Quantum Computing

Lecture 1

Anuj Dawar

Bits and Qubits

What is Quantum Computing?

Aim to use quantum mechanical phenomena that have no classical counterpart for computational purposes.

Central research tasks include:

- *Building devices* — with a specified behaviour.
- *Designing algorithms* — to use the behaviour.

Mediating these two are models of computation.

Bird's eye view

A computer scientist looks at Quantum Computing:

Algorithmic Languages

Theory/complexity

System Architecture

____Specified Behaviour

Physics

Dragons

Why look at Quantum Computing?

- *The world is quantum*
  - classical models of computation provide a level of abstraction
  - discrete state systems
- *Devices are getting smaller*
  - Moore's law
  - the only descriptions that work on the very small scale are quantum
- *Exploit quantum phenomena*
  - using quantum phenomena may allow us to perform computational tasks that are not otherwise possible/efficient
  - understand capabilities/resources

Course Outline

A total of eight lecturers.

1. *Bits and Qubits* (this lecture).
2. *Linear Algebra*
3. *Quantum Mechanics*
4. *Models of Computation*
5. *Some Applications*
6. *Search Algorithms*
7. *Factorisation*
8. *Complexity*

Useful Information

Some useful books:

- Nielsen, M.A. and Chuang, I.L. (2010). *Quantum Computation and Quantum Information*. 2nd ed. Cambridge University Press.
- Mermin, N.D. (2007). *Quantum Computer Science*. CUP.
- Kitaev, A.Y., Shen, A.H. and Vyalyi, M.N. (2002). *Classical and Quantum Computation*. AMS.

Course website:

`http://www.cl.cam.ac.uk/teaching/1213/QuantComp/`

Bits

A building block of classical computational devices is a two-state system.

$$0 \quad \longleftrightarrow \quad 1$$

Indeed, any system with a finite set of *discrete, stable* states, with controlled transitions between them will do.

Qubits

Quantum mechanics tells us that any such system can exist in a *superposition* of states.

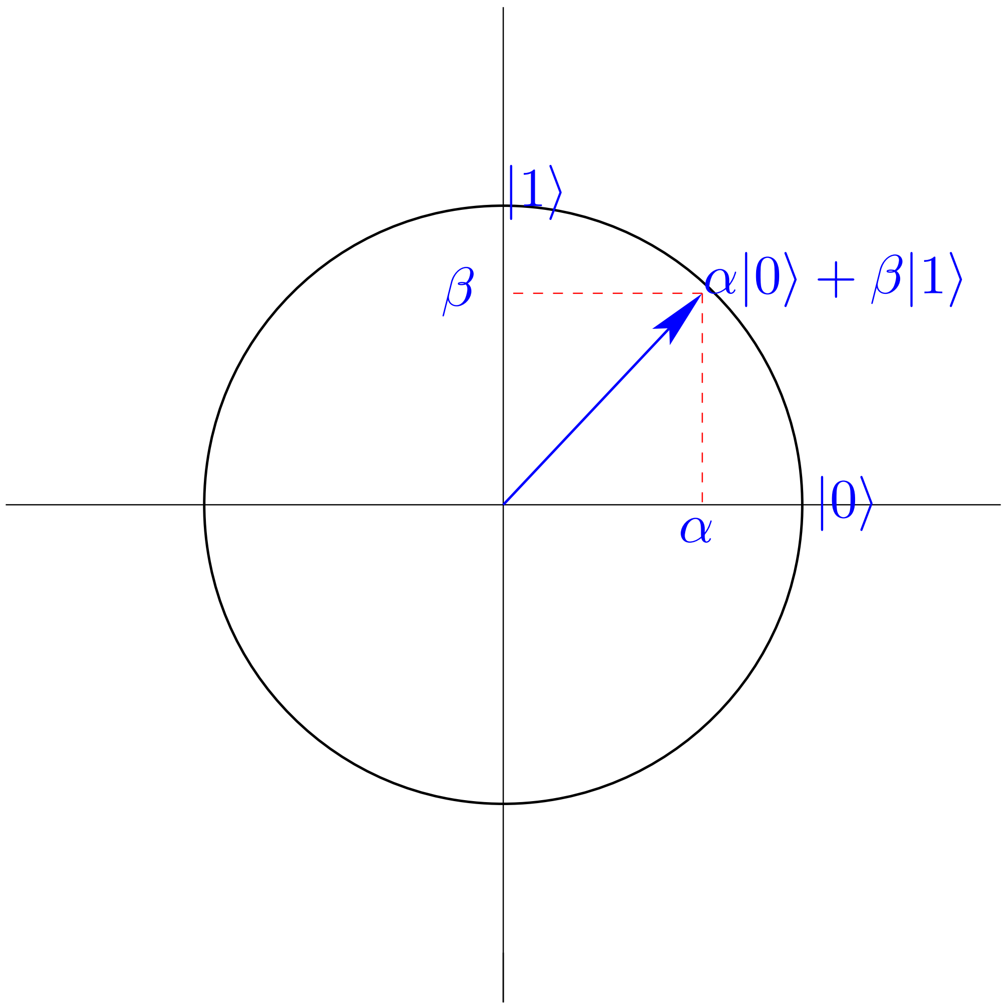
In general, the state of a *quantum bit* (or *qubit* for short) is described by:

$$\alpha|0\rangle + \beta|1\rangle$$

where, α and β are complex numbers, satisfying

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

Qubits



A qubit may be visualised as a unit vector on the plane.

In general, however, α and β are *complex* numbers.

Measurement

Any attempt to measure the state

$$\alpha|0\rangle + \beta|1\rangle$$

results in $|0\rangle$ with probability $|\alpha|^2$, and $|1\rangle$ with probability $|\beta|^2$.

After the measurement, the system is in the measured state!

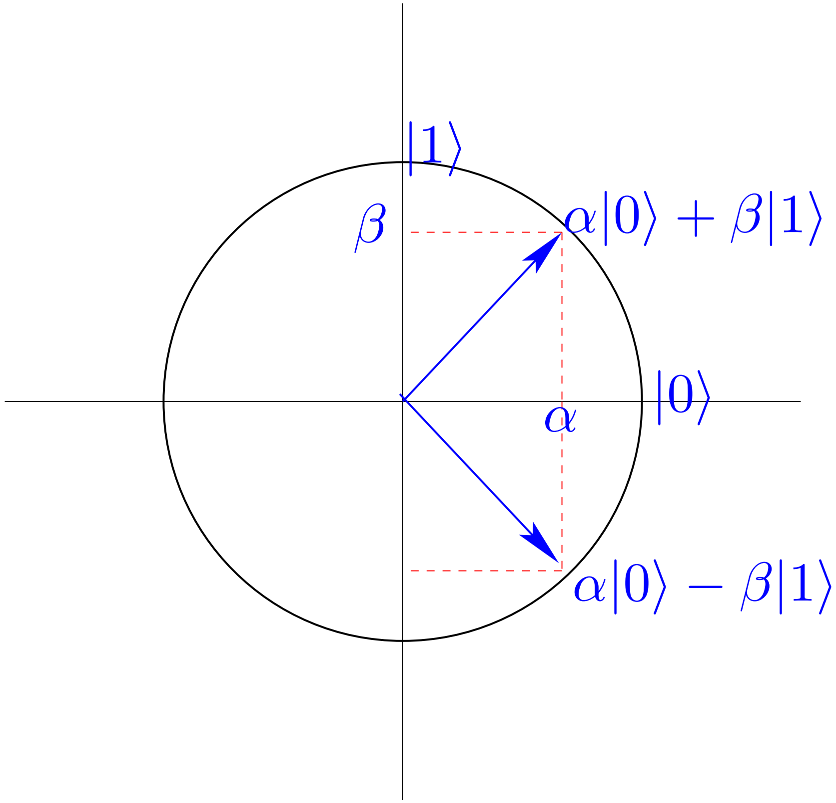
That is, further measurements will always yield the same value.

We can only extract one bit of information from the state of a qubit.

Measurement

$\alpha|0\rangle + \beta|1\rangle$ and $\alpha|0\rangle - \beta|1\rangle$ have the same probabilities for their measurement

However, they are *distinct* states which behave differently in terms of how they evolve.



Vectors

Formally, the state of a qubit is a unit vector in $\mathbb{C}^2$—the 2-dimensional complex *vector space*.

The vector $\begin{bmatrix} \alpha \\ \beta \end{bmatrix}$ can be written as

$$\alpha|0\rangle + \beta|1\rangle$$

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

$|\phi\rangle$— a *ket*, Dirac notation for vectors.

Basis

Any pair of vectors $|\phi\rangle, |\psi\rangle \in \mathbb{C}^2$ that are linearly independent could serve as a basis.

$$\alpha|0\rangle + \beta|1\rangle = \alpha'|\phi\rangle + \beta'|\psi\rangle$$

The basis is determined by the measurement process or device.

Most of the time, we assume a standard (orthonormal) basis $|0\rangle$ and $|1\rangle$ is given.

This will be called the *computational basis*

Example

The vector $\begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}$ measured in the computational basis gives either outcome with probability $1/2$.

Measured in the basis

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

it gives the first outcome with probability 1.

Entanglement

An n-qubit system can exist in any superposition of the 2^n *basis* states.

$$\alpha_0|000000\rangle + \alpha_1|000001\rangle + \cdots + \alpha_{2^n-1}|111111\rangle$$

with $\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1$

Sometimes such a state can be decomposed into the states of individual bits

$$\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

Entanglement

Compare the two (2-qubit) states:

$$\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle) \quad \text{and} \quad \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

If we measure the first qubit in the first case, we see $|0\rangle$ with probability 1 and the state remains unchanged.

In the second case (*an EPR pair*), measuring the first bit gives $|0\rangle$ or $|1\rangle$ with equal probability. After this, the second qubit is also determined.