Quantum Information and Computing
Topic 13 : Shor's Factorization Algorithm

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

April 14, 2017

1 Introduction

In the last lecture we discussed the implementation of QFT for the case of one, two and three qubits and provided a way to generalize to the case of n qubits. This was an essential component in understanding Shor's algorithm for integer factorization of a large composite number. However, before we discuss the factorization algorithm, it will be appropriate to make a few comments about the problem of factorization in classical computation.

Consider a number $N = pq$ where p and q are large prime numbers, though for the purpose of illustration in this lecture, we will take these numbers to be small so that a back of the envelop calculation can be done. 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. A point which needs to be appreciated is that multiplication of two numbers can be done in polynomial time though the factorization cannot. To get an idea of the difficulty involved consider factorization of a reasonably sized number such as 29803. To factorize this we may use, for instance, Euclid algorithm. If you are manually doing this factorization, you may take a couple of hours doing this. However, if we are told that this number is 229×127, we can check it by doing a multiplication in under a minute. Thus multiplication is easy but factorizaton is hard. It is good to recollect Euclid algorithm, as is taught to us in schools.

Suppose we take two numbers a and b whose greatest common divisor is c. By definition, c divides both a and b, where $a > b$. Let $a = mc$ and $b = nc$, where m and n are integers. When we divide a by b, unless b is a factor of a, a long division of a by b will leave a

remainder. Let $r = a - bq$ be the remainder of such a division. Clearly, since c divides both a and b, it also divides r. Euclid algorithm works like this. We do a long division of a by b. Let $q_1 = \left[\frac{a}{b}\right]$ be the quotient where [ ] is the greatest integer function and let $r_1 = a - bq_1$ be the remainder. We now divide b by this remainder r_1, getting a quotient q_2 and a remainder r_2. We carry on like this till we find a zero remainder at the n-th stage of the algorithm. The last divisor r_n then is the greatest common divisor that we are trying to find. The problem in this method is while this is a reasonably good algorithm to find gcd of two numbers, it is not particularly useful in finding factors of a single number as there is no suitable starting point and we must check numbers from 2 upward up to $\sqrt{N}$. In this lecture we discuss an algorithm due to Peter Shor, which could be implemented using a quantum computer to provide a fast factorization. This is done by solving an equivalent problem of finding a period of a function.

2 Shor's Algorithm

Shor's algorithm for factorizing N has the following steps:

1. Take a random number $m < N$. Calculate G.C.D. of m, N by some standard algorithm, such as Euclid algorithm. If $GCD(m, N) \neq 1$, we have found a factor!. Very unlikely scenario. The number m that we choose is obviously co-prime with N, i.e. m and n have no common factor. We will illustrate by choosing $N = 799$ whose factors are 17 and 47. Choose $m = 7$ whose GCD with 799 is 1.

2. Define a function $f_N : \mathbb{N} \to \mathbb{N}$ such that $f_N(a) = m^a \mod N$. We need to find the smallest $P \in \mathbb{N}$ such that $m^P = 1 \mod N$. This is called the period of f_N This step (period finding) requires a quantum computer. It turns out that $7^{368} = 1 \mod 799$, i.e. $P = 368$..

3. If P is odd, the method fails and we must return to step 1 to choose a different m and start all over. (In the lecture a small number $N = 21$ is used to illustrate, which can be worked out easily. We can choose m to be any number which is co-prime with 21. Thus $m \in \{2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$. Choosing $m = 2$, various powers of 2 are$2^2 = 4, 2^3 = 8, 12^4 = 6, 2^5 = 32, 2^6 = 64$of which the last number 64 is 1 mod 21. Thus in this case P=6).
   Let us consider some results from linear algebra which we will only illustrate here but not prove them (these can be found in any text book on discrete mathematics at college level). Consider a quadratic equation, e.g. $x^2 = 1 \mod N$. Now if N is an odd prime, one can show that this equation only has the trivial solutions, viz., $x = \pm 1$. On the other hand, if N is a composite number, there are non-trivial solutions of the type $x = \pm a$. (Remember we are doing modular arithmetic here which implies that to a we could add kN.)To illustrate consider an example. Consider the equation $x^2 = 1 \mod 41$. This equation only has trivial solutions ± 1.

However consider $N = 55$, in this case $x^2 = 1 \bmod 55$, in addition to having the trivial pair has non trivial solutions $x = \pm 21$ as $x^2 = 441 = 1 \bmod 55$ because $441 = 55 \times 8 + 1$. Since we have, by definition of a period, $m^P = 1 \bmod N$, if we choose $x = m^{P/2}$, this equation would become equivalent to the quadratic equation $x^2 = 1$. In order that we may do it P should be even and we should then choose a different m and repeat the algorithm.

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. One can find the factor by finding the GCD of these two numbers. For the example given, $P = 368$ so that $P/2 = 184$. We then have

$$(7^{184} + 1)(7^{184} - 1) = 799k$$

One can check that the factors are 17 and 47.
As an example which you can work out, let $N = 21$. choose $m = 2$ for which we have seen that $P = 6$ Check that Thus

$$(2^3 + 1)(2^3 - 1) = 21k$$

Thus factors of 21 are contained in 9 and 7. (the factors are 3 and 7).
As yet another example consider $N = 35$. Choose $m = 13$ for which various even powers (mod 35) are $13, 13^2 = 169 \equiv 29, 13^4 = 28561 = 13 \times 816 + 1$ so that in this case $P = 4$. So we get $(13^2 + 1)(13^2 - 1) = 170 \times 168$, the former contains the factor 5 and trhe latter by 7.

We assume that N is not power of some prime for Shor's algorithm fails in this case. (It has been shown that the probabilities of these two things happening is greater than 1/2). it is this order finding part which needs to be done by a quantum computer because such a computer can calculate various powers of m simultaneously.

2.1 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 $2N^2 \leq 2^l \leq 3N^2$. 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

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

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

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

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 $N^2 = 55^2 = 3025$, $2N^2 = 6050$ and $3N^2 = 9075$.

We choose $Q = 2^l$ such that $6050 < Q < 9075$, which gives $l = 13$, yielding $Q = 8192$. Let us choose $m = 13$ (arbitrary nothing to do with the l value which coincidentally was 13). 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

$$\mid \psi_1\rangle = \frac{1}{\sqrt{8192}} (\mid 0,0\rangle + \mid 1,0\rangle + \ldots + \mid 8191,0\rangle)$$

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:

$$13^{8191} = 13^{409\times20+11} \equiv 13^{11} = 2 \mod 55$$

The oracle gives

$$\mid \psi_2\rangle = \frac{1}{\sqrt{8192}} \left[\mid 0,1\rangle + \mid 1,13\rangle + \mid 1,13^2 \mathrm{mod}\ 55\rangle + \ldots + \mid 20,13^{20} \equiv 1\rangle + \mid 21,13\rangle + \ldots + \mid 8191,2\rangle\right]$$

We now measure the second register. Suppose this gives the state of the second register to be $\mid 9\rangle$. Looking at the table above, the state of the system is then

$$\mid \psi_3\rangle \frac{1}{\sqrt{410}} [\mid 6,9\rangle + \mid 26,9\rangle + \ldots + \mid 8186,9\rangle]$$

(Since the periodicity is 20, there are 410 states with the second register being $\mid 9\rangle$. Quite generally, the state at this stage is

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

where $m^{x+dr} = m^x = k \mod N$. Clearly r is the period and d is the number of terms within a period.

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

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

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

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

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

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

$$\mid \psi_3\rangle = \frac{1}{\sqrt{410}} [\mid 6,9\rangle + \mid 26,9\rangle + \ldots + \mid 8186,9\rangle]$$

On applying Fourier transform to the first register, this becomes

$$\mid \psi_4\rangle = \frac{1}{\sqrt{3358720}} \sum_{y=-0}^{8191} e^{2\pi i \times 6y/8192} (\sum_{d=0} z^{409}) \mid y,9\rangle$$

The denominator arose because $3358720 = 8192 \times 410$ Recalling that $r = 20$, we have,

$$z = e^{2\pi i \times 20y/8192}$$

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

$$\frac{1}{3358720} \times \mid \sum_{d=0}^{409} z^d \mid^2$$

Suppose our measurement gave the state to be $y = 4096$. We have $z = e^{2\pi i \times 20 \times 4096/8192} = e^{20\pi i} = 1$, so that the probability becomes $(410)^2/3358720 \approx 0.05$, 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 410. Thus we may infer the period r 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.

3 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 problem 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 the Mth convergent is x itself. Suppose we got as a result of measurement of the first register $y/Q = 409/8192$. We can write this as a continued fraction as

$$\begin{aligned} \frac{y}{Q} &= \frac{409}{8192} \\ &= 0 + \cfrac{1}{20 + \cfrac{12}{409}} \\ &= 0 + \cfrac{1}{20 + \cfrac{1}{34 + \cfrac{1}{12}}} \end{aligned}$$

Various convergence are as follows:

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

$$\frac{1}{20 + \cfrac{1}{34}} = \frac{34}{681}$$

$$\cfrac{1}{20 + \cfrac{1}{34 + \cfrac{1}{12}}} = \frac{409}{8192}$$

We stop when the denominator of the approximated fraction exceed the number N; in this case in the first convergent itself, i.e. $r = 20$.

Suppose, our result of measurement was $\frac{y}{Q} = \frac{4095}{8192}$. The number is represented as $[1, 1, 2, 1638]$. The first convergent is 1, the second is $1/2$, the third is $3/5$ but the fourth is $409/8192$. Thus the approximation that we use is $3/5$, which gives $r_1 = 5$. Possible values of the period r are multiples of 5. We have

a	$13^a \bmod 55$
5	43
10	34
15	32
20	1

which gives the period correctly as 20. The factors are in $(13^{10}+1)(13^{10}-1) = 35 \times 33$. The factors are

$$p = gcd(33, 55) = 11$$

and

$$q = gcd(35, 55) = 5$$