A PERFECT BEGINNERS GUIDE TO QUANTUM COMPUTING

An Applied Approach Program ;Next-Gen Computers for Hard, Real-World Applications

William Owen PH.D

Table of Contents

introduction

Quantum Bit or Qubit is the fundamental unit of quantum information that represents subatomic particles such as atoms, electrons, etc. as a computer's memory while their control mechanisms work as a computer's processor. It can take the value of 0, 1, or both simultaneously. It is a million times more powerful than today's strongest supercomputers. Production and management of qubits are tremendous challenges in the field of engineering. They acquire both, digital as well as analog nature which gives the quantum computer their computational power.

What Is Quantum Computing

Quantum computing is an area of computing focused on developing computer technology based on the principles of quantum theory, which explains the behavior of energy and material on the atomic and subatomic levels.

Classical computers that we use today can only encode information in bits that take the value of 1 or 0. This restricts their ability. Quantum computing, on the other hand, uses quantum bits or qubits. It harnesses the unique ability of subatomic participles that allows them to exist in more than one state i.e. a 1 and a 0 at the same time. Superposition and entanglement are two features of quantum physics on which these supercomputers are based. This empowers quantum computers to handle operations at speeds exponentially higher than conventional computers and at much lesser energy consumption.

History of computing

Evolution in one region of science and technology leads to the discovery of a new one. In less than a century, research and development of functional computing technologies have renovated science, technology, and nation massively. The first practical computer around the 20th century was not capable of doing mathematical computations, on its own. Practical devices need a solid physical implementation of theoretical concepts. Nowadays, computers are solving problems instantly and accurately provided the input is relevant, and a set of instructions given are favorable. It all started from World War II when Alan Turing created a real general-purpose computer with a storable program model and is known as the 'Universal Turing Machine'. It was redesigned by Von Neumann and is now the most important architecture for almost every computer. The computers and their physical parts kept improving with time in terms of performance and their strengths. And gradually, the industry of computers became larger than the military department which initiated it. The advancement in control and understanding of humans over nature and physical systems has given us the latest electronic devices we are utilizing today.

Where the concept of bits came from?

Transistors are the fundamental construction blocks for an IC which are connected through wires in a circuit. They conduct electric signals between devices. The communication between transistors within an IC takes place through electric signals. The behavior of the signals is analog in nature. Therefore, their values are real numbers that change smoothly between 0 and 1. These electric signals can also interact with the environment resulting in noise. Therefore, a little change from 0 to 0.1 due to temperature or vibrations from the environment can drastically change the system's behavior. There are two types of noise present in the environment. The first type of noise results from energy instabilities occurring suddenly within the object like temperature above absolute zero Kelvin. These are fundamental in nature. Other types of noise are the consequences of signal interactions. This type of noise could have corrected or designed. But neither of them got designed nor corrected or maybe left intentionally uncorrected at the hardware layer. They are systematic in nature [5].

QUANTUM COMPUTING FUNDAMENTALS

All computing systems rely on a fundamental ability to store and manipulate information. Current computers manipulate individual bits, which store information as binary 0 and 1 states. Quantum computers leverage quantum mechanical phenomena to manipulate information. To do this, they rely on quantum bits, or qubi

Understanding Quantum Computing

While the classical computer is very good at calculus, the quantum computer is even better at sorting, finding prime numbers, simulating molecules, and optimization, and thus could open the door to a new computing era," a Morgan Stanley report noted.

According to the Institute for Quantum Computing at the University of Waterloo, the field of quantum computing started in the 1980s. It was then discovered that certain computational problems could be tackled more efficiently with quantum algorithms than with their classical counterparts.

Quantum computing could contribute greatly in the fields of finance, military affairs, intelligence, drug design and discovery, aerospace designing, utilities (nuclear fusion), polymer design, Artificial Intelligence (AI) and Big Data search, and digital manufacturing.

Its potential and projected market size has engaged some of the most prominent technology companies to work in the field of quantum computing, including IBM, Microsoft, Google, D-Waves Systems, Alibaba, Nokia, Intel, Airbus, HP, Toshiba, Mitsubishi, SK Telecom, NEC, Raytheon, Lockheed Martin, Rigetti, Biogen, Volkswagen, and Amgen.

RESEARCH CHALLENGES IN QUANTUM COMPUTING

EPiQC researchers are developing and delivering tutorials for professionals on the topic of quantum computation, compelling computation problems, and the ways in which computer scientists can contribute to this work.

In this video, Fred Chong opens the EPiQC tutorial at ISCA 2018 with an introduction to the field of quantum computing and the related research challenges. He also discusses the motivation for the co-design structure of the EPiQC Project. Slides from this presentation are available here.

CATEGORIES OF QUANTOM COMPUTING

Analog quantum computer

This type of system performs its operation by manipulating the analog values in the Hamiltonian representation. It does not use quantum gates. It includes quantum annealing, quantum simulation and adiabatic quantum computing. The quantum annealing is done using some initial set of qubits that gradually changes the energy encountered by the system until the problem parameters are defined by Hamiltonian. This is done in order to get the highest probability final state of the qubits that corresponds to the solution of that problem. The adiabatic quantum computer performs computation using some initial set of qubits in the Hamiltonian ground state and then Hamiltonian is changed slowly enough such that it stays in its ground state or lowest possible energy while the process takes place. It has processing power similar to a gate-based computer but still cannot perform full error correction.There are three basic types of analog quantum computing. These are divided on the basis of the required amount of processing power (number of qubits) and time to become practically and commercially available.

Quantum Annealing

A basic rule of physics is that everything inclines towards a minimum energy state of a problem. This behavior is also true in the world of quantum physics. Quantum annealing is naturally used for real low-energy solutions such as optimization problems. It is useful where the best solution is needed out of all possible solutions available. However, it is least powerful among all the types available. An example of this demonstrates an experiment to optimize traffic flows in a crowded city. Such an algorithm could successfully decrease traffic by choosing a convenient path. Volkswagen performs this with Google and D-wave system partnership. Such an experiment can be applied on a universal scale for all to get the cost-productive travel. This method can be applied to a collection of industry problems. For example, optimization of the flight route, petroleum price, weather and temperature information and passenger details, developing commercial aircraft.Quantum annealing is also used for digital modeling, sampling problems and other science fields. This will take only a couple of hours to model all the individual atoms of air flowing over an airplane's wing at every tilts and speeds to formulate an optimized wing design. Using a sampling problem from energy-based distribution, the shape of energy can be characterized and is useful in machine learning problems. The samples improve the model using information about the state of the model for the given parameters.

Quantum Simulation

Quantum simulations examine certain problems in quantum mechanics that are beyond classical physics. Simulating quantum phenomena that are complex in nature is one of the most important applications of quantum computing such as quantum chemistry. It includes modeling of chemical reactions on a large number of quantum subatomic particles. Quantum simulators can be used to simulate the misfolded protein structure. Diseases like Alzheimer's are caused by misfolded proteins. Using random computer simulation, researchers test new treatment drugs and learn reactions. To achieve correctly folded protein structure and study all drug-induced effects, sequential sampling is done which could take more than a million years. Quantum computers can help evaluate it for making more effective treatments and medicines and it would be a significant healthcare improvement. In the future, quantum simulations will facilitate quick drug designing and testing by evaluating every possible drug combinations of protein.

ABSTRAC:

The simplest "theoretical" digital computer is the Turing machine [44, 45]. Here the word "digital" indicates that the computer operates only with definite numbers (and does not use any quantum mechanical superposition of states). This machine was suggested by the British mathematician, A.M. Turing. The Turing machine has three parts, a tape divided into the squares, a scanner, and a dial,

This machine can write a symbol X or 1 in a blank square, and erase them. Any positive integer is written as a sequence of 1's. For example, the number 5 corresponds to the sequence 11111. The symbol X indicates where a number begins or ends. For example, Fig. 2.1 shows two numbers 1 which are "prepared" for addition. The program for addition is presented in Tbl. 2.1. The symbol D is the command to "write the digit 1" in the corresponding square on the tape; X means "write X"; E means "erase"; R means "move the tape one square to the right"; L means "move tape one square to the left". The numbers 1 to 6 after the letter indicate the command to "change the dial setting to this number". The question mark represents a "mistake"; an exclamation mark means "job is completed"…

Quantum Physics and Computation

We often think of information in terms of an abstract mathematical concept. Toget into the theory of what information is, and how it is quantified, would easilytake a whole course in itself. For now, we fall back on an intuitive understanding of the concept of information. Whatever information is, to be useful it mustbe stored in some physical medium and manipulated by some physical process.

This implies that the laws of physics ultimately dictate the capabilities of anyinformation-processing machine. So it is only reasonable to consider the laws ofphysics when we study the theory of information processing and in particularthe theory of computation.

Up until the turn of the twentieth century, the laws of physics were thought to be what we now call classical. Newton's equations of motion and Maxwell's equations of electromagnetism predicted experimentally observed phenomena with remarkable accuracy and precision.

At the beginning of the last century, as scientists were examining phenomena on increasingly smaller scales, it was discovered that some experiments did not agree with the predictions of the classical laws of nature. These experiments involved observations of phenomena on the atomic scale, that had not been accessible in the days of Newton or Maxwell.

The work of Planck, Bohr, de Broglie, Schr¨odinger, Heisenberg and others lead to the development of a newtheory of physics that came to be known as 'quantum physics'. Newton's andMaxwell's laws were found to be an approximation to this more general theory of quantum physics.

The classical approximation of quantum mechanics holds up very well on the macroscopic scale of objects like planets, airplanes, footballs, or even molecules. But on the 'quantum scale' of individual atoms, electrons, and photons, the classical approximation becomes very inaccurate, and the theory of quantum physics must be taken in to account.

A new kind of computing

We experience the benefits of classical computing every day. However, there are challenges that today's systems will never be able to solve. For problems above a certain size and complexity, we don't have enough computational power on Earth to tackle them.

To stand a chance at solving some of these problems, we need a new kind of computing. Universal quantum computers leverage the quantum mechanical phenomena of superposition and entanglement to create states that scale exponentially with number of qubits, or quantum bits.

Learn more about one of the first, most promising application areas of quantum computing:

QUANTUM WORKSPACE

You use the Azure Quantum service by adding an Azure Quantum workspace resource to your Azure subscription in the

Azure portal. A Quantum workspace resource, or workspace for short, is a collection of assets associated with running quantum or optimization applications. One of the properties configured in a workspace is an Azure Storage Account resource, where Azure Quantum stores your quantum programs and optimization problems for access.

Providers and targets

Another property configured in the workspace is the provider that you want to use to run programs in that workspace. A single provider may expose one or more targets, which can be quantum hardware or simulators, and are ultimately responsible for running your program.

By default, Azure Quantum adds the Microsoft QIO provider to every workspace, and you can add other providers when you create the workspace or any time afterward. For more information, see the Microsoft QIO provider.

Provider billing

Each additional provider you add to a workspace requires a billing plan, which defines how that provider bills for usage. Each provider may have different billing plans and methods available. For more information, see the documentation on the provider you would like to add.

You can only select one billing plan for each provider in a single workspace; however, you can add multiple workspaces to your Azure subscription.

Jobs

When you run a quantum program or solve an optimization problem in Azure Quantum, you create and run a job. The steps to create and run a job depend on the job type and the provider and target that you configure for the workspace. All jobs, however, have the following properties in common:

How q uantum computers will revolutionize everything

For decades, computer scientists have relied on bettering software to run increasingly complex programs. But, there are limitations to software optimization. Sooner or later, we'll need more powerful machines to meet our requirements.

Quantum computers could help researchers help simulate complex biological processes. They could help decode encryption puzzles and map climate change.

With superpowered processors, quantum computers could redefine how we interact with fields as diverse as engineering, medical science, and geopolitics. Perhaps the most salient issue quantum computers could address is our ability to properly document, study, and use big data.

We aren't too far from a 300-qubit computer, either. IBM has already created a 50-qubit processor. Only a year ago, a computer with qubits in the teens was an impressive feat. The advance of quantum computers in many ways has already eclipsed itself.

This leads us to an important question: what could we do with this power today? What's next for AI developers and quantum computer manufacturers? What could they jointly improve?

How quantum computing and AI will change big data

According to Northeastern University, we create 2.5 exabytes of data every single day. To put that number in perspective, that's equivalent to about 90 years of HD Video. This massive daily production of data has generated a new field: big data.

What we could do with data collected from laptops, computers, phones, and wearable technology seems limitless. Big data means we have access to incredibly large data sets about everything from the number of emails sent on a particular day to how consumer behavior is affected by exercise.

Actually analyzing big data on a granular level is near impossible, however. Finding correlated data with big data is like trying to find a needle in a haystack. What's more, certain patterns may not be obvious to research. We lose precious data in a sea of noise.

Big data is one of the areas in which the marriage of artificial intelligence and quantum computers shines. Powerful quantum processors would be able to handle massive data sets, and artificial intelligence could analyze big data on a granular level.

Researchers are already using artificial intelligence to analyze large data sets. One medical startup has used AI to expedite cancer research. More powerful AI could make these computations much more quickly and effectively.

Quantum Computing: How it differs from classical computing?

understand how a quantum computer works, and the quantum mechanics on which it is based, we should look back to the beginning of the 20th century, when this physical theory was first raised. Among other subjects of study, quantum physics began with the study of an atom's particles and its electrons at a microscopic scale, something that had never been done before. Arnau Riera — doctor in theoretical physics; high school teacher; and advisor to Quantum, an exhibition hosted at the Center of Contemporary Culture of Barcelona (CCCB) — defines it as a conceptual change. “In the classical world, the properties of the systems that we study are well defined. In the quantum world, this isn’t the case: particles can have different values, they are not isolated objects, their states are diluted,” he explains.

Quantum physics is so complex that even Richard Feyman, 1965 Nobel Laureate in Physics and one of the fathers of quantum computing in the 1980s famously said, “I think I can safely say that nobody understands quantum mechanics”.

As the reality of a quantum computer comes closer, it is useful for us to understand both how one functions and how it’s different from a traditional computer. The first thing to bear in mind is that they use different basic units of data: ‘bits’ and ‘qubits’. Every element of a classical computer is written in binary code (1s and 0s) and is translated into electricity: high voltage is represented by 1, and low voltage by 0. In quantum computing, qubits are the basic unit and their value can be 1, 0, or 1 and 0 simultaneously, overlapping (superposition) and intertwining (entanglement) according to the laws of physics. This means that qubits, as opposed to bits, can take on various values at one time and can perform calculations that a conventional computer cannot.

The topography of q uantum technology

The quantum phenomena are not limited to just quantum computing but they apply to other technologies also including quantum information science, quantum communication, and quantum metrology. The progresses of all these technologies are mutually dependent on each other and can control as well as transform the entire quantum system. They share the same theory of physics, common hardware and related methods.Quantum Information Science seeks the methods of encoding the information in a quantum system. It includes statistics of quantum mechanics along with their limitations. It provides a core for all other applications such as quantum computing, communications, networking, sensing and metrology.Quantum Communication and networking concentrates on the conversation or exchange of information by encoding it into a quantum system to facilitate communication between quantum computers. Quantum cryptography is the subset of quantum communication in which quantum properties help to design the secure communication system.Quantum sensing and metrology is the study and development of quantum systems. The drastic sensitivity of such a system to environmental nuisances can be utilized in order to measure important physical properties (e.g. electric and magnetic fields, temperature, etc.) more accurately than classical systems. Quantum sensors are based on qubits and are carried out using the experimental quantum systems.Quantum computing is the central focus of this research which exploits the quantum mechanical properties of superposition, entanglement and interference to enact computations. In common, a quantum computer is a physical system that comprises a collection of qubits that must be isolated from the environment for their quantum state to stay coherent until it performs the computation. These qubits are organized and manipulated in order to enforce an algorithm and to achieve a result with high probability from the measurement of its final state.

Properties of q uantum computing

In quantum physics, the quantum object does not exist in an entirely determined state. It looks like a particle but behaves like a wave when not being observed. This dual nature of particles leads to interesting physical phenomena. The state of any quantum object is expressed as a sum of possible participating states or a wave-function. Such states are coherent due to the interference of all the participating states either in a constructive or a destructive manner. Observation of quantum objects when they interact with some larger physical system results in the extraction of information. Such observation of quantum objects is called quantum measurement. Measurement can also result in the loss of information by disrupting the quantum state. These are some of the properties of quantum objects. Quantum objects referred here are the qubits in the case of quantum computing. The progress of any quantum system is regulated by Schrodinger's equation that tells us about the change in the wave-function of the system due to the energy environment. This environment is the system Hamiltonian which is a mathematical description of energies experiencing from all forces felt by all components of the system. To control any quantum system, there is a need to control this environment by isolating the system from the forces of the universe that cannot be controlled easily and by assigning energy within this isolated area only. A system cannot be completely isolated. However, energy and information exchanges can be minimized. This interaction with the outside environment can lead to loss of coherence and can result in Decoherence.

The properties are the conceptual rules and mathematical manifestations that describe the behavior of the particles. Quantum computers use three fundamental properties of quantum mechanics to store, represent, and perform operations on data in such a way so that it can compute exponentially faster than any classical computer. The three properties are given as follows [8]:

SUPERPOSITION

Superposition in quantum mechanics states that any two quantum states can be summed up (superposed) resulting in another valid quantum state. It is a fundamental principle of quantum mechanics. Oppositely we can say that any quantum state is the sum of two or more than two other unique states.

Superposition in quantum computing refers to the ability of a quantum system where quantum particle or qubit can exist in two different positions or say, in multiple states at the same time. It provides high-speed parallel processing in an unbelievable way and is very different from their classical equivalents that have binary constraints. The quantum computer system holds the information that exists in two states simultaneously. Qubits are brought into a superposition by influencing them with the help of lasers so that it can simultaneously store 0 and 1 at the same time. In classical computing, if there are 2 bits, the total possible values after combining we get are 4, out of which only 1 value is possible at any instant. But on the other hand, if there are 2 qubits in the quantum computer. The total possible values after combination are 4 and all are possible at once. It looks like unthinkable because it is not like gravity that can be proved easily just by looking at the falling of an apple. The laws of classical physics fail here because superposition only exists in the territory of quantum particles.

For example, when solving a puzzle-like maze, a quantum particle can decide to take the various paths at the same time using superposition. This process matches the function of the parallel computer. Due to this property, the qubit is able to navigate the maze in exponentially less time than a classical bit

ENTANGLEMENT

Entanglement in quantum mechanics is a physical phenomenon where two or more quantum objects are inherently linked such that measurement of one rules the possible measurement of another. In other words, a pair or a group of particles interacts or share spatial locality such that the quantum state of each particle cannot be characterized independently of the other particle’s state in the same group even when they are separated by a large distance.

How quantum computers will change everything without you noticing

The recent string of quantum computing breakthroughs has optimism in the field at an all-time high. That quantum computers are imminent seems certain, but we shouldn't expect IBM or Apple to start shipping the first generation of personal quantum computers (PQCs maybe?) anytime soon — or ever.

Understanding what quantum computing means to the world is as much a matter of philosophical guesswork as mathematical certainty. Humans don't have a firm grasp on how the universe works, especially when it comes to quantum mechanics. Quantum computers promise to unlock those mysteries, but predicting the future of this technology would be akin to asking Benjamin Franklin his thoughts on smartphones that support wireless charging.

The idea that quantum computers will one day replace regular computers should be taken with an understanding that it won't be an ubiquitous takeover. They will almost certainly replace specific classical computers, even rendering many obsolete. But, for the same reason you don't need a supercomputer inside of an adding machine, we're not going to put quantum processors in all computers.

Quantum supremacy, the point where quantum systems perform useful functions that classical ones can't, won't happen overnight. And once it does, it could take years for developers and researchers to figure out how best to use this new technology. But, it'll almost certainly happen.

When dedicated quantum systems, designed to perform a specific function, do become a part of the global technological landscape, there's no denying they'll have a huge impact. We'll "know" more than we ever have as a species, and that's going to be great for science, but could put a damper on a lot of cultural, social, and economical norms that place a premium on human guesswork.

Before Google Search came along, as those of us old enough to remember will recall, we used to argue and debate things like whether it was Christopher Walken or Al Pacino in that one movie where the guy does that thing. Now we can just Google both actors' filmography immediately with the tap of a button.

Some people have said this has caused a lack of social discourse. Who among us hasn't heard someone complain about how everyone is always on their phones now and nobody talks to each other anymore?

The closer we get to understanding the ground-truths of the universe, the less we'll need pedantic debate about facts. Quantum computers promise to eliminate more of the fuzzy gray areas that exist in humanity's understanding of the universe – basically doing for science what Google Search did for your ability to win an argument with your ridiculous uncle who thinks he knows everything, but for some stupid reason thinks Prince sang Beat It instead of Michael Jackson.

If quantum computers unravel metaphysical puzzles and solve some of science's toughest problems, the biggest change we'll see from them will come in the form of knowledge. Gravity, for example, has only been explained through theory at this point. A quantum system might fundamentally answer this and many more of science's outstanding questions.

Need for q uantum computers

Quantum computers can solve any computational problem that any classical computer can. According to the Church-Turing thesis, the converse is also true that classical computers can solve all the problems of quantum computers too. It means they provide no extra benefit over classical computers in terms of computability but there are some complex and impossible problems that cannot be solved by today's conventional computers in a practical amount of time. It needs more computational power. Quantum computers can solve such problems in reasonably and exponentially lower time complexities, also known as “Quantum Supremacy”.

Peter Shor in 1993 showed that Quantum computers can help to solve these problems considerably more efficiently like in seconds without getting overheated. He developed algorithms for factoring large numbers quickly. Since their calculations are based on the probability of an atom’s state before it is actually known. These are having the potential to process data in an exponentially huge quantity. It also explains that a practical quantum computer could break the cryptographic secret codes. It can risk the security of encrypted data and communication. It can expose private and protected secret information. But the advantages of quantum computers are also kept in mind that is significantly more than its flaws. Hence, they are still needed and further research is going towards a brighter future.

Design limitations of quantum computer

The exponential computing power of quantum computers can be accomplished by assessing and rectifying any kind of design limitation which helps to avoid their quality degradation. There are four major design limitations. The first limitation is that the number of coefficients in Dirac notation that defines the state of a quantum computer rise exponentially with the rise in the number of qubits, only when all the qubits get entangled with each other. To obtain the full potential of quantum computing, qubits must follow the property of entanglement where the state of any qubit must be linked with states of other qubits. It cannot be achieved directly since it is hard to generate a direct relation between qubits. But it can be decomposed into a number of simple fundamental operations directly aided by the hardware. One can also perform indirect coupling which is known to be an overhead in machines in classical computing and is crucial at the early stages of development especially when qubits and gate operations are confined.The second limitation is that it is impossible to copy an entire quantum system because of a principle called a no-cloning principle. There is a risk of deletion of arbitrary information from the original qubits since the state of qubits or set of qubits are moved to another set of qubits rather than being copied. The generation and storage of copies of intermediate states or partial outcomes in memory is a necessary aspect of classical computing. But quantum computers need a different strategy. There are quantum algorithms that help to access classical bits from the storage so that it can be known which bits are loaded and being queried into the memory of the quantum system to perform its task successfully.The third limitation is due to the absence of noise protection of qubit operations. The small deformities in gate operations or input signals are collected over time disturbing the state of the system because they are not discarded by the fundamental gate operations. This can highly affect the calculation preciseness, measurements and coherence of the quantum systems and lessen the qubit operations integrity.The final limitation is the incapability of the quantum machine to identify its full state even after it has finished its operation. Assume quantum computer has introduced an initial set of qubits with the superposition of all states combination. After applying a function to this state, the new quantum state will have information about the function value for each possible input and measuring this quantum system will not give this information. Therefore, a successful quantum algorithm can be achieved by manipulating the system in such a way so that states after finishing the operations have a higher probability of getting measured than any other probable result.

Importance of q uantum computing

It is clearly possible to build a quantum computer that could perform computations that would run a lifetime on a classical computer. Practical applications of quantum computing need controlling the quantum phenomena and thus the quantum world to an exceptional level. This job requires substantial engineering and research to build, manage and employ a noiseless quantum system. The experiment with quantum supremacy is an important test of the theory of quantum mechanics that will help to improve the support of quantum theory and leads to unexpected discoveries. The development of aspects and components of quantum information technology and computing has already started to influence the area of physics. The quantum error correction theory to attain the fault-tolerant quantum system has proven important. The quantum information theory is practically useful to study physics and dynamics of multibody systems like a massive number of quantum subatomic particles and even in blackhole and related concepts. Advancement in this area is important for an accurate understanding of various physical structures. It has contributed to many other engineering fields like physics, mathematics, chemistry, computer science, material science, etc. It has also advanced classical computing. Strategies to develop a quantum computing algorithm have helped in improving the classical computing algorithm also. Research in the quantum algorithm has answered many questions in the computer science area. It can help to evaluate the safety of cryptographic systems, clarifying the limitations of physical computational and advancing computational methods. It will help to advance the human's understanding of the universe. The qubits that are recently being used in quantum computing is also used for building sensors, precision clocks, and other applications. Quantum communication is used for communicating two quantum systems at distance. There is an increased risk of asymmetric cryptography as well as the entire security system. Hence, the actions are being taken towards new quantum cryptography. The development of quantum information, science, technology and computing is a global area now.

Major challenges in q uantum computing

The good news is that at any instant of time, the quantum state with the same number of quantum bits can stretch over all possible states as compared to classical computers and thus works in an exponentially massive space. However, to be able to use this space requires all qubits to remain interconnected. Even after such progress, improvements are still needed. The bad news is that making new and high-quality qubits does not guarantee the creation and efficient use of fault-tolerant quantum computers and is still having challenges in its path.Qubits cannot naturally ignore the noise. Hence, the quantum system is more error-prone. It suffers from Decoherence. The biggest challenge is how it can handle any undesirable deviations or noise in quantum computers. Classical computers can produce clean noise-free outcomes by simply putting its state as off or '0', which is not possible for quantum computers where errors occur in physical circuits. Qubits will gradually lose its information as well as interconnection (entanglement) between each other. The error rate is seen as a design parameter for such systems which should be improved in large qubit systems also. However, to make the qubits stable and error-free, they are being insulated from the outside environment in super-refrigerated fridges or vacuum chambers and accurately handled.Qubits are neither completely binary nor digital. It is having analog properties also. Gate can reject noise by dealing with the input signal value of 0.8 and treating it as 1. But in the analog signal, every value between 0 and 1 is permitted since they have their meanings. Signals cannot be checked for any kind of noise or corruption. Since 0.8 can be 1 with some error or 0.8 without error. Presuming the error as 0 like Gates do or taking some noise value even if it was not present there can affect the adherence of the resulting quantum computation. Hence, there is a need for algorithms like quantum error correction similar to the logical error correction in classical computers. These algorithms can be run on a noisy gate-based quantum computer to eliminate the errors and noises present in them.It is possible to employ a Quantum Error Correction algorithm on a quantum system. But quantum error correction requires dealing with the overhead such as a large number of qubits and their fundamental operations and generally needs more resources. Also, problems with large data inputs require a large amount of time to create the input quantum state that would monopolize the computation time lessening the quantum benefits.Quantum algorithm development is another challenge since achieving quantum speedup expects entirely new types of algorithm design as the speed of computation depends on the design of the algorithm. The design of the algorithm should be corresponding to the number of qubits used.Further development of software tools in addition to hardware, is required to create and debug quantum systems to help explain unknown issues and push towards designs.Debugging quantum hardware and software is of utmost importance which depends on memory and intermediate machine states in classical computers. But in the case of quantum computing, states cannot be copied directly for later evaluation, and directly measuring intermediate state can bring it to halt. Hence, new strategies for debugging are essential for their development.

What can we do with a q uantum computer?

Areas where quantum computing can deliver new applications and developments range from the pharmaceutical industry and medicine research, the creation of new materials, and even what is being called "quantum finance" — an area in which BBVA has already taken an interest. In this sector, we can use classical computing and mathematical algorithms to make predictions about the future risk of a portfolio or we can study the stock market during a window of time. But quantum computing opens a completely new range of options to be explored. "A quantum computer can create superposition with multiple probabilities that we cannot achieve today, let alone examine the features of those probabilities. With this type of application, the quantum computer will be much more efficient than a classical computer," asserts García Ripoll.

Despite all the possibilities promised by quantum computing, we mustn't get ahead of ourselves, particularly in everyday life. We won't see massive improvements in speed when downloading videos; nor will video game players benefit from even better graphics cards. Researchers are working on algorithms and mathematical models so that in a near future tasks that take a long time today can be executed more efficiently. “Quantum computing is just getting started, we are very much in the early days,” concludes Garcáa Ripoll.

FINAL THOUGHT

Quantum Computing is a new and exciting field at the intersection of mathematics, computer science and physics. It concerns a utilization of quantum mechanics to improve the efficiency of computation. Here we present a gentle introduction to some of the ideas in quantum computing. The paper begins by motivating the central ideas of quantum mechanics and quantum computation with simple toy models. From there we move on to a formal presentation of the small fraction of (finite dimensional) quantum mechanics that we will need for basic quantum computation. Central notions of quantum architecture (qubits and quantum gates) are described. The paper ends with a presentation of one of the simplest quantum algorithms: Deutsch's algorithm. Our presentation demands neither advanced mathematics nor advanced physics.

Conclusion

At present, a normal home computer wouldn't have the ability to process large amounts of data at once. Quantum computers could have the capability of reaching into a database, instantly accessing all items at once, and deliver an analysis within seconds. With quantum computers, we could uncover patterns instantly. What's next for AI and quantum computers? It is truly hard to say what we should expect from two areas of research that are advancing at lightning speed. At present, it seems like the first area of research to be most impacted by the melding of these two subsets of computer science will be big data.