IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 11, Issue 4, April 2022

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.118

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 4, April 2022||

|DOI:10.15680/IJIRSET.2022.1104029|

QUANTUM COMPUTER

Manoj Lakhan

Assistant Professor, Department of Physics, M.L.V. Government College, Bhilwara, Rajasthan, India

ABSTRACT: Quantum computing is a type of computation that harnesses the collective properties of quantum states, such as superposition, interference, and entanglement, to perform calculations. The devices that perform quantum computations are known as quantum computers. Though current quantum computers are too small to outperform usual (classical) computers for practical applications, they are believed to be capable of solving certain computational problems, such as integer factorization (which underlies RSA encryption), substantially faster than classical computers.The study of quantum computing is a subfield of quantum information science. There are several types of quantum computers (also known as quantum computing systems), including the quantum circuit model, quantum Turing machine, adiabatic quantum computer, one-way quantum computer, and various quantum cellular automata. The most widely used model is the quantum circuit, based on the quantum bit, or "qubit", which is somewhat analogous to the bit in classical computation. A qubit can be in a 1 or 0 quantum state, or in a superposition of the 1 and 0 states. When it is measured, however, it is always 0 or 1; the probability of either outcome depends on the qubit's quantum state immediately prior to measurement. Efforts towards building a physical quantum computer focus on technologies such as transmons, ion traps and topological quantum computers, which aim to create high-quality qubits. These qubits may be designed differently, depending on the full quantum computer's computing model, as to whether quantum logic gates, quantum annealing, or adiabatic quantum computation are employed. There are currently a number of significant obstacles to constructing useful quantum computers. It is particularly difficult to maintain qubits' quantum states, as they suffer from quantum decoherence and state fidelity. Quantum computers therefore require error correction.

KEYWORDS: quantum, computer, calculations, machine, state, qubits, adiabatic, logic, gates

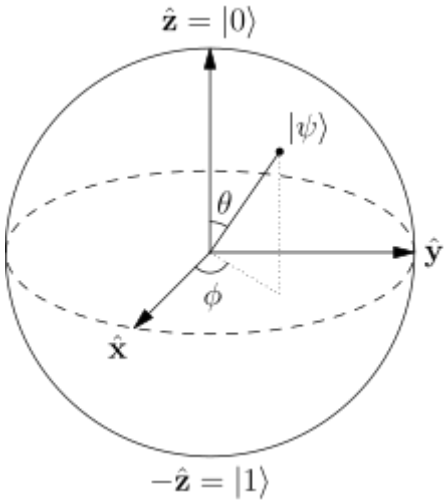
I. INTRODUCTION

Any computational problem that can be solved by a classical computer can also be solved by a quantum computer. Conversely, any problem that can be solved by a quantum computer can also be solved by a classical computer, at least in principle given enough time. In other words, quantum computers obey the Church–Turing thesis. This means that while quantum computers provide no additional advantages over classical computers in terms of computability, quantum algorithms for certain problems have significantly lower time complexities than corresponding known classical algorithms. [1,2] Notably, quantum computers are believed to be able to quickly solve certain problems that no classical computer could solve in any feasible amount of time—a feat known as "quantum supremacy." The study of the computational complexity of problems with respect to quantum computers is known as quantum complexity theory. The prevailing model of quantum computation describes the computation in terms of a network of quantum logic gates. This model is a complex linear-algebraic generalization of boolean circuits. In quantum mechanics, probability vectors can be generalized to density operators. The quantum state vector formalism is usually introduced first because it is conceptually simpler, and because it can be used instead of the density matrix formalism for pure states, where the whole quantum system is known.[3,4]

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 4, April 2022||

|DOI:10.15680/IJIRSET.2022.1104029|



The Bloch sphere is a representation of a qubit, the fundamental building block of quantum computers.

Progress in finding quantum algorithms typically focuses on this quantum circuit model, though exceptions like the quantum adiabatic algorithm exist. Quantum algorithms can be roughly categorized by the type of speedup achieved over corresponding classical algorithms.Quantum algorithms that offer more than a polynomial speedup over the best known classical algorithm include Shor's algorithm for factoring and the related quantum algorithms for computing discrete logarithms, solving Pell's equation, and more generally solving the hidden subgroup problem for abelian finite groups. These algorithms depend on the primitive of the quantum Fourier transform. No mathematical proof has been found that shows that an equally fast classical algorithm cannot be discovered, although this is considered unlikely. Certain oracle problems like Simon's problem and the Bernstein–Vazirani problem do give provable speedups, though this is in the quantum query model, [5] which is a restricted model where lower bounds are much easier to prove and doesn't necessarily translate to speedups for practical problems.Other problems, including the simulation of quantum physical processes from chemistry and solid-state physics, the approximation of certain Jones polynomials, and the quantum algorithm for linear systems of equations have quantum algorithms appearing to give super-polynomial speedups and are BQP-complete. Because these problems are BQP-complete, an equally fast classical algorithm for them would imply that no quantum algorithm gives a super-polynomial speedup, which is believed to be unlikely.[6]
Some quantum algorithms, like Grover's algorithm and amplitude amplification, give polynomial speedups over corresponding classical algorithms.Though these algorithms give comparably modest quadratic speedup, they are widely applicable and thus give speedups for a wide range of problems. Many examples of provable quantum speedups for query problems are related to Grover's algorithm, including Brassard, Høyer, and Tapp's algorithm for finding collisions in two-to-one functions,which uses Grover's algorithm, and Farhi, Goldstone, and Gutmann's algorithm for evaluating NAND trees, which is a variant of the search problem.[7,8]

II. DISCUSSION

A notable application of quantum computation is for attacks on cryptographic systems that are currently in use. Integer factorization, which underpins the security of public key cryptographic systems, is believed to be computationally infeasible with an ordinary computer for large integers if they are the product of few prime numbers (e.g., products of two 300-digit primes).[29] By comparison, a quantum computer could efficiently solve this problem using Shor's algorithm to find its factors. This ability would allow a quantum computer to break many of the cryptographic systems in use today, in the sense that there would be a polynomial time (in the number of digits of the integer) algorithm for solving the problem. In particular, most of the popular public key ciphers are based on the difficulty of factoring integers or the discrete logarithm problem, both of which can be solved by Shor's algorithm. In particular, the RSA, Diffie–Hellman, and elliptic curve Diffie–Hellman algorithms could be broken. These are used to protect secure Web pages, encrypted email, and many other types of data. Breaking these would have significant ramifications for electronic privacy and security.[9]

Identifying cryptographic systems that may be secure against quantum algorithms is an actively researched topic under the field of post-quantum cryptography. Some public-key algorithms are based on problems other than the integer factorization and discrete logarithm problems to which Shor's algorithm applies, like the McEliece cryptosystem based

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 4, April 2022||

|DOI:10.15680/IJIRSET.2022.1104029|

on a problem in coding theory. Lattice-based cryptosystems are also not known to be broken by quantum computers, and finding a polynomial time algorithm for solving the dihedral hidden subgroup problem, which would break many lattice based cryptosystems, is a well-studied open problem. It has been proven that applying Grover's algorithm to break a symmetric (secret key) algorithm by brute force requires time equal to roughly 2n/2 invocations of the underlying cryptographic algorithm, compared with roughly 2n in the classical case, meaning that symmetric key lengths are effectively halved: AES-256 would have the same security against an attack using Grover's algorithm that AES-128 has against classical brute-force search .

Since chemistry and nanotechnology rely on understanding quantum systems, and such systems are impossible to simulate in an efficient manner classically, many believe quantum simulation will be one of the most important applications of quantum computing.Quantum simulation could also be used to simulate the behavior of atoms and particles at unusual conditions such as the reactions inside a collider.Quantum simulations might be used to predict future paths of particles and protons under superposition in the double-slit experiment. About 2% of the annual global energy output is used for nitrogen fixation to produce ammonia for the Haber process in the agricultural fertilizer industry while naturally occurring organisms also produce ammonia. Quantum simulations might be used to understand this process increasing production.Quantum cryptography could potentially fulfill some of the functions of public key cryptography. Quantum-based cryptographic systems could, therefore, be more secure than traditional systems against quantum hacking.[10,11]

III. RESULTS

Since quantum computers can produce outputs that classical computers cannot produce efficiently, and since quantum computation is fundamentally linear algebraic, some express hope in developing quantum algorithms that can speed up machine learning tasks. For example, the quantum algorithm for linear systems of equations, or "HHL Algorithm", named after its discoverers Harrow, Hassidim, and Lloyd, is believed to provide speedup over classical counterparts.Some research groups have recently explored the use of quantum annealing hardware for training Boltzmann machines and deep neural networks. In the field of computational biology, quantum computing has played a big role in solving many biological problems. One of the well-known examples would be in computational genomics and how computing has drastically reduced the time to sequence a human genome. Given how computational biology is using generic data modeling and storage, its applications to computational biology are expected to arise as well.
Deep generative chemistry models emerge as powerful tools to expedite drug discovery. However, the immense size and complexity of the structural space of all possible drug-like molecules pose significant obstacles, which could be overcome in the future by quantum computers. Quantum computers are naturally good for solving complex quantum many-body problems and thus may be instrumental in applications involving quantum chemistry. Therefore, one can expect that quantum-enhanced generative models including quantum GANs may eventually be developed into ultimate generative chemistry algorithms. Hybrid architectures combining quantum computers with deep classical networks, such as Quantum Variational Autoencoders, can already be trained on commercially available annealers and used to generate novel drug-like molecular structures.[12,13]

One of the greatest challenges involved with constructing quantum computers is controlling or removing quantum decoherence. This usually means isolating the system from its environment as interactions with the external world cause the system to decohere. However, other sources of decoherence also exist. Examples include the quantum gates, and the lattice vibrations and background thermonuclear spin of the physical system used to implement the qubits. Decoherence is irreversible, as it is effectively non-unitary, and is usually something that should be highly controlled, if not avoided. Decoherence times for candidate systems in particular, the transverse relaxation time T2 (for NMR and MRI technology, also called the dephasing time), typically range between nanoseconds and seconds at low temperature. Currently, some quantum computers require their qubits to be cooled to 20 millikelvin (usually using a dilution refrigerator in order to prevent significant decoherence. A 2020 study argues that ionizing radiation such as cosmic rays can nevertheless cause certain systems to decohere within milliseconds.

As a result, time-consuming tasks may render some quantum algorithms inoperable, as maintaining the state of qubits for a long enough duration will eventually corrupt the superpositions.[14,15]
These issues are more difficult for optical approaches as the timescales are orders of magnitude shorter and an often-cited approach to overcoming them is optical pulse shaping. Error rates are typically proportional to the ratio of operating time to decoherence time, hence any operation must be completed much more quickly than the decoherence time.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 4, April 2022||

|DOI:10.15680/IJIRSET.2022.1104029|

As described in the Quantum threshold theorem, if the error rate is small enough, it is thought to be possible to use quantum error correction to suppress errors and decoherence. This allows the total calculation time to be longer than the decoherence time if the error correction scheme can correct errors faster than decoherence introduces them. An often cited figure for the required error rate in each gate for fault-tolerant computation is 10−3, assuming the noise is depolarizing.Meeting this scalability condition is possible for a wide range of systems. However, the use of error correction brings with it the cost of a greatly increased number of required qubits. The number required to factor integers using Shor's algorithm is still polynomial, and thought to be between L and L2, where L is the number of digits in the number to be factored; error correction algorithms would inflate this figure by an additional factor of L. For a 1000-bit number, this implies a need for about 104 bits without error correction.[63] With error correction, the figure would rise to about 107 bits. Computation time is about L2 or about 107 steps and at 1 MHz, about 10 seconds.[16,17]
A very different approach to the stability-decoherence problem is to create a topological quantum computer with anyons, quasi-particles used as threads and relying on braid theory to form stable logic gates.[18,19]

IV. CONCLUSIONS

Any computational problem solvable by a classical computer is also solvable by a quantum computer.Intuitively, this is because it is believed that all physical phenomena, including the operation of classical computers, can be described using quantum mechanics, which underlies the operation of quantum computers.

Conversely, any problem solvable by a quantum computer is also solvable by a classical computer. It is possible to simulate both quantum and classical computers manually with just some paper and a pen, if given enough time. More formally, any quantum computer can be simulated by a Turing machine. In other words, quantum computers provide no additional power over classical computers in terms of computability. This means that quantum computers cannot solve undecidable problems like the halting problem and the existence of quantum computers does not disprove the Church–Turing thesis.[20]

REFERENCES

1. The National Academies of Sciences, Engineering, and Medicine (2019). Grumbling, Emily; Horowitz, Mark (eds.). Quantum Computing : Progress and Prospects (2018). Washington, DC: National Academies Press. p. I-5. doi:10.17226/25196. ISBN 978-0-309-47969-1. OCLC 1081001288. S2CID 125635007.
2. ^ Aaronson, Scott (8 June 2021). "What Makes Quantum Computing So Hard to Explain?". Quanta Magazine. Retrieved 9 November 2021.
3. ^ Franklin, Diana; Chong, Frederic T. (2004). "Challenges in Reliable Quantum Computing". Nano, Quantum and Molecular Computing. pp. 247–266. doi:10.1007/1-4020-8068-9_8. ISBN 1-4020-8067-0.
4. ^ Pakkin, Scott; Coles, Patrick (10 June 2019). "The Problem with Quantum Computers". Scientific American.
5. ^ "Quantum computing use cases are getting real—what you need to know". McKinsey & Company. McKinsey & Company. 14 December 2021. Retrieved 1 April 2022.
6. ^ Nielsen, p. 29
7. ^ Benioff, Paul (1980). "The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines". Journal of Statistical Physics. **22** (5): 563–591. Bibcode:1980JSP....22..563B. doi:10.1007/bf01011339. S2CID 122949592.
8. ^ Feynman, Richard (June 1982). "Simulating Physics with Computers" (PDF). International Journal of Theoretical Physics. **21** (6/7): 467–488. Bibcode:1982IJTP...21..467F. doi:10.1007/BF02650179. S2CID 124545445. Archived from the original (PDF) on 8 January 2019. Retrieved 28 February 2019.
9. ^ Manin, Yu. I. (1980). Vychislimoe i nevychislimoe [Computable and Noncomputable] (in Russian). Sov.Radio. pp. 13–15. Archived from the original on 10 May 2013. Retrieved 4 March 2013.
10. ^ Feynman, Richard P. (1986). "Quantum mechanical computers". Foundations of Physics. Springer Science and Business Media LLC. **16** (6): 507–531. Bibcode:1986FoPh...16..507F. doi:10.1007/bf01886518. ISSN 0015-9018. S2CID 122076550.
11. ^ Mermin, David (28 March 2006). "Breaking RSA Encryption with a Quantum Computer: Shor's Factoring Algorithm" (PDF). Physics 481-681 Lecture Notes. Cornell University. Archived from the original (PDF) on 15 November 2012.
12. ^ Chuang, Isaac L.; Gershenfeld, Neil; Kubinec, Markdoi (April 1998). "Experimental Implementation of Fast Quantum Searching". Phys. Rev. Lett. American Physical Society. **80** (15): 3408–3411. Bibcode:1998PhRvL..80.3408C. doi:10.1103/PhysRevLett.80.3408.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 4, April 2022||

|DOI:10.15680/IJIRSET.2022.1104029|

13. ^ "quantum computer". Encyclopædia Britannica. Retrieved 4 December 2021.
14. ^ Preskill, John (2018). "Quantum Computing in the NISQ era and beyond". Quantum. **2**: 79. arXiv:1801.00862. doi:10.22331/q-2018-08-06-79. S2CID 44098998.
15. ^ Gibney, Elizabeth (2 October 2019). "Quantum gold rush: the private funding pouring into quantum start-ups". Nature. **574** (7776): 22–24. Bibcode:2019Natur.574...22G. doi:10.1038/d41586-019-02935-4. PMID 31578480.
16. ^ Rodrigo, Chris Mills (12 February 2020). "Trump budget proposal boosts funding for artificial intelligence, quantum computing". The Hill.
17. ^ Gibney, Elizabeth (23 October 2019). "Hello quantum world! Google publishes landmark quantum supremacy claim". Nature. **574** (7779): 461–462. Bibcode:2019Natur.574..461G. doi:10.1038/d41586-019-03213-z. PMID 31645740.
18. ^ Aaronson, Scott (30 October 2019). "Opinion | Why Google's Quantum Supremacy Milestone Matters". The New York Times. ISSN 0362-4331. Retrieved 25 September 2021.
19. ^ "On 'Quantum Supremacy'". IBM Research Blog. 22 October 2019. Retrieved 9 February 2021.
20. ^ Pan, Feng; Zhang, Pan (4 March 2021). "Simulating the Sycamore quantum supremacy circuits". arXiv:2103.03074 [quant-ph].

Impact Factor: 8.118

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details