Comparisons of Conventional Computing and Quantum Computing Approaches

Qiyu Liu*

Department of Physics, University of California, San Diego, the U.S.

*Corresponding author: q4liu@ucsd.edu

Abstract. Quantum computers are capable of ultra fast computation in the fields where classical computers fail. Even though quantum computers are nowhere near commercialization, many researchers have developed quantum algorithms in fields such as modern encryption and molecular simulation, which, in theory, are exponentially faster than their classical counterparts. In this case, this paper will discuss the advantages of quantum computers over classical computers in those fields by examining and analyzing the various quantum algorithms. To be specific, the develop routine as well as detail examples will be exhibited to illustrate the differences and preferences. In addition, this study will also fully aware of the challenges that quantum computing researchers are facing. On this basis, possible limitations of quantum computers are also presented. The aim is to promote interest in quantum computing by introducing their supremacy in modern encryption and biological science. These results shed light on guiding further exploration of quantum computing algorithms.

Keywords: Quantum computers; conventional computing; algorithms.

1. Introduction

The 21st century has been a time characterized by modern computers. Almost every modern task that humans overtake involves using computers in one way or another. Classical computers have great power in areas like analyzing data, implementing classical algorithms, and simulating physical prediction. However, modern computers, or classical computers, fall short when it comes to handling algorithms and problems that scale exponentially. In addition, there are currently no efficient ways to simulate molecular interactions without making various compromises to simplify the molecular system on classical computers, due to its low computational power. These limitations challenge scientists and researchers to develop tools that address the problems that are too difficult to classical computing [1].

The concept of quantum computer was first introduced in 1981 by Richard Feymann in his lecture "Quantum Mechanical Computers". It would be a field that combines physics, computer science and mathematics to achieve inconceivable computational power that is exponentially faster than classical computers. After Feymann proposed the possibility and viability of quantum computing, scientists began to brainstorm the applications of quantum computing in various fields [2-4].

Researchers were eager to show the prospect of quantum computers when it comes to the future direction of computer science. They aimed to provide concrete proofs that quantum computing excels classical computing in certain areas, and this notion of overtaking classical computing is defined as quantum supremacy [5]. In 1994, Peter Shor proposed his groundbreaking shor's algorithm. The shor's algorithm dramatically speeds up the process of prime factorization of large numbers on which the RSA encryption system is based. In the past, Classical computers struggled on the RSA encryption because of their limitation on computational speed. Quantum computers, with their ability to solve RSA encryption, became a milestone for quantum computing history, since the RSA system is a common encryption technology and breaking it with quantum computers presents great potential of what quantum computers are capable of [6]. With these advances, scientists and professionals started to consider quantum computers as revolutionary devices that changed the way of modern cryptography.

This paper will deal with the comparison of classical computers and quantum computers in different fields of application. Specifically, this paper will look into the fields of molecular simulation

and modern cryptography to analyze the advantages of quantum computers over classical computers by looking at the quantum circuits and quantum algorithms. It will start on a brief description of quantum computing and the current progresses and challenges on constructing functional quantum computers.

2. Description of Quantum Computing

The concept of quantum mechanics was introduced by scientists back in the 1910s. It is the fundamental principle that governs the motion of tiny particles in the micro-realm. Quantum computing utilizes the principle of quantum mechanics to construct machines that are unique in every way from classical circuits. This section describes quantum computing by going over two of the most vital concepts in quantum computing from quantum mechanics: superposition and entanglement. In the 20th century, Richard Feymann introduced the idea of superposition in his paper. According to this paper, quantum particles behave differently than classical objects [7]. Instead of being fixed in one state, quantum particles can exist in different states simultaneously. This is also evident in Schrodinger's paper where he presented Schrodinger's equation [8]. The solution to Schrodinger's wave equation consisted of the linear combination of energy eigenstates. The electron exists in those different eigenstates with different probabilities. Measurements on the quantum system destroy the superposition and the system collapses into an eigenstate with probabilities embedded in the eigenvalues.

This principle is extended over to quantum computing. In classical computers, information is binarily encoded as a combination of 0 and 1. A classical bit, during its computational process, can only take the value of 0 and 1, implemented by switching on and off a transistor in most modern computers. Quantum qubits, on the other hand, have less limitations. Just like electrons can exist in superposition of eigenstates, qubits in quantum computers can also be in superposition. For instance, applying the hadamard gate to a simple one qubit quantum circuit results in (1/sqrt(2)(0 + 1)), a superposition of state in 0 and 1. Measuring this qubit yields a result of 1 50% of the time and 0 50% of the time. This unique phenomenon of Qubits grants tremendous flexibility during the computational process, allowing quantum computers to achieve fast computation that is impossible classically.

Another key concept in quantum computing is entanglement. Often in quantum mechanics, the quantum state of one particle cannot be accessed independently. A measurement on one quantum particle will simultaneously affect the measurement on another quantum particle, regardless of the distance between the two quantum entities. Quantum circuits utilize entanglement between Qubits and the probabilities associated with their superposition to enhance the probabilities of the result that one desires to achieve their fascinating speed when compared with classical computers.

3. Comparison

This section delves into the various areas of implication where quantum computers have advantages over classical computers. Presumably, it will provide a general understanding of what quantum computers excel and better views of why quantum computers are the future in many areas.

3.1. Shor Algorithms & Modern Encryption Compared with Classical Computer

Modern cryptography is essentially developing approaches to prevent hackers from intercepting information during the data transfer. One of the most well known approaches to modern encryption is the RSA encryption developed by Ron Rivest, Adi Shamir and Leonard Adleman in 1977. This algorithm exploits the level of difficulty for classical computers to factor large numbers to ensure the security of the key. The messages are encoded by the public key, which is the large number N. However, the messages can only be decoded by people possessing these two primes numbers p, q whose product is N5. Since the factorization of large numbers N takes classical computer exponential

runtime, it is deemed to be impossible for hackers to attack and intercept the messages being encrypted.

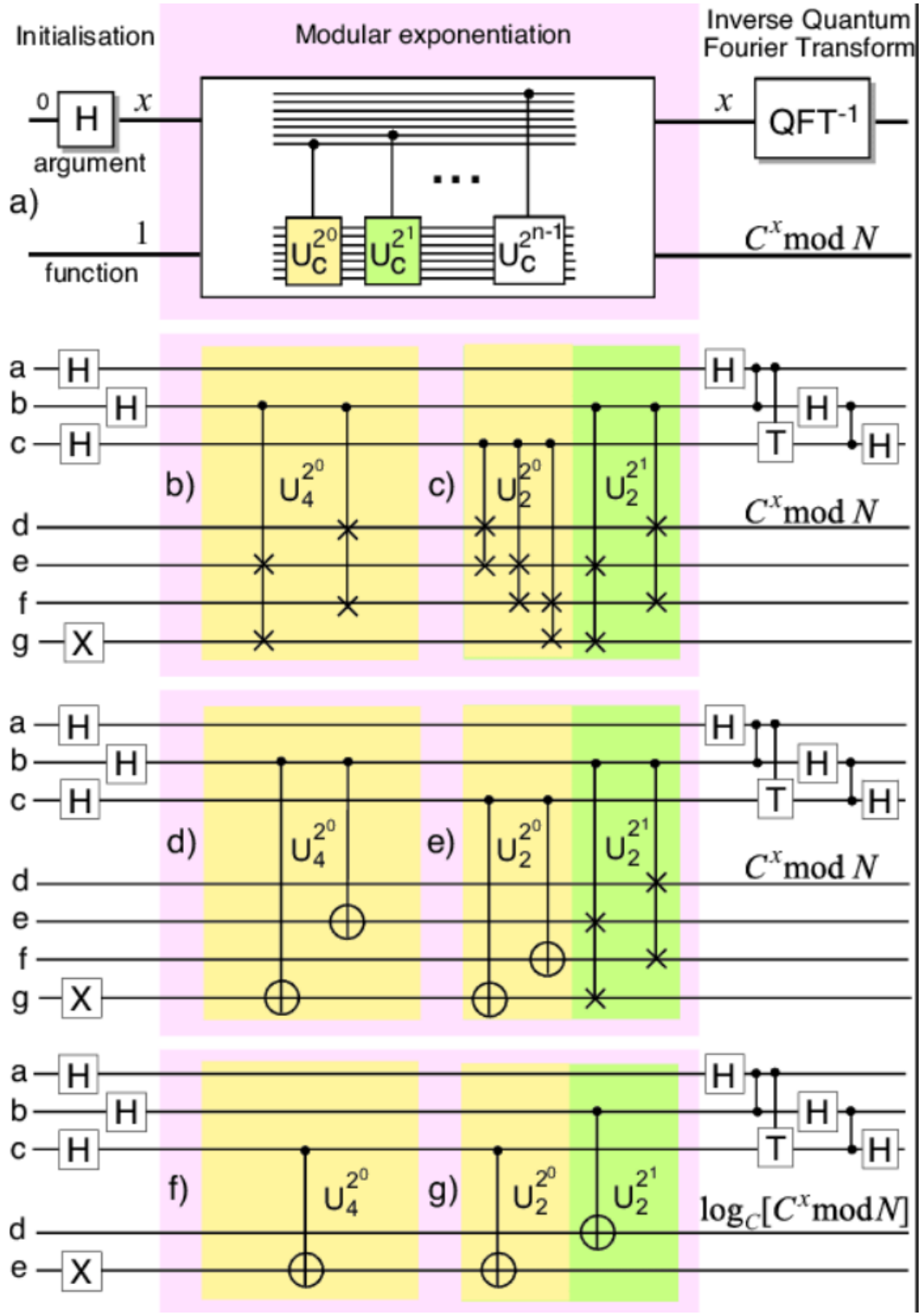

Fig. 1 A general quantum circuit of the Shor's algorithm.

In 1993, Peter Shor presented in his publication "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer" that quantum computers dramatically accelerates the problem of finding the prime factorization [8]. RSA encryption is then proven to be bristled against quantum computers. The algorithm combines the resources of classical and quantum computers to solve the RSA encryption [6]. Shor converted the RSA decryption problem from finding the prime factorization of N to finding the period. A typical sketch of the circuit is shown in Fig. 1. The algorithm does the following for finding p,q such that pq = N:

Pick a number “a” that is coprime with N
Find the period r of “a” with respect to N with quantum computer
If the period r is even: proceed to step d; else, go back to step a
Find x such that x is a^(r/2) mod (N)
If x + 1 does not equal to 0 (mod N), proceed to step f; else, go back to step a
gcd(x+1, N) and gcd(x-1, N) contains at least either p or q (Euclid’s algorithm)
Extract either p or q => getting N = pq

As it can clearly be seen, the third step is the only part within this algorithm that requires a quantum computer. The quantum circuit first applies the hadamard operation to create the superposition of qubits. Then with intentional measuring of the output register qubit to collapse the qubits into periodic arrangement, quantum fourier transform can be applied to extract the periodic information encoded in the input-register.

3.2. Molecular Simulations & Classical Computer

This subsection presents the impact of quantum computers in computational biology and molecular simulations. The study of quantum dynamics plays an important role in modern molecular science, which involves analyzing non-equilibrium processes of complicated potential surfaces. The study deals with solving systems of differential equations of electron and nuclear interaction governed by Schrodinger's equation. However, obtaining solutions of these complicated differential equations is an extremely challenging task for classical computers. Researchers often have to compromise the complexity of the system to obtain approximated solutions. With quantum computers and quantum algorithms, there are new ways for solving problems for molecular structure and condensed matter systems. This part will discuss the general protocol for quantum computers in molecular dynamics.

Finding the hamiltonian for the electrons in the molecular structure is an essential step in molecular simulations. Quantum computers are exponentially more efficient in this task when compared with classical computers. This can be easily shown with the quantization of N electrons in M points grid based format. While classical simulators require $M^{3N}*2^{N}$ complex amplitude, encoding the same system in quantum computers only require 3*(log2(M)+1)N qubits. When the system gets increasingly complicated with larger N and M, as all real world problems would, quantum computers can easily overtake classical computers due to the exponential speed increase. When it comes to the excited states for electrons in molecular structure, quantum computers are also ahead of classical computers. The Algorithm presented in the figure shows how quantum computers deal with excited electrons. In this Quantum-OEM approach, the solution is approximated by expressing the excitation operator as the basis with coefficients. The excitation energy can be extracted from the blue matrix equation in Fig. 2. From the matrix equation, quantum computers achieve efficiency by measuring individual matrix elements [9]. Thus, the physical property of the electrons including energy and forces in molecular structure can be computed with these quantum algorithms efficiently.

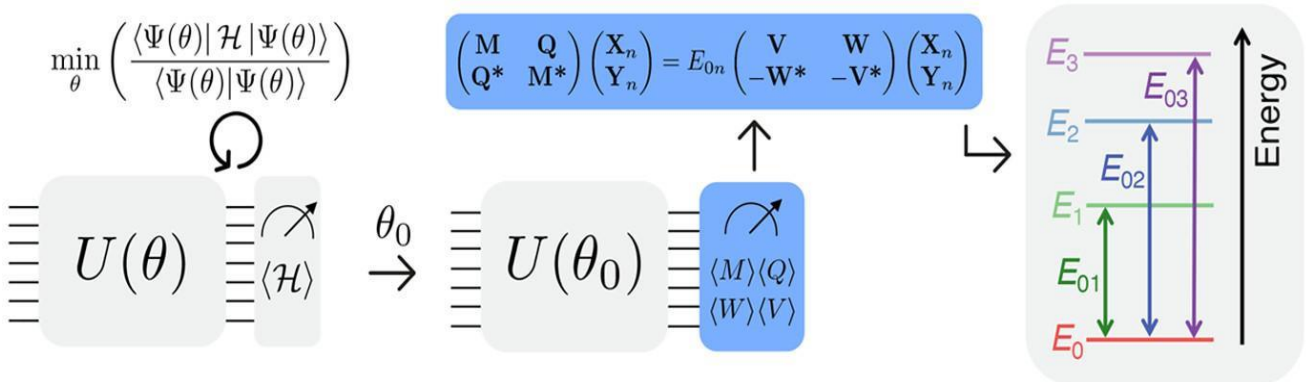

Fig. 2 Graphical representation of the qEOM algorithm.

When it comes to actual quantum dynamics simulation, classical computers fail to scale efficiently when the nuclear degrees of freedom increase. For quantum computers, there are different algorithms,

applied in various scenarios, that aim to produce more promising outcomes with minimal error than classical computers. One such approach is using the product formulas for hamiltonian simulation. In this algorithm, the time propagator can be approximated by Lie–Trotter–Suzuki formula, and as t is approaching 0, the formula gives

$$e^{-iHt} = sum\left(e^{-ih\frac{t}{d}}\right)^{d} + O(Nb^2t^2/d) \quad (1)$$

With the reduction of scaling error to $Nh^{O\left(\frac{Nbt^2}{d}\right)}$ [10]. Since each individual e^{-iht} can be implemented into a quantum circuit, the algorithm implies the viability of the decomposition of the hamiltonian. Another approach for hamiltonian simulation is the variational quantum algorithm (VQA). In Ying Li and Simon C Benjamin's paper on Efficient Variational Quantum Simulator Incorporating Active Error Minimization, they presented a hybrid algorithm to solve the Schrodinger equation. They elect to use classical computers to numerically solve the differential equation, and the solution allows them to project their parameters forward by a small time increment and repeat the classical step. Eventually, they reach the parameters of interest and it permits them to prepare the final state in quantum computers [11]. Since this algorithm can run in parallel, the computing speed can be accelerated by a cluster of coprocessors independently.

4. Limitations & Prospects

With its versatile application in modern cryptography, molecular simulation, and many more scientific fields, quantum computers have a bright future ahead of them. Their power and ability to decipher classical encryption technology with amazing efficiency have been discussed in this work. In addition, their ability to produce promising results when solving the molecular structural problems and performing biological simulation involving protein structure prediction are also outlined in this paper. However, there's one question remaining. It turns out that the current stage of quantum computers are no way near universal commercialization. Even though scientists have reached quantum computing's historic milestone, quantum supremacy, the idea is still largely theoretical. Currently, IBM launches the Eagle, the world's most powerful quantum processor with 127 qubits. They also promised a 1000 qubits quantum computer by 2023. Nevertheless, these are nowhere near the level of development required for industry-wide commercialization. There are still many challenges that are holding researchers back. Quantum computers, unlike classical computers, contain plenty of useless information during its operation, and it is difficult to filter out the garbage and extract the useful result [12]. Furthermore, quantum qubits are sensitive to their surroundings, and isolating surrounding noise including maintaining near 0 kelvin temperature and lowering magnetic interference is still a hard issue that researchers need to overcome. Last but not least, the current scale of the quantum computers are just not large enough to yield useful computation for real world systems. For instance, modern RSA encryption's public keys are of the scale of a few hundred digits, and even the most advanced quantum computers are not capable of deciphering the RSA encryption of that scale.

However, these limitations do not prevent quantum computers from shining in the spotlight. Other scholars points out that commercialization of quantum technologies can happen faster than people have anticipated. There are several early stage quantum-computing devices that can achieve commercialization and produce short-term returns for investors in the field. Quantum simulation, quantum assisted optimization and quantum sampling would be appealing advantages in sectors including artificial intelligence to finance and health care [13]. Researchers working in biological simulation are eager for the computational power of quantum computers. Moreover, regardless of the hardware development in quantum computing, professionals in modern cryptography and cyber security are already alerted by quantum computing's capability. They have to be on par or even ahead of the hardware development to prevent the catastrophic effect quantum computers will bring on information security.

5. Conclusion

In summary, quantum computers perform certain tasks dramatically better than classical computers. When it comes to modern cryptography, quantum algorithms that utilize the vast phase-space revolutionize the way researchers had prior to their occurrence. For molecular simulation, quantum computers have led to multiple approaches to pursue complex simulation of quantum dynamics from the Qubits approach to storing information to the VQA approach to reduce noise in molecular structural analysis. This study highlights the advantages for quantum computers over classical computers with the examples in different applications, and it emphasizes the necessity of scholars and investors to face it. Although this technology is still in early stages, this paper provides a glimpse of the future of quantum computer's future. These results will stir up interest in this topic and prompt more brilliant researchers in the development, from where many possibilities are anticipated to take place.

References

[1] Hassan S, Asghar M. Limitation of silicon based computation and future prospects. 2010 Second International Conference on Communication Software and Networks. IEEE, 2010: 559-561.

[2] Gruska J. Quantum computing. London: McGraw-Hill, 1999.

[3] Steane A. Quantum computing. Reports on Progress in Physics, 1998, 61(2): 117.

[4] Hirvensalo M. Quantum computing. Springer Science & Business Media, 2003.

[5] Terhal B M. Quantum supremacy, here we come. Nature Physics, 2018, 14(6): 530-531.

[6] Mavroeidis V, Vishi K, Zych M D, et al. The impact of quantum computing on present cryptography. arXiv preprint arXiv:1804.00200, 2018.

[7] Zeh H D. Feynman's interpretation of quantum theory. The European Physical Journal H, 2011, 36(1): 63-74.

[8] Schrödinger E, Trimmer J D. The present situation in quantum mechanics: a translation of Schrödinger's 'cat paradox'paper. Proceedings of the American Philosophical Society, 1980, 124(5): 323-338.

[9] Shor P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM review, 1999, 41(2): 303-332.

[10] Ollitrault P J, Miessen A, Tavernelli I. Molecular quantum dynamics: A quantum computing perspective. Accounts of Chemical Research, 2021, 54(23): 4229-4238.

[11] Li Y, Benjamin S C. Efficient variational quantum simulator incorporating active error minimization. Physical Review X, 2017, 7(2): 021050.

[12] Outeiral C, Strahm M, Shi J, et al. The prospects of quantum computing in computational molecular biology. Wiley Interdisciplinary Reviews: Computational Molecular Science, 2021, 11(1): e1481.

[13] Mohseni M, Read P, Neven H, et al. Commercialize quantum technologies in five years. Nature, 2017, 543(7644): 171-174.