Quantum Physics Letters
An International Journal

http://dx.doi.org/10.18576/qpl/070202

A New Simple and Efficient Quantum Algorithm for Factoring Composite Integers

Dhananjay P. Mehendale

Department of Physics, Savitribai Phule University of Pune, Pune, India-411007.

Received: 7 Jun. 2018, Revised: 18 Jul. 2018, Accepted: 20 Jul. 2018
Published online: 1 Aug. 2018

Abstract: We present a new simple and efficient quantum algorithm for factoring composite integers. The key step consists of making use of the new exponentially fast search algorithm [1]. Let $M = PQ$, $0 < M < 2^n$, be a composite integer with two nearly equal prime factors P, Q to be determined. We prepare register, say $A = A_1 \otimes A_2$, where A_1 and A_2 are sub-registers containing equally weighted superposition of states $|x\rangle$ and $|y\rangle$ respectively such that $0 \leq x, y \leq 2^n - 1$. Register A thus contains equally weighted superposition of the tensor product states $|x\rangle|y\rangle$. We also prepare register B to keep the images of elements in register A produced under the action of the function, f, $f : A \to B$, defined as $f(|x\rangle|y\rangle) = |xy\rangle$. The transformation, U_f, corresponding to the given fuction f is defined as $U_f : (|x\rangle|y\rangle)_A(|0\rangle)_B \to (|x\rangle|y\rangle)_A(|xy\rangle))_B$, which can also take superposition of states as input. Thus, register A is entangled with register B through U_f. After building up quantum registers A and B we operate on register B a unitary operator, U, defined as $U = \sum_z |v\rangle\langle v|$, where $0 \leq z \leq 2^n - 1$, and $|v\rangle = |00\cdots 0\rangle_n|z\rangle$. The action of U will change the state in register B into the uniform superposition state $\frac{1}{\sqrt{2^n}}\sum_{z=0}^{2^n-1}|v\rangle$, so that that this state now becomes separable and the algorithm in [1] becomes applicable for searching a target state present as a component state in this modified register B. We then perform the key step of applying [1] on register B for searching the target state $|t\rangle = |00\cdots 0\rangle_n|M\rangle$, and amplify to the full extent the amplitude of this target state so that if we now partially measure the register B it will almost always be found in this target state $|t\rangle = |00\cdots 0\rangle_n|M\rangle$. As a consequence of this the state in register A now changes into the superposition state $\frac{1}{\sqrt{2}}(|1\rangle|M\rangle + |P\rangle|Q\rangle + |Q\rangle|P\rangle) + |M\rangle|1\rangle)$. This new state in register A now clearly contains the desired prime factorization which is easily revealed after further partial measurement done on any one of the sub-registers A_1, A_2.

Keywords: Factorization problem, Quantum parallelism, Multiple number of Oracles

1 Introduction

We present a new simple and efficient quantum algorithm to be worked on a quantum computer for factoring composite integers having two prime factors comparable in size. The case of factoring a composite integer with just two prime factors is actually the most difficult one for the factoring problem. Shor's quantum algorithm for factoring a composite integer [2] has shown that quantum computers can find the two prime factors of an n-bit integer using only $O(n^2 log(n) loglog(n))$ operations for which the classical computers require $exp(\Theta(n^{1/3} log^{2/3}(n))$ operations [3]. Thus, Shor's quantum algorithm offers exponential speedup over its classical counterpart for the problem of factoring composite integers. This paper proposes a new alternative to Shor's factoring algorithm which is simpler than Shor's algorithm and solves the problem almost instantaneously by just doing few partial measurements. This new quantum algorithm for factoring composite integers is based on using the new exponentially fast search algorithm [1]. This new algorithm demonstrates how those strange features, namely, superposition and entanglement, which are absent in classical systems and are present only in quantum systems can cause exponential rise in the efficiency. Superposition is that feature possessed only by quantum systems which allows a quantum computer to act simultaneously upon an input state made up of an exponential number of different classical inputs present in the superposition of basis states, $|k\rangle, 0 \leq k \leq 2^n - 1$. Entanglement is the most quintessentially quantum effect present only in quantum systems that allows strong correlations to exist between different subsets of qubits such that measurements made on one subset of qubits can affect the likelihood of the

* Corresponding author e-mail: dhananjay.p.mehendale@gmail.com

outcomes of measurements made on other subsets of qubits, even though they were not touched in any direct way [4]. One can prepare two entangled quantum registers, E and F say, such that register E contains a set of indices running from 0 to 2^n-1 and register F contains a set of values of a function whose behavior depends upon the value of the index in register E. So the joint state (ignoring the normalization factor) can be something like $\sum_{i=0}^{2^n-1}|i\rangle_E|f(i)\rangle_F$. By measuring the value of the function (in register F), "c" say, we can project out the set of indices (in register E) consistent with the observed function value, giving rise to a superposition of the form $\sum_{(i':f(i')=c)}|i'\rangle|c\rangle$, and this is a neat trick because in one shot we get all the index values (in register E) that give the same value for the function, equal to "c"(in register F).

2 Preparing quantum registers

Let $M=PQ$, where P,Q are nearly equal prime factors to be determined. We choose n such that $0<M<N$, where $N=2^n$.

A quantum register is the "storing place" for the quantum states and their superposition. A function mapping a quantum register to another quantum register can be so defined that it maps a quantum state in one register, say the "domain register", on to a quantum state in the other register, say the "range register". The operator representing this function in effect correctly maps the quantum state presented to it in the "domain register" on to the appropriate quantum state in the "range register".

We now begin with preparing two quantum sub-registers A_1,A_2 both to contain quantum states representing $N=2^n$ integers $\{0,1,\cdots,N-1\}$ i.e. quantum states $\{|0\rangle,|1\rangle,\cdots,|N-1\rangle\}$. In classical terms these sub-registers will be just two bags of indices, x and y, such that $0\le x,y\le N-1$. In quantum mechanical language: the quantum analog of these bags of indices, x and y, are two quantum sub-registers containing equally weighted superposition of basis states, $|x\rangle$, and $|y\rangle$, respectively, i.e. sub-registers A_1 and A_2 will contain the superposition $\frac{1}{\sqrt{N}}\sum_{x=0}^{(N-1)}|x\rangle$ and $\frac{1}{\sqrt{N}}\sum_{y=0}^{(N-1)}|y\rangle$, respectively. We now prepare the quantum register $A=A_1\otimes A_2$. Clearly, register A will contain the equally weighted superposition of the tensor product states, $|x\rangle|y\rangle$, i.e. the superposition $\frac{1}{N}\sum_{x,y=0}^{(N-1)}|x\rangle|y\rangle$. This register A will form the domain register for function, f, that we will define soon. We prepare the quantum register, B say, to store the images (image states) under the action of the function $f:A\to B$. Thus, register B represents range register for our function, f, $f:\{0,1\}^n\times\{0,1\}^n\to\{0,1\}^{2n}$ such that $f(|x\rangle|y\rangle)=|xy\rangle$. We note here that since $N=2^n$ we can express the basis states $|x\rangle$, $|y\rangle$ in sub-registers A_1,A_2 respectively in terms of computational basis states using $n=\log_2 N$ qubits and also from the definition of the function it is clear to see that we can express the image states in register B, which contains images of elements in register $A=A_1\otimes A_2$ under f, in terms of computational basis states using $2n=2\log_2 N$ qubits. Further, it is easy to see that we can express the basis states $|x\rangle$, and $|y\rangle$, belonging to registers A_1 and A_2 respectively, in terms of the corresponding computational basis states containing n qubits by replacing each integer x and y, $0\le x,y\le N-1$, by its corresponding binary representation containing n bits and juxtaposing them to find binary representation for tensor product state $|x\rangle|y\rangle$. Also, we can express the image states, $|xy\rangle$, $0\le x,y\le N-1$, in the image register B in terms of the corresponding computational basis states containing $2n$ qubits by replacing products xy by their corresponding binary representation containing $2n$ bits, e.g. let the binary representations of x and y be $i_1i_2\cdots i_n$ and $j_1j_2\cdots j_n$ respectively then the corresponding tensor product state will be $|x\rangle|y\rangle=|i_1i_2\cdots i_n\rangle|j_1j_2\cdots j_n\rangle$. Similarly, let the binary representations of xy be $k_1k_2\cdots k_{2n}$ then the image state of $|x\rangle|y\rangle$ under f will be $|xy\rangle=|k_1k_2\cdots k_{2n}\rangle$. It is clear to check that the above mentioned equally weighted superposition states $\frac{1}{\sqrt{N}}\sum_{x=0}^{(N-1)}|x\rangle$ and $\frac{1}{\sqrt{N}}\sum_{y=0}^{(N-1)}|y\rangle$, in sub-registers A_1 and A_2 respectively can then be looked upon as prepared by applying a separate 1-qubit Hadamard gate H on each of n qubits prepared initially in the state $|0\rangle$. Thus the superposition in sub-registers A_1 and A_2 can be prepared as $H^{\otimes n}|0\rangle^{\otimes n}$. It is a well known fact that when one performs measurement on any superposition one gets some single index nondeterministically in accordance with one more special feature possessed by quantum systems other than the special features superposition and entanglement mentioned above, namely, the non-determinism. Non-determinism means our inability to predict with certainty what answer we will get when we read a quantum memory register that exists in a superposition state. However, we can calculate the probabilities with which we expect to see the various possible outcomes. The fuction f defined above gives rise to the following transformation, U_f, $U_f:(|x\rangle|y\rangle)_A(|0\rangle)_B\to(|x\rangle|y\rangle)_A(f(|x\rangle|y\rangle))_B$. It is straightforward to check that when we prepare in the (domain) register A the superposition $\frac{1}{N}\sum_{x,y=0}^{(N-1)}|x\rangle|y\rangle$ then under the action of the above transformation, U_f, we will get the corresponding superposition of states $|xy\rangle$, $0\le x,y\le N-1$, $\frac{1}{N}\sum_{x,y=0}^{(N-1)}|xy\rangle$, in the image register B.

With these preliminaries we now proceed to discuss the steps of a new exponentially fast quantum algorithm to find two prime factors of a large composite integer using the new exponentially fast search algorithm [1] and few partial measurements.

3 Algorithm

The steps of the algorithm are as follows:

(i) We prepare quantum sub-register A_1 by starting with n qubits all initialized to the state $|0\rangle$ and then we apply Hadamard gate H on each of these n qubits all initialized to $|0\rangle$. Thus sub-register A_1 contains equally weighted superposition of all computational basis states of length n, i.e. A_1 contains $H^{\otimes n}(|0\rangle)^{\otimes n}$.

(ii) We prepare quantum sub-register A_2 exactly identical to above prepared sub-register A_1.

(iii) We prepare quantum register $A = A_1 \otimes A_2$. Let $x = i_1 i_2 \cdots i_n$ and $y = j_1 j_2 \cdots j_n$ in binary notation. The elements in register A_1 are $|x\rangle = |i_1 i_2 \cdots i_n\rangle$ and the elements in register A_2 are $|y\rangle = |j_1 j_2 \cdots j_n\rangle$, respectively. The elements in register A are tensor product states $|x\rangle|y\rangle = |i_1 i_2 \cdots i_n\rangle|j_1 j_2 \cdots j_n\rangle$, obtained by juxtaposition of the above binary sequences for x and y.

(iv) We now apply the transformation U_f, $U_f : (|x\rangle|y\rangle)_A(|0\rangle)_B \to (|x\rangle|y\rangle)_A(f(|x\rangle|y\rangle))_B$. Since U_f can also operate on superposition therefore we have

$$\frac{1}{N}\sum_{x,y=0}^{(N-1)}(|x\rangle|y\rangle)_A(|00\cdots 0\rangle_{2n})_B \to \frac{1}{N}\sum_{x,y=0}^{(N-1)}(|x\rangle|y\rangle)_A(f(|x\rangle|y\rangle))_B \to \frac{1}{N}\sum_{x,y=0}^{(N-1)}(|x\rangle|y\rangle)_A(|xy\rangle)_B.$$

Note that the state $|00\cdots 0\rangle_{2n}$ is made up of $2n-$qubits and also both the registers A and B contain states with $2n-$qubits. Note that we get the elements in register B as follows: We find the usual product of elements x and y, namely, xy, we then find the binary representation for xy, namely, $xy = k_1 k_1 \cdots k_{2n}$ and prepare state $|xy\rangle = |k_1 k_1 \cdots k_{2n}\rangle$.

(v) Our aim now is to change the state in register B into the state which is the equally weighted uniform superposition of states $|v\rangle = |00\cdots 0\rangle_n|z\rangle$ such that $0 \le z \le N-1$. It is easy to check that thus transformed new state in register B then becomes completely factorable (separable) state and further it also contains the "desired target state", $|t\rangle = |00\cdots 0\rangle_n|M\rangle$, as a component state so that the new search algorithm [1] becomes applicable. For this to achieve we operate the superposition state $\frac{1}{N}\sum_{x,y=0}^{(N-1)}(|xy\rangle)$ in register B by the unitary operator, U, defined as follows: $U = \sum_z |v\rangle\langle v|$. The action of U will reduce the register B to contain equally weighted superposition of states $|v\rangle$, i.e. register B (after normalization) will now contain the state $\frac{1}{\sqrt{N}}\sum_{z=0}^{2^n-1}|v\rangle = |00\cdots 0\rangle_n \frac{1}{\sqrt{N}}\sum_{z=0}^{2^n-1}|z\rangle$.

(vi) Now we perform **the key step** of the algorithm. It consists of calling (as subroutine) the algorithm in [1]. We choose the state $|t\rangle = |00\cdots 0\rangle_n|M\rangle$ which is present as a component state in the superposition state in the image register, B, i.e. $|t\rangle = |00\cdots 0\rangle_n|M\rangle = |v_0\rangle = |00\cdots 0\rangle_n|z_0\rangle$ for some $0 \le z_0 \le N-1$, as the target state for the algorithm [1] and amplify the amplitude of this chosen target state to the full extent. Note that due to the application of the new exponentially fast search algorithm [1] one can do this amplitude amplification to the full extent of the desired target state in one shot.

(vii) We now carry out the partial measurement on register B. It will almost always produce the desired target state with hunderd percent guarranttee. Due to this partial measurement done on register B the state in register A will then change into superposition state $\frac{1}{2}(|1\rangle|M\rangle + |P\rangle|Q\rangle + |Q\rangle|P\rangle) + |M\rangle|1\rangle)$. This changed state in register A now contains the desired prime factorization which is easily revealed after further partial measurement done on any one of the sub-registers A_1, A_2.

4 An example

Suppose we are given a composite integer $M = 15 < 2^4 = 16$ as a product of two primes and our aim is to find those prime factors of $M = 15$. We choose $n = 4$ and further prepare the so called domain register, A, to contain the superposition of tensor product states $|x\rangle|y\rangle$, $0 \le x, y \le 2^4 - 1$, and the corresponding image register, B, will then contain the superposition of states $|xy\rangle$. Note that we are essentially working in **binary system** and the states in register A as well as B, are of length eight, i.e. made up of eight qubits. Further note that each of the states $|x\rangle$ and $|y\rangle$ in the tensor product states $|x\rangle|y\rangle$ is made up of four qubits.

As per the algorithm developed above we now carry out the following steps:

(1) We prepare quantum register $A = A_1 \otimes A_2$ to contain $\frac{1}{2^4}\sum_{x,y=0}^{(2^4-1)}|x\rangle|y\rangle$, where sub-registers A_1 and A_2 contain superposition $\frac{1}{\sqrt{2^4}}\sum_{x=0}^{(2^4-1)}|x\rangle$ and $\frac{1}{\sqrt{2^4}}\sum_{y=0}^{(2^4-1)}|y\rangle$, respectively. Thus, the state in register A will be

$$\frac{1}{2^4}(|0\rangle|0\rangle + \cdots + |1\rangle|15\rangle + \cdots + |3\rangle|5\rangle + \cdots + |5\rangle|3\rangle + \cdots + |15\rangle|1\rangle + \cdots + |15\rangle|15\rangle).$$

(2) We now apply the transformation U_f, $U_f : (|x\rangle|y\rangle)_A(|0\rangle)_B \to (|x\rangle|y\rangle)_A(|xy\rangle)_B$. Since U_f can also operate on superposition therefore we have

$$\frac{1}{2^4}\sum_{x,y=0}^{(2^4-1)}(|x\rangle|y\rangle)_A(|00\cdots 0\rangle_8)_B \to \frac{1}{2^4}\sum_{x,y=0}^{(2^4-1)}(|x\rangle|y\rangle)_A(|xy\rangle)_B.$$

Thus, the state in register B will be

$$\frac{1}{2^4}(|0\rangle + |1\rangle + |2\rangle + \cdots + |15\rangle + |16\rangle + |18\rangle + |20\rangle + \cdots + |30\rangle + \cdots + |225\rangle).$$

(3) We now apply the unitary operator $U = \sum_z |v\rangle\langle v|$, where $0 \le z \le 2^4 - 1$ and $|v\rangle = |0000\rangle|z\rangle$ on register B.

This will change the superposition state present in register B to

$$\frac{1}{\sqrt{2^4}}\sum_{z=0}^{(2^4-1)}|v\rangle = |0000\rangle\frac{1}{\sqrt{2^4}}\sum_{z=0}^{(2^4-1)}|z\rangle.$$

Thus, the state in register B now changes to

$$\frac{1}{\sqrt{2^4}}(|0000\rangle)\otimes[|0000\rangle+|0001\rangle+|0010\rangle+\cdots+|1111\rangle)].$$

(4) We now perform **the key step** of the algorithm. It consists of calling (as subroutine) the algorithm in [1] by choosing $|t\rangle = |0000\rangle|M\rangle = |0000\rangle|15\rangle = |0000\rangle|1111\rangle$ which is present as one of the component states in the superposition state contained in register B, as the target state for the algorithm [1] and amplify the amplitude of this chosen target state to full extent. Note that due to the use of this new exponentially fast search algorithm in [1] one can achieve this amplitude amplification of the desired target state with amazing speed, in fact, in one shot. The target searching using [1] happens as follows:

(a) We rewrite the state in register B as

$$\frac{1}{\sqrt{2^4}}(|0000\rangle)\otimes[(|00\rangle+|01\rangle+|10\rangle+|11\rangle))\otimes(|00\rangle \\ +|01\rangle+|10\rangle+|11\rangle)]$$

The state $|0000\rangle$ is common to all component states in B so we can ignore it and take as search space the superposition state formed with last four qubits:

$$|\psi\rangle = \frac{1}{\sqrt{2^4}}(|00\rangle+|01\rangle+|10\rangle+|11\rangle))\otimes(|00\rangle+|01\rangle \\ +|10\rangle+|11\rangle) = (|\Theta\rangle\otimes|\Theta\rangle)$$

where $|\Theta\rangle = \frac{1}{2}[|00\rangle+|01\rangle+|10\rangle+|11\rangle]$ in the above expression for the state in register B.

(b) We define operators, $O_i, i = 1,2$ such that $O_1 = I-2|11\rangle\langle 11|$, and $O_2 = I-2|11\rangle\langle 11|$.

(c) We define two identical diffusion transforms

$$W = [2|\Theta\rangle\langle\Theta| - I].$$

(d) We create the product operator, $P = (\prod_{i=1}^{\otimes(2)}(WO_i))$ and operate this product operator on $|\psi\rangle$ given above. This gives rise to state

$$(\prod_{i=1}^{\otimes(2)}(WO_i|\Theta\rangle)) = |11\rangle\otimes|11\rangle \ = |1111\rangle.$$

(e) Now, taking tensor product of this state that resulted after application of [1] with the above ignored common multiplyer state $|0000\rangle$ we get as a result the desired target state

$$|t\rangle = |0000\rangle\otimes|1111\rangle = |0000\rangle|15\rangle = |0000\rangle|M\rangle$$

in one shot.

(5) When the above mentioned amplitude amplification is carried out the register B then will now prominantly contain the state

$$|t\rangle = |0000\rangle\otimes|1111\rangle = 0000\rangle|15\rangle = |0000\rangle|M\rangle.$$

As an effect of this amplitude amplification of the target state in register B (and further by just going ahead and measuring it) the state in register A changes into the following superposition state, namely,

$$\frac{1}{2}(|1\rangle|15\rangle+|3\rangle|5\rangle+|5\rangle|3\rangle)+|15\rangle|1\rangle).$$

This changed state in register A now contains the desired prime factors and they are easily revealed after further partial measurement done on any one of the sub-registers A_1, A_2.

Acknowledgement

I thank Dr. M. R. Modak, S. P. College, Pune-411030, India, for carefully reading the mannuscript and making useful comments and suggestions.

References

[1] D. P. Mehendale, A Simple Quantum Algorithm for Exponentially Fast Target Searching in the Unstructured Database, Quant. Phys. Lett. 6, No. 2, 95-98, (2017)

[2] P. W. Shor, Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, in Proc. of the 35th Annual Symposium on Foundations of Computer Science, IEEE Computer Society, New York, pp. 124-134, (1994)

[3] Nielsen A and Chuang I, Quantum Computation and Quantum Information, Cambridge : Cambridge university Press, (2000)

[4] Colin P. Williams, Explorations in Quantum Computing, 2nd edition: Springer-Verlag London Limited, (2011)

Dhananjay P. Mehendale, Prof. Dhananjay P. Mehendale served as associate professor in S. P. College, affiliated to Savitribai Phule University of Pune, Pune, India-411007. The subjects of his interest and study are Physics, Mathematics, and Engineering and students of science and engineering have successfully completed their project work under his supervision. He taught various courses in Physics, Electronic Science, and Computer Science departments, and has done research in various areas of these subjects. He worked on various science and engineering projects and one of his projects won award in the national science projects competition organized by Department of Science and Technology. His research interest at present is topics in Quantum Computation and Quantum Information.