Introduction to quantum computing — Professor Elías Fernández-Combarro Álvarez
(Universidad de Oviedo)

Lecture 1

Part 1 - Definitions

Quantum Computing is a computing paradigm that exploits quantum mechanical properties (superposition, entanglement, interference...) of matter in order to do calculations

Models of Quantum computing

- Quantum Turing machines
- Quantum Circuits
- Measurement based Quantum computing (MBQC)
- Adiabatic quantum computing
- Topological quantum computing

Regarding computacional capabilities, they are equivalent to Turing Machines

What technologies are used to build quantum computers?

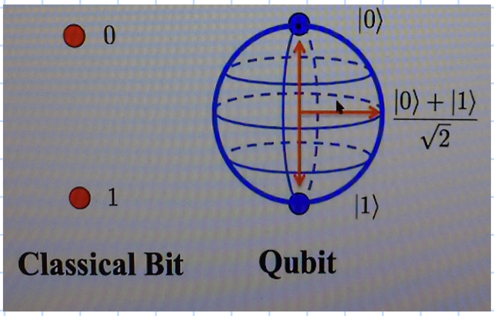
- Superconducting Loops
- Trapped ions
- Diamond Vacancies
- Silicon Quantum dots
- Topological qubits

mainly used by Google, IBM, etc...

Elements of a Quantum Circuit

- Data → qubits
- Operations → quantum gates (unitary transformations)
- Results → measurements

Part 2 - One-qubit Systems



- Classical bits can take two values (1 or 0). → Discrete
- Qubit can "take" infinitely many different values → Continuous
- Qubit live in Hilbert Vector Space with a basis of two elements $|0\rangle$ y $|1\rangle$
- A generic qubit is in a superposition

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$ where α and β are complex numbers such that $|\alpha|^2 + |\beta|^2 = 1$

- The way to know the value of a qubit is to perform a measurement. However
    - The result of a measurement is random
    - When we measure, we only obtain one (classical) bit of information

- Measuring: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \implies \begin{array}{l} 0 \to |\alpha|^2 \text{ probability} \\ 1 \to |\beta|^2 \text{ probability} \end{array}$

- So, the result after measuring will be $|0\rangle$ or $|1\rangle$ depending of the result

- We cannot perform independent measures of $|\psi\rangle$ because we cannot copy the state (no-cloning theorem)

Quantum Gates

- Quantum Mechanics tells us that the evolution of an isolated state is given by Schrödinger equation $\longrightarrow$ $H(t)|\psi(t)\rangle = i\hbar\frac{\partial}{\partial t}|\psi(t)\rangle$

- In the case of quantum circuits, this implies that the operations that can be carried out are given by unitary matrices. That is, matrices U of complex numbers verifying

$$U.U^{+} = U^{+}.U = I$$

where U^{-1} is the conjugate transpose of U

- Each such matrix is a possible quantum gate in a circuit

Reversible Computation

- All the operations have an inverse: reversible computing
- Every gate has the same number of inputs and outputs
- We cannot directly implement some classical gates
- But we can simulate any classical computation

One-Qubit gates

- Qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \xrightarrow{\text{represented}} \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$

- One-Qubit gate can be represented with a transformation matrix

$U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ that satisfies $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$\bar{a}, \bar{b}, \bar{c}, \bar{d}$ conjugates of complex numbers a, b, c, d

- A state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is transformed

to: $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} a\alpha + b\beta \\ c\alpha + d\beta \end{pmatrix}$

that is: $|\psi\rangle = (a.\alpha + b.\beta).|0\rangle + (c\alpha + d\beta).|1\rangle$

- Since it is unitary $\rightarrow$ $|a\alpha + b\beta|^2 + |c\alpha + d\beta|^2 = 1$

X-Gate (Not)

- $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ $\rightarrow$ X-Gate Unitary Matrix

- In Quantum Circuit:

  $|0\rangle - \boxed{X} - |1\rangle$

  $|1\rangle - \boxed{X} - |0\rangle$

  it acts like the classical NOT gate

- On a general qubit

  $\alpha|0\rangle + \beta|1\rangle - \boxed{X} - \beta|0\rangle + \alpha|1\rangle$

Z-Gate

- $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

- $|0\rangle - \boxed{Z} - |0\rangle$

  $|1\rangle - \boxed{Z} - -|1\rangle$

H-Gate (Hadamard Gate)

- $\frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

- $|0\rangle - \boxed{H} - \frac{|0\rangle + |1\rangle}{\sqrt{2}}$

  $|1\rangle - \boxed{H} - \frac{|0\rangle - |1\rangle}{\sqrt{2}}$

- Usually denote:

  $|+\rangle := \frac{|0\rangle + |1\rangle}{\sqrt{2}}$

  $|-\rangle := \frac{|0\rangle - |1\rangle}{\sqrt{2}}$