Quantum Computation

Research Proposal · October 2019

DOI: 10.13140/RG.2.2.24387.35365

Abdul Majid
Quaid-e-Awam University of Engineering, Science and Technology
13 PUBLICATIONS **35** CITATIONS

Quantum Computation

Short Papers (WiP)

Abdul Majid

Department of Information Technology, Quaid-e-Awam University, Nawabshah Sindh, Pakistan

Keywords:

1.Quantum Computation

- Quantum Bit
- Quantum Register
- Quantum Logic Gate

2.Quantum Mechanics

- Superposition
- Entanglement
- Decoherence

3.Algorithm & Programming

4.Network & Communication

5.Applications

6.Conclusion

The main purpose of this paper is to examine some (potential) applications of quantum computation and to review the interplay between quantum theory and quantum computation. For the readers who are not familiar with quantum computation, a brief introduction is provided, and famous applications are introduced so that they can appreciate the power of quantum computation.

1. Quantum Computation

Quantum computers were first envisaged by Nobel Laureate physicist **Feynman** in 1982. He conceived that no classical computer could simulate certain quantum phenomena without an exponential slowdown, and so realized that quantum mechanical effects should offer something genuinely new to computation. In 1985, Feynman's ideas were elaborated and formalized by Deutsch in a seminal paper, where a quantum Turing machine was described. In particular, Deutsch introduced the technique of quantum parallelism based on the superposition principle in quantum mechanics by which a quantum Turing machine can encode many inputs on the same tape and perform a calculation on all the inputs simultaneously. Furthermore, he proposed that quantum computers might be able to perform certain types of computation that classical computers can only perform very inefficiently.

One of the most striking advances was made by **Shor** in 1994. By exploring the power of quantum parallelism, he discovered a polynomial-time algorithm on quantum computers for prime factorization of which the best known algorithm on classical computers is exponential. In 1996, **Grover** offered another killer application of quantum computation, and he found a quantum algorithm for searching a single item in an unsorted database in square root of the time it would take on a classical computer. Since database search and prime factorization are central problems in computer science and cryptography, respectively, and the quantum algorithms for them are much faster than the classical ones, Shor and Grover's works stimulated an intensive investigation in quantum computation. Since then, quantum computation has been an extremely exciting and rapidly growing field of research.

Quantum Bit

The basic data unit in a quantum computer is a qubit, which can be physically realized by a two-level quantum mechanical system, e.g. the horizontal and vertical polarizations of a photon, or the up and down spins of a single electron. A qubit is quantum version of the classical binary bit.

Mathematically, a qubit is represented by a unit vector in the two-dimensional complex Hilbert space, and it can be written in the Dirac notation:

|ψ = α0|0+ α1|1

Where |0 and |1 are two basis states, and α0 and α1 are complex numbers with |α0|2 + |α1|2 = 1. The states |0 and |1 are called computational basis states of qubits. Obviously, they correspond to the two states 0 and 1 of classical bits. The number α_0 and α_1 are called probability amplitudes of the state |ψ.

Quantum Register

In quantum computing, a quantum register is a system comprising multiple qubits. It is the quantum analog of the classical processor register. Quantum computer perform calculations by manipulating qubits within a quantum register. The Hilbert Space in which the data stored is given by:

$$\mathcal{H} = \mathcal{H}_{n-1} \otimes \mathcal{H}_{n-2} \otimes \ldots \otimes \mathcal{H}_0$$

Quantum Logic Gate

In quantum circuit model of computation, a quantum logic gate or Quantum Gate is a basic quantum circuit operating on a small number of qubits. They are the building blocks of quantum circuit, like classical logic gates are for conventional digital circuits. Quantum logic gates are represented by unitary matrix. No. of qubits in the input and output must be equal. The Vector representation of two qubits is:

$$|ab\rangle = |a\rangle \otimes |b\rangle = v_{00}|00\rangle + v_{01}|01\rangle + v_{10}|10\rangle + v_{11}|11\rangle \rightarrow \begin{bmatrix} v_{00} \\ v_{01} \\ v_{10} \\ v_{11} \end{bmatrix}$$

<u>Notable Example</u>

Hadamard (H) Gate

This gate acts on a single qubit. It maps the basis state $|0\rangle$ to $\frac{|0\rangle + |1\rangle}{\sqrt{2}}$ and $|1\rangle$ to $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$ which means that a measurement will have equal probabilities to become 1 or 0 (creates a superposition).

2. Quantum Mechanics

Actually it's just quantum theory in action. A Quantum computer is as kind of new device based on the science of quantum physics. Well, quantum physics describes the behavior of atoms and fundamental particles like electrons and photons. So quantum computer operates by controlling the behavior of these particles but in a way that is completely different from our regular computers. In many aspects modern technology operates at a scale where quantum effects are significant. Quantum computers are expected to perform certain computational tasks exponentially faster than classical computers. Instead of using classical bits, quantum computers use qubits, which can be in super positions of states.

Superposition

Qubits can represent numerous possible combinations of 1 and 0 at the same time. This ability to simultaneously be in multiple states is called superposition. Working of a quantum computer is based on using the particles in superposition. It states that any two or more quantum states can be added together and the result will be another valid quantum state.

Superposition refers to the quantum phenomenon where a quantum system can exist in multiple states or places at the exact same time

Entanglement

Nobody really knows quite how or why entanglement works? But it is key to the power of quantum computers. Most researchers believe that entanglement is necessary to realize quantum computing.

They can generate pairs of qubits that are entangled which means the two members of a pair exist in a single quantum state. Changing the state of one of the qubits will instantaneously change the state of other one in a predictable way. Quantum state of each particle cannot be described independently of the state of the others.

Best-known application of entanglement is quantum teleportation.

Decoherence

Noise in quantum speak still cause's lots of errors to creep into calculations. Interaction of qubits with their environment in ways that cause their quantum behavior to decay and ultimately disappear is called decoherence. Decoherence represents a challenge for the practical realization of quantum computers. Researchers do their best to protect qubits from the outside world in those super cooled fridges and vacuum chambers. They require the coherent states be preserved and that decoherence is managed, in order to actually perform quantum computation.

Their quantum state is extremely fragile. The slightest vibration or change in temperature, can cause them to tumble out of superposition before their job has been properly done.

3. Quantum Algorithm & Programming

Research on quantum algorithms has been the driving force of the whole field of quantum computation because some quantum algorithms indicate that quantum computation may provide considerable speedup over classical computation. Unfortunately, I am not an expert in quantum algorithms and thus can only give a very brief survey of this area. Three classes of quantum algorithms have been discovered, which show an advantage over known classical algorithms:

(1) Algorithms based on quantum Fourier transforms, e.g. the Deutsch–Jozsa algorithm and Shor’s algorithm for factoring and discrete logarithm;

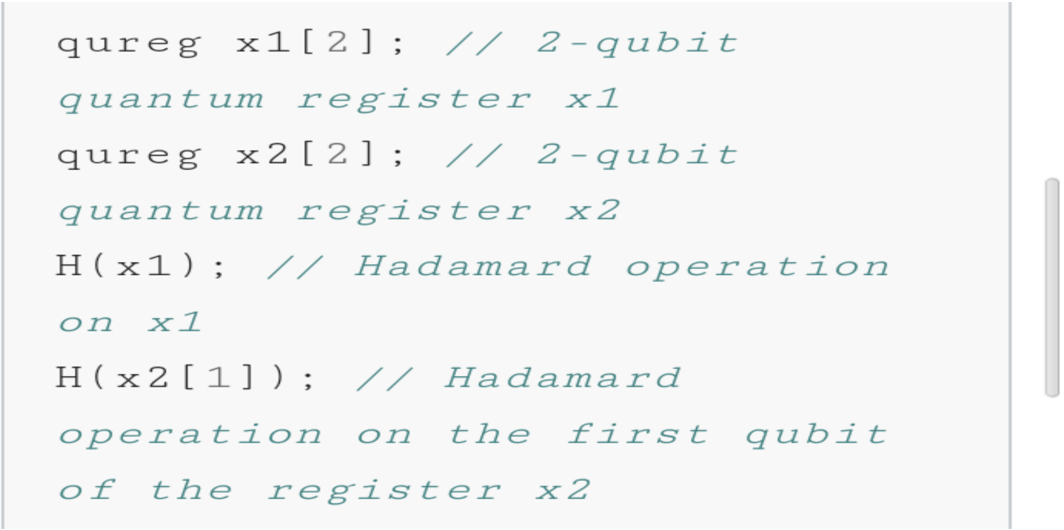
(2) Quantum search algorithms, that is, Grover’s algorithms and its extensions;

(3) Quantum algorithms for simulation of quantum systems, with the basic idea tracing back to Feynman.

When quantum computers becomes available in the future, quantum softwares will play a key role in exploiting their power. Quantum Programming is the process of assembling sequences of instructions, called quantum programs, which are capable of running on quantum computer. Quantum programming languages help express quantum algorithms using high level constructs. There are two main groups (imperative and functional) of quantum programming languages. The first quantum language of the functional programming paradigm, QFC, was defined by Selinger, based on the idea of classical control and quantum data. A quantum functional programming language with quantum control was introduced.

Quantum Computation Language (QCL) is one of the first implemented quantum programming languages. The most important feature of QCL is the support for user-defined operators and functions.

Quantum software development kits provide collections of tools to create and manipulate quantum programs. They also provide the means to simulate the quantum programs, or prepare them to be run using cloud-based quantum devices.



```
qureg x1[2]; // 2-qubit
quantum register x1
qureg x2[2]; // 2-qubit
quantum register x2
H(x1); // Hadamard operation
on x1
H(x2[1]); // Hadamard
operation on the first qubit
of the register x2
```

4. Quantum Communication & Network

Today, sensitive data is typically encrypted and then sent across fiber-optic cables and other channels together with the digital keys needed to decode the information. The data and the keys are sent as classical bits, a stream of electrical or optical pulses representing 1s and 0s, and that makes them vulnerable. Smart hackers can read and copy bits in transit without leaving a trace.

Quantum communication takes advantage of the laws of quantum physics to protect data. These laws allow particles typically photons of light for transmitting data along optical cables to take on a state of superposition, which means they can represent multiple combinations of 1 and 0 simultaneously. The particles are known as qubits.

The beauty of qubits from a cyber security perspective is that if a hacker tries to observe them in a transit, their super fragile quantum state collapses to either 1 or 0. This means a hacker cannot temper with the qubits without leaving behind a telltale sign of the activity. Quantum uncertainty could be used to create private keys for encryption. Some companies have taken advantage of this property to create networks for transmitting highly sensitive data based on a process called quantum key distribution, or QKD. So that hackers could not secretly copy the key perfectly. They would have to break the laws of quantum physics to hack the key.

In theory, these networks are ultra-secure. QKD involves sending encrypted data as classical bits over networks, while the keys to decrypt the information are encoded and transmitted in a quantum state using qubits.

Various protocols have been developed for implementing QKD. A widely used one known as **BB84** works like this.

Materials in cables can absorb photons, which means they can typically travel for no more than a few tens of Kilometers. In a classical network, repeaters at various points along a cable are used to amplify the signal to compensate for this.

QKD networks have come up with a similar solution, creating trusted nodes at various points. At these waystations, quantum keys are decrypted into bits and then re encrypted in a fresh quantum state for their journey to the next node. But this means trusted nodes can’t really be trusted.

Ideally, we need quantum repeaters, or waystations with quantum processors in them that would allow encryption keys to remain on quantum form as they are amplified and sent over long distances. It is possible in principle to build such repeaters, but researchers are working on an alternative approach, a one of the quantum computer’s real applications, known as Quantum Teleportation.

5. Applications

One of the areas that I have been researching is what application can best make use of the power of quantum computing. Although this is a work in progress, I am providing a preliminary assessment based upon research I have done so far. Successful implementation of these applications areas will probably be based upon a hybrid platform that combines classical and quantum computing in a cloud environment to achieve the best of both worlds. So, let me give you two examples of potential applications that could change our lives.

Quantum Teleportation

Teleportation of information from one location to another without physically transmitting the information. This may sound like science fiction, but it's a real method that involves transmitting data in wholly quantum form. This approach relies on a quantum phenomenon known as Entanglement. These fluid identities of the quantum particles can get entangled across space and time in such a way that when you change something about one particle, it can impact the other and that creates a channel for teleportation. Just like the traditional internet this would be a globe-spanning network of networks (quantum internet).
China is the vanguard of the push toward a quantum internet. It launched a dedicated quantum communication satellite called Micius a few years ago, and in 2017 the satellite helped stage the world's first intercontinental, QKD-secured video conference, between Beijing and Vienna.

Computational Chemistry

Quantum technologies could also transform healthcare and medicine. For example, the design and analysis of molecules for drug development is a challenging problem today, and that's because exactly describing and calculating all of the quantum properties of all the atoms in the molecule is a computationally difficult task, even for our super computers. But a quantum computer could do better, because it operates using the same quantum properties as the molecule it's trying to simulate. So future large-scale quantum simulations for drug development could perhaps lead to treatment for diseases like Alzheimer's, which affects thousands of lives.

6. Conclusion

Quantum computing will give rise to a wave of technological applications, creating new business opportunities and helping solve some of today's most pressing global challenges. Previously untapped effects of quantum theory can now be used as a resource in technologies with far-reaching applications: secure communication networks, ultra-precise sensors, and study of chemical reactions for pharmacology, novel materials and fundamentally new paradigms of computation. In the last few years, governments and companies around the world, including Google, Microsoft, Intel, Toshiba and IBM, are considerably investing to unleash this potential. Although there has been significant progress in quantum computing, the field faces a number of challenges including the difficulty of building a large-scale quantum computer; designing new quantum algorithms and building expenses.

Researchers in the field have won many other prizes, as well, and likely there will be more to come. But for us as engineers and scientists, and for many others in research and engineering, with support from governments and venture capitalists, the time has come to build systems that can be used to solve some of the critical problems facing society. We hope that this is the beginning of your interest in, and study of, quantum computing, rather than its end. It is increasingly clear not just to us, as researchers, but too many people, that quantum technology will be one of the fundamental paradigm shifts of the twenty-first century.