IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Quantum Computing: Principles, Progress And Future Prospects

Ayush

Assistant Professor, Department of Engineering, Saraswati Group of Colleges.

Abstract

In recent studies, quantum computing has turned out as a new paradigm of computation and has been able to solve the problems with many classes of problems that are still unsolvable by ordinary classical machines. In contrast to the commutative architecture of binary computing, which needs bits being limited to either zero or one, quantum computing utilizes superposition, entanglement and unitary evolution, which permit computations on exponentially large spaces. This article provides a systematic coverage of the literal principles, quantum mathematical procedures, computer tumult, and the recent applications of the quantum technologies. It further examines the constraints of Noisy Intermediate-Scale Quantum (NISQ) devices and explains the possible ways that could be taken to achieve scalable, fault-tolerant architecture. The review highlights the importance of continuous interdisciplinary cooperation between physics, engineering, and computer science solutions that make quantum computing a feasible idea.

Keywords: Quantum Computing, Qubits, Superposition, Quantum Algorithms, NISQ

Introduction

Quantum computing combines quantum mechanics and computer engineering to create quantum devices that are essentially different systems of their classical counterparts. In contrast to classical computers, which process bits which are defined to be 0 or 1, quantum computers have access to superpositions between 0 and 1, and thus support parallel evolution among many states at the same time (Nielsen and Chuang, 2010) [1]. The concept is all the way back to Feynman who made the argument that quantum systems cannot be well classical simulated [2]. Later Deutsch developed the concept of a universal quantum computer and determined the mathematical foundations of quantum algorithms [3].

The last several years have been characterized by a high rate of development in the field. Using a quantum processor, the 2019 quantum supremacy performance of a 53-qubit processor by Google by demonstrating a task inaccessible to classical supercomputers (Arute et al., 2019) [4] was a breakthrough. Leading companies in the industry like IBM, IonQ, Rigetti, and Microsoft continue to work on the hardware architectures of a variety of qubit technologies, which keep fostering a consistent advancement in both theoretical investigation and practical work.

Theoretical Foundations

2.1 Qubits and Superposition

In quantum theory one qubit is able to be in a superposition of the basis states |human|:|human|>In quantum theory a qubit can be in a superposition of the two basis states:|human|>In quantum theory a qubit is allowable to be in a superposition of the two basis states. N qubits form a Hilbert space of size 2n, thus, bringing the state space to increase exponentially with the quantity of qubits, fact mentioned by Preskill (2018) [5]. Quantum algorithms control the probability distribution of an observational measurement by tuning relative to each basis state such that the result of that observational measurement is the one desired with a large probability.

2.2 Entanglement

Entanglement refers to one of the quintessentially quantum correlations in which the joint system of two or more qubits cannot be broken down to a collection of product systems. The result of measuring a single qubit can accordingly have an instantaneous effect on the state of a remote partner (this phenomenon, the basis of quantum teleportation, dense coding, high-fidelity protocols to correct errors, and protocols in the past) [6].

2.3 Quantum Gates and Circuits

The quantum gate dependency is characterised by unitary matrices in the circuit model, examples of which are the canonical Hadamard, Pauli -X, phase and controlled -NOT gates. The basic transformations are concatenated to create quantum circuits which implement computational tasks of interest. With any finite universal set of gates (see Barenco et al. 1995 [7]) it is possible to approximate any unitary operation to an arbitrarily small level and, thus, enabling the realization of arbitrarily complex algorithms.

Quantum Algorithms

3.1 Shor's Algorithm

The revolutionary algorithm with integer factorisation by Shor gains an exponential pre-eminence over the existing classical methods, causing the security of popular public-key algorithms like RSA to be threatened (Shor, 1997). The key element of this impressive performance is based on the ability of a quantum computer to perform quantum Fourier transforms on superpositions of computation basis states.

3.2 Grover's Algorithm

A search algorithm by Grover provides a quadratic speed up in the search of a marked element in an unsorted database and the number of necessary oracle queries is no longer (N) but (√N). The impact of such a reduction is extensive to combinatorial optimisation, cryptanalytic attacks and other machine-learning subroutines.

3.3 Uni-directional Variational Quantum Algorithms.

The examples of hybrid quantum classical paradigm include variational quantum eigensolvers (VQE) and quantum approximate optimisation algorithms (QAOA). The parameterised quantum circuits of these protocols are optimised by external classical optimisers after measurement feedback. Their small depth of circuits are particularly suitable to noisy intermediate-scale quantum (NISQ) hardware where the limit is on the number of successive Sveratedou of the overly decohering circuit (Peruzzo et al., 2014; Farhi et al., 2014).

Quantum Hardware Platforms

4.1 Superconducting Qubits

Several qubit upscale Superconducting qubit architectures use Josephson junctions to design anharmonic oscillators as qubits at cryogenic temperatures. Google came up with the Sycamore processor which demonstrated quantum supremacy based on this technology [4]. Despite the ability of these devices to run with gate speeds in the tens of nanoseconds, its implementation is still limited by decoherence phenomena and the scale- factor bottleneck of manufacturing, as Kjaergaard and colleagues (2020) describe (12).

4.2 Trapped-Ion Qubits

The charged atoms are isolated in trapped-ion systems through electromagnetic traps with coherence times of minutes and gate fidelity greater than 99.9% (Bermudez et al., 2017) [13]. This method has been commercialised by commercial organisations, such as IonQ and Quantinuum; however, the relatively low frequency of the gate is a major obstacle to scalability.

4.3 Photonic Quantum Systems

The quantum processors based on photons represent the logical qubits in optical modes, and provide intrinsically low decoherence rates which are ideal in activities such as communication. The main challenge, though, is to design deterministic photonphoton interactions at scale, which O Brien and others (2009) [14] note is a challenge.

4.4 Topological Qubits

Topological qubits are trying to store quantum data in non-Abelian quasiparticle excitations, and hence are a way of offering passive error protection against local perturbations (Nayak et al., 2008) [15]. Although this idea sounds theoretically interesting, larger-scale implementation of topological hardware continues to be an experimental project.

5. Applications of Quantum Computing

5.1 Cryptography

It is evident that quantum computing is a serious threat to the traditional forms of public-key cryptographic, courtesy of the Shor algorithm. In their turn, quantum key distribution (QKD) attains secure communication with the help of unalterable laws of quantum mechanics (Gisin and Thew, 2007) [16].

5.18 Chemistry and Material Science.

Molecular architectures can be simulated on quantum processors with a fidelity that is better than classical methods of computation. Initial experiments using Variational Quantum Eigensolver (VQE) methods were able to compute energy landscapes of simple molecules including H 2 and LiH (Aspuru -Guzik et al, 2005) [17]. These developments are indicative of a faster rate of drug discovery, catalytic development, and materials development.

5.3 Optimization and Machine Learning.

Quantum machine learning uses the opportunity of state-preparation, sampling, and nevertheless kernel-established procedures to improve pattern-recognization tasks. In addition, quantum optimization is shown to be effective in various fields of logistics, financial modeling, and supply, as well as control systems (Biamonte et al., 2017) [18].

5.4 Industrial Adoption

Quantum platforms are also offered by quality industry players, including Google, IBM, and Amazon, on a pay-as-you-use basis, providing initial experience with quantum hardware, which can be used to explore the experimental work on network routing, energy-grid optimization, and risk-analysis-modeling (Gambetta, 2020) [19].

Challenges and Limitations

6.1 Decoherence

When quantum states are interacting with the environment, decoherence proceeds very fast and thus greatly limits the depth of the circuits and the reliability of algorithms to a point of being a limiting factor (Zurek, 2003) [20].

6.2 Scalability

Fault tolerant quantum computers will require up to several millions of physical qubits to encode only a few thousand logical qubits, which is way beyond what current hardware has to offer (Fowler et al., 2012) [21].

6.3 Error Correction

Quantum error-correcting codes, including the surface code, are based on a large qubit overhead and require extremely high gate fidelities to be effectively used (Terhal, 2015) [22].

6.4 Engineering Complexity

The cost and engineering skills needed to construct the operational quantum systems are dilution refrigerators, vacuum chambers, and high-precision laser equipment, which are expensive and require high-level engineering skills.

Future Directions

The next steps in this direction will be limited to longer coherence times, better gate fidelity and building networked and modular quantum architectures. It is expected that the near term should be characterized by hybrid quantum-classical systems. With development in scalability, the availability of quantum technologies will be expanded with the introduction of new algorithmic frameworks and programming tools. Moreover, post-quantum cryptographic standards have to be introduced by governments and industries at the same time to the extent of maintaining the security of data (Preskill, 2018) [5].

Conclusion

Quantum computing is an area with a rosier future of radically changing the ability to compute developments, but current systems are still limited by noise, small scale, and engineering realities. Constant interdisciplinary studies are the key to going beyond demonstrations on the NISQ level all the way to complete fault-tolerant systems. Guided by further improvements in algorithms and hardware technology and with error control techniques, quantum computing promises to have a dramatic impact on cryptography, chemistry, and optimization and artificial intelligence in the next few decades.

References

1. Nielsen M.A., Chuang I.L., Quantum Computation and Quantum Information, Cambridge University Press, 2010

2. Feynman R., Simulating Physics with Computers, International Journal of Theoretical Physics, 1982, 21 (6), 467–488.

3. Deutsch D., Quantum Theory, the Church–Turing Principle and the Universal Quantum Computer, Proceedings of the Royal Society A, 1985, 400 (1818), 97–117.

4. Arute F., et al., Quantum Supremacy Using a Programmable Superconducting Processor, Nature, 2019, 574, 505–510.

5. Preskill J., Quantum Computing in the NISQ Era and Beyond, Quantum, 2018, 2, 79.

6. Horodecki R., et al., Quantum Entanglement, Reviews of Modern Physics, 2009, 81 (2), 865–942.

7. Barenco A., et al., Elementary Gates for Quantum Computation, Physical Review A, 1995, 52 (5), 3457–3467.

8. Shor P.W., Polynomial-Time Algorithms for Integer Factorization and Discrete Logarithms, SIAM Journal on Computing, 1997, 26 (5), 1484–1509.

9. Grover L., A Fast Quantum Mechanical Algorithm for Database Search, STOC, 1996, 212–219.

10. Peruzzo A., et al., A Variational Eigenvalue Solver on a Photonic Quantum Processor, Nature Communications, 2014, 5, 4213.

11. Farhi E., Goldstone J., Gutmann S., A Quantum Approximate Optimization Algorithm, 2014.

12. Kjaergaard M., et al., Superconducting Qubits: Current State of Play, Annual Review of Condensed Matter Physics, 2020.

13. Bermudez A., et al., Assessing Trapped-Ion Quantum Processors, Annalen der Physik, 2017.

14. O'Brien J.L., et al., Photonic Quantum Technologies, Nature Photonics, 2009.

15. Nayak C., et al., Non-Abelian Anyons and Topological Quantum Computation, Reviews of Modern Physics, 2008, 80 (3), 1083.

16. Gisin N., Thew R., Quantum Communication, Nature Photonics, 2007, 1 (3), 165–171.

17. Aspuru-Guzik A., et al., Simulated Quantum Computation of Molecular Energies, Science, 2005, 309 (5741), 1704–1707.

18. Biamonte J., et al., Quantum Machine Learning, Nature, 2017, 549 (7671), 195–202.

19. Gambetta J., IBM Quantum Roadmap, IBM Research, 2020.

20. Zurek W., Decoherence and the Transition from Quantum to Classical, Reviews of Modern Physics, 2003.

21. Fowler A., et al., Surface Codes: Towards Practical Large-Scale Quantum Computation, Physical Review A, 2012.

22. Terhal B., Quantum Error Correction, Reviews of Modern Physics, 2015.