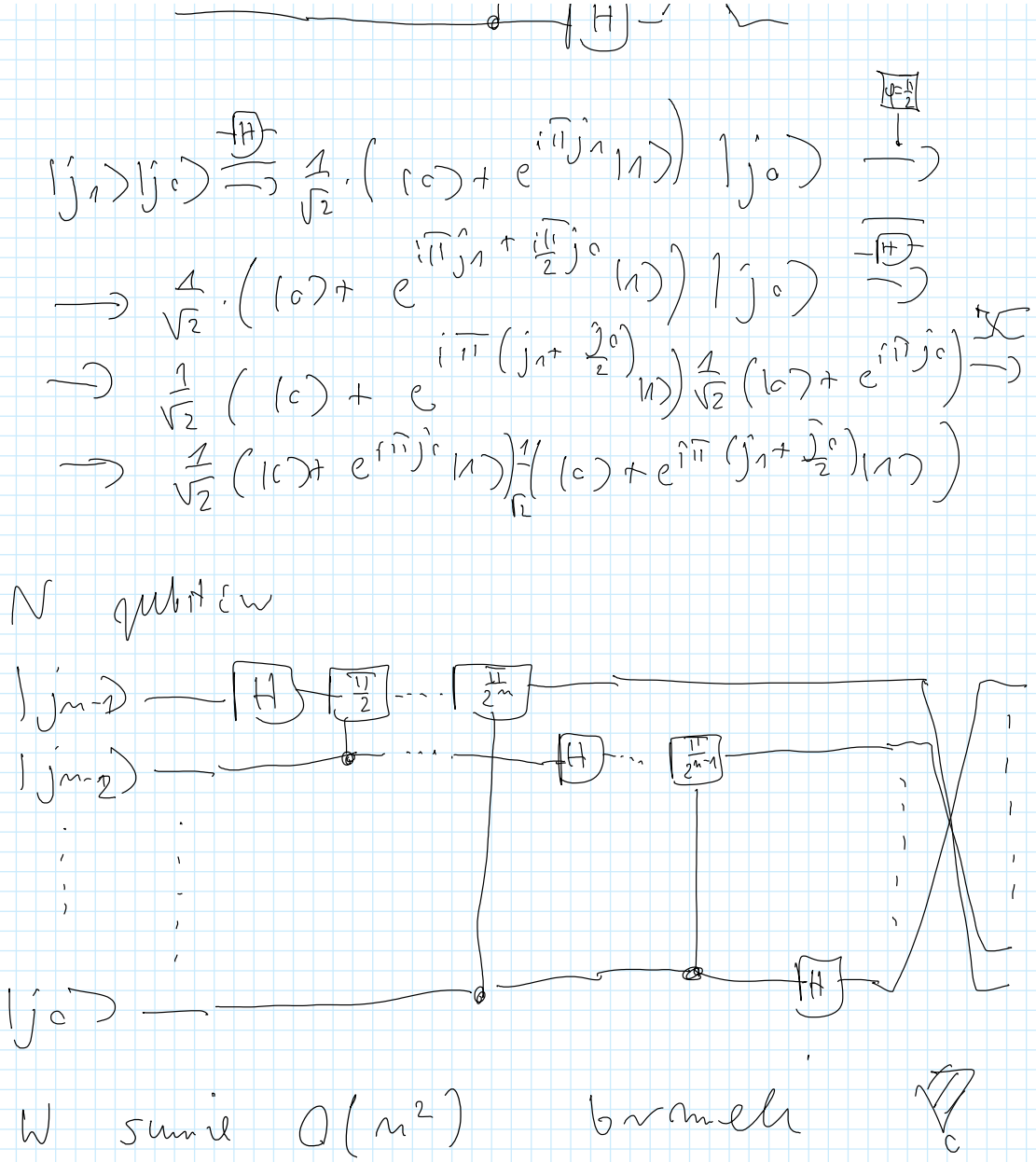
- 1 qubit $|j\rangle \to \frac{1}{\sqrt{2}} \left(|0\rangle + e^{i\pi j_0} |1\rangle \right)$

$|j_0\rangle$ — H —

- 2 qubity

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





Podkreslić, że skoro na końcy wykonujemy pomiar w bazie obliczeniowej, a kontrol-phase można traktowac jako kontrol w drugą stronę, to w zasadzie możemy zrobić QFT używając bramek jednoqubitowych zależnych od wyniku pomiaru na kolejnych qubitach - nie potrzebujemy dwu-qubitowych bramek kwantowych!!!

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_{m+1} jest współnym 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 $8^r \mod 15 = 1$

$r = 4$

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

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

$= 63$, $= 65$

$GCD(63, 15) = 3$

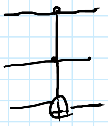
$GCD(63, 15) = 5$

ok.

4. Złożoność $a^x \mod N$

Pamiętamy, że musimy je robić odwracalnie. Uniwersalna bramka do klasycznych obliczeń odwracalnych: Bramka Toffoliego

$|x\rangle|y\rangle|z\rangle \longrightarrow |x\rangle|y\rangle|z \oplus xy\rangle$



Możemy z niej zrobić dowolne klasyczne bramki

$|x\rangle|y\rangle|0\rangle \rightarrow |x\rangle|y\rangle|xy\rangle$ ≡ odwracalny AND itp.

$|x\rangle|y\rangle|0\rangle \to |x\rangle|y\rangle|x \cdot y\rangle$ = dwuargumentowa AND itp

$x = x_{n-1}, \dots, x_0$

$a^x = \prod_j \left(a^{2^j}\right)^{x_j}$

input | output | work

$|x\rangle|0\dots1\rangle|a\rangle$

- $j = 0$
- Mnożymy output $\cdot$ by work jeśli $x_j = 1$
- Zestawiamy work register przez jego kwadrat mod N (n^2 obliczeń)
- $j = j + 1$

Na końcu mamy a^x mod N w output

Mamy $n \times n^2 = n^3$ kroków

Work register na końcu $|2^n\rangle$ umożliwia mi to zrównoważenie