Quantum Information and Computing Lecture- 28 : Implementation of Shor's Algorithm

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

August 14, 2016

1 Introduction

In the last lecture we discussed Shor's algorithm for integer factorization of a large composite number. It was remarked that there are several classical algorithms to do this job though they are not fast enough. The most elementary algorithm is the one due to Euclid which requires of the order of $\sqrt{N}$ operations, as if there exists a factor, one of them has to be less than or equal to $\sqrt{N}$. Euclid algorithm is inefficient for handling large numbers. There are faster classical algorithms, the best among them requiring $\exp\left((\log N)^{1/3}(\log\log N)^{2/3}\right)$ steps, which is still slow. We discussed Shor's algorithm which solves the equivalent problem of finding the period of a number co-prime with the given number N mod N. The essential steps in Shor's algorithm are as follows:

1. Take a random number $m < N$ which is co-prime with N. This may be done by finding the G.C.D. of m, N by some standard algorithm, such as Euclid algorithm and checking if it is equal to 1.

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.

1.1 Implementation of Quantum computation part of the algorithm

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 $Q = 2^l$. (Some authors recommend the size to be taken larger $2N^2 \leq 2^l \leq 3N^2$. The reason for taking the size of the registers to be a power of 2 is to make calculation of quantum Fourier transform easier. 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

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

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.

1. Set both the registers to n qubit null states: $\mid \psi_0\rangle = \mid 0\rangle^{\otimes l} \mid 0\rangle^{\otimes l}$.

2. Apply QFT on the first register to get

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

For instance, if $Q = 2^2 = 4$, we have

$$\mid \psi_1\rangle = \frac{1}{2} [\mid 00, 00\rangle + \mid 01, 00\rangle + \mid 00, 10\rangle + \mid 11, 00\rangle]$$

Since the states are initialized to null, this is done by passing all qubits of the register through Hadamard gates.

3. 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

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

4. 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 mod 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 $13^{20} = 1 \pmod{55}$, 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

$$\mid \psi_2\rangle = \frac{1}{\sqrt{4096}}\left[\mid 0,1\rangle + \mid 1,13\rangle + \mid 2,13^2 \text{mod } 55 = 4\rangle + \ldots + \mid 20,13^{20} \equiv 1\rangle \right.$$
$$\left. + \mid 21,13\rangle + \ldots + \mid 204 \times 20 = 4080,1\rangle + \mid 4081,13\rangle + \ldots \mid 4095,32\rangle\right]$$

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 $m^{x+dP} = m^x = k \mod N$. 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.

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

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

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

6. 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

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

If yr/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 yr/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 $\frac{y}{Q} \approx \frac{n}{r}$, where n is an integer. In the next lecture wewill see how we are able to extract the value of P from this measurement.