International Journal of Science and Research (IJSR)
ISSN: 2319-7064
ResearchGate Impact Factor (2018): 0.28 | SJIF (2019): 7.583

Quantum Computing

Shaifali Rastogi

Abstract: ***Quantum computing is an emerging technology. The clock frequency of current computer processor systems may reach about 40 GHz within the next 10 years. By then, one atom may represent one bit. Electrons under such conditions are no longer described by classical physics, and a new model of the computer may be necessary by that time.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.In this paper we briefly survey what is quantum computing, potential quantum applications, and useful areas of Quantum Computing.***

Keywords: Quantum Computing, Quantum Applications, Useful areas of Quantum Computing

1. Introduction

Quantum computing began in the early 1980s, when physicist Paul Benioff proposed a quantum mechanical model of the Turing machine [1].Richard Feynman and Yuri Manin later suggested that a quantum computer had the potential to simulate things that a classical computer could not [2], [3]. In 1994, Peter Shor developed a quantum algorithm for factoring integers that had the potential to decrypt all secured communications.[4] Despite ongoing experimental progress since the late 1990s, most researchers believe that "fault-tolerant quantum computing [is] still a rather distant dream".
[5]

Quantum computing is the use of quantum-mechanical phenomena such as superposition and entanglement to perform computation. A quantum computer is used to perform such computation, which can be implemented theoretically or physically [6]. There are currently two main approaches to physically implementing a quantum computer: analog and digital. Analog approaches are further divided into quantum simulation, quantum annealing, and adiabatic quantum computation. Digital quantum computers use quantum logic gates to do computation. Both approaches use quantum bits or qubits [6].

Quantum Computing is not about changing the notion of computation itself. The change starts at the most basic level: the fundamental unit of computation is no longer the bit, but rather the quantum bit or qubit.[7]Qubits are fundamental to quantum computing and are somewhat analogous to bits in a classical computer. Qubits can be in a 1 or 0 quantum state, or they can also be in a superposition of the 1 and 0 states. However, when qubits are measured the result is always either a 0 or a 1; the probabilities of the two outcomes dependon the quantum state that the qubits were in immediately prior to the measurement. Computation is performed by manipulating qubits with quantum logic gates, which are somewhat analogous to classical logic gates.

There are currently two main approaches to physically implementing a quantum computer: analog and digital. Analog approaches are further divided into quantum simulation, quantum annealing, and adiabatic quantum computation. Digital quantum computers use quantum logic gates to do computation. Both approaches use quantum bits or qubits [6]. There are currently a number of significant obstacles in the way of constructing useful quantum computers. In particular, it is difficult to maintain the quantum states of qubits as they are prone to quantum decoherence, and quantum computers require significant error correction as they are far more prone to errors than classical computers.[8],[9]

2. Quantum Applications

2.1 Cryptography

Integer factorization, which underpins the security of public key cryptographic systems, is believed to be computationally infeasible with an ordinary computer for large integers if they are the product of few prime numbers (e.g., products of two 300-digit primes).[10] By comparison, a quantum computer could efficiently solve this problem using Shor's algorithm to find its factors. This ability would allow a quantum computer to break many of the cryptographic systems in use today, in the sense that there would be a polynomial time (in the number of digits of the integer) algorithm for solving the problem. In particular, most of the popular public key ciphers are based on the difficulty of factoring integers or the discrete logarithm problem, both of which can be solved by Shor's algorithm. These are used to protect secure Web pages, encrypted email, and many other types of data. Breaking these would have significant ramifications for electronic privacy and security.

However, other cryptographic algorithms do not appear to be broken by those algorithms.[11],[12] Some public-key algorithms are based on problems other than the integer factorization and discrete logarithm problems to which Shor's algorithm applies, like the McEliece cryptosystem based on a problem in coding theory. [11],[13] Lattice-based cryptosystems are also not known to be broken by quantum computers, and finding a polynomial time algorithm for solving the dihedral hidden subgroup problem, which would break many lattice based cryptosystems, is a well-studied open problem.[14]

It has been proven that applying Grover's algorithm to break a symmetric (secret key) algorithm by brute force requires time equal to roughly $2^{n/2}$ invocations of the underlying cryptographic algorithm, compared with roughly 2^n in the classical Potential applications Cryptography case,[15] meaning that symmetric key lengths are effectively halved: AES-256 would have the same security against an attack

using Grover's algorithm that AES-128 has against classical brute-force search.

Quantum cryptography could potentially fulfill some of the functions of public key cryptography. Quantumbased cryptographic systems could, therefore, be more secure than traditional systems against quantum hacking.[16]

2.2 Quantum Search

Besides factorization and discrete logarithms, quantum algorithms offering a more than polynomial speedup over the best known classical algorithm have been found for several problems,[17] including the simulation of quantum physical processes from chemistry and solid state physics, the approximation of Jones polynomials, and solving Pell's equation. No mathematical proof has been found that shows that an equally fast classical algorithm cannot be discovered, although this is considered unlikely. [18] However, quantum computers offer polynomial speedup for some problems. The most well-known example of this is quantum database search, which can be solved by Grover's algorithm using quadratically fewer queries to the database than that are required by classical algorithms. In this case, the advantage is not only provable but also optimal, it has been shown that Grover's algorithm gives the maximal possible probability of finding the desired element for any number of oracle lookups. Several other examples of provable quantum speedups for query problems have subsequently been discovered, such as for finding collisions in two-to-one functions and evaluating NAND trees.

Problems that can be addressed with Grover's algorithm have the following properties:

1) There is no searchable structure in the collection of possible answers.
2) The number of possible answers to check is same as the number of inputs to the algorithm.
3) There exists a boolean function which evaluates each input and determines whether it is the correct answer.

For problems with all these properties, the running time of Grover's algorithm on a quantum computer will scale as the square root of the number of inputs (or elements in the database), as opposed to the linear scaling of classical algorithms. A general class of problems to which Grover's algorithm can be applied [19] is Boolean satisfiability problem. In this instance, the database through which the algorithm is iterating is that of all possible answers. An example (and possible) application of this is a password cracker that attempts to guess the password or secret key for an encrypted file or system. Symmetric ciphers such as Triple DES and AES are particularly vulnerable to this kind of attack. This application of quantum computing is a major interest of government agencies. [20]

2.3 Quantum simulation

Since chemistry and nanotechnology rely on understanding quantum systems, and such systems are impossible to simulate in an efficient manner classically, many believe quantum simulation will be one of the most important applications of quantum computing. [21] Quantum simulation could also be used to simulate the behavior of atoms and particles at unusual conditions such as the reactions inside a collider. [22]

2.4 Quantum supremacy

John Preskill has introduced the term quantum supremacy to refer to the hypothetical speedup advantage that a quantum computer would have over a classical computer in a certain field. [23] Google announced in 2017 that it expected to achieve quantum supremacy by the end of the year though that did not happen. IBM said in 2018 that the best classical computers will be beaten on some practical task within about five years and views the quantum supremacy test only as a potential future benchmark.[24]

Although skeptics like Gil Kalai doubt that quantum supremacy will ever be achieved,[25][26] in October 2019, a Sycamore processor created in conjunction with Google AI Quantum was reported to have achieved quantum supremacy, with calculations more than 3,000,000 times as fast as those of Summit, generally considered the world's fastest computer. [27] Bill Unruh doubted the practicality of quantum computers in a paper published back in 1994.[28] Paul Davies argued that a 400-qubit computer would even come into conflict with the cosmological information bound implied by the holographic principle. [29]

3. Useful areas of Quantum Computing

Computers don’t exist in a vacuum. They serve to solve problems, and the type of problems they can solve are influenced by their hardware. Graphics processors are specialized for rendering images; artificial intelligence processors for AI; and quantum computers designed for…what?While the power of quantum computing is impressive, it does not mean that existing software simply runs a billion times faster. Rather, quantum computers have certain types of problems which they are good at solving, and those which they aren’t. Below are some of the primary applications we should expect to see as this next generation of computers becomes commercially available.

3.1 Artificial Intelligence

A primary application for quantum computing is artificial intelligence (AI). AI is based on the principle of learning from experience, becoming more accurate as feedback is given, until the computer program appears to exhibit “intelligence.”The use of quantum algorithms in artificial intelligence techniques will boost machines’ learning abilities. This will lead to improvements in the development, among others, of predication systems, including those of the financial industry. However, we’ll have to wait to start these improvements being rolled out.

Machine learning and artificial intelligence technologies are the two key areas of research in the application of quantum computing algorithms. One of the particularities of this calculation system is that it allows representing several states at the same time**,** which is particularly convenient when using AI techniques. The ability to represent and

handle so many states makes quantum computing extremely adequate for solving problems in a variety of fields.

3.2 Weather Forecasting

The ability to better predict the weather would have enormous benefit to many fields, not to mention more time to take cover from disasters. While this has long been a goal of scientists, the equations governing such processes contain many, many variables, making classical simulation lengthy. Director of engineering at Google Hartmut Neven also noted that quantum computers could help build better climate models that could give us more insight into how humans are influencing the environment. These models are what we build our estimates of future warming on, and help us determine what steps need to be taken now to prevent disasters.

The United Kingdom's national weather service Met Office has already begun investing in such innovation to meet the power and scalability demands they'll be facing in the 2020-plus timeframe, and released a report on its own requirements for exascale computing.When quantum computing becomes practical, supercomputers will be able to predict micro-meteorological events like the formation of each individual cloud or wind eddy – it might even be possible to forecast conditions in your own back yard!

3.3Cryptography

Public key encryption (also known as asymmetric encryption) actually relies on a number of mathematical algorithms that are considered too complex to break, especially when using an encryption key of a good size such as RSA-2048, ECDSA-256. Again, even with a massive amount of conventional computing power it might take an amount of time equivalent to the age of our universe (no, this is not a joke!) to ensure that cryptography will, in fact, be broken.

Quantum computing is a game-changer. It is possible to use something like the Shor's algorithm, which explores quantum mechanics to solve the problem of integer factorization (i.e., given an integer **N**, find its prime factors) or another similar hypothesis such as the discrete logarithm problem. This is something essentially unfeasible for regular computers when the numbers involved are too large. But why would that matter? Well, many asymmetric cryptographic algorithms, such as RSA, are based on the assumption that large integer factorization is computationally unfeasible.

It may be true that quantum computing is already a reality, but maybe it's still a little early for us to worry too much. Essentially, the quantum computing power needed to break current asymmetric algorithms will still be very expensive, which — at least initially — will probably be restricted to governments, especially those who like to pry into the secrets of other nation-states.

3.4 Financial Modeling

The finance industry has many areas where faster and more secure processing are welcome. The financial sector has many transactions run by algorithms. Using quantum computing would exponentially increase the speed of these transactions, allowing institutions to scale their processing with lower costs as opposed to employing more human or IT resources. Thus, quantum computing is increasingly attracting the interest of financial services firms that are seeking to boost their trade, transactions, and data speed. Quantum computing is a field which applies theories developed under quantum mechanics to solve problems.

Faster processing is made possible because, in quantum computing, data is represented using qubits as opposed to traditional binary units (0 and 1). Qubits are more flexible and allow for a combination of 0 and 1 simultaneously, whereas in the previous data had to be either a 0 or a 1. As such, a set of qubits stores more data than traditional bits.

4. Conclusion

In this paper we have reviewed the introduction of quantum computing, the potential quantum applications and some of the useful areas of Quantum Computing. Several research groups are investigating qubits and quantum 231 logic circuitry using different resources (i.e., atom, ion, electron, and photon, among others). Efforts at realization for quantum computers have just begun. Undoubtedly, we need more intensive research in a physical realization of components of quantum computers. Computer scientists/ engineers will need to consider the various architectural solutions for quantum computers as well as the various new (practical) quantum algorithms to advance the state of the art for quantum computers.

References

[1] Benioff, Paul (1980). "The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines". Journal of Statistical Physics.
[2] Feynman, Richard (June 1982). "Simulating Physics with Computers"(PDF). International Journal of Theoretical Physics.
[3] Manin, Yu. I. (1980). Vychislimoe i nevychislimoe [Computable and Noncomputable] (in Russian).
[4] Mermin, David (March 28, 2006). "Breaking RSA Encryption with a Quantum Computer: Shor's Factoring Algorithm" (PDF).
[5] John Preskill (2018). "Quantum Computing in the NISQ era and beyond".
[6] The National Academies of Sciences, Engineering, and Medicine (2019). Grumbling, Emily; Horowitz, Mark (eds.). Quantum Computing : Progress and Prospects (2018). Washington, DC: National Academies Press.
[7] Quantum Computing: A Gentle Introduction by Eleanor G. Rieffel, Wolfgang H. Polak.

[8] Franklin, Diana; Chong, Frederic T. (2004). "Challenges in Reliable Quantum Computing". Nano, Quantum and Molecular Computing.
[9] Pakkin, Scott; Coles, Patrick (10 June 2019). "The Problem with Quantum Computers". Scientific American.
[10] Lenstra, Arjen K. (2000). "Integer Factoring" (PDF). Designs, Codes and Cryptography.
[11] Bernstein, Daniel J. (2009). "Introduction to post-quantum cryptography".
[12] A bibliography maintained by Daniel J. Bernstein and Tanja Lange on cryptography not known to be broken by quantum computing.
[13] McEliece, R. J. (January 1978). "A Public-Key Cryptosystem Based On Algebraic Coding Theory" (PDF).
[14] Kobayashi, H.; Gall, F.L. (2006). "Dihedral Hidden Subgroup Problem: A Survey". Information and Media Technologies.
[15] Bennett, Charles H.; Bernstein, Ethan; Brassard, Gilles; Vazirani, Umesh (October 1997). "Strengths and Weaknesses of Quantum Computing". SIAM Journal on Computing.
[16] Katwala, Amit (5 March 2020). "Quantum computers will change the world (if they work)". Wired UK.
[17] Quantum Algorithm Zoo Archived 2018-04-29 at the Wayback Machine – Stephen Jordan's Homepage
[18] Schiller, Jon (2009-06-19). Quantum Computers. ISBN 9781439243497.
[19] Ambainis, Ambainis (June 2004). "Quantum search algorithms". ACM SIGACT News.
[20] Rich, Steven; Gellman, Barton (2014-02-01). "NSA seeks to build quantum computer that could crack most types of encryption". Washington Post.
[21] Norton, Quinn (2007-02-15). "The Father of Quantum Computing". Wired.
[22] Ambainis, Andris (Spring 2014). "What Can We Do with a Quantum Computer?"Institute for Advanced Study.
[23] Boixo, Sergio; Isakov, Sergei V.; Smelyanskiy, Vadim N.; Babbush, Ryan; Ding, Nan; Jiang, Zhang; Bremner, Michael J.; Martinis, John M.; Neven, Hartmut (2018). "Characterizing Quantum Supremacy in Near-Term Devices". Nature Physics. 14 (6): 595–600.
[24] Savage, Neil. "Quantum Computers Compete for "Supremacy".
[25] "Quantum Supremacy and Complexity". 23 April 2016.
[26] Kalai, Gil. "The Quantum Computer Puzzle" (PDF). AMS.
[27] "Google researchers have reportedly achieved "quantum supremacy"". MIT Technology Review.
[28] Unruh, Bill (1995). "Maintaining coherence in Quantum Computers". Physical Review A. **51** (2): 992–997. arXiv:hep-th/9406058.
[29] Davies, Paul. "The implications of a holographic universe for quantum information science and the nature of physical law" (PDF). Macquarie University.