On the Complexity of Shor's Algorithm for Factorization

Zhengjun Cao
Department of Mathematics, Shanghai University
Departement D'informatique,
Université Libre de Bruxelles, Belgium
zhencao@ulb.ac.be or caozhj@yahoo.cn

Lihua Liu
Department of Mathematics,
Shanghai Maritime University.

Abstract

The complexity analysis of Shor's quantum algorithm for factorization consists of:

1) The probability p that we see any particular state$|c, x^k \,(mod\, n)\rangle$ with $\{rc\}_q \leq r/2$ is at least $\frac{1}{3r^2}$.

2) There are $\phi(r)$ possible values of c, and r possible values of $x^k \,(mod\, n)$.

3) The success probability is at least $\phi(r) \cdot r \cdot \frac{1}{3r^2}$.

That is, the inventor views p as the joint probability $P(X = c, Y = x^k \,(mod\, n))$. In this paper, we show that the argument for the estimation of $P(X = c, Y = x^k \,(mod\, n))$ is not sound. Therefore, the problem that Shor's algorithm takes polynomial time remains open.

Keywords *factorization, Shor's algorithm, quantum register*

1 Introduction

Shor's algorithm for factorization [15] uses two quantum registers. An observer has to measure the final quantum state [12] in the first register and interpret the measurement result as a scalar c. The complexity analysis of Shor's algorithm for factorization consists of:

1) The probability p that we see any particular state$|c, x^k \,(\mathrm{mod}\, n)\rangle$ with $\{rc\}_q \leq r/2$ is at least $\frac{1}{3r^2}$.

2) There are $\phi(r)$ possible values of c, and r possible values of $x^k \,(\mathrm{mod}\, n)$.

3) The success probability is at least $\phi(r) \cdot r \cdot \frac{1}{3r^2}$, namely, $\frac{\phi(r)}{3r}$.

According to the third part, we know the inventor views the probability p as the joint probability $P(X = c, Y = x^k \,(\mathrm{mod}\, n))$, where $\{rc\}_q \leq r/2$, the random variables X and Y take values from $\{0, 1, \cdots, q-1\}$, $\{1, x, \cdots, x^{r-1} \,(\mathrm{mod}\, n)\}$, respectively. (From now on, for convenience we will omit the notation $\mathrm{mod}\, n$.)

In this paper, we show that the argument for the joint probability $P(X = c, Y = x^k)$ is not sound. Our method is to introduce another quantum register. Using the Shor's argument for the estimation of p, we can obtain the estimation for the probability $P(X = c, Y = x^k, Z = x^k)$ seeing any state$|c, x^k, x^k\rangle$ with $\{rc\}_q \leq r/2$. It is easy to show that,

$$P(X = c, Y = x^k, Z = x^k) = P(X = c, Y = x^k)$$

Since the observed values in the second register and the third register are random, the probability

$$P(X = c, Y = x^k, Z = x^l)$$

seeing any state$|c, x^k, x^l\rangle$ with $\{rc\}_q \leq r/2$ and any $k, l \in \{0, \cdots, r-1\}, k \neq l$, is greater strictly than

$$P(X = c, Y = x^k, Z = x^k)$$

Hence,

$$\begin{aligned} P(X = c, Y = x^k, Z = x^l) &> P(X = c, Y = x^k, Z = x^k) \\ &= P(X = c, Y = x^k) \end{aligned}$$

But

$$\begin{aligned} & P(X = c, Y = x^k, Z = x^l) \\ = \;& P(X = c, Y = x^k) \cdot P(Z = x^l | \{X = c, Y = x^k\}) \\ \leq \;& P(X = c, Y = x^k) \end{aligned}$$

where $P(Z = x^l | \{X = c, Y = x^k\})$ is the conditional probability. It leads to a contradiction. This shows that Shor's argument for the estimation of success probability ($\geq \phi(r)/3r$) is not sound. Therefore, the problem that Shor's algorithm takes polynomial time remains open.

978-0-7695-3991-1/09 $26.00 © 2009 IEEE
DOI 10.1109/ISISE.2009.86

2 Shor's algorithm and its complexity

2.1 Review of Shor's algorithm

The algorithm aims to find the order of $x \pmod n$ on a quantum computer because factorization can be reduced to finding the order of an element [9]. It uses two quantum registers.

Given x and n, to find the order of x, i.e., the least r such that $x^r \equiv 1 \pmod n$, we do the following. First, we find q, the power of 2 with $n^2 \leq q < 2n^2$. Next, we put the first register in the uniform superposition of states representing numbers $a \pmod q$. This leaves the machine in the state

$$\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle|0\rangle$$

Next, we compute x^a in the second register. Since we keep a in the first register, this can be done reversibly. This leaves the machine in the state

$$\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle|x^a\rangle$$

We perform the Fourier transform on the first register [1, 3, 10, 11, 18]. This leaves the machine in the state

$$\frac{1}{q} \sum_{a=0}^{q-1} \sum_{c=0}^{q-1} \exp(2\pi iac/q)|c\rangle|x^a\rangle$$

Finally, we observe the machine. *It would be sufficient to observe solely the value of $|c\rangle$ in the first register, but for clarity we will assume that we observe both $|c\rangle$ and $|x^a\rangle$.* We now compute the probability that our machine ends in a particular state $|c, x^k\rangle$, where we may assume $0 \leq k < r$. Summing over all possible ways to reach the state $|c, x^k\rangle$, we find that this probability is

$$\left| \frac{1}{q} \sum_{a:\, x^a \equiv x^k} \exp(2\pi iac/q) \right|^2 \tag{1}$$

where the sum is over all $a, 0 \leq a < q$, such that $x^a \equiv x^k$.

The probability seeing a particular state $|c, x^k\rangle$ will be at least $1/3r^2$ if there is a d such that

$$\frac{-r}{2} \leq rc - dq \leq \frac{r}{2}$$

Dividing by rq and rearranging the terms gives

$$\left| \frac{c}{q} - \frac{d}{r} \right| \leq \frac{1}{2q}$$

We know c and q. Because $q > n^2$, there is at most one fraction d/r with $r < n$ that satisfies the above inequality. Thus, we can obtain the fraction d/r in lowest terms by rounding c/q to the nearest fraction having a denominator smaller than n.

2.2 Review of its complexity argument

The sum in Eq.(1) is over all a satisfying $a \equiv k \pmod r$ because the order of x is r. Writing $a = br + k$, we find that the probability is

$$\left| \frac{1}{q} \sum_{b=0}^{\lfloor (q-k-1)/r \rfloor} \exp(2\pi i(br + k)c/q) \right|^2$$

We can ignore the term of $\exp(2\pi ikc/q)$, as it can be factored out of the sum and has magnitude 1. We can also replace rc with $\{rc\}_q$, where $\{rc\}_q$ is the residue which is congruent to $rc \pmod q$ and is in the range $-q/2 < \{rc\}_q \leq q/2$. This leaves us with the expression

$$\left| \frac{1}{q} \sum_{b=0}^{\lfloor (q-k-1)/r \rfloor} \exp(2\pi ib\{rc\}_q/q) \right|^2$$

We will now show that if $\{rc\}_q$ is small enough, all the amplitudes in this sum will be in nearly the same direction (i.e., have close to the same phase), and thus make the sum large. Turning the sum into an integral, we obtain

$$\begin{aligned} & \frac{1}{q} \int_{b=0}^{\lfloor \frac{(q-k-1)}{r} \rfloor} \exp(2\pi ib\{rc\}_q/q) db \\ + \quad & O\left(\frac{\lfloor (q-k-1)/r \rfloor}{q} (\exp(2\pi i\{rc\}_q/q) - 1) \right) \end{aligned}$$

If $|\{rc\}_q| \leq r/2$, the error term in the above expression is easily seen to be bounded by $O(1/q)$. We now show that if $|\{rc\}_q| \leq r/2$, the above integral is large, so the probability of obtaining a state $|c, x^k (\mathrm{mod}\, n)\rangle$ is large. *Note that this condition depends only on c and is independent of k.* Substituting $u = rb/q$ in the above integral, we get

$$\frac{1}{r} \int_0^{\frac{r}{q} \lfloor \frac{q-k-1}{r} \rfloor} \exp\left(2\pi i \frac{\{rc\}_q}{r} u \right) du$$

Since $k < r$, approximating the upper limit of integration by 1 results in only a $O(1/q)$ error in the above expression. If we do this, we obtain the integral

$$\frac{1}{r} \int_0^1 \exp\left(2\pi i \frac{\{rc\}_q}{r} u \right) du$$

Letting $\{rc\}_q/r$ vary between $-\frac{1}{2}$ and $\frac{1}{2}$, the absolute magnitude of the integral is easily seen to be minimized when $\{rc\}_q/r = \pm\frac{1}{2}$, in which case the absolute value of the expression is $2/(\pi r)$. The square of this quantity is a lower bound on the probability that we see any particular state $|c, x^k \pmod n\rangle$ with $\{rc\}q \leq r/2$; this probability is thus asymptotically bounded below by $4/(\pi^2 r^2)$, and so is at least $1/3r^2$ for sufficiently large n.

We now count the number of states $|c, x^k \pmod n\rangle$ which enable us to compute r. There are $\phi(r)$ possible values of d relatively prime to r, where ϕ is Euler's totient function [4, 5]. There are also r possible values for x^k, since r is the order of x. Thus, there are $r\phi(r)$ states $|c, x^k \pmod n\rangle$ which would enable us to obtain r. Since each of these states occurs with probability at least $1/3r^2$, we obtain r with probability at least $\phi(r)/3r$. Using the theorem that $\phi(r)/r > \delta/\log\log r$ for some constant δ, this shows that we find r at least a $\delta/\log\log r$ fraction of the time, so by repeating this experiment only $O(\log\log r)$ times, we are assured of a high probability of success. In a word, the complexity analysis of the algorithm can be depicted as following Graph-1.

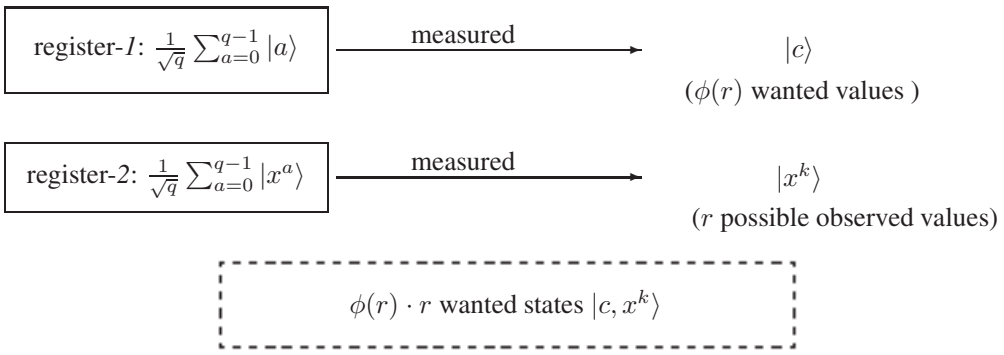
use the same analysis of Shor's argument to estimate the probability seeing a particular state $|c, x^k, x^k\rangle$.

We now consider the variation of Shor's algorithm using three quantum registers. Similarly, we put the first register in the uniform superposition of states representing numbers $a \pmod q$. This leaves the machine in the state

$$\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle|0\rangle|0\rangle$$

Next, we compute $x^a \pmod n$ in the second and the third registers. This leaves the machine in the state

$$\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle|x^a\rangle|x^a\rangle$$



Graph-1: Two quantum registers for Shor's algorithm

3 The argument for the joint probability is not sound

It seems that it is difficult to mathematically verify the Shor's argument for the complexity analysis, because it involves the correlation of the observed values from the first quantum register and the second quantum register. We are not sure that whether the observed value c in the first register is independent of the observed value $x^k \pmod n$ in the second register. All these literatures [2, 6, 7, 8, 13, 14, 16, 17] relate to the Shor's algorithm. But none of them investigates the correlation of two quantum registers.

From the Shor's complexity argument, we know the inventor views $1/3r^2$ as the lower bound to the joint probability $P(X = c, Y = x^k)$, where $\{rc\}_q \leq r/2$, the random variables X and Y take values from $\{0, 1, \cdots, q-1\}$, $\{1, x, \cdots, x^{r-1} \pmod n\}$, respectively. However, by the Eq.(1), it seems reasonable to view it as the lower bound to the conditional probability $P(X = c \,|\, Y = x^k)$.

In what follows, we will show that the Eq.(1) can not be viewed as the joint probability $P(X = c, Y = x^k)$. Our method is to introduce another quantum register. We then

We perform the Fourier transform on the first register. This leaves the machine in the state

$$\frac{1}{q} \sum_{a=0}^{q-1} \sum_{c=0}^{q-1} \exp(2\pi iac/q)|c\rangle|x^a\rangle|x^a\rangle$$

Finally, we observe the machine. We now compute the probability that our machine ends in a particular state $|c, x^k, x^k\rangle$, where we assume $0 \leq k < r$. Summing over all possible ways to reach the state $|c, x^k, x^k\rangle$, we find that this probability is

$$\left| \frac{1}{q} \sum_{a:\, x^a \equiv x^k} \exp(2\pi iac/q) \right|^2 \qquad (1')$$

where the sum is over all $a, 0 \leq a < q$, such that $x^a \equiv x^k \pmod n$.

Notice that the Eq.(1') is identical to Eq.(1). Thus the remainder argument for the joint probability $P(X = c, Y = x^k, Z = x^k)$ is exactly the same as that Shor's argument for the joint probability $P(X = c, Y = x^k)$, where

$\{rc\}_q \leq r/2$, the random variables X and Y, Z take values from $\{0, 1, \cdots, q-1\}$, $\{1, x, \cdots, x^{r-1}\}$, respectively. Therefore, we have

$$P(X = c, Y = x^k, Z = x^k) = P(X = c, Y = x^k)$$

Since the observed values in the second register and the third register are random, the probability

$$P(X = c, Y = x^k, Z = x^l)$$

seeing any state$|c, x^k, x^l\rangle$ with $\{rc\}_q \leq r/2$ and any $k, l \in \{0, \cdots, r-1\}, k \neq l$, is greater strictly than

$$P(X = c, Y = x^k, Z = x^k)$$

Hence,

$$\begin{aligned} & P(X = c, Y = x^k, Z = x^l) \\ > \quad & P(X = c, Y = x^k, Z = x^k) = P(X = c, Y = x^k) \end{aligned}$$

But

$$\begin{aligned} & P(X = c, Y = x^k, Z = x^l) \\ = \quad & P(X = c, Y = x^k) \cdot P(Z = x^l | \{X = c, Y = x^k\}) \\ \leq \quad & P(X = c, Y = x^k) \end{aligned}$$

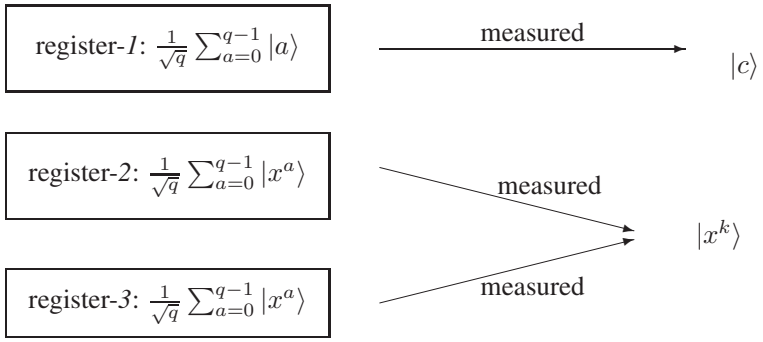
where $P(Z = x^l | \{X = c, Y = x^k\})$ is the conditional probability. It leads to a contradiction. This shows that Shor's argument for the estimation of success probability ($\geq \phi(r)/3r$) is not sound.

He also stresses that the condition $\{rc\}_q \leq r/2$ depends only on c and is independent of k. According to his remarks and his analysis, it seems that the observation about the second register has no relation to the observation about the first register.

But in the calculation of $\phi(r) \cdot r \cdot \frac{1}{3r^2}$, he has to use the fact that there are r possible values of $x^k \pmod n$ in the second register. Moreover, the Eq.(1) is directly defined on x^k. Taking into account these facts, we think, the probability represented by Eq.(1) should be viewed as the conditional probability $P(X = c \,|\, Y = x^k)$, instead of the joint probability $P(X = c, Y = x^k)$.

One might argue that the observed values in the second register and the third register should be identical. That means one can not see the particular state $|c, x^k, x^l\rangle, k \neq l$. The machine always ends in the particular state $|c, x^k, x^k\rangle$. Regretfully, it is false because there are r possible observed values for the second register and the third register, respectively, according to the Shor's argument. To understand this best, we only need to investigate the following case (depicted as Graph-2), where 3 quantum registers are used for Shor's algorithm.

On the one hand, one admits that there are r possible observed values $|1\rangle, \cdots, |x^{r-1}\rangle$ for the second register. On the other hand, one claims that there is only one possible observed value $|x^k\rangle$ for two registers with the same premeasurement state $\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |x^a\rangle$. Obviously, it is a contradiction.



Graph-2: Three quantum registers for Shor's algorithm

4 Further discussion

P. Shor had ever pointed out that:

> "it would be sufficient to observe solely the value of $|c\rangle$ in the first register, but for clarity we will assume that we observe both $|c\rangle$ and $|x^a \pmod n\rangle$."

5 Conclusion

In this letter, we investigate the variation of Shor's algorithm for factorization which uses three quantum registers. The result shows that Shor's complexity analysis is not

sound. Thus the problem that Shor's algorithm takes polynomial time remains open.

Acknowledgement We thank professor Olivier Markowitch, Dr. Evgueni Karpov and Dr. Thomas Durt for discussions. We acknowledge the Cryptasc Project (Institute for the Encouragement of Scientific Research and Innovation of Brussels), the National Natural Science Foundation of China (Project 60873227), the Shanghai Leading Academic Discipline Project (S30104) and the Innovation Program of the Shanghai Municipal Education Commission.

References

[1] E. Bernstein and U. Vazirani, Quantum complexity theory, SIAM Journal on Computing, 26 (5), 1411-1473 (1997)

[2] A. Fowler, S. Devitt, and L. Hollenberg, Implementation of Shor's Algorithm on a Linear Nearest Neighbour Qubit Array, Quant. Info. Comput. 4, 237-251 (2004)

[3] I. Hiroshi and H. Masahito, Quantum Computation and Information, Springer (2006)

[4] G. Hardy and E. Wright, An Introduction to the Theory of Numbers, Fifth ed., Oxford University Press, New York, 1979.

[5] D. Knuth, The Art of Computer Programming, Vol. 2: Seminumerical Algorithms, Second ed., Addison-Wesley, 1981

[6] V. Kendon and W. Munro, Entanglement and its Role in Shor's Algorithm, Quantum Information and Computation, 6 (7) pp. 630-640 (2006)

[7] B. Lanyon et al., Experimental Demonstration of a Compiled Version of Shor's Algorithm with Quantum Entanglement, Phys. Rev. Lett 99 (2007)

[8] CY Lu, D. Browne, T. Yang, and JW Pan, Demonstration of Shor's quantum factoring algorithm using photonic qubits, Phys. Rev. Lett 99 (2007)

[9] G. Miller, Riemann's hypothesis and tests for primality, J. Comput. System Sci., 13, pp. 300-317. (1976)

[10] R. Meter and K. Itoh, Fast quantum modular exponentiation, Phys. Rev. A 71, 052320 (2005)

[11] M. Nielsen and I. Chuang, Quantum Computation and Quantum Information, Cambridge University Press (2000)

[12] A. Peres, Quantum Theory: Concepts and Methods, Kluwer Academic Publishers (1993)

[13] P. Shor, Why haven't more quantum algorithms been found, Journal of the ACM, Vol. 50, 1 (January), pp. 87-90 (2003)

[14] P. Shor, Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, SIAM Review, Vol. 41, No. 2 (Jun.) pp. 303-332 (1999)

[15] P. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. arxiv.org/abs/quant-ph/9508027v2 This preprint was eventually published as SIAM J.Sci.Statist.Comput. 26 (1997)

[16] Y. Shimoni, D. Shapira, and O. Biham, Entangled quantum states generated by Shor's factoring algorithm, Phys. Rev. A 72, 062308 (2005)

[17] LF. Wei, X. Li, XD Hu, and F. Nori, Effects of dynamical phases in Shor's factoring algorithm with operational delays, Phys. Rev. A 71, 022317 (2005)

[18] N. Yoran and A. Short, Efficient classical simulation of the approximate quantum Fourier transform, Phys. Rev. A 76, 042321 (2007)