Lecture 2-Introduction to Quantum Algorithms

Costas Daskaloyannis

2014-2015

Factorization

Def. Order of x modulo N

$\gcd(x, N) = 1$, $r =$ order of x modulo N
r is the least natural number such that $x^r \equiv 1 \mod (N)$

Algorithm for finding a factor of the odd number N

Step 1 : Choose a random number $x < N$. If $\gcd(x, N) \neq 1$ then Return $\gcd(x, N)$.

Step 2 : Find the order r of x modulo N. If r is odd then go to Step 1.

Step 3 : If $1 < \gcd\left(x^{\frac{r}{2}} - 1, N\right) < N$ then Return $\gcd\left(x^{\frac{r}{2}} - 1, N\right)$.

Step 4 : If $1 < \gcd\left(x^{\frac{r}{2}} + 1, N\right) < N$ then Return $\gcd\left(x^{\frac{r}{2}} + 1, N\right)$ else go to Step 1.

Definition: Simple Continued fraction

$$[a_0; a_1, a_2, \ldots, a_M] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{a_M}}}}$$

Any rational number can be represented by a simple continued fraction

$$\frac{327}{29} = [11; 4, 1, 5] = 11 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{5}}}$$

$$\sqrt{2} = [1; 2, 2, 2, \ldots] = [1; \overline{2}], \ \sqrt{12} = [3, 2, 6, 2, 6, \ldots] = [3; \overline{2, 6}]$$

Definition: Generalized Continued fraction

$$[a_0; b_1, a_1, b_2, a_2, \ldots, b_M, a_M] = a_0 + \cfrac{b_1}{a_1 + \cfrac{b_2}{a_2 + \cfrac{1}{\cdots + \cfrac{b_M}{a_M}}}}$$

Definition: Convergents

$$\frac{p_n}{q_n} = [a_0, b1, a_1, b_2, a_2, \ldots, b_n, , a_n]$$

$$p_0 = a_0,\ q_0 = 1\ p_1 = 1 + a_0 a_1,\ q_1 = a_1$$

$$p_n = a_n p_{n-1} + b_n p_{n-2},\ q_n = a_n q_{n-1} + b_n q_{n-2}$$

If $\lim_{n\to\infty} \frac{p_n}{q_n}$ then $\frac{p_k}{q_k}$ for $k = 1, 2, \ldots$ is a "covergent".

Continued fractions of real numbers

Set of all continued fractions $= \mathbb{R}_+ =$ positive real numbers

Theorem

If $x \in \mathbb{R}$ and $\left|\frac{p}{q} - x\right| \leq \frac{1}{2q^2} \Rightarrow \frac{p}{q}$ is a convergent of the continued fraction of x.

Classical Discrete Fourier Transform - FFT

$$\mathbb{R}^N \ni x = \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ \vdots \\ x_{N-1} \end{pmatrix} \xrightarrow{F} y = \begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ \vdots \\ y_{N-1} \end{pmatrix} \in \mathbb{R}^N$$

$$\omega = \exp\left[\frac{2\pi i}{N}\right], \qquad y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \omega^{k\,j} x_j$$

$$F \leftrightarrow \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2(N-1)} \\ 1 & \omega^3 & \omega^6 & \cdots & \omega^{3(N-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \cdots & \omega^{(N-1)(N-1)} \end{pmatrix}$$

$$\omega^N = 1, \, \overline{\omega}^j = \frac{1}{\omega^j} = \omega^{N-j} \rightsquigarrow \sum_{j=0}^{N-1} \left(\omega^k \overline{\omega}^\ell\right)^j = N\delta_{k\,\ell} \rightsquigarrow F^\dagger F = \mathbb{I}$$

Quantum Fourier Transform - QFT

$$j = \sum_{m=1}^{n} j_m 2^{n-m} \rightsquigarrow \underbrace{\bar{j} = j_1\, j_2\, j_3\, \ldots\, j_n,}_{\text{binary system}} \qquad j_m = 0 \text{ or } 1$$

$$\frac{j}{2^n} = \sum_{m=1}^{n} \frac{j_m}{2^m}$$

$$|j\rangle \equiv |\bar{j}\rangle = |j_1\, j_2\, j_3\, \ldots\, j_n\rangle = |j_1\rangle \otimes |j_2\rangle \otimes \cdots \otimes |j_n\rangle \equiv \bigotimes_{m=1}^{n} |j_m\rangle$$

Definition QFT

$$|j\rangle \xrightarrow{\text{QFT}} \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \omega^{j\,k} |k\rangle, \; \omega = \exp\left[\frac{2\pi i}{2^n}\right]$$

QFT factorization

$$|\bar{j}\rangle \xrightarrow{\text{QFT}} \sum_{k_1=0}^{1}\sum_{k_2=0}^{1}\cdots\sum_{k_n=0}^{1} \exp\left[\frac{2\pi i}{2^n} j \overbrace{\left(\sum_{\ell=1}^{n} k_\ell 2^{n-\ell}\right)}^{k}\right] \bigotimes_{m=1}^{n} |k_m\rangle =$$

$$= \sum_{k_1=0}^{1}\sum_{k_2=0}^{1}\cdots\sum_{k_n=0}^{1} \left(\prod_{\ell=1}^{n} \exp\left[\frac{2\pi i}{2^n} j\ k_\ell 2^{n-\ell}\right]\right) \bigotimes_{m=1}^{n} |k_m\rangle = \bigotimes_{m=1}^{n} \left(\sum_{k_m=0}^{1} \exp\left[\frac{2\pi i\, j\ k_m}{2^m}\right] |k_m\rangle\right)$$

$$\exp\left[\frac{2\pi i\, j}{2^m}\right] = exp\left[2\pi i \overbrace{\left(\sum_{\ell=1}^{n} j_\ell 2^{n-\ell}\right)}^{j} /2^m\right]$$

$$\frac{\left(\sum_{\ell=1}^{n} j_\ell 2^{n-\ell}\right)}{2^m} = \frac{j_1 2^{n-1} + j_2 2^{n-2} + \cdots + j_{n-m-1} 2^{m+1} + j_{n-m} 2^m}{2^m} +$$

$$+ \frac{j_{n-m+1} 2^{m-1} + j_{n-m+2} 2^{m-2} + \cdots + j_n}{2^m} =$$

$$= 0.j_{n-m+1} j_{n-m+2} \ldots j_n + M,\ M \in \mathbb{Z}$$

$$exp\left[2\pi i\ k_m \left(\sum_{\ell=1}^{n} j_\ell 2^{n-\ell}\right) /2^m\right] = \exp\left[2\pi i\ k_m \underbrace{0.j_{n-m+1} j_{n-m+2} \ldots j_1}_{\text{binary}}\right] |1\rangle$$

$$|j\rangle \xrightarrow{\text{QFT}} \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \exp\left[\frac{2\pi i\, jk}{2^n}\right] |k\rangle =$$

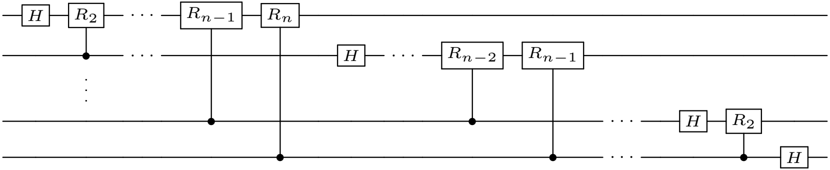
$$= \frac{1}{\sqrt{2^n}} \bigotimes_{m=1}^{n} \left(\sum_{k_m=0}^{1} \exp\left[\frac{2\pi i\, j\, k_m}{2^m}\right] |k_m\rangle \right) =$$

$$= \bigotimes_{m=1}^{n} \left(\frac{|0\rangle + \exp\left[\frac{2\pi i\, j}{2^m}\right] |1\rangle}{\sqrt{2}} \right) =$$

$$= \bigotimes_{m=1}^{n} \left(\frac{|0\rangle + \exp\left[2\pi i \;\; 0.j_{n-m+1} j_{n-m+2} \ldots j_1\right] |1\rangle}{\sqrt{2}} \right)$$

QFT gate

$$R_k = \begin{bmatrix} 1 & 0 \\ 0 & \exp\left[\frac{2\pi i}{2^k}\right] \end{bmatrix}$$



Quantum phase estimation

Let $U|u\rangle = \exp[2\pi i\,\sigma]|u\rangle = \exp[2\pi i\,\frac{\phi}{q}]|u\rangle$, $q = 2^n$, $q\sigma = \phi \in \mathbb{R}$

Step 1: **initial state** $\rightsquigarrow |0\rangle \otimes |u\rangle$

Step 2: **apply** $H^{\otimes n} \otimes \mathbb{I} \rightsquigarrow \frac{1}{\sqrt{q}} \sum_{j=0}^{q-1} |j\rangle \otimes |u\rangle$

Step 3: **apply "black box"**

$$\rightsquigarrow \frac{1}{\sqrt{q}} \sum_{j=0}^{q-1} |j\rangle \otimes U^j|u\rangle \longrightarrow \frac{1}{\sqrt{q}} \sum_{j=0}^{q-1} \exp[2\pi i\, j\frac{\phi}{q}]|j\rangle \otimes |u\rangle$$

Step 4: **apply Inverse QFT** $\sum_{k=0}^{q-1} \underbrace{\left(\frac{\sum_{j=0}^{q-1} \exp\left[2\pi i\, j\frac{\phi - k}{q}\right]}{q} \right)}_{A_k(\sigma)} |k\rangle \otimes |u\rangle$

Step 5: The probabiity to be in the state $\left|\widetilde{\phi}\right\rangle \otimes |u\rangle$ is larger than 40%
measure of the first register and the result is larger than 40%
to find $\widetilde{\phi}$

Where $\widetilde{\phi}$ is the nearest integer for the number $\phi \rightsquigarrow \left|\frac{\phi}{q} - \frac{\widetilde{\phi}}{q}\right| \leq \frac{1}{2q}$

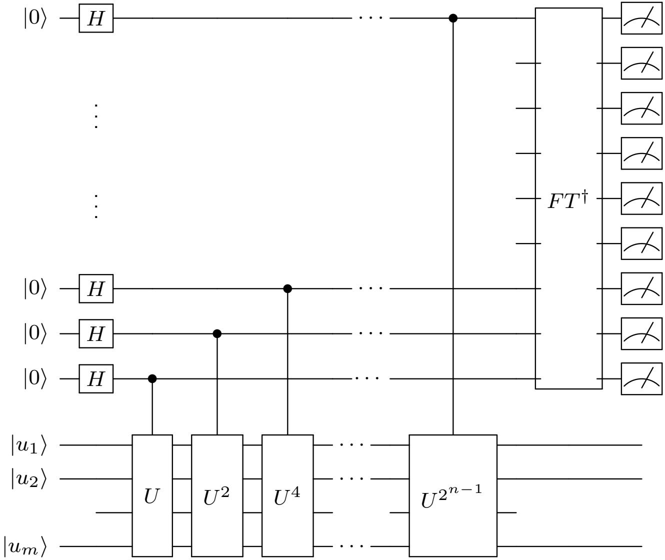
Probability of finding $|k\rangle$ in the first register

$$|A_k(\sigma)|^2 = P(k) = \left| \frac{1}{q} \sum_{j=0}^{q-1} \exp\left[2\pi i\, j \frac{\phi - k}{q}\right] \right|^2 = \frac{\sin^2(\pi(\phi - k))}{q^2 \sin^2\left(\pi \frac{\phi - k}{q}\right)}$$

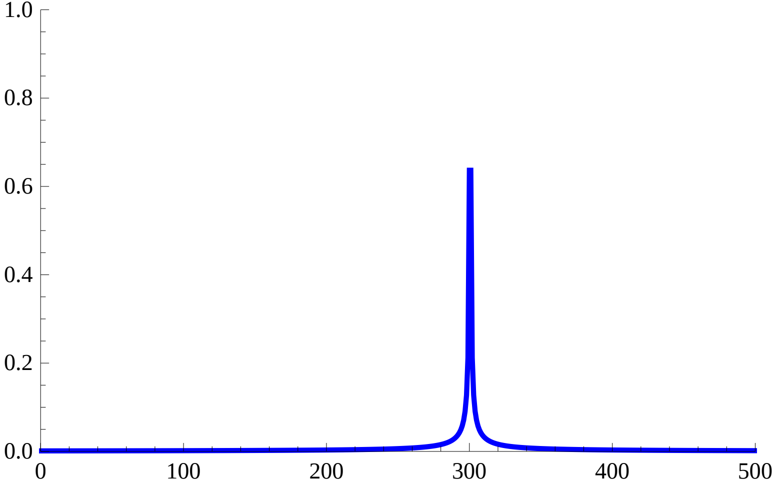
$\widetilde{\phi}$ is the nearest integer for the number $\phi \rightsquigarrow \left|\phi - \widetilde{\phi}\right| \leq \frac{1}{2}$

$$P(\widetilde{\phi}) = \frac{\sin^2\left(\pi(\phi - \widetilde{\phi})\right)}{q^2 \sin^2\left(\pi \frac{\phi - \widetilde{\phi}}{q}\right)} = \underbrace{\frac{\sin^2\left(\pi(\phi - \widetilde{\phi})\right)}{\left(\pi(\phi - \widetilde{\phi})\right)^2}}_{\geq \left(\frac{\sin\frac{\pi}{2}}{\frac{\pi}{2}}\right)^2} \underbrace{\frac{\left(\pi \frac{\phi - \widetilde{\phi}}{q}\right)^2}{\sin^2\left(\pi \frac{\phi - \widetilde{\phi}}{q}\right)}}_{\geq 1}$$

$P(\widetilde{\phi}) \geq \frac{4}{\pi^2} \approx 0.4053 \rightsquigarrow$ Probability larger than 40 % to find $\widetilde{\phi}$



|0⟩
H
|0⟩
H
|0⟩
H
|0⟩
H
|u1⟩
|u2⟩
|um⟩
U
U^2
U^4
U^{2^{n-1}}
FT†



$n = 5$ qu-bits, $\phi = 300.5$

Order Calculation Algorithm

$$|u_s\rangle = \frac{1}{\sqrt{r}}\sum_{k=0}^{r}\exp[-2\pi i\,\frac{sk}{r}]\Big|x^k \mod N\Big\rangle \rightsquigarrow \Big|x^k \mod N\Big\rangle = \frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}\exp[2\pi i\,\frac{sk}{r}]|u_s\rangle$$

$$\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|u_s\rangle = |\bar{1}\rangle$$

$$U|y\rangle = |xy \mod N\rangle \rightsquigarrow U|u_s\rangle = \exp[2\pi i\,\frac{s}{r}]|u_s\rangle = \exp[2\pi i\,\frac{\phi_s}{q}]|u_s\rangle$$

$\frac{s}{r} = \sigma = \dfrac{\phi_s}{q}$ quantum phase of the operator U $\rightsquigarrow$

we apply the Quantum phase algorithm for U

$$\frac{1}{\sqrt{q}}\sum_{j=0}^{q-1}|j\rangle\otimes|x^j \mod N\rangle = \frac{1}{\sqrt{q}}\sum_{j=0}^{q-1}|j\rangle\otimes\left(\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}\exp[2\pi i\,\frac{js}{r}]|u_s\rangle\right) =$$

$$= \frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}\left(\sum_{j=0}^{q-1}\exp\left[2\pi i j\frac{s}{r}\right]|j\rangle\right)\otimes|u_s\rangle \xrightarrow{\text{QFT}^\dagger} \frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}\left(\sum_{k=0}^{q-1}A_k\left(\frac{s}{r}\right)|k\rangle\right)\otimes|u_s\rangle$$

We measure the left register we find some $k = \widetilde{\phi_s}$ with probability 40%
to be an approximation to $\frac{s}{r}q$

Classical Part

Factorization Problem

Given an integer N, find another integer p between 1 and N that divides N.

Classical part

Step 1: Pick a pseudo-random number $x < N$

Step 2: Compute $\gcd(x, N)$. (Euclidean algorithm).

Step 3: If $\gcd(x, N) \neq 1$, then there is a nontrivial factor of $N \mapsto$ **Return**.

Step 4: Use the quantum period-finding subroutine to find r, the "period" of x, $x^r \equiv 1 \mod N$

Step 5: If r is odd $\mapsto$ **step 1**.

Step 6: If $x^{r/2} = -1 \pmod N \mapsto$ **step 1**.

Step 7: The factors of N are $\gcd(x^{r/2} \pm 1, N) \mapsto$ **Return**.

Quantum Part

QStep 1: Starting with a pair of input and output qubit registers with $n > \log_2 N^2$ qubits each, we apply a Hadamard gate ($q = 2^n$) on the first register

$$|\overline{0}\rangle \otimes |\overline{1}\rangle \longrightarrow \frac{1}{\sqrt{q}} \sum_{\overline{k}=0}^{q-1} |\overline{k}\rangle \otimes |\overline{1}\rangle$$

QStep 2: We construct the "power" function

$$\frac{1}{\sqrt{q}} \sum_{\overline{k}=0}^{q-1} |\overline{k}\rangle \otimes |\overline{1}\rangle \longrightarrow \frac{1}{\sqrt{q}} \sum_{\overline{k}=0}^{q-1} |\overline{k}\rangle \otimes |\overline{x}^k \mod (N)\rangle$$

QStep 3: We apply the Quantum Fourier Transform on the first register

$$\frac{1}{\sqrt{q}} \sum_{\overline{k}=0}^{q-1} |\overline{k}\rangle \otimes |\overline{x}^k \mod (N)\rangle \xrightarrow{\text{QFT}^\dagger} \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \left|\widetilde{\phi_s}\right\rangle \otimes |u_s\rangle$$

QStep 4: We perform a measure on the first register and we find $\widetilde{\phi_s}$ an approximation to some ϕ_s

$$\left|\frac{\phi_s}{q} - \frac{\widetilde{\phi_s}}{q}\right| \leq \frac{1}{2q}$$

If $N^2 < q = 2^n < 2N^2 \rightsquigarrow n \approx [2\ln_2 N + 1]$ and we know that $r < N$ then

$$\left|\frac{s}{r} - \frac{\widetilde{\phi_s}}{q}\right| < \frac{1}{2r^2}$$

$\frac{s}{r}$ is a convergent of the measured $\frac{\widetilde{\phi_s}}{q}$

QStep 5: We start calculate the convergents $\frac{s}{r}$ of the $\frac{\widetilde{\phi_s}}{q}$ and we stop if the previous condition is true. Then we find the period r.

The complexity=number of basic gates $\sim$ Polynomial of $n \rightsquigarrow$ Polynomial of $\log N$
$N = 10^{10} \rightsquigarrow n \approx 70$