Week 1 : Introduction to Quantum Computing

Contents

1 Introduction

Modern classical computing is carried out on transistor based chips which obey the laws of classical physics. Traditional parallel computing is carried out on classical computers, but instead of a single problem being solved, we have multiple problems being solved on as many processors in tandem – say we are trying to multiply two different matrices, the final values in different indices in the resultant matrices are independant and can be computed simultaneously on multiple processors.

Quantum computing is an area of research that ties together the progress made in the fields of computer science, information theory, and quantum mechanics. The idea of data being an essential ingredient in the study of physics is a new one, and yet the existance of a relation between the fields of information theory and quantum mechanics is undeniable. While classical computing works on bits, a twofold arrangement of ones and zeros. Quantum computing uses qubits, which can not only exist as ones and zeroes but also as a combination of the two – in other words, a quantum system can exist in mutliple states at once. Qubits can also be 'entangled' – quantum particles can be linked so strongly that they exist in perfect unison, even if separated by cosmic distances. It is these properties of superposition and entaglement which make the foundation that elevates quantum computing above classical computing and allows quantum computers to process vast amounts of information simultaneously.

It is only natural that quantum computers are used in areas of research where the limited computational power of classical computers just wouldn't cut it. One such area is molecular modelling in chemistry where quantum computing is used to calculate bond lengths, transition amplitudes, energies of molecules etc. Molecular behaviour at the atomic level is immensely complex since it is dictated by intricate forces, modelling which a problem beyond the reach of classical computer. Thus, quantum computers have opened up many new and exciting areas of research which were earlier beyond our reach.

1.1 Classical Computing

Classical computers have been around a long time, and in fact have only gotten faster with time. So what's the big deal about quantum computers? Why not build a faster classical computer? It seems to worked out so far!

These are extremely poignant questions, however it is essential that we first understand the fundamentals of classical computing before answering them. After that we shall discuss some of the methods that have been used thus far to speed up classical computation.

parallel computing turing machine reversible computing

1.1.1 Turing Machine

Studying computation on typical laptop or desktop would be immensely complex due to the vast amounts of variables involved such as the operating system, the hardware etc. To simplify this process computer scientists and mathematicians using an abstract model of computers which was initially proposed by Alan Turing – the Turing machine.

Turing machines were designed to capture the notion of algorithm running on a computer allowing a computer scientist to analyse properties of the algorithm and the underlying problem it attempts to solve in simplified manner.

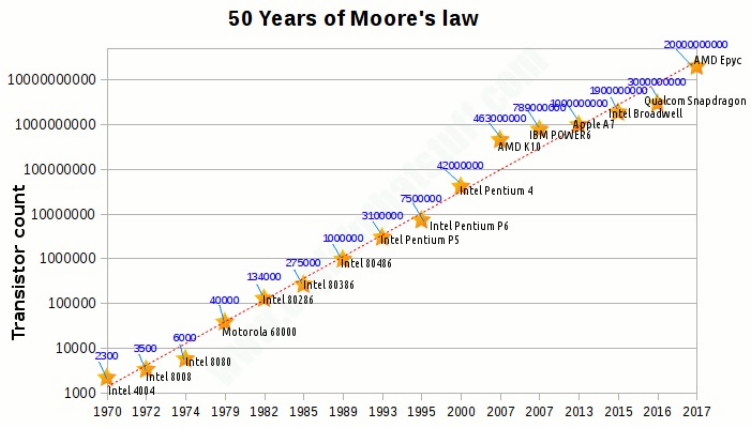
Turing machines consist of four elements – a program, a finite state control, a tape, and a read/write head. The Turing machine's program is set of instructions which must be followed. The finite state control acts like the processor of computer, it executes the instructions of the program. The tape provides infinite memory which may be read/written upon by the head. Thus, a Turing machine behaves like an idealized computer.

In fact such a quantum turing machine can be designed in a analogous manner. This allows computer scientists to study problems on problems on both systems and carry out a comparitive analysis.

Another model of computation is the circuit model of computation which we shall be discussing in the coming weeks.

1.1.2 Moore's Law

Moore's Law is observation named after Gordon Moore (the co-founder and chairman emeritus of Intel). In 1965, Moore described a trend in which the number of transistors double on chips every year (a figure he later updated to two years). The observation has mostly held true, and as a consequence the transistors on chips have been getting smaller and smaller. So much so that, they are now approaching sub-atomic sizes. At such size quantum effects such as "electron tunnelling" start becoming apparent resulting in adverse effects on computation. Increase in number of transistors also results in increased heat production which adversely effects computation. We have therefore hit a wall in terms how many transistors we can squeeze onto a single chip.



Moore's Law over the last 50 years

1.1.3 Parallel Computing

Given that there due to the way quantum mechanics works there a strict limit on how fast a single processor can get. It is a natural progression of thought to use multiple processors to solve a particular problem. This is called parallel computing.

While parallel computing looks good in principle, it in fact has it's own fair share of issues. Since the parallelism isn't inherent in the way it is being carried out, it must be artificially introduced by programming the computer to solve the task using the additional resources at hand; this isn't always easy to do. Moreover, not every problem can parallelised in this fashion.

1.1.4 Reversible Computing

Landauer's principle is a physical principle which says that if the observer loses any information about a physical system, then the observer loses the ability to extract work from the system. In other words the more information about a system we lose, the more inefficient the system becomes.

This is a serious consideration in the case of computation since, most of the operations we carry out are irreversible (think of a logical AND gate, given just the output bit, there is no way determining the input bits). One solution is offered in the form of reversible computing, however, the number of extra bits that need to be introduce a large overhead.

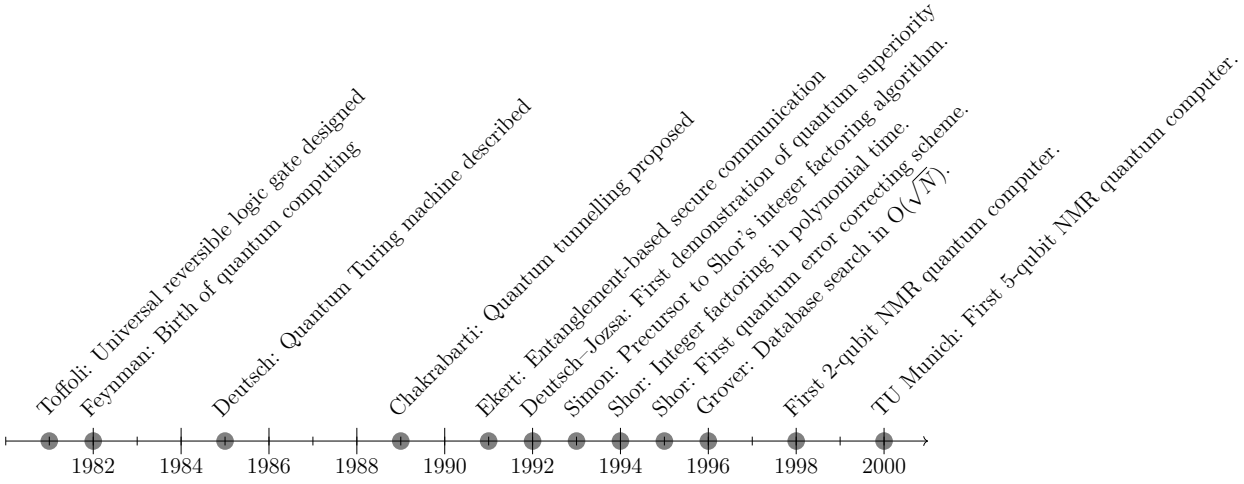
1.2 Why Quantum Computing?

The reason that we need quantum computers can summarised by the following points:

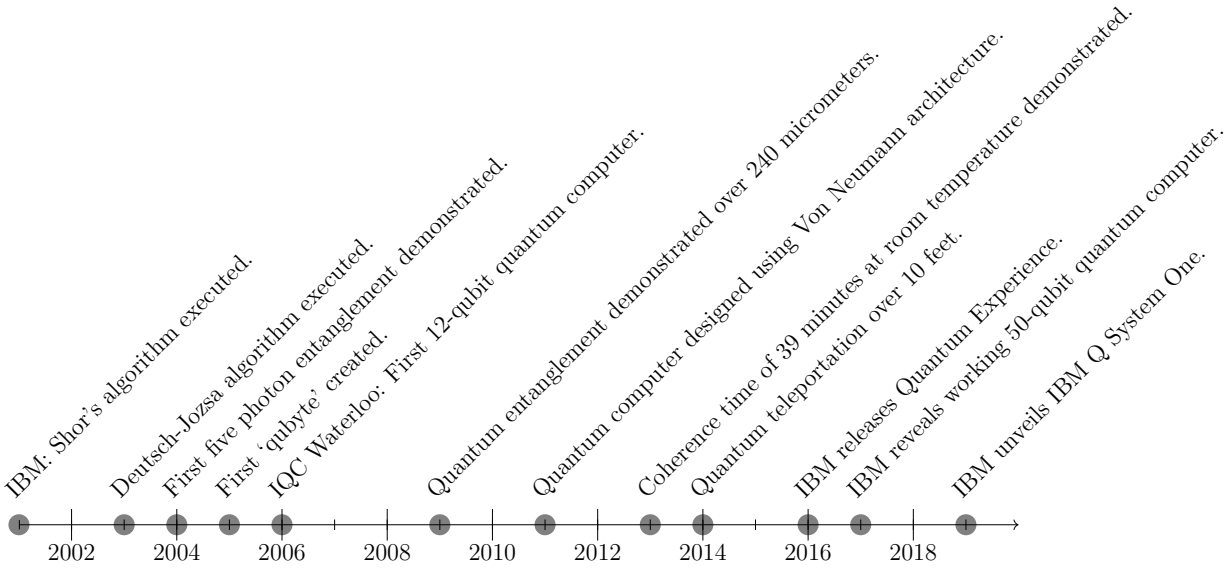
1. Single processor classical computers are nearly as fast as they can be in terms of number of transistors on chip. We need an alternative.

2. Parallel computers exist, however they are difficult to use (when they can be used) since the parallelism in computation isn't natural as opposed to quantum computers.
3. Classical computing involves the irreversible loss of bits leading to loss in efficiency by Landauer's principle. Reversible classical computing involves a large overhead in terms of number of bits that need to be stored. Qunatum computing on the hand is reversible by design.

2 A brief history of Quantum Computing (1981–2000)



3 A brief history of Quantum Computing (2001–Now)



4 Quantum Computing

We now the why quantum computing is necessary, and have a brief idea of the work that has been done in the field over the last few decades. It is now our turn to study quantum computing, however, before jumping in we must study the fundamentals of quantum mechanics.

4.1 Postulates of Quantum Mechanics

Quantum mechanics is a mathematical framework for the development of physical theories. Quantum mecahnics by itself doesn't tell you what laws a physical system must obey, it provides a mathematical and conceptual framework for the development of such laws. Over the coming sections we give a description of the basic postulates of quantum mechanics. These postulates provide a connection between the physical world and the mathematical formalism of quantum mechanics.

Postulate 1. An isolated physical system has an associated complex vector space with inner product (i.e. a Hilbert space) called the state space of the system. The system is completely described a unit vector in the system's state space, called the state vector.

The most basic quantum mechanical system is the *qubit*. It is in fact the system that we will be most interested in. A qubit has a two dimensional state space (with the underlying values drawn from the complex field $\mathbb{C}^2$). Say $|0\rangle$ and $|1\rangle$ form the basis of this vector space (here, $|\psi\rangle$ is called the *ket* notation of the vector ψ). Then any arbitrary vector may be written as

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle$$

where a and b are complex numbers satisfying the condition $a^2 + b^2 = 1$ (this is equivalent to saying that the inner product $\langle\psi|\psi\rangle = 1$, where it is the *dual vector* of $|\psi\rangle$ being denoted by the *bra* notation $\langle\psi|$). This is called the *normalisation condition for vectors*.

We say that any linear combination of qubits, $|\psi\rangle = \sum_i a_i\,|\psi_i\rangle$, is a superposition of the states $|\psi_i\rangle$ with the amplitudes a_i. (In fact, when these states are orthogonal unit vectors, such as in the case of the basis vectors, the amplitude of $|\psi_i\rangle$ may found computing $\langle\psi_i|\psi\rangle$. Why?)

Any physical state that we represent in a Hilbert space is represented by a *ray* instead of a vector i.e. a one dimenionsal subspace of the Hilbert space. Therefore for all vectors $|\psi\rangle$, we have, $c\,|\psi\rangle = |\psi\rangle$, where c is a complex number.

These qubits, since they belong to a Hilbert space, satisfy all the other properties of the inner product as well – linearity of the inner product, the Schwartz inequality etc.

While we treat qubits as abstract mathematical ojbects it is essential that we are able to realise them as a physical system because quantum computing is not just a theoretical endevour.

Qubits can be realised by electron spins. Any electron has a spin, $\vec{S} = S_X\hat{i} + S_Y\hat{j} + S_Z\hat{k}$, where

$$S_X = \frac{\hbar}{2}\begin{bmatrix}0,1\\1,0\end{bmatrix} = \frac{\hbar}{2}\sigma_X, \quad S_Y = \frac{\hbar}{2}\begin{bmatrix}0,-i\\i,0\end{bmatrix} = \frac{\hbar}{2}\sigma_Y, \quad S_Z = \frac{\hbar}{2}\begin{bmatrix}0,1\\1,0\end{bmatrix} = \frac{\hbar}{2}\sigma_Z,$$

and σ_X, σ_Y, and σ_Z are called the Pauli X, Y, and Z matrices respectively ($\hbar$ is the reduced Planck's constant).

Qubits can also be realised by the polarisation of photons, where a vertically polarised photon represents $|1\rangle$, and a horizontally polarised photon represents $|0\rangle$.

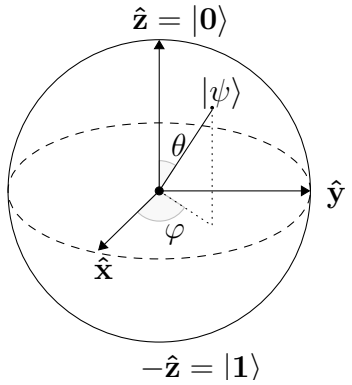
As a consequence of the normalisation condition for vectors, we can express any vector as,

$$|\psi\rangle = e^{i\lambda}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\right).$$

In fact, since any physical state is represented as ray, we have,

$$|\psi\rangle = \left(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\right).$$

The numbers θ and ϕ define a point on a three dimenionsal sphere as shown in the figure below. This is called the blochsphere reprentation of a qubit. For instance, $|0\rangle$ and $|1\rangle$ would have the parameters $(0,0)$ and $(\pi,0)$ for (θ,φ) respectively.



A 2-D reprentation of a blochsphere.

Finally, since qubits belong to a vector space it is natural to represent them as collumn vectors,

$$|0\rangle = \begin{bmatrix}1\\0\end{bmatrix}, \quad |1\rangle = \begin{bmatrix}0\\1\end{bmatrix}.$$

Postulate 2. The evolution of a closed quantum system is described by a unitary transformation. That is, the state $|\psi\rangle$ of the system at time t_1 is related to the state $|\psi'\rangle$ of the system at time t_2 by a unitary operator U which depends only on the times t_1 and t_2,

$$|\psi'\rangle = U|\psi\rangle.$$

We have seen such unitary operators in the past, such as the Pauli X, Y, and Z matrices. There exist other such operators as well. All of them can be experssed as unitary matrices.

These operators represent physical *observables*, i.e. quantities that can be measured. As a consequence of Heisenberg's uncertainty principle, for any operators to be simultaneously measurable, they must commute. In other words, for operators A and B to simultaneously measurable we must have $AB - BA = 0$. (Note that the Pauli X, Y, and Z matrices don't commute.)

Postulate 3. Quantum measurements are described by a collection $\{M_m\}$ of measurement operators. These are operators acting on the state space of the system being measured. The index m refers to the measurement outcomes that may occur in the experiment. If the state of the quantum system is $|\psi\rangle$ immediately before the measurement then the probability that result m occurs is given by,

$$p(m) = \langle\psi| M_m^\dagger M_m |\psi\rangle ,$$

and post measurement state is given by,

$$\frac{M_m |\psi\rangle}{\sqrt{\langle\psi| M_m^\dagger M_m |\psi\rangle}}.$$

The measurement operators satisfy the completeness condition,

$$\sum_i M_m^\dagger M_m = I.$$

The completeness equation expresses the fact that probabilities sum to one:

$$\sum_m p(m) = \sum_m \langle\psi| M_m^\dagger M_m |\psi\rangle = 1.$$

Closed systems evolve according to unitary evolution. However, there are times when an experimentalist must measure the value of the system. As a result of this act of measurement, the system is no longer closed, and therefore may not be subject to unitary evolution. This postulate comes in handy then.

An important example is the measurement of a qubit in the computational basis, $|0\rangle$ and $|1\rangle$. This is a measurement on a single qubit with two outcomes defined by the two measurement operators $M_0 = \langle 0|0\rangle$, $M_1 = \langle 1|1\rangle$. Each of these measurement operators satisfies the properties, $M_i^2 = M_i$. Therefore, we have $I = \sum_i M_i^\dagger M_i = \sum_i M_i$ (note that these measurement operators are Hermitian). If the state being measured is $|\psi\rangle = a|0\rangle + 1|1\rangle$, then probability of the outcome being is 0 is,

$$p(0) = \langle\psi| M_0^\dagger M_0 |\psi\rangle = \langle\psi| M_0 |\psi\rangle = |a|^2.$$

We can similarly calculate $p(1)$.

Postulate 4. The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. Moreover, if we have n systems , and system number i is prepared in the state $|\psi_i\rangle$, then the joint state of the total system is $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$.

We have dealt with 1 qubit systems so far, this postulate allows us to describe states with more than 1 qubit.

However, why are we using the tensor product to describe such a state? Here is one heuristic that is sometimes used. Physicists sometimes like to speak of the superposition principle of quantum mechanics, which states that if $|x\rangle$ and $|y\rangle$ are two states of a quantum system, then any superposition $a|x\rangle + b|y\rangle$ should also be an allowed state of a quantum system, where $a^2 + b^2 = 1$. For composite systems, it seems natural that if $|A\rangle$ is a state of system A, and $|B\rangle$ is a state of system $|B\rangle$, then there should be some corresponding state, which we might denote $|A\rangle\ |B\rangle$, of the joint system AB. Applying the superposition principle to product states of this form, we arrive at the tensor product postulate given above.

4.2 Density Matrices

We have formulated quantum mechanics using the language of state vectors. An alternate formulation is possible using a tool known as the density operator or density matrix. This alternate formulation is mathematically equivalent to the state vector approach, but it provides a much more convenient language for thinking about some commonly encountered scenarios in quantum mechanics. This is especially useful in qunatum information.

4.2.1 Ensembles of quantum states

The density operator language provides a convenient means for describing quantum systems whose state is not completely known.

Say the system exists in a state $|\psi_i\rangle$ with probability p_i, then the density matrix is defined as,

$$\rho \equiv \sum_i p_i \langle\psi_i|\psi_i\rangle .$$

If the evolution of some closed system is described by some unitary operator U, and the system is in $|\psi_i\rangle$ with probability p_i, then the after the evolution the system would be in state $U|\psi_i\rangle$ with probability p_i. Therefore, the evolution is described the density operator as,

$$\rho \equiv \sum_i p_i \langle\psi_i|\psi_i\rangle \xrightarrow{U} \sum_i p_i U \langle\psi_i|\psi_i\rangle U^\dagger = U\rho U^\dagger.$$

Measurements can also be described using density matrices. If the initial state was $|\psi_i\rangle$, then probability of us getting m is,

$$p(m|i) = \langle\psi_i| M_m^\dagger M_m |\psi_i\rangle = \mathrm{tr}\big(M_m^\dagger M_m \langle\psi_i|\psi_i\rangle\big).$$

Therefore, the probability of getting m is,

$$p(m|i) = \sum_i p(m|i)p_i = \sum_i p_i \,\mathrm{tr}\big(M_m^\dagger M_m \langle\psi_i|\psi_i\rangle\big) = \mathrm{tr}\big(M_m^\dagger M_m \rho\big)$$

Exercises

Theory Exercises

1. The following matrix H, is called the Hadamard operator,

$$\frac{1}{\sqrt{2}}\begin{bmatrix} 1, 1 \\ 1, -1 \end{bmatrix}.$$

   Verify that the Hadamard operator is unitary.

2. Verify the following statement. An operator ρ is the density operator associated to some ensemble $p_i, |\psi_i$ if and only if:

   (a) ρ has trace equal to one.

   (b) ρ is a positive operator.

3. Verify that the Pauli X, Y, and Z matrices are in fact unitary operators, and that they don't commute.

4. The vectors,

$$|+\rangle = \frac{1}{\sqrt{2}}\big(\,|0\rangle + |1\rangle\big), \quad |-\rangle = \frac{1}{\sqrt{2}}\big(\,|0\rangle - |1\rangle\big),$$

   are called the Hadamard basis vectors. Find the (θ, φ) parameters for their blochsphere reprentation.

5. We know that $|\psi\rangle = a\,|\psi\rangle$, where a is called the global phase. There is however another kind of phase called the relative phase. Two amplitudes, a and b, differ by a relative phase if $a = e^{i\theta}b$. As an example, condsider the amplitudes of $|1\rangle$ in the vectors $|+\rangle$ and $|-\rangle$ defined above. How can we find the a relative phase of a vector?

Qiskit Exercises

1. Install Qiskit and set up your programming environment as described in file `setup.pdf`.

2. Create a new notebook and learn how to carry out some basic operations using the accompanying file `intro.ipynb`.