

Innovations and Applications of Quantum Computing

Bhanu Prakash

MSCS (AI & ML), Sofia University, Palo Alto, CA, 94303 USA

Moore's law will cease to be relevant once transistors are the size of electrons. Once this occurs, we will no longer be able to use silicon for technological advancement. However, breakthroughs will continue in the form of a sixth paradigm: a 3D molecular computing model such as quantum computing. Some of the promising areas of quantum computing researched in this study are (i) algorithmic advancements - such as Shor's, Grover's, error correction, fault tolerance and other new algorithms; (ii) hardware - such as the quantum system architecture, circuit models, entanglement, superposition and no-cloning qubits; (iii) market segments - such as finance, healthcare, and chemistry; (iv) the supremacy established over classical computing; and (v) areas of applicability. Significant progress has been made in these areas in recent decades, and they have garnered immense interest, attention and the funding required to make good progress.

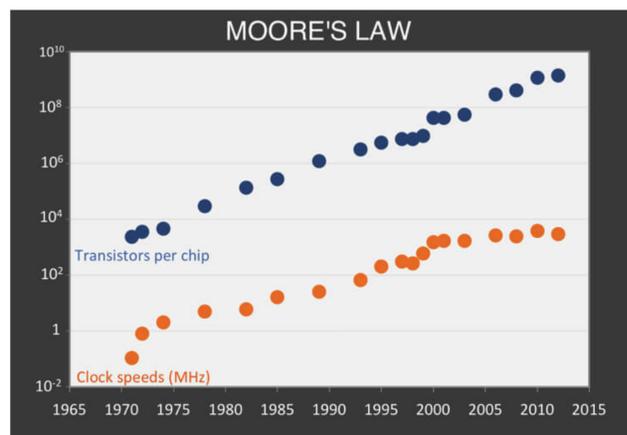
Keywords: Quantum Computing, Quantum Systems, Quantum Algorithms, Error Correction

Moore's law has been undisputed for decades; it states that the "complexity for minimum component costs has increased at a rate of roughly a factor of two per year," and the research has shown proven improvements of 1.5 times every two years **Dorrier2016**, as shown in Figure 1. For similar costs and sizes, we will obtain 1.5 times the memory or processor speed every 2 years. This progress will stop when transistors are the size of electrons; consequently, we will no longer be able to use silicon for technological advancement. Will the innovations stop, and is this the best speed and accuracy we can achieve? As Ray Kurzweil stated, exponential growth will continue in the form of a sixth paradigm - 3D molecular computing. More on this can be found in .

Physicists observed a peculiar phenomenon that could not be explained by normal physics, and there were many terms for this 'spooky' occurrence, which eventually branched into quantum mechanics. Although this was identified more than a century ago, there was no clear research, theory or usage. Approximately 3 decades ago, foundations for research on QC (quantum computer/computing), i.e., quantum mechanics applied to computer science, were laid out by Richard Feynman et al. They found that the quantum phenomenon associated with entangled particles could not be realized on a Turing machine **Rieffel2011**. This triggered research on a new realm of computing, in which quantum mechanics was used for information processing since it was

Figure 1

Moore's law, plotting transistors per chip and clock speed
Dorrier2016.



thought to be faster.

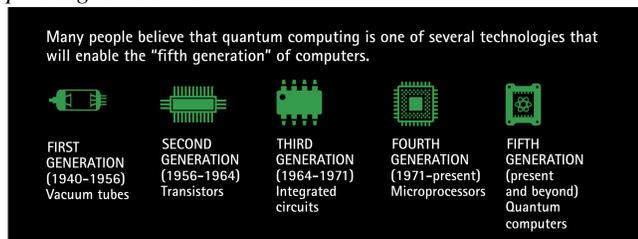
Contrary to popular belief, a QC solves problems with certainty that the CC (classical computer/computing) solves with high probability. A QC is closer to an analog computer than to a digital computer. It does not operate on discrete values of inputs but rather on a stream of values. Analog devices, however, do not support special situations such as entanglement or superposition, which are introduced in the next section. In the late 20th century, there were significant inventions in quantum hardware and software. The amazing benefits of QCs slowly started to emerge. Figure 2 shows the evolution of the computer architecture, and Figure 3 shows the increases in the interest and papers

on QCs. In the 1980s and 1990s, much research was conducted on QCs and indicated that a classical quantum Turing machine could be created using a quantum circuit model and that any calculation could be executed on it. At the same time, Shor's algorithm coupled with efficient quantum error correction generated much interest. It was proven for the first time that a certain task could be evaluated on a QC with exponential speed; this demonstrated the elegance of a quantum algorithm, but it was still theoretical. Gates for the quantum circuit model and quantum error correction to remove decoherence in quantum circuits also came into existence in the 1990s. Further research was conducted in the early 2000s. Grover's algorithm, more advanced error correction, novel approaches to qubit technologies, and different kinds of QCs have all been researched and incorporated in the last two decades. Few of the leading next-generation high-speed processors are QC based **Hamilton2020**, and quantum circuits are supposed to significantly outperform CC circuits in many areas.

This paper brings together a history of the QC, its evolution, its mathematics, the technology, various modernizations and the most favorable applications. The first few sections detail the innovations in quantum computing. The first section details the motivation behind quantum algorithms. Then, we establish quantum supremacy based on some of the algorithms that have outperformed CCs. The following sections evaluate the potential market segments finding applicability of QCs; then, we explore the advancements in quantum hardware, architecture, software and quantum error correction algorithms. The rest of the sections detail the applicability of QCs to specific areas of computing.

Figure 2

*Evolution of computing technology from vacuum tubes to the present: a QC is believed to be the fifth generation or sixth paradigm **Accenture2017**.*

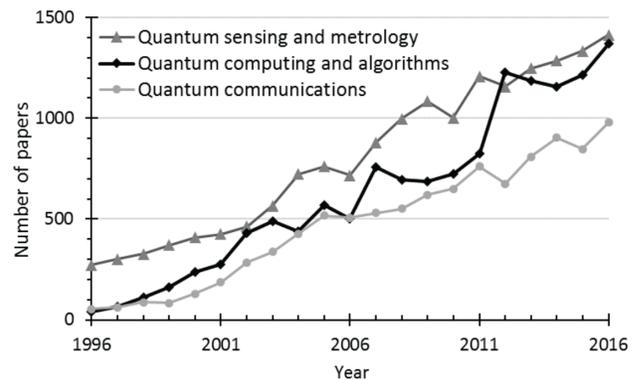


Motivation

QC algorithms are aimed at exponential time speed up of a few NP (nondeterministic polynomial time) algorithms **Shor2003**. These are not the P (polynomial time) algorithms already solved by a CC; instead, they are among NP, NP-complete or NP-hard algorithms. P and NP are as identified and defined in reference **Cormen2009**. Solving NP category

Figure 3

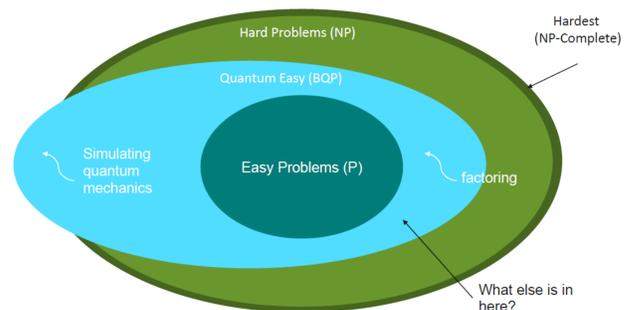
*Increase in the number of papers on QCs **Sciences2019**.*



problems is similar to looking for a needle in an exponentially large haystack. It has already been established that $P \neq NP$ and that classical algorithms display exponential complexity in solving them. With the invention of the factorization algorithm by Shor, the search algorithm by Grover and other algorithms, solving NP problems has been a new motivation for QCs. A new category of problems called 'quantum easy' problems has emerged, as shown in Figure 4. They are NP problems in CCs, taking an enormous amount of time, if at all solvable, whereas a QC can solve a subset of them in a surprising amount of time, thus achieving quantum supremacy. This has been a major extension of the focus and areas of application motivating quantum research, in addition to the appropriate hardware and other electronics.

Figure 4

*New categorization of algorithms as 'quantum easy' problems **Frisch2017**.*

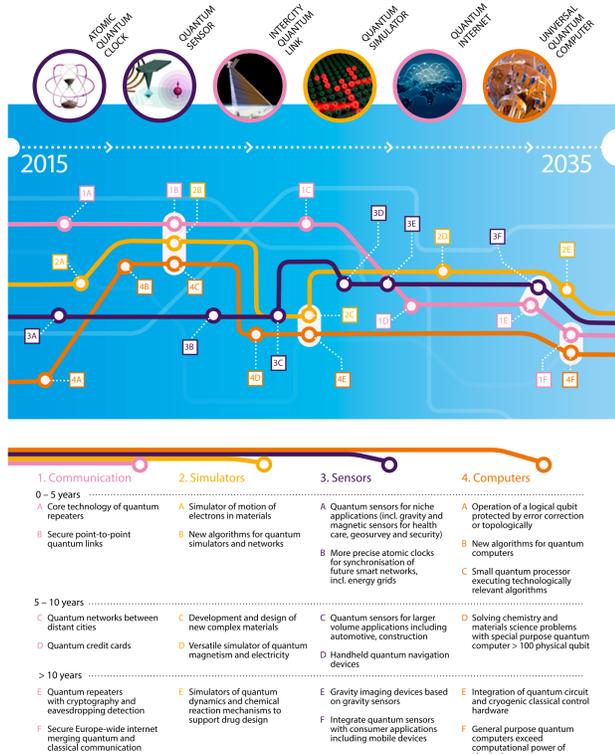


Quantum Supremacy

Quantum supremacy is a term coined by J. Preskill et al. at a quantum computing talk **Calude2020**. They stated "The postulate of quantum computation: Computational devices based on quantum mechanics will be computationally superior compared to digital computers". Supremacy is proven

by establishing that when performing a formal computational task, a QC cannot be outperformed by a CC using any known algorithm offering a better running time. Figure 5 shows the supremacy and growth of quantum-related technologies.

Figure 5
Quantum technology timeline showing the supremacy and proposed growth of quantum hardware
TheEuropeanCommission2016.

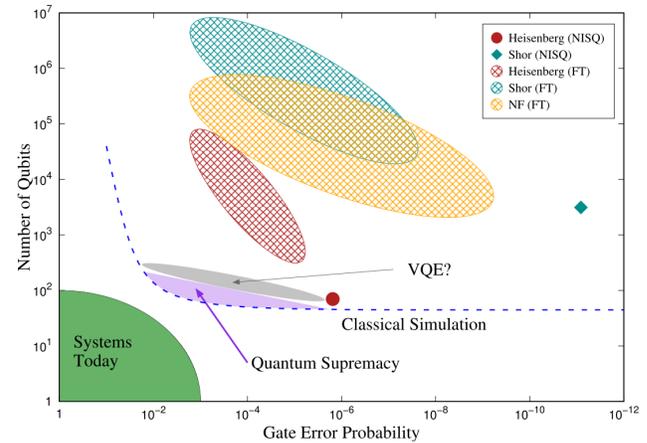


Google's sampling experiment using noisy intermediate-scale quantum (NISQ) computers **Villalonga2020** recently achieved supremacy. This experiment proves that the QC processing capacity far exceeds that of a CC while consuming less power. As part of this experiment, sampling was carried out on NASA's Electra and ORNL's Summit supercomputers along with a Google NISQ quantum device. While Electra took 59 hours and consumed 96.8 MWh and Summit took 2.44 hours with 21.1 MWh consumed, the NISQ device could finish this task in 0.028 hours, consuming less than 0.004 MWh of power. After this, many similar experiments were planned and performed by IBM, Accenture, D-Wave and others.

Referring to Figure 6, solid areas are the actual gate implementations in NISQ computers. The blue dotted line demarcates the QC simulation area from the actual implementation area. The area in purple is where the hypothetical simulations showing quantum supremacy are being established. Meshed regions for different algorithms and QC architectures illus-

trate the targeted logistics for solving them.

Figure 6
The performance space of a QC Maslov2019.



Potential Markets

In the past few years, since the success of Shor's algorithm and the triumph of quantum supremacy experiments, a growing list of market segments have opened up for QCs. More advanced computing is revolutionizing the following sectors **Srivastava2016 Accenture2017**:

Financial Services

Financial services employing fintech (financial technology) will benefit from the superfast computing of QCs by running many models and then identifying optimized portfolios, dynamically managing them, performing scenario analysis, determining options pricing for complex derivatives, etc. Cybersecurity is of the greatest importance to financial products. Since QCs have direct applicability to security, they could make financial transactions even more secure.

Healthcare

Accelerated computing increases the odds of drug discovery for deadly illnesses such as cancer and Alzheimer's disease. Simulated quantum annealing algorithms can recommend a precise drug composition, significantly reducing its side effects. Oncology is an area that could benefit from bespoke treatments. Unrestrained availability of extensive computing could help alleviate resource limitations hindering studies such as those on protein folding, which is emerging as a crucial advancement in finding cures for Parkinson's disease and many other types of cancers.

Chemistry

Chemistry is one of the most relevant areas for QC application. Devising a reliable way of analyzing and predicting

chemical reaction rates is crucial for the advancement of this sector. For example, an advanced understanding of catalysts for carbon sequestration could result in better battery manufacturing. A precise understanding of ammonia production could be a game changer in agriculture because the amount of fertilizers produced is approximately 450 tons annually, and more than 2% of the world's energy is invested in this process.

Logistics

The logistics industry faces the typical 'vehicle routing problem' or 'traveling salesman problem': an inability to establish the most efficient route between multiple destinations. A decisive routing algorithm could revolutionize this industry. Quantum annealing algorithms are supposed to be very efficient in solving such problems.

Engineering

Critical engineering modeling, such as in aircraft wing design, consumes an enormous amount of processing power for simulation and hence could take months if not years. Speeding this process up could save massive amounts of fuel and other costs. Defense tools and software are extremely complex and hence lack adequate security. Organizations such as Lockheed Martin spend half the cost of a project in solving these problems alone. In one of the use cases, a classic supercomputer would normally take 6 months to detect bugs in an aircraft, whereas a D-Wave quantum computer could do so in just 6 weeks.

Quantum Systems

Qubits are the building blocks of a QC, similar to bits for CCs. As the simple Polaroid experiment by Rieffel2011 showed, photon polarization states can be used as qubits, i.e., quantum bits. Vertical polarization is written as $|\uparrow\rangle$, whereas $|\rightarrow\rangle$ indicates horizontal polarization. Figures 7 and 8 show one such state. The vertical and horizontal spins can be replaced by bits, and the same effect will still be achieved.

Figure 7

Single-Qubit System: Sample measurement of 0 and 90 degree polarizations of individual qubits forming a 45 degree polarization, i.e., a unit vector of 45 degrees Rieffel2011.

The state space of a CC is the Cartesian product of states, whereas in a QC, it is a tensor product, and hence, the state space grows exponentially as the number of particles grows. Many computations are performed by qubits simultaneously through this quantum mechanical phenomenon. Even though CCs are also built on the phenomenon of quantum mechanics, a QC per se is made up of qubits, quantum gates and quantum algorithms. Quantum algorithms are described in a separate section. Unlike bits that have only a discrete 0 or

Figure 8

Single-Qubit System: Bloch sphere representation of the same system. It is easy to visualize the same system in multiple dimensions. The only difference from the previous representation is that the angle between the two states is twice that of the previous angle. Any state can be represented by a complex number as $\alpha = s + it$, representing a point (x, y, z) on the sphere such that $|x|^2 + |y|^2 + |z|^2 = 1$ Rieffel2011.

1 state, QC qubits have an infinite number of intermediate states between 0 and 1, with both values included, as shown in 8. In a CC, bits are processed sequentially, but in a QC, bits are entangled such that a change in one can influence a change in the rest **Accenture2017**. In a CC, a bit state of n bits is a combination of n digits of 0 and 1, but in a QC, 2^{n-1} complex numbers are used to depict n states. These states leave some of the resultant vector in a limbo state between 0 and 1, which is called **superposition**. Qubits are connected even if they are not physically linked, which is called **entanglement**. A multi-qubit system or n qubit system cannot be represented by n single qubit systems, and the vast number of states that cannot be written as tensor products of n single bit states are responsible for this. The states of these qubits are not independent of one another, and QCs use this feature to speed up calculations. Rieffel2011 described entanglement as "... there are many distinctly different types of multipartite entanglement; for entanglement between four (or more) subsystems, the different types of entanglement are uncountable infinite!". The **no-cloning** principle is another critical concept of QCs absent in CCs. It prevents copying or cloning of entangled quantum states, which makes it a good candidate for implementing security.

Quantum Gates

Figures 9 to 11 show the standard transformations performed Rieffel2011, Frisch2017, which are hence quantum gates in a QC.

Figure 9

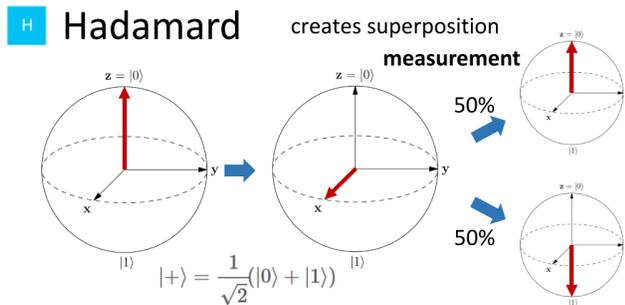
Pauli's transformation gates: I is identity, which is the $f(x) = x$ transformation; X is negation, which is equivalent to the NOT gate in a CC; Z alters the superposition; and Y is negation and change of phase.

Qubit Technologies

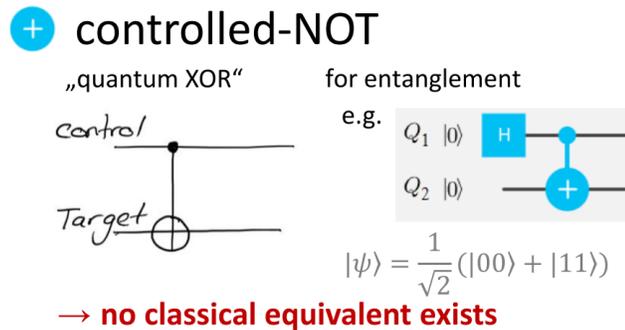
Constructing a QC is extremely challenging. Any disturbance to the operating environment will cause decoherence, and vital information will be lost **Srivastava2016**. Currently, there are three popular engineering approaches. A few others have been developed, as detailed at the end of this section, but the following three are the most popular approaches:

Figure 10

Hadamard gate creating an even superposition.

**Figure 11**

CNOT or controlled-NOT gate, which flips the least significant bit or the last bit if the most significant bit or the first bit is 1; otherwise, it leaves the bit as is.



Trapped Ion Qubits: This is by far the strongest candidate for future QCs, and most of the existing QCs use this technology. It uses a trapped ion, which is an atom stripped of electrons, at a very low temperature as a qubit. This ion is manipulated by an electromagnetic field for computation.

Superconducting Qubits: Circuits made from superconducting materials such as aluminum and niobium behave like artificial atoms when cooled to a very low temperature and operated at microwave frequencies. In this scheme, these are used to store qubits. An advantage of these structures is that the existing integrated circuit fabrication techniques could be used to manufacture them.

Solid-Stage Spin Qubits: A vacancy or an atom missing in a material such as diamond is a defect. If a nitrogen atom is placed next to this vacancy in the defective material, then it displays a special property called a 'spin', which is a superposition state of a combination of up and down spins, both of which are included. This is then used as a qubit.

Other emerging technologies **Sciences2019** are photonic quantum computation, neutral atom quantum computation, semiconductor qubits, optically gated qubits in crystals, electrically gated semiconductor qubits, and topological qubits.

Models for Building a QC

There are many different models for building QCs. However, over the years, two models have found business relevance and viability as of today:

The circuit model aka gate model aka universal QC - a basic quantum circuit operating on qubits; similar to the CC, it can perform general purpose computations.

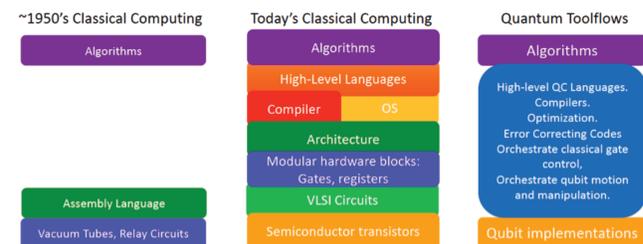
The adiabatic QC aka annealer QC aka annealing machine - a type of quantum annealer that uses the adiabatic theorem for processing, best suited for solving optimization problems.

Architecture

The architecture for a QC is still in its nascent stages. Figure 12 shows a comparison of CC architectures from the 1950s and early 2000s and the present QC architecture. The current architecture of a QC that has been used in NISQ computers and the QCs used to show QC supremacy resembles that of the early CC. Another alternative architec-

Figure 12

Computer architecture comparisons, showing a generic flow for quantum programming languages. The code from the quantum programming language is translated from high-level language to machine-level code by a series of compilers, schedulers and optimizers. These instructions at the lowest level are then mapped to run on specific firmware gates **Martonosi2018**.



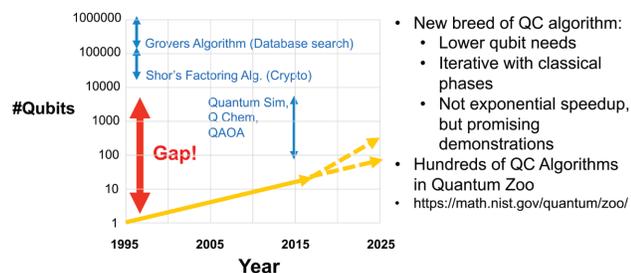
ture was suggested by **Britt2017**, who showed two ways of connecting a QC with high-performance computing (HPC), such as via a graphic processing unit (GPU), to achieve a hybrid quantum architecture. In this approach, a QC can be combined with HPC, and there are two ways of doing so: either through a multiprocessor model by connecting HPC and a QC by tailing the information or by connecting them through cloud-based quantum computing. Another success in the hybrid approach was achieved by **Mazouzi2020**, who were able to achieve a quadratic improvement in outlier detection, i.e., anomaly reduction in machine learning computations, by performing the initial preparation for this using a CC and by using a QC in the later stages. Present-day leading QCs are classified as either NISQ (noisy intermediate-scale quantum) or FT (fault tolerant) QCs.

Quantum Algorithms and Languages

The number of quantum algorithms invented over the past decade has been limited. Regarding this, **Shor2003** stated that "Any quantum algorithm offering a speed-up over classical computation must use interference; this phenomenon is unknown in classical computer science, and most theoretical computer scientists are not used to reasoning about it. Thus, it seems quite likely that several new and significant quantum algorithmic techniques have yet to be discovered". Tests have shown that quantum algorithms have disproved the Church-Turing thesis **Sciences2019** by solving certain tasks with exponentially fewer steps; theoretically, this was already established in the early 1990s. While slow, the algorithm space is steadily improving, but the quantum hardware has not been able to keep up with the advancement, as shown in Figure 13. Some of the leading algorithms are listed in this section.

Figure 13

Algorithms to machines gap: Algorithm progress Martonosi2018.



Quantum Algorithms

The following are some of the recent advancements in quantum algorithms **Rieffel2011** and **Sciences2019**:

- Deutsch's algorithm.
- Deutsch-Jozsa algorithm.
- Bernstein-Vazirani algorithm.
- Quantum Fourier transform and quantum Fourier sampling.
- Quantum factoring and finding hidden structures, i.e., Shor's algorithm.
- Grover's algorithm and quantum random walks.
- Hamiltonian simulation algorithms.
- Quantum algorithms for linear algebra.
- Simon's algorithm.

Quantum Languages

FJQuantum **Feitosa2016** is a high-level object-oriented quantum programming language suitable for programming a QC; a sample code snippet is provided in 14. It is Featherweight Java adapted to quantum computing since the language for a QC has to handle additional intricacies such as entanglement, superposition, error correction, and validation. This is an extension of the work already done through monads and QJava libraries. In addition to Java, QC-compliant versions of Python, C#, JavaScript and many other languages have been developed.

Figure 14

Code snippet showing a 'controlled-NOT' usage Feitosa2016.

```
class QOp extends Object {
    (boolean -> Vec<boolean>) not() {
        return (boolean i) ->
            if (i == false) {
                mreturn true
            }
            else {
                mreturn false
            }
    };
    (boolean -> Vec<boolean>) hadamard() {
        return (boolean b) ->
            if (b == false) {
                (ComplexHalf $* mreturn false) mplus
                (ComplexHalf $* mreturn true)
            } else {
                (ComplexHalf $* mreturn false) mplus
                (ComplexMHalf $* mreturn true)
            }
    };
    ({boolean,boolean} -> Vec<{boolean,boolean}>)
    controlledNot() {
        return ({boolean,boolean} b) ->
            if (b.1 == true) {
```

Error Correction and Approximation

Error correction is the process of eliminating the environmental interactions that interfere with calculations **Rieffel2011**. This is as important as the algorithms themselves. When earlier algorithms such as Shor's were built, error correction was considered a theoretical approach, and errors would lead to the algorithms failing. Only after this algorithm was coupled with a good error correction method did the approach truly take off. Advanced error correction mechanisms are an active area of research. There are two methods of error correction: quantum error correction (QEC) and quantum error mitigation (QEM) **Sciences2019**. Of the two, QEC is the most widely used and efficient. This involves appending additional qubits to the qubits performing calculations and using a QECC, i.e., a quantum error correction code, to use this redundancy and identify stable qubits. Error correction alone is insufficient for robust quantum computations; it has to be supplemented with fault tolerance to achieve the desired accuracy. There have been many ad-

vancements, such as Steane's code, and this field is still an active area of research.

Quantum Approximation

As seen in the previous section, quantum computations are subject to unwanted interference from the environment called errors. One way of dealing with such errors was described earlier, which is a slightly expensive process; another way of eliminating the effect of errors is approximation **Sciences2019**. Forgoing the desire to obtain the exact solution, approximation is used in this approach. This has opened up another dimension for quantum computing, i.e., the quantum and classical hybrid. There are two approaches to this: variational quantum algorithms and analog quantum algorithms.

Robustness Analysis

Quantum programming languages do not address errors or fault tolerance **Hung2019**; these tasks are assigned to the hardware. No clear architecture has been developed for this yet. The NISQ computers used until now do not perform any real fault tolerance since the algorithms run on them are mostly theoretical. The while-language experimented on in the paper attempted to fill the void; it offers semantics for erroneous quantum while-programs, and it measures the robustness.

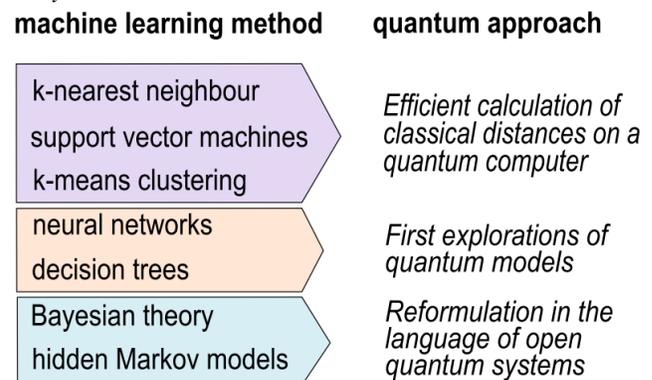
Applications of Quantum Computing

Quantum Machine Learning & Deep Learning

Machine learning (ML), deep learning (DL) and artificial intelligence (AI) are by far the most researched applications of QCs. Since they involve working with and improving multivariate systems, they might translate directly to quantum annealing and adiabatic quantum computing **Wittek2014**, and a QC can easily learn from unknown functions quite fast. This could lead to the fastest realization of QC advantages, and many articles have been written on this topic. In a quantum deep learning study, **Wiebe2016** established that a QC not only reduced the amount of time required to train a restricted Boltzmann machine (RBM) but also optimized the underlying function better. They found that the problem could be reduced to a problem of merely quantum state preparation and hence achieve a quadratic reduction in the amount of time it takes. This allowed the algorithms to be better parallelized over multiple qubit systems, which was a major shortcoming of any deep learning system. In another study, **Arunachalam2017** showed that the number of queries required for learning a concept could be polynomially smaller in QCs, which meant that the time complexity could be exponentially faster.

Figure 15

Figure showing how a QC can be applied to various ML, DL and AI methods **Schuld2014**. Efficient algorithms and problem solving gain a significant advantage; for example, Larry Page's PageRank algorithm patent led to the rise of Google today.



Quantum Security

QCs have enormous potential to offer robust security **Humble2018** through cryptography, quantum key distribution and dense coding and teleportation. They also offer security at the server level via delegated quantum computing (DQC) or blind quantum computing (BQC), which are methods for offering more security by hiding the computations from the server. As per **Dunjko2014** and **Fitzsimons2017**, this has been another major area of focus, and many secure protocols have been written around it.

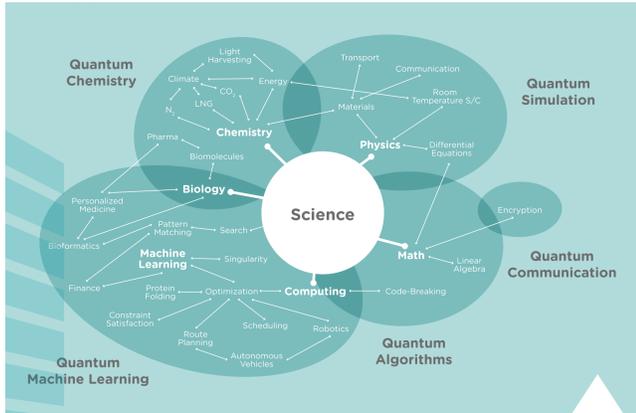
Experimental Applications of QCs

An increasing number of companies, sectors, domains, businesses and even governments are finding use cases for QCs. For example, Figure 16 from the NQIT 2018 report shows the ever-changing landscape of QC adaptation to general science.

Conclusion

Quantum mechanics is a relatively old field of study. Scientists have always been puzzled by the spooky behavior of electrons since Einstein. Only in the last few decades has harnessing of this behavior been realized, though on a very small scale. However, as the law of accelerating returns suggests, change is going to be exponential; it just has not been experienced yet. The harnessing of this behavior might seem minimal now, but as we continue to make substantial progress, its success will be hard to miss. As detailed in earlier sections, it is becoming increasingly clear where the niche of QCs lies. Research has diverged in both niche areas, such as machine learning/deep learning, and in many experimental areas, as shown in the later sections. Supremacy of QCs

Figure 16
The ever-expanding landscape of QC adaptation
Gheorghiu2018.



has already been achieved, as shown experimentally. Along with state-of-the-art quantum algorithms that aim to solve even NP-complete problems, advancements in quantum error correction could not have come at a better time, which were instrumental in the amount of recognition this field has achieved. Hardware has not been catching up with the speed of algorithms and implementations, but when it does, the industry and market might not be ready for the kind of impact it is going to make. Moore's law gave us a good indication of where the CC was headed in the mid/late 20th century; hopefully, the law of accelerating returns does the same, i.e., provides a sense of where the industry is headed. Some of the research on quantum algorithms, quantum gates and models for QCs has been promising, and much more is in progress. As increasing investments are channeled into this, we might be headed into either an era of explosive ideas or an era where the research will be underreported for security reasons and to obtain a first innovator edge; only time will tell.

Appendix A

Linear growth is measured against some time bracket (yearly in the following example); it is constant growth such

as 1x in year 1, 2x in year two, 3x in year three and so on. Exponential growth, in contrast, is 2x in year 1, 4x in year 2, 8x in year 3 and so on. Analysis of technological history shows that the growth in this sector will be exponential. Growth in the next few decades will be equivalent to linear growth over thousands of years **Kurzweil2004**. This is comparable to the story of the emperor and chess board inventor; the emperor promised twice the previous grains of rice per square to the inventor: one grain for the first square, two grains for 2nd and so on. By the time they reached the 63rd square, the emperor would owe an amount of rice equivalent to the surface area of the earth. The initial steps might seem small, but as we progress, the later growth will be astounding.

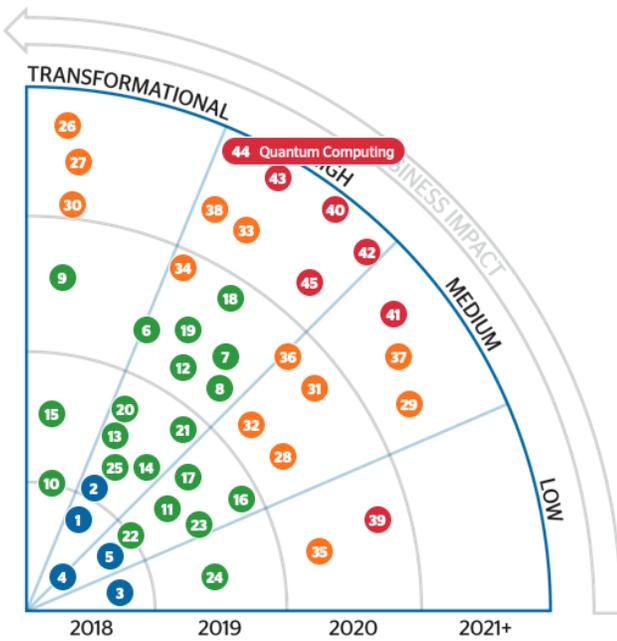
As per the law of accelerating returns, evolution also operates like a positive feedback loop. The evolutionary process returns from one phase are improved and supplied to the next phase. As the process becomes more effective in every phase, an increasing amount of resources is invested in this process, thereby accelerating the progress at an exponential pace. This exponential growth is supplied to the next phase, and the learning is further advanced, thereby exponentially accelerating the already exponential growth. This constant feedback mechanism is the law of accelerating returns. Biological evolution is one such example. This law is essential in predicting the future of computing. The growth trends of the computational power, RAM cost and size, secondary storage size, modem cost and performance all follow this pattern, and hence, it becomes relatively less complex to predict the future of computing. While exponential growth is not forever **E.Berman2018**, when one technology slows down, another picks up, and the progress continues. This paradigm of thinking reduces disruptive stress and encourages us to look for alternative opportunities. Better planning simply eases the stress of switching from one paradigm to another.

Appendix B

Market research on companies and their interest in QCs.

Figure 17

Atos 2018 prediction of QC business impact
Gheorghiu2018: *This company predicted the QC to be one of the high-impact innovations of the future, and it is slowly tending towards a transformational concept that is going to make a significant impact on all industries.*



© Atos 2018 All rights reserved.
 Source : Atos industry and technology experts