Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 13, No. 1, (2022),
ISSN : **1906-9685**

Current Challenge and Limitations in Quantum Computation

Rajkumar Saini
Assistant Professor
Computer Science Engineering
Arya Institute of Engineering and Technology, Jaipur, Rajasthan

Ranu Sewada
Assistant Professor
Computer Science Engineering
Arya Institute of Engineering and Technology, Jaipur, Rajasthan

Aaryan Arora
Science Student
Shri Lal Bahadur Shastri S S Sr Sec Sch, Sadokan Road, Nagaur , Rajasthan
Baid Goutam Sunil Kumar
Science Student
Godavari International Public School and Jr. College, Nanded, Maharashtra

I. Abstract:

This paper reviews various engineering hurdles facing the field of quantum computing. Specifically, problems related to decoherence, state preparation, error correction, and implement ability of gates are considered. Computer computation is very advanced computers used in recent days for various applications, including cryptography, optimization problems, financial modelling, route and traffic optimization, manufacturing drug, chemical research, batteries, simulation of quantum systems, and even machine learning. In a quantum computer, two qubits can also represent the exact same four states (00,01,10 or 11). It's an exciting field with lots of potential. But it faces lots of challenges and problems like maintaining qubits, interaction with the environment can cause decoherence. However, the adventure to harness the enormous power of quantum computer systems is packed with challenges and boundaries. In this

http://doi.org/10.36893/JNAO.2022.V13I02.0026-035

discussion, we can embark on an exploration of the current boundaries that researchers and engineers face within the world of quantum computing, losing mild on the complexities and constraints that ought to be overcome to fully free up its ability. Reacher's are working on error correction techniques to address this issue and make quantum computations more reliable. It's fascinating area of ongoing research. In recent development in quantum computing on 4 October 2022 The Royal Swedish Academy of Sciences has decided to award the Nobel Prize in Physics 2022 to Alain Aspect (Institute d'Optique Graduate School – Université Paris-Saclay and École Polytechnique, Palaiseau, France), John F. Clauser (J.F. Clauser & Assoc., Walnut Creek, CA, USA) Anton Zeilinger University of Vienna, Austria"for experiments with entangled photons, establishing the violation of Bell inequalities and pioneering quantum information science"

Keywords:

Quantum Computing, Qubits, Hardware Challenges, Quantum Algorithms Quantum Cryptography, Energy Consumption

II. Introduction:

Quantum mechanics is as a branch of physics in the early 1900s to explain nature on the topic of atoms and led it to advances such as transistors, lasers, and magnetic resonance imaging. The idea to merge quantum mechanics and information theory arise in the 1970s but collect little attention until 1982, when physicist Richard Feynman gave a talk in which he mentioned that computing based on classical logic could not tractably process calculations describing quantum phenomena. Computing based on quantum phenomena configured to simulate other quantum phenomena, however, would not be subject to the same narrowing. Although this application eventually became the field of quantum simulation, it didn't speed up much research activity at the time.

In 1994, however, interest in quantum computing increase dramatically when mathematician Peter Shor developed a quantum algorithm, which could find the prime factors of large numbers efficiently. Here, **"**efficiently**"** means in a time of practical relevance, which is beyond the capability of state-of-the-art classical algorithms. Although this may seem simply like an oddity, it is impossible to overstate the importance of Shor's insight. The security of nearly every online transaction today relies on an RSA cryptosystem that hinges on the intractability of the factoring problem to classical algorithms. The field of quantum computing emerged in the 1980s. It was discovered that certain computational problems could be tackled more efficiently with quantum algorithms than with their classical counterparts. Quantum computing has the capability to sift through huge numbers of possibilities and extract potential solutions to complex problems and challenges. Where classical computers store information as bits with either 0s or 1s, quantum computers use qubits. Qubits carry information in a quantum state that engages 0 and 1 in a multidimensional way. Such massive computing potential and the projected market size for its use have

http://doi.org/10.36893/JNAO.2022.V13I02.0026-035

attracted the attention of some of the most prominent companies. These include IBM, Microsoft, Google, D-Waves Systems, Alibaba, Nokia, Intel, Airbus, HP, Toshiba, Mitsubishi, SK Telecom, NEC, Raytheon, Lockheed Martin, Righetti, Biogen, Volkswagen, and Amgen. Quantum computation is a different type of computer which is totally different from classical computer. It's is based on the subject of quantum physics like proton, electron, atom and almost everything in the molecular and sub molecular atoms and specialized in very advance problem solving. Its behavior is totally different from classical computers. it's working on qubits. Quantum computing works on superposition and entanglement (quantum physics).

Quantum and classical computers both try to solve problems, but the way they manipulate data to get answers is fundamentally different. This section provides an explanation of what makes quantum computers unique by introducing two principles of quantum mechanics crucial for their operation, superposition and entanglement.

Superposition is the counter intuitive ability of a quantum object, like an electron, to simultaneously exist in multiple "states." With an electron, one of these states may be the lowest energy level in an atom while another may be the first excited level. If an electron is prepared in a superposition of these two states it has some probability of being in the lower state and some probability of being in the upper. A measurement will destroy this superposition, and only then can it be said that it is in the lower or upper state .Understanding superposition makes it possible to understand the basic component of information in quantum computing, the qubit. In classical computing, bits are transistors that can be off or on, corresponding to the states 0 and 1. In qubits such as electrons, 0 and 1 simply correspond to states like the lower and upper energy levels discussed above. Qubits are distinguished from classical bits, which must always be in the 0 or 1 state, by their ability to be in super positions with varying probabilities that can be manipulated by quantum operations during computations.

Entanglement is a phenomenon in which quantum entities are created or manipulated such that none of them can be described without referencing the others. Individual identities are lost. This concept is exceedingly difficult to conceptualize when one considers how entanglement can persist over long distances. A measurement on one member of an entangled pair will immediately determine measurements on its partner, making it appear as if information can travel faster than the speed of light. This apparent action at a distance was so disturbing that even Einstein dubbed it "spooky"

The popular press often writes that quantum computers obtain their speedup by trying every possible answer to a problem in parallel. In reality a quantum computer leverages entanglement between qubits and the probabilities associated with superpositions to carry out a series of operations (a quantum algorithm) such that certain probabilities are enhanced (i.e., those of the right answers) and others depressed, even to zero (i.e., those of the wrong answers). When a measurement is made at the end of a computation, the probability

http://doi.org/10.36893/JNAO.2022.V13I02.0026-035

of measuring the correct answer should be maximized. The way quantum computers leverage probabilities and entanglement is what makes them so different from classical computers.

Despite of having lots of research and development it's is facing lots of challenges and limitations in recent times in which research is going on to solve that problems and improve it for the betterment of the technology. Let's move towards the limitations and talk about it .

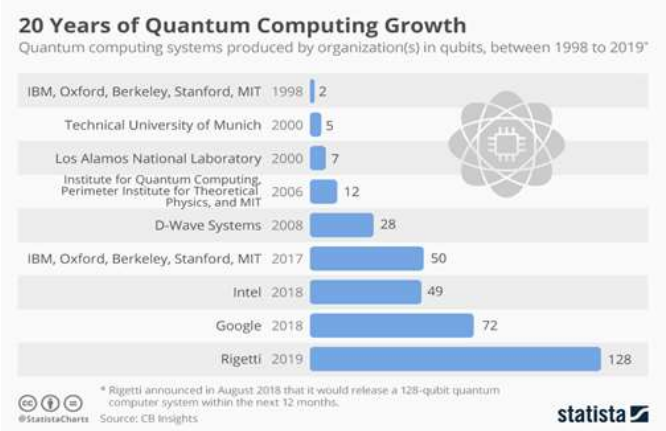

Figure 1. 20 years of quantum computing growth

Challenges And Limitations

1. Sensitivity to interaction with environment

Quantum computers are extremely sensitive to interaction with the surroundings since any interaction (or measurement) leads to a collapse of the state function. This phenomenon is called decoherence. It is extremely difficult to isolate a quantum system, especially an engineered one for a computation, without it getting entangled with the environment . The larger the number of qubits the harder is it to maintain the coherence. In a recent review, H.D. Zeh argues that decoherence cannot be reversed by redundancy coding: "Dislocalization of superpositions requires a distortion of the environment _by the system φ rather than a distortion of the system by the environment (such as by classical "noise"). This leads to the important consequence that decoherence in quantum computers cannot be error-corrected for in the usual manner by means of redundant information storage. Adding extra physical quantum bits to achieve redundancy, as it would be appropriate to correct spin or phase flips in the system, would in general even raise the quantum computer's vulnerability against decoherence – for the same reason as the increased size of an object normally strengthens its classicality. ("Error correction codes proposed in the literature for this purpose are based on the presumption of decoherence-free auxiliary qubits, which may not be very realistic.)" In another paper , the influence of spontaneous symmetry breaking on the decoherence of a many-particle quantum system was studied and it was shown that this symmetry breaking imposes a fundamental limit to the time

http://doi.org/10.36893/JNAO.2022.V13I02.0026-035

that a system can stay quantum coherent. Miniaturization of the systems seems to lower the time limit. This means that the decoherence constraints on quantum computing are even more severe than thought before.

2. Reliable matrix transformations

Quantum computation on qubits is accomplished by operating upon them with an array of transformations that are implemented in principle using small gates . It is imperative that no phase errors be introduced in these transformations. But practical schemes are likely to introduce such errors. It is also possible that the quantum register is already entangled with the environment even before the beginning of the computation. Furthermore, uncertainty in initial phase makes calibration by rotation operation inadequate . In addition, one must consider the relative lack of precision in the classical control that implements the matrix transformations. This lack of precision cannot be completely compensated for by the quantum algorithm.

4. Errors and their correction

Computation invariably involves errors, which are internal or externally induced. The classical computers have the capacity to perform well because the non-linearly (clamping or hard-limiting) of the computation process makes it possible to eliminate small errors, subsequent to which the larger bit errors can be eliminated using error-correction coding. In the proposed quantum error correction schemes, the assumption is that only qubit is in error but the method would not work if we have more than one qubit error. Current error correcting algorithms. Consider only bit flips, phase flips or both between the relative phases but these are not all the errors that we might encounter in a quantum computation. Unlike the situation in classical computing, small errors cannot be eliminated in quantum computing as it is a linear process, and it rules out operations analogous to clamping and hard-limiting. Furthermore, the no-cloning theorem prevents us from copying an unknown state and doing additional testing on it. Random unitary transformation errors can occur in initializing a qubit. The important characteristics of errors that need to be considered are component proliferation, non local effects and amplitude errors. In a quantum register the errors can be due to a variety of reasons and we cannot group the errors in a systematic way. Errors perturbation of information in quantum arena is non local compared to the local in classical arena and hence the concept of controlling errors using higher dimensional code word space is not realistic. Constraints on state preparation State preparation is the essential first step to be considered before the beginning of any quantum computation. In most schemes, the qubits need to be in a superposition state for the quantum computation to proceed correctly. We have a variety of problems due to the nature of superposition and entanglements, and state transition using local transformations is not realistic in a large system. Macro systems that have been used as model quantum computing systems appear to implement not pure states but mixtures. Thus, it appears that the NMR experiments do not validate quantum algorithm. Quantum statistical constraints also need to be

http://doi.org/10.36893/JNAO.2022.V13I02.0026-035

considered while designing algorithms to be used in quantum computers as they will directly affect the computation. Since this is not always done, it appears that many models are unrealistic.

5. **Constraints on state preparation**

State preparation is the essential first step to be considered before the beginning of any quantum computation. In most schemes, the qubits need to be in a superposition state for the quantum computation to proceed correctly. We have a variety of problems due to the nature of superposition and entanglements, and state transition using local transformations is not realistic in a large system. Macro systems that have been used as model quantum computing systems appear to implement not pure states but mixtures. Thus it appears that the NMR experiments do not validate quantum algorithm. Quantum statistical constraints also need to be considered while designing algorithms to be used in quantum computers as they will directly affect the computation . Since this is not always done, it appears that many models are unrealistic . Quantum information, uncertainty and entropy of quantum gates Classical information is easy to obtain by means of interaction with the system. On the other hand, the impossibility of cloning means that any specific unknown state cannot be determined. This means that unless the system has specifically been prepared, our ability to control it remains limited. The average information of a system is given by its entropy. The determination of entropy would depend on the statistics obeyed by the object . If the gate is a physical device then from an information point of view its control can be characterized in terms of entropy. For example, consider the quantum teleportation protocol implemented with a rotation Hadamard gate . The state cannot be recovered if the angle of rotation is less than the precision available on the receiving side. Computation with noisy components would require that the quantum circuit employed have the entropy rate smaller than the information capacity of the controller used. Kak has argued "The control of the gate – a physical device – is by modifying some classical variable, which is subject to error. Since one cannot assume infinite precision in any control system, the implications of varying accuracy amongst different gates becomes an important problem. In certain arrangements a stuck fault cannot be reversed down the circuit stream using a single qubit operator, for it converted a pure state into a mixed state."

III. Previous Research:

In last decade quantum computing grow from a niche research endeavour to a large-scale business operation. While it's exciting that the field is experiencing a surge of private funding and media publicity, it's worth remembering that nobody yet knows how to build a useful fault-tolerant quantum computer. The path ahead is not "just engineering", and in the coming decade we have to pay attention to all the "alternative approaches", "crazy ideas" and "new ways of doing things". Some of names in research are as follows :

1.Electrical Control of Quantum Phenomenon Could Improve Future Electronic Devices

2.Exploring Parameter Shift for Quantum Fisher Information

3.A New Way to Erase Quantum Computer Errors.

http://doi.org/10.36893/JNAO.2022.V13I02.0026-035

4.Powering the Quantum Revolution: Quantum Engines on the Horizon

5. Machine Learning Used to Probe the Building Blocks of Shapes.

IV. In recent development in quantum computing on 4 October 2022 The Royal Swedish Academy of Sciences has decided to award the Nobel Prize in Physics 2022 to Alain Aspect (Institute d'Optique Graduate School – Université Paris-Saclay and École Polytechnique, Palaiseau, France), John F. Clauser (J.F. Clauser & Assoc., Walnut Creek, CA, USA) Anton Zeilinger University of Vienna, Austria"for experiments with entangled photons, establishing the violation of Bell inequalities and pioneering quantum information science"

V. Future Of Quantum Computating:

In coming years the quantum computing will replace the classical computing completely and also takes the place in industries. It will use in machine learning, financial modelling and many more such field n In short, quantum computing can deliver better quality results faster. Let's now discus some of them in brief. Here are several practical applications of quantum computing we could see in the future:

AI and machine learning (ML). The capability of calculating solutions to problems simultaneously, as opposed to sequentially, has huge potential for AI and ML. Organizations today use AI and ML to discover ways to automate and optimize tasks. When used in combination with quantum computing, optimization can happen much faster and at scale, especially when processing and analyzing highly complex or even unstructured big data sets.

Financial modeling. With the modeling capabilities of quantum computing, financial organizations could use the technology to better model the behavior of investments and securities at scale. This could help reduce risk, optimize large-scale portfolios and help financial organizations better understand the trends and movements of the global financial economy.

Cybersecurity. Quantum computing could have a direct impact on privacy and encryption. Given the rapidly evolving nature of the cybersecurity landscape, quantum computers could help keep data encrypted while in use, providing both in-transit and at-rest protections.

Route and traffic optimization. Optimal route planning is key to smooth supply chain logistics and transportation. The biggest challenge is harnessing all the real-time data -- from changing weather patterns to traffic flow -- that affects this planning. This is where quantum computers can excel. They could process all that data in real time and adjust routes for an entire fleet of vehicles at once, putting each on the optimal path forward.

Manufacturing. Quantum computers can run more accurate and realistic prototyping and testing. In the manufacturing space, this could help reduce the cost of prototyping and result in better designs that don't need as much testing.

http://doi.org/10.36893/JNAO.2022.V13I02.0026-035

Drug and chemical research. Quantum computers can create better models for how atoms interact with one another, leading to a superior and more precise understanding of molecular structure. This may directly impact drug and chemical research and impact the way new products and medicines are developed. The predictive power of quantum computers could also provide foresight into how chemical compounds and drugs would develop, evolve and interact with other elements over time.

Batteries. Quantum computing could help manufacturers better understand how to incorporate new materials into products such as batteries and semiconductors. This could provide more insight into how to optimize batteries for longevity and efficiency. Quantum computing can also help manufacturers gain a better understanding of lithium compounds and battery chemistry. For example, quantum computing could tap into and understand how the docking energy of proteins works, which results in better batteries for electric vehicles.

How data centres can adapt as quantum computing becomes mainstream

It will take time before organizations can apply quantum computing in their operations on a wider scale -- anywhere from five to 10 years at the earliest -- but it's never a bad idea to keep an eye on trends and advancements in the space as the tech develops. Data centre admins should already track disruptive trends to stay one step ahead of the curve, but this goes double for quantum computing. Watch the thought leaders in the space, and take note of risks and opportunities.

VI. Conclusion:

http://doi.org/10.36893/JNAO.2022.V13I02.0026-035

We have examined several problems associated with the implementation of quantum computers and we conclude that we currently do not possess technical solutions related to the fundamental tasks of quantum gate design, state preparation, and error correction. The basic problem of implementation is a result of quantum computation being essentially an analog process. Using unitary transformations to solve real problems involving rotations, as in factorization, is an attractive mathematical idea, but there remain fundamental engineering hurdles in the implementation of this idea.

References:

1) R. Landauer, Irreversibility and heat generation in the computing process. IBM J. Res. Dev. 5: 183-190, 1961.

2) C.H. Bennett, The thermodynamics of computation – a review. Int. J. Theo. Phys., 21, pp. 905-940, 1982

3) S. Kak, On information associated with an object. Proc. of the Indian National Science Academy, 50: 386-396,

4) P.W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Computing 26, 1474, 1997.

5) L. K. Grover, A fast quantum mechanical algorithm for database search. Proceedings, 28th Annual ACM Symposium on the Theory of Computing, pp. 212-219, 1996.

6) C.H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing. Proceedings IEEE Intl. Conf. On computers, Systems and Signal Processing. Bangalore, 1984.

7) S. Kak, Quantum key distribution using three basis states. Pramana 54: 709-713, 2000; arXiv: quant-ph/9902038. 13. S. Kak, A three-stage quantum cryptography protocol. Found. Phys. Lett. 19: 293- 296, 2006; arXiv: quant-ph/0503027.

8) M. A. Nielsen and I.L. Chuang, Quantum Computation and Quantum Information. Cambridge University Press, 2000.

9) W.H. Zurek, Decoherence and transition from quantum to classical. Physics Today, October 1991.

10) D. Jonathan, M. B. Plenio, Minimal conditions for local pure-state entanglement manipulation. Phys. Rev. Lett., 83, pp. 1455-1458, 1999.

11) M. Schlosshauer, Decoherence, the measurement problem, and interpretations of quantum mechanics. Rev Mod Physics Vol. 76, pp. 1267-1305, 2004.

12) J. van Wezel, J. van den Brink, J. Zaanen, An intrinsic limit to quantum coherence due to spontaneous symmetry breaking" Phys. Rev. Lett., 94, 230401, 2005.

http://doi.org/10.36893/JNAO.2022.V13I02.0026-035

13) D. P DiVincenzo, Two-bit gates are universal for quantum computation. Phys. Rev. A, 51, pp. 1015-1022, 1995.

14) K. Svore, B.M. Terhal, D. P. DiVincenzo, Local fault-tolerant quantum computation. arXiv: quant-ph/0410047.

15) D.G. Cory, A.F. Fahmy, and T.F. Havel, Ensemble quantum computing by NMR spectroscopy. Proc. Nat. Acad. Sci. USA, 94: 1634-1639, 1997.

16) S. L. Braunstein, C. M. Caves, R. Jozsa, N. Linden, S. Popescu, R. Schack, Separability of Very Noisy Mixed States and Implications for NMR Quantum Computing. Physics Review Letters, 83, pp. 1054–1057, 1999.

17) *in Engineering (ICACITE)*, Greater Noida, India, 2021, pp. 415-420.

18) P. K. Bhatt and R. Kaushik, "Intelligent Transformer Tap Controller for Harmonic Elimination in Hybrid Distribution Network," *2021 5th International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, Coimbatore, India, 2021, pp. 219-225

19) R. Kaushik, O. P. Mahela and P. K. Bhatt, "Events Recognition and Power Quality Estimation in Distribution Network in the Presence of Solar PV Generation," *2021 10th IEEE International Conference on Communication Systems and Network Technologies (CSNT)*, Bhopal, India, 2021, pp. 305-311

20) Jain, B.B., Upadhyay, H. and Kaushik, R., 2021. Identification and Classification of Symmetrical and Unsymmetrical Faults using Stockwell Transform. *Design Engineering*, pp.8600-8609.

21) Rajkumar Kaushik, Akash Rawat and Arpita Tiwari, "An Overview on Robotics and Control Systems", *International Journal of Technical Research & Science (IJTRS)*, vol. 6, no. 10, pp. 13-17, October 2021.

http://doi.org/10.36893/JNAO.2022.V13I02.0026-035