iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** IX **Month of publication:** September 2018

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue IX, Sep 2018- Available at www.ijraset.com

Quantum Computing and Quantum Algorithms

Rishabh Bhatt[1], Rushikesh Gawande[2], Shreiya Indulkar[3]
[1, 2, 3]*B.E. Computer Engineering, VES Institute Of Technology,Mumbai-74*

Abstract: ***The size of transistors in the CPU is shrinking over time, making modern computers faster and more compact. Moore's law is the observation that the number of transistors in a dense integrated circuit doubles roughly every 2 years. But there is a limit to how small transistors can get. It is time we start planning for the end of Moore's Law and find alternate ways of faster computing. One such technology is Quantum Computing, which introduces the principles of Quantum mechanics in computing. It states that not only a bit can be 1 or 0 but also can be in a superposition state of both 1 and 0, this state is called as a coherent state which enables us to perform operation on two diverse value at the same time. Quantum bits are called as qubits and follow the property of quantum entanglement which means that the quantum state of each particle cannot be described independently of the state of the other but only as a whole. Quantum computers run on Quantum algorithm which are specifically designed for the sole purpose of Quantum computing. The most well-known Quantum algorithms is Shor's algorithm for factoring which can factor two numbers in polynomial time, whereas classical computers require exponential time for the same. Grover's search algorithm is another Quantum algorithm for searching an unstructured database or an unordered list much faster than its classical counterpart. Quantum computers increase the computing speed drastically but the problem of a largescale quantum computer still persists. The highest number which has been factorized using Shor's Quantum algorithm is just 21. Quantum computers are far from reality and it will many years to develop a large scale working quantum computer. This paper discusses basic concepts of quantum computing like qubits, superposition, entanglement, decoherence and an introduction to Shor's and Grover's Quantum algorithm briefly***

Keywords: Quantum computing, Quantum algorithm, Decoherence, Shor's, Grover's, qubits

I. INTRODUCTION

Moore's law is the observation that the number of transistors in a dense integrated circuit doubles roughly every 2 years [1]. This could mean up to a hundredfold increase in transistor count per chip within a decade which means more computer processing power and faster calculations. Shrinking transistors have powered 50 years of advances in computing—but now other ways must be found to make computers more capable as shrinking the size transistors keeps on becoming more difficult as we are headed to the future Processor's speed can also be improved by overclocking it using liquid nitrogen cooling techniques [2]. But the increase in speed from CPU cooling techniques is insignificant. Quantum computing is a different approach from traditional computing. Quantum Computation was first thought of by Richard Feynman in 1982 who said that by using the quantum mechanical effects, faster computation can be achieved [3]. Classical computers are unable to simulate speed of Quantum computers. Quantum computers exploit the unique, non-classical properties of the quantum systems from which they are built, allowing them to process exponentially large quantities of information in only polynomial time. The most widely known development in quantum computation was Peter Shor's 1997 publication of a quantum algorithm for performing prime factorization of integers in essentially polynomial time [4]. Shor's algorithm is one of the few quantum algorithms whose result is obtained as a numeric value. This algorithm could factor a 512-bit product in about 3.5 hours with 1 GHz clock rate [5], whereas the number field sieve could factor the same product in 8400 MIPS years [6]. (One MIPS year is the number of instructions that a processor can execute in a year, at the rate of millions of instructions per second.) Another famous quantum algorithm is a database search algorithm proposed by Lov Grover that will find a single item from an unsorted list of N elements with $O(\sqrt{N})$ time [7]. We know that when classical computers are used for computation, the speed can be improved by using parallelism. This aids in reducing the running time. However, this exponential reduction in time can only be achieved if we augment the number of processors exponentially. This requires an exponential increase in the physical space as well. When contrasted with quantum systems, parallelism is exponentially increased with the linear increase in the size of the system. Parallelism is inbuilt in quantum systems because of the properties it inherits. Thus, Quantum computer enable faster computing capability than its classical counterpart.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue IX, Sep 2018- Available at www.ijraset.com

II. BASIC PRINCIPLE OF QUANTUM COMPUTER

A. Superposition State

In classical computers, electrical signals such as voltages represent the 0 and 1 states as one-bit information. Two bits indicate four states 00, 01, 10, and 11, and n bits can represent 2^n states. In the quantum computer, a quantum bit called "qubit" which not only can be 1 or 0 but also can be in a superposition state of both 1 and 0, this state is called as a coherent state. For instance, instead of an electrical signal in classical computers, an electron can be used as a qubit. The spin-up and spin-down of an electron represent two states: 0 and 1, respectively. A photon can also be used as a qubit, and the horizontal and vertical polarization of a photon can be used to represent both states. Using qubits and quantum algorithms quantum computers can perform arithmetic and logical operations . The important difference, however, is that one qubit can also represent the superposition of 0 and 1 states. When we represent 0 and 1 states as state vectors $|0\rangle$ and $|1\rangle$ respectively, such a superposition state is expressed as a linear combination of $|0\rangle$ and $|1\rangle$, $|\psi\rangle=a|0\rangle+b|1\rangle$. The symbol "$|\rangle$" is called 'ket-vector' in Dirac notation, whereas the coefficients a and b are called probability amplitudes. $|a|^2$ indicates a probability that we get $|\psi\rangle=|0\rangle$ as a result of the measurement on the qubit $|\psi\rangle=a|0\rangle+b|1\rangle$. They also satisfy $|a|^2+|b|^2=1$. For example, when the probability amplitudes a and b are equal to $1/\sqrt{2}$, we can express a superposition state of two states as follows: $|\psi\rangle=(1/\sqrt{2})|0\rangle+(1/\sqrt{2})|1\rangle$, where vectors $|0\rangle=(1, 0)^T$ and $|1\rangle= (0, 1)^T$.

In short, when we measure a state of $|\psi\rangle$, the state will be observed as $|0\rangle$ with probability $(1/\sqrt{2})^2=1/2$ and as $|1\rangle$ with probability $(1/\sqrt{2})^2=1/2$

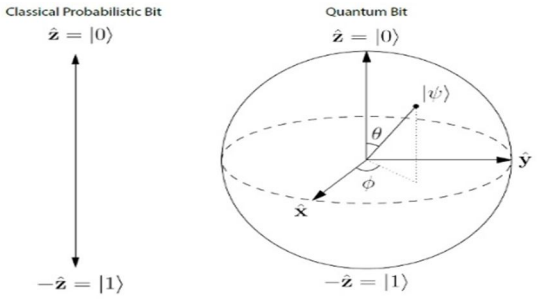


Figure 1: Classical Probabilistic bit and Quantum bit

B. Quantum Logic Gates

In classical computing, logic gates are used to perform arithmetic and logical operations. The binary values are stored in a register which provide input to these gates and produce a binary output. Boolean algebra is used to describe classical logic gates mathematically. In a similar way, quantum computers use quantum logic gates, these gates are applied to a quantum register which map the quantum superposition to another, together allowing the evolution of the system to some desired final state, a correct answer. Quantum logic gates can be represented mathematically as transformation matrices, or linear operators which are applied to a quantum register by tensoring the transformation matrix with the matrix representation of the register. All linear operators that are used in quantum logic gates must be unitary. Unitary transformations performed on a single qubit may be visualized as rotations and reflections about the x, y, and z axes of the Bloch sphere. All the possible linear combinations $a|0\rangle+b|1\rangle$ correspond to all the points (θ, ψ) on the surface of the unit sphere, where $a=\cos(\theta/2)$ and $b=e^{i\Theta}\sin(\theta/2)$.

$$|\psi\rangle = a|0\rangle+b|1\rangle$$
$$= \cos(\theta/2)\,|0\rangle+ e^{i\Theta}\sin(\theta/2)\,|1\rangle$$
$$= \cos(\theta/2)\,|0\rangle+(\cos\emptyset +i*\sin\emptyset)\sin(\theta/2)\,|1\rangle \qquad (1)$$

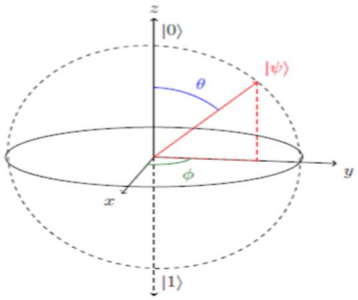


Figure 2: The Bloch sphere

While circuit diagrams are useful in understanding the flow of operation in quantum algorithms and picture how they work to obtain the solution to a problem, the Bloch sphere is used as an intuitive remainder of the underlying implementations that separates quantum computers from its classical counterpart. The Bloch sphere geometrically represents the pure state space of a two-level quantum mechanical system as shown in Figure 2. In an actual quantum computer, the wire of a circuit diagram may correspond to a single electron moving through time while each gate represents a change in movement of that electron. As quantum gates are tightly coupled to their underlying quantum mechanical systems, it is important to know how these gates are evolving the quantum system to obtain the desired result.

C. Entangled States

Along with superposition, Quantum bits experience a phenomenon called as quantum entanglement, which means that the quantum state of each particle cannot be described independently of the state of the other but only as a whole. This is a phenomenon which hold true exclusively for quantum computers and not classical computers. If one system is measured, entanglement makes it possible to conclude the measurement of the other system. This is done when no measurement has been applied on the second system. An entangled state can be fashioned by allowing a qubit to pass a Hadamard gate and then a CNOT gate [12]. It is because of the entangled states that exponential growth in state spaces is accomplished. A limitation is that to mimic for a small quantum system, it requires large resources on a traditional computer.

D. Quantum Computer Simulators

It will take many more years before quantum gates are available for the computer scientist/engineer to use. Meanwhile, we require a quantum computer simulator to find new algorithms. Vectors and matrices can be used to represent quantum computer simulators mathematically. When we define $|0\rangle=(1, 0)^T$ and $|1\rangle= (0, 1)^T$, a NOT operation for one qubit can be expressed with 2×2 unitary matrices as:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} |0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$$

We can represent an operation that an initial condition $|1\rangle$ is converted to a superposition state $(1/\sqrt{2})|0\rangle+(1/\sqrt{2})|1\rangle$ by using a matrix:

$$H \cdot |1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$
$$= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

This operation is known as Hadamard transformation
[10].

Multiple qubits can be represented as a tensor product of two vectors $|0\rangle$ and $|1\rangle$ .For example, two qubit resisters are represented as follows:

$$|00\rangle = |0\rangle \otimes |0\rangle = (1\ 0\ 0\ 0)^T, \quad |01\rangle = |0\rangle \otimes |1\rangle = (0\ 1\ 0\ 0)^T$$

$$|10\rangle = |1\rangle \otimes |0\rangle = (0\ 0\ 1\ 0)^T, \quad |11\rangle = |1\rangle \otimes |1\rangle = (0\ 0\ 0\ 1)^T$$

The controlled-NOT operation is:

$$|00\rangle \rightarrow |00\rangle, \quad |01\rangle \rightarrow |01\rangle, \quad |10\rangle \rightarrow |11\rangle, \quad |11\rangle \rightarrow |10\rangle$$

The first bit is called the controlled bit and the second bit is the target bit. A unitary matrix of controlled-NOT operations for two qubits is represented as:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Thus, by using the vectors and unitary matrices we can simulate theoretical quantum computer mathematically.

E. Decoherence Of Qubits

The loss of quantum coherence is called as Quantum decoherence. In quantum mechanics, electrons represent the state of a system. Quantum coherence is a fundamental property of the quantum particles and is essential for the functioning of a quantum computer. But, when the quantum system is not perfectly isolated coherence decays with time. That is because superpositions of states are generally very unstable, and will collapse into one of the pure states $|0\rangle$ or $|1\rangle$ quickly as a result of interactions with the environment. Decoherence time is the time remaining before the state of a qubit is completely destroyed. The whole process is known as decoherence. The decoherence time is an extremely important factor when considering practical implementations of quantum computers. To build a quantum computer that works, we will have to design the system in such a way that environmental effects are minimized as much as possible so as to increase the decoherence time. A reasonable amount of calculations should be carried out on a qubit before it decoheres.

III. QUANTUM ALGORITHMS

A. Shor's quantum method for factorising

Cryptography is used to encode the secret transactions of banks, governments, and the military. The encryption method widely employed is a DES (data encryption standard) based on RSA. RSA is named after its inventors Ronald Rivest, Adi Shamir, and Leonard Adleman [Rivest et al., 1978] and is a public key encryption system[8]. The success of RSA depends on the seeming intractability of the problem of finding the prime factors of very large integers.

The problem of factoring numbers becomes exponentially harder the larger they are. However, Shor [4] outlined a quantum algorithm that would factorize RSA-129 in a few seconds, if we could build a quantum computer that ran as fast as a modem PC.

The 'many universes' interpretation is used by Shor in his quantum computing method for extracting prime factors of very large integers, in which a memory register is placed in a superposition of all possible integers it can contain which is followed by a different calculation being performed in each 'universe'. The computation halts when the different universes 'interfere' with each other as repeating sequences of integers are found in each universe and across universes. Although there is no guarantee that the results are correct, a subsequent check can be made at this point to identify whether the numbers returned are indeed prime factors of the given large integer.

To factor a number n (the product of two primes),

specify an arbitrary number of parallel universes p(0, 1, 2, ...), and randomly select an integer x between 0 and n. Then, in every universe, raise 1:to the power of the number of the universe. Divide by n and store the remainder in the universe. For the next number in the sequence for a universe, 1: is raised to the power of the number last stored, divided by n, and the remainder stored. This continues in each universe to form a repeating sequence.

For the sake of exposition, let n (the number to

be factored into prime factors) be 33. Let $2 = 7$ $(0 < 2 < n)$ and $p = 17$. Consider u_2 and $u_{5:}$

u_2: $7^2 \bmod 33 = 16$, $7^{16} \bmod 33 = 4$, $7^4 \bmod 33 = 25$, $7^{25} = \bmod 33 = 10$, $7^{10} \bmod 33 = 1$, etc.

u_5: $7^5 \bmod 33 = 10$, $7^{10} \bmod 33 = 1$, $7^l \bmod 33 = 7$, $7^7 \bmod 33 = 28$, $7^{28} \bmod 33 = 31$, etc.

The frequency of repeat across universes, the vertical frequency, v*f*, is 10, and this can be seen if we examine u_o and u_{1O}, u_1 and u_{11}, u_2 and u_{12} and so on. That is, in each of these universes the repeating frequency starts at the same point and repeats the same numbers. While other universes share the repeating pattern, they do not share the common starting point. This is the quantum computation equivalent of standing waves in each universe: a repetition of numerical values. We now perform the calculation $x^{vf/2} - 1$, where 'x' is the arbitrarily chosen number between 0 and n and v^f is the frequency of common repeating patterns across universes. This gives us $7^{10/2} - l \pmod{33}$, which is 9. Now, finding the greatest common divisor of 9 and 33 gives one of the factors, i.e. 3.

Shor's method is not guaranteed to always work, and if the derived number turns out not to be a prime factor of n, the procedure is repeated using a different 'x'. It is claimed that on average only a few trials will be required to factorize n, even when n is very

large. So, although there are no known fast classical algorithms for factorizing large numbers into primes, Shor's method uses known fast algorithms for taking a candidate prime factor of n and determining whether it is in fact a prime factor.

B. Grover's Algorithm

Grover's algorithm performs a search over an unordered set of $N = 2^n$ items to find the unique element that satisfies some condition. While the best classical algorithm for a search over unordered data requires O(N) time [9], Grover's algorithm performs the search on a quantum computer in only $O(\sqrt{N})$ operations, a quadratic speedup.

Grover's search algorithm is a good introduction to quantum algorithms because it demonstrates how the qualities of quantum systems can be implemented for improving the lower runtime bounds of classical algorithms. For achieving such a speed, Grover algorithm relies on the quantum superposition of states. Similar to many quantum algorithms, Grover's algorithm begins by putting the machine into an equal superposition of all possible 2^n states of the n-qubit register. All these possible states correspond to all the possible entries in Grover's database, and so we start by assigning equal amplitudes to each element in the search space, every element can be considered at once in a quantum superposition, and their amplitudes can be manipulated to produce the correct entry in the database with a probability of at least ½ [7]. The circuit diagram for Grover's search is shown in Figure 3.

Grover's algorithm is summarized nicely in [10] as follows:

1) Input

a) A quantum Oracle *O* which performs the operation $O|x\rangle=(-1)^{f(x)}|x\rangle$, where $f(x)=0$ for all $0<x<2^n$ except x^0, for which $f(x_0)=1$.

b) n qubits initialized to the state $|0\rangle$

2) *Output:* x_0

3) *Runtime:* $O(\sqrt{2^n})$ operations, with O(1) probability of success.

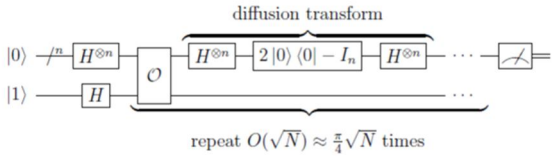


Figure 3: Circuit diagram for Grover's algorithm, with a scratch qubit for the oracle [11].

IV. CURRENT DEVELOPMENT IN QUANTUM COMPUTING

Quantum computers increase the computing speed drastically but the problem of a largescale quantum computer still persists. The highest number which has been factorized using a Shor's Quantum algorithm is just 21 and the circuit had to be hardwired for just factorizing the number 21.

More research is needed in this field which is only possible via simulation on quantum computers using classical computers. These simulations must be able to handle quantum computers which are operating on very large number of qubits. These theoretical quantum computers simulators are used to perform highly idealized unitary operations. Whereas, unitary operations on an actual quantum computer are much more complex. Thus, another type of quantum computer simulator has been developed as an emulator of quantum computer hardware [13].

A quantum-dot-based quantum computer uses spins [14] or energy levels [15] of electrons confined in quantum dots (QDs) as qubits that are fabricated in semiconductor materials. Because we can control states of qubits electrically, as we do in classical circuits, this scheme has an advantage because current semiconductor technology may be applied to the fabrication of a quantum computer.

Another recent development is the study of quantum communication complexity. If two people share quantum entanglement, as well as a classical communications channel, this permits them to send each other qubits, but does not reduce the number of bits required for transmission of classical information. However, if they both have some classical data, and they wish to compute some classical function of this data, shared quantum entanglement may help reduce the amount of purely classical communication required to compute this function. This was first shown by Cleve and Burhman [16].

V. ACKNOWLEGEMENT

We, want to convey thanks to Mrs. Priya R.L, Assistant Professor, VES Institute Of Technology for guiding us during this research paper and suggesting necessary changes in the paper.

VI. CONCLUSION

In this paper we have reviewed the principles, algorithms of quantum computing along with the concept of qubits and the gates used for its implementation. The realization of a practical quantum computer is expected before we encounter the limit of Moore's law with respect to improvements that may be possible using the classical computer model.

We have seen how quantum computers use qubits which are in a superposition states of 1 and 2 and how quantum algorithm works by putting the machine into an equal superposition of the states. Due to this property of coherence of quantum bits, quantum computers can achieve higher speeds which their classical counterparts cannot. One of the major problems faced by quantum computers is the decoherence of coherent state. It simply means that the qubits cannot be in the superposition state for a longer period of time and will collapse to the pure states of either 1 or 0.

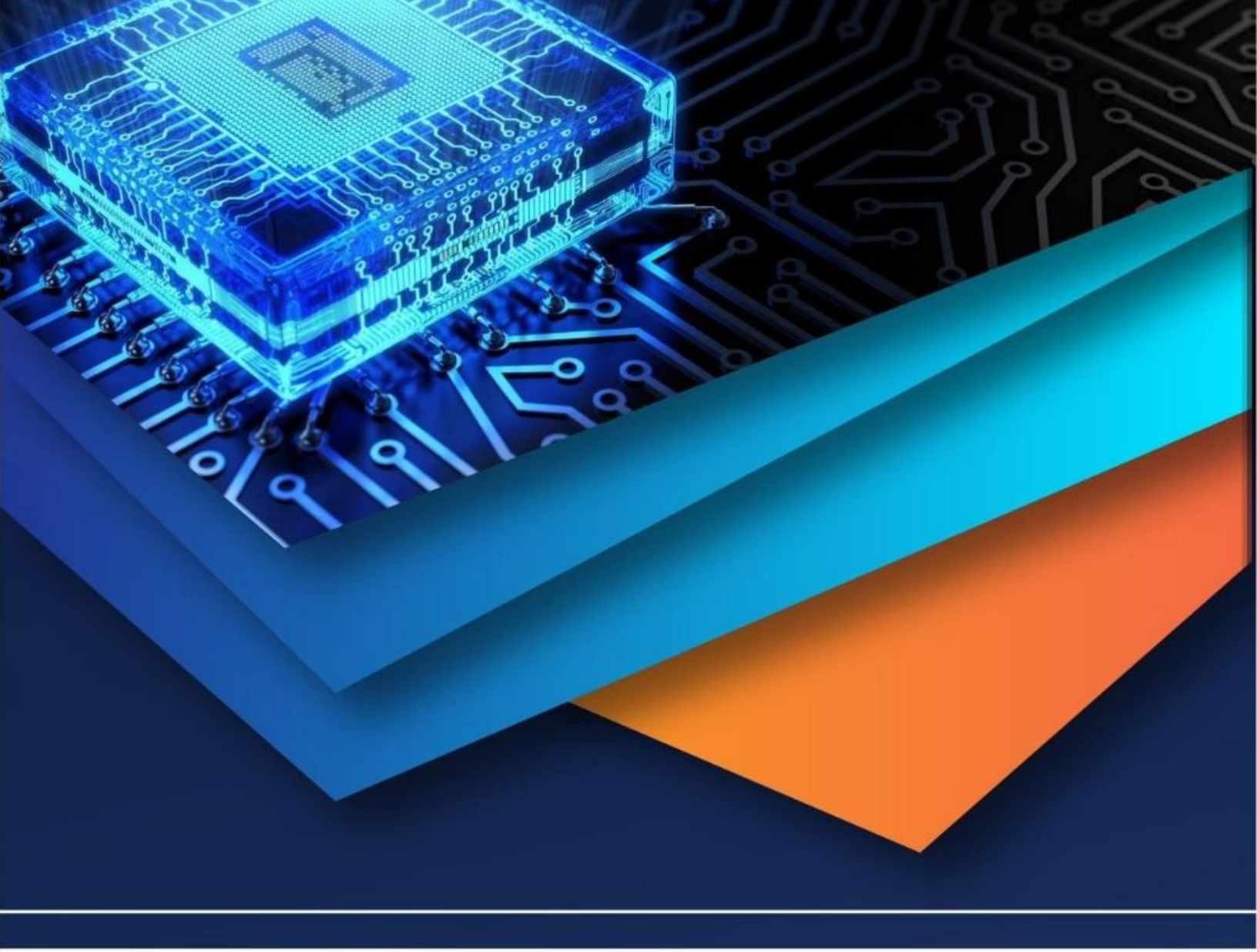
A brief introduction about Shor's factoring algorithm is given in this paper. Shor's algorithm is able to factorize a number in polynomial time whereas classical computer requires exponential time for the same. Groover's search algorithm is another quantum algorithm which is used to perform a search over an unordered set of items to find the unique element that satisfies some condition, with $O(\sqrt{N})$ complexity.

Even quantum programming languages have been proposed which will help us to program quantum computers and tackle quantum computers problems in an abstract manner. [17–18].

The current challenge hold in not only building a quantum computer right away but also to be able to perform experiments in which we can control various quantum phenomenon and not only just observe them. Obviously, this mind-boggling level of computing power has enormous commercial, industrial, and scientific applications, but there are some significant technological and conceptual issue to resolve first.

REFERENCES

[1] Moore, Gordon E. (1965-04-19). "Cramming more components onto integrated circuits". Electronics. Retrieved 2016-07-01.J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.
[2] D.M. Carlson, D.C. Sullivan, R.E. Bach, D.R. Resnick, "The ETA 10 liquid-nitrogen-cooled supercomputer system," IEEE Transactions on Electron Devices (Volume: 36, Issue: 8, Aug 1989).
[3] R. P. Feynman, "Simulating Physics with Computers," International Journal of Theoretical Physics, vol. 21, no. 6/7, pp. 467-488, 1982.
[4] P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," SIAM Journal on Computing, no. 5, p. 1484.
[5] M. Oskin, F.T. Chong, & I. Chuang, "A practical architecture for reliable quantum computers" , IEEE Computer, January 2002, 79–87.
[6] B. Preneel (Ed.), "Factorization of a 512-bit RSA modules" , Lecture Notes in Computer Science, Vol. 1807 (Berlin: Springer-Verlag, 2000).
[7] L.K. Grover, "A fast quantum mechanical algorithm for database search" , Proc. STOC, Philadelphia, 1996, 212–219.
[8] [Rivest et al., 1978] Rivest, R. L., Shamir, A., and Adleman, L. (1978). "A method for obtaining digital and public-key cryptosystems". Communications of the ACM, 21(2).
[9] J. Marko (2010) Quantum Computing Reaches for True Power. New York Times. (Accessed 3 January, 2011). [Online]. Available: http://www.nytimes.com/2010/11/09/science/09compute.html.
[10] M. A. Nielsen and I. L. Chuang, "Quantum Computation and Quantum Information." New York, New York, USA: Cambridge University Press, 2000.
[11] J. C. Benoist. Quantum circuit representation of Grover's algorithm. Wikimedia, Inc. (Accessed 5 January, 2011). [Online]. Available: http://en.wikipedia.org/wiki/File:Grovers_algorithm.svg.
[12] M. A. Nielson and I. L. Chuang. 2000. "Quantum Computation and Quantum Information". Cambridge University Press.
[13] H. De Raedt, A.H. Hams, K. Michielsen, & K. De Raedt, "Quantum computer emulator", Computer Physics Communications, 132(1–2), 2000, 1–20.
[14] D. Loss & D.P. DiVincenzo, "Quantum computation with quantum dots", Physical Review A, 57, 1998, 120–126.
[15] M.S. Sherwin, A. Imamoglu, & T. Montroy, Quantum computation with quantum dots and terahertz cavity quantum electrodynamics, Physical Review A, 60, 1999, 3508–3514.
[16] R. Cleve and H. Burhman, Substuting quantum entaglement for communication,Phys. Rev. A 56 (1997),1201-1204.
[17] J.W. Sanders & P. Zuliani, Quantum programming, Mathematics of program construction, Lecture Notes in Computer Science, 1837 (Heidelberg: Springer Verlag, 2000), 80–99.
[18] B. Omer, Classical concepts in quantum programming, Quantum Structures, 2002, http://arxiv.org/abs/quant-ph/0211100.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY