2007 International Conference on Computational Intelligence and Security

A Period-finding Method for Shor's Algorithm

Weiqiang Zhang Chen Xu Feipeng Li Jiqiang Feng
Institute of Intelligent Computing Science
Shenzhen University Shenzhen China
weiqiangzhangchina@yahoo.com.cn

Abstract

Shor's algorithm is a significant quantum algorithm for factoring a number N. The key technique of the Shor's algorithm is turning the factoring problem into the problem of finding the period of a function. Based on the key technique and the monotony of the mode function, an approach how to determine the period of a function is introduced. Meanwhile an important parameter selection for period-finding is optimized. Several experiments discussed imply that the approach and the parameter selection are both rigorous.

1. Introduction

How to develop high-powered computation becomes a key issue in signal processing domain. One way is to enhance the performance of microprocessor. The other way is improving the computer model and algorithm design through which the problem can be solved more essentially. The most development of quantum computing is in the parallel quantum algorithm, which is a product of quantum physics and algorithm theory. The essential character of the parallel quantum algorithm is based on the quantum superposition, quantum coherence and the quantum entanglement of qubits [1].

Given a fixed large number, it is more difficult to factor it into two numbers using the classical algorithm. That is the mechanism of the public key cryptography, such as RSA that uses a public key N, the product of two large prime numbers. Shor's algorithm which was one typical quantum algorithm designed by Peter Shor can crack RSA in polynomial time. Shor's algorithm has even been extended to attack many other public key cryptosystems [2].

Shor's algorithm is a significant quantum algorithm for factoring a number N in O((log N)3) time and O(log N) space. One key technique of the Shor's algorithm is turning the factoring problem into the problem of finding the period of a function [3] and [4]. In addition studying the character of the mode function, the period can be easily gained by the monotony of the mode function. Meanwhile an important parameter for period-finding is optimized.

2. The Shor's Algorithm

The Shor's algorithm is composed of two parts. One it turning the factoring problem into the problem of finding the period of a function, and this part is a prominent technique of the Shor's algorithm. The other is finding the period using the quantum Fourier transform, and this part is the kernel of the Shor's algorithm [5].

2.1. Decomposition basis for period-finding

The aim of the Shor's algorithm is that a large number N can be factored into two small factors N_1, N_2 of the N. It is easy to see that the integers, less than N and comprise with N, can form a finite group under multiplication modulo N. An integer a can be found in this finite group. The periodic function is set to the mode function with the number 'a', which implements the transform from the factoring problem to the problem of finding the period of a function, such that

$$f(x) = a^x modN, \tag{1}$$

where the number 'a' is from 0 to N-1 and should be comprise with N,the number 'x' is from 0 to 2^L, such that $N^2 < 2^L < N^2$.

Since the group of the number 'a' is finite, the number 'a' may exist a finite order r that is the smallest positive and even integer such that . If let x=0, this relation remains true for the same integer 'r'. Thus

$$a^r modN \equiv a^0 modN, a^r modN \equiv 1 modN \tag{2}$$

Consequently,

$$a^r - 1 = (a^r/2 + 1)(a^r/2 - 1) \equiv 0 modN \tag{3}$$

By the definition of the greatest common divisor, we can conclude that

$$gcd(a^r/2 + 1, N) \neq 1, gcd(a^r/2 - 1, N) \neq 1 \tag{4}$$

0-7695-3072-9/07 $25.00 © 2007 IEEE
DOI 10.1109/CIS.2007.28

Since

$$gcd(a^r/2+1)|N, gcd(a^r/2-1)|N \qquad (5)$$

Hence, the two factors of the number N can be got, denoting $N_1 = gcd(a^r/2+1, N)$, $N_2 = gcd(a^r/2-1, N)$ that satisfy the equation

$$N = N_1 \times N_2 \qquad (6)$$

2.2. The Process of Shor's Algorithm

An important technique of the Shor's algorithm is turning the factoring problem into the problem of finding the period of a function. Another technique is that the period of the function can be obtained by the Quantum Fourier Transform. The two techniques are the main part of Shor's algorithm, whose idea can be carried out by the following steps:

Step1: Pick a pseudo-random number 'a' less than N and a number 'L' such that $N^2 < 2^L < N^2$;

Step2: Compute the greatest common divisor of the number 'a' and 'N', denoting $gcd(a, N)$

Step3: If $gcd(a, N) = 1$, then there is a nontrivial factor of N; If $gcd(a, N) \neq 1$, then the mode function$f(x) = a^x mod(N)$ to find the smallest integer 'r';

Step4: If the period 'r' is odd, go back to step 1;

Step5: If , go back to step 1;

Step6: The factors of N are $gcd(a^r/2+1, N)$ and $gcd(a^r/2-1, N)$. The process is over.

These computation are done successively for a=0,1,2,...N-1, x=0,1,2L-1[6] and [7].

2.3. Quantum Fourier Transform

To compute the period of a function f, we should evaluate the function value at all points $(x_1, x_2, \ldots, x_n\ )$ simultaneously. A measurement will yield only one of all possible values and destroy others by the character quantum entanglement. This is achieved by the quantum Fourier Transform [8]. A quantum Fourier Transform on N points is defined by:

$$QFT : |x> = \frac{1}{\sqrt{2^L}} \sum_{t=0}^{2^L-1} e^{\frac{2\pi ixt}{2^L}} |t> \qquad (7)$$

The quantum states $|x>$ and $|f(x)>$ are set as two registers using more complicated quantum entanglement state, then the following entanglement state includes all the information at all points $(x_1, x_2, \ldots, x_n\ )$

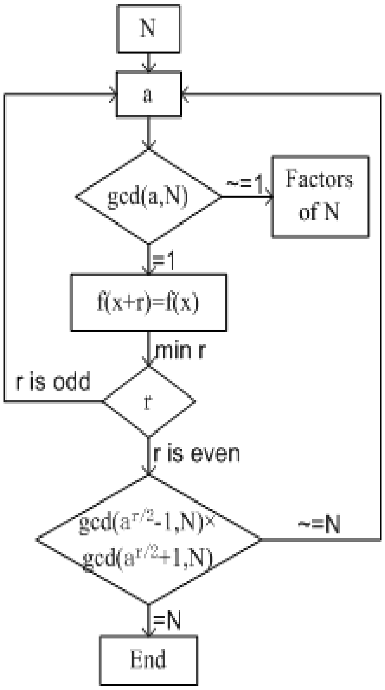

Figure 1. The process of the Shor's algorithm.

$$\sum_{i=1}^{n} |x_i> \otimes |f(x_i)> = |x_1> \otimes |f(x_1)> + \ldots + |x_n> \otimes |f(x_n)> \qquad (8)$$

Thus the quantum Fourier Transform values at n points $(x_1, x_2, \ldots, x_n\ )$ can be obtained simultaneously via replacing the function f(x) with QFT.

3. A New Way of Period-finding

From the second segment, it is easy to see the period-finding problem is the key to the Shor's algorithm. Another way of period-finding is proposed based on the theorem of the number and the monotony of the mode function. The mode function$f(x) = a^x modN$, where the number 'a' is less than N and is prime with the N; the number 'x' is from 0 to $2^L - 1$.

The mode function values is clearly from 1 to $N-1$ during some fixed time segment. Then it can be regarded as a period function [8]. During a period the function values must increase by degrees in the anterior part and decrease by degrees in the posterior part. Its period is obtained through the same function value at the nearest two points by the monotony of the mode function.

Let N=14, then the length of N in the binary 'L' is 8; the number 'x' is from 0 to 255, the number 'a' can be set from

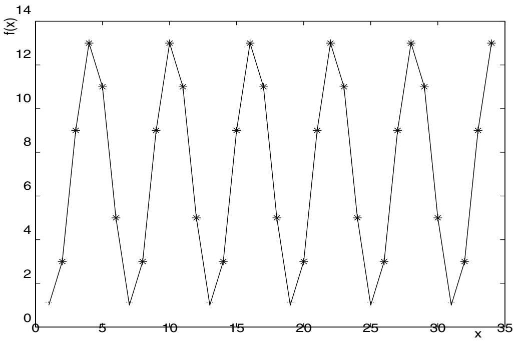

Figure 2. The Period-finding of ’14’

0 to 255. The period ’r’ is obtained through the process in the fig.1, r=6. The process of period-finding is illustrated for the anterior 34 values in the fig.2 clearly.

From the process of the Shor’s algorithm in the Fig.1, it is easy to see that the number ’a’ is important to determine the last result. After a large number of experiments, we find the number ’a’ is generally set to anterior elements. Ten numbers is experimented: different ’a’ and its location in the set of ’a’, the relevant period and the relevant factors are separately listed in the table.1.

Table 1. The location of the number ’a’ and the decomposition process

Number	a	Location	The period	N1	N2
14	3	2/5	6	2	7
21	2	1/11	6	3	7
33	5	3/19	12	3	11
35	2	1/23	12	5	7
57	5	3/35	18	3	19
77	2	1/59	30	7	11
91	2	1/71	12	7	11
115	2	1/17	44	5	23
119	2	1/45	24	7	17
143	2	1/119	60	11	13
221	2	1/191	24	13	17

From the location of ’a’ in the table.1, the ’a’ in their each set is anterior element. And many of them are the second element in the set of the number ’a’. This regularity indicates that the set of the number ’a’ can shrink into only small sets, relative to the original set. Since the elements of back half of the set are generally larger than front ones, the computation of the back elements is fairly far higher. Thus the calculation quantity can be reduced heavily using the regularity.

4. Conclusion

Using the character that the mode function values must increase by degrees in the anterior part and decrease by degrees in the posterior part during a period, new way to determine the period of Shor’s algorithm is proposed based on the key techniques of Shor’s algorithm. Meanwhile the selection of number ’a’ is given. Lastly two simulation experiments respectively illustrate the monotony of the mode function and the selection of the number ’a’.

5. Acknowledgements

Thanks the Institute of Intelligent Computing Science of Shenzhen University for supplying a ascendant environment for this research. Thanks for the funds support from the scientific research projects of Shenzhen University (No.200740).

References

[1] Jianguo Huang, Kewe Liu, Yi Sun and Hong Qin. Quantum Computing and Its Applications in Signal and Information Processing. Systems Engineering and Electronics, 2003(07), pp:800-803,July 2003.

[2] Xin L, Zhi Ma, and Dengguo Feng. Quantum Secure Direct Communication Using Quantum Calderbank-Shor-Steane Error Correcting Codes. Journal of Software, 2006(03):509-515, March 2006.

[3] Shor Peter. Polynomial Time Algorithms for Prime Factorization and Discrete Logarithm s on Quantum Compute. SIAM Journal of Computing. 26(5):1484-1590, May 1997.

[4] Ying Zhu. Shor’s algorithm principle and simulation of program. Computer Applications and Software, 2004(09):118-120, September 2004.

[5] Piotr Gawron. Shor’s factoring algorithm. www. quantiki. org/wiki/index. php/Shor’s factoring algorithm. September 2005.

[6] Zhengjun Cao and Lihua Liu. A Note on Shor’s Quantum Algorithm. Journal of Shanghai Jiaotong University. 2006(03):368-370, March 2006.

[7] Jirong Li. Research on Quantum Computation and its Applications. Control and Automation, 2006(27):275-277, September 2006

[8] Yu I. Manin and A.A Panchishkin.Introduction to modern number theory. China Science Press, Beijing, 2006.