Quantum Information and Computing Lecture- 29 : Shor's Algorithm- Method of Continued Fraction

Dipan Kumar Ghosh
Physics Department,
Indian Institute of Technology Powai, Mumbai 400076

August 14, 2016

1 Introduction- Summary of Shor's Algorithm so far

In the last lecture we discussed Shor's algorithm for integer factorization of a large composite number. Today we will discuss how exactly this algorithm is implemented. The essential part of the algorithm is to find period of a function which can be very efficiently done by a quantum computer. We begin by recapitulating the essential points of the algorithm, which are as follows:

1. Take a random number $m < N$ which is co-prime with N.

2. Define a function $f_N : \mathbb{N} \to \mathbb{N}$ such that $f_N(a) = m^a \bmod N$. We need to find the smallest $P \in \mathbb{N}$ such that $m^P = 1 \bmod N$. This is called the period of f_N This step (period finding) requires a quantum computer. If N is large, a classical computer may require $\emptyset(N)$ powers of m while in a quantum computer all powers of m would be simultaneously calculated by the oracle.

3. If P is odd, the method fails and we must return to step 1 to choose a different m and start all over.

4. if P is even, then, we can factorize $m^P - 1$

$$m^P - 1 = (m^{P/2} + 1)(m^{P/2} - 1)$$

Since by definition $m^P = 1 \bmod N$, $m^P - 1 = 0 \bmod N$. If Now, $(m^{P/2} - 1) \neq 0 \bmod N$ because P is the smallest integer which satisfies $m^P - 1 = 0$. If $m^{P/2} + 1 = kN$ for some integer k, then again the problem is not solved and we need to go back to step 1 and select a different m. If, however, $m^{P/2} + 1$ is a not a multiple of N then, $m^{P/2} \pm 1$ must contain factors of N.

5. The challenge is to find P with a high degree of probability of success.

The quantum part of the algorithm is implemented by the following steps:

Assume $N = pq$ with p and q primes. We first find $l \in \mathbb{N}$ such that $N^2 \leq 2^l \leq 2N^2$. We will also denote $Q = 2^l$. (We define a quantum computer with $Q^2 = 2^{2l}$ quits, plus extra quits for work space. The two registers contain vectors of length l

$$\mid Reg_1\rangle \mid Reg_2\rangle = \mid a_{l-1} \ldots a_0\rangle \mid b_{l-1} \ldots b_0\rangle \equiv \mid a\rangle \mid b\rangle$$

where $a = \sum_j 2^j a_j$ and $b = \sum_j 2^j b_j$ any time the state of the computer is given by

$$\mid \psi\rangle = \sum_{a=0}^{Q-1} \sum_{b=0}^{Q-1} C_{ab} \mid a, b\rangle$$

where $C_{ab} \in \mathbb{C}$.

We now follow the following steps.

- Set both the registers to n qubit null states: $\mid \psi_0\rangle = \mid 0\rangle^{\otimes l} \mid 0\rangle^{\otimes l}$.
- Apply QFT on the first register to get

  $$\mid \psi_1\rangle = \frac{1}{\sqrt{Q}} \sum_{x=0}^{Q-1} \mid x\rangle \mid 0\rangle$$

  Since the states are initialized to null, this is done by passing all qubits of the register through Hadamard gates.
- For a randomly chosen m, apply an oracle which calculates $f = m^x \bmod N$. Suppose U_f realizes the action of f on x such that (oracle)

  $$U_f \mid x\rangle \mid 0\rangle = \mid x\rangle \mid f(x)\rangle$$

  This makes the states entangled

  $$U_f \mid \psi_1\rangle = \mid \psi_2\rangle = \frac{1}{\sqrt{Q}} \sum_{x=0}^{Q-1} \mid x\rangle \mid f(x) = m^x \bmod N\rangle$$

- Measure the second register only. The second register, before measurement, was in a linear combination of various possible base states which are obtained by the modular exponentiation. As a result of measurement, it will be found to be in one of the base states $\mid k\rangle$ where k is some power of m mod N. We write

  $$\mid \psi_2\rangle = \frac{1}{\sqrt{M}} \sum_{x \in A} \mid x, k\rangle$$

where A is the set of all $x < Q$ such that $m^x \bmod N$ is k

$$A = \{x_0, x_0 + r, x_0 + 2r + \ldots, x_0 + (M-1)r\}$$

and $M \approx \dfrac{Q}{r} \gg 1$.

The following numerical example with small number will illustrate the steps (1) to (4) above. Let $N = 55$. We have $N^2 = 55^2 = 3025,\ 2N^2 = 6050$. We choose $Q = 2^l$ such that $3025 < Q < 6050$, which gives $l = 12$, yielding $Q = 4096$. Let us choose $m = 13$ (arbitrary number which is co-prime with 55). Various powers of 13 mod 55 are listed below:

$13^1 = 13$	$13^2 = 4$	$13^3 = 52$	$13^4 = 16$	$13^5 = 43$
$13^6 = 9$	$13^7 = 7$	$13^8 = 36$	$13^9 = 28$	$13^{10} = 34$
$13^{11} = 2$	$13^{12} = 26$	$13^{13} = 8$	$13^{14} = 49$	$13^{15} = 32$
$13^{16} = 31$	$13^{17} = 18$	$13^{18} = 14$	$13^{19} = 17$	$13^{20} = 1$

Our initial state, $\mid 000\ldots0, 000\ldots0\rangle \equiv \mid 00\rangle$, after passing the first register through Hadamard gate becomes

$$\mid \psi_1\rangle = \frac{1}{\sqrt{4096}} \left(\mid 0,0\rangle + \mid 1,0\rangle + \ldots + \mid 4095,0\rangle\right)$$

This is now subjected to the oracle which computes the modular exponentiation of 13, as shown in the table above. Note that since $13^{20} = 1$, the second register will repeat with a periodicity of 20. The last state, for instance can be calculated as follows:

$$13^{4095} = 13^{204\times 20+15} \equiv 13^{15} = 32 \mod 55$$

The oracle gives

$$\begin{aligned}\mid \psi_2\rangle = \frac{1}{\sqrt{4096}} \big[&\mid 0,1\rangle + \mid 1,13\rangle + \mid 2, 13^2 \bmod 55 = 4\rangle + \ldots + \mid 20, 13^{20} \equiv 1\rangle \\ &+ \mid 21,13\rangle + \ldots + \mid 204\times 20 = 4080, 1\rangle + \mid 4081, 13\rangle + \ldots \mid 4095, 32\rangle\big]\end{aligned}$$

We now measure the second register. We would then get a random value and we can use any one of the possible values to do our calculation.Suppose this gives the state of the second register to be $\mid 9\rangle$. Looking at the table above, we find that the smallest power of 13 which gives 9 is 6. Thus the same value will be repeated for 26, 46, etc and will end at $4086 = 204 \times 20 + 6$. the state of the system is then

$$\mid \psi_3\rangle \frac{1}{\sqrt{205}} \left[\mid 6,9\rangle + \mid 26,9\rangle + \ldots + \mid 4086,9\rangle\right]$$

(Since the periodicity is 20, there are 205 states with the second register being $\mid 9\rangle$). Quite generally, the state at this stage is

$$\mid \psi_3\rangle = \frac{1}{\sqrt{M}} \sum_{d=0}^{M-1} \mid x_0 + dP, k\rangle$$

where $m^{x+dP} = m^x = k \bmod N$. Clearly P is the period and d is the number of terms within a period. Here M is the number of states in the second register corresponding to a given value in the first register.

- If we now apply QFT on the first register once more on $\mathbb{Z}_Q$, we would get

$$\mid \psi_4\rangle = (U_{QFT}) \otimes I) \mid \psi_2\rangle = \frac{1}{\sqrt{QM}} \sum_{y=0}^{Q-1} e^{2\pi i y x_0/Q} \times [\sum_{d=0}^{M-1} z^d] \mid y, k\rangle$$

where $z = e^{2\pi i y P/Q}$.

- We now measure the first register. It will be in a state $\mid y\rangle$ with a probability $\frac{1}{QM} \mid \sum_{d=0}^{M-1} z^d \mid^2$. The sum over d is done by observing the series to be a geometric one which gives the sum to be

$$\mid \frac{1-z^M}{1-z} \mid^2 = \frac{\sin^2(\pi y P M/Q)}{\sin^2(\pi y P/Q)}$$

If yP/Q is not close to an integer, the powers of z will nearly cancel out, i.e., the probability is small except where $z \approx 1$. If yP/Q is an integer, say n, $\Pr(y) = M/QM = 1/Q$. Thus the observed probability of distribution of y is concentrated around values such that $\frac{y}{Q} \approx \frac{n}{P}$, where n is an integer. In this lecture we will see how we are able to extract the value of P from this measurement.

Let us return to our example to illustrate this last step. We had, after measurement of the second register,

$$\mid \psi_3\rangle = \frac{1}{\sqrt{205}} [\mid 6, 9\rangle + \mid 26, 9\rangle + \ldots + \mid 4096, 9\rangle]$$

On applying Fourier transform to the first register, this becomes

$$\mid \psi_4\rangle = \frac{1}{\sqrt{839680}} \sum_{y=-0}^{4095} e^{2\pi i \times 6y/4096} (\sum_{d=0}^{204} z^d) \mid y, 9\rangle$$

The denominator arose because $839680 = 4096 \times 205$ Recalling that $P = 20$, we have,

$$z = e^{2\pi i \times 20y/4096}$$

The probability of the first register to be in a particular state $\mid y\rangle$ is

$$\frac{1}{839680} \times \mid \sum_{d=0}^{204} z^d \mid^2$$

Suppose our measurement gave the state to be $y = 2048$. We have $z = e^{2\pi i \times 20 \times 2048/8096} = e^{20\pi i} = 1$, so that the probability becomes $(205)^2/839680 \approx 0.05$, i.e. about 5%. There

are 20 states in the second register. The coefficient of each vector becomes sizable when y becomes a multiple of 205. Thus we may infer the period P by repeated measurement. As N becomes large, the number of measurement required becomes large and the method becomes inefficient. In the following we discuss the method of continued fraction, which is more efficient.

2 Method of Continued Fraction

Let us define ceiling and floor functions as

$$\lceil x \rceil = \inf\{n \in \mathbb{Z} \mid x \leq n\}$$

$$\lfloor x \rfloor = \sup\{n \in \mathbb{Z} \mid x \geq n\}$$

For example,

$$\lceil 2 \rceil = 2, \lceil 2.6 \rceil = 3, \lceil -4.5 \rceil = -4, \lceil -5 \rceil = 5$$

Thus the ceiling function evaluates to the nearest integer greater than or equal to the argument of the function. Similarly,

$$\lfloor 4.5 \rfloor = 4, \lfloor 2.6 \rfloor = 2, \lfloor -4.5 \rfloor = -5, \lfloor -5 \rfloor = -5$$

Thus the floor function is the nearest integer less than or equal to the argument of the function. If the argument is positive, the floor function is just the integer part of the argument. Continued function expansion of a rational number is obtained as follows:
Example:

$$\begin{aligned}
\frac{17}{47} &= 0 + \frac{1}{47/17} = 0 + \cfrac{1}{2 + \cfrac{13}{17}} \\
&= 0 + \cfrac{1}{2 + \cfrac{1}{17/13}} = 0 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{13/4}}} \\
&= 0 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{4}}}} \\
&\equiv [0, 2, 1, 3, 4]
\end{aligned}$$

The steps to find the continued fraction are as follows:
1. First find the integral part a_0 of the argument x. In our case the integral part is zero.
2. Find the fractional part by $x - a_0 = r_0$.
3. Find integral part of r_0^{-1}. $\lfloor \frac{1}{r_0} \rfloor = a_1$
4. $r_1 = \frac{1}{r_0} - a_1$ and $a_2 = \lfloor \frac{1}{r_1} \rfloor$
5. Let $m = 1$, we have $a_m = \lfloor \frac{1}{r_{m-1}} \rfloor$ and $r_m = \frac{1}{r_{m-1}} - a_m$. The process is continued till $r_M = 0$. M always turns out to be finite and we get

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\cdots}}}}$$

Given $x = [a_0, a-1, \ldots a_M]$, the expansion in continued fraction $[a_0, a_1, \ldots, a_j]$ with $j \leq M$ is the $j-$th convergent of x is x itself. Suppose we got as a result of measurement of the first register $y/Q = 408/4096$. We can write this as a continued fraction as

$$\begin{aligned}\frac{y}{Q} &= \frac{408}{4096} \\ &= 0 + \cfrac{1}{10 + \cfrac{16}{408}} \\ &= 0 + \cfrac{1}{20 + \cfrac{1}{25 + \cfrac{1}{12}}}\end{aligned}$$

Various convergence are as follows:

$$\frac{1}{20}$$

$$\frac{1}{20 + \cfrac{1}{25}} = \frac{25}{251}$$

$$0 + \cfrac{1}{20 + \cfrac{1}{25 + \cfrac{1}{12}}} = \frac{408}{4096}$$

We stop when the denominator of the approximated fraction exceed the number N; in this case in the first convergent itself, i.e. $r = 10$. The period is then a multiple of 10, which can be 10, 20, 30, 40 or 50. We now calculate a^P for each of these and confirm it to be 20 in this case.