JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Quantum Computing

The Future of Computing

FAISAL HASSAN
ASIF MUSHTAQ
WAQIB AHMAD
SYED IRFAN YAQOOB – ASSISTANT PROFESSOR, DEPARTMENT OF CSE
SSM COLLEGE OF ENGINEERING

Abstract

Quantum theory is one of the most successful theories that have influenced the course of scientific progress during the twentieth century. It has presented a new line of scientific thought, predicted entirely inconceivable situations and influenced several domains of modern technologies. There are many different ways for expressing laws of science in general and laws of physics in particular. Similar to physical laws of nature, information can also be expressed in different ways. The fact that information can be expressed in different ways without losing its essential nature, leads for the possibility of the automatic manipulation of information.

Quantum computing is a study area that focuses on developing computers based on the properties of "quantum theory" & "quantum physics". Quantum theory defines the behavior & nature of energy and matter on the "atomic" and "subatomic" levels also known as the quantum levels. A quantum computer is a computational device that utilizes the phenomena of quantum mechanics with its quantum properties to structure & process data. A large-scale quantum computer is capable of performing operations in exponentially enormous speed compared to a classical computer. Development of such computers is considered a massive leap for mankind in computing abilities with huge performance gains for simulations or brute force for example.

All ways of expressing information use physical system, spoken words are conveyed by air pressure fluctuations: "No information without physical representation".

Quantum computers are not meant to replace typical computers. In practice, they will be separate instruments used to solve complex, data-heavy problems, particularly those that make use of machine learning, where the system can make predictions and improve over time.

Keywords: computation, EPR, quantum mechanics, superposition, unitary transformation, decoherence.

INTRODUCTION

With the development of science and technology, leading to the advancement of civilization, new ways were discovered exploiting various physical resources such as materials, forces and energies. The history of computer development represents the culmination of years of technological advancements beginning with the early ideas of Charles Babbage and eventual creation of the first computer by German engineer Konard Zeise in 1941. The whole process involved a sequence of changes from one type of physical realization to another from gears to relays to valves to transistors to integrated circuits to chip and so on. Surprisingly however, the high-speed modern computer is fundamentally no different from its gargantuan 30-ton ancestors which were equipped with some 18000 vacuum tubes and 500 miles of wiring. Although computers have become more compact and considerably faster in performing their task, the task remains the same: to manipulate and interpret an encoding of binary bits into a useful computational result.

The number of atoms needed to represent a bit of memory has been decreasing exponentially since 1950. An observation by Gordon Moore in 1965 laid the foundations for what came to be known as “Moore’s Law” – that computer processing power doubles every eighteen months. If Moore’s Law is extrapolated naively to the future, it is learnt that sooner or later, each bit of information should be encoded by a physical system of subatomic size. As a matter of fact, this point is substantiated by the survey made by Keyes in 1988 as shown in fig. 1. This plot shows the number of electrons required to store a single bit of information. An extrapolation of the plot suggests that we might be within the reach of atomic scale computations within a decade or so at the atomic scale

however.

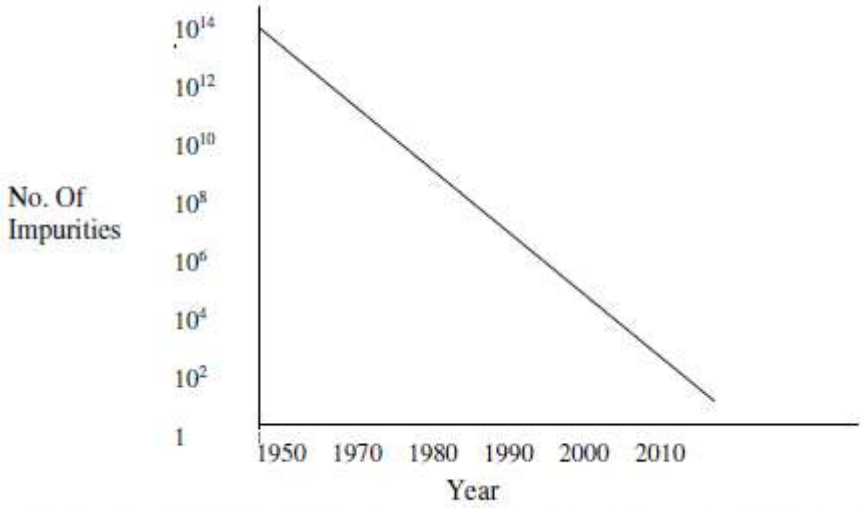

Fig 1: Showing number of dopant impurities in logic in bipolar transistors with year.

Matter obeys the rules of quantum mechanics, which are quite different from the classical rules that determine the properties of conventional logic gates. So if computers are to become smaller in future, new, quantum technology must replace or supplement what we have now. Notwithstanding, the quantum technology can offer much more than just cramming more and more bits to silicon and multiplying the clock speed of microprocessors. It can support entirely a new kind of computation with quantitatively as well as qualitatively new algorithms based on the principles of quantum mechanics. With the size of components in classical computers shrinking to where the behavior of the components, is practically dominated by quantum theory than classical theory, researchers have begun investigating the potential of these quantum behaviors for computation. Surprisingly it seems that a computer whose components are all to function in a quantum way are more powerful than any classical computer can be. It is the physical limitations of the classical computer and the possibilities for the quantum computer to perform certain useful tasks more rapidly than any classical computer, which drive the study of quantum computing.

A computer whose memory is exponentially larger than its apparent physical size, a computer that can manipulate an exponential set of inputs simultaneously – a whole new concept in parallelism; a computer that computes in the twilight (space like) zone of Hilbert Space (or possibly a higher space – Grassman Space & so on), is a quantum computer. Relatively few and simple concepts from quantum mechanics are needed to make quantum computers a possibility. The subtlety has been in learning to manipulate these concepts. If such a computer is inevitability or will it be too difficult to build on, is a million dollars question.

BACKGROUND

The concept of electronic components reaching microscopic scale was noted by physicist Richard Feynman in 1959. This concept set a base for the concept of scaling down components and thus predict quantum computing, but it wasn't until 1985 until the British physicist in the University of Oxford "David Deutsch" portrayed the building of quantum logic gates for a "universal quantum computer". In 1994, American

mathematician “Peter Shor” developed the Shor algorithm that factors numbers in a quantum computer and requires only 6-qubits. Yet, it was not until 1998 till Isaac Chuang of “Los Almost National Laboratory”, Neil Gershenfeld of “MIT” & Mark Kubinec “University of California Berkley” built the first 2- qubit quantum computer that can perform basic functions. In 2000, “Emanuel Knill”, “Raymond Laflamme” & “Rudy Martinez” of “Los Alamos” & “Ching-Hua Tseng” of “MIT” created a 7-qubit quantum computer using “trans-crotonic acid”. Theories & algorithms kept rolling in since the early 2000s. In 2019, Google released their quantum computer “Sycamore” and it was upgraded in 2020 to 54-qubit as Google claims. In September 2020, IBM claimed supremacy with its 53-qubit quantum computer. In October 2020, Google claimed supremacy with its 54-qubit system after managing to solve an operation considered computationally impossible to solve with a normal computer

Qubits

Qubits represent atoms, ions, photons, or electrons & a qubit is regarded as the “basic unit of information” for quantum computers. It is the “quantum equivalent” of a classical bit in classical computers, information is encoded in bits that have either 1 or 0 as a value. Thus, a bit can only be in one of the either states, ON or OFF (1 or 0). However, this is not the case for qubits as qubits are not limited to being in one state and can exist in superposition. Thus, a qubit can exist in 0, 1 or a linear combination of both states.

As computers break down information into bits, a quantum computer wouldn’t use a classical switch circuits with each switch denoting ON or OFF; instead, a quantum physical system relies on the fact that qubits can exist in ON & OFF simultaneously although this might go against our understanding of everyday physics. The powerful computational power of a quantum computer can only be attained if qubits undergo “entanglement”, which is the process of entangling qubits into groups (quantum registers) creating an extremely potent information-processing hardware. For the sake of comparison, a 30-qubit quantum computer has the processing power of 10 teraflops (trillions of floating-point operations per second) of a conventional computer. A typical desktop computer runs at gigaflop speed (billions of floating-point operations per second)

DESIGN CONSTRAINTS

Entanglement Constraint: Since the exponential computational power of quantum computers denoted by the exponential increase of coefficients after adding an additional qubit is attained only by entangling all the qubits in the system, adding any additional qubit without undergoing entanglement adds nothing in terms of computational power. In fact, adding a qubit without entanglement would have the effect of 2N + 2 rather than 2N+1 which translates to 2 N * 2. Thus, not implementing correct entanglement leads to loss of desired computational power. To achieve entanglement between two qubits, there should interact

directly or indirectly via a midway "quantum system" whether a "photon" or "qubit" that relates to each of the qubits to achieve entanglement.

Copying Constraint: The "no-cloning theorem" in quantum computers means that it's impossible to make an identical copy of an unknown state in a quantum system thus implying that one can't make a copy of another quantum system. Although one can move a set of qubits from a system to another, this implies the literal meaning of moving & not copying because this has the effect of deleting the data from the original qubits. Such issue changes our whole approach to the design of quantum algorithms that must definitely differ from the design of classical computing algorithms.

Lack of Noise Immunity: As there are no "basic gate operations" like classical logical gates in classical computers to remove imperfections & noise from the "input signals" or "gate operations", such imperfections will accumulate over time and unsettle the state of the quantum system. Such imbalance lead to less accurate calculation results, measurement errors in large calculations, or even loss of coherence thus eliminating any quantum advantage over classical computers. Some of the noise sources may be wrongly isolated environment, unfixed changes in the physical preparation or even the manufacturing of the qubits themselves.

APPLICATIONS

Cryptography: A quantum computer is able to solve the computationally infeasible functions of "integer factorization & discrete logarithm" using Shor's Algorithm. If quantum computers managed to overcome the "quantum noise" & "quantum incoherence" phenomena, then "Shor's Algorithms" can be utilized to break schemes like "public-key cryptography" used especially in RSA encryption. Quantum computers can also create quantum-based cryptographic systems that can face quantum hacking.

Quantum Search: Quantum algorithms offer "polynomial speedup" over the best-known classical algorithm for various problems especially the "quantum database search" that can be tackled using "Grover's Algorithm" that uses "quadratically" less queries to search in a database compared to a classical computer thus proving to be "optimal" rather than strictly a proof of concept.

Quantum Simulation: Nanotechnology and chemistry scientists are highly anticipating the use of quantum simulations to simulate complex experiments that are impossible on a classical computer. One of the experiments/ simulations is studying the behavior of atoms at uncommon environments like a "collider"

Double-Slit Experiment: With quantum computers, we might be able to predict the paths of particles & protons and solve the mystery once and for all. Solve Linear Equations: Quantum algorithms used for linear equations demonstrate speed superiority over their classical counterparts especially the “HHL Algorithm”. Such speedup is mostly noticed in the field of “Quantum Machine Learning”

Quantum Supremacy: Quantum supremacy refers to the “hypothetical speedup advantage” of quantum computers over classical computers in certain fields. Although some experts like “Gil Kalai” believe that quantum supremacy is unachievable, Google has already announced supremacy with its “Sycamore” CPU performing over 3 million times faster than the fastest supercomputer “Summit”

HARDWARE COMPONENTS

Since quantum computers serve for a specific computational purpose rather than being a user-friendly computer in terms of interface, quantum computers can in fact utilize conventional computers to serve as an interface and perform tasks that can better be employed on a classical computer. In addition, controlling the qubits can be done on a classical computer thus efficiently dedicating the quantum computer for a very specific purpose. The components that constitute a quantum computer are:

• **Quantum Data Plane** This plane is considered the heart of the quantum computer & it holds the physical qubits and structures used to set everything in place. It may also contain circuits that measure the state of qubits and perform gate operations.

• **Control & Measurement Plane** This plane transforms the “digital signals” from the “control’s processor” to “analog control signals” required for operations on qubits in the data plane. And vice versa, it transforms the analog signals from the qubits measurement to binary data that can be handled by the “control processor”. Such analog to binary conversion can be hard to handle as minor control signal errors or faulty qubits design would undoubtedly affect calculation results. The nature of the control signals varies depending on the qubit technology used. For instance, “microwave” or “optical signals” are used for “trapped ion qubits” whereas “microwave “and “low-frequency electrical signals” are used for “superconducting qubit” systems and are delivered through wires running into a cooling mechanism to tackle overheating

• **Control Processor Plane & Host Processor** The control processor plane recognizes and stimulates the correct sequence of quantum gate operations and measurements. Such sequence is provided by the host processor and is responsible for executing the program for implementing a quantum algorithm. A major task for the control processor plane is correcting errors through a “quantum error correction” algorithm if the quantum computer supports error correction. Regarding design, creating a “control processor plane”

for big quantum computers is a tough task, and an active research area. The most famous approach is splitting the plane into two sections. The first is a “conventional processor” that operates & manages the “quantum program”. The second is a “scalable hardware block” that acts as an interface with the “measurement plane” and combine the main controller instructions with the measurements to calculate the following processes to be operated on the qubits. The host processor is a conventional computer that uses a conventional operating system and utilizes libraries to operate. It runs development tools and software to create programs for the control processor (quantum machine). It also provides storage and networking services in case quantum computers needed to store or communicate online while running. We therefore use conventional computers with quantum computers to cut the hassle of building features from scratch and reinventing the wheel for quantum computers.

• **Qubit Technologies** The two most developed “qubit technologies” are “superconducting & trapped ion qubits”. The current challenge for quantum scientists is scaling up such small systems to huge processors

CONCLUSIONS AND FUTURE SCOPE

The very first quantum logic gate presented in 1995 used “trapped atomic ions” through a research proposal. Advanced in that field later enabled quantum scientists to create the very first small quantum processor to implement basic quantum algorithms in limited conditions. For future development, building a quantum computer based on trapped atomic ions would require integrating several technologies like microwave, radio frequency, optical systems, laser, vacuum & coherent electronic controllers. Any advancement through this field would require a solution for the integration challenges. Our latest quantum computers based on trapped ions are small-scale systems of 5-20 qubits able to run programmable quantum logic operations. However, we must tackle the 2-5% error margin for each 2-qubit gates in order to scale up those system to become practically usable. It is expected in the early 2020s to implement small-scale 20-100 bits quantum computers based on ion traps. Such system is expected to consist of a single chain of ions and feature all-to-all connectivity among the qubits within the chain to efficiently implement any quantum circuit. Yet, there are several issues to address before we could call for a fully scalable, error-tolerant ion trap quantum computer especially issues with difficulty in isolating individual ions as the chain gets bigger and bigger, measuring individual qubits & increasing the number of ions that can be individually targeted using “gate laser beams” . To sum up, quantum computing is still a new field with a whole lot of research yet needed to achieve the long-anticipated quantum supremacy. Scientists have gone a long way theoretically, but they yet have to tackle practical obstacles that prevent us from building full-scale quantum computers that would change the world of computation, biology, physics, chemistry, mathematics & every other science that requires computation, machine learning, artificial intelligence,

image processing, cryptography… as implementing any of the operations on a quantum computer is a game changer for the operation's field. We also must design & analyse new quantum algorithms because our approach to the quantum computational field differs from that of the classical counterpart

RESULTS

Quantum computers have the potential to revolutionize computation by making certain types of classically intractable problems solvable. While no quantum computer is yet sophisticated enough to carry out calculations that a classical computer can't, great progress is under way.

REFERENCES

1. K.Brading, and E.Castellani (2003), Symmetries in Physics: Philosophical Reflections, Cambridge University Press, 2003.

2. Sanjeev Kumar (2002), Reformulation of Classical Electrodynamics, Jiwaji University, Gwalior, INDIA.

3. Michael Nielsen, and Isaac Chuang, Quantum Computation, Cambridge University Press.