

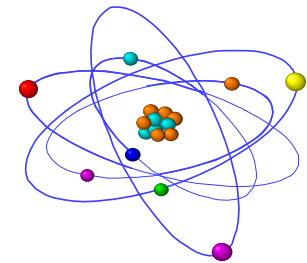
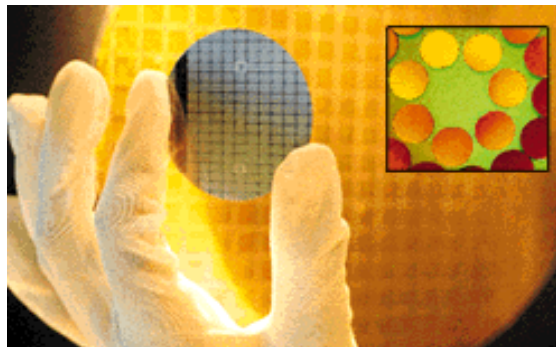
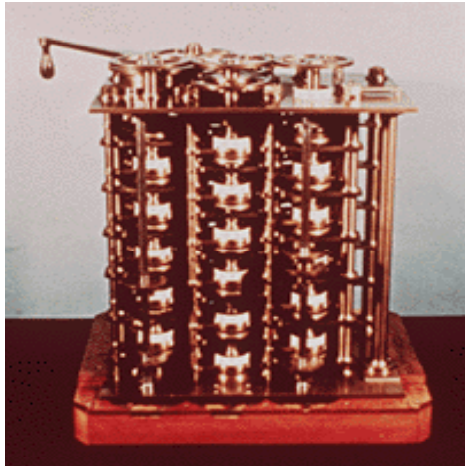
Quantum Computing - Next-Generation Computers

Dr. Steven R Skinner

Dr. Preethika Kumar

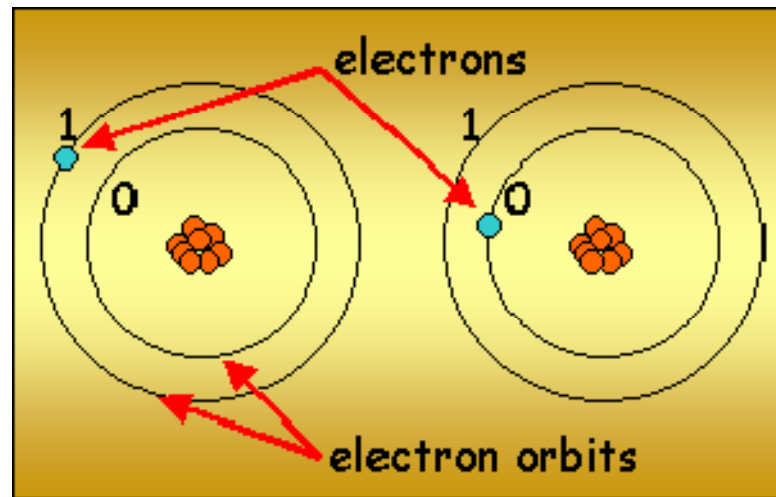
The nineteenth century was known as the machine age, the twentieth century will go down in history as the information age. I believe the twenty-first century will be the quantum age. Paul Davies, Professor Natural Philosophy – Australian Centre for Astrobiology

Computing Device Sizes



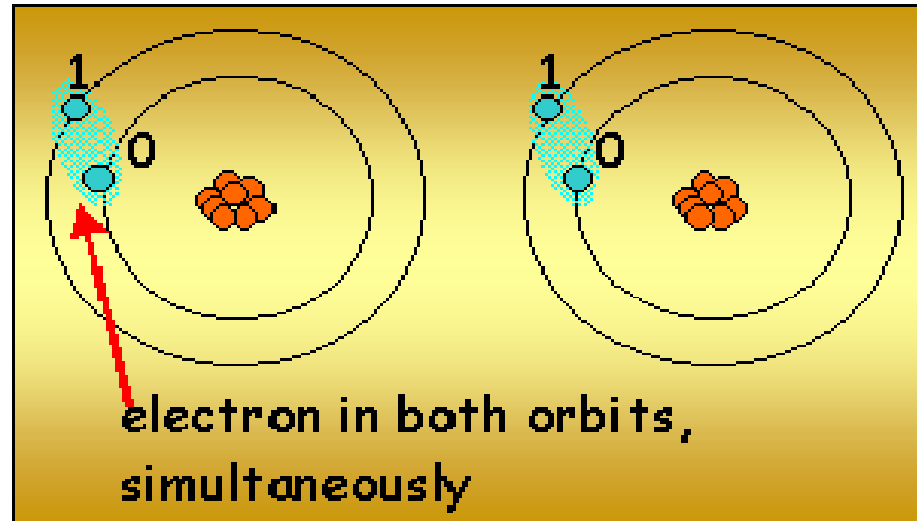
- Computer technology is making devices smaller and smaller
- Reaching a point where classical physics is no longer a suitable model

Single Electron Device



- The orbits available to a single outermost electron in each atom can be used to represent the two bit values, logic 0 and 1.
- Given quantum nature of electrons: **Qubits**

Quantum Nature of Qubits



- Electrons have a property that allows them to be in the two orbits (logic values) simultaneously: **Quantum Superposition**.
- Allows many computations to be performed simultaneously: **Quantum Parallelism**.

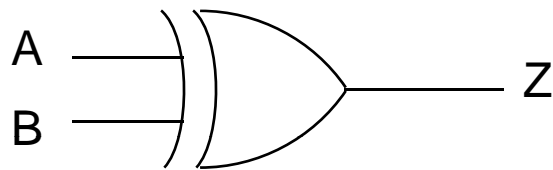
Quantum Logic States

- Quantum two level system
 - $|0\rangle$ and $|1\rangle$ are *states*
- General state is a superposition
 - $\psi = \alpha|0\rangle + \beta|1\rangle$
- Result of measurement:
 - $|0\rangle$ with probability $|\alpha|^2$
 - $|1\rangle$ with probability $|\beta|^2$

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

Classical and Quantum Gates

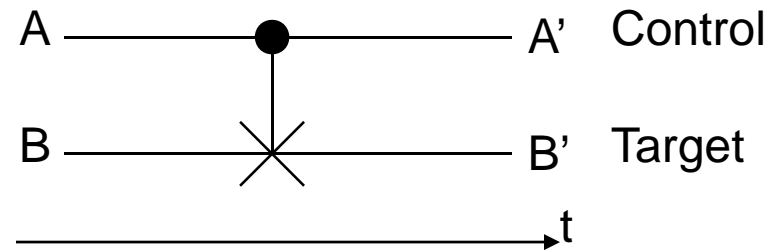
XOR (Controlled-Not)



A	B	Z
0	0	0
0	1	1
1	0	1
1	1	0

Classical

Controlled-Not (CNOT)



AB	A'B'
$ 00\rangle$	$ 00\rangle$
$ 01\rangle$	$ 01\rangle$
$ 10\rangle$	$ 11\rangle$
$ 11\rangle$	$ 10\rangle$

Quantum

Quantum Computing Research

- Quantum Devices (EE and Physics)
- Quantum Circuits (EE and CE)
 - CNOT and Toffoli Gate Designs
 - Universal Gate Design
 - Shift Register (quantum wire) Design
- Quantum Architectures (CE and EE)
 - Linear (1-D) Nearest Neighbor Designs
 - 2-D NN Computing Designs
- Quantum Algorithms (CS)

Quantum Algorithms

- Quantum algorithms are being developed that use quantum parallelism, interference, and entanglement in order to solve astronomically hard problems
- Examples:
 - Simulation of quantum mechanical systems
 - Grover's Search Algorithm
 - N items in $N^{1/2}$ steps (instead of N)
 - Shor's Factoring Algorithm

Shor's Factoring Algorithm

- In 1994, Peter Shor developed a quantum algorithm for factoring an N-digit number using only $\sim N^2$ steps
- Best *known* classical algorithm uses $\sim 2^{N^{1/3}}$ steps
- Can be used to break RSA (Rivest, Shamir, Adleman) public-key cryptography system

Any Questions?

