Quantum Computers

Deepti
III Sem, MCA
Christ University

Evolution of Classical computers

- First generation(1939-’54)-Vacuum tubes
- Second generation(1954-’59)-Transistors
- Third generation(1959-’71)- IC
- Fourth generation(1971-’91)- Microprocessor
- Fifth generation(1991 & beyond)

Introduction

- Gordon Moore, Intel Co-founder said that the number of transistors economically crammed into a single computer chip was doubling every two years.

Classical Computers

- Accurate and speedy computation machine
- Part of life because logical work can also be done
- Advantages
  - Makes work easy and faster
  - Any complex computation or logical work like laboratory work become easy

- Many kinds of numerical problems cannot be solved using conventional computers.
- Example: Factorization of a number
- The computer time required to factor an integer containing N digits is believed to increase exponentially with N.

History

- In 1918- Max Planck's -Energy quantum
- In 1921-Einstein's discovery of the photon
- In 1980- Idea of quantum computation
- In 1994, Shor's algorithm was able to factorize large integers in polynomial time using quantum approach.
- In 1996, Grover's came up with an algorithm to search a name in unsorted database.

Concepts of quantum computers..

Qubit

- A quantum bit or qubit is a unit of quantum information.
- Many different physical objects can be used as qubits such as atoms, photons, or electrons.
- Exists as a ‘0’, a ‘1’ or simultaneously as a superposition of both ‘0’ & ‘1’

Quantum information

- Quantum information is physical information that is held in the "state" of a quantum system.

- Though the amount of information that can be retrieved in a single qubit is equal to one bit, the difference lies in the processing of information

Quantum superposition

- An electron has dual nature.
- It can exhibit as a particle and also as wave.
- Wave exhibits a phenomenon known as superposition of waves.
- This phenomena allows the addition of waves numerically.

Conti…

- Superpositions occur all the time at the quantum level.
  - i.e any quantum object like a electron or photon is in superposition

Decoherence

- As the number of Qubits increases, the influence of external environment perturbs the system.
- This causes the states in the computer to change in a way that is completely unintended and is unpredictable, rendering the computer useless.
- This is called decoherence.

Quantum entanglement

- In Quantum Mechanics, it sometimes occurs that a measurement of one particle will effect the state of another particle, even though classically there is no direct interaction.

- When this happens, the state of the two particles is said to be entangled.

Quantum Entanglement

UNLIKE ORDINARY BITS of information, qubits can be linked in a way that has no analog in the digital world. This linkage, called entanglement, acts instantaneously over any distance.

LASER

1 Two qubits are entangled through the action of a laser.

2 Once they have been entangled, they are in an indeterminate state.

3 The qubits can then be separated by any distance, but they will remain linked.

4 When one of the qubits is manipulated—say, to perform a step in a quantum computer program—the manipulation happens instantly to its entangled twin as well.

5 If the manipulation includes reading the state of one of the qubits, the entanglement ends, and both qubits' states are revealed.

Building a quantum computer

- A quantum computer is nothing like a classical computer in design; transistors and diodes cannot be used.

- A new type of technology is needed, a technology that enables 'qubits' to exist as coherent superposition of 0 and 1 states.

Quantum Dots

- It is one of the possible ways to produce quantum computers.
- A single electron trapped inside a cage of atoms.
- When the dot is exposed to a pulse of laser light of the right wavelength & duration, the electron is raised to an excited state: a second burst of laser light causes the electron to fall back to its ground state.
- Ex: NOT gate

Computing liquids

- The quantum computer in this technique is the molecule itself and its qubits are the nuclei within the molecule – a 'mug' of liquid molecules.

- Advantage: Though the molecules of the liquid bump into one another, the spin states of the nuclei within each molecule remain unchanged.

Quantum teleportation

- Quantum teleportation is a technique used to transfer information on a quantum level, usually from one particle to another.

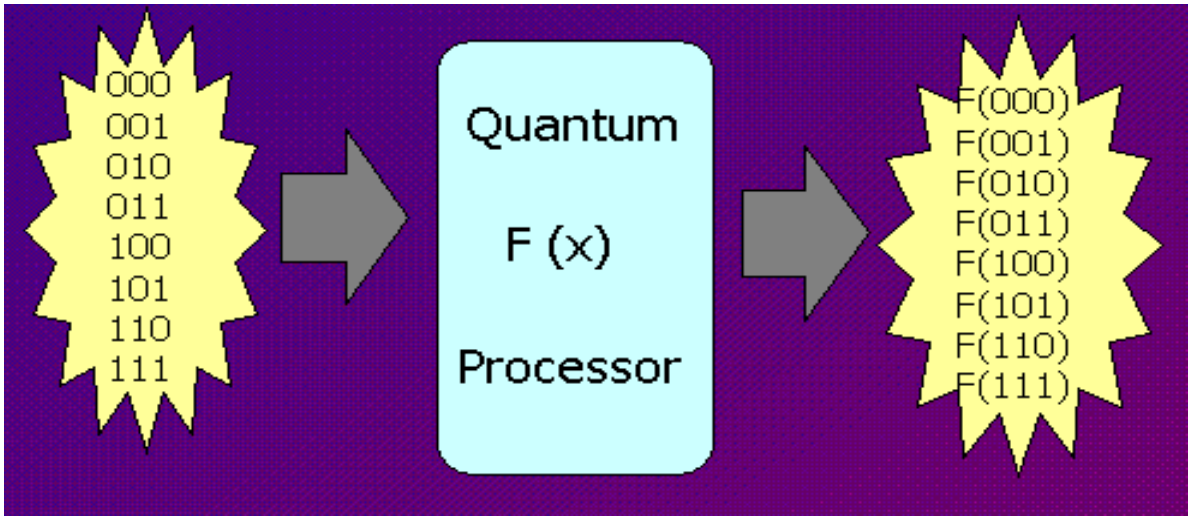
- Its distinguishing feature is that it can transmit the information present in a quantum superposition, useful for quantum communication and computation.

Classical Facsimile Transmission

Quantum Teleportation

Quantum parallelism

- It is the method in which a quantum computer is able to perform two or more computations simultaneously.
- In classical computers, parallel computing is performed by having several processors linked together.
- In a quantum computer, a single quantum processor is able to perform multiple computations on its own.



- Parallelism allows a quantum computer to work on many computation at once.

Issues in Implementation

- Key technical challenge: prevent decoherence or unwanted interaction with environment
- Larger computations will require quantum error-correcting codes

Applications

Quantum networking

- One possible use of quantum computers is that of networking, both intranet and internet.
- Quantum teleportation using light beams may be able to carry a great deal more information, enough perhaps to support practical computing.
- But the issue in this is, creating large enough beams of light in both locations, sending and receiving, to send all of the data within a reasonable amount of time.

Encryption

- Current encryption methods work by factoring numbers.
  - Ex. 12=2*2*3.
  - Very easy to do for small numbers.

- Current encryption numbers use over 400 digits in size.
  - Today's computers would take about a billion years to factor these numbers.

- A quantum computer with a similar performance as modern computers would need seconds.

Ultra-secure & Super-dense Communications

- It is possible to transmit information without a signal path by using quantum teleportation.
  - There is no way to intercept the path and extract information.

- Ultra-secure communication is also possible by super-dense information coding where quantum bits can be used to allow more information to be communicated per bit than the same number of classical bits.

Molecular Simulations

- A quantum computer can simulate physical processes of quantum effects in real time.
- Molecular simulations of chemical interactions.
- Allows chemists and pharmacists to learn more about how their products interact with each other, and with biological processes.
  - Ex: How a drug may interact with a person's metabolism or disease.

True Randomness

- Classical computers do not have the ability to generate true random numbers i.e. there is always a cycle or a trend.

- Quantum computers can generate true randomness, thus give more veracity to programs that need true randomness in their processing.

Need for Quantum computers

- Quantum computers work on an atomic level
  - That is roughly 200 times smaller than Intel's brand new 45nm architecture.
- Would be very useful in research and algorithm computation

Cont…

- Scaling
- Energy
- Economic

Current challenges

- Number of bits in a word.
  - 12-qubit machines is the most advanced to date.
  - Difficulty with large words is, too much quantum interaction can produce undesired results. Since all the atoms interact with each other.
- Physical size of the machines.
  - Current machines are too large to be of practical use to everyday society.

Conti…

- If these drawbacks could be overcome and if scientists could control even 50 atoms, researchers claim that the computing power of that computer would be more than the current supercomputers.

Future prospects

- When processor components reach atomic scale, Moore's Law breaks down
  - Quantum effects become important whether we want them or not

But huge obstacles in building a practical quantum computer!

Conclusion

- Quantum Computing could provide a radical change in the way computation is performed.
- The advantages of Quantum Computing lie in the aspects of Quantum Mechanics that are peculiar to it, most notably entanglement.
- Classical Computers will be significantly larger than Quantum Computers for the foreseeable future.

THANK YOU !!!