Shor's Algorithm for Quantum Factoring

Manisha J. Nene and Gaurav Upadhyay

Abstract The strength of the famous RSA algorithm depends on the difficulty of factoring large integers in polynomial time. Shor's quantum algorithm has the potential to break RSA in reasonable time. Although, development and commercial availability of high power (16-qubit and more) quantum computers is still some years away, efforts in the direction of simulating quantum algorithms on a classical system are welcome. This paper presents a systematic approach in the direction of factoring integers using the Shor's quantum algorithm on a classical system, where the results of simulation are corroborated with theoretical results.

Keywords Quantum computing · Shor's algorithm · Factorization

1 Introduction

In near future a more fundamental science, that of quantum physics, will catapult the world of computing at such a pace which had been unprecedented. As the transistors on the chips get smaller, the weird and fascinating effects of quantum physics dominate the manner in which interactions between various components take place. Of particular interest are the phenomenon of *entanglement* and *superposition* which can be made use of in Quantum Information Processing (QIP). Construction of quantum information theory on the lines of Shannon's classical information theory is a landmark event in the history of QIP. Unique properties of quantum states as highlighted by the quantum information theory are: "Quantum states are impossible to copy" and "Quantum states cannot be measured with certainty". In order to fully appreciate the power of QIP, an understanding of the

M.J. Nene (✉) · G. Upadhyay
Defence Institute of Advanced Technology, Girinagar, Pune 411025, India
e-mail: mjnene@diat.ac.in

G. Upadhyay
e-mail: gaurav_signals@yahoo.co.in

R.K. Choudhary et al. (eds.), *Advanced Computing and Communication Technologies*,
Advances in Intelligent Systems and Computing 452,
DOI 10.1007/978-981-10-1023-1_33

concepts of No-cloning theorem, Holevo bound, quantum error-coding, quantum data compression and communication over noisy quantum channel is required [1]. Fascinating advances have been made in the field since the First Conference on the Physics of computation held at MIT in which Richard Feynman drew a parallel between an exponentially powerful quantum computation methodology and a multi-particle interference experiment and its measurement [2]. Numerous algorithms and protocols have been developed which have strengthened the foundations of quantum computing. Deutsch algorithm [3], Simon algorithm [4], Shor's quantum algorithm [5] and BB84 protocol [6] are some of them. Related work in the field of factoring large integers and particularly Shor's algorithm can be found in [5, 7–14].

2 Quantum Computing and Shor's Algorithm

The fundamental unit in quantum computing is a qubit, a quantum bit. A qubit, unlike a classical bit can take on infinite values and be in superposition. This is represented by linear combination of vectors, which are called states in quantum mechanics. Dirac-ket notation, which is standard in quantum mechanics, is used to represent the states of a qubit. The classical bit '0' and '1' are replaced by the qubit $|0\rangle$ and $|1\rangle$. A 2-qubit quantum state will have its resultant vector in 4-dimensional space. These states form an ortho-normal computational basis for the computer. Measurement of the state of the register will collapse onto any one of the four states non-deterministically. One needs to have many copies of the same state in order to access the state via measurement [9]. It can be seen that an n-qubit quantum computer can be in a superposition of 2^n states or computational basis, for such a computer will have 2^n values. With the Shor's quantum algorithm the problem of factoring and finding discrete logarithm becomes computationally feasible. The problem of finding factors is reduced to the problem of finding order of an integer x less than N. The number x is selected randomly and if they have common factors, then the GCD will bring out the factors for N. If x is co-prime to N then the case is investigated and a least positive integer r is found which is the order of x modulo N.

3 Problem Statement and Proposed Solution

3.1 Problem Statement and Scope

To simulate Shor's algorithm for quantum factoring on classical computer. To analyze the periodicity of the values or amplitudes of the computational basis for up to 3-digit integer values of N.

3.2 Simulation Platform

The simulation is made on a classical computer running Microsoft Window® 7 Ultimate (64-bit) running on an a Intel® core™ i5-4260U CPU@1.40 GHz having 4 GB RAM. The software platform used is MATLAB 7.12.0 (R2011a) with Quantum Computing Function (QCF) Tool box.

3.3 Algorithm

Step 1. Choose N and x, $\ni$ gcd (N, x) = 1.
Step 2. Choose q, $\ni N^2 < 2^q < 2N^2$. Let $2^q = Q$.
Step 3. Generate computational basis vector (C) having values from 1 to Q.
Step 4. Generate a zero vector (Z) of same length Q, first element initialized to x.
Step 5. Generate elements 2 to Q for $Z \ni Z(i) = x \times Z(i-1) \bmod N$.
Step 6. Find the Quantum Discrete Fourier Transform (QDFT) of Z and normalize the values to 1.
Step 7. Select the values in C, where Z is having a peaks i.e local maximum.
Step 8. Calculate Continued Fraction Expansion of selected values of C and Q.
Step 9. Check if r is even. If No, then choose another x and goto Step 2.
Step 10. The factors of N are given by $\gcd(x^{(r/2)} - 1, N)$ and $\gcd(x^{(r/2)} + 1, N)$

4 Simulation Results

4.1 Qu-bit Simulation

Simulation of registers containing 2- and 9-qubits was carried out and measurements made 10 times. The results are as listed (Table 1).

Table 1 Measurement of superimposed qu-bits

Measurement no.	Result (2 qubit)	Result (9 qubit)
1	$1\|11\rangle$	$1\|110011001\rangle$
2	$1\|11\rangle$	$1\|011111000\rangle$
3	$1\|00\rangle$	$1\|010111000\rangle$
4	$1\|10\rangle$	$1\|101111001\rangle$
5	$1\|11\rangle$	$1\|011011000\rangle$
6	$1\|00\rangle$	$1\|110011011\rangle$
7	$1\|01\rangle$	$1\|001101000\rangle$
8	$1\|10\rangle$	$1\|000100100\rangle$
9	$1\|11\rangle$	$1\|111100000\rangle$
10	$1\|00\rangle$	$1\|100110110\rangle$

In superposition, the 2-qubit register will be in all 4-possible states simultaneously. However, the act of measurement collapses the state to any one of the computational basis, which for a 2-qubit register is $|00\rangle$, $|01\rangle$, $|10\rangle$ or $|11\rangle$. The notation $1|10\rangle$ means that the qubit has value '10' with probability '1'. Similar inference can be drawn for 9-qubit register. The 9-qubit register is in all 512 states (0–511) simultaneously; however the act of measuring collapses the superimposed state to one of the states in a non-deterministic manner.

4.2 *Shor's Quantum Algorithm Simulation*

In this sub-section, the results of simulation of Shor's algorithm for quantum factoring are presented (Table 2).

A visual representation of values of computational basis vector (C) and normalized QDFT vector (Z) in form of graphs is presented for further understanding. The graphs for $N = 21$ and $N = 247$ are presented.

Table 2 Result of Shor's quantum algorithm simulation

S. No.	N	x	r	q	Q	Factors
1	21	2	6	9	512	3, 7
2	35	2	12	11	2048	5, 7
3	55	2	20	12	4096	5, 11
4	77	2	30	13	8192	7, 11
5	247	2	36	16	65,536	13, 19

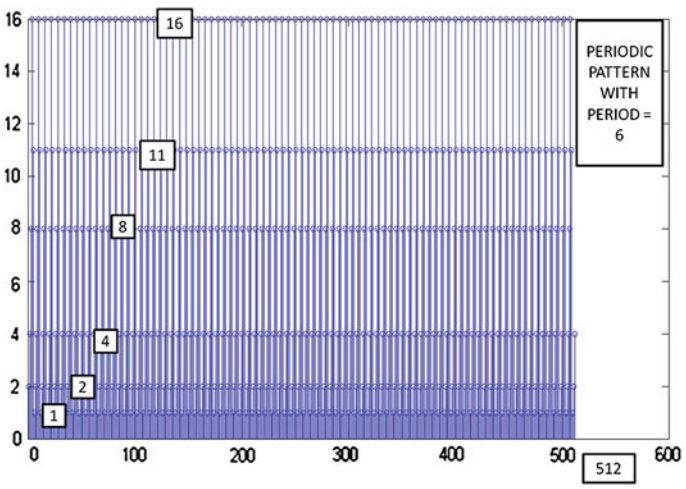

Fig. 1 Plot of values of vector C for $N = 21$. This highlights the order of x modulo N visually

The graph at Fig. 1 visually brings out the pattern 1,2,4,8,11,16, 1,2,4,8,11,16, 1,2,4,8,11,16 …. It can be seen that the period here is 6, which is the order we need to find. The QDFT graph of vector Z for $N = 21$ generated a total of 5 peaks. The plot is given in Fig. 2. Same can be inferred from Figs. 3 and 4 for $N = 247$.

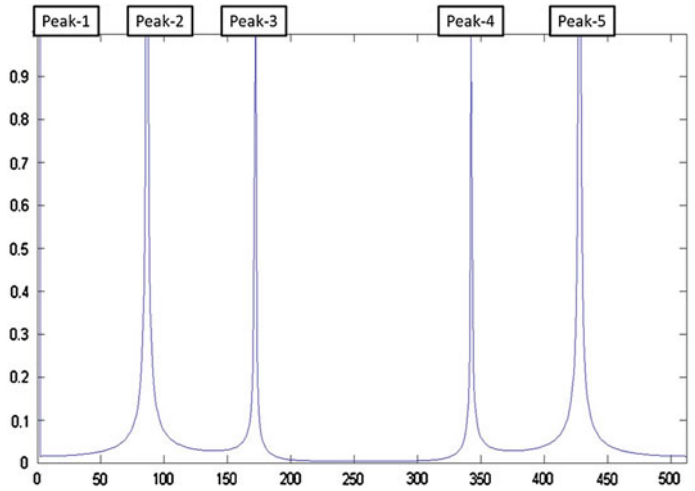

Fig. 2 Plot of values of vector Z for $N = 21$. Plot highlights the places where either 'r' or a factor or 'r' can be found

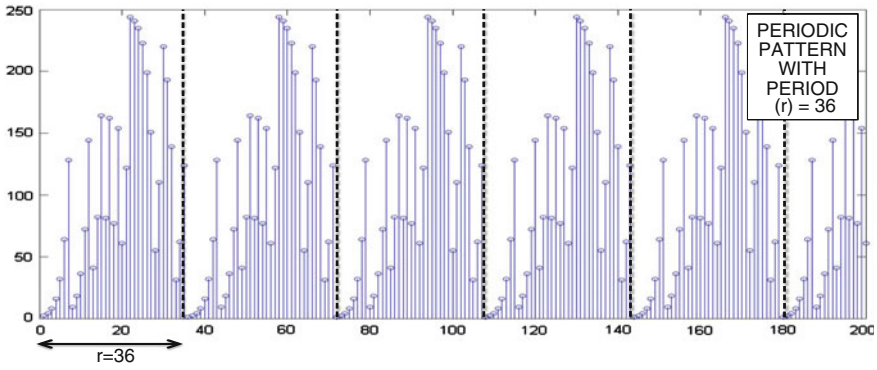

Fig. 3 Plot of values of vector C for $N = 247$. The plot has been clipped for values upto 200 to highlight the period of 36

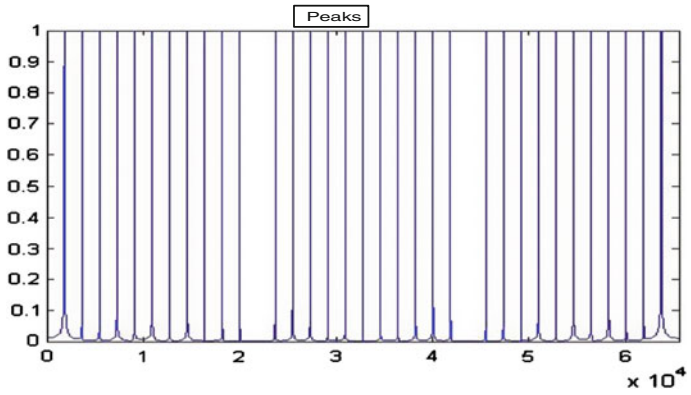

Fig. 4 Plot of values of vector Z for $N = 247$

5 Conclusion

The problem of factoring can be solved and results verified using Shor's algorithm for quantum factoring on a classical computer using primitive simulation. The representation of the results in visual format aids in better understanding of the working of the mathematics behind factorization and helps to arrive at the correct solution faster. The limitations of the present work are that there is no way of making use of superimposed registers which were simulated with the process of factoring. The limitation draws from the fact that the registers on a classical computers cannot be in superposition. The second and a major limitation is that as the value of N increases the order finding, r, becomes exceedingly difficult in the simulation. Although the probability of homing on to correct computational basis is high, in the proposed approach a combination of visual and manual sifting through the data does the trick.

References

1. Nielsen, M.A., Chuang, I.L.: "Quantum Computation and Quantum Information". Cambridge University Press, Part-III, Chap. 8–12, Edition (2002)
2. Feynman, R.P.: Simulating physics with computers. Int. J. Theor. Phys. **21**, 467–488 (1982)
3. Deutsch, D., Jozsa, R.: Rapid solution of problems by quantum Computation. Proc. R. Soc. London **A439**, 553–558 (1992)
4. Simon, D.: "On the power of quantum computation". In: Proceedings of the 35th Annual Symposium on Foundations of Computer Science, 116 pp. (1994), and SIAM J. Comput. **26**, 1474–1483 (1997)
5. Shor, P.: "Algorithms for quantum computation: discrete logarithm and factoring". Proceedings of the 35th Annual Symposium on Foundations of Computer Science, pp. 124–134 (1994), and SIAM J. Comput. **26**, 1484–1509 (1997)

6. Bennett, C.H., Brassard, G.: "Quantum cryptography: public key distribution and coin tossing". In: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, pp. 175–179 (1984)
7. Vandersypen, M.K., Steffen, M., Breyta, G., Yannoni, C.S., Sherwood, M.H., Chuang, I.L.: "Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance". Nature **414**, 883 (2001)
8. Nam, Y.S.: "Running Shor's algorithm on a complete, gate-by-gate implementation of a virtual, universal quantum computer". A Dissertation submitted to the faculty of Wesleyan University, Departmental Honors in Physics (2011)
9. Lavpor, C., Manssur, L.R.U, Portugal, R.: "Shor's Algorithm for factoring Large Integers", Lecture notes from graduate courses in Quantum computation given at LNCC, 3 pp. (2008)
10. Politi, A.M., Jonathan, C.F., O'Brien, J.L.: "Shor's quantum factoring algorithm on a photonic chip". J. Sci. **325**(5945), 1221–1221 (2009)
11. Wang, W-Y., Shang, B., Wang, C., Long, G-L.: "Prime factorization in the duality computer". Commun. Theor. Phys. **47**(3), 471 (2007)
12. Browne, D.E.: "Efficient classical simulation of the quantum Fourier transform", New J. Phys. **9**(5), 146 (2007)
13. Lu, C-Y., Browne, D.E., Yang, T., Pan, J-W.: "Demonstration of a compiled version of shor's quantum factoring algorithm using photonic qubits. Phys. Rev. Lett. **99**(25), 250504 (2007)
14. Nagaich, S., Goswami, Y.C. "Shor's algorithm for quantum numbers using MATLAB simulator". In: Fifth International Conference on Advanced Computing and Communication Technologies, pp. 165–168 (2015)