North Asian International Research Journal of Multidisciplinary

IRJIF IMPACT FACTOR:6.019

ISSN: 2454-2326 Vol.11, Issue, 3 March-2025

Index Copernicus Value: 58.12 Indian Citation Index

NAIRJC A Peer Reviewed Refereed Journal

doiglobal.org/doilink/10.2025/67e4033e3a625

QUANTUM COMPUTING: MAKING THE CONCEPT CRYSTAL CLEAR

*KITY MAURYA

Assistant Professor, Chemistry, SBS Govt. P.G. College Pipariya

ABSTRACT

One of the biggest developments in the history of quantum computing has been the creation of quantum computers in recent years. Over eight years have passed since the release of the D-Wave quantum computer. Through its cloud service, IBM has made its quantum computer available. Additionally, NASA, Google, Intel, and Microsoft have all made significant investments in the advancement of quantum computing and its uses. Information system researchers appear to be interested in the quantum computer as well as physicists and computer scientists. For those who are not scientists, this paper presents the fundamental ideas of quantum computing and outlines popular quantum applications. Additionally, the current state of quantum computing advancements is discussed.

KEYWORDS- Qubits, Bits, Quantum Computers, Algorithms, Problems

INTRODUCTION

In order to understand nature at the atomic level, quantum mechanics first appeared as a field of study in the early 1900s. This field of study gave rise to innovations like transistors, lasers, and magnetic resonance imaging. The concept of combining quantum mechanics and information theory first surfaced in the 1970s, but it didn't receive much attention until 1982, when physicist Richard Feynman made the argument that calculations describing quantum processes could not be processed in a tractable manner by computing based on conventional logic. However, the same limitations would not apply to quantum-based computing that is set up to mimic other quantum processes. This application didn't generate much research interest at the time, but it eventually led to the development of quantum simulation.

In 1994, mathematician Peter Shor created a quantum algorithm that could efficiently find the prime factors of large numbers—here, "efficiently" means in a time of practical relevance—beyond the capabilities of state-of-the-art classical algorithms. While this may seem like a simple oddity, the significance of Shor's

discovery cannot be overstated. Today, almost every online transaction is secured by an RSA cryptosystem, which depends on the factoring problem being intractable by classical algorithms.

MEANING OF QUANTUM COMPUTING

While both quantum and conventional computers attempt to solve problems, they do so in fundamentally different ways. By explaining two fundamental concepts of quantum mechanics—superposition and entanglement—that are essential to the functioning of quantum computers, this section explains what makes them special.

The paradoxical capacity of a quantum item, such as an electron, to exist in several "states" at the same time is known as superposition. One of these states could be an electron's lowest energy level, while another could be the atom's first excited level. An electron has a chance of being in the lower state and a chance of being in the upper state if it is prepared in a superposition of these two states.

The qubit, the fundamental building block of information in quantum computing, may be understood via comprehending superposition. The states 0 and 1 in classical computing are represented by transistors that can be either off or on. In qubits like electrons, 0 and 1 merely represent states similar to the previously mentioned lower and upper energy levels. In contrast to classical bits, which are always required to be in the 0 or 1 state, qubits can be in superpositions with different probabilities, which can be altered by quantum operations while doing calculations.

When quantum entities are produced and/or altered in such a way that none of them can be explained without mentioning the others, this phenomenon is known as entanglement. Individual identities are lost. Given how entanglement can endure over great distances, this idea is very challenging to understand. It appears as though information can move faster than the speed of light because measurements on one member of an entangled pair instantly dictate measurements on its mate. This seemingly distant motion was so unsettling that Einstein himself called it "spooky."

ELEMENTS OF QUANTUM COMPUTING

1. Bits and Qubits - A physical system's state space is made up of all of its potential states. A qubit can be thought of as any quantum mechanical system that can be represented by a two-dimensional complex vector space. These systems include electron spin, photon polarization, and an atom's ground state and excited state. The way component systems integrate is a significant distinction between classical and quantum systems. The condition of each of a classical system's constituent parts can be used to fully describe the system's state. The fact that most states of quantum systems cannot be explained in terms of the states of the system's constituent parts is a startling and counter-intuitive feature.We refer to these states as entangled states. Quantum measurement is another important characteristic. Any measurement of a system of qubits has only a discrete set of possible outcomes, even though there is a continuum of possible states; for n qubits, the maximum number of possible outcomes is 2n. The system will be in one of the potential outcome states following measurement. Probabilistic outcomes are those that are most likely to resemble the measured state. Measurement alters the state unless it is already in one of the potential outcome states; an unknown state cannot be successfully measured without being disturbed. The maximum number of quantum states that a copying mechanism may accurately replicate for a system with

n qubits is 2n. There is a mechanism that can accurately replicate any state, but it is impossible to tell which mechanism to apply if the state is unknown. The no cloning principle, a feature of quantum physics, states that an unknown state cannot be successfully replicated.

2. Entangled States- It is possible for subatomic particles to become entangled, which implies that they are linked despite their separation. They have an immediate impact on one another when measured. In terms of computing, this can be helpful. The correlations between entangled states are taken into account when measuring them.
3. Quantum Circuits - Quantum circuits are "one shot circuits" that only run once from left to right, in contrast to conventional circuits, which may have loops. They are also specific purpose, meaning that each algorithm uses a different circuit. It should be mentioned that quantum circuits can always be rearranged so that all measurements are made at the circuit's end. The following limitations set quantum circuit diagrams apart from classical diagrams.
   A. They have no loops and are acyclic.
   B. No FANIN because FANIN suggests that the circuit is not unitary because it is not reversible.
   C. No FANOUT, since the no-cloning theorem prevents us from copying a qubit's state while it is being computed.

IMPORTANCE OF QUANTUM COMPUTERS

One of the main drivers behind the advancement of quantum computation has been the prospect of creating a quantum computer that is advanced enough to carry out Shor's algorithm for big numbers. But in order to get a more comprehensive understanding of quantum computers, it's critical to realize that they will probably only provide enormous speedups for particular kinds of tasks. In addition to developing algorithms to illustrate quantum speed-ups, researchers are trying to determine which tasks are most suited for them. Generally speaking, optimization problems—which are crucial for everything from financial trading to defense—are thought to be greatly aided by quantum computers.

Although they are outside the purview of this overview, there are numerous other qubit system applications that are not associated with computation or simulation and are currently the subject of active study.
Two of the most well-known fields are (1) quantum sensing and metrology, which make use of qubits' extraordinary sensitivity to their surroundings to achieve sensing that goes beyond the classical shot noise limit, and (2) quantum networks and communications, which could result in ground-breaking methods of information exchange.
Building a Quantum Computer
Quantum computer construction is extremely challenging. The physicists, engineers, and materials scientists who are attempting to perform quantum operations on the many potential qubit systems that exist on the size of individual atoms must continually balance two conflicting requirements. First, since the environment can damage the fragile quantum states required for processing, qubits must be protected from it. A qubit's "coherence time" increases with the amount of time it remains in its intended state. Isolation is valued from this angle. Second, though, qubits must be entangled, moved around physical architectures, and controlled on demand in order for algorithms to execute. The more their "fidelity," the better these operations can be executed.

After decades of research, a few systems are starting to emerge as the best options for large-scale quantum information processing, despite the challenge of striking a balance between the necessary isolation and interaction. Some of the most promising materials for creating a quantum computer are semiconductors, superconducting systems, and trapped atomic ions. Regarding coherence, fidelity, and ultimate scalability to massive systems, each has pros and cons. To be reliable enough to perform significant computations, all of these platforms will obviously require some kind of error correction protocols, and the design and implementation of these protocols is a vast field of study in and of itself.

In reality, operational frameworks come in a variety of forms. The most well-known type of quantum computing is most likely logical, gate-based. Depending on the kind of qubit, it prepares qubits in initial states before exposing them to a sequence of "gate operations," such as current or laser pulses. The qubits are entangled, placed in superpositions, and put through logic operations such as the AND, OR, and NOT gates of conventional processing through these gates. After that, a result is produced by measuring the qubits.

Measurement-based computation is another framework, where the starting point is highly entangled qubits. The intended single qubit is then left in a definitive state after single qubit measurements are carried out rather than qubit manipulation operations. Additional measurements are made on different qubits based on the outcome, and ultimately a solution is found.

Topological computation is a third framework, where quasiparticles and their braiding operations serve as the basis for qubits and operations. The technique is appealing because topological quantum computers are theoretically protected against noise, which breaks the coherence of other qubits, even though fledgling implementations of their constituent parts have not yet been proved.

Lastly, there are Feynman's imagined analog quantum computers or quantum simulators. One way to conceptualize quantum simulators is as specialized quantum computers that can be configured to simulate quantum systems. With this capability, they may focus on issues like the operation of high-temperature superconductors, the reactions of certain compounds, and the construction of materials with particular characteristics.

CONCLUSION

By solving some kinds of problems that are traditionally unsolvable, quantum computers have the potential to completely transform computation. Significant progress is being made, even if no quantum computer is currently advanced enough to do computations that a classical computer cannot. Non-error-corrected quantum computers made up of several tens of qubits are currently in operation in a few big businesses and tiny start-ups; some of these are even publicly available via the cloud. Furthermore, quantum simulators are advancing in a variety of domains, including many-body physics and molecular energetics. A discipline devoted to near-term uses of quantum computers is beginning to take shape as modest devices come online. Long before the search for a large-scale, error-corrected quantum computer is finished, this advancement might allow for the realization of some of the advantages and insights of quantum computation.

REFERENCES

[1]. Ewald, R. H. (2019). An Introduction to Quantum Computing and Its Application. In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) (Vol. 11413 LNCS, pp. 3–8). Springer Verlag. https://doi.org/10.1007/978-3030-14082-3_1

[2]. Acín, A., Bloch, I., Buhrman, H., Calarco, T., Eichler, C., Eisert, J., … Wilhelm, F. K. (2018). The quantum technologies roadmap: a European community view. New Journal of Physics, 20(8), 080201. https://doi.org/10.1088/13672630/aad1ea

[3]. Aleksic, S., Hipp, F., Winkler, D., Poppe, A., Schrenk, B., & Franzl, G. (2015). Perspectives and limitations of QKD integration in metropolitan area networks. Optics Express, 23(8), 10359–10373. https://doi.org/10.1364/OE.23.010359

[4]. Bernstein, D. J. (2010). Grover vs. McEliece. In Third International Workshop, PQCrypto 2010 (pp. 73–80). Darmstadt, Germany: Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-12929-2_6

[5]. Chen, W., Han, Z. F., Zhang, T., Wen, H., Yin, Z. Q., Xu, F. X., … Guo, G. C. (2009). Field experiment on a "star type" metropolitan quantum key distribution network. IEEE Photonics Technology Letters. https://doi.org/10.1109/LPT.2009.2015058

[6]. D-Wave: Quantum Computing Applications. (2019). Retrieved June 27, 2019, from https://www.dwavesys.com/quantum-computing/applications

[7]. Gobby, C., Yuan, Z. L., & Shields, A. J. (2004). Quantum key distribution over 122 km of standard telecom fiber. Applied Physics Letters, 84(19), 37623764. https://doi.org/10.1063/1.1738173

[8]. IBM. (n.d.). IBM Q Experience. Retrieved June 27, 2019, from https://www.research.ibm.com/ibm-q/

[9]. MagiQ Technologies. (n.d.). Retrieved June 27, 2019, from https://www.magiqtech.com/solutions/network-security/

[10]. Meter, R., & Touch, J. (2013). Designing quantum repeater networks. IEEE Communications Magazine, 51(8), 64–71. https://doi.org/10.1109/MCOM.2013.6576340

[11]. O'Brien, J. L., Pryde, G. J., White, A. G., Ralph, T. C., & Branning, D. (2003). Demonstration of an all-optical quantum controlled-NOT gate. Nature, 426(6964), 264–267. https://doi.org/10.1038/nature02054

[12]. Pednault, E., Gunnels, J., Maslov, D., & Gambetta, J. (2019). On "Quantum Supremacy." Retrieved January 25, 2020, from https://www.ibm.com/blogs/research/2019/10/on-quantum-supremacy/

[13]. Quantum Development Kit | Microsoft. (2019). Retrieved June 27, 2019, from https://www.microsoft.com/en-us/quantum/development-kit

[14]. Sara Castellanos. (2019). Quantum Computing Holds Promise for Banks, Executives Say 'You could argue that finance has got the shortest path to impact,' says Goldman's head of research-and-development engineering. Retrieved January 24, 2020, from https://www.wsj.com/articles/quantumcomputing-holds-promise-for-banks-executives-say-11573230983

[15]. Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. In Proceedings 35th Annual Symposium on Foundations of Computer Science (pp. 124–134). Santa Fe, NM: IEEE. https://doi.org/10.1109/SFCS.1994.365700