Factoring by Quantum Computers

Ragesh Jaiswal
University of California, San Diego

A *Quantum computer* is a device that uses quantum phenomenon to perform a computation. A classical system follows a single computation path. On the other hand a quantum system utilizes the superposition of input states to simultaneously move along all possible paths and finally move to one definite state when measured. This type of parallelism is exploited to find efficient algorithms for problems that are hard in a classical system. In this paper we will study one such classically hard problem. We will study efficient randomized algorithm for *Integer Factorization* problem for quantum computers.

1. INTRODUCTION

In 1982, Richard P. Feynman observed that a quantum system is exponentially hard to simulate on a classical system. He hypothesized that a quantum computer might be exponentially more powerful than a classical computer. The power of quantum computers was revealed when Peter Shor in 1994 came out with efficient randomized algorithms for Integer Factorization and Discrete Logarithm problem.

In this paper we will look at one of the two problems discussed in Peter Shor's paper. We will consider the *Integer Factorization* problem. The next section contains preliminaries for the quantum phenomenons that would help in understanding the algorithm later. Section 3 defines the problem and gives the algorithm. Section 4 gives some of the follow up work.

2. PRELIMINARIES

2.1 Qubit

A *qubit* is a 2 state quantum system with probability amplitudes of occurring in either of the states. The system is said to be in superposition of these two states. We denote these two basis states by $|0>$ and $|1>$. If the probability amplitudes are α and β then the state of the system is denoted by $\alpha|0> + \beta|1> (\alpha, \beta \in C)$. The probability of the system being in state $|0>$ is $|\alpha|^2$ and in state $\|1>$ is $|\beta|^2$ when measured. Therefore $|\alpha|^2 + |\beta|^2 = 1$.

2.2 Multiple Qubits and Measurement

Suppose we have a 2 qubit system, we will have 4 basis states $00, 01, 10, 11$. The quantum state of this 2 qubit system will then be represented by the vector:

$$|\psi> = \alpha_{00}|00> + \alpha_{01}|01> + \alpha_{10}|10> + \alpha_{11}|11> \quad (1)$$

where $\sum_{x=\{0,1\}^2} |\alpha_x|^2 = 1$. α's are the probability amplitudes. The quantum state of multiple qubit system with the qubits in the quantum state ψ_1, ψ_2, ..., ψ_m can be found by taking the tensor product, $|\psi> = |\psi_1> \otimes |\psi_2> ... \otimes |\psi_m>$.

If measurement of only the first bit is made in the 2 qubit system, the post-measurement quantum state would be the superposition of all the states(present in pre-measurement) which have the first bit same as measured, normalized to have unit length. For example consider equation 1, if the first bit is measured to be in state 0, then the post-measurement state would be:

$$|\psi' >= \frac{\alpha_{00}|00> +\alpha_{01}|01>}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}} \tag{2}$$

2.3 Quantum Gates

Quantum gates are simple transformations that can be applied to qubits(linear transformations to quantum vector state). Any change in the quantum state can be modeled by a quantum circuit consisting of wires and quantum gates. For example consider the following single qubit gate which flips the probability amplitudes.

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix} = \begin{pmatrix} \alpha_2 \\ \alpha_1 \end{pmatrix}$$

The following CNOT gate represents a 2 qubit gate(input and outputs both are 2 qubits). Classically it basically outputs the first bit as it is, and flips the second bit if the first input bit was 1. The transformation matrix for the CNOT gate is:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Note that both the above gates are reversible, which is in fact true for all quantum gates.

2.4 Reversible Computation

Since $\sum_{x=\{0,1\}^n} |\alpha_x|^2 = 1$ for any n-qubit quantum state, the transformation that can be applied to a quantum state are unitary. It can be shown that any linear transformation U, is unitary iff $U^{-1} = U^c$. This implies that a quantum gate is essentially reversible, making quantum computation reversible.

2.5 Quantum Fourier Transforms

A quantum Fourier transform is basically a unitary transformation which is defined as:

$$|a > \longrightarrow_{FT_{Z_q}} \frac{1}{q^{1/2}} \sum_{c=0}^{q-1} \omega^{ca}|c > \tag{3}$$

$|a>$ is basis state, $0 \leq a < q$ for some q, and ω is the qth root of unity.

Some observations about ω that will be helpful later are:

$$1 + \omega^j + \omega^{2j} + \omega^{3j} + ... + \omega^{(q-1)j} = 0 \; if \; j \neq 0 \; (mod \; q) \tag{4}$$

$$1 + \omega^j + \omega^{2j} + \omega^{3j} + ... + \omega^{(q-1)j} = q \; if \; j = 0 \; (mod \; q) \tag{5}$$

[3] gives a quantum circuit that gives the quantum fourier transform in time polynomial in the number of qubits.

3. INTEGER FACTORIZATION

3.1 Problem

Given an odd composite N, find N_1 such that $N_1 \neq 1$ and $N_1|N$
The best known classical randomized algorithm for this problem is sub-exponential ($2^{(logN)^{1/3}}$). The quantum algorithm presented runs in polynomial number of steps.

3.2 Basic Idea and Number Theory

Given N, consider the multiplicative group $< Z_N^*, . >$. Let r be the order of any randomly chosen element $x \in Z_N^*$. We have:

$$x^r - 1 = 0 \pmod N$$
$$\Rightarrow (x^{r/2} - 1)(x^{r/2} + 1) = 0 \pmod N$$

Note that $x^{r/2} - 1 \neq 0 \pmod N$ when r is even(else it becomes the order of x). So if r is not odd and $x^{r/2} + 1 \neq 0 \pmod N$, we can compute a non-trivial factor of N by finding $gcd(x^{r/2} - 1, N)$. This can be done in linear lime. We will now show that for randomly chosen x there is a high probability that these two properties hold.

Let $N = \prod_{i=1}^{k} p_i^{\alpha_i}$, p_i's are the odd prime factors of N. Let r_i be the order of element $x \pmod{p_i^{\alpha_i}}$

Fact 1: $r = LCM(r_1, r_2, ..., r_k)$.

Claim 1: The algorithm fails if and only if the largest powers of 2 dividing the r_i's are the same.(Note that the algorithm fails iff r is odd or $x^{r/2} + 1 = 0\ (mod\ N)$)
proof: Let $r_i = 2^{l_i} * q_i$, q_i is odd.
($\Rightarrow$)
Case 1: $l_i = 0, \forall i : 1 \leq i \leq k$
In this case r is odd, so the algorithm fails.

Case 2: $l_i = c, \forall i : 1 \leq i \leq k$
In this case $r = 2^c * t$, t is odd.
For any j we will have:
$x^{r/2} - 1 \pmod{p_j^{\alpha_j}} = x^{2^{c-1}t} - 1 \pmod{p_j^{\alpha_j}}$

The RHS is $0 \pmod{p_j^{\alpha_j}}$ iff $2^{c-1}t = 0 \pmod{2^c * q_j}$ which is not possible. Now, since p_j is an odd prime we will have

$$x^{r/2} + 1 = 0\ (mod\ p_j^{\alpha_j}) \tag{6}$$

From Chinese remaindering theorem [1] we get $x^{r/2} + 1 = 0 \pmod N$ {since 6 is true for all j}. So the algorithm fails.

($\Leftarrow$)
Now suppose the powers are not the same.

Let $LCM(r_1, r_2, ..., r_k) = 2^m * k$, where $m = max(l_i)$, k is odd.
Now consider a j such that $l_j < m$ (Note that such a j exists from our assumption).
We have:
$r = 2^{m-l_j} * 2^{l_j} * q_j * t$, t is odd, $m - l_j > 0$

Therefore,
$x^{r/2} - 1 \pmod{p_j^{\alpha_j}}$
$= x^{2^{l_j} 2^{m-l_j-1} q_j t} \pmod{p_j^{\alpha_j}}$
$= (x^{2^{l_j} q_j})^{t 2^{m-l_j-1}}$ - 1 $\pmod{p_j^{\alpha_j}}$
$= (x^{r_j})^{(\cdots)}$ - 1 $\pmod{p_j^{\alpha_j}}$
$= 0 \pmod{p_j^{\alpha_j}}$\{since r_j is the order of $x \ mod \ p_j^{\alpha_j}$\}

$\Rightarrow x^{r/2} + 1 \neq 0 \pmod{p_j^{\alpha_j}}$\{since p_j is an odd prime\}
$\Rightarrow x^{r/2} + 1 \neq 0 \pmod{N}$ [From Chinese Remaindering Theorem [1]]
So the algorithm succeeds.
(proved)

Choosing a random $x \pmod{N}$ is same as choosing for each i a random number$x_i \pmod{p_i^{\alpha_i}}$. Now $< Z_{p^\alpha}^*, . >$ is a cyclicgroup for any prime power p^α, so for any $p_i^{\alpha_i}$ the probability of choosing an x_i such that the largest power of 2 that divides its order is the same as that for $p_{i-1}^{\alpha_{i-1}}$ is 1/2. Therefore the probability that our choice of x would fail is $1 - 1/2^{k-1}$ which is reasonably small.

3.3 Simple Case

Let us consider a simple case to understand the basic techniques of quantum algorithms. We start with two quantum registers in the initial state $|0> |0>$. We will take fourier transforms over Z_q. In the simple case we assume $r|q$.
We apply fourier transform to the first register to get a uniform superposition of states.

$$|0> |0> \longrightarrow_{FT_{Z_q}} 1/\sqrt{q} \sum_{a \in Z_q} |a> |0> \tag{7}$$

We then apply modular exponentiation to get the state:

$$1/\sqrt{q} \sum_{a \in Z_q} |a> |x^a \ (mod \ n)> \tag{8}$$

At this point we observe the second register. Suppose the state observed is $x^k \ (mod \, n)$. The post-measurement of the system would be:

$$\frac{1}{\sqrt{q}} \frac{1}{\sqrt{q/r}} \sum_{\forall b \in Z_q, st \ x^b = x^k \ mod \ n} |b> |x^k \ mod \ n> \tag{9}$$

since r is the order of $x \ mod \ n$, $b = lr + k \ 0 \leq l < q/r$. So we have:

$$\frac{\sqrt{r}}{q} \sum_{l=0}^{q/r} |lr + k> |x^k \ mod \ n> \tag{10}$$

Now we again apply fourier transform to the first register to get.

$$\frac{\sqrt{r}}{q}\sum_{l=0}^{q/r}\sum_{u\in Z_q}\omega^{(lr+k)u}|u>|x^k \ mod\ n> \tag{11}$$

$$or, \frac{\sqrt{r}}{q}\sum_{u\in Z_q}\omega^{ku}\sum_{l=0}^{q/r}(\omega^r)^{lu}\ |u>|x^k \ mod\ n> \tag{12}$$

Now ω^r is the q/rth root of unity. From equations 4 and 5 we get that the amplitudes of all states except those where $u = 0\ mod\ q/r$, cancel out. Only terms with $u = 0\ mod\ q/r$ remain. So we get the state:

$$\frac{\sqrt{r}}{q}\frac{q}{r}\sum_{l=0}^{r-1}|l\frac{q}{r}> \tag{13}$$

We get uniform superposition of all states that are multiples of q/r. With high probability $gcd(l, \frac{q}{r}) = 1$, in such a case $gcd(q, l\frac{q}{r}) = \frac{q}{r}$. So with high probability we get r by dividing q by $gcd(q, l\frac{q}{r})$.

To get a better idea let us try to intuitively understand equation 11 which is the most important step. In this step we are, in some sense, taking a discrete fourier transform over Z_q, on the general function $f : Z_q \rightarrow C$, which in this case:

$$f(x) = constant, 0 \leq x < q, x = lr + k\ and \tag{14}$$

$$f(x) = 0, otherwise. \tag{15}$$

Now f is a periodic function with a period of r. This implies that in the transformed domain the peaks will occur at multiples of q/r (analogous to frequency in signal processing). Which means that states which are multiples of q/r would occur with high, uniform probability which is exactly what we get in equation 13.

3.4 General Case

Now that we are familiar with the techniques used in quantum computing we can go to the general case when we drop the assumption that $r|q$. The initial steps of the algorithm until equation 10 remain the same. We start with:

$$\frac{\sqrt{r}}{q}\sum_{l=0}^{\lfloor q/r\rfloor}|lr + k>|x^k \ mod\ n> \tag{16}$$

Applying fourier transform to the first register we get:

$$\frac{\sqrt{r}}{q}\sum_{u\in Z_q}\omega^{ku}\sum_{l=0}^{\lfloor q/r\rfloor}(\omega^{ru})^l\ |u>|x^k \ mod\ n> \tag{17}$$

If $ru\ mod\ q$ is small, the summation $\sum_{l=0}^{\lfloor q/r\rfloor}(\omega^{ru})^l$ (for certain u) covers a small angle in the complex plane, so there is a constructive interference for such u. On the other hand if $ru\ mod\ q$ is large the summation will be distributed evenly around

the unit circle and the terms will cancel out, reducing the chances of occurrence of such u. We will analyze a specific case of small $ru \ mod \ q$ to get the value of r. Let:

$$-r/2 \leq ru \ mod \ q \leq r/2 \tag{18}$$

Note that in this case the summation covers only half of the unit circle. Now, for some l:

$$-r/2 \leq ru - lq \leq r/2 \tag{19}$$

Dividing the inequality by rq:

$$|\frac{u}{q} - \frac{l}{r}| \leq \frac{1}{2q} \tag{20}$$

If we chose $q > N^2$ then there is at most one value of $\frac{l}{r}$ satisfying the above inequality. The denominator of $\frac{l}{r}$ is less than N. The difference of two fractions with their denominators at most N can be at least N^2. So we can get the value of $\frac{l}{r}$ by continued fraction expansion of $\frac{u}{q}$ until the denominator is less than$N$.

Now what remains to show is that the case $-r/2 \leq ru \ mod \ q \leq r/2$ occurs with reasonably high probability. [3] presents a detailed analysis to compute the probability with a small error. Here we will look at a coarser analysis given in [4] which serves our purpose.

The summation $\sum_{l=0}^{\lfloor q/r \rfloor}(\omega^{ru})^l$ is distributed uniformly over half of the unit circle in the complex plane. This implies that at least half of the terms in the summation make less than 45^o with the resulting complex number. Each of these terms make a contribution of at least $\frac{1}{\sqrt{2}}$ to the sum. So the probability amplitude $|\alpha_u| \leq \frac{\sqrt{r}}{q}\frac{q}{r}\frac{1}{2}\frac{1}{\sqrt{2}} = \frac{1}{\sqrt{r}}\frac{1}{2\sqrt{2}}$. So such a u will be observed with a probability, at least $1/8r$ which is a constant.

4. FOLLOW UP WORK

At present Quantum Computing remains in its pioneering stage. Error correction, decoherence and possible hardware architecture are the obstacles in coming up with a quantum computer. Quantum error correction proposed in 1995 increased the possibility of such systems. Presently work is in progress in realizing a quantum computer using NMR techniques.

[2] gives a comprehensive coverage on the developments in Quantum theory. There have been interesting developments in the theory of quantum computing after Shor's work. In 1996, Grover gave a quadratic speed-up quantum search algorithm. The limits of quantum computers was explored by Bennet, Bernstein, Brassard and Vazirani who showed that quantum computation cannot speed up search by more than a quadratic factor and that, relative to a random oracle, quantum computers cannot solve NP-complete problems. The class BQNP, the quantum analog of NP was studied by Kitaev and he showed that QSAT(quantum analog of satisfiability) is complete for the class. Watrous showed that the class IP (Interactive proofs with polynomially number of rounds) can be simulated with only three rounds of communication. Burhman, Cleve and Wigderson showed how two parties could decide set disjointness by communicating only square root n quantum bits. There

has also been good amount of work in Quantum Information Theory and Quantum Cryptography.

REFERENCES

A. Cormen, P. Leiserson, and R. Rivest. *Introduction to Algorithms*. Prentice Hall, 2nd edition, 1999.

G. Doolen and B. Whaley. Theory component of the quantum information processing and quantum computing roadmap, part 1, section 6.8. Produced for the Advanced Research and Development Activity(ARDA), December 2002.

Peter W. Shor. Algorithms for quantum computation: discrete logarithm and factoring. pages 124–134. Proceedings of the 35thAnnual Symposium on the Foundations of Computer Science(FOCS94), (IEEE Computer Society Press, Los Alamitos, California, USA, 1994).

U. Vazirani. Lecture notes for course on quantum computing, Fall 1997.