WYKŁAD

Algorytm faktoryzacji Shora

Peter Shor, ~~1995~~ 1994

Najpierw wstęp do obliczeń kwantowych.
Dopiero na drugim wykładzie będziemy
rozmawiali o algorytmie Shora.

Historia

- pierwsza połowa XX w. – rozwija się mechanika kwantowa. Okazuje się, że wiele rzeczy jest dane rozkładami prawdop. i dopiero po zmierzeniu konkretne jest coś z tego rozkładu. Wszechświatem rządzą ~~rządzą~~ prawa mechaniki kwantowej, przy czym one ujawniają się dlatego dopiero w mikroskali. W makroskali wszystko wygląda inaczej.
- Feynman, Benioff (± 1982) zadają pytanie, czy te efekty dadzą się jakoś wykorzystać do obliczeń
- Deutsch 1985, kwantowe maszyny Turinga, może lepiej jakaś ~~maszyna~~ wersja kwantowych obwodów boolowskich – równoważnego modelu
- Shor 1994, algorytm faktoryzacji
  - szybko rosnące pole badań
  - ~~1995~~ na razie nie zbudowano komputera kwantowego istotnego rozmiaru. Maksymalnie rozłożono $21 = 7 \cdot 3$. (2012) Podobno też IBM (2001) $15 = 5 \cdot 3$. $143 = 13 \cdot 11$, ale

Źródłem efektów kwantowych są takie efekty jak:

polaryzacja światła, spin elektronu itp.

Problemy komp. kwant. są takie, że trzeba bardzo precyzyjnie manipulować i bardzo dobrze odizolować od otoczenia.

Model obliczeń

Normalny komputer używa bitów. Są dwa równoważne modele obliczeń: maszyny Turinga i obwody boolowskie. ~~Często~~ wygodniejsze wydaje się maszyny Turinga.

Do kwantowych obliczeń jednak wygodniejsze wydają się obwody.

bit ⟶ ~~qubit~~ kubit (quantum bit), ~~qubit~~

~~Normalne bramki Bit~~

Normalnie bramki logiczne to AND, OR, NOT,

teraz dużo szersza rodzina bramek: bramki unitarne (wytłumaczenie zaraz).

Założenie czytania bitu wyjściowego będziemy nazywać ~~qubitem~~ wyjściowe.

Bit: 0 lub 1

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

Kubit to superpozycja $|0\rangle$ i $|1\rangle$:

$\alpha \cdot |0\rangle + \beta \cdot |1\rangle$, gdzie $\alpha, \beta \in \mathbb{C}$, $|\alpha|^2 + |\beta|^2 = 1$.

Gdy zmierzymy kubit to z praw. $|\alpha|^2$ wyjdzie $|0\rangle$, a z pr. $|\beta|^2$ wyjdzie $|1\rangle$.

Przykłady: $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$, $\frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle$,

$\sin(x)|0\rangle + \cos(x)|1\rangle$.

$\alpha|0\rangle + \beta|1\rangle = \begin{pmatrix}\alpha\\ \beta\end{pmatrix} \in \mathbb{C}^2$

Jak oznaczać 2 kubity?

Oznaczamy je używając produktu tensorowego, tzn.

$$A \otimes B = \begin{pmatrix} A_{11}B & \cdots & A_{1n}B \\ \vdots & & \vdots \\ A_{m1}B & \cdots & A_{mn}B \end{pmatrix},$$

szczególny przypadek to wektory

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \otimes \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} = \begin{pmatrix} a_1 b_1 \\ a_1 b_2 \\ \vdots \\ a_1 b_m \\ a_2 b_1 \\ \vdots \\ a_2 b_m \\ \vdots \\ a_n b_1 \\ \vdots \\ a_n b_m \end{pmatrix}$$

Czyli ~~przestrzeń~~ bazą dla ~~przestrzeni~~ przestrzeni 2 kubitów są 4 wektory $|0\rangle \otimes |0\rangle$, $|0\rangle \otimes |1\rangle$, $|1\rangle \otimes |0\rangle$, $|1\rangle \otimes |1\rangle$

$$\begin{pmatrix}1\\0\\0\\0\end{pmatrix} \quad \begin{pmatrix}0\\1\\0\\0\end{pmatrix} \quad \begin{pmatrix}0\\0\\1\\0\end{pmatrix} \quad \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$

Oznaczamy $|a\rangle \otimes |b\rangle = |ab\rangle$

~~Przykłady~~

stany splątane: $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle \in \mathbb{C}^4$

stan n-kubitowy $|\varphi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle \in \mathbb{C}^{2^n}$

Jak zmierzymy $\sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$, to on z prawd. $|\alpha_x|^2$ dla $|x\rangle$.

Możemy też zmierzyć część stanu.

Weźmy np. stan

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |f(x)\rangle$$

i zmierzmy drugi rejestr, niech da $|a\rangle$.

Wtedy całość się skolapsuje do

$$\frac{1}{\sqrt{|\{x : f(x)=a\}|}} \sum_{x : f(x)=a} |x\rangle |a\rangle$$

Obserwacja

Odpowiednikiem bramek logicznych są bramki unitarne.

Niech A to macierz ~~$n \times n$~~ $n \times n$ nad $\mathbb{C}$.

Wówczas A^* to $\overline{A^T}$, czyli A transponowane i sprzężone.

Mówimy, że A jest unitarna jeśli $A \cdot A^* = I$.

Przykłady

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad A^T = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad A^* = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad AA^* = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$$

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad A^T = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad A^* = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad AA^* = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$$

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad H^T = H, \quad H^* = H, \quad HH^* = \frac{1}{2} \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = I$$

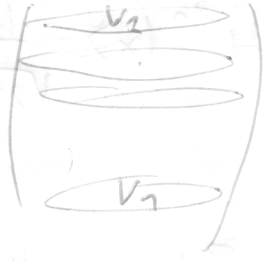
$$A = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ -i & -1 \end{pmatrix}, \quad A^T = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -i \\ i & -1 \end{pmatrix}, \quad A^* = A, \quad AA^T = \frac{1}{2}\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = I$$

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{pmatrix}, \quad T^T = T, \quad T^* = \begin{pmatrix} 1 & 0 \\ 0 & e^{-\frac{i\pi}{4}} \end{pmatrix}, \quad TT^* = I$$

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad C^T = C^* = C, \quad CC^* = I$$

Znaczenie C: Kontrolowany NOT:

$$C(|00\rangle) = |00\rangle$$
$$C(|01\rangle) = |01\rangle$$
$$C(|10\rangle) = |11\rangle$$
$$C(|11\rangle) = |10\rangle$$

Idea macierzy unitarnych: $A =$ 

$AA^* = I \Leftrightarrow$

$\forall_j \; v_j \overline{v_j} = 1$ – wektory dł. 1

$\forall_{i \neq j} \; v_i \overline{v_j} = 0$ – wektory prostopadłe w $\mathbb{C}^n$

Macierze unitarne = macierze nie zmieniające długości wektora (czyli sumy prawdopodobieństw, która ma pozostać 1).

to pewien układ w przyrodzie.

Policzmy:

$$H|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\cdot\begin{pmatrix}1\\0\end{pmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) =: |+\rangle$$

$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) =: |-\rangle$$

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

$$H|-\rangle = |1\rangle, \text{ bo } H^2 = I$$

$$H^{\otimes 2} = \frac{1}{2}\begin{pmatrix}1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1\\ 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1\end{pmatrix}$$

$$H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}}\sum_{y\in\{0,1\}^n}(-1)^{x\cdot y}|y\rangle$$

$x\cdot y$ – iloczyn skalarny

Zobaczmy dlaczego

$$H^{\otimes 2}|a_1a_2\rangle = \frac{1}{\sqrt{2^2}}\cdot\sum\cdot\alpha|b_1b_2\rangle$$

$$\begin{array}{c} \\ a_1=0 \\ a_1=1 \end{array}\overset{\begin{matrix} b_1=0 & b_1=1 \end{matrix}}{\begin{pmatrix}1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1\\ 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1\end{pmatrix}}$$

Jeśli $a_1=1 \wedge b_1=1$, to mnożymy przez -1, wpp. nie. Zatem α to (-1) do potęgi $\#\{i \mid a_i=b_i=1\}$. Inaczej $\alpha = (-1)^{a_1a_2\cdot b_1b_2}$

Jak można wykorzystać zjawisko kwantowości?

Niech $f: \{0,1\}^n \to \{0,1\}^m$

Niech pewien obwód kwantowy U spełnia $|x\rangle|0\rangle \to |x\rangle|f(x)\rangle$

Wtedy $$U\left(\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle|0\rangle\right) = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle|f(x)\rangle$$

Czyli w pewnym sensie wszystkie 2^n wartości funkcji zostały policzone naraz. Przy czym obserwacja da tylko jedno, losowe $|x\rangle|f(x)\rangle$.

Trzeba tu więcej sprytu.

Problem Deutscha-Jozsa

Dana: funkcja $f: \{0,1\}^n \to \{0,1\}$ t.że albo
- $f(x)=0$ dla wszystkich $x\in\{0,1\}^n$ (stała), albo
- $f(x)=0$ dla dokładnie połowy $x\in\{0,1\}^n$ (zbalansowana)

Pytanie: która z tych dwóch opcji zachodzi

To jest prosta ilustracja działania alg. kwantowych.

Klasycznie do pewności potrzeba przeglądnąć $2^{n-1}+1$ zapytań.

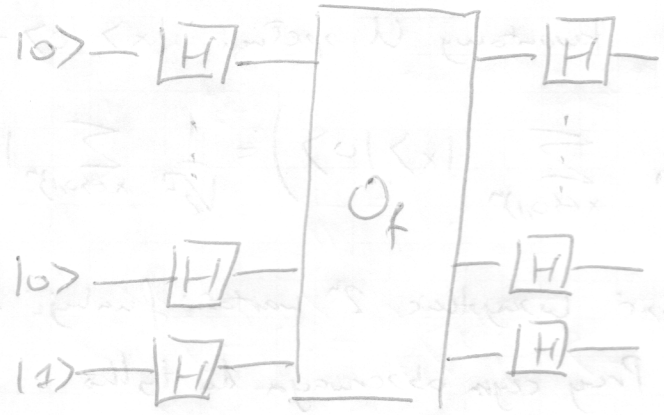
Kwantowo zrobimy w $O(n)$ bramkach. Załóżmy, że dysponujemy bramką $O_f: |x\rangle|0\rangle \longmapsto |x\rangle|f(x)\rangle$. To jest unitarne.

Ogólniej $O_f: |x\rangle|b\rangle \longmapsto |x\rangle|b \oplus f(x)\rangle$.

Zauważmy, że $O_f(|x\rangle|-\rangle) = \begin{cases} |x\rangle|-\rangle & \text{jeśli } f(x)=0 \\ |x\rangle(-1)|-\rangle & \text{jeśli } f(x)=1, \text{ czyli} \end{cases}$

$$O_f(|x\rangle|-\rangle) = (-1)^{f(x)}|x\rangle|-\rangle$$

Obwód jest taki:



- Zaczynamy od $|\underbrace{0\ldots0}_{n}\rangle|1\rangle$

- Po pierwszych Hadamardach:

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle|-\rangle$$

- Po O_f

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle|-\rangle$$

I grupujemy teraz ostatnie wyrazy, tzn. jest potrzebna tam bzdura

- Po drugich Hadamardach

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} H\left(|x\rangle \text{[illegible]}\right) = \text{bzdura}$$

$$= \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle$$

$|100\ldots0\rangle$ (n zer).

Wynosi ono $\frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} (-1)^{x \cdot 100\ldots0} =$

$$= \frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} = \begin{cases} 0 & \text{gdy } f \text{ zbalansowana} \\ 1 & \text{gdy stała} \end{cases}$$

Czyli jeśli zmierzymy $|10\ldots0\rangle$ to f stała, wpp. f zbalansowana.

Algorytm Shora

Najpierw pokażemy, że faktoryzację można (klasycznie) zredukować do problemu znajdowania okresu funkcji:

$f(a) = x^a \bmod N$.

Losujemy x ze zbioru $\{2, \ldots, N-1\}$.

Spr., czy $NWD(x, N) = 1$ (jeśli nie, to mamy pozafaktoryzację).

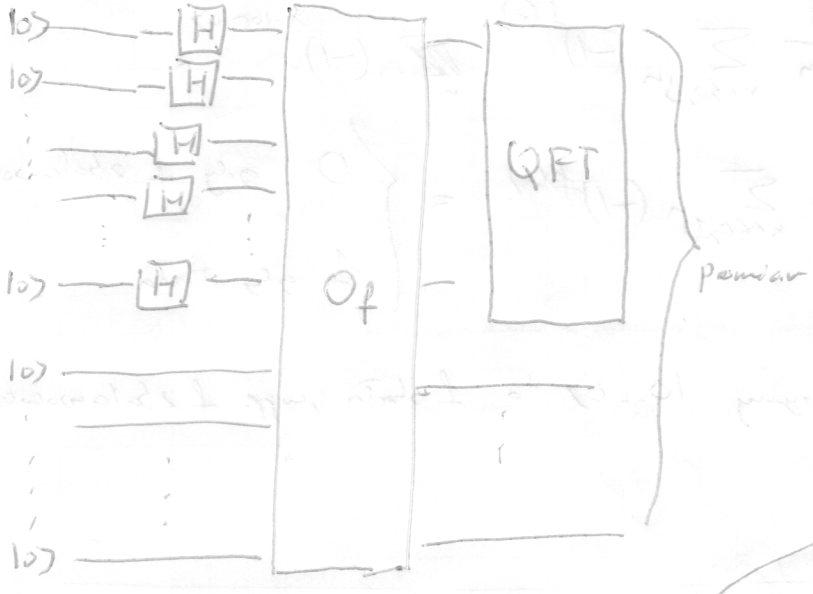
Nasz okres to r, czyli minimalny r t., że $x^r = 1 \bmod N$.

Ew. Pokażemy, że dla ostatniej przypadki ($\geq \frac{1}{4}$) x-ów (o ile $N \notin P$ jak sprawdzić) zachodzi:

- $2 \mid r$
- $x^{\frac{r}{2}} \not\equiv 1, -1 \bmod N$

Wtedy mamy $x^r = 1 \bmod N \Rightarrow N \mid (x^r - 1) = (x^{\frac{r}{2}} + 1)(x^{\frac{r}{2}} - 1)$, ale $N \nmid (x^{\frac{r}{2}} + 1)$, $N \nmid (x^{\frac{r}{2}} - 1)$. Przez policzenie NWD łatwo znaleźć czynniki.

Ogólna idea jest taka:



zakładamy, że x, n ; liczba kubitów jest zawyżona w obwodzie

gdzie $O_f((a,0)) = (a, x^a \bmod n)$, a QFT to kwantowa transformata Fouriera (quantum Fourier transform).

O_f można zaimplementować z grubsza tak jak klasycznie, czyli
$a = \sum_{i=0}^{k} a_i 2^i$, $x^a \bmod n = \left(\prod_{i=0}^{k} (x^{a_i 2^i} \bmod n)\right) \bmod n$.

Kwantowa transformata Fouriera to to, co się pojawiło na ćwiczeniach.

Załóżmy, że $q = 2^k$, jest k q kubitów.
Wówczas dla $j \in \{0, \dots, q-1\}$ QTF przekształca

$$|j\rangle \longmapsto \frac{1}{\sqrt{q}} \sum_{k=0}^{q-1} \omega^{jk} |k\rangle, \text{ gdzie } \omega = e^{\frac{2\pi i}{q}}$$

(zapisane)

$$\frac{1}{\sqrt{q}} \sum_{k=0}^{q-1} \omega^{jk} |k\rangle$$

Mamy, dla $s=4$, $l=2$ to

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 \\ 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega^9 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & \omega & -1 & -\omega \\ 1 & 1 & 1 & -1 \\ 1 & -\omega & -1 & \omega \end{bmatrix}$$

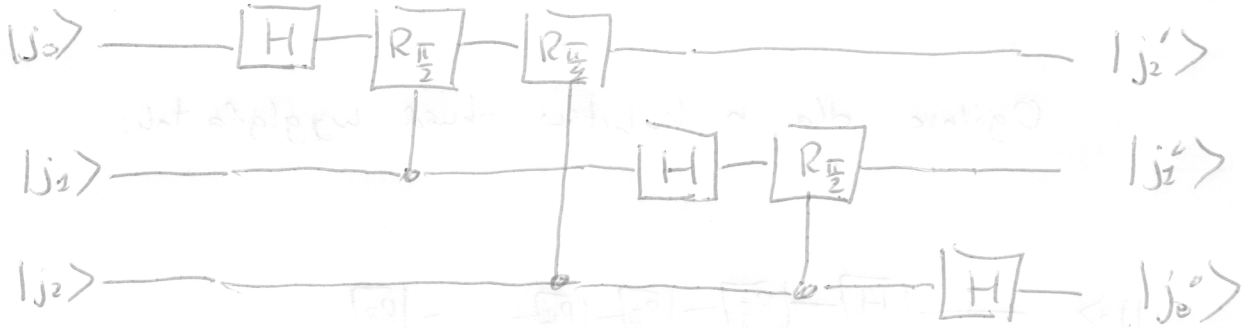
Będziemy używali

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

oraz

$$R_{\frac{\pi}{2^k}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{\frac{2\pi i}{2^k}} \end{bmatrix}$$, która obraca drugi bit o ile pierwszy i drugi są jedynkami

Spojrzmy jak wygląda taki obwód dla 3 kubitów.
Niech $j = \langle j_0 j_1 j_2 \rangle_2 = 4j_0 + 2j_1 + j_2$



Zobaczmy, że $|j_0'\rangle = H(|j_2\rangle) = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$,

a konkretnie $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ dla $j_2 = 0$ i
$\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ dla $j_2 = 1$.

Można to zapisać jako $\frac{1}{\sqrt{2}}(|0\rangle + (-1)^{j_2}|1\rangle)$

albo lepiej $\frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i \cdot (0.j_2)}|1\rangle)$,

gdzie $0.j_2$ interpretujemy bitowo (tzn. np. $0.101 = \frac{5}{8}$).

Teraz policzmy $|j_1'\rangle$.

Po Hadamardzie mamy $\frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i \cdot (0.j_1)}|1\rangle)$.

Potem jeszcze ~~przekręcamy~~ obracamy o $e^{2\pi i \cdot \frac{1}{2}} = e^{2\pi i \cdot (0.0j_2)}$ jeśli $j_2 = 1$.

Czyli obracamy ~~dodatkowo~~ $|1\rangle$ o $e^{2\pi i \cdot (0.0j_2)}$.

W sumie mamy

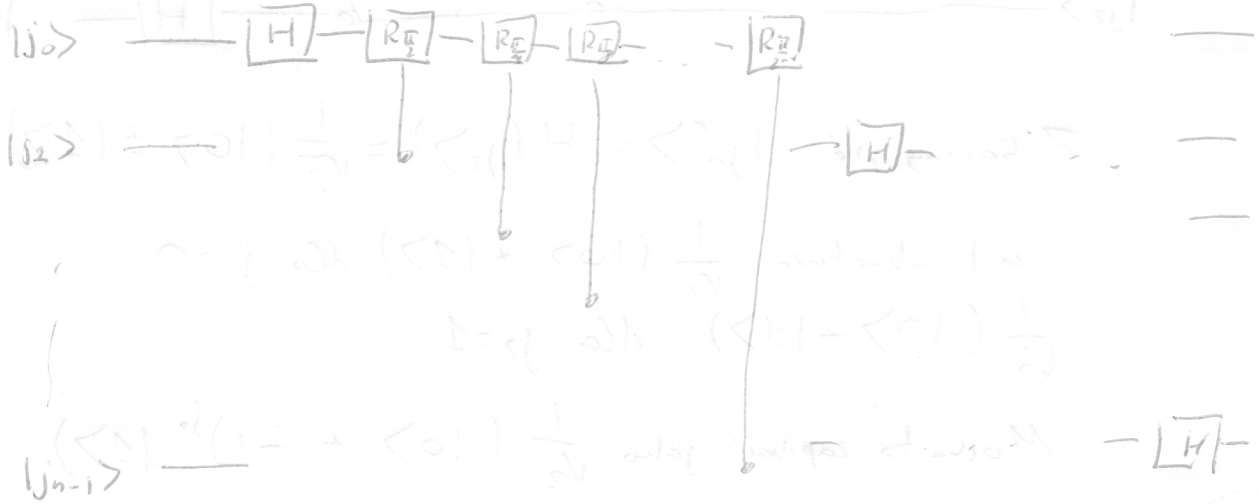
$$|j_1'\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i \cdot (0.j_1 j_2)}|1\rangle).$$

Analogicznie $|j_2'\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i \cdot (0.j_0 j_1 j_2}|1\rangle)$.

Ogólnie

$$|j\rangle \longmapsto \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i \cdot 0.j_0 j_1 j_2}|1\rangle)\otimes\frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i \cdot 0.j_1 j_2}|1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i \cdot 0.j_2}|1\rangle)$$

Ogólnie dla n kubitów obwód wygląda tak:



i oczywiście podobny zależność funkcyjny.

Teraz wystarczy pokazać że

$$|j\rangle \longmapsto \frac{1}{\sqrt{q}} \sum_{k=0}^{q-1} e^{\frac{2\pi i}{q} \cdot j \cdot k} |k\rangle \otimes$$

$$|j\rangle \longmapsto (|0\rangle + e^{2\pi i \, 0.j_0 j_1 - j_{n-1}} |1\rangle) \otimes \dots$$

to te same przekształcenia.

Zrobimy to na ćwiczeniach ĆW

Ogólnie można zrobić tak. Trzeba pokazać, że dla każdego $k \in \{0, \dots, q-1\}$ współczynnik przy $|k\rangle$ jest taki sam w obu przekształceniach.

Zobaczmy to dla 3 kubitów. Niech $\omega = e^{\frac{2\pi i}{8}}$.

$$|j\rangle \longmapsto (|0\rangle + \omega^{4j_2} |1\rangle) \otimes (|0\rangle + \omega^{4j_1 + 2j_2} |1\rangle) \otimes (|0\rangle + \omega^{4j_0 + 2j_1 + j_2} |1\rangle).$$

Czyli $j = 4j_0 + 2j_1 + j_2$. Niech $k = 4k_0 + 2k_1 + k_2$.

Oczywiście $\omega^{jk} = \omega^{jk \bmod 8}$.

Chcemy, by współczynnik przy $|k\rangle$ był $\omega^{jk \bmod 8}$. Pokażemy, że pierwszy nawias daje $\omega^{j \cdot 4k_0 \bmod 8}$, drugi $\omega^{j \cdot 2k_1 \bmod 8}$, a trzeci $\omega^{j \cdot k_2 \bmod 8}$.

Istotnie $j \cdot 4k_0 \equiv_{\bmod 8} j_2 \cdot 4k_0$, a to właśnie liczy pierwszy nawias. Podobnie

$$j \cdot 2k_1 \equiv (2j_1 + j_2) \cdot 2k_1 \equiv (4j_1 + 2j_2) \cdot k_1 \bmod 8$$

$$j \cdot k_2 \equiv (4j_0 + 2j_1 + j_2) \cdot k_2 \bmod 8$$

Analogicznie pokazuje się w ogólności.

Teraz wróćmy do algorytmu.

Chcemy rozłożyć N. Ustalamy ~~$q \in [N^2, 2N^2]$~~ $q \in [n^2, 2n^2]$ która jest potęgą dwójki. To, że $q > n^2$ przyda się później do pewnych oszacowań. Niech $q = 2^l$.

Dwoimy nasze wejście na dwa rejestry (tak, tyle samo), każdy po l kubitów. Rozważamy obwód ze strony 10. Na początku mamy stan ~~$|0\ldots0\rangle$~~ $|0\ldots0\rangle |0\ldots0\rangle$. Po bramkach Hadamarda mamy $\ldots |0\rangle$

$$\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle |0\rangle$$

Teraz po bramce O_f mamy

$$\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle |x^a \bmod n\rangle$$

Teraz aplikujemy QFT do pierwszego rejestru, która ma mapuje pojedyncze $|a\rangle$ na

$$\frac{1}{\sqrt{q}} \sum_{b=0}^{q-1} \omega^{ac} |b\rangle, \text{ gdzie } \omega = e^{\frac{2\pi i}{q}}$$

Dostajemy więc ogólnie

$$\frac{1}{q} \sum_{a=0}^{q-1} \sum_{b=0}^{q-1} \omega^{ac} |b\rangle |x^a \bmod n\rangle$$

Teraz obserwujemy stan.

Policzmy jakie jest prawdopodobieństwo, że zaobserwujemy pewne $|b\rangle|x^k \bmod n\rangle$ dla $0 \le k < r$.

Trzeba zsumować prawdopodobieństwa wszystkich możliwości uzyskania takiego wyniku.

Dostajemy

$$\left| \frac{1}{q} \sum_{\substack{a : x^a \equiv x^k \\ \bmod n}} \omega^{ab} \right|^2$$

Teraz są dwa przypadki: Łatwy, gdy $r|q$ i trudny, gdy $r \nmid q$.

Najpierw zrobimy łatwy, a potem nauczymy się rozwiązywać trudnego.

I. Przypadek $r|q$. Wtedy a takie $x^a \equiv x^k \bmod n$ są postaci $a = j \cdot r + k$, $j \ge 0$, $j \cdot r + k < q$, dla pewnego j $j \cdot r + k \le (\frac{q}{r} - 1) r$

Mamy wtedy $\sum_{\substack{a : x^a \equiv x^k \\ \bmod n}} \omega^{ab} =$

$$= \sum_{j=0}^{\frac{q}{r}-1} \omega^{(j \cdot r + k) b} = \omega^{kb} \cdot \sum_{j=0}^{\frac{q}{r}-1} e^{\frac{2\pi i}{q} \cdot j \cdot r \cdot b} =$$

$$= \omega^{kb} \cdot \sum_{j=0}^{\frac{q}{r}-1} \left(e^{2\pi i \cdot \frac{r \cdot b}{q}} \right)^j$$

To jest różne od 0 wtw. gdy $e^{2\pi i \cdot \frac{rb}{q}} = 1$, czyli $\frac{rb}{q} \in \mathbb{N}$. Czyli praw. $\neq 0$ mają tylko $|b\rangle$ takie, że $\frac{rb}{q} \in \mathbb{N}$.

Powiedzmy więc, że zaobserwowaliśmy pewne b t.że $b \cdot \frac{v}{q} \in \mathbb{N}$, mech $b : \frac{v}{q} = c$.

Wówczas $\frac{b}{q} = \frac{c}{v}$. Znamy q i b, ~~skąd~~ nie znamy c i v.

Jest fakt, że prawd., że $c \perp v$ to $\Omega\left(\frac{1}{\log\log v}\right)$, czyli sporo. Jeśli $c \perp v$, to po prostu skracamy ułamek $\frac{b}{q}$ i bierzemy mianownik.

Jeśli nie, to

$$\frac{b}{q} = \frac{c'}{v'}, \quad c' \perp v', \text{ gdzie } v' \leq v.$$

Zatem robiąc to parę razy, zawsze otrzymamy $v' \leq v$.

Bierzemy najmniejszy z dwóch prawd. to jest v.

II. Przypadek $v \nmid q$. Wówczas nie mamy $\frac{b}{q} = \frac{c}{v}$, ale ~~można~~ można pokazać, że z dwóch prawd. dostajemy

$$\left|\frac{b}{q} - \frac{c}{v}\right| \leq \frac{1}{2q}$$

Ponieważ $q > n^3$, to w każdym przedziale o dł. $\frac{1}{q} < \frac{1}{n^3}$ jest maksymalnie jeden ułamek o mianowniku $\leq n$.

Zatem $\frac{c}{v}$ jest wyznaczony jednoznacznie. To się da policzyć np. przez ułamki Taśmuchowe ~~dla tego też~~

W ten sposób rozwiązuje się ten trudniejszy przypadek.