Quantum Computing

Vraj Parikh
B.E.-G.H.Patel College of Engineering & Technology, Anand (Affiliated with GTU)

Abstract

Formerly, Turing Machines were the exemplar by which computability and efficiency have been defined. This is based on Church's thesis. According to it everything that is computed effectively can be computed using Turing Machine. But as our world behaves according to principle of Quantum Mechanics, it is sensible to consider computing models that make use of quantum mechanical properties.

Quantum Computing is an extremely exciting and rapidly growing field research. An increasing number of researchers from different backgrounds, ranging from physics via computer science and information theory to mathematics and philosophy, are involved in researching quantum-based computation.

This paper gives general overview about the subject.

INTRODUCTION-

Civilization has advanced as people discovered new ways of exploiting various physical resources such as materials, forces and energies. In the twentieth century information was added to the list when the invention of computers allowed complex information processing to be performed outside human brains. The history of computer technology has involved a sequence of changes from one type of physical realization to another - from gears to relays to valves to transistors to integrated circuits and so on.

Today's advanced lithographic techniques can squeeze fraction of micron wide logic gates and wires onto the surface of silicon chips. Soon they will yield even smaller parts and inevitably reach a point where logic gates are so small that they are made out of only a handful of atoms. On the atomic scale 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 the future, new, quantum technology must replace or supplement what we have now. The point is, however, that quantum technology can offer much more than stuffing more and more bits to silicon and multiplying the clock-speed of microprocessors. It can support entirely new kind of computation with qualitatively new algorithms based on quantum principles.

HISTORY OF QUANTUM COMPUTING-

The story of quantum computation started as early as 1982, when the physicist Richard Feynman considered simulation of quantum-mechanical objects by other quantum systems. However, the unusual power of quantum computation was not really anticipated until the 1985 when David Deutsch of the University of Oxford published a crucial theoretical paper in which he described a universal quantum computer. After the Deutsch paper, the hunt was on for something interesting for quantum computers to do. At the time all that could be found were a few rather contrived mathematical problems and the whole issue of quantum computation seemed little more than an academic curiosity. It all changed rather suddenly in 1994 when Peter Shor from AT&T's Bell Laboratories in New Jersey devised the first quantum algorithm that, in principle, can perform efficient factorization. This became a `killer application' --- something very useful that only a quantum computer could do. Difficulty of factorization underpins security of many common methods of encryption; for example, RSA --- the most popular public key cryptosystem which is often used to protect electronic bank accounts gets its security from the difficulty of factoring large numbers. Potential use of quantum computation for code-breaking purposes has raised an obvious question --- what about building a quantum computer.

Today's computers are classical, a fact which is actually not entirely obvious. A basis of modern computers rests on semiconductor technology. Transistors, which are the "neurons" of all computers, work by exploiting properties of semiconductors. However, the explanation of how semiconductors function is entirely quantum mechanical in nature: it simply cannot be understood classically. Are we thus to conclude that classical physics cannot explain how classical computers work?! Or are we to say that classical computers are, in fact, quantum computers! The answer to both these questions is yes and no. Yes, classical computers are in a certain, restricted, sense quantum mechanical, because, as far as we understand today, everything is quantum mechanical. No, classical computers, although based on quantum physics, are not fully quantum, because they do not use “quantumness” of matter at the information-theoretical level, where it really matters.

Gordon Moore proposed Moore’s law in 1965, which originally stated that processor power and speed would double in size every eighteen months (this was later revised to two years). This law still holds but is starting to falter, and components are getting smaller. Soon they will be so small, being made up of a few atoms that quantum effects will become unavoidable, possibly ending Moore’s law. There are ways in which we can use quantum effects to our advantage in a classical sense, but by fully utilizing those effects we can achieve much more. This approach is the basis for quantum computing.

QUANTUM MECHANICS-

Quantum mechanics is generally about the novel behavior of very small things. At this scale matter becomes quantized, this means that it can be subdivided no more. Quantum mechanics has never been wrong, it explains why the stars shine, how matter is structured, the periodic table, and countless other phenomena. One day scientists hope to use quantum mechanics to explain everything, but at present the theory remains incomplete as it has not been successfully combined with classical theories of gravity. Some strange effects happen at the quantum scale.

The following are main parts of quantum mechanics that are important for quantum computing:

- Superposition and interference
- Uncertainty
- Entanglement
- Linear algebra
- Dirac notation
- Representing information

1. Superposition

Superposition means a system can be in two or more of its states simultaneously. For example a single particle can be traveling along two different paths at once. This implies that the particle has wave-like properties, which can mean that the waves from the different paths can interfere with each other. Interference can cause the particle to act in ways that are impossible to explain without these wave-like properties.

The ability for the particle to be in a superposition is where we get the parallel nature of quantum computing: If each of the states corresponds to a different value then, if we have a superposition of such states and act on the system, we effectively act on all the states simultaneously.

2. Uncertainty

The quantum world is irreducibly small so it’s impossible to measure a quantum system without having an effect on that system as our measurement device is also quantum mechanical. As a result there is no way of accurately predicting all of the properties of a particle. There is a trade off - the properties occur in complementary pairs (like position and momentum, or vertical spin and horizontal spin) and if we know one property with a high degree of certainty then we must know almost nothing about the other property.

3. Entanglement

In 1935 Einstein (along with colleagues Podolski and Rosen) demonstrated a paradox (named EPR after them) in an attempt to refute the undefined nature of quantum systems. The results of their experiment seemed to show that quantum systems were defined, having local state BEFORE measurement. Although the original hypothesis was later proven wrong (i.e. it was proven that quantum systems do not have local state before measurement). The effect they demonstrated was still important, and later became known as entanglement.

Entanglement is the ability for pairs of particles to interact over any distance instantaneously. Particles don’t exactly communicate, but there is a statistical correlation between results of measurements on each particle that is hard to understand using classical physics. To become entangled, two particles are allowed to interact; they then separate and, on measuring say, the velocity of one of them (regardless of the distance between them), we can be sure of the value of velocity of the other one (before it is measured). The reason we say that they communicate instantaneously is because they store no local state and only have well defined state once they are measured. Because of this limitation particles can’t be used to transmit classical messages faster than the speed of light as we only know the states upon measurement. Entanglement has applications in a wide variety of quantum algorithms and machinery.

4. Linear Algebra

Quantum mechanics leans heavily on linear algebra. Some of the concepts of quantum mechanics come from the mathematical formalism, not thought experiments, that’s what can give rise to counter intuitive conclusions.

5. Dirac Notation

Dirac notation is used for quantum computing. We can represent the states of a quantum system as kets. For example, an electron’s spin can be represented as |0> spin up and |1> as spin down. The electron can be thought of as a little magnet, the effect of a charged particle spinning on its axis. When we pass a horizontally traveling electron through an inhomogeneous magnetic field, in say, the vertical direction, the electron either goes up or down. If we then repeat this with the up electron it goes up, with the down electron it goes down. We say the up electron after the first measurement is in the state |0> and the down electron is in state |1>.

But, if we take the up electron and pass it through a horizontal field it comes out on one side 50% of the time and on the other side 50% of the time. If we represent these two states as | + > and | - > we can say that the up spin electron was in a superposition of the two states |+> and | - > :

$$|0\rangle = 1/\ (2)^{1/2}|+\rangle + 1/\ (2)1/2|-\ \rangle$$

such that, when we make a measurement with the field horizontal we project the electron into one or the other of the two states, with equal probabilities ½ (given by the square of the amplitudes).

6. Representing Information

Quantum mechanical information can be physically realised in many ways. To have something analogous to a classical bit we need a quantum mechanical system with two states only, when measured.

Methods for representing binary information in a way that is capable of exhibiting quantum effects (e.g. entanglement and superposition) are: electron spin, photon direction, polarisation of photons and nuclear spins.

ELEMENTS OF QUANTUM COMPUTING-

Generally we’ll think of a quantum computer as a classical computer with a quantum circuit attached to it with some kind of interface between conventional and quantum logic. Since there are only a few things a quantum computer does better than a classical computer it makes sense to do the bulk of the processing on the classical machine.

1. Bits and Qubits

These are the ”nuts and bolts” of quantum computing. It describes qubits, gates, and circuits. Quantum computers perform operations on qubits which are analogous to conventional bits but they have an additional property in that they can be in a superposition.

A quantum register with 3 qubits can store 8 numbers in superposition simultaneously, and a 250 qubit register holds more numbers (superposed) than there are atoms in the universe. The amount of information stored during the ”computational phase” is essentially infinite - it’s just that we can’t get at it. The inaccessibility of the information is related to quantum measurement: When we attempt to readout a superposition state holding many values the state collapses and we get only one value (the rest get lost). This is tantalizing but, in some cases, can be made to work to our computational advantage.

Single Qubits

Classical computers use two discrete states (e.g. states of charging of a capacitor) to represent a unit of information, this state is called a binary digit (or bit for short). A bit has the following two values:

0 and 1

There is no intermediate state between them, i.e. the value of the bit cannot be in a superposition.

Quantum bits, or qubits, can on the other hand be in a state ”between” 0 and 1, but only during the computational phase of a quantum operation. When measured, a qubit can become either:

|0> OR |1>

i.e. we readout 0 or 1. This is the same as saying a spin particle can be in a superposition state but, when measured, it shows only one value. The | > symbolic notation is part of the Dirac notation.

In terms of the above it essentially means the same thing as 0 and 1, just like a classical bit. Generally, a qubit’s state during the computational phase is represented by a linear combination of states otherwise called a superposition state.

$$\alpha|0\rangle + \beta|1\rangle$$

Here α and β are the probability amplitudes. They can be used to calculate the probabilities of the system jumping into |0> or |1> following a measurement or readout operation. There may be, say a 25% chance a 0 is measured and a 75% chance a 1 is measured. The percentages must add to 100%. In terms of their representation qubits must satisfy:

$$| \alpha |^2 + | \beta |^2 = 1$$

Once the qubit is measured it will remain in that state if the same measurement is repeated provided the system remains closed between measurements. The probability that the qubit's state, when in a superposition, will collapse to states |0> or |1> is

$$| \alpha |^2 \text{ FOR } |0>$$

And

$$| \beta |^2 \text{ FOR } |1)$$

|0> and |1> are actually vectors, they are called the computational basis states that form an orthonormal basis for the vector space C2.

The state vector φ of a quantum system describes the state at any point in time of the entire system. Our state vector in the case of one qubit is:

$$|\varphi> = \alpha|0> + \beta|1>$$

The α and β might vary with time as the state evolves during the computation but the sum of the squares of α and β must always must be equal to 1.

Multiple Qubits

The potential amount of information available during the computational phase grows exponentially with the size of the system, i.e. the number of qubits.

This is because if we have n qubits the number of basis states is 2n. E.g. if we have two qubits, forming a quantum register then there are four (=22) computational basis states: forming,

$$|00>, |01>, |10> \text{ AND } |11>$$

Here |01> means that qubit 1 is in state |0> and qubit 2 is in state |1>, etc. We actually have | 01 > = | 0 > |1 >, where is the tensor product.

Like a single qubit, the two qubit register can exist in a superposition of the four states (below we change the notation for the complex coefficients, i.e. probability amplitudes):

$$|\varphi> = \alpha_1|00> + \alpha_2|01> + \alpha_3|10> + \alpha_4|11>$$

All of the probabilities must sum to 1.

2. Entangled States

Subatomic particles can be entangled; this means that they are connected, regardless of distance. Their effect on each other upon measurement is instantaneous. This can be useful for computational purposes. Consider the following state (which is not entangled):

$$1/(2)^{1/2}(|00> + |01>)$$

it can be expanded to:

$$1/(2)^{1/2}|00> + 1/(2)^{1/2}|01> +0|10> + 0|11>$$

Upon measuring the first qubit (a partial measurement) we get 0 100% of the time and the state of the second qubit becomes:

$$1/(2)^{1/2}(|0> + |1>)$$

CONCLUSION-

The laws of quantum mechanics imply a different kind of information processing to the traditional one based on the laws of classical physics. The central difference, as we emphasised, was in the fact that quantum mechanics allows physical systems to be in an entangled state, a phenomenon non-existent in classical physics. This leads to a quantum computer being able to solve certain tasks faster than its classical counterpart.

REFERENCES-

1. http://www.consciousness.arizona.edu/quantum/Library/qmlecture1.htm
2. http://www.cse.iitd.ernet.in/~suban/quantum/lectures/lecture1.pdf
3. http://www.Qubit.org/library/intros/comp/comp.html
4. http://www.sra.itc.it/people/serafini/quantum-computing/20001006.ps
5. http://www.cs.ualberta.ca/~bulitko/qc/schedule/qcss-notes.pdf
6. http://www.cl.cam.ac.uk/Teaching/current/QuantComp/