Quantum Computing

Mohammad Makki

Beirut Arab University

Email: makki.51x3@gmail.com

***Abstract -*The study seeks to explore quantum computing. However, this initial report provides the history of quantum computing since the inception of the concept in 1982 by Richard Feynman. It covers a brief review of the development of the first quantum physical system, the theory of quantum computation, and the first quantum model for computation that describes what would be a universal quantum computer. It also covers the historical timelines in which the universal quantum Turing machine with polynomial efficiency was constructed, the introduction of quantum algorithms, and quantum error correction schemes. Finally, the report provides the topical issues under quantum computing that are expected under the full essay paper.**

***Keywords***

***Polynomial slowdown, Quantum physics, Quantum computing, classical computing, quantum computer, universal quantum computer, quantum mechanics, qubit or quantum bit, quantum system, quantum state, superposition, entanglement, quantum information, quantum computation, quantum algorithm, superconducting, probability, and probabilistic, quantum error correction, quantum cryptography, teleportation.***

**Introduction**

Historically, the theory of quantum computation was initially proposed around the beginning of the 1980s [1]. First, scientist Richard Feynman claimed that a quantum physical system with R particles could not be properly simulated using merely a polynomial slowdown. The major explanation for the absence of simulation, according to the reasoning, is that the description size of a particle system is linear in R in classical physics but exponential in R in quantum physics [1]. Furthermore, Feynman proposed that this slowdown could be avoided by utilizing a computer that operated according to quantum physics laws because a quantum computer could work exponentially quicker than a deterministic classical computer. The theory of quantum computation was then developed by Deutsch, who introduced a fully quantum model for computation and described a universal quantum computer [7]. Bernstein and Vazirani expanded on this approach by building a universal quantum Turing machine with polynomial efficiency. Later, Peter Shor boosted this breakthrough by developing quantum algorithms for factoring integers and extracting discrete logarithms in polynomial time [5]. Shor also demonstrated the creation of quantum error correction (QEC) schemes, which are used to rectify errors in quantum computers [2]. This lay the groundwork for large-scale quantum computers.

The theory of quantum information and computing has provided new insights into the use of quantum states to allow secure transmission of classical information (quantum cryptography), the use of quantum entanglement to allow reliable transmission of quantum states (teleportation), and the possibility of maintaining quantum coherence in the presence of irreversible noise processes (quantum error correlation), the use of controlled quantum evolution for efficient computation (quantum computation) [3]. These findings also show that a Quantum Computer can more efficiently compute a narrow set of functions. However, even though the principles of quantum information physics may be tested on smaller devices, building a universal quantum computer is not feasible with current technology [2].

This paper will cover Shannon's theorem, error-correcting codes, Turing machines, and computational complexity as an introduction to classical information theory and quantum computation. The distinction between quantum and classical information theory and classical physics will also be explored. The essay will also discuss and outline quantum physics concepts, the Einstein, Podolsky, and Rosen (EPR) experiment, EPR-Bell correlations, and quantum entanglement in general [4]. The essay will then go into concepts like qubits and data compression [6], quantum gates [8], the no-cloning feature, and teleportation, as well as quantum cryptography and the universal quantum computer (QC), which is based on the Church-Turing principle and a network model of computation [4].

**Shannon's Theorem**

The noisy-channel coding theorem, also known as Shannon's theorem in information theory, establishes an upper bound to the capacity of a link, in bits per second (bps), as a function of the available bandwidth and the signal-to-noise ratio of the link. Its formula is as follows:

**C = B \* log2(1+ S/N)**

C represents the achievable channel capacity, B represents the bandwidth, S represents the average signal power and N represents the average noise power. The signal to noise ratio (S/N) is usually in decibels (dB) [9].

**Quantum Shannon theory**

Named after Claude Shannon, the founder of classical information theory, Quantum Shannon theory involves the study of the upmost capability of noisy physical systems that are governed by the laws of quantum mechanics, to preserve information and correlations. It refers to the asymptotic theory of quantum information. He was able to proof mathematically that, by keeping the transmission rate within the channel's bandwidth, aided by error-correction, even in a noisy channel with relatively low bandwidth, error-free communication could be achieved. One way to correct errors that occur during quantum operations is known as the surface code, its robust and suited to being set out on a two-dimensional plane. This method utilizes the quantum phenomenon known as entanglement to enable single qubits to share information with other qubits on a lattice layout. Hence, once qubits are measured, they reveal errors in neighboring ones[10].

**Turing machine**

A Turing machine is an abstract mathematical model for all machines, like state machines or automata. It is made up of three main parts: tape, head and state register. All a Turing machine does is read, write, and erase a symbol, using the head, from the tape. move left or right, while updating the state register which holds the current state the machine is in. It’s a theoretical description of computers used to prove properties of computable things in general and discover the limits of algorithms [11].

**Computational complexity**

Computational complexity theory is the classification of computational problems according to their inherent difficulty and relating those classes to each other. It does so by quantifying the number of resources needed to solve them. For example, if the problem requires significant resources to get it solved, it lacks in performance and is considered as difficult.

Diagram, venn diagram

Description automatically generated

Figure 1 Quantum complexity theory [12]

From figure 1, The complexity class of decision problems that can be solved: on a deterministic Turing machine in polynomial time and is known to be efficiently solved by classical computers is P; on a non-deterministic Turing machine in polynomial time is NP; with 2-sided error on a quantum Turing machine in polynomial time and is known to be efficiently solved by quantum computers is BQP short for “bounded error quantum polynomial time”. Any problem that is NP-Hard would still be hard for a quantum computer. The BQP class includes all the P problems such as match making factoring and graph connectivity. In addition to a few other NP problems such as factoring and the discrete logarithm. a quantum computer would still require more than a polynomial number of steps to solve NP problems. But it is believed that it could solve certain problems much faster than a classical one [13].

**Quantum physics concepts**

Fundamental concepts of the quantum theory include indeterminism, interference, uncertainty, superposition, and entanglement.

In classical theory governed by Newtonian laws we can predict the trajectories of all objects involved in an interaction if the initial positions and velocities of all the objects are known. However, in quantum theory that is governed by quantum mechanics, that is not the case, due to its indeterministic feature and the lack of information about the positions and velocities of every object in any physical system, we can only make predictions about probabilities of the events.

Another feature in quantum physics is Interference. As known in classical theory, wave interference is a phenomenon in which two input waves superpose to form an output wave of either greater, lower, or the same amplitude depending on whether it is constructive or destructive. The unique aspect of interference in quantum theory is that even a single “particle” such as an atom can exhibit wave-like features, as demonstrated in the double slit experiment where light and matter can display characteristics of both classically defined waves and particles, this implies wave-particle duality to every fundamental component of matter.

Uncertainty in quantum physics differs from uncertainty in classical physics. In quantum theory, it occurs for a single particle that has two complementary variables momentum and position. The uncertainty principle states that it is impossible to know both the particle’s position and momentum to arbitrary accuracy. hence, we can only know a particle’s position after precisely measuring it. But we lose all information about the position of the particle after learning about its momentum.

Superposition is a result of the linearity of quantum theory it states that a quantum particle can be in a superposed state of any other allowable states at the same time. This means that a particle can be in one location and another at the same instant in time. Decoherence can occur when a particle interacts with its environment. As a result, quantum superposition states may be altered during the process causing information stored by the quantum computer to be lost.

Entanglement refers to the strong quantum correlations that two or more quantum particles can possess. Technically these correlations are stronger than classical theory. Entanglement occurs when a pair of particles interact physically. Take for example the photons coming out of a laser beam fired through a crystal. The photons are split into pairs of entangled photons. These photons can later be separated by any large distance, hundreds of kilometers or more and still be entangled.

The non-classical correlation of entanglement plays a major part in many protocols of quantum information science. One such a protocol is teleportation that disembodies a quantum state in one location and reproduces it in another.

In 1935 a famous thought experiment proposed by Einstein, Podolsky, and Rosen known as the EPR experiment, presented a paradox involving entanglement that raised concerns over the completeness of the quantum theory. The paradox suggests that quantum particles traveled at a speed faster than light, this was direct violation for the theory of general relativity. They suggested that there might be a secret variable that could explain the results of the experiments. This paradox was later resolved in 1964 by John Bell. He presented a simple inequality known as Bell’s inequality. The inequality proofs that any two-particle with classical correlations that satisfy the assumptions of the EPR experiment must be less than a certain amount and that the correlations of the two entangled quantum particles violates this inequality. Hence, it was decided that entanglement cannot be explained in terms of classical correlations. After many years of experiments. Scientists, in 1981, verified that two entangled quantum particles violated Bell’s inequality[12].

**Data Representation on a Quantum Computer**

Unlike classical computers, quantum computers are based on the unique principles of quantum mechanics such as entanglement and superposition. In a quantum computer a qubit or a quantum bit, could be both 0 and 1 at the same time. So, for four qubits of data, a quantum computer can store all sixteen combinations of 0 and 1 simultaneously. That means a four-qubit quantum computer could calculate sixteen times faster than a four-bit classical computer. This implies that a quantum computer can be exponentially faster than a classical one. A physical implementation of a qubit can use the energy levels of an atom to represent data. Such that an excited state of the atom represents 1 and a ground state represents 0 [12].

**Universal Quantum Computer**

For a quantum computer to handle complicated tasks, error-correction codes need to be able to perform quantum gate operations. Quantum gates mostly operate on vector spaces of one or two qubits. The implementation of quantum logic gates usually introduces errors, and the quantum states fidelities decrease over time. In classical computing universal gates include NAND and NOR gates. While in quantum computers, Physicists describe two types of universal quantum gate operations. One of them is the Clifford gate set that needs to be combined with a purification protocol which uses multiple noisy quantum states to perform non-Clifford gate operations. Without the use of this purification protocol quantum computers would lack in functionality. However, the combination of Clifford and non-Clifford gates require so much of the computer’s resources and barely leaves any to deal with the target problem[12].

Table

Description automatically generated

Figure list of common quantum logic gates, circuit form and unitary matrices.

**Quantum Cryptography**

With the rise of quantum computers and quantum supremacy has been achieved. The integrity of encrypted data is at risk. Thus, quantum cryptography that is based on the complex principles of quantum mechanics is needed to build unbreakable encryption. quantum key distribution (QKD), uses a series of photons to transmit data from one location to another over a fiber optic cable. By comparing measurements of the properties of a fraction of these photons, the two endpoints can determine the secure key and whether it is safe for usage or not. The process starts when a sender transmits photons through a filter which randomly gives one of the following polarizations: Vertical, Horizontal, 45 degrees right, or 45 degrees left and bit designations of 1 for both vertical and 45 degrees right and zero for both horizontal and 45 degrees left. Next, the photons reach a receiver that uses two beam splitters, the splitters can be horizontal, vertical, or diagonal, to detect the polarization of each photon. The receiver does not know which beam splitter to use for each photon and must guess instead. After the stream of photons has been sent successfully, the receiver notifies the sender which beam splitter was used for each of the photons and the sender compares that information with the sequence of polarizers used to send the key. Finally, any photons that was misread are discarded, and the result is a sequence of bits that is the key. Note that if an eavesdropper tries to read or copy a photon it’s state will change. Hence, it will be detected by the sender/receiver [10].

**Conclusion**

Quantum computers have the potential to revolutionize computation as we know it making some types of previously intractable problems on classical computers solvable. Even though no quantum computer is subtle enough to carry out problems that a classical computer can't, hopefully great progress is under way leading the way to a new era of new technologies.

**REFERENCES**

[1] M. Hirvensalo, *Quantum computing: With 5 figures*. Berlin etc.!: Springer, 2001.

[2] J. Preskill, “Quantum Computing in the NISQ era and beyond,” *The open journal for quantum science*, vol. 2, pp. 79–79, Aug. 2018.

[3] R. Steane, IOP Publishing Ltd, rep., 1998.

[4] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, “Quantum entanglement,” *Reviews of Modern Physics*, vol. 81, no. 2, pp. 865–942, 2009.

[5] C. P. Williams, *Explorations in quantum computing*. Springer London, 2011.

[6] S.-S. Li, G.-L. Long, F.-S. Bai, S.-L. Feng, and H.-Z. Zheng, “Quantum computing,” *PNAS*, 09-Oct-2001. [Online]. Available: https://www.pnas.org/content/98/21/11847.short. [Accessed: 12-Sep-2021].

[7]T. Hey, “Quantum (Davie 1996) computing: an introduction,” *Computing & Control Engineering Journal*, vol. 10, no. 3, pp. 105–112, 1999.

[8] E. Knill, “Quantum computing with Realistically noisy devices,” *Nature News*. [Online]. Available: https://www.nature.com/articles/nature03350. [Accessed: 12-Sep-2021].

[9]

Davie, L L Peterson and B S. 1996. "Computer Networks:a systems approach (Morgan Kaufmann)." 94-95.

[10] Boyd, John. 2020. Novel Error Correction Code Opens a New Approach to Universal Quantum Computing. June 3. Accessed 11 26, 2021. https://spectrum.ieee.org/novel-error-correction-code-opens-a-new-approach-to-universal-quantum-computing.

[11] Benčević, Marin. 2019. What’s a Turing Machine? (And Why Does It Matter?). April 1. Accessed 11 25, 2021. https://medium.com/background-thread/whats-a-turing-machine-and-why-does-it-matter-1cd1b4606c6a.

[12] Wilde, Mark M. 2019. From Classical to Quantum Shannon. Baton Rouge, Louisiana 70803, USA: Hearne Institute for Theoretical Physics.

[13] Scott Aaronson. 6.845 Quantum Complexity Theory. Fall 2010. Massachusetts Institute of Technology: MIT OpenCourseWare, https://ocw.mit.edu. License: Creative Commons BY-NC-SA.