IET Quantum Communication

Review Article

Forthcoming applications of quantum computing: peeking into the future

eISSN 2632-8925
Received on 26th September 2020
Revised 5th November 2020
Accepted on 9th November 2020
E-First on 30th November 2020
doi: 10.1049/iet-qtc.2020.0026
www.ietdl.org

Vikas Hassija[1], Vinay Chamola[2] ✉, Adit Goyal[1], Salil S. Kanhere[3], Nadra Guizani[4]

[1]Department of CSE and IT, Jaypee Institute of Information Technology, Noida, India
[2]Department of Electrical and Electronics Engineering, BITS Pilani, Pilani, India
[3]School of Computer Science and Engineering, UNSW Sydney, Australia
[4]School of Electrical Engineering and Computer Science, Washington State University, Pullman, WA 99163, USA
✉ *E-mail: vinay.chamola@pilani.bits-pilani.ac.in*

Abstract: We all have been using classical computers for a long time. Quantum computing uses the phenomena of quantum mechanics like superposition and entanglement. Quantum computations can help achieve for the breakthroughs we have been looking for in science, machine learning, financial planning, medicine, etc., where classical computers' computing power is not enough. It was not long back when quantum computing's applications in our life were all just theoretical. However, to utilise the power of quantum computations for real-life applications, several recent developments have been made. Keeping that in mind, this study aims to explore the existing and upcoming applications of quantum computing. In this study, they start with an introduction of quantum computing fundamentals, following which, they give a brief overview of various applications of quantum computing in several significant areas of computer science, such as cryptography, machine learning, deep learning, and quantum simulations. They also cover various real-life scenarios such as risk analysis, logistics, and satellite communication.

1 Introduction

Classical computers have been around for a long time now, and they have played a significant role in scientific breakthroughs. Quantum computing, on the other hand, has shown promising results for solving such large complex problems. Quantum computers, generally, utilise the quantum mechanical phenomena of superposition and entanglement to create states that scale exponentially with the number of qubits or quantum bits [1].

The classical computers manipulate individual bits, 0 and 1, to store information as binary data, whereas quantum computers use the probability of an object's state before it is measured [2]. Therefore, it gives them the potential to process exponentially more data compared to classical computers. Unlike classical computers that use the binary bit, quantum computers use qubits that are produced by the quantum state of the object to perform operations. Since these qubits are quantum in nature, they follow phenomena like superposition and entanglement. Superposition is the ability of a quantum system to be in multiple states at the same time. Entanglement is the strong correlation between quantum particles. These phenomena help the quantum computer work with 0, 1, and superposition of 0 and 1, giving them the advantage in doing complex calculations that modern classical systems cannot do or would take a significant amount of time to get the desired result [3].

Currently, quantum computing is the metaphorical elephant in the room for researchers because of its potential for altering the time and space complexity of many algorithms we have been using, such as a solution to a linear system of equations [4]. With these changes, there is an increasing threat to the security of our data. Many cryptography systems rely on the complexity of the mathematical problems for their security. It was impossible to get an optimal solution for these problems in time, with the processing capacity of classical computers. However, since the advent of quantum computations, cryptography is at a significant threat [5]. There have been developments in research for post-quantum cryptography [6], and possibly, we will be able to transfer all the encrypted data to these 'quantum-safe' systems. Quantum simulation is one of the most promising and exciting areas of quantum computers, it has the potential to solve the complexities of molecular and chemical interactions, which can lead to the discovery of new medicines and materials.

This paper will give the readers a very broad perspective of the applications of quantum computers in the next four sections. Section 2 explains the various applications of quantum algorithms, such as the well-known Shor's algorithm in cryptography [7], and Grover's algorithm for unstructured search [8]. Section 3 deals with how some of the most basic and standard machine learning algorithms can be modified to be used on a quantum computer for faster and better results. Furthermore, Section 4 talks about various quantum simulations, and the need for quantum simulators for performing simulations that are beyond the scope of classical computers. Finally, Section 5 explains various day-to-day areas where quantum computers would be very useful to save cost and can provide a better quality of service [9]. An overview of this paper is shown in Fig. 1.

2 Applications of various quantum algorithms

Many different algorithms have been developed using the principles of quantum computing. These algorithms have shown significant improvements in terms of efficiency over their classical counterparts, and we have discussed a few of the most common algorithms in this section.

2.1 Cryptography

One of the first applications of quantum computing, i.e. Shor's algorithm [7], can break today's most widely used public-key cryptosystems, such as RSA that use complex mathematical problems such as integer factorisation as their basis for security. Given an integer $N = p \times q$ for some prime numbers p and q, Peter Shor was able to determine p and q in time $O(\log N^3)$. This is exponentially faster as compared to any existing classical algorithms.

Shor's algorithm is analogous to the hidden subgroup problem (HSP) for finite Abelian groups. The HSP is described by a group G, in the case of Shor's algorithm $G = \mathbb{Z}$. Other cryptosystems can be broken by solving the HSP for other G groups. In Table 1, we have summarised different HSPs, their corresponding groups, and

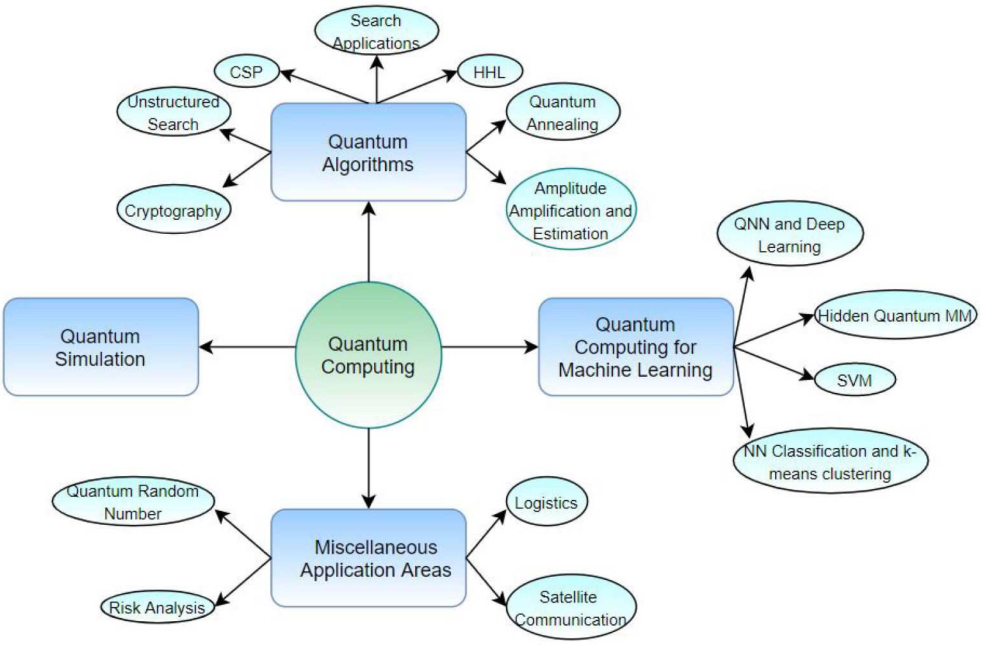

Fig. 1 *Overview of this article*

Table 1 Some groups *G* for a given hidden subgroup problem (HSP) and the corresponding cryptosystems that are broken

Reference	Problem	Group	Complexity	Cryptosystem
[7]	factorisation	$\mathbb{Z}$	polynomial	RSA
[7]	discrete log	$\mathbb{Z}_{p-1}\mathbb{Z}_{p-1}$	polynomial	Diffie–Hellman, DSA
[10]	elliptic curve discrete log	elliptic curve	polynomial	ECDH, ECDSA
[11]	principal ideal	$\mathbb{R}$	polynomial	Buchmann–Williams
[12]	shortest lattice vector	dihedral group	subexponential	NTRU, Ajtai–Dwork

The best known time complexity for a given HSP is also mentioned.

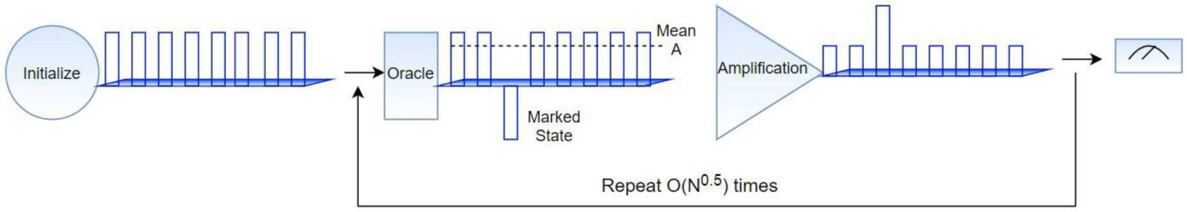

Fig. 2 *3-Qubit Grover's search algorithm on a quantum computer (adapted from [13])*

the cryptosystems that can be broken using a particular group in the HSP.

2.2 Unstructured search

As of now, unstructured data accounts for a significant portion of the total data generated. It may consist of text, dates, and values that result in data not organised in any pre-defined manner. In an unstructured search within a list of k elements, assuming $n = 2^k$ for the index to become an n bit string, function f is given such that $f:\{0,1\}^n \rightarrow \{0,1\}$ to tell us whether that specific unique element is present or not.

Grover's algorithm, based on quantum computing, was devised in 1997 for searching in an unstructured data set [8]. Grover's algorithm does not use any internal structure of the given function f, even if it has one. f is a black box or oracle to the algorithm. This algorithm requires a time complexity of $O(\sqrt{N})$, which is an improvement by a quadratic factor over the classic computational models. Fig. 2 shows the complete working of Grover's search algorithm for 3 qubits. The amplitude of the marked state becomes negative through the oracle, and then that state is amplified. After an appropriate number of iterations, the amplitude of the desired state is maximised [13].

Sergey Sysoev proposed an improvised algorithm based on Grover's algorithm to solve NP-tasks [14], which would be exponentially faster than the speed achieved by Grover's algorithm. However, this requires the use of two quantum systems at the same time to alternate the roles between each iteration, and this kind of quantum computational model is yet to be developed.

2.3 Amplitude amplification and estimation

Let's assume that the probability of finding an element x_0 in the list of elements $X\{x_1, x_2, \ldots, x_n\}$ is p. Each time we execute this search algorithm, the probability of finding the element would increase by p, making the probability $2p, 3p, \ldots$, and so on. Applying the same logic in quantum computations, we get the concept of amplitude amplification. We can consider a Boolean function $f(x)$, $x \in X$, wherein it's value is true if $x_0 = x$ otherwise, it's false. In amplitude amplification, instead of increasing the probability after each iteration, we would be increasing the amplitude of being in one amongst the two possible states (true/false) residing in a complex separable Hilbert space. The quantum algorithm which was proposed by Brassard *et al.* [15] is a generalisation of Grover's algorithm [8] where there has to be a unique solution only. This

Table 2 Comparison of speed-ups achieved due to Grover's algorithm and amplitude amplification when used as subroutines

Application	Classical complexity	Quantum complexity
finding minimum of an unordered list	$O(N)$	$O(\sqrt{N})$
determine graph connectivity	$O(N^2)$	$O(N^{3/2})$
pattern matching	$O(n+m)$	$O(\sqrt{n}+\sqrt{m})$

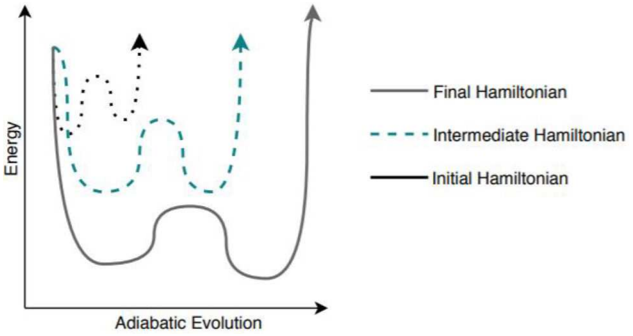

Fig. 3 *Graphical representation of quantum annealing (adapted from [23])*

algorithm can find the element in $O(1/\sqrt{p})$ time, which is a quadratic speedup over classical algorithms.

Amplitude estimation uses the ideas behind Grover's [8] and Shor's algorithms [7] to obtain the approximate number of times a ‘True’ value is obtained in the simulation.

2.4 Applications of search

Grover's search and amplitude amplification can be used as subroutines for more complicated quantum algorithms. Refer Table 2 for a summary. A quantum algorithm by Durr and Hoyer [16] can be used to find the minimum of an unsorted list of N integers with $O(\sqrt{N})$ evaluations. More generally, it finds the minimum of an unknown function $f:\{0,1\}^n \longrightarrow \mathbb{Z}$. Their algorithm applies Grover's algorithm to a function $g:\{0,1\}^n \longrightarrow \{0,1\}$ defined by $g(x)=1$ if and only if $f(x)<T$, where T is some threshold initially set randomly. The threshold is then updated as inputs x are found such that $f(x)<T$.

Determining graph connectivity is another application. A classical computer requires time $O(N^2)$ in the worst case, where N is the number of vertices in the graph. The authors of [17] give a quantum algorithm that runs in time $O(N^{3/2})$, up to logarithmic factors. Efficient algorithms for other graph problems, such as strong connectivity, minimum spanning tree, and shortest path, were also proposed in the same paper.

A fundamental problem in text processing and bioinformatics is pattern matching. Ramesh and Vinay [18] have proposed an algorithm that can find a given pattern p of length m within a text t of given length n. The required time is of the order $O(\sqrt{n}+\sqrt{m})$ up to logarithmic factors. The best possible classical complexity is $O(n+m)$.

2.5 Constraint satisfaction problem (CSP)

A CSP means some limitations or constraints applied over a set of objects. CSP is under research in various domains that have a common basis to solve many problems of many different varieties. A lot of these problems are NP-complete. The authors of [19] proposed a quantum algorithm based on adiabatic evolution to solve any CSP. In the algorithm, a quantum state with uniform superposition over all possible solutions of CSP is prepared in the starting. This quantum state is considered as the ground state of a Hamiltonian [A Hamiltonian is a mathematical description of a physical system in terms of its energies.]. This Hamiltonian is modified ‘slowly enough’ to give a new Hamiltonian. The newly prepared ground state encodes a solution that maximises the number of satisfied constraints. The adiabatic theorem guarantees that if we modify slowly enough, then the system remains in its ground state for the whole process. The worst-case time complexity for this algorithm is unknown.

2.6 Harrow, Hassidim, and Lloyd (HHL) algorithm

It is one of the algorithms that has provided unparalleled applications for quantum computers. The HHL algorithm designed by Harrow, Hassidim, and Lloyd can solve a system of linear equations. In particular, the algorithm does not solve for the solution, but estimates the result of a scalar operation on the solution [4]. However, it has a few limitations like the linear system of equations in N variables should be sparse, the matrix needs to be a Hermitian matrix and have a low condition number κ. The result of some scalar operation on the solution requires time $O(N\sqrt{\kappa})$ on a classical computer, whereas this algorithm provides the result in time $O((\log N)\kappa^2)$. Clader *et al.* [20] have shown that we can use the HHL algorithm to compute the electromagnetic scattering cross-section of an arbitrary target. Some other applications include solving linear differential equations [21] and data fitting [22]. Many of the machine learning algorithms also use the HHL algorithm as a subroutine for various tasks.

2.7 Quantum annealing

Adiabatic quantum computation (AQC), also known as quantum annealing, is a method to solve optimisation problems. It can be used to find the global minimum value from the data set with the help of an objective function. The ground state (lowest energy state) of a complicated Hamiltonian describes the solution to the problem. Initially, we take a simple Hamiltonian in its ground state to solve the problem. Thereafter, a complicated Hamiltonian evolves adiabatically from the simple Hamiltonian. Fig. 3 provides a graphical representation for the quantum annealing process [23]. According to the adiabatic theorem, the system will always remain in the ground state. The processor D-Wave 2X from the D-wave company, developed recently, can outperform classical processors implementing quantum Monte Carlo and simulated annealing [24].

Similar to the Shor's algorithm, quantum annealing can be used to factor integers into primes. This makes it very important from the perspectives of cryptography. Burges in [25] did fundamental research in this direction. The author used factoring of bi-primes as a framework for solving combinatorically hard problems using optimisation algorithms. His work was further improved by the authors of [26] in 2012.

3 Applications of quantum computing for machine learning

In the field of machine learning, we develop algorithms which can learn from the given examples of inputs and desired outputs, following which, we expect the algorithms to predict values for future unknown inputs.

The most common use of quantum computing in machine learning is using the computational speed-ups achieved by quantum algorithms as subroutines for classical machine learning algorithms. On the other hand, deep learning algorithms use specialised hardware such as quantum annealers (quantum computers based on AQC) to enhance performance. Table 3 provides a summary of how a machine learning algorithm achieves speed-up in comparison to a classical computer.

3.1 Nearest neighbour classification and k-means clustering

It is a standard algorithm in machine learning. *K*-nearest neighbour (KNN) algorithm takes all the previous data under consideration while evaluating a new data item that we need to classify based on how similar it is and how it's neighbours are classified. The closer a vector is to another vector, the more similar they are. Standard

Table 3 Approaches used for improving machine learning algorithms

Machine learning method	Quantum enhancement
nearest neighbour classification	quantum subroutine to improve existing machine learning algorithms
	K-means clustering
	SVM
neural network	exploration of quantum model
deep quantum learning	special hardware to training existing neural networks
hidden quantum Markov module (HQMM)	open quantum systems with instantaneous feedback

methods for evaluating closeness or distance are the inner product, the Hamming distance, or the Euclidean.

In [27], the authors use a technique of overlap or fidelity $|\langle a|b\rangle|$ of two quantum states $\langle a\rangle$ and $\langle b\rangle$ to measure the similarity between vectors. The overlap is acquired through a subroutine known as a *swap test*. Based on [27], the authors in [28] proposed a quantum algorithm that takes time $O(\log MN)$. This introduced an exponential speed-up [29].

The authors of [30] have also presented algorithms for measuring the distance between feature vectors. The approach, which is based on the swap test, provides methods for calculating Euclidean distance both directly and using the inner product. It is coupled with the use of amplitude amplification applied together with Grover's search. However, the representation of classical information through qubits is different. In the worst case, the algorithm leads to polynomial reductions when compared to Monte Carlo algorithms.

3.2 Support vector machine (SVM)

SVMs are widely used supervised machine learning algorithms for data models. They are mainly used for classification analysis and also for regression. It uses a test sample for training the data model and assigning each value to one of the categories available. The task in such problems is to find an optimal hyperplane that separates two-class regions very clearly and acts as a decision boundary for future inputs.

In the early 2000s, the authors of [31] proposed the first version of the quantum SVM, which used a variant of Grover's search. More powerful methods have been developed recently. The data input can come from, sources such as qRAM accessing classical data, or it can be a quantum subroutine preparing quantum states. Specifically, quantum phase estimation and matrix invasion are used to create the optimal hyperplane and test the input vector, which in principle requires time poly $(\log N)$. N is the dimension of the matrix that is required to produce a quantum version of the hyperplane vector. The methods described in [32–34] can be used to analyse data using the HHL algorithm.

3.3 Quantum neural networks (QNNs) and deep learning

QNNs are computational neural networks working on the principles governed by quantum mechanics. Artificial neural networks are specifically researched because of their help in pattern recognition and big data applications. It is believed that concepts such as entanglement, parallelism, and interference may help. An increasing number of publications have explored the idea of quantum artificial networks [35–37]. Current work in the field uses the concept of replacing the classic binary bit with a qubit and thus creating a neural unit that is in a superposition of the activated and not activated states.

Quantum annealers are easily scalable and commercially available and well suited for constructing deep quantum learning networks [38]. A deep learning network that is the Boltzmann machine is the easiest to approximate [39]. The quantum Boltzmann machine outputs quantum data which is in qubits. Schuld *et al.* [40] have concluded in their survey that there are no proposals that truly harness the power of quantum computers. The reason why this is just theoretical till now is that quantum states need to be normalised. Using a unitary operator like addition in a Hilbert space (a real or complex inner product space satisfying certain properties) would render an invalid state. Moreover, classical neural networks have non-linear dynamics, whereas QNN has linear dynamics.

3.4 Hidden quantum Markov models

A Markov model is a stochastic model that models temporal or sequential data which helps in predicting future value based on the current information. A hidden Markov model (HMM) is a Markov model where states of the model are hidden and can be observed only when it is given as output by the state. Recorded speech is an example of the Markov chain of successive words. HMM is particularly useful to model sequential data in fields such as NLP (Natural Language Processing).

In 2010, the authors of [41] first introduced hidden quantum Markov models (HQMMs). HQMMs have an edge in that they are a generalisation when compared to the classical HMM. In [42], the authors have proposed open quantum systems with instantaneous feedback to implement the HQMM. They also note that HQMMs can find application as simulators of stochastic processes. Recently an iterative maximum likelihood algorithm has been proposed [43]. The algorithm could successfully learn HQMM and better model certain sequential data.

4 Quantum simulation

Classical computer encounters many problems when it tries to simulate quantum mechanics. Direct simulation on a classical computer is very challenging to achieve because it requires a massive amount of computational memory to store the vast number of explicit states of the quantum system. It happens because quantum states are described by many parameters that grow exponentially as the system size increases [44]. It was in 1982 when Richard Feynman proposed the idea of quantum simulators to do what the most powerful classical simulation methods or supercomputers could not do [45].

Feynman proposed the alternative method of quantum simulation that can be defined as simulating a quantum system by quantum mechanical means. The idea is to have ‘one controllable quantum system simulate another’ [45]. With this approach, quantum simulators would be able to solve quantum many-body problems. It would provide new results that could not be predicted and be very hard to be classically simulated. Being quantum systems themselves, they would help us give more insights into the vast quantum phenomenon. Additionally, it would also allow us to test and verify various models. For instance, it is possible to study hard problems in condensed matter physics like quantum magnetism and correlated electrons. A big advantage of quantum simulation is that it does not require explicit quantum gates. Error correction does not act as a major obstacle, and less accuracy is required while dealing with quantum simulations.

One very apparent advantage of simulation over the other quantum computational processes is that one could easily perform a quantum simulation with just tens of qubits. On the other side, well-known algorithms such as Shor's algorithm require thousands of qubits to work. Secondly, it would be possible to build a quantum simulator with current technologies in the near future. Thirdly, the quantum simulation applications are diverse, ranging from condensed-matter physics to cosmology and from nuclear physics to quantum chemistry. This resulted in an increased interest in quantum simulators.

5 Miscellaneous applications

5.1 Logistics

For any transportation purpose, finding the optimum route is very essential. The global logistics market is predicted to have a compound annual growth rate of 3.48% from the years 2016–2022 and capture a market worth $12,256 billion by the year 2022. With the increased globalisation of the markets and increased demand

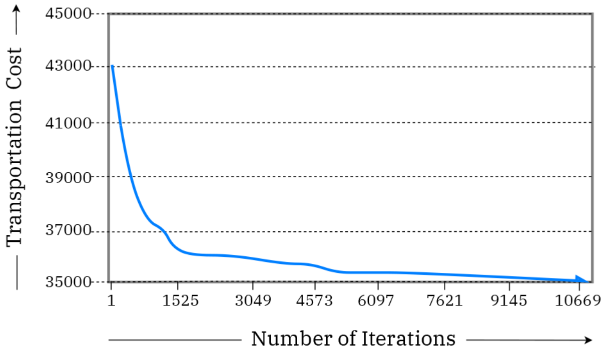

Fig. 4 *Drop in cost with a quantum algorithm [9]*

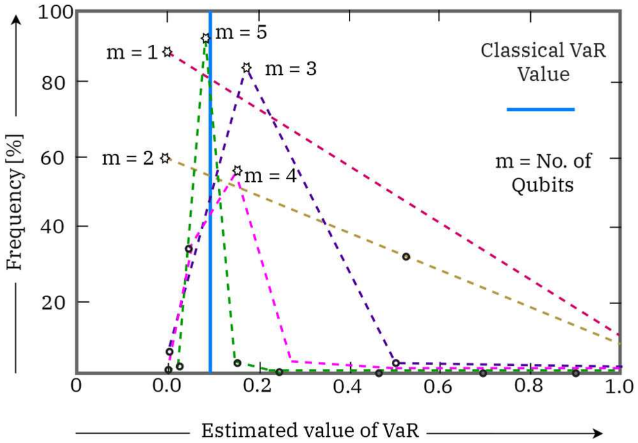

Fig. 5 *Measurement of VaR value on a classical versus a quantum computer. As the number of qubits increases, the value of VaR calculated by a quantum computer gets closer to the classical VaR value [48]*

for movement of stock products from one place to another, logistics have played a significant role in the development of many economies. The functioning in a supply chain is an essential decisive factor in a competitive business. The transport business has unhealthy consequences on human life as it is one of the main contributors to air pollution and greenhouse gases, which thereby leads to global warming [46].

Visiting just ten cities can make up to 200,000 different routes. This problem increases exponentially, and with more cities, the complexity goes beyond the capabilities of a classical computer. This problem is better known as VRP or 'Vehicle Routing Problem.' The referred paper by Wang *et al.* [9] proposes an algorithm, quantum-inspired evolutionary algorithm (IQEA), which follows a heuristics approach and utilises the quantum nature of exponential growth. It serves as a good solution for VRPTW or 'Vehicle Routing Problem with Time Windows,' which applies more constraints VRP to make it similar to the real-life scenarios. Experimental results have shown that by following this method, the cost of transport operations can have a 19.8% reduction in cost (from $44,157 to $35,408) when implemented on twenty vehicles [9]. Fig. 4 shows that the value of the optimal solution decreases significantly as we increase the number of iterations. Similar to the above-discussed applications of quantum computers, there can be many other applications that can help in improving the efficiency of many day-to-day processes.

5.2 Financial risk analysis

Suppose you hold a portfolio of financial products, and the value of these products' profits and losses depends on future prices. These future prices are uncertain, and you do not know how they will develop with time. This uncertainty raises many questions, such as whether a particular investment will yield profit or loss or whether the capital in hand is good enough not to go bankrupt. Risk management, thus, is a very crucial part of our financial system. To get these future estimations, many algorithms have been developed over time.

Value at Risk (VaR) and Conditional VaR (CVaR) are the two units for calculating the risk. VaR is used to determine the loss distribution, while the CVaR is used to determine the expected loss for losses greater than the VaR. CVaR is more sensitive to extreme events in the loss distribution. Monte Carlo simulations are the most widely used methods to find these predictions on traditional classical computers. Monte Carlo simulation is the process of the generation of random objects or processes that can be achieved on a computer [47]. It follows a stochastic model to sample for future prices. This requires a large number of random samples of future realisation of these prices. If the random data sample is big, and the model designed to predict results is good, it can yield a possibility or probability of identifying the risk factor in our investments. This approach to finding the risk factor faces some obstacles. Sometimes a million samples are needed to draw out relevant results. Also, calculations performed on a classical computer may take overnight or even weeks for big datasets. However, quantum methods can achieve this very quickly. Quantum techniques can not only assist machine learning to solve financial problems, but also can optimise risk returns for the financial assets and portfolios.

Amplitude estimation can be used to estimate and achieve speedups over classical algorithms such as Monte Carlo [15]. This approach to finding risk estimates has significant advantages over classical computer algorithms. These quantum algorithms can estimate the risk for a given portfolio for a given financial derivative. Only a few thousand samples are required for them to work, whereas Monte Carlo requires millions of samples. It can take weeks for a classical computer to run this algorithm, whereas a quantum computer can run this in a few hours. Fig. 5 shows that by increasing the number of qubits, better results are achieved for the VaR calculation. With the increase of qubits, i.e. *m*, VaR calculations by the quantum computer show lesser deviation from the classical values. Even though a small number of samples can provide a significant quantum speed-up, but more are provided to get a practical quantum advantage.

5.3 Quantum random number

In this day and age, random number serves as the fundamental element in several applications. It is used in modern electronic casino machines and lottery games for gambling. Many statistical methods, such as the bootstrap method, require random numbers to work. Random numbers play a very significant role in cryptography. It is used in the generation of crypto codes, which serves as the base for many modern cryptographic algorithms. Not just cryptography, it is also used in many other programming aspects and well-known algorithms, such as Monte Carlo simulation. The deterministic system of present-day computers does not generate truly random numbers. Computers follow complex algorithms to generate pseudo-random numbers. These pseudo-random numbers serve as a base for cryptography, which is very critical for privacy. To solve this problem, a random number generator is required, which follows a random physical phenomenon. Since quantum systems are random inherently, they are able to generate truly random numbers.

The referred paper by Stefanov *et al.* [49] has a good demonstration for the construction of a cheap, simple, and easy to use quantum random number generator. This prototype is small (68 × 150 × 188 mm) and fast enough to be implemented for cryptography. It is possible to make a quantum random number generator based on a beam splitter that generates true binary random signals at a rate of 1 Mbit/s, having an autocorrelation time of 11.8 ns [50]. For prospects, it is feasible to develop a random number generator based on quantum processes that could produce truly random numbers at a rate of 1 Gbit/s or even above that [51].

5.4 Satellite communication

Although the quantum computer is in its initial state, many algorithms and protocols have already developed, which can help in communication. At present, many applications are reliant on satellite and play a vital role in our day-to-day life. These are television, telephones, weather, navigation, business & finance, earth observation, space station, and military purposes. The list of

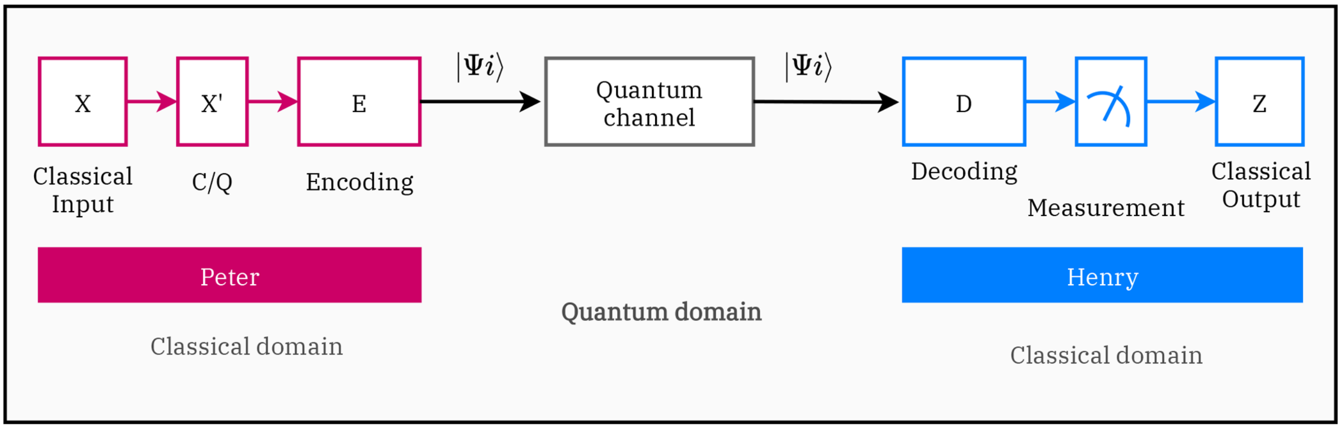

Fig. 6 *Satellite communication, transfer of classical information over a quantum channel [52]*

Table 4 Summary of various applications of quantum computing

Application	Application area	Related works
quantum algorithms	cryptography	[7, 10, 11, 12]
	unstructured search	[8, 14]
	amplitude amplification and estimation	[15]
	search applications	[16–18]
	constraint satisfaction problem	[19]
	HHL algorithm	[4, 20–22]
	quantum annealing	[23–26]
quantum machine learning	nearest neighbour classification and *k*-means clustering	[27–30]
	SVM	[31–34]
	quantum neural networks and deep learning	[35–40]
	HQMMs	[41–43]
quantum simulation	quantum simulator	[44, 45]
miscellaneous applications	financial risk analysis	[15, 47, 48]
	quantum random number	[49–51]
	satellite communication	[52, 53]
	logistics	[9]

its use cases is long, and applications based on it have become an integral part of our life.

A quantum channel is a communication channel meant to transfer classical or quantum information to a satellite. A free quantum space is required for communication to be made possible. Fig. 6 illustrates how classical information is transmitted in a quantum channel [52]. In the figure, Peter represents the sender's side, and Henry represents the receiver side. Peter starts the communication, and box *X* represents all the initial protocols to produce the classical input. This information is then followed by two steps: conversion of classical to quantum bits (box *X*′) and conversion of initial quantum bits (box *E*). This information is passed on to the quantum channel, which is further transmitted to the decoding phase on the receiving side (box *D*). On decoding and measuring, this is converted back to the classical signals (box *Z*) [52].

In the future, it is possible that free-space quantum key distribution applications can have direct communication: free space, satellite-to-satellite, and ground-to-satellite communication will be possible on low earth orbit, middle earth orbit, and geostationary orbits, respectively [53]. It can change the notation of the information, the way it's processed and transferred. China has been focusing on quantum communications for a while now, and they have developed the world's first mobile quantum satellite station. They use quantum key distribution for secure communication using the transmission of photons.

6 Conclusion

While it is demonstrated theoretically that quantum computers have a significant advantage, we cannot yet anticipate the true potential of quantum computers. There are several quantum algorithms that provide an edge over classical algorithms. Quantum simulations will continue to attract researchers in quantum computations for several years, because of its wide possibilities. Novel and practical use cases for existing quantum algorithms is a useful future research direction. Researchers have used quantum algorithms as subroutines for large machine learning algorithms. Theoretically, the proposed algorithms provide a speed-up, but practically they may be expensive to run. Quantum algorithms also face the problem of the physical realisation of a quantum computer. Quantum computers are expected to be made available via cloud computing in the future, which will make their integration with our existing classical computers easier. That said, quantum computations and its applications will be an exciting field for research because of its endless possibilities, and what we have seen till now might only be the tip of the iceberg. In this paper, we have tried to cover most of the significant applications of this technology, as summarised in Table 4, and we look forward to providing a deeper understanding of quantum computations and its applications in our future works.

7 References

[1] IBM: 'A new kind of computing', Available at https://www.ibm.com/quantum-computing/learn/what-is-quantum-computing/, accessed 12 September 2020

[2] Science Alert: 'How Do quantum computers work?', Available at https://www.sciencealert.com/quantum-computers, accessed 12 September 2020

[3] Institute of Quantum Computing, University of Waterloo: 'Quantum computing 101', Available at https://uwaterloo.ca/institute-for-quantum-computing/quantum-computing-101, accessed 12 September 2020

[4] Harrow, A.W., Hassidim, A., Lloyd, S.: 'Quantum algorithm for linear systems of equations', *Phys. Rev. Lett.*, 2009, **103**, (15), p. 150502

[5] Bernstein, D.J., Lange, T.: 'Post-quantum cryptography-dealing with the fallout of physics success', *IACR Cryptol ePrint Arch*, 2017, **2017**, p. 314

[6] Freeman, J.: 'The progression of lattice-based cryptography', 2018

[7] Shor, P.W.: 'Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer', *SIAM Rev.*, 1999, **41**, (2), pp. 303–332

[8] Grover, L.K.: 'Quantum mechanics helps in searching for a needle in a haystack', *Phys. Rev. Lett.*, 1997, **79**, (2), p. 325

[9] Wang, L., Kowk, S., Ip, W.: 'Design of an improved quantum-inspired evolutionary algorithm for a transportation problem in logistics systems', *J. Intell. Manuf.*, 2012, **23**, (6), pp. 2227–2236

[10] Proos, J., Zalka, C.: 'Shor's discrete logarithm quantum algorithm for elliptic curves', arXiv preprint quant-ph/0301141, 2003

[11] Hallgren, S.: 'Polynomial-time quantum algorithms for Pell's equation and the principal ideal problem', *J. ACM (JACM)*, 2007, **54**, (1), pp. 1–19

[12] Kuperberg, G.: 'A subexponential-time quantum algorithm for the dihedral hidden subgroup problem', *SIAM J. Comput.*, 2005, **35**, (1), pp. 170–188

[13] Figgatt, C., Maslov, D., Landsman, K., *et al.*: 'Complete 3-qubit Grover search on a programmable quantum computer', *Nat. Commun.*, 2017, **8**, (1), pp. 1–9

[14] Sysoev, S.: 'The effective solving of the tasks from np by a quantum computer', arXiv preprint arXiv:14016030, 2014

[15] Brassard, G., Hoyer, P., Mosca, M., *et al.*: 'Quantum amplitude amplification and estimation', *Contemp. Math.*, 2002, **305**, pp. 53–74

[16] Durr, C., Hoyer, P.: 'A quantum algorithm for finding the minimum', arXiv preprint quant-ph/9607014, 1996

[17] Dürr, C., Heiligman, M., HOyer, P., *et al.*: 'Quantum query complexity of some graph problems', *SIAM J. Comput.*, 2006, **35**, (6), pp. 1310–1328

[18] Ramesh, H., Vinay, V.: 'String matching in o(n + m) quantum time', *J. Discret. Algorithms*, 2003, **1**, (1), pp. 103–110

[19] Farhi, E., Goldstone, J., Gutmann, S., *et al.*: 'Quantum computation by adiabatic evolution', arXiv preprint quant-ph/0001106, 2000

[20] Clader, B.D., Jacobs, B.C., Sprouse, C.R.: 'Preconditioned quantum linear system algorithm', *Phys. Rev. Lett.*, 2013, **110**, (25), p. 250504

[21] Berry, D.W.: 'High-order quantum algorithm for solving linear differential equations', *J. Phys. A: Math. Theor.*, 2014, **47**, (10), p. 105301

[22] Wiebe, N., Braun, D., Lloyd, S.: 'Quantum algorithm for data fitting', *Phys. Rev. Lett.*, 2012, **109**, (5), p. 050505

[23] Alba Cervera-Lierta: 'Quantum annealing', Available at https://medium.com/@quantum_wa/quantum-annealing-cdb129e96601, accessed 28 October 2020

[24] Denchev, V.S., Boixo, S., Isakov, S.V., *et al.*: 'What is the computational value of finite-range tunneling?', *Phys. Rev. X*, 2016, **6**, (3), p. 031015

[25] Burges, C.J.: 'Factoring as optimization', Microsoft Research MSR-TR-200, 2002

[26] Xu, N., Zhu, J., Lu, D., *et al.*: 'Quantum factorization of 143 on a dipolar-coupling nuclear magnetic resonance system', *Phys. Rev. Lett.*, 2012, **108**, (13), p. 130501

[27] Aïmeur, E., Brassard, G., Gambs, S.: 'Machine learning in a quantum world'. 19th Conference of the Canadian Society for Computational Studies of Intelligence, 2006, Quebec City, Quebec, Canada pp. 431–442

[28] Lloyd, S., Mohseni, M., Rebentrost, P.: 'Quantum algorithms for supervised and unsupervised machine learning', arXiv preprint arXiv:13070411, 2013

[29] Buhrman, H., Cleve, R., Watrous, J., *et al.*: 'Quantum fingerprinting', *Phys. Rev. Lett.*, 2001, **87**, (16), p. 167902

[30] Wiebe, N., Kapoor, A., Svore, K.: 'Quantum algorithms for nearest-neighbor methods for supervised and unsupervised learning', arXiv preprint arXiv:14012142, 2014

[31] Anguita, D., Ridella, S., Rivieccio, F., *et al.*: 'Quantum optimization for training support vector machines', *Neural Netw.*, 2003, **16**, (5-6), pp. 763–770

[32] Rebentrost, P., Mohseni, M., Lloyd, S.: 'Quantum support vector machine for big data classification', *Phys. Rev. Lett.*, 2014, **113**, (13), p. 130503

[33] Chatterjee, R., Yu, T.: 'Generalized coherent states, reproducing kernels, and quantum support vector machines', arXiv preprint arXiv:161203713, 2016

[34] Zhao, Z., Fitzsimons, J.K., Fitzsimons, J.F.: 'Quantum-assisted Gaussian process regression', *Phys. Rev. A*, 2019, **99**, (5), p. 052331

[35] Rigatos, G.G., Tzafestas, S.G.: 'Neurodynamics and attractors in quantum associative memories', *Integr. Comput.-Aided Eng.*, 2007, **14**, (3), pp. 225–242

[36] Behrman, E.C., Steck, J.E.: 'A quantum neural network computes its own relative phase'. 2013 IEEE Symp. on Swarm Intelligence (SIS), Singapore, 2013, pp. 119–124

[37] Gupta, S., Zia, R.: 'Quantum neural networks', *J. Comput. Syst. Sci.*, 2001, **63**, (3), pp. 355–383

[38] Adachi, S.H., Henderson, M.P.: 'Application of quantum annealing to training of deep neural networks', arXiv preprint arXiv:151006356, 2015

[39] Biamonte, J., Wittek, P., Pancotti, N., *et al.*: 'Quantum machine learning', *Nature*, 2017, **549**, (7671), pp. 195–202

[40] Schuld, M., Sinayskiy, I., Petruccione, F.: 'The quest for a quantum neural network', *Quantum Inf. Process.*, 2014, **13**, (11), pp. 2567–2586

[41] Monras, A., Beige, A., Wiesner, K.: 'Hidden quantum Markov models and nonadaptive read-out of many-body states', arXiv preprint arXiv:10022337, 2010

[42] Clark, L.A., Huang, W., Barlow, T.M., *et al.*: 'Hidden quantum Markov models and open quantum systems with instantaneous feedback', *Emerg., Complex. Comput.*, 2015, **14**, Springer, Cham, pp. 143–151. Available at http://dx.doi.org/10.1007/978-3-319-10759-2_16

[43] Srinivasan, S., Gordon, G., Boots, B.: 'Learning hidden quantum Markov models', arXiv preprint arXiv:171009016, 2017

[44] Buluta, I., Nori, F.: 'Quantum simulators', *Science*, 2009, **326**, (5949), pp. 108–111

[45] Feynman, R.P.: 'Simulating physics with computers', *Int. J. Theor. Phys.*, 1982, **21**, pp. 467–488, https://doi.org/10.1007/BF02650179

[46] Yang, C.S., Lu, C.S., Xu, J., *et al.*: 'Evaluating green supply chain management capability, environmental performance, and competitiveness in container shipping context', *J. Eastern Asia Soc. Transp. Stud.*, 2013, **10**, pp. 2274–2293

[47] Kroese, D.P., Brereton, T., Taimre, T., *et al.*: 'Why the Monte Carlo method is so important today', *Wiley Interdiscip. Rev.: Comput. Stat.*, 2014, **6**, (6), pp. 386–392

[48] Woerner, S., Egger, D.J.: 'Quantum risk analysis', *Npj Quantum Inf.*, 2019, **5**, (1), pp. 1–8

[49] Stefanov, A., Gisin, N., Guinnard, O., *et al.*: 'Optical quantum random number generator', *J. Mod. Opt.*, 2000, **47**, (4), pp. 595–598

[50] Jennewein, T., Achleitner, U., Weihs, G., *et al.*: 'A fast and compact quantum random number generator', *Rev. Sci. Instrum.*, 2000, **71**, (4), pp. 1675–1680

[51] Lalanne, P., Rodier, J.C., Chavel, P.H., *et al.*: 'Optoelectronic devices for Boltzmann machines and simulated annealing', *Opt. Eng.*, 1993, **32**, (8), pp. 1904–1915

[52] Bacsardi, L.: 'On the way to quantum-based satellite communication', *IEEE Commun. Mag.*, 2013, **51**, (8), pp. 50–55

[53] Bacsardi, L.: 'Satellite communication over quantum channel', *Acta Astronaut.*, 2007, **61**, (1–6), pp. 151–159