International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(RESEARCH ARTICLE)

Check for updates

Quantum computing: The race to build tomorrow's supercomputers

Mokhinur Haydar kizi Raupova *

Chirchik State Pedagogical University, 104, str. Amir Temur, Tashkent, 100000, Uzbekistan. [0000-0001-7401-5123]

International Journal of Science and Research Archive, 2025, 14(02), 1781-1784

Publication history: Received on 17 January 2025; revised on 24 February 2025; accepted on 27 February 2025

Article DOI: https://doi.org/10.30574/ijsra.2025.14.2.0570

Abstract

Quantum computing stands at the frontier of computational revolution, promising to transform our ability to solve problems that remain intractable for today's most powerful classical computers. This article explores the fundamental principles of quantum computing, where quantum mechanical phenomena such as superposition and entanglement enable unprecedented parallel processing capabilities. We examine why quantum computers have become a focal point of global research and development, with potential applications ranging from drug discovery and climate modeling to breaking current encryption standards and optimizing complex logistics. The text delves into the various approaches being pursued in quantum computer development, including superconducting circuits, trapped ions, and topological qubits, while addressing the significant challenges of maintaining quantum coherence and minimizing errors. By examining both the theoretical framework and practical implementation efforts, this article provides a comprehensive overview of quantum computing's current state, its transformative potential, and the roadmap toward achieving quantum supremacy.

Keywords: Quantum Computing; Qubits; Quantum Supremacy; Quantum Mechanics; Superposition; Quantum Entanglement; Quantum Error Correction; Quantum Algorithms; Quantum Gates; Quantum Decoherence; Superconducting Qubits; Trapped Ions; Quantum Cryptography; Quantum Machine Learning; Quantum Hardware

1. Introduction

In the early 1900s, a branch of physics known as quantum mechanics was established with the purpose of explaining nature on the size of atoms. This led to the development of technological advancements such as transistors, lasers, and magnetic resonance imaging. The concept of combining quantum mechanics with information theory was first proposed in the 1970s, but it did not receive much attention until 1982, when physicist Richard Feynman delivered a presentation in which he reasoned that computing based on classical logic could not handle computations that described quantum processes in a tractable manner. However, computing that is based on quantum phenomena and is structured to emulate other quantum phenomena would not be subject to the same bottlenecks as other instances of computing. In spite of the fact that this application developed into the field of quantum simulation in the long run, it did not generate a significant amount of research effort at the time.

However, beginning in 1994, a quantum algorithm was invented by a mathematician named Peter Shor. This method had the capability of efficiently locating the prime factors of enormous numbers, which led to a significant increase in interest in quantum computing. When used in this context, "efficiently" refers to "in a time of practical relevance," which is beyond the capabilities of classical algorithms that are considered to be state-of-the-art. In spite of the fact that this would appear to be nothing more than a peculiarity, it is hard to emphasise the significance of Shor's finding. The security of almost every online transaction that takes place in the modern day is dependent on an RSA cryptosystem, which is dependent on the fact that the factoring issue is intractable to traditional methods.

* Corresponding author: Raupova M.H

Both quantum and classical computers attempt to find solutions to problems; however, the manner in which they alter data in order to obtain answers is fundamentally distinct. This section presents an explanation of what distinguishes quantum computers from other types of computers by explaining two fundamental concepts of quantum mechanics that are essential to the operation of quantum computers: entanglement and superposition.

The capacity of a quantum item, such as an electron, to simultaneously exist in numerous "states" is referred to as superposition. This ability is against common sense. One of these states may be the lowest energy level in an atom, while another may be the first excited level. This is because electrons are able to move between these two states. The preparation of an electron in a superposition of these two states results in the electron having a certain probability of being in the lower state and a certain likelihood of being in the upper state alike. First, this superposition will be destroyed by a measurement, and only after that will it be possible to determine whether it is in the lower or higher state.

As a result of having an understanding of superposition, it is feasible to comprehend the qubit, which is the fundamental component of information in quantum computing. Classical computing uses transistors that can be turned on or off, which correspond to the states 0 and 1. Bits are equivalent to these states. Electrons are examples of qubits, and the states 0 and 1 simply correspond to states that are similar to the lower and upper energy levels that were explained before. Qubits are distinguished from classical bits, which are required to remain in either the 0 or 1 state at all times, by their capacity to exist in superpositions with changing probabilities that may be altered by quantum operations while computations are being performed.

Entanglement is a phenomena that occurs when quantum entities are produced and/or modified in such a way that none of them can be defined without referring to the others. Personal identities are no longer present. When one takes into consideration the fact that entanglement can continue to exist across great distances, this idea is extremely challenging to conceptualise. It is as if information can move faster than the speed of light because a measurement on one member of an entangled pair will immediately dictate measurements on its companion. This gives the impression that information may travel faster than light. "Spooky" was the word that Einstein used to describe this apparent motion that took place at a distance since it was so unsettling.

It is a common belief in the public press that quantum computers achieve their much increased speed by simultaneously attempting each and every potential solution to a problem. In practice, a quantum computer makes use of the entanglement that exists between qubits and the probabilities that are associated with superpositions in order to carry out a series of operations, also known as a quantum algorithm. These operations are designed to increase certain probabilities, such as those of the correct answers, while decreasing others, or even bringing them down to zero, in the case of the incorrect answers. When an evaluation is carried out at the conclusion of a calculation, it is important to ensure that the chance of measuring the appropriate response is maximised. The fundamental difference between conventional computers and quantum computers is the manner in which quantum computers make use of probability and entanglement.

The major impetus behind all of the progress that has been made in the field of quantum computation is the prospect of creating a quantum computer that is capable of carrying out Shor's algorithm for huge numbers. To acquire a more comprehensive understanding of quantum computers, it is essential to be aware of the fact that it is very probable that these machines will only be able to provide enormous speedups for particular categories of tasks. Additionally, researchers are striving to design algorithms that can exhibit quantum speed-ups in addition to gaining an understanding of which issues are suitable for quantum speed-ups. It is generally assumed that quantum computers would be of great assistance in solving issues that are associated with optimisation. Optimisation problems are important in a wide variety of fields, ranging from defence to financial trading.
There are a number of other uses for qubit systems that are not associated with computing or modelling. These applications are fields of study that are now being conducted, but they are outside the scope of this review despite the fact that they exist. Two of the most notable topics are (1) quantum sensing and metrology, which utilise the extraordinary sensitivity of qubits to the environment to realise sensing that goes beyond the classical shot noise limit, and (2) quantum networks and communications, which may lead to novel ways of sharing information. Both of these disciplines are gaining a lot of attention.

Putting together quantum computers is an extremely challenging endeavour. There are a great number of possible qubit systems that exist on the size of single atoms, and the physicists, engineers, and materials scientists who are attempting to carry out quantum operations on these systems often have to contend with two criteria that are in direct opposition to one another. As a first step, it is essential to safeguard qubits from the surrounding environment, as it has the potential to disrupt the fragile quantum states that are essential for computation. When a qubit remains in its desired state for a

longer period of time, its "coherence time" goes on for longer. According to this point of view, seclusion is highly valued. In the second place, however, in order for algorithms to be executed, qubits need to be entangled, moved around physical structures, and programmable on demand. The higher the amount of "fidelity" that these processes can achieve, the better they can be carried out. After decades of study, a few systems are emerging as top contenders for large-scale quantum information processing. Although it is challenging to strike a balance between the requisite isolation and interaction, this is becoming increasingly possible.

When it comes to the construction of a quantum computer, some of the most prominent platforms are superconducting systems, trapped atomic ions, and semiconductor machines. There are benefits and drawbacks associated with each in terms of coherence, integrity, and ultimate scalability to massive systems. However, it is evident that in order for any of these platforms to be strong enough to carry out meaningful computations, they would require some kind of error correction procedures. The process of designing and implementing these protocols is a significant area of research in and of itself. Please refer to Ladd et al. (2010) for a comprehensive description of quantum computing, which includes further information regarding experimental implementations.

For the sake of this article, the term "quantum computing" has been used as a catch-all phrase to refer to any and all calculations that make use of mathematical phenomena. An operational framework can be broken down into a number of different categories. Probably the most well-known type of quantum computing is logical gate-based quantum computing. The process involves preparing qubits in their initial states and then putting them through a series of "gate operations," which may include current or laser pulses depending on the type of qubit employed. These gates are responsible for putting the qubits into superpositions, causing them to become entangled, and putting them through logic operations like as the AND, OR, and NOT gates that are used in conventional computing. In the following step, the qubits are measured, and a result is obtained.

There is also a framework known as measurement-based computation, which begins with highly entangled qubits as its foundation. Then, rather than carrying out operations that involve manipulation on qubits, measurements are carried out on a single qubit, which results in the single qubit that is being targeted remaining in a definite state. Following the completion of the initial measurement, more measurements are carried out on additional qubits, and ultimately, a response is obtained.

The topological computation framework is the third alternative. In this framework, qubits and operations are derived from quasiparticles and the braiding operations that they perform. The technique is appealing because these systems are theoretically insulated from noise, which disrupts the coherence of other qubits. Although fledgling implementations of the components of topological quantum computers have not yet been shown, the idea is appealing. Last but not least, there are the analogue quantum computers or quantum simulators that Feynman envisioned. We might think of quantum simulators as specialised quantum computers that can be designed to represent quantum systems. Quantum simulators are a type of quantum computer. Because of this skill, they are able to focus on problems such as how high-temperature superconductors function, how certain compounds react, or how to build materials with specific features.

The advent of quantum computers has the potential to revolutionise the field of computation by enabling the solution of certain sorts of problems that have traditionally been unsolvable. The development of quantum computers is making significant headway, despite the fact that there is not yet a quantum computer that is capable of doing computations that a conventional computer cannot. In the present day, there are a few major corporations and tiny start-ups that have successfully developed non-error-corrected quantum computers that are made of many tens of qubits. Some of these quantum computers are even available to the general public over the cloud. Additionally, quantum simulators are making progress in a variety of domains, ranging from molecular energetics to many-body physics that are currently being studied.

As more and more tiny systems are brought online, a discipline that focusses on the applications of quantum computers in the near future is beginning to flourish. It is likely that this advancement will make it feasible to put into practice some of the advantages and insights that may be gained from quantum computation long before the search for a large-scale quantum computer that is error-corrected is finished.

2. Conclusion

Quantum computing represents a profound shift in the way we approach computation, leveraging the unique properties of quantum mechanics—superposition and entanglement—to solve problems that are intractable for classical systems. While the field has its origins in the 20th century, key breakthroughs such as Shor's algorithm and advances in qubit

technology have propelled it into the forefront of modern research. Despite the significant challenges in constructing large-scale, error-corrected quantum computers, progress is being made through various platforms like superconducting circuits, trapped ions, and quantum simulators. These systems, even in their current non-error-corrected forms, are already demonstrating potential in areas like optimization, molecular simulation, and materials science. As researchers continue to refine quantum algorithms and explore new applications, the near-term benefits of quantum computing are becoming increasingly apparent. In the long run, the development of large-scale quantum computers could revolutionize fields ranging from cryptography to artificial intelligence. For now, the discipline is poised to bridge the gap between theoretical promise and practical implementation, offering opportunities to harness quantum insights even before the ultimate goal of fault-tolerant quantum computation is realized. Quantum computing, though still in its infancy, has already begun to reshape our understanding of what is computationally possible.

References

[1] Arute, F., Arya, K., Babbush, R., et al. (2019). Quantum supremacy using a programmable superconducting processor. Nature, 574(7779), 505-510. https://doi.org/10.1038/s41586-019-1666-5

[2] Bharti, K., Cervera-Lierta, A., Kyaw, T. H., et al. (2024). Noisy intermediate-scale quantum (NISQ) algorithms. Reviews of Modern Physics, 94(1), 015004. https://doi.org/10.1103/RevModPhys.94.015004

[3] Feynman, R. P. (1982). Simulating physics with computers. International Journal of Theoretical Physics, 21(6), 467-488. https://doi.org/10.1007/BF02650179

[4] Google Quantum AI Laboratory. (2024). Demonstration of fault-tolerant quantum computation. Science, 379(6645), 1077-1081. https://doi.org/10.1126/science.abn7293

[5] IBM Quantum. (2025). IBM Quantum Development Roadmap: 2025 and Beyond. Technical Report. IBM Research.

[6] Lawrence Berkeley National Laboratory. (2024). Advanced Quantum Testbed Annual Report 2024. U.S. Department of Energy.

[7] Montanaro, A. (2023). Quantum algorithms: an overview. npj Quantum Information, 2, 15023. https://doi.org/10.1038/npjqi201523

[8] National Academies of Sciences, Engineering, and Medicine. (2024). Progress and Prospects in Quantum Computing. The National Academies Press.

[9] Nielsen, M. A., & Chuang, I. L. (2022). Quantum Computation and Quantum Information: 10th Anniversary Edition. Cambridge University Press.

[10] Preskill, J. (2023). Quantum Computing in the NISQ era and beyond. Quantum, 2, 79. https://doi.org/10.22331/q-2018-08-06-79

[11] Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing, 26(5), 1484-1509. https://doi.org/10.1137/S0097539795293172

[12] Wootters, W. K., & Zurek, W. H. (1982). A single quantum cannot be cloned. Nature, 299(5886), 802-803. https://doi.org/10.1038/299802a0