International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2020 IJSRCSEIT | Volume 6 | Issue 3 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/IJSRCSEIT

Quantum Computers for Next Generation

Prof. Nagaraj Telkar[1] , Prof. Pavankumar Naik[2] , Akash Mabali[3], Girish S H[4], Gurusiddeshwar S H [5], Sahana Balikai[6]

[1,2,3,4,5,6] Department of Computer Science and Engineering, SKSVMACET Laxmeshwar, Karnataka, India

ABSTRACT

Computers reduce human effort and also focus on increasing the performance to push the technology forward. Many approaches have been devised to increase the performance of the computers. One such way is to reduce the size of the transistors used in the systems. Another very significant tactic is to use quantum computers. It proved to be very effective when used to factor large numbers. It was found that it could decrypt codes in 20 minutes which took billions of years with classical computers. This was a great motivation for focusing on this topic. A quantum computer allows a `quantum bit' or qubit to have three states - 0, 1, and 0 or 1. The last state is the coherent state. This enables an operation to be performed on two diverse values at the same time. However, this brings out a problem of decoherence. It becomes difficult to perform the computation using quantum computers. A quantum computer is desired to have five capabilities - scalable system, initialized state, long decoherence time, universal set of quantum gates, high efficiency measurements. Architecture of the quantum computer is the new research area. It is affected by quantum arithmetic, error management, and cluster-state computing. Without it, the quantum algorithms would not prove to be as efficient. To fully utilize the power of a quantum computer, the algorithms used should be based on quantum parallelism.

Keywords : Transistors, Quantum, Quantum Bit (Qubit) , Parallelism , Algorithm.

I. INTRODUCTION

The development of science and technology, leading to the advancement of civilization, new ways were discovered exploiting various physical resources such as materials, forces and energies. The history of computer development represents the culmination of years of technological advancements beginning with the early ideas of Charles Babbage and eventual creation of the first computer by German engineer Konard Zeise in 1941. The whole process involved a sequence of changes from one type of physical realization to another from gears to relays to valves to transistors to integrated circuits to chip and so on. Surprisingly however, the high speed modern computer is fundamentally no different from its gargantuan 30 ton ancestors which were equipped with some 18000 vacuum tubes and 500 miles of wiring. Although computers have become more compact and considerably faster in performing their task, the task remains the same: to manipulate and interpret an encoding of binary bits into a useful computational result [1].

The number of atoms needed to represent a bit of memory has been decreasing exponentially since 1950. An observation by Gordon Moore in 1965 laid the foundations for what came to be known as “Moore’s Law” – that computer processing power doubles every eighteen months. If Moore’s Law is extrapolated naively to the future, it is learnt that sooner or later, each bit of information should be encoded by a physical system of subatomic size [2].

Today’s computers are classical, a fact which is actually not entirely obvious. A basis of modern

computers rests on semiconductor technology. Transistors, which are the "neurons" of all computers, work by exploiting properties of semiconductors [10]. Classical computers are in a certain, restricted, sense quantum mechanical, because, as far as we understand today, everything is quantum mechanical. No, classical computers, although based on quantum physics, are not fully quantum, because they do not use "quantumness" of matter at the information-theoretical level, where it really matters.

II. LITERATURE REVIEW

Literature survey or study is an important phase of any system development process. Literature survey is the process of gathering and interpreting facts, diagnosing problems and using the information to recommend improvements on the system.

In [1], published by Michael Nielsen in 2011, worked on the "Quantum Computation and Quantum Information" and proposed a theory at Cambridge University Press.

In [2], published by Peter Shor in 2013, Designed an algorithms for the quantum computers to cope up with as "Algorithms for Quantum Computation: Discrete Logarithms and Factoring." Proceedings of the 35th Annual Symposium on Foundations of Computer Science

In [3], published by R. Feynman in 2014 developed an Simulating Physics with computers.

In [4], published by P. Benioff in 2015, made the performance analysis of computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines.

In [5], published by D. Deutsch in 2015, came out with the "Quantum theory, the Church–Turing principle and the universal quantum computer".

In [6], published by A. Berthiaume, D. Deutsch, and R. Jozsa, in 2016, came out with "The stabilisation of quantum computations", in Proceedings of the Workshop on Physics of Computation: PhysComp '16, IEEE Computer Society Press, Los Alamitos, CA

In [7], published by C. Bennett, E. Bernstein,G. Brassard, and U. Vazirani in 2016, says that "Strengths andweaknesses of quantum computing".

Thus , by comparing all literature surveys, There has been an effort in making a physical and completely working model of a Quantum Computer.

III.QUANTUM MECHANICS

The Quantum mechanics is generally about the novel behaviour of very small things. At this scale matter becomes quantized, this means that it can't be subdivided no more. Quantum mechanics has never been wrong, it explains why the stars shine, how matter is structured, the periodic table, and countless other phenomena [10].

The following are main parts of quantum mechanics that are important for quantum computing

A. Superposition

Superposition means a system can be in two or more of its states simultaneously. For example a single particle can be traveling along two different paths at once. This implies that the particle has wave-like properties, which can mean that the waves from the different paths can interfere with each other. Interference can cause the particle to act in ways that are impossible to explain without these wave-like properties. The ability for the particle to be in a superposition is where we get the parallel nature of quantum computing: If each of the states corresponds to a different value then, if we have a superposition

of such states and act on the system, we effectively act on all the states simultaneously.

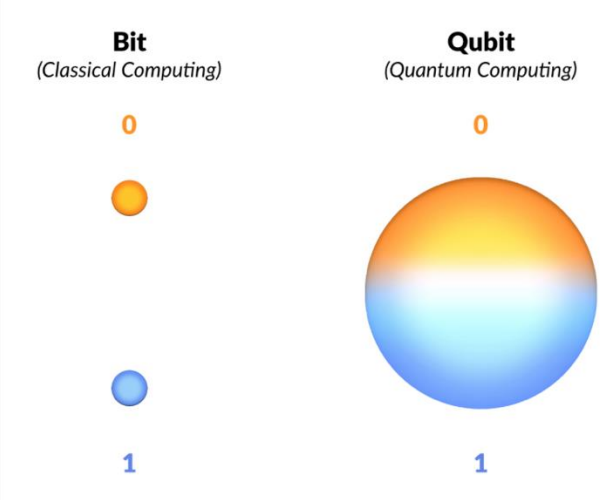


Figure III.A.I Superposition of Computing Bits

B. Uncertainty

The quantum world is irreducibly small so it's impossible to measure a quantum system without having an effect on that system as our measurement device is also quantum mechanical. As a result there is no way of accurately predicting all of the properties of a particle. There is a trade off - the properties occur in complementary pairs (like position and momentum, or vertical spin and horizontal spin) and if we know one property with a high degree of certainty then we must know almost nothing about the other property. That unknown property's behavior is essentially random. An example of this is a particle's position and velocity: if we know exactly where it is then we know nothing about how fast it is going. This indeterminacy is exploited in quantum cryptography.

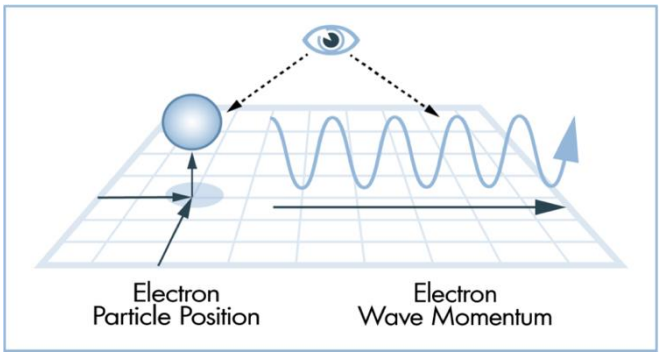


Figure III.B.I Uncertainty Principle

C. Entanglement

In 1935 Einstein (along with colleagues Podolski and Rosen) demonstrated a paradox (named EPR after them) in an attempt to refute the undefined nature of quantum systems. The results of their experiment seemed to show that quantum systems were defined, having local state BEFORE measurement. Although the original hypothesis was later proven wrong (i.e. it was proven that quantum systems do not have local state before measurement). The effect they demonstrated was still important, and later became known as entanglement. Entanglement is the ability for pairs of particles to interact over any distance instantaneously.

Particles don't exactly communicate, but there is a statistical correlation between results of measurements on each particle that is hard to understand using classical physics. To become entangled, two particles are allowed to interact; they then separate and, on measuring say, the velocity of one of them (regardless of the distance between them), we can be sure of the value of velocity of the other one (before it is measured).

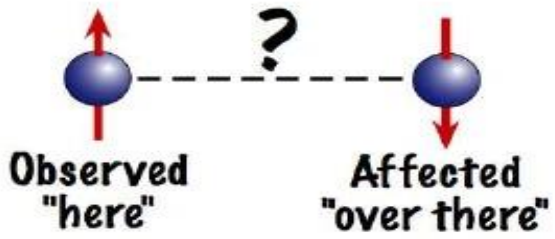


Figure III.C.I Entanglement of Particles

IV. QUANTUM COMPUTERS

Quantum Computing is the use of quantum-mechanical phenomena such as superposition, entanglement and computation. A quantum computer is used to perform such computation, which can be implemented theoretically or physically. There are currently two main approaches to physically implementing a quantum computer: analog and digital. Analog approaches are further divided into Quantum Simulation, Quantum Annealing, and Adiabatic Quantum Computation. Digital Quantum Computers use quantum logic gates to do computations. Both approach uses quantum bits or qubits.

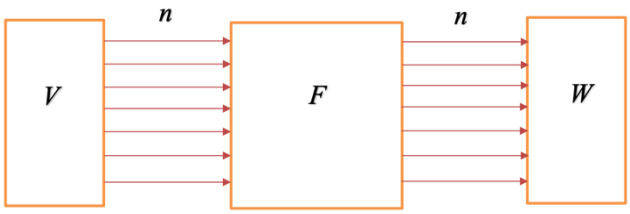


Figure IV.I Basic Quantum Architecture

A quantum computer looks like this, taking n input qubits, the register V, and producing n output qubits, the register W. The input register can be prepared as a superposition of states,

e.g. an equal superposition of all integers from 0 to 2n:

$$v = \sum_{i=0}^{2n} 1/n\sqrt{2}\,(|0_i> + |1_i>)$$

A. What Quantum Computers can do?

The biggest success so far -- and the event which ignited the current explosive growth of the field of quantum computing -- was Peter Shor's 1994 discovery of an efficient quantum algorithm for finding the prime factors (factoring) of large integers[8].

By making clever use of superposition's, interference, quantum parallelism, and some classical number theory, Shor's algorithm finds a factor of a number N in time roughly the square of the length of the input (which is log N bits). In contrast, every known classical algorithm requires exponential time to factor. Since factoring is one of the most elementary aspects of number theory, the oldest mathematical discipline, and centuries of efforts by the greatest mathematicians have not yielded better methods, it is widely believed that such better methods either do not exist or are prohibitively difficult to find.

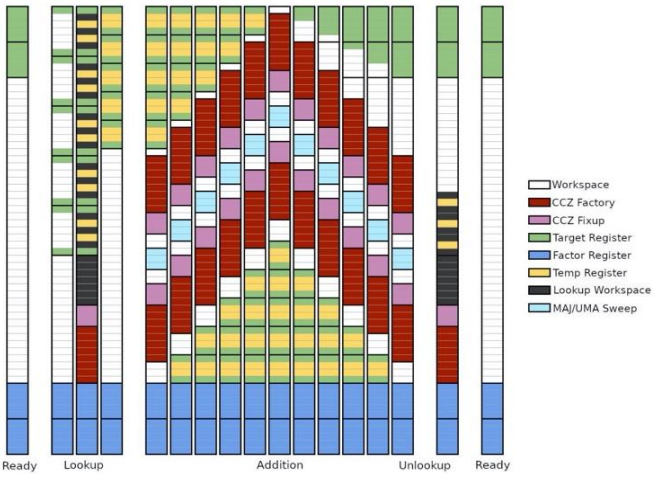


Figure IV.A.I Register Assignment

B. How Quantum Computer do it?

The above results are very promising, but so far mostly theory. How about actually building quantum computers which can run the fast algorithms like Shor's, Grover's, or CWI's? To date only very small quantum algorithms (and slightly bigger quantum crypto devices) have been implemented, but the physical realization of quantum computers is still in its infancy [9]. The main problem is that quantum superpositions are extremely vulnerable and any interactions with its environment will quickly cause errors, which degrade the performance of the computer.

Quantum versions of error-correcting codes have been developed recently which to a large extent solve this problem in theory, but not yet in the brittle practice of the physical lab (let alone the brittle practice of our desktops). This is related to development of Quantum Information Theory--the quantum extension of classical information theory.

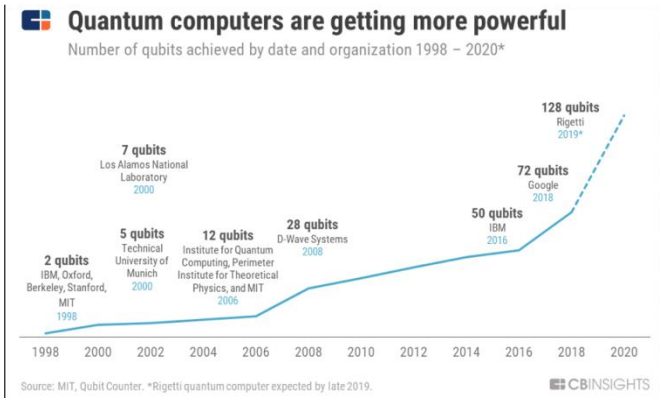


Figure IV.B.I Power in terms of Q-Bits

A simple scheme would be for Alice to send her x to Bob and then let Bob do all the work by himself, but this may take a lot of bits of communication and often there are much more clever schemes requiring less communication. The field of communication complexity examines the optimal number of bits that have to be communicated in order to compute the function at hand. What happens if we generalize this setting to the quantum world and allow Alice and Bob the use of quantum computers and qubit-communication?

C. Comparison of Classic and Quantum Computers

Classical computing relies, at its ultimate level, on principles expressed by Boolean algebra, operating with a (usually) 7-mode logic gate principle, though it is possible to exist with only three modes (which are AND, NOT, and COPY). Data must be processed in an exclusive binary state at any point in time - that is, either 0 (off / false) or 1 (on / true).

Point of Comparison	Classical Computing	Quantum Computing
Information Representation	A Bit: Either 0 or 1	A qubit: a superposition of 1 and 0
Number of Simultaneous Calculations	1	Multiple
Method of Calculations	Moving bits through logic gates	Altering State of Atoms
Information Delivered	Information can be copied without being disturbed	Information cannot be copied or read
Information Behavior	One Single Direction	Spread out to many routes simultaneously like waves.
Noise Tolerance	High: Information Carried in a	Low: Delivery Channel

	noisy way	needs to be noiseless.
Security	Lower: Eavesdropper can break into the communication with high computing power.	Higher: Any interruption in the communication will be detected by the communicating parties.
Computation/Computation Cost	Higher as communication volume increases.	Lower as communication volume increases.

V. ELEMENTS OF QUANTUM COMPUTERS

The basic element of quantum computing includes the Qubits, the Quantum Gates[12].

A. Qubits

The qubit is the quantum analogue of the bit, the classical fundamental unit of information [20]. It is a mathematical object with specific properties that can be realized physically in many different ways as an actual physical system. Just as the classical bit has a state (either 0 or 1), a qubit also has a state. Yet contrary to the classical bit, 0 and 1 are but two possible states of the qubit, and any linear combination (superposition) thereof is also physically possible. In general, thus, the physical state of a qubit is the superposition

$$\psi = \alpha 0 + \beta 1$$

(Where α and β are complex numbers). The state of a qubit can be described as a vector in a two-dimensional Hilbert space, a complex vector space. The special states 0 and 1 are known as the computational basis states, and form an orthonormal basis for this vector space. According to quantum theory, when we try to measure the qubit in this basis in order to determine its state, we get either 0 with probability $\alpha 2$ or 1 with probability $\beta 2$.

Since $\alpha 2 + \beta 2 = 1$ (i.e., the qubit is a unit vector in the aforementioned two-dimensional Hilbert state), we may (ignoring the overall phase factor) effectively write its state as $\psi = \cos(\theta)0 + e^{i\varphi}\sin(\theta)1$, where the numbers θ and φ define a point on the unit three-dimensional sphere.

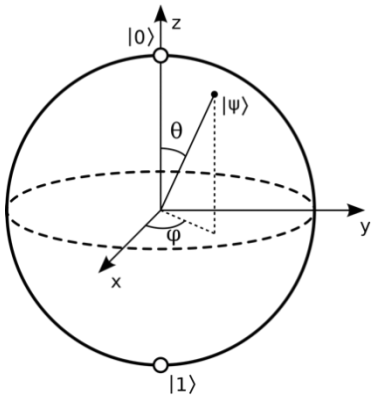


Figure V.I Blob Sphere Representation

B. Quantum Gates

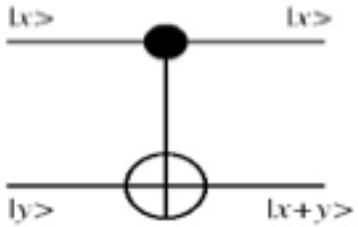
Classical computational gates are Boolean logic gates that perform manipulations of the information stored in the bits. In quantum computing these gates are represented by matrices, and can be visualized as rotations of the quantum state on the Bloch sphere. This visualization represents the fact that quantum gates are unitary operators, i.e., they preserve the norm of the quantum state (if U is a matrix describing a single qubit gate, then U†U=I, where U† is the ad joint of U, obtained by transposing and then complex-conjugating U).

As in the case of classical computing, where there exists a universal gate (the combinations of which can be used to compute any computable function), namely, the NAND gate which results from performing an AND gate and then a NOT gate, in

quantum computing it was shown that any multiple qubit logic gate may be composed from a quantum CNOT gate (which operates on a multiple qubit by flipping or preserving the target bit given the state of the control bit, an operation analogous to the classical XOR, i.e., the exclusive OR gate) and single qubit gates. One feature of quantum gates that distinguishes it from classical gates is that they are reversible: the inverse of a unitary matrix is also a unitary matrix, and thus a quantum gate can always be inverted by another quantum gate [13].

$$\mathrm{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

Unitary gates manipulate the information stored in the quantum register, and in this sense ordinary (unitary) quantum evolution can be regarded as computation (showed how a small set of single-qubit gates and a two-qubit gate is universal, in the sense that a circuit combined from this set can approximate to arbitrary accuracy any unitary transformation of n qubits)[2].



The measurement gate is a non-unitary gate that "collapses" the quantum superposition in the register onto one of its terms with the corresponding probability. Usually this measurement is done in the computational basis, but since quantum mechanics allows one to express an arbitrary state as a linear combination of basis states, provided that the states are orthonormal (a condition that ensures normalization) one can in principle measure the register in any arbitrary orthonormal basis. This, however, doesn't mean that measurements in different bases are efficiently equivalent. Indeed, one of the difficulties in constructing efficient quantum algorithms stems exactly from the fact that measurement collapses the state, and some measurements are much more complicated than others.

VI. CONCLUSION AND FUTURE SCOPE

It is important that making a practical quantum computing is still far in the future. Programming style for a quantum computer will also be quite different. Development of quantum computer needs a lot of money. Even the best scientists can't answer a lot of questions about quantum physics. Quantum computer is based on theoretical physics and some experiments are already made. Building a practical quantum computer is just a matter of time. Quantum computers easily solve applications that can't be done with help of today's computers. This will be one of the biggest steps in science and will undoubtedly revolutionize the practical computing world.

VII. REFERENCES

[1] Michael Nielsen, Isaac Chuang, "Quantum Computation and Quantum Information" , Cambridge University Press (2000).

[2] Peter Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," Proceedings of the 35th Annual Symposium on Foundations of Computer Science 124-134(1994).

[3] R. Feynman Simulating physics with computers, Internat. J. Theoret. Phys., 21, pp. 467– 488(1982).

[4] P. Benioff The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines, J. Statist. Phys., 22, pp. 563–591(1980).

[5] D. Deutsch, "Quantum theory, the Church–Turing principle and the universal quantum computer", Proc. Roy. Soc. London Ser. A, 400, pp. 96–117(1985).

[6] A. Berthiaume, D. Deutsch, and R. Jozsa, "The stabilisation of quantum computations", in Proceedings of the Workshop on Physics of Computation: PhysComp '94, IEEE Computer Society Press, Los Alamitos, CA, pp. 60–62(1994).

[7] C. Bennett, E. Bernstein,G. Brassard, and U. Vazirani. "Strengths andweaknesses of quantum computing". SIAM Journal on Computing, 26(5):1510–1523(1997).

[8] D. Simon" On the power of quantum computation", in Proceedings of the 35th Annual Symposium on Foundations of Computer Science, IEEE Computer Society Press, Los Alamitos, CA, pp. 116–123(1994).

[9] S. Lloyd , A potentially realizable quantum computer, Science, 261, pp. 1569– 1571(1993).

[10] R. Landauer, "Is quantum mechanics useful?" Philos. Trans. Roy. Soc. London Ser. A(1995).

[11] O. Goldreich. "On promise problems" (a survey in memory of Shimon Even [1935– 2004]). Electronic Colloquium on Computational Complexity, Report TR05-018, (2005).

[12] Barenco, A. et al. , 'Elementary gates for quantum computation', Phys. Rev., A 52: 3457–3467(1995).

[13] DiVicenzo, D. 'Two-bit gates are universal for quantum computation', Phys. Rev., A 51: 1015–1022(1995).

[14] Deutsch, D. and Jozsa, R.'Rapid solution of problems by quantum computer', Proc. Roy. Soc. Lond, A 439: 553–558(1992).

[15] E. Knill. Quantum randomness and nondeterminism. Technical Report LAUR-96-2186, Los Alamos National Laboratory, 1996. Available as arXiv.org e-Print quant-ph/9610012.

Cite this article as :

Prof. Nagaraj Telkar, Prof. Pavankumar Naik, Akash Mabali, Girish S H, Gurusiddeshwar S H, Sahana Balikai, "Quantum Computers for Next Generation", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6 Issue 3, pp. 452-459, May-June 2020.
Journal URL : http://ijsrcseit.com/CSEIT2063118