TEST Engineering & Management

January - February 2020
ISSN: 0193 - 4120 Page No. 2882 - 2886

Quantum Computing: A Brief Introduction to the Emerging Technology and Its Engineering Paradigm

Sachin Aralikatti, Assistant Professor, Department of Electronics and Communication, CMRIT Banglore

Article Info
Volume 82
Page Number: 2882 - 2886
Publication Issue:
January-February 2020

Article History
Article Received*: 14 March 2019*
Revised*: 27 May 2019*
Accepted*: 16 October 2019*
Publication*: 18 January 2020*

Abstract:
Quantum computing is considered as good mixture of quantum physics, computer science and information theories. This paper introduces fundamentals needed to understand different layers associated with quantum computing some of them are superposition, entanglement, quantum gates and circuit models like Grover's algorithm, Shor's algorithm. Thereafter, it will elaborate hurdles encounter in constructing a quantum computer like Constructing, verification, architecture, quantum error correction, compiler and programming issues. Finally some of the applications like quantum cryptography is discussed.

Keywords:*Quantum Computing, physics, Superposition, entanglement, Grover's Algorithm*

I. INTRODUCTION

The evolution of quantum computing was initiated by Moore's law, which says that complexity of IC's doubles every 1.5 years. Quantum effects will play a vital role in modeling of tiny transistor by exploiting fundamental phenomenon of quantum physics like superposition and entanglement. The quantum computer has a ability to outperform in solving complex problems like factoring large number, computation of triangles in a graph, searching databases and simulating physical systems.

The major challenge here is precise valuation of the resource needed for expressing quantum based algorithms like execution of gates used and number of qubit required. The basic fundamental storage unit is quantum bit (Qubit). Qubit in more general sense is a two state variable zero and one, written as |0> and |1> respectively. It might be either logical qubit (Quantum variable encoded as a collection of physical qubit) or physical qubit (A true two-level system like, single photon polarization or spinning directions of electron). The only difference that make qubit different from bit is superposition of two known state.

The qubit in Bra – Ket Notation is expressed as | x >:

$$| x > = a | 0 > + b |1 > \quad \ldots\ldots\ldots\ldots (1)$$

In expression 1, a along with b are considered as complex quantity, |a|2 is square of amplitude "a" which express probability of observing the qubit in the state 0, |b|2 is square of amplitude "b" which express probability of observing the qubit in the state 1. The |a|2 + |b|2 = 1 implies the available qubit must be exist in any one of the state [1]. < ; || ; > is known as Bra-Ket symbol introduced by Dirac in quantum mechanics.

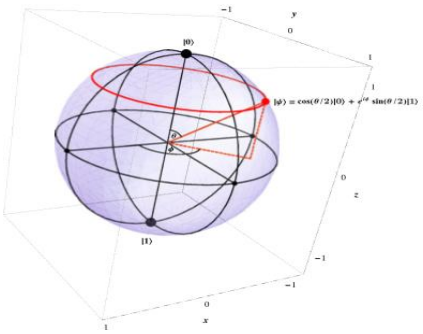

Fig.1 Bloch sphere picture of qubit

The Bloch sphere geometrically express the pure state available space for a two-level quantum system. A single qubit process is explained as rotation about 3-dimensional axes like x, y, z of Bloch sphere. In quantum computing n qubit will

TEST Engineering & Management

January - February 2020
ISSN: 0193 - 4120 Page No. 2882 - 2886

exist as superposition of all possible 2^n states, written as:

$|x> = a_0 |0....00> + a_1 |0....01> + ... a_{(2^n - 1)} |1....11>$ ...(2)

In expression (2) a_i corresponds to complex number and summation of $|a_i|^2 = 1$.An Depiction of 3- qubit state is

$| x > = 1/(2\sqrt{2}) \{(|000> + |001> + |010> + |011> + |100> + |101> + |110> + |111>)\}$ ……(3)

Another important concept to understand is entanglement which is a special evidence related to superposition of many qubits where the united qubit states is impossible to decompose as multiple of specific states. Central idea of n-qubit superposed states involve storing of 2^n various states and operate simultaneously on all of states at the single time which leads to exponential speed up .Suppose if we have told that Person X and Person Y qubits are given by

$1/2 |a_0 >|b_0 > +1/2 |a_0 > |b_1 > +1/\sqrt{2} |a_1 >|b_0 > + 0|a_1 > | b_1 >$...(4)

Then computation of the products of the outer along with inner probability will be there. The product of the outer terms will be zero. The product of the inner terms will not be equal to zero, the 2 qubits are said to be entangled. Normally both Alice and Bob will make measurements. Another approach is we can make use of the probability amplitudes to inform us what happens when both Alice and Bob compute their qubits. They will get 00 with probability 1/4, 01 having probability 1/4, 10 having probability 1/2, and 11 with probability 0. We observe that there is nothing strange happening. This is exactly the same calculation as observed in untangled case study. [1][2][3][4]

II. Quantum Gates (QG)

Quantum algorithms normally explained in terms of computational circuit which includes information qubits and quantum gates operating on them. All quantum gates obey unitary and reversible conditions.

Gate name	# Qubits	Circuit Symbol	Unitary Matrix	Description
Hadamard	1	H	$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$	Transforms a basis state into an even superposition of the two basis states.
T	1	T	$\begin{bmatrix}1 & 0\\ 0 & e^{i\pi/4}\end{bmatrix}$	Adds a relative phase shift of π/4 between contributing basis states. Sometimes called a π/8 gate, because diagonal elements can be written as $e^{-i\pi/8}$ and $e^{i\pi/8}$.
CNOT	2		$\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}$	Controlled-not; reversible analogue to classical XOR gate. The input connected to the solid dot is passed through to make the operation reversible.
Toffoli (CCNOT)	3		$\begin{bmatrix}1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&1&0&0&0&0&0\\0&0&0&1&0&0&0&0\\0&0&0&0&1&0&0&0\\0&0&0&0&0&1&0&0\\0&0&0&0&0&0&0&1\\0&0&0&0&0&0&1&0\end{bmatrix}$	Controlled-controlled-not; a three-qubit gate that switches the third bit for states where the first two bits are 1 (that is, switches |110⟩ to |111⟩ and vice versa).
Pauli-Z	1	Z	$\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$	Adds a relative phase shift of π between contributing basis states. Maps |0⟩ to itself and |1⟩ to −|1⟩. Sometimes called a "phase flip."
Z-Rotation	1	$R_z(\theta)$	$\begin{bmatrix}e^{-i\theta/2} & 0\\ 0 & e^{i\theta/2}\end{bmatrix}$	Adds a relative phase shift of (or rotates state vector about z-axis by) θ.
NOT	1		$\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$	Analogous to classical NOT gate; switches |0⟩ to |1⟩ and vice versa.

Fig 2. Quantum gates: Symbol, matrices and description [11]

III. Fault Tolerant Calculation and Quantum Error Correction (QEC) Technique:

Existing quantum technologies are subjected to error prone because qubit gets effected by decoherence (Loosing information due to interaction with surrounding environment). There are different ways in measuring decoherence, some of them are amplitude damping and phase damping. The quantum gates presently exhibit error rates around 10^{-2}, to run large scale quantum circuit this error rates should get reduced to 10^{-12} to 10^{-15}.The quantum information is secured by quantum error correction code (QECC) and looking after the errors. The entanglement will help in encoding data qubit and errors are identified by error syndrome measurement (ESM) and using ancilla bits. Once the error occurred is detected, it will be decoded by classical control electronic circuitry. Most commonly surface codes are used in error correction because of its simple structure which fits for most of the quantum technologies. Planar based and defect based surface codes are different ways of encoding single logical bit. By increasing the code distance

January - February 2020
ISSN: 0193 - 4120 Page No. 2882 - 2886

error rate can be reduced considerably and higher the distance more robust the system will be obtained. [7][6]

IV. System View of Quantum Computer

Fig 3. System View of quantum computer

The above mentioned diagram introduce the top level programming explanations of quantum algorithms for existing physical operation on available processor. At top level the known quantum algorithms like Grover's, Shor's algorithm will be formulated then compiler will convert those quantum algorithms into native instruction sets which will be easy to execute. The micro level design will give hardware based control logic circuit needed for running instruction.

The need of quantum computer simulators is useful for design and testing of available algorithms, it has become easy to check accuracy and predict behavior in original quantum computer in the presence quantum noise. The assembly level language helps in describing quantum circuits easier. The validation of physical qubit layout with protocols and examine hardware - software co design helps in improvement of software and hardware infrastructure. [5][8]

The above mentioned features are condensed into following points:

1. QASM is a expressive programming language which helps programmers to represent circuit in easy and straight way, including parallelism.

2. The programming interface helps to validate quantum circuit, algorithms.

3. The provision to use different quantum noise models

4. High performance providing quantum algorithm simulations.

V. Quantum Computer Simulator Design

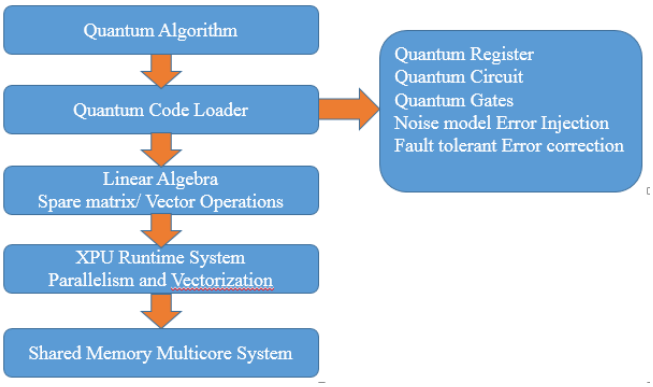

Fig 3. Quantum computer simulator design

Suppose if there is unavailability of large physical quantum computer, the high precision software simulation environment of quantum computers on a classical computers is much needed to perform simulation and execution of available quantum algorithms and to understand the behavior of a quantum computer and QX is one of the simulation platform to execute algorithm and to improve its design.[5]

The above mentioned figure represents the QX simulator architecture overview :

1. The Quantum Code Loader (QCL) takes given input codes and create equivalent circuit model. It also give provision to take execution variables such as error model and quantum gate scheduling scheme.

2. Main part of architecture includes the execution components like quantum gates, quantum circuits and qubit registers.

3. The error models helps in executing quantum circuits in noisy environment.

TEST Engineering & Management

January - February 2020
ISSN: 0193 - 4120 Page No. 2882 - 2886

4. Fault tolerant modules will produce fault tolerant circuit.

5. The linear algebra layer implements matrix/vector operation focusing on efficient usage of operators

6. Supports XPU parallel execution runtime at thread and instruction level.

Grover's search algorithm:

Grover's search algorithm outperforms operation quadratically sooner than known existing methods. Suppose there exist single answer like a deterministic brute force search takes total of ((2^n) −1) questions. The known classical method finds a answer with probability of 2/3, should make $\Omega(2^n)$ queries in extreme case. The Grover's algorithm will take only f ($\sqrt{(2^n)}$) = f($2^{(n/2)}$) queries [3].

Steps followed are:

1. Begin with available n-qubit state | 00...0 >.

2. Use n-qubit Hadamard gate (H) to ready the state 1 √N|ψ> = $\sum_{x=0}^{N-1}$ | x > $(where\ N\ = 2\hat{}n)$.

3. Make use of the Grover iterate (G) a overall of [π /4 1√N] times.

4. Then measure the final resulting state.

Shor's Algorithm used for prime factorization:

1. Let us consider number n = p*q be a multiple of two primes.

2. Let us consider x be a nontrivial square root of 1 mod n

3. $x^2 \equiv 1 \pmod n$, where x not equal to ±1 (mod n).

4. These conditions tell us that 1 < x < n−1 and $x^2 - 1 = (x + 1)(x-1) \equiv 0 \pmod n$.

5. Consider the greatest common divisors gcd(x + 1 , n) gcd(x−1 , n). At least one of these must be a nontrivial factor of n since 1 < x < n−1.

Shor's algorithm prime factorizes by finding such an x:

The algorithm follows

1. Select a random integer a < n. If GCD(a,n) not equal to 1, then we lost balance to a nontrivial factor of n.

2. Find the period "r" of the function $f(k) = a^k \pmod n$. In other words, we want a^r to be the identity, with $a^r \equiv 1 \pmod n$.

3. Notice that if r is even, we let $x = a^{(r/2)}$. And if x satisfies x not equal ±1 (mod n), then we can obtain nontrivial factors of n. [2]

VI. Quantum Cryptography

Here we will look into one of the application of quantum computing weather quantum cryptography will replace classical method. The first quantum cryptography we will study is known as BB84 protocol. There are 3 key ideas of BB84 QKD [9]:

1. No-cloning theorem which explains quantum states will not be stolen or reproduced. So that person X will not tap a quantum communications channels and quantum state to generate the copy of key for himself and send the true copy down the line to other person Y.
2. Any measurement makes to state to collapse. The main part of QKD is various base numbers can be utilized to generate a string of bit. When the measurements done for given base number the process will lead to state collapse. So the main conclusion is extractings little message/ information about the state will create disturbance in systems state.
3. Measurements are irreversible.[1][4]

VII. CONCLUSION

In this addresses the basic quantum gates used to build quantum algorithms (Grover's and Shor's). Later we have discussed major challenges involved to build quantum computers like significant memory,

January - February 2020
ISSN: 0193 - 4120 Page No. 2882 - 2886

designing of basic level languages to introduce quantum circuits and proper simulation environment like system tools with runtime support for routing. Finally the well-known quantum algorithms are discussed. Preparation of this article is motivated by the ability of quantum computers to solve intractable classical problems.

VIII. REFERENCES

[1] M.A Nielson and I.L Chuang, Quantum computation and quantum information. Cambridge university press, 2010.
[2] P.W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in SFCS, 1994
[3] L. K. Grover, "Quantum Mechanics helps in searching for a needle in a haystack," Physical review letters, vol. 79, no. 2, p, 325, 1997
[4] Phillip Kaye, "Introduction to Quantum Computing" -Oxford University Press, USA (2007)
[5] N. Khammassi, I. Ashraf, X. Fu, C.G. Almudever, K.Bertels, "QX: A High-Performance Quantum Computer Simulation Platform. 978-3-9815370-8-6, 2017 IEEE.
[6] Paul Issac Hagouel and Ioannis G Karafyllidis ," Quantum computers : Registers, Gates and Algorithms", Proc, 28th international Conference on Microelectronics, NIS SERBIA, 2012.
[7] Rodney Van Meter, " Counting Gates, Moving Qubits : Evaluating the Execution Cost of Quantum Circuits" , 2012 IEEE Computer society , 21st Asian Test Symposium.
[8] Anderson Avila, Renata H.S. Reiser, Adenauer C. Yamin, Mauricio L. Pilla, "Efficient In-Situ Quantum Computing Simulation of Shor's and Grover's Algorithms", 2017 29th International Symposium on Computer Architecture and High Performance Computing Workshops.
[9] Jiawei Han, Yanheng Liu, Xin Sun, Lijun Song, " Enhancing Data and Privacy Security in Mobile Cloud Computing through Quantum Cryptography", 978-1-4673-9904, 2016 IEEE.
[10]Enrico Prati, Davide Rotta, " From the quantum Moore's law toward silicon based Universal Quantum Computing" , 978-1-5386-1553-9 , 2017 IEEE.
[11]2 Quantum Computing: A New Paradigm Quantum Computing: Progress Prospects (2019). National Academic press.21ps03-vidmar