Quantum Computation: Prospects and Challenges

Aman Pathak

apathakcse@gmail.com

Abstract

Quantum computation is an entirely new way of information processing. The traditional methods of computation and information processing used by the human civilization are therefore referred to as classical information and classical computation. The way classical information is stored and used is in for of bits. The bit is the most basic piece of information. While the systems built using the principle are robust as of todays standard, they will become irrelevant in the coming future due to the arise of analog and quantum computers. In similar manner, we define a basic unit of computation and information processing which is used in quantum computation. This basic unit of information in quantum computing is called the qubit, which is short for quantum bit. Analog computers are different topic which will not be discussed in this paper.

Introduction

In simple words, bits represent information in True or False form. Mathematically, it is represented by using base 2, which in formal language is known as binary numbers. A binary number can be either 0 or 1. A bit can take any one of these values at a moment which in turn represent data. Different systems store this classical information in different ways. Certain systems use the presence or absence of electrons to represent 1 or 0 respectively, while others define 0 as ground or zero volts, and 1 as an arbitrary voltage, let us say +5 volts. The number of bits required to represent something can be determined by supposing that some quantity can assume one of *m* different states,

$2^n \geq m$

for some *n*. The smallest *n* for which this holds true gives us the number of bits we need to represent or encode that quantity. We use 2 here because each of bits can have one possible state out of the two, 0 or 1.

Though a qubit looks very similar to our classical bit, it is fundamentally different and that its difference allows us to do information processing in new and interesting ways. While a bit in a normal computer can exist in the state 0 or in the state 1, a qubit is a more general form. A qubit can exist in the state $|0\rangle$ or the state $|1\rangle$, but it can also exist in what we call a superposition state. This is a state that is a linear combination of the states $|0\rangle$ and $|1\rangle$. This comes from the fact that Quantum Mechanics takes hold of the properties of particles when we are talking at the quantum level. The mathematics and derivations are too complex for a simple review paper like this; hence we shall be skipping that part, assuming it to be an axiom rather than that requiring a proof.

Theory

The methods which allow us to use such intricate technology are rather complex, as to use the properties like quantum entanglement and superposition, we need to work at the quantum scale. Superposition states that we can add two or more quantum states and the result will be another valid quantum state. Quantum entanglement occurs when two systems link so closely that knowledge about one gives you immediate knowledge about the other, independent on the separation between them. Quantum processors can draw conclusions about one particle by measuring another one. Quantum entanglement allows quantum computers to solve complex problems faster. When a quantum state is measured, the wavefunction collapses and we measure the state as either a zero or a one. In this known or deterministic state, the qubit acts as a classical bit. Decoherence is the loss of the quantum state in a qubit. Factors like radiation can cause the quantum state or the wave function of the qubits to collapse.

Before diving into the preparation and usage of qubits, we shall look upon the mathematical methods which allow us to use them in theory. In quantum mechanics, the general quantum state of a qubit can be represented by a linear superposition of its basis vectors. They are written in the conventional Dirac, or the bra-ket notation, which was developed by Paul Dirac. These two basis states, are together called the computational basis, are said to span the two-dimensional linear vector space of the qubit.

A pure qubit is a coherent superposition of the basis states. This means that a single qubit $|\psi\rangle$ can be described by a linear combination of qubit $|0\rangle$ and $|1\rangle$. It is mathematically represented by

$$|\psi\rangle = \alpha|0\rangle + \beta|0\rangle$$

Where α and β are the probability amplitudes, which are themselves complex. According to Born hypothesis, the probability outcome $|0\rangle$ with value "0" is $|\alpha|^2$ and the probability of outcome $|1\rangle$ with value "1" is $|\beta|^2$. As both absolute squares of the amplitude are equal to the probabilities, it must be constrained by the second axiom of probability theory which state

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

The possible quantum states for a single qubit can be visualised using a Bloch Sphere. Represented on such a sphere, a classical bit could only be at the "North Pole" or the "South Pole", in the locations where $|0\rangle$ and $|1\rangle$ are respectively. However, this particular choice of the polar axis is arbitrary. The rest of the surface of the Bloch sphere is not accessible using a classical bit, but a pure qubit state can be represented by any point on the surface. The pure qubit state would lie on the equator of the sphere at the positive X-axis. If we apply classical limits to this system, a qubit, which can have quantum states anywhere on the Bloch sphere, reduces to the classical bit, which can be found only at either pole.

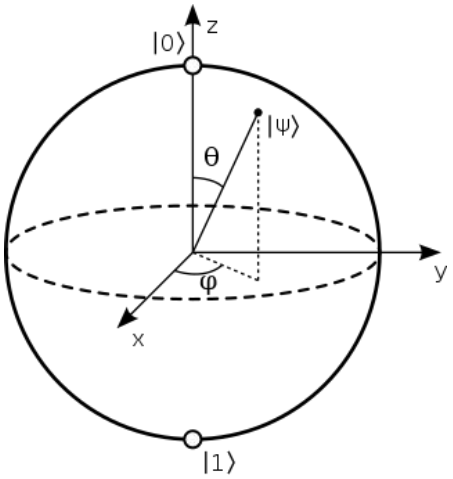

fig: Bloch Sphere representation of a qubit

This fancy science stuff will not work without any real technology, though it looks interesting and works on papers, it is quite difficult to create and use qubits. Any two-level quantum mechanical system can theoretically be used as a qubit. Without going into much detail, we will discuss in brief some possible methods for creation of qubits. One of such methods is a "Trapped ion quantum computer". In this method, charged atomic particles are trapped in free space using electromagnetic fields. Qubits are stored in stable electronic states of each ion and hence computation can be done on them. The fundamental operations of a quantum computer have been demonstrated experimentally with the currently highest accuracy in trapped ion systems. Another method is to use the property of Bose-Einstein condensate which states that when matter is cooled to sub zero kelvin temperatures or near to picokelvin scale, it starts behaving like a quantum particle and exhibits all the quantum phenomena mentioned above. Hence these systems can be used as qubits. These are usually prepared by firing strontium or rubidium atoms which are then slowed down using a Zeeman coil. Further, they are trapped at a point in space using a magneto optical trap and laser evaporative cooling is used to reach picokelvin range.

Discussion

Quantum Computer can solve some problems by several order of magnitude. This brings today's intractable problems to be easy to solve tomorrow. We could carry all possible classical state on operations. This would increase the memory needed. Not only in cryptography and computer security, but also, they have the potential to make important contributions to medical science. Quantum computers could more accurately replicate and model the behaviour of complex molecules than traditional computers. This capacity has the potential to revolutionise drug discovery by allowing scientists to more efficiently identify and create new medications. They can model protein behaviour, predict drug efficacy, and analyse molecular interactions, providing insights into disease causes and prospective treatment targets. Quantum computers are capable of correctly simulating the behaviour of biomolecules like proteins and enzymes. Quantum simulations could aid researchers in understanding disease mechanisms at the molecular level by offering deep insights into their structure, behaviour, and interactions. This knowledge could pave the way for the development of targeted medicines and personalised medicine techniques.

A comparison of classical bits and qubits:

# of qubits	# bits	RAM
1	2	2 bits
2	4	4 bits
3	8	1 byte
4	16	2 bytes
5	32	4 bytes
6	64	8 bytes
7	128	16 bytes
8	256	32 bytes
9	512	64 bytes
10	1024	128 bytes
11	2048	256 bytes
12	4096	512 bytes
13	8192	1 kB
20	1048576	128 kB
23	8388608	1 MB
33	8589934592	1 GB
43	8.8×10^{12}	1 TB
53	9.0×10^{15}	1 PB
63	9.2×10^{18}	1 EB
1000	1.1×10^{301}	1.3×10^{282} EB

Due to the theory of superposition, it only takes 13 qubits to store a kilobyte of data. It would take 1.1×10^{301} classical bits to store the amount of data which qubits can store in just 1000 qubits. For a 1000 qubit system, if we need to store the same amount of data on a classical system, the number of bits required will be 1.1×10^{301}. This number is tremendous, because it is believed that our universe has only around 10^{80} Hydrogen atoms. Quantum computers not only speed up our calculations, but also open different domains where humanity could excel.

Though these numbers are lucrative, it is not easy to create, store and use qubits. Quantum systems are highly susceptible to noise and environmental interference, leading to decoherence. Decoherence causes the fragile quantum states of qubits to lose their coherence and information, stopping the reliable execution of quantum computations. This in turn turns them into normal classical system rendering them useless for our purpose. Building quantum computers with a large number of qubits is essential to tackle complex problems efficiently. However, scaling up quantum systems is challenging due to the need for maintaining qubit coherence, reducing cross-talk between qubits, and implementing precise control over a growing number of qubits. Though there has been significant amount of funds put in this research, we are far from creating scalable quantum computers which are efficient too. Another problem is that qubits are prone to errors. These are caused by factors such as noise, thermal fluctuations, and errors in hardware components. Ensuring high-quality qubits with long coherence times and low error rates is crucial for the reliable operation of quantum computers. Quantum computing requires the development of new software frameworks, programming languages, and algorithms optimized for quantum architectures. Designing efficient quantum algorithms, mapping them onto available hardware, and developing quantum error correction codes are areas of active research.

References

(1) David McMahon (2007), Quantum Computing Explained.
(2) David J. Griffiths (1994), Introduction to Quantum Mechanics.
(3) Feynman, R.P., Leighton, R.B. & Sands, M. (1965), The Feynman Lectures on Physics
(4) Messiah, Albert (1958), Quantum Mechanics, Vol. I.