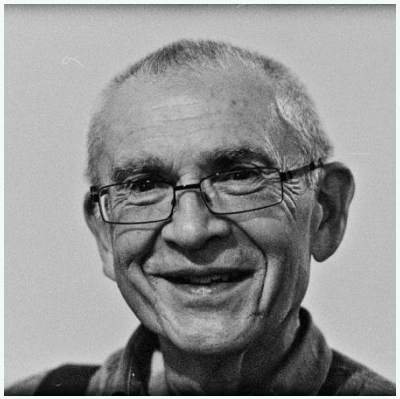
Quantum Computing: An Introduction

Khalid Muhammad

- History of Quantum Computing
- Bits and Qubits
- Problems with the Quantum Machine

Who Introduced the Idea?



Soviet scientist Yuri Manin in the book: *Vychislimoe i nevychislimoe* published in 1980 originally written in Russian.

The idea was described in further detail by the American scientist Richard Feynmann on May 7th 1981 during a speech: ***Simulating physics with computers,*** delivered at the California Institute of Technology

What are Quantum Computers?

- Normal computers what we may one day come to call ‘classical computers’ follow classical rules of physics which involve only one state.
- Quantum computers overcome this through the implementation of quantum mechanical two state systems, where there is no confining to two basic states but instead existence as a superposition.

Bits and Qubits

- An ordinary bit is a physical system which can be prepared in one of the two different states representing two logical values, for example 0 or 1.
- Quantum bits, i.e. qubits however exist in superpositions, thus effectively a qubit is both in state 0 and state 1, reminiscent of Erwin Schrödinger's cat.
- Therefore a 16-bit quantum machine can be in 2^16, or 65,536, states at once, while a 128-qubit device could occupy 3.4 x 10^38 different configurations.

Problems with the Quantum machine

- Answers given by a quantum machine are probabilistic. Therefore might be wrong and must be checked.
- If a given solution is wrong, the calculation must be repeated until the correct answer emerges. This hampers the speed of processing correct information.
- However a phenomenon in quantum mechanics known as interference can override such an issue.

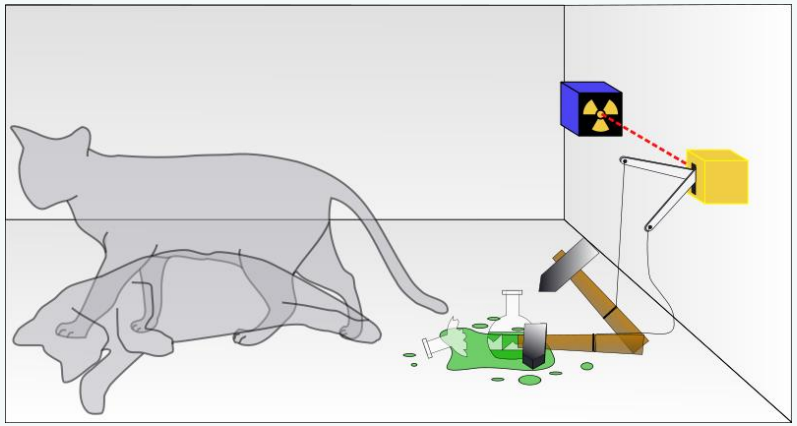
The physics behind Quantum Computers

Nick Harden

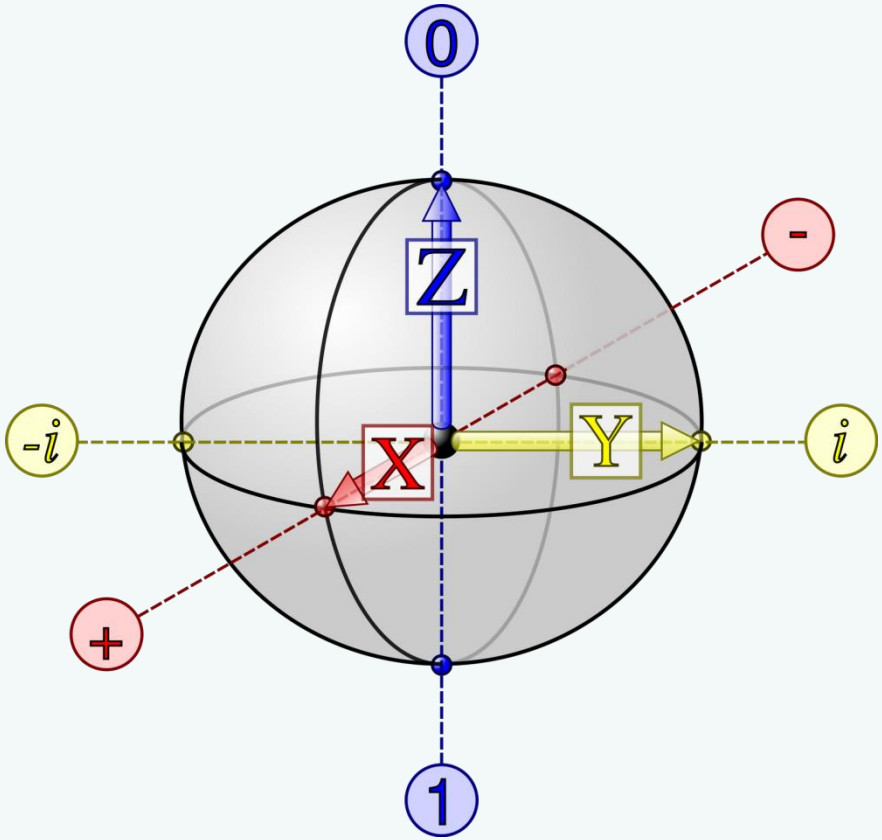
- Quantum Superposition
- Qubits
- Quantum Entanglement

Quantum Superposition

- A physical system that can be in a number of theoretical states exists simultaneously in all its states until it is observed.
- Qubits, unlike classical bits, experience quantum superposition.



Qubits

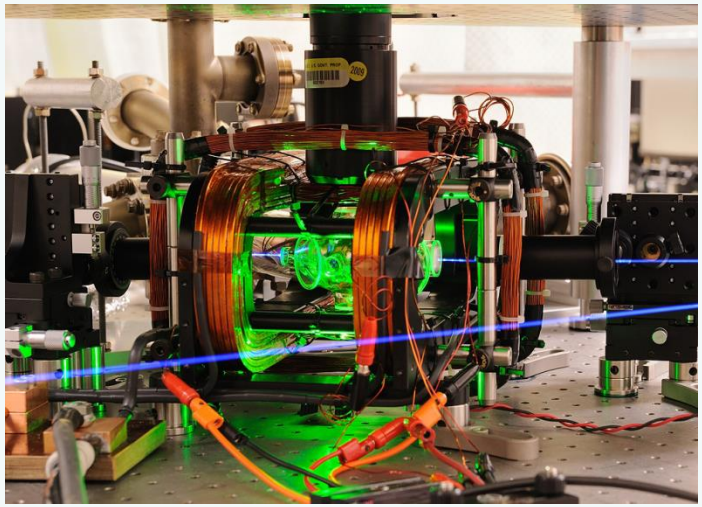


Quantum Entanglement

- Observing a qubit will collapse its wavefunction, therefore we need to find a way to gain information from qubits without observing them.
- We do this through quantum entanglement.

Control and manipulation of Qubits

- Various methods, mostly involving the use of electric and magnetic fields, are used to manipulate qubits.
- This is a set of an Ion Trap, which can be used to manipulate qubits.



Computing with Qubits

Jaime van Oers

- Classical Computing
- Logical operators
- Qubit Computing

Classical Computing

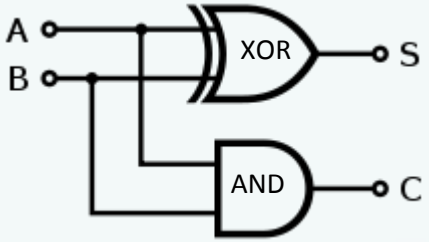
1: 0 0 1

5: 1 0 1

```
  0 0 1
  1 0 1
-------
Sum:  1 0 0
      -\-\-
Carry: 0 1 -
-------
Final: 1 1 0  : 6
```

XOR: If the two inputs are the same, output 0, if different, output 1.

AND: Only outputs 1 if both inputs are 1.



Qubit systems

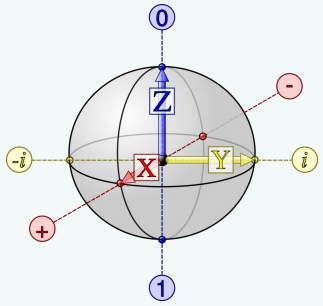
1 qubit system:

$|0\rangle$ is the '0' result eigenstate

$|1\rangle$ is the '1' result eigenstate

System: $\Psi = c_0|0\rangle + c_1|1\rangle$

$$\Psi = \begin{pmatrix} c_0 \\ c_1 \end{pmatrix}$$



2 qubit system:

$|00\rangle$ is the '0 0' result eigenstate

$|01\rangle$ etc.

$$\Psi = \begin{pmatrix} c_{00} \\ c_{01} \\ c_{10} \\ c_{11} \end{pmatrix}$$

$\Psi = c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle$

Qubit logic gates

$$\mathrm{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Controlled NOT

2 qubit system, maps:

$|00\rangle \rightarrow |00\rangle$
$|01\rangle \rightarrow |01\rangle$
$|10\rangle \rightarrow |11\rangle$
$|11\rangle \rightarrow |10\rangle$

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

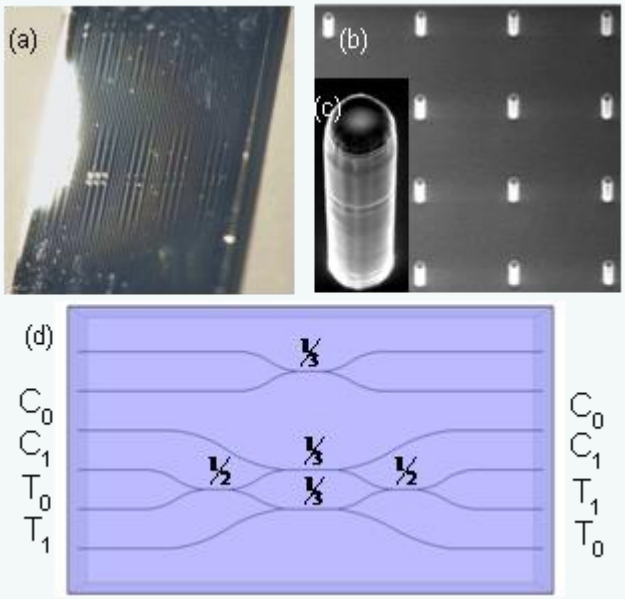
Hadamard gate

1 qubit system, maps:

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

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

Optical gate



Qubit logic gates

$$\mathrm{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Controlled NOT

2 qubit system, maps:

$|00\rangle \rightarrow |00\rangle$
$|01\rangle \rightarrow |01\rangle$
$|10\rangle \rightarrow |11\rangle$
$|11\rangle \rightarrow |10\rangle$

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Hadamard gate

1 qubit system, maps:

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

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

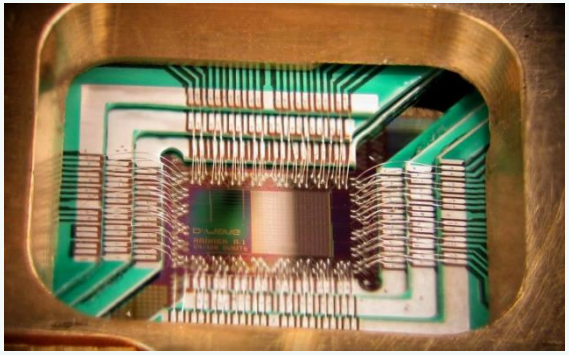
From here to the future

Luca Fruzza

- Adiabatic Quantum Computing
- D-Wave Quantum Computer
- Encryption
- Shor's Algorithm

D-Wave

The Quantum Computing Company™



Adiabatic Quantum Computing

- A system using a pool of qubits rather than individual logic gates.
- The pool of qubits naturally seeks it's lowest energy state.
- Adjusting a system so that this lowest energy state gives the answer is the premise of AQC.

Making the grade?

- In spring 2012 a 4-bit “quantum computer” factorised 143 into its prime factors, using AQC technology.

But is it spooky enough?

- In march of this year, D-Wave developed qubit tunnelling spectroscopy, to determine whether the energy of the qubits in their “quantum computers” correspond to an entangled system.
- There is strong evidence to show that D-wave has managed to use entangled qubits.

Defining D-wave as quantum

- The entanglement of the system must be shown to yield a superior performance for it to be considered a quantum computer.

Encryption Systems

- Encryption systems protect data from third parties using different encoding methods. One of these methods relies on factorising numbers into their prime constituent factors.

Shor's Algorithm

- An algorithm developed by Peter Shor, designed to utilise the Parallelism of the qubit. It's purpose is to factorise numbers into their prime constituents.

Advantages of the Algorithm

- Carried out by a normal computer, the task of factorising numbers larger than 200 into their prime constituents would take in excess of 1,000,000,000 years.
- A quantum computer running Shor's algorithm would do it in 8 hours.

- The consequences of someone having a quantum computer capable of running this today would make the internet a lot less safe place.