FUTURE OF QUANTUM COMPUTING ALGORITHMS

Kartickey Aggarwal

BTech CSE
2018867

ABSTRACT

The future of quantum computing algorithms holds great promise for revolutionizing various fields such as cryptography, drug discovery, and supply chain optimization. With the rapid development of quantum hardware, it is expected that quantum algorithms will become increasingly efficient and practical, enabling new applications that were previously infeasible. In particular, quantum machine learning and quantum optimization algorithms are areas of active research that have the potential to greatly improve performance compared to classical algorithms. Furthermore, the development of hybrid classical-quantum algorithms may provide a bridge between the strengths of classical and quantum computing, leading to even more impactful solutions.

1 INTRODUCTION

Quantum computing exploits quantum-mechanical effects superposition, entanglement, and quantum tunneling to execute a computation more efficiently. In comparison to traditional computing, quantum computing provides a huge advantage over computational speed and accuracy.

Quantum computers are not an advancement to classical computers but a whole different concept. A classical computer works on mathematical operations and algorithms, whereas a quantum computer uses quantum mechanics and quantum laws.

For example, there is a game of heads and tails played between a classical computer and a user in which each flips a coin and if the result is what user predicted, the user wins. In a classical computer the winning rate of user will be around 50 percent because a classical computer is either in '0' state or '1' but the chance of the computer winning in a quantum computer will rise to 99 percent, this happens because in a quantum computer the result lies between '0' and '1' both and the result is generated only when the result is asked.

There are numerous quantum computing algorithms used to implement quantum computation. Quantum computing algorithms can revolutionize the computing landscape soon. These algorithms can solve complex problems much faster than traditional computing methods, and they are able to tackle problems that are intractable using classical computing methods.

The recent developments in quantum computing have opened new possibilities for researchers and industrialists to explore. This research paper will discuss the current state of various quantum computing algorithms that are currently available for quantum computing. It will also include a comparison of the different algorithms for quantum computing and their respective strengths and weaknesses. Next, the paper will discuss the current trends in quantum computing algorithms. This will include an analysis of the current research being done in this field, an exploration of the current direction of research, and an exploration of the potential applications of quantum computing algorithms. Finally, the paper will conclude by discussing the prospects of quantum computing algorithms and their potential to revolutionize the computing landscape.

2 GROVER'S ALGORITHM

2.1 Introduction

Grover's Algorithm, one of the most used quantum algorithms, is used to search a specific item in a randomly ordered pair."Grover's algorithm is a quantum algorithm that solves the problem of unstructured search.It finds with high probability the unique input to a black box function that produces a particular output value, using just Grover's Algorithm is supposed to provide quadratic speed up over classical computing algorithms. While a classical computer takes O(N) time to do the job, on the contrary a Grover's Algorithm takes only O($\sqrt{N}$) searches to do so"[1]. Grover's Algorithm is optimal in the sense that no quantum Turing machine can do the job in less than O($\sqrt{N}$).

Not only searching a specific item, Grover's Algorithm can be used in much wider context. It can be used to speed up search algorithms where a quantum oracle can be constructed. It is more commonly used to separate needle from a haystack but both the needle and the haystack has to be the part of the database.

2.2 Algorithm Description

Suppose a number N is being search in the database. So, the Grover's Algorithm will find the iterations of all the elements called Grover's iterations and will store these iterations in the databse. Then an operator known as Grover's Operator Ux is applied on these iterations. The Grover's Operator amplifies the amplitude of the targeted element while decreasign the amplitude of all the other elements. The algorithm keeps doing this untill the amplitude of the targeted element is significatly higher than all the other elements in the database. For example take the below circuit:- The circuit is a 2 qubit quantum circuit for Grover's

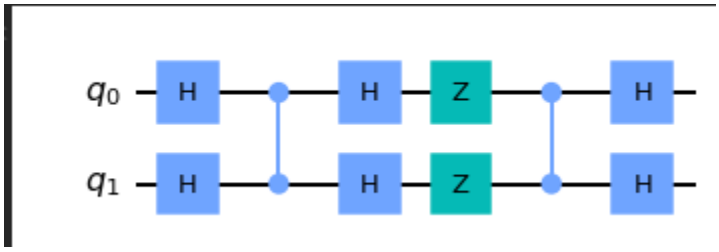

Figure 1: Grover's Circuit for find '11' in oracle

Algorithm. In the circuit, it is hard coded to search '11' in the oracle. The probabilty graph will be as follows:-

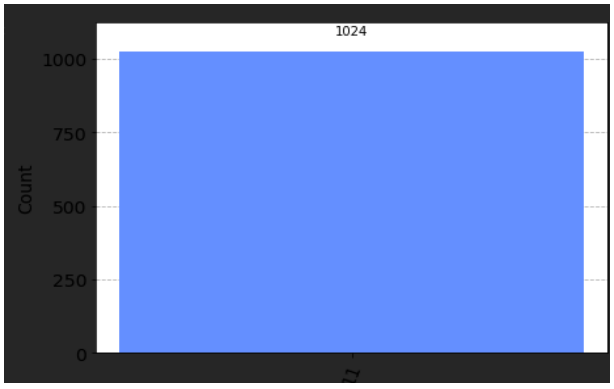

Figure 2: Probability of finding '11' in oracle

2.3 Limitations

Though Grover's can be used to speed up search algorithms, it has its limitations.

For example, it could be used to search two integers between 1 ¡ a ¡ b such that ab =n for some integer n, it would turn into a factoring algorithm and of course Grover's can't match the performance of Shor's algorithm for the purpose.

Added to this, the probability of the search algorithm is around 50% - 60% which is much less than the probability simulated by the simulators. Deeper and more complex oracles will lead to less satisfactory results and less accuracy.[2]

2.4 Conclusion

"Reading a full database item by item and converting it into such a representation may take a lot longer than Grover's search. To account for such effects, Grover's algorithm can be viewed as solving an equation or satisfying a constraint"[3]. Though, Grover's Algorithm provides a quadratic speed up, but it still lacks in accuracy and handling large and complex oracles. Grover's Algorithm still needs to be developed further in order to be used in future quantum computers. Currently we have very less qubit quantum computers for which Grover's Algorithm works fairly well, but as the qubits will increase, the probability of success will decrease and we will need to find better ways to perform the functions. So Grover's Algorithm needs to be improved in order to perform well and give satisfactory results in future.

3 SHOR'S ALGORITHM

3.1 Introduction

Every integer has a unique decomposition in the products of prime numbers, but factoring an integer is considered to be an uphill task. As factoring an integer having thousands of digits seems to be impossible, it is used in the security of our online transactions and cryptography. So, to solve the problem of factoring Peter Shor came up with an algorithm which solves the problem in polynomial time.

"Shor's algorithm is arguably the most dramatic example of how the paradigm of quantum computing changed our perception of which problems should be considered tractable".[4] Suppose we need to factor an integer N with d decimal digits, brute force algorithm goes to all primes from p to $\sqrt{N}$ and check whether p divides N or not. The worst case will take $\sqrt{N}$ time to solve the problem.

Shor's algorithm turns this factoring problem into perioding problem. Suppose we are given co-prime integers a,N. So, Shor's algorithm computes the period of a modulo N, for the smallest integer r such that $a^r = 1(moduloN)$ basic idea is to construct a unitary operation U that implements the modular multiplication function x -¿ ax(modulo N).

3.2 Algorithm Description

Reducing factorization to period finding. One way to factor an integer is by using modular exponentiation. Specifically, let an odd integer N = N1*N2 be given where, 1¡N1*N2¡N. Pick any integer k¡N such that gcd of(k,N) = 1, where gcd denotes the greatest common divisor. It can be shown that there exist an exponent p¿0 such that $k^p = 1(modN)$

$$(k^p - 1 = (k^p/2 - 1)(k^p/2 + 1))$$

But since the difference between N1 = $k^p/2+1$ and N2 = $k^p/2-1$ is 2, N1 and N2 have no common factor greater than 2. Moreover, both numbers are nonzeros by the minimality of p. Since N = N1*N2 was assumed to be odd, then N1 is a factor of either N1 or N2. Assume N1 is a factor of n1. Since N1 is also a factor of n, then N1 divides both n1 and N and one can find N1 by computing gcd(n1, N). Hence, if

one can compute such a p, one can find the factors of N efficiently as gcd can be computed in polynomial time.[5]

The Shor's ALgorithm finds a quantum fourier transform of the number to find its factors and turns the problem into a perioding problem. For example below is the quantum fourier transform of 32 done by Shor's Algorithm.

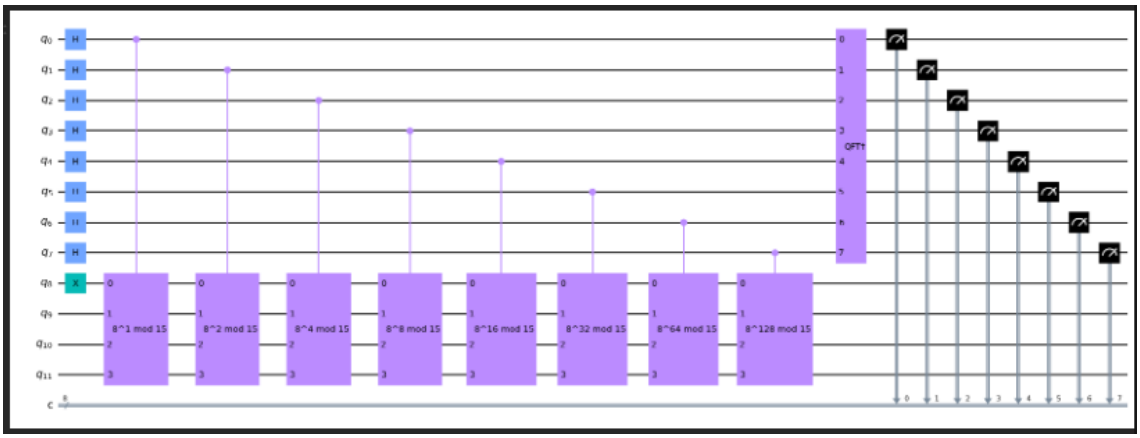

Figure 3: Quantum Fourier Transform of 32

3.3 Limitations

Although Shor's quantum factorization algorithm reduces to find period of a periodic sequence, but until optimized, the general case for factorizing small numbers like 15 can be too large, both with respect to number of qubits and number of resources used as well as the number of gates, to be implemented on 5 qubit system.

In the current state, either we need to increase the qubits available or optimize Shor's algorithm to work with the present quantum computers available. Until optimized, it will be nearly impossible to implement Shor's algorithm. We are able to produce correct results with the algorithm, however, comparing the results with the simulator produced a lot of noise.

Moreover, the algorithm is probabilistic, which means that it may not find the factors of a given number in a single run, and may require multiple runs to find the factors.

3.4 Conclusion

Shor's Algorithm is one of the best algorithm when it comes to factorizing a number, but it still lacks the development and optimization to work with current quantum systems available. So, to go along with the future trends and work with the current we need to find a better alternative to it as it is not yet clear whether Shor's algorithm should be opted for factoring polynomials.

4 QUANTUM SIMULATION

4.1 Introduction

Quantum simulation is a type of algorithm which is used to simulate the behavior of quantum systems, behavior of molecules, atoms, and subatomic particles. It is most widely used in the field of chemistry and research.

The basic idea behind quantum simulation is to use a quantum computer to model the dynamics of a quantum system. This is done by encoding the properties of the system into the state of the quantum computer and using quantum gates to evolve the state of the system over time.

One of the most well-known examples of a quantum simulation algorithm is the Quantum Phase Estimation algorithm, which is used to estimate the energy eigenvalues of a Hamiltonian. This algorithm is based on the observation that the eigenvalues of a Hamiltonian can be determined by measuring the phase of a quantum system that is in an eigenstate of the Hamiltonian.

"The advantage of quantum simulators over classical devices is that, being quantum systems themselves, they are capable of storing large amounts of information in a relatively small amount of physical space. For example, the storage capacity of N qubits is exponentially larger than that of N classical bits."[7]

4.2 Algorithm Description

Considering a search problem with a unique solution, we should be able to find the solution with the form of the Hamiltonian, when all possible items are encoded in a superposition state $|\psi>$ and given as the initial state, same as in Grover's algorithm, while $|x>$ The following circuit encodes the phase π on the solution state and zero on the other items through phase kickback with the 5th qubit as an auxiliary. Therefore, the

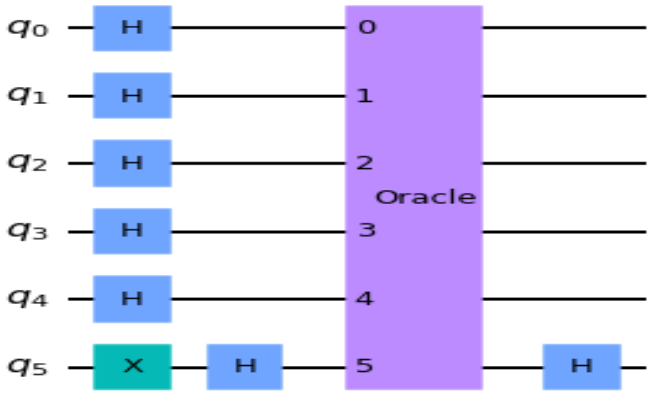

Figure 4: Circuit for Quantum Simulation

output state of the circuit is $|\psi> - |x>) + e^i e^{\pi}|x>$, which can be confirmed visually using a qsphere plot where the color indicates the phase of each basis state.[6]

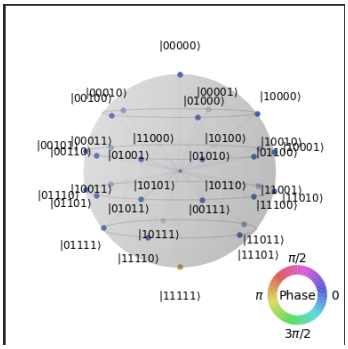

Figure 5: Bloch Sphere

Looking at the above circuit and the bloch sphere we can evolve the qubit over time in a quantum computer to see various outcomes and simulate the behaviour of the qubits. It can also be used to search for a particular no. or a state by running various simulations.

4.3 Limitations

Quantum simulation has a very wide implementation in numerous fields. It is used in chemistry, physics and determining the behavior of quantum systems. However, it is still in development phase and it is still unclear how well these algorithms will perform on practical levels due to the limitation of quantum technology currently available. To apply most of the quantum simulations there is a need to develop quantum computers. Added to this, the algorithm is followed by many problems such as, efficiency and accurate methods for simulations.

Quantum computers are very sensitive to noise around them and even a small amount of noise can interfere with the results of simulations. Moreover, applying simulations on large quantum systems can be computationally complex and it is yet not clear how to use the algorithm efficiently.

Conclusion

So, quantum simulation is a wide field to research and includes constant developing and studying of new methods to apply the algorithm. Currently it is exceedingly difficult to understand the algorithm fully due to the lack of resources.

5 QUANTUM KEY DISTRIBUTION

5.1 Introduction

Quantum Key distribution (QKD) is an algorithm used for cryptography which makes use of state of a photon which makes it nearly impossible to crack, also making it resistant to eavesdropping. Quantum cryptography used the concepts of physics which makes it impossible for the hacker or eavesdropper to crack the code.

Because of the fundamental properties of quantum mechanics, any attempt to intercept or measure the key will inevitably introduce errors or disturbance to the system, which can be detected by the sender and receiver which allows a secure connection between the two and makes the sharing the encryption key secure and seamless.

QKD can be seen as a solution to the key exchange problem and can be used to provide an unconditionally secure communication channel.

5.2 Algorithm Description

QKD is a method for securely distribution of encryption key using the principles of quantum mechanics and creating a channel between the sender and the receiver.

It encodes the key on photons which is then transmitted through optical fibers. This can then be decoded using the conventional methods. Encoding the key on photons makes it sensitive to changes and any changes made to the key or any attempt of eavesdropping can immediately be caught.

Moreover, using a quantum system and methods based on it makes it impossible for the intruder to make any changes to the key making the transfer of information secure.

Suppose a person has to send an information to his friend lets say ”0”. What he will do is he will prepare a qubit and encode it according to his basis keeping it private to himself. The qubit should look like Fig. 6 if he encodes it on X-basis and the friend also measures it in X- basis. The friend is sure to find ”0”

if there are no interceptions. Now suppose there is an eavesdropper who tried to read the message before

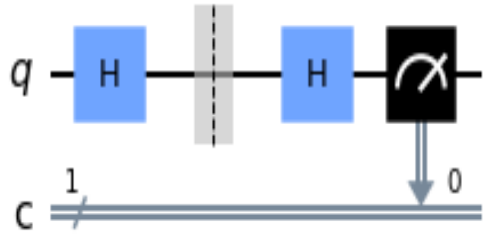

Figure 6: Qubit sent and received

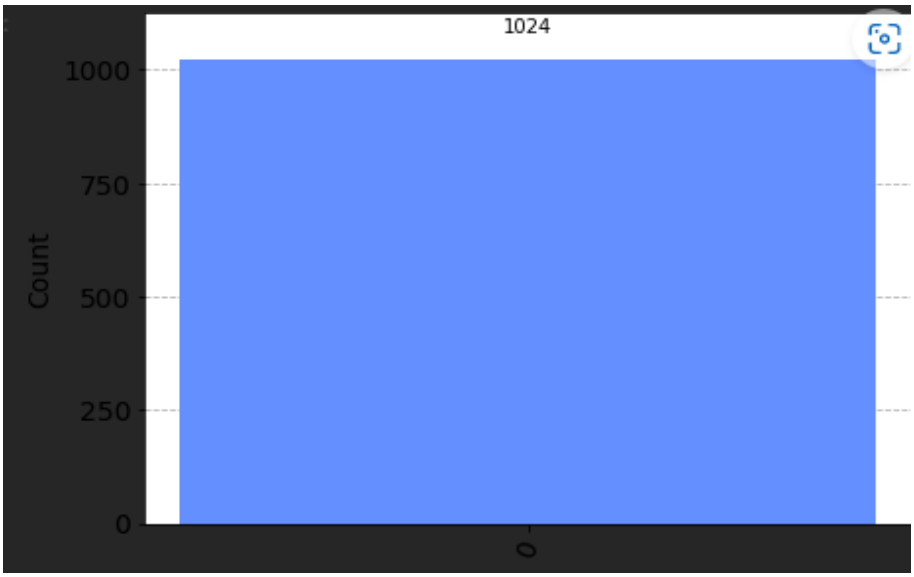

Figure 7: Probability of finding ”0”

it reaches the receiver, so, the qubit should look like Fig. 8 and the receiver will have a 50% of finding ”1” and ”0” which will make them aware that there had been an interception in the message. So, Quantum key distribution provides high security while sharing information and messages making it impossible for the eavesdroppers to change the messages or the information received as any type of interception can easily be caught.[8]

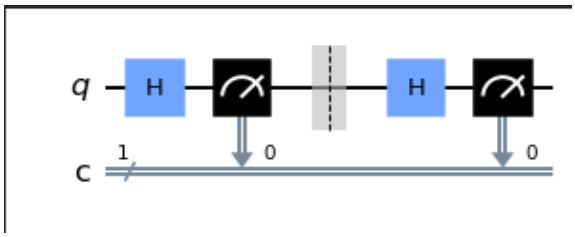

Figure 8: Qubit when there is interception

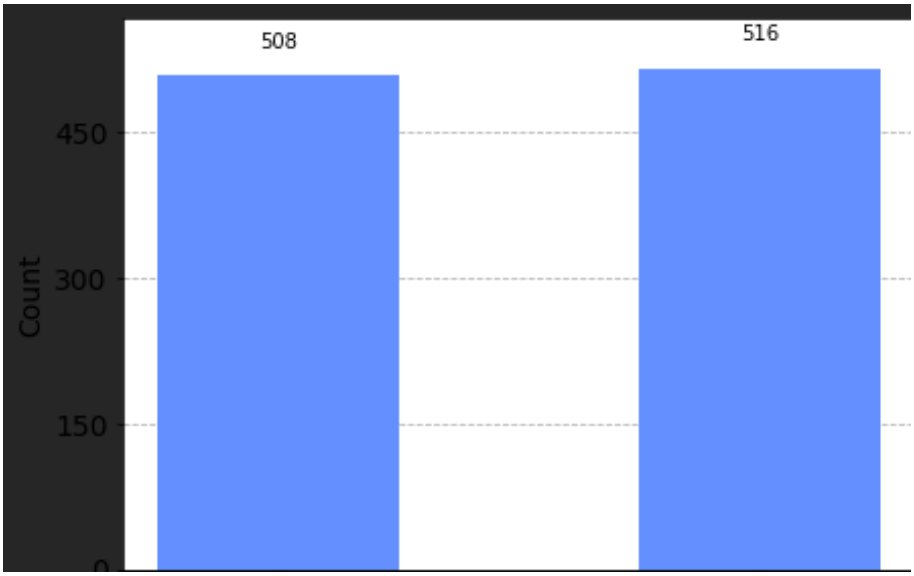

Figure 9: Probabilty of finding desired message

5.3 Limitations

QKD is a promising field of study sure to deliver promising results over time, but in the current state it doesn't seem to be an adoptable method. QKD is limited by the distance over which a photon is transmitted and the transmission medium. Currently QKD only works best for short distances as over a large distance the photons get lost and it can lead to errors in the information received.

Moreover, current communication infrastructure is more or less not compatible with QKD which makes it more difficult to adopt the technology.

While QKD provides unconditional security in theory, in practice the security of the system depends on various assumptions such as the trustworthiness of the devices and the absence of side-channel attacks. QKD systems can detect eavesdropping, but they cannot identify the source of the attack, making it difficult to hold the attacker accountable.

5.4 Conclusion

"Quantum key distribution (QKD),promises in principle unconditional security—the Holy Grail of communication security—based on the laws of physics only.QKD has the advantage of being future-proof unlike classical key distribution, it is not possible for an eavesdropper to keep a transcript of quantum signals sent in a QKD process, owing to the quantum non-cloning theorem".[9]

Quantum Key Distribution is still considered to be a promising technology for secure communication despite of its limitations and research is ongoing to address these limitations making it more practical for real-world applications. QKD has very few limitations and these limitations can be overcome with time and evolving technology. QKD can be a promising technology to use in the future for secure communication and information transfer.

6 QUANTUM NEURAL NETWORK

6.1 Introduction

Quantum Neural Network(QNN) is a quantum machine learning algorithm which makes the use of quantum qubits. Alike classical neural network, it has layers of interconnected nodes or neurons. It process information just like the human brain. However, QNN makes used of quantum system and principles of quantum mechanics to perform a task. It can be used for various purposes like optimization, quantum annealing and what not. However, it's still in early stages of development.

"The motivation behind quantum machine learning (QML) is to integrate notions from quantum computing and classical machine learning to open the way for new and improved learning schemes. QNNs apply this generic principle by combining classical neural networks and parametrized quantum circuits".[10]

6.2 Algorithm Description

In a QNN, the input data is first encoded into quantum states using quantum gates, similar to how classical neural networks use activation functions. The qubits then undergo a series of quantum operations that perform computations on the encoded data. Finally, the output is extracted by measuring the final state of the qubits.

There are several types of QNNs, including the quantum version of the classical neural network, known as the quantum neural network, and the quantum circuit-based approach, known as the variational quantum circuit. The latter is a more flexible approach that uses quantum circuits to represent the model and allows for greater control over the structure of the network.

6.3 Limitations

As QNN is still in its early stages of development, which prevents it from being widely adopted. There are only few algorithms available that can be used for machine learning and research is still going to develop better and more reliable algorithms.

Added to this, The field of quantum machine learning is still relatively new, and there is still much to be understood about how to design and train QNNs effectively. Also, QNN are based on quantum systems which are highly sensitive to noise and decoherence, so it becomes more prone to errors and noise which limits it form providing accurate results on more complex computations.

6.4 Conclusion

Despite of its limitations, QNN is a promising field of research and scientists are finding new ways to overcome these limitations such as adopting hybrid quantum-classical algorithms and quantum correction techniques.

7 FUTURE WORK

7.1 Cryptography

1. Quantum computing has the potential to significantly impact the future of cryptography. Traditional cryptographic methods rely on the computational complexity of mathematical problems to ensure security. However, quantum computers can potentially solve these problems much faster than classical computers, which could render current cryptographic protocols vulnerable to attacks.
2. Quantum computing has the potential to significantly impact the future of cryptography. Traditional cryptographic methods rely on the computational complexity of mathematical problems to ensure security. However, quantum computers can potentially solve these problems much faster than classical computers, which could render current cryptographic protocols vulnerable to attacks.
3. Cryptography will continue to emerge with IT and business plans in regard to protecting personal, financial, medical, and ecommerce data and providing a respectable level of privacy. As stated in [10],The future of cryptography relies on a management system generating strong keys to ensure that only the right people with the right keys can gain access, while others without the keys cannot.

7.2 Machine learning

1. Current machine learning algorithms processed on classical computers limits their ability to process data and give significant results with minimum errors. Quantum computing can revolutionize machine learning as quantum computers provide seamless accuracy and quantum machine learning algorithms speedup the process and works better than classical computers.
2. Quantum machine learning algorithms provides optimization such as finding the cost function to fit a data set or finding the local minima with least errors.
3. The generic nature of the quantum speed-ups for dealing with large numbers of high dimensional vectors suggests that a wide variety of machine learning algorithms may be susceptible to exponential speed-up on a quantum computer. Quantum machine learning also provides advantages in terms of privacy.

7.3 Energy and Environment

1. Quantum computing can change the problem of energy entirely. Quantum computing can help in finding new ways to extract different items and optimize the use of the items used to generate

energy. It can help cope up with emerging energy crisis and find new ways to use energy while also conserving the environment. Quantum computers can perform certain types of calculations much faster than classical computers, using significantly less energy. This means that quantum computing could help reduce the energy consumption of data centers and other computing facilities.

2. Quantum computing can help design new materials for use in renewable energy technologies, such as solar cells and batteries. By simulating the behavior of atoms and molecules, quantum computing can predict the properties of new materials and identify those that are most likely to be effective in capturing or storing energy.

7.4 Quantum optimization

1. Quantum computing can help optimize the complex network of suppliers, manufacturers, and distributors in a supply chain. By analyzing large amounts of data and making complex calculations, quantum computing can identify the most efficient ways to allocate resources and minimize costs.
2. Quantum computing can help optimize traffic flow by analyzing data on traffic patterns, road conditions, and other factors. By making complex calculations, quantum computing can identify the most efficient routes and help reduce congestion.

In summary, quantum computing and algorithms have the potential to revolutionize a wide range of fields, from chemistry and materials science to finance and logistics."Algorithms that make use of noisy quantum computers are in high demand. Clever algorithms can lower the physical and engineering requirements in order to build useful quantum machines. Such algorithms are useful not only because they provide applications and benchmarks for current quantum computers, but they provide insight into the potential of quantum computing and motivate efforts towards ever larger scale implementations".[11]

REFERENCES

[1] L.K. Grover. "a fast quantum mechanical algorithm for database search", proceedings of the 28th annual acm symposium on the theory of computing. pages 212–219, 1996.

[2] Scott Pakin Adetokunbo Adedoyin Patrick J. Coles, Stephan Eidenbenz. "quantum algorithm implementations for beginners". 2018.

[3] Andrew M. Childs Anirudh Ravi and Robin Kothari. "grover's search algorithm as a quadratic unconstrained binary optimization problem". 2019.

[4] IBM Quantum. Refer to the link https://quantum-computing.ibm.com/composer/docs/iqx/guide/shors-algorithm.

[5] Scott Pakin Adetokunbo Adedoyin Patrick J. Coles, Stephan Eidenbenz. "quantum algorithm implementations for beginners". 2018.

[6] Qiskit.org. Refer to the link https://qiskit.org/textbook/ch-labs/lab07$_{q}$*uantumsimulationsearchalgorithm.html*.

[7] Ivan M. Deutsch and Peter P. Rohde. "quantum simulation". 2017.

[8] Qiskit.org. Refer to the link https://qiskit.org/textbook/ch-algorithms/quantum-key-distribution.html.

[9] Bing Qi Eleni Diamanti, Hoi-Kwong Lo and Zhiliang Yuan. "practical challenges in quantum key distribution".

[10] Qiskit.org. Refer to the link https://qiskit.org/documentation/machine-learning/tutorials/01$_{n}$*eural*$_{n}$*etworks.html*.

[11] Rodney Van Meter and Mark Oskin. "the road ahead for quantum computing". 2018.