International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Quantum Computing: Explained in QU-Bits of Future

Tanishka Gupta[1], Prof. Pranjali Bahalkar[2]

D. Y. Patil College of Engineering, Pune 411044, India, guptatanishka34@gmail.com

ABSTRACT

Theoretically, quantum computers could have computing power many orders of magnitude larger than that of conventional computers. The quantum bit, or qubit, which refers to the quantum state of electrons in an atom, is the fundamental data unit in a quantum computer. Qubits theoretically can be in multiple superposed states at once, allowing them to transport much more data than is possible with traditional two-state bits. The proportionality of qubit states has a mathematical foundation similar to the input weights of neural networks. Although quantum computer technology has made considerable progress, there is still much work to be done in research and development before quantum computers can be considered a viable mainstream technology.

Keywords: quantum, magnitude, qubit, superposed.

Introduction

The studies and discoveries related to quantum computers are surveyed in this study. A novel form of computation called quantum computing, based on quantum mechanics, deals with the physical world's stochastic and erratic nature. Because quantum mechanics is a more comprehensive model of physics than classical mechanics, quantum computing is a more comprehensive model of computing and has a greater potential to address issues that classical computing cannot address. They use their quantum bits, also known as "Qubits," to store and manipulate the information, in contrast to traditional classical computers, which are based on conventional computing and utilize binary bits 0 and 1 separately. Quantum Computers are the term for the computers that use this kind of computing.

Problem Definition

The future of quantum computing and its uses. Developing computer-based technologies based on the concepts of quantum theory is the focus of the field of study known as quantum computing. The quantum (atomic and subatomic) level of energy and matter is where quantum theory describes the nature and behavior of these two entities.

Motivation, Objective, and Social Relevance

One of the top scientific theories explaining the laws that govern the universe is quantum mechanics. The transistor and the laser were both developed as a result of their discovery, which was one of the most significant revolutions in human history.

Quantum computing is a field of computational science that processes, stores, and manipulates massive amounts of data and performs calculations that are too complex for conventional computing systems and supercomputers to handle. It makes use of the quantum mechanics concepts of entanglement, superposition, and interference.

The next phase in data processing will be quantum computers. They will be able to find solutions to issues that are currently intractable and make significant advancements in a variety of sectors of inquiry. It's possible that in the future, medical applications will utilize quantum computers.

Planned Outcome

Within the next five to 10 years, quantum computing may become a reality. Quantum computers were one step closer to becoming a reality in 2020, and in 2021, research and development will bring quantum computers one step closer to becoming a reality. Researchers and companies are presently competing to build quantum computing as rapidly as feasible. However, there is a race between quantum algorithms and the cryptography used by your company, and you have no time to waste.

To create remedies for post-quantum cryptography, DigiCert is constantly working with professionals in the field. For instance, we provide a post-quantum cryptography maturity model to help you better understand how PQC is handled and how your organization may prepare for it as well as a post-quantum cryptography (QPC) toolbox that enables you to test digital certificates against quantum algorithms.

Literature Survey of Topic

Numerous new fields of scientific and technological inquiry and development have been made possible by the advent of quantum physics.

One such area is quantum computing and communication, where a door to a locked room that previously held a dream has been closed. This article provides a concise overview of the state of the industry and highlights the numerous opportunities in information processing systems, notably in Big Data Analytics. We discuss quantum computing and communication in this essay. The demand for quick processing speed and miniaturization is increasing, and traditional computers are unable to keep up with the demand for these two essential qualities. Classical computers' proliferation is at its peak as they deal with classical mechanics. Due to these restrictions, quantum mechanics is becoming a game-changer in the quest for computational power.

Getting any kind of insight from a massive amount of data is a very difficult task at hand. The term "big data" refers to data that is larger than the storage and processing capacities of a traditional computer.

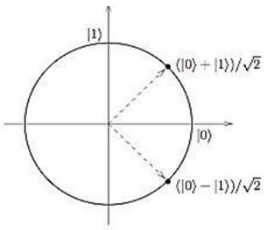
The solution is provided by quantum computing, which offers to analyze the literature on big data analytics utilizing quantum computing for machine learning and its state-of-the-art. This study focuses on a survey in the fascinating area of quantum computing. A brief history of quantum mechanics is highlighted in the paper's first paragraph. Next, a physics viewpoint on key components of quantum computing is presented, including quantum superposition, quantum tunneling, and qubits. Also looked at are different quantum physics techniques and applications.

Discussion of Base paper

Like a PC or a smartphone, a functioning quantum computer is probably not something that can be had at home. Although IBM has constructed a working quantum computer and one can utilize IBM's quantum computer via its website, many research papers on quantum computers have been published over the years, but the majority of them remain theoretical. The reason why these quantum computers are taking so long to develop is that they are extremely susceptible to interference. Quantum computers must be kept insulated from all types of electrical interference and chilled to nearly absolute zero since almost anything can cause a qubit to lose its delicate condition of superposition.

Algorithm

It should come as no surprise that a quantum computer can emulate this kind of computing by employing another well-known quantum gate, the Hadamard gate, which takes the state 0 as an input and outputs the state (0 + 1)/2. This output state's measurement returns a 50/50 chance of 0 or 1, which can be used to imitate a fair coin flip.

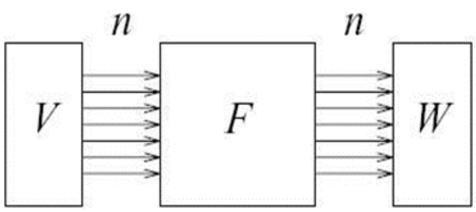

$|1\rangle$
$(|0\rangle + |1\rangle)/\sqrt{2}$
$|0\rangle$
$(|0\rangle - |1\rangle)/\sqrt{2}$

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

(1) (2)

Fig. 1 - (a) graph; (b) formula.

This is how a quantum computer appears; it accepts n input qubits, the register V, and generates n output qubits, the register W:



(a)

Fig. 2 – (a) quantum computer presentation.

The input register can be set up as a superposition of states, such as a superposition of n equal integers ranging from 0 to 2:

$$V = \sum_{i}^{2^n} 1/\sqrt{2}\,(\,|0_i> + \,|1_i>)$$

(b)

Fig. 3 – (b) Superposition Formula.

n

After that, the computer does a parallel calculation of the function applied to both integers concurrently. When we measure W, according to the QMP (Quantum Measurement Postulate), each bit of the output register will be set to a Boolean depending on the entangled wave function of the output qubits. Design F to maximize the likelihood that the output we measure corresponds to the desired solution.

Get Boolean values for all the qubits in W by measuring the output, which collapses the wave function. One of the outputs that could occur is the outcome.

Think of F as (integer) W's square root divided by V. Then, after running the computer and measuring n W, prepare V as the n superposition of all integers from 0 to 2.

The outcome will be the square root of an integer between 0 and 2. with equal likelihood, the square root of any such number. QMP claims that we can only learn about one of the square roots of each number while F performs this task in parallel. To get the desired output from F in real-world situations, organize F so that the probability amplitudes of the output state strongly favor it.

Since a quantum computer operates on a probabilistic model, we might have to run it several times before we receive the desired result.

Summary

A sizable number of quantum algorithms have been described, each of which addresses a sizable number of issues. Still, one can wonder why more algorithms, and in particular, more exponential speedups, are not well recognized.

One explanation is that under the query complexity model, where the only variable taken into account for determining difficulty is the number of queries to the input, substantially lower constraints on the capacity of quantum computation have been established. For instance, Grover's algorithm's level of complexity cannot be increased by even one query while keeping the same success probability. In the query complexity model, there must be a guarantee on the input, or else some potential inputs must be forbidden, to achieve an exponential speedup over classical computation. There are latent issue structures that quantum computers can take advantage of in a way that classical computers cannot, and this is one explanation for the effectiveness of quantum algorithms in cryptography. Another significant outstanding topic is locating similar hidden structures in other practical problems.

Illustrations

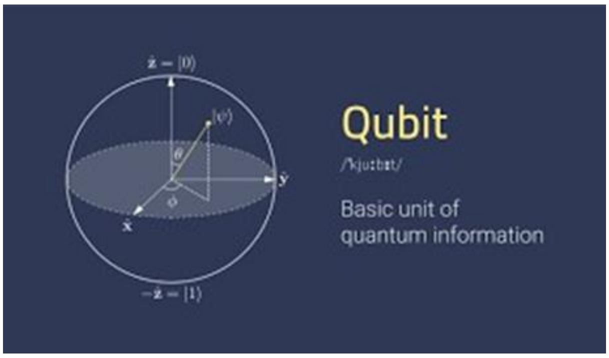


Fig. 1 - (a) Qubit diagram and meaning

References

a. Information is Inevitably Physical by (I. R. Landauer), published in (Anthony J. G. Hey)'s edited volume "Feynman and Computation" (Addison Wesley Longman, Reading, MA, 1998).

b. (J.A. Wheeler), "Information, Physics, and Quantum: The Search for Links," reproduced in "Feynman and computation," ibid. ; first published in Proceedings of the Third International Symposium on Foundations of Quantum Mechanics, Tokyo, p. 354 (1989).

c. In the 50th Annual Symposium on Foundations of Computer Science Proceedings, (Reichardt, B). (Atlanta, GA, USA, 2009), p. 544-551.

d. In Proceedings of 29th Annual IEEE Conference on Computational Complexity, 22–31 (Vancouver, Canada, 2014), (Belovs.A.) Quantum algorithms for learning symmetric juntas via adversarial bound.

e. (Rieffel, Eleanor and Polak, Wolfgang 2011) Quantum computing: A gentle introduction Cambridge, ma: Mit press. Print.

f. (Kaye, Phillip, Laflamme, Raymond and more), (Michele) (2007) an introduction to quantum computing new york, NY: oxford university press. Print.

g. (Mermin, n. David, 2007) Quantum computer science. An introduction to new york, NY: Cambridge university press. Print.

h. Shor's discrete logarithm quantum method for elliptic curves by (Proos and Zalka) Quantum Inform. Comp. 3, 317-344 (2003).