Introduction to Quantum Computation

Week 8

Introduction

Introduction

- Quantum computing is reputed to be able to solve problems with a large state space which we couldn't solve on classical computers earlier.
    - e.g. Calculating bond lengths of molecules, transition amplitudes etc.
- This possible because of two reasons,

  Superposition quantum bits (or qubits for short), the building blocks of quantum computers can exist in a combination of states simultaneously.

  Entanglement qubits can be strongly linked together that they can exist in perfect unison even at cosmic distances.
- But why bother with quantum computers at all? Why not build a faster classical computer? It has worked out so far.

Classical Computing

Moore’s Law

- Moore’s Law is an observation, according to which the number of transistors on a chip double every two years. The observation has held well up till now.
- This is a consequence of transistor technology getting smaller. However, now transistors are approaching atomic scales, where quantum effects such as electron tunneling are leading to adverse effects on computation.

Parallel Computing

- If we can longer make a single chip faster, why don't we just use many of them?
- While this works in principle, it is difficult to implement since parallelism doesn't occur naturally in the classical model of computation. Moreover, many problems aren't parallelisable.

Reversible Computing

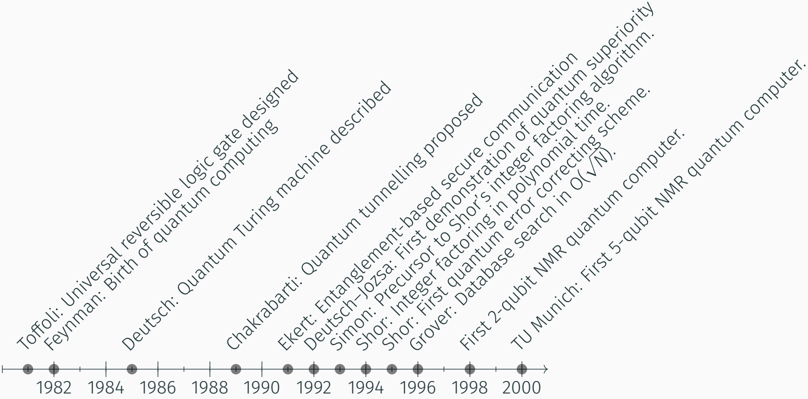
- Landauer's principle, a physical principle states that, if an observer loses information about a physical system, then they lose ability to extract work from it. In other words, losing information about a system makes it less efficient.
- The way classical computing works, most operations are irreversible because we lose out information on every step.
    - Given just the output of an AND gate, it isn't possible to tell the value of both the inputs.
- Reversible classical computing is a solution to this particular problem, but it involves considerable overhead due to additional bits that need to be stored.

Why Quantum Computing?

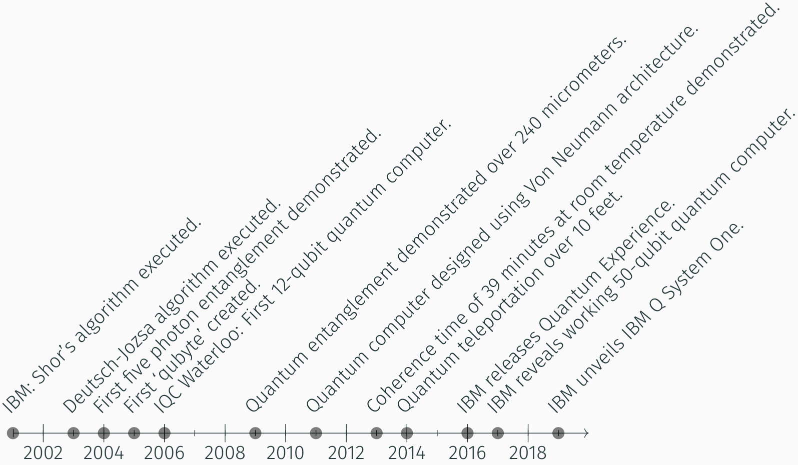
- Single processor classical computers are nearly as fast as they can be in terms of number of transistors on chip. We need an alternative.
- Parallel computers exist, however they are difficult to use (when they can be used) since the parallelism in computation isn’t natural as opposed to quantum computers.
- 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. Quantum computing on the hand is reversible by design.

A Brief History of Quantum Computing

1981 – 2000


Toffoli: Universal reversible logic gate designed
Feynman: Birth of quantum computing
Deutsch: Quantum Turing machine described
Chakrabarti: Quantum tunnelling proposed
Ekert: Entanglement-based secure communication
Deutsch–Jozsa: First demonstration of quantum superiority
Simon: Precursor to Shor's integer factoring algorithm.
Shor: Integer factoring in polynomial time.
Shor: First quantum error correcting scheme.
Grover: Database search in $O(\sqrt{N})$.
First 2-qubit NMR quantum computer.
TU Munich: First 5-qubit NMR quantum computer.
1982
1984
1986
1988
1990
1992
1994
1996
1998
2000

2001 – Now


IBM: Shor's algorithm executed.
Deutsch-Jozsa algorithm executed.
First five photon entanglement demonstrated.
First 'qubyte' created.
IQC Waterloo: First 12-qubit quantum computer.
Quantum entanglement demonstrated over 240 micrometers.
Quantum computer designed using Von Neumann architecture.
Coherence time of 39 minutes at room temperature demonstrated.
Quantum teleportation over 10 feet.
IBM releases Quantum Experience.
IBM reveals working 50-qubit quantum computer.
IBM unveils IBM Q System One.
2002
2004
2006
2008
2010
2012
2014
2016
2018

Quantum Computing

Postulate 1 i

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.

Postulate 1 ii

- The quantum system we are most interested in is the qubit.
- Any qubit may written as a linear combination of it's vector spaces basis vectors as $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$ where a a and b are complex numbers satisfying the condition $a^2 + b^2 = 1$.
- Any physical state that we represent in a Hilbert space is represented by a *ray* instead of a vector i.e. a one dimensional subspace of the Hilbert space. Therefore for all vectors $|\psi\rangle$, we have, $c\,|\psi\rangle = |\psi\rangle$, where c is a complex number.

Postulate 1 iii

- While we treat qubits as abstract mathematical objects it is essential that we are able to realise them as a physical system because quantum computing is not just a theoretical endeavor.
- Qubits can be realised as the electron spins, and polarisation of photons.

Postulate 1 iv

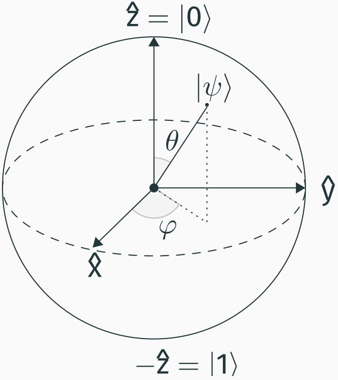
As a consequence of the normalisation condition for vectors, we can express any vector as,

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

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 dimensional sphere as shown in the figure below. This is called the blochsphere representation 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.

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,

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

- Operators such as that act on vectors, must be unitary matrices.

Postulate 3 i

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,

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

Postulate 3 ii

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 are described by unitary evolution. However, when we are measuring a system, it is no longer closed. Thus, this postulate allows us to measure systems.

The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. That is, 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 $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$.

- Up until now we have only discussed single qubit systems. This postulate helps describe multiple qubit systems.