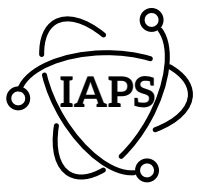
Lecture 20

QUANTUM CRYPTOGRAPHY. PART 5 - Periods of functions using a quantum circuit

of the course "Fundamentals of Quantum Computing"

(by IAPS *and* QUANTERALL*)*

Stoyan Mishev



INSTITUTE *for* ADVANCED
PHYSICAL STUDIES

October 28, 2022

Steps in Shor's algorithm

Steps in Shor's algorithm

Input: An odd natural number N that has at least two distinct prime factors

Step 1: Choose $b \in \mathbb{N}$ with $b < N$ and determine $\gcd(b,N)$.
If

$\gcd(b,N) > 1$, then we are done. Go to Output and show $\gcd(b,N)$ and $\frac{N}{\gcd(b,N)}$ — $\gcd(b,N)$ is a non-trivial factor of N and

$\gcd(b,N) = 1$, then go to Step 2

Step 2: Determine the period r of the function

$$f_{b,N} : \mathbb{N}_0 \longrightarrow \mathbb{N}_0$$
$$n \longmapsto f_{b,N}(n) := b^n \bmod N .$$

If

r is odd, then start anew with Step 1

r is even, then go to Step 3

Step 3: Determine $\gcd(b^{\frac{r}{2}} + 1, N)$.
If

$\gcd(b^{\frac{r}{2}} + 1, N) = N$, then start anew with Step 1

$\gcd(b^{\frac{r}{2}} + 1, N) < N$, then with $\gcd(b^{\frac{r}{2}} + 1, N)$ we have found a non-trivial factor of N. Calculate $\gcd(b^{\frac{r}{2}} - 1, N)$ as a further factor of N. Go to Output and show $\gcd(b^{\frac{r}{2}} \pm 1, N)$

Output: Two non-trivial factors of N

Examples of order of modulo

m	1	2	3	4	5	6	7	8	9	10	11	...
$7^m \bmod 15$	7	4	13	1	7	4	13	1	7	4	13	...

m	1	2	3	4	5	6	7	8	9	10	11	...
$7^m \bmod 10$	7	9	3	1	7	9	3	1	7	9	3	...

https://www.youtube.com/watch?v=fwuj4yzoX1o

Functions as unitary transformations

1. The function f can be implemented as a unitary transformation U_f on a suitable HILBERT space so that the growth in the number of computational steps S_{U_f} required to execute U_f is suitably bounded.
2. An upper bound of the period r in the form

$$r < 2^{\frac{L}{2}}$$

   exists, where $L \in \mathbb{N}$ is known.
3. The function is injective within a period.

$$\begin{aligned} U_f : \mathbb{H}^{\otimes L} \otimes \mathbb{H}^{\otimes K} &\longrightarrow \mathbb{H}^{\otimes L} \otimes \mathbb{H}^{\otimes K} \\ |x\rangle \otimes |y\rangle &\longmapsto |x\rangle \otimes |y \boxplus f(x)\rangle \end{aligned}$$

Th. Existence of q. algo for period determination

Theorem 6.8 *Let $r, L \in \mathbb{N}$ with $19 \leq r < 2^{\frac{L}{2}}$ and let r be the period of a function $f : \mathbb{N}_0 \to \mathbb{N}_0$ that is injective within one period and bounded by 2^K. Furthermore, let U_f be a unitary transformation that implements f as follows*

$$\begin{aligned} U_f : \P\mathbb{H}^{\otimes L} \otimes \P\mathbb{H}^{\otimes K} &\longrightarrow \P\mathbb{H}^{\otimes L} \otimes \P\mathbb{H}^{\otimes K} \\ |x\rangle \otimes |y\rangle &\longmapsto |x\rangle \otimes |y \boxplus f(x)\rangle \end{aligned} \tag{6.28}$$

(where $\boxplus$ is defined in Definition 5.31) and requires a number of computational steps $\mathrm{S}_{U_f}(L)$, which satisfies:

$$S_{U_f}(L) \in O\left(L^{K_f}\right) \qquad \text{for } L \to \infty$$

for a $K_f \in \mathbb{N}$. Then there exists a quantum mechanical algorithm A with which we can find the period r with a probability of at least $\frac{1}{10 \ln L}$. *The number of computational steps of this algorithm $S_A(L)$ satisfies*

$$S_A(L) \in O\left(L^{\max\{K_f, 3\}}\right) \qquad \text{for } L \to \infty. \tag{6.29}$$

1. Preparation of the input register and the initial state
2. Exploiting massive quantum parallelism
3. Application of the quantum FOURIER transform
4. Probability in measurement of the input register
5. Probability to find r as the denominator in the continued fraction approximation
6. Aggregation of the number of computational steps

Preparation of the input register and the initial state

$$|\Psi_0\rangle := |0\rangle^A \otimes |0\rangle^B = \underbrace{|0\rangle \otimes \cdots \otimes |0\rangle}_{L-\text{times}} \otimes \underbrace{|0\rangle \otimes \cdots \otimes |0\rangle}_{K-\text{times}}$$

where $M := \max\{f(x)|x \in \{0, ..., 2^L - 1\}\}$

Preparation of the input register and the initial state

$$|\Psi_0\rangle := |0\rangle^A \otimes |0\rangle^B = \underbrace{|0\rangle \otimes \cdots \otimes |0\rangle}_{L-\text{times}} \otimes \underbrace{|0\rangle \otimes \cdots \otimes |0\rangle}_{K-\text{times}}$$

where $M := \max\{f(x)|x \in \{0, ..., 2^L - 1\}\}$ and L is related to the period $r < 2^{L/2}$.

Preparation of the input register and the initial state

$$|\Psi_0\rangle := |0\rangle^A \otimes |0\rangle^B = \underbrace{|0\rangle \otimes \cdots \otimes |0\rangle}_{L-\text{times}} \otimes \underbrace{|0\rangle \otimes \cdots \otimes |0\rangle}_{K-\text{times}}$$

where $M := \max\{f(x)|x \in \{0, ..., 2^L - 1\}\}$ and L is related to the period $r < 2^{L/2}$.

$$|\Psi_1\rangle := H^{\otimes L} \otimes \mathbf{1}^B |\Psi_0\rangle = \frac{1}{2^{\frac{L}{2}}} \sum_{x=0}^{2^L-1} |x\rangle^A \otimes |0\rangle^B$$

where H is the Hadamard gate.

$$S_{\text{Prep}}(L) \in O(L) \text{ for } L \to \infty. \tag{1}$$

Exploiting massive quantum parallelism

$$U_f\left(|x\rangle^A \otimes |y\rangle^B\right) = |x\rangle^A \otimes |y \boxplus f(x)\rangle^B = |x\rangle^A \otimes \bigotimes_{j=K-1}^{0} |y_j \overset{2}{\oplus} f(x)_j\rangle$$

$$U_f\left(|x\rangle^A \otimes |y\rangle^B\right) = |x\rangle^A \otimes |y \boxplus f(x)\rangle^B = |x\rangle^A \otimes \bigotimes_{j=K-1}^{0} |y_j \overset{2}{\oplus} f(x)_j\rangle$$

$$|\Psi_2\rangle := U_f|\Psi_1\rangle = U_f\left(\frac{1}{2^{\frac{L}{2}}}\sum_{x=0}^{2^L-1}|x\rangle^A \otimes |0\rangle^B\right) = \frac{1}{2^{\frac{L}{2}}}\sum_{x=0}^{2^L-1}|x\rangle^A \otimes |f(x)\rangle^B$$

$$U_f\left(|x\rangle^A \otimes |y\rangle^B\right) = |x\rangle^A \otimes |y \boxplus f(x)\rangle^B = |x\rangle^A \otimes \bigotimes_{j=K-1}^{0} |y_j \overset{2}{\oplus} f(x)_j\rangle$$

$$|\Psi_2\rangle := U_f|\Psi_1\rangle = U_f\left(\frac{1}{2^{\frac{L}{2}}}\sum_{x=0}^{2^L-1}|x\rangle^A \otimes |0\rangle^B\right) = \frac{1}{2^{\frac{L}{2}}}\sum_{x=0}^{2^L-1}|x\rangle^A \otimes |f(x)\rangle^B$$

$$|a \boxplus b\rangle := \bigotimes_{j=m-1}^{0} |a_j \overset{2}{\oplus} b_j\rangle$$

$$u \overset{2}{\oplus} v := (u+v) \mod 2$$

Rewrite $|\Psi_2\rangle$

$$|\Psi_2\rangle = \frac{1}{2^{\frac{L}{2}}} \sum_{k=0}^{r-1} \sum_{j=0}^{J_k} |jr+k\rangle^A \otimes |f(k)\rangle^B$$

Rewrite $|\Psi_2\rangle$

$$|\Psi_2\rangle = \frac{1}{2^{\frac{L}{2}}} \sum_{k=0}^{r-1} \sum_{j=0}^{J_k} |jr+k\rangle^A \otimes |f(k)\rangle^B$$

$$J := \left\lfloor \frac{2^L - 1}{r} \right\rfloor \tag{6.36}$$

$$R := (2^L - 1) \bmod r. \tag{6.37}$$

Then we have

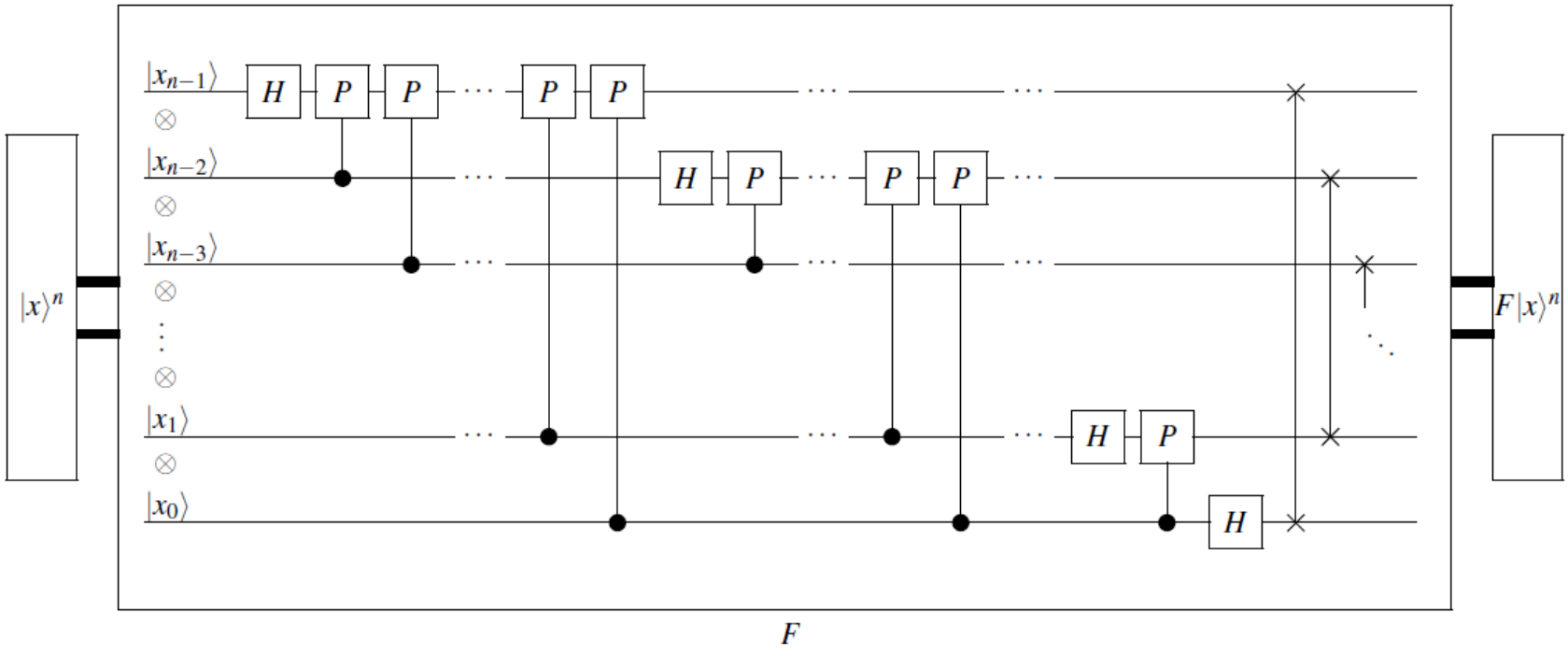
$$\begin{aligned}
|\Psi_2\rangle = \\
\frac{1}{2^{\frac{L}{2}}} \Big[& |0\rangle^A \otimes |f(0)\rangle^B + \cdots + |r-1\rangle^A \otimes |f(r-1)\rangle^B \\
+ & |r\rangle^A \otimes \underbrace{|f(r)\rangle^B}_{=|f(0)\rangle^B} + \cdots + |2r-1\rangle^A \otimes \underbrace{|f(2r-1)\rangle^B}_{=|f(r-1)\rangle^B} \\
+ & \vdots \quad \vdots \quad \vdots \qquad \vdots \quad \vdots \quad \vdots \\
+ & |(J-1)r\rangle^A \otimes \underbrace{|f((J-1)r)\rangle^B}_{=|f(0)\rangle^B} + \cdots + |Jr-1\rangle^A \otimes \underbrace{|f(Jr-1)\rangle^B}_{=|f(r-1)\rangle^B} \\
+ & |Jr\rangle^A \otimes \underbrace{|f(Jr)\rangle^B}_{=|f(0)\rangle^B} \cdots + |Jr+R\rangle^A \otimes \underbrace{|f(Jr+R)\rangle^B}_{=|f(R)\rangle^B} \Big]
\end{aligned}$$

$$= \frac{1}{2^{\frac{L}{2}}} \left[\sum_{j=0}^{J-1} \sum_{k=0}^{r-1} |jr+k\rangle^A \otimes |f(k)\rangle^B + \sum_{k=0}^{R} |Jr+k\rangle^A \otimes |f(k)\rangle^B \right].$$

Furthermore, defining for $k \in \mathbb{N}_0$

$$J_k := \begin{cases} J & \text{if } k \le R \\ J-1 & \text{if } k > R, \end{cases} \tag{6.38}$$

Q. Fourier transform of $|\Psi_2\rangle$



Theorem 5.56 *The quantum* FOURIER *transform F can be built from the swap operator $S^{(n)}$ defined in (5.30),* HADAMARD *transforms and conditional phase shifts as follows:*

$$F = S^{(n)} \prod_{j=0}^{n-1} \left(\left[\prod_{k=0}^{j-1} P_{jk} \right] H_j \right) \tag{5.133}$$
$$= S^{(n)} H_0 P_{1,0} H_1 P_{2,0} P_{2,1} H_2 \ldots P_{n-1,0} \ldots P_{n-1,n-2} H_{n-1} \,.$$

Q. Fourier transform of $|\Psi_2\rangle$

Lemma 5.52 *Let $n \in \mathbb{N}$ and*

$$x = \sum_{j=0}^{n-1} x_j 2^j \,, \tag{5.126}$$

where $x_j \in \{0,1,\}$ for $j \in \{0,\ldots,n-1\}$.

Then the action of the quantum FOURIER *transform F on any vector $|x\rangle$ of the computational basis of $\mathbb{H}^n$ can be written as*

$$F|x\rangle = \frac{1}{\sqrt{2^n}} \bigotimes_{j=0}^{n-1} \left[|0\rangle + \mathrm{e}^{2\pi \mathrm{i} 0.x_j \ldots x_0} |1\rangle \right] . \tag{5.127}$$

Definition 5.51 For $a_1,\ldots,a_m \in \{0,1\}$ we define

$$0.a_1 a_2 \ldots a_m := \frac{a_1}{2} + \frac{a_2}{4} + \cdots \frac{a_m}{2^m} = \sum_{l=1}^{m} a_l 2^{-l}$$

$$S^{(n)} \prod_{j=0}^{n-1} \left(\prod_{k=0}^{j-1} \left(P_{jk}\right) H_j \right) |x\rangle \underbrace{=}_{(5.134)} \frac{1}{\sqrt{2^n}} S^{(n)} \bigotimes_{k=n-1}^{0} \left[|0\rangle + \mathrm{e}^{2\pi \mathrm{i} 0.x_k \ldots x_0} |1\rangle \right]$$

$$\underbrace{=}_{(5.34)} \frac{1}{\sqrt{2^n}} \bigotimes_{k=0}^{n-1} \left[|0\rangle + \mathrm{e}^{2\pi \mathrm{i} 0.x_k \ldots x_0} |1\rangle \right]$$

$$= F|x\rangle \,.$$

Q. Fourier transform of the A registers of $|\Psi_2\rangle$

$$
\begin{aligned}
|\Psi_3\rangle &:= \left(F \otimes \mathbf{1}^B\right) |\Psi_2\rangle \\
&= \left(F \otimes \mathbf{1}^B\right) \left(\frac{1}{2^{\frac{L}{2}}} \sum_{k=0}^{r-1} \sum_{j=0}^{J_k} |jr+k\rangle^A \otimes |f(k)\rangle^B \right) \\
&\underbrace{=}_{(6.39)} \frac{1}{2^{\frac{L}{2}}} \sum_{k=0}^{r-1} \sum_{j=0}^{J_k} \left(F|jr+k\rangle^A\right) \otimes |f(k)\rangle^B \\
&\underbrace{=}_{(6.40)} \frac{1}{2^L} \sum_{k=0}^{r-1} \sum_{j=0}^{J_k} \sum_{l=0}^{2^L-1} \exp\left(2\pi i \frac{l}{2^L}(jr+k)\right) |l\rangle^A \otimes |f(k)\rangle^B
\end{aligned}
$$

NEXT LECTURE

NOVEMBER 11, 2022

THANK YOU FOR YOUR ATTENTION!

БЛАГОДАРЯ ЗА ВНИМАНИЕТО!