Quantum Physics Letters
An International Journal

http://dx.doi.org/10.18576/qpl/090102

A New Simple Quantum Algorithm for Finding Two Prime Factors of a Composite Integer

Dhananjay P. Mehendale

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

Received: 2 Jan. 2020, Revised: 2 Feb. 2020, Accepted: 2 Mar. 2020
Published online: 1 Apr. 2020

Abstract: We present a new simple quantum algorithm for factoring composite integers assuming that we can successfully perform the non-unitary operation of projecting certain quantum state by some quantum dynamics in a reasonably less time. Let M be a "known" composite integer with two nearly equal "unknown" prime factors P,Q. Thus, $M = PQ$, $0 < M < 2^n - 1$. 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 f, $f : A \rightarrow B$, defined as $f(|x\rangle|y\rangle) = |xy\rangle$, where xy is the product of x and y. The unitary transformation, U_f, corresponding to f is defined as $U_f : (|x\rangle|y\rangle)_A(|0\rangle)_B \rightarrow (|x\rangle|y\rangle)_A(|xy\rangle)_B$ which can also take superposition of states as input. Thus, we get a "sum" state through operating U_f, namely, $|\Psi_1\rangle = \frac{1}{2^n}\sum_{x=0}^{2^n-1}\sum_{y=0}^{2^n-1}(|x\rangle|y\rangle)_A(|xy\rangle)_B$ and thus register A gets entangled with register B through U_f. We then operate $V = I \otimes U$, on $|\Psi_1\rangle$ where I is Identity operator operating on register A and $U = \sum_{z=0}^{2^n-1}|z\rangle\langle z|$, operating on register B, leading to $V|\Psi_1\rangle = |\Psi_2\rangle$. We further operate a non-unitary operator $W = I \otimes |M\rangle\langle M|$ on $|\Psi_2\rangle$ producing $|\Psi_3\rangle = W|\Psi_2\rangle$ where $|M\rangle\langle M|$ operating on register B is projector in the direction of a "known" computational basis state $|M\rangle$. After the action of unitary operator V if we can perform the "successful" action of the non-unitary operator W by some quantum dynamics in reasonably less time then we will arrive at the following required quantum state: $|\Phi\rangle = \frac{1}{2}(|1\rangle|M\rangle + |P\rangle|Q\rangle + |Q\rangle|P\rangle) + |M\rangle|1\rangle)_A(|M\rangle)_B$. The desired prime factors will then be revealed through partial measurement of any of the sub-registers A_1, A_2.

Keywords: Factorization problem, Quantum Projection Operator, Inner Product

1 Introduction

We present a new simple and quantum algorithm for factoring composite integers having two prime factors which are comparable in size. The case of factoring a composite integer with just two prime factors is actually the most difficult case for the factoring problem. Shor's quantum algorithm for factoring a composite integer [1] 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 [2]. 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 factoring algorithm which solves the problem by making use of projection operator and few partial measurements. This new algorithm demonstrates how superposition and entanglement, absent in classical systems and are present only in quantum systems, can be used to improve 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 outcomes of measurements made on other subsets of qubits, even though they were not "touched" in any direct way [3]. One can prepare two entangled quantum registers, E and F say, such that register E contains a set

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

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). The proposed algorithm for factoring problem requires to make use of a non-unitary operation which is necessarily probabilistic. The success and efficiency of the proposed algorithm depends upon the "successful" application of the above mentioned non-unitary operator, $I\otimes|M\rangle\langle M$ by some quantum dynamics in a reasonably less time.

2 Preparing quantum registers

Let $M=PQ$, where M is known and P,Q are nearly equal "unknown" prime factors to be determined. We choose n such that $0<M<N$, and 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 be identical and 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 function f defined above gives rise to the following unitary transformation, $U_f:(|x\rangle_n|y\rangle_n)_A(|0\rangle_{2n})_B\to(|x\rangle_n|y\rangle_n)_A(|xy\rangle_{2n})_B$. Since U_f can take superposition as input so we get after operating the unitary operator U_f the following "sum' state $\frac{1}{N}\sum_{x=0}^{2^n-1}\sum_{y=0}^{2^n-1}(|x\rangle_n|y\rangle_n)_A(|xy\rangle_{2n})_B$ and thus register A is entangled with register B through U_f.

With these preliminaries we now proceed to discuss the steps of a new quantum algorithm to find two prime factors of a large composite integer using few partial measurements. We assume that we can efficiently perform the "successful" action of a non-unitary operator $W=I\otimes|M\rangle\langle M|$ with unit probability by some quantum dynamics where M is the given "known" composite

integer having two "unknown" prime factors P,Q to be determined.

3 Algorithm

The steps of the algorithm are as follows:

(i) We prepare a 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 one more quantum sub-register A_2 exactly identical to the 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 prepare image register, B, to keep images the images of elements in register A produced under the action of the unitary transformation U_f. Thus:

$$U_f : (|x\rangle_n|y\rangle_n)_A(|0\rangle_{2n})_B \to (|x\rangle_n|y\rangle_n)_A(|xy\rangle_{2n})_B$$

Since U_f can also operate on superposition therefore we have

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

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

Note that the state $|0\rangle_{2n}$ is made up of $2n-$qubits and also both the registers A and B contain states with $2n-$qubits. Note that the elements in register B are made 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 $|xy\rangle_{2n} = |k_1 k_1 \cdots k_{2n}\rangle$.

(v) We thus get the "sum" state

$$|\Psi_1\rangle = \frac{1}{N}\sum_{x,y=0}^{(N-1)}(|x\rangle_n|y\rangle_n)_A(|xy\rangle_{2n})_B.$$

Now we operate on this "sum" state, $|\Psi_1\rangle$, the unitary operator $V = I \otimes U$, where I is identity operator that operates on elements in register A and $U = \sum_{z=0}^{2^n-1}|z\rangle\langle z|$ that operates on elements in register B. As an effect the "sum" state, $|\Psi_1\rangle$, will now change (after normalization) to:

$$|\Psi_2\rangle = C_0\sum_{x,y,xy=0}(|x\rangle|y\rangle)_A(|0\rangle)_B + C_1\sum_{x,y,xy=1}(|x\rangle|y\rangle)_A(|1\rangle)_B + \cdots + C_{2^n-1}\sum_{x,y,xy=2^n-1}(|x\rangle|y\rangle)_A(|2^n-1\rangle)_B$$

such that $\sum_{i=0}^{2^n-1}|C_i|^2 = 1$.

(vi) We further operate on the above changed "sum" state, $|\Psi_2\rangle$, a non-unitary operator $W = I \otimes |M\rangle\langle M|$ where I is identity operator that operates on elements in register A and the projection operator $|M\rangle\langle M|$ operates on register B. This operation changes the above state, $|\Psi_2\rangle$, to

$$\begin{aligned}|\Psi_3\rangle = {} & C_0\sum_{x,y,xy=0}(|x\rangle|y\rangle)_A(\langle M|0\rangle|M\rangle)_B \\ & + C_1\sum_{x,y,xy=1}(|x\rangle|y\rangle)_A(\langle M|1\rangle|M\rangle)_B + \cdots \\ & + \cdots \\ & + C_M(|1\rangle|M\rangle + |P\rangle|Q\rangle + |Q\rangle|P\rangle) + |M\rangle|1\rangle)_A(\langle M|M\rangle|M\rangle)_B \\ & + \cdots \\ & + C_{2^n-1}\sum_{x,y,xy=2^n-1}(|x\rangle|y\rangle)_A(\langle M|2^n-1\rangle|M\rangle)_B\end{aligned}$$

such that $\sum_{i=0}^{2^n-1}|C_i|^2 = 1$. As this operation being non-unitary, it has some probability of failing. Assuming success in this non-unitary operation by some quantum dynamics we see that (using $\langle i|j\rangle = \delta_{ij}$, where $\delta_{ij} = 0$, if $i \neq j$, and $\delta_{ij} = 1$, if $i = j$,) the state, $|\Psi_3\rangle$, changes (after normalization) into the state $|\Phi\rangle$, where

$$|\Phi\rangle = \frac{1}{2}(|1\rangle|M\rangle + |P\rangle|Q\rangle + |Q\rangle|P\rangle) + |M\rangle|1\rangle)_A(|M\rangle)_B$$

(vii) The desired prime factors will then be revealed through partial measurement of any of the sub-registers A_1, A_2.

(vii) This changed state in register A now contains the desired prime factorization which is easily reveled after further partial measurement done on any one of the sub-registers A_1, A_2.

Remark: The efficiency of this algorithm depends upon the assumed " successful non-unitary operation" of projecting a superposition state onto a "known" state, $|M\rangle$, by some quantum dynamics in a reasonably less time. The result of projecting an $N = 2^n$-dimensional state $|\Psi\rangle$ onto a 1-dimensional basis state $|M\rangle$ leads us to the 1-dimensional basis state $|M\rangle$ scaled by the inner product $\langle M|\Psi\rangle$ i.e. we get the state $\langle M|\Psi\rangle|M\rangle$. Note that the inner product of two N-dimensional vectors can be obtained in $log(N)$ time [4].

4 An example

Suppose we are given a composite integer $M = 6 < 2^3 = 8$ as a product of two primes and our aim is

to find those prime factors of $M = 6$. We choose $n = 3$ and further prepare the so called domain register to contain the superposition of tensor product states $|x\rangle|y\rangle$, $0 \leq x, y \leq 2^3 - 1$, and the corresponding image register B will then contain the superposition of states $|xy\rangle$, where xy stands for product of x and y.

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 $\frac{1}{2^4}\sum_{x,y=0}^{(2^3-1)}|x\rangle|y\rangle$, where sub-registers A_1 and A_2 contain superposition $\frac{1}{\sqrt{2^3}}\sum_{x=0}^{(2^3-1)}|x\rangle$ and $\frac{1}{\sqrt{2^3}}\sum_{y=0}^{(2^3-1)}|y\rangle$, respectively. Thus, the state in register A will be
$\frac{1}{2^3}(|0\rangle|0\rangle + \cdots + |1\rangle|7\rangle + \cdots + |2\rangle|3\rangle + \cdots + |3\rangle|2\rangle + \cdots + |7\rangle|1\rangle + \cdots + |7\rangle|7\rangle)$.

(2) We prepare image register, B, to keep images the images of elements in register A produced under the action of the unitary transformation U_f. Thus: $U_f : (|x\rangle|y\rangle)_A(|0\rangle)_B \rightarrow (|x\rangle|y\rangle)_A(|xy\rangle)_B$. Since U_f can also operate on the superposition therefore we get the "sum" state:

$$\frac{1}{2^3}\sum_{x,y=0}^{(2^3-1)}(|x\rangle|y\rangle)_A(|0\rangle)_B \rightarrow \frac{1}{2^3}\sum_{x,y=0}^{(2^3-1)}(|x\rangle|y\rangle)_A(|xy\rangle)_B.$$

Thus, we will get the following entangled state, partly belonging to register A and partly to register B, as

$$\begin{aligned}|\psi_1\rangle = \frac{1}{2^3}[&(|0\rangle|0\rangle + |0\rangle|1\rangle + |0\rangle|2\rangle + \cdots + |0\rangle|7\rangle + \\ &|1\rangle|0\rangle + |2\rangle|0\rangle + |3\rangle|0\rangle + \cdots + |7\rangle|0\rangle)_A(|0\rangle)_B + \\ &(|1\rangle|1\rangle)_A(|1\rangle)_B + (|1\rangle|2\rangle + |2\rangle|1\rangle)_A(|2\rangle)_B + \\ &(|1\rangle|3\rangle + |3\rangle|1\rangle)_A(|3\rangle)_B + \cdots + \\ &(|1\rangle|6\rangle + |2\rangle|3\rangle + |3\rangle|2\rangle + |6\rangle|1\rangle)_A(|6\rangle)_B + \cdots + \\ &(|1\rangle|7\rangle + |7\rangle|1\rangle)_A(|7\rangle)_B + \cdots + \\ &(|2\rangle|4\rangle + |4\rangle|2\rangle)_A(|8\rangle)_B + (|3\rangle|3\rangle)_A(|9\rangle)_B + \\ &(|2\rangle|5\rangle + |5\rangle|2\rangle)_A(|10\rangle)_B + \\ &(|2\rangle|6\rangle + |3\rangle|4\rangle + |4\rangle|3\rangle + |6\rangle|2\rangle)_A(|12\rangle)_B + \\ &(|2\rangle|7\rangle + |7\rangle|2\rangle)_A(|14\rangle)_B + \cdots + \\ &(|6\rangle|7\rangle + |7\rangle|6\rangle)_A(|42\rangle)_B + (|7\rangle|7\rangle)_A(|49\rangle)_B].\end{aligned}$$

(3) We now apply a unitary operator $V = I \otimes U$ on $|\Psi_1\rangle$ where where I is identity operator which operates on elements in register A and the unitary operator $U = \sum_{z=0}^{7}|z\rangle\langle z|$ which operates on elements in register B produces the following new state, $|\Psi_2\rangle$:

$$\begin{aligned}|\psi_2\rangle = \frac{1}{2^3}[&(|0\rangle|0\rangle + |0\rangle|1\rangle + |0\rangle|2\rangle + \cdots + |0\rangle|7\rangle + \\ &|1\rangle|0\rangle + |2\rangle|0\rangle + |3\rangle|0\rangle + \cdots + |7\rangle|0\rangle)_A(|0\rangle)_B + \\ &(|1\rangle|1\rangle + |1\rangle|1\rangle)_A(|1\rangle)_B + (|1\rangle|2\rangle + |2\rangle|1\rangle)_A(|2\rangle)_B + \\ &(|1\rangle|3\rangle + |3\rangle|1\rangle)_A(|3\rangle)_B + \cdots + \\ &(|1\rangle|6\rangle + |2\rangle|3\rangle + |3\rangle|2\rangle + |6\rangle|1\rangle)_A(|6\rangle)_B + \cdots + \\ &(|1\rangle|7\rangle + |7\rangle|1\rangle)_A(|7\rangle)_B].\end{aligned}$$

(4) We further apply the non-unitary operator $W = I \otimes |6\rangle\langle 6|$ where I is identity operator that operates on elements in register A and the projection operator $|6\rangle\langle 6|$ operates on elements in register B. This will change state $|\Psi_2\rangle$ to the state $|\Psi_3\rangle$, where

$$\begin{aligned}|\psi_3\rangle = \frac{1}{2^3}[&(|0\rangle|0\rangle + |0\rangle|1\rangle + |0\rangle|2\rangle + \cdots + |0\rangle|7\rangle + \\ &|1\rangle|0\rangle + |2\rangle|0\rangle + |3\rangle|0\rangle + \cdots + |7\rangle|0\rangle)_A(\langle 6|0\rangle|6\rangle)_B + \\ &(|1\rangle|1\rangle)_A(\langle 6|1\rangle|6\rangle)_B + (|1\rangle|2\rangle + |2\rangle|1\rangle)_A(\langle 6|2\rangle|6\rangle)_B + \\ &(|1\rangle|3\rangle + |3\rangle|1\rangle)_A(\langle 6|3\rangle|6\rangle)_B + \cdots + \\ &(|1\rangle|6\rangle + |2\rangle|3\rangle + |3\rangle|2\rangle + |6\rangle|1\rangle)_A(\langle 6|6\rangle|6\rangle)_B + \cdots + \\ &(|1\rangle|7\rangle + |7\rangle|1\rangle)_A(\langle 6|7\rangle|6\rangle)_B].\end{aligned}$$

As this operation being non-unitary, it has some probability of failing. Assuming success in this non-unitary operation by some quantum dynamics in reasonably less time (using $\langle i|j\rangle = \delta_{ij}$, where $\delta_{ij} = 0$, if $i \neq j$, and $\delta_{ij} = 1$, if $i = j$,) the state, $|\Psi_3\rangle$, changes (after normalization) into the state $|\Phi\rangle$, where

$$|\Phi\rangle = \frac{1}{2}(|1\rangle|6\rangle + |2\rangle|3\rangle + |3\rangle|2\rangle) + |6\rangle|1\rangle)_A(|6\rangle)_B$$

This changed state in register A now contains the desired prime factors and they are easily reveled after the 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 useful discussion.

References

[1] 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 Com- puter Science, ed. S. Goldwasser, IEEE Computer Society, New York, pp. 124–134, (1994)

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

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

[4] Seth Lloyd, Masoud Mohseni, Patrick Rebentrost, Quantum algorithms for supervised and unsupervised machine learning, arXiv 1307.0411v2, quant-ph, (2013).

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.