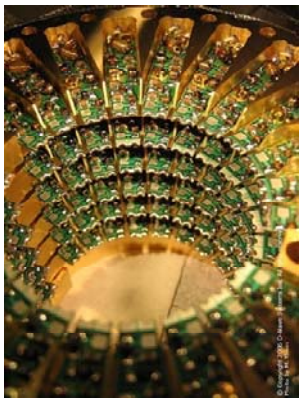
CS 190C
Science Education in Computational Thinking



QUANTUM COMPUTING:

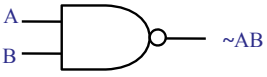
- Hardware encoding
- Computations
- Current reality

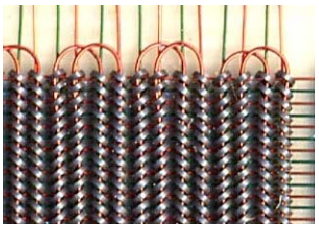
Hoffmann, 2008

Conventional Computing

- Manipulates binary numbers 0 and 1
  - Bits encoded by current strength or magnetic state
  - Manipulated by gates and combinational circuits such as NAND, NOR, etc.
  - Transistor is underlying technology for switching
- With *n* bits memory, can be in one of 2^n states.

NAND	0	1
0	1	1
1	1	0

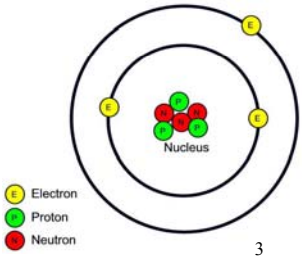




2

Atoms

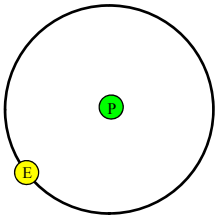
- Elementary particles paradox
- Ernest Rutherford model – 1911
- Niels Bohr model – 1913
  - Quantization of momentum
  - Refinements by
    - Erwin Schrödinger
    - Werner Heisenberg
- Wave/particle issue:
    - Louis de Broglie



3

Quantum Matters

- Coding at the elementary particle level:
  - Instead of encoding by current, encode states by state of atoms. For hydrogen
    - Primary state $|0\rangle$ electron in lowest orbit
    - Excited state $|1\rangle$ electron in first elevated orbit
- We do not know the quantum state (qubit)
  - State is determined by measurement and depends on the interaction with the observer



4

Superposition Principle

- If a quantum system can be in one state A as well as in another state B, then it also can be in a mixed state $uA+vB$, where $|u^2|+|v^2| = 1$, and u and v are complex numbers
  - Example 1: spin (up or down)
  - Example 2: electron state (ground or excited)
- Analogy: Toss a fair coin…

5

Qubit (Quantum Bit) State

- By superposition principle, a set of n qubits can be in "all" of 2^n states:

$$a_0|00\rangle + a_1|01\rangle + a_2|10\rangle + a_3|11\rangle$$

- The $|a_k|^2$ are the probability of seeing state k when "reading" the system state.
- Note $\sum_k |a_k|^2 = 1$

6

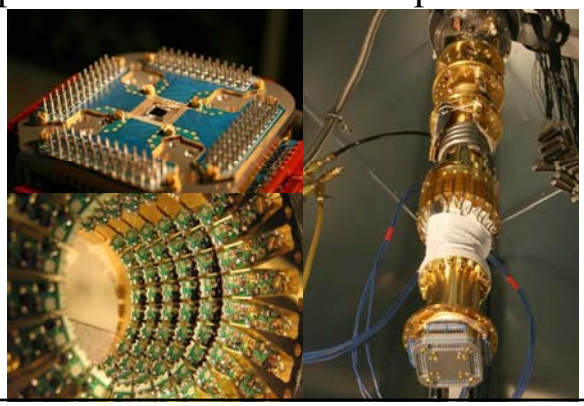
Entanglement

- Quantum states of two or more objects are somehow linked together even though they may be spatially separated.
- Example:
  - Spin is random; measure spin; the larger the sample of objects, the more the outcome tends to half up and half down
  - For two entangled objects: as soon as one spin has been measured, the other is fixed; outcomes are either $|0\rangle_A|1\rangle_B$ or $|1\rangle_A|0\rangle_B$
- Experimental evidence…

7

Quantum Computer

- A device in which state is encoded by qubits, and superposition and entanglement are exploited to achieve a computation.



8

Quantum Computation

- Initialization
  - Set up n qubits to be in the appropriate state with probabilities implied by the a_k
- Execution
  - Transform the state in a sequence of steps
  - Multiplication with a unitary matrix ($\sum_k |a_k|^2 = 1$)
- Completion
  - Read the state at the end of execution
- Note: Need to run multiple times to get correct result with high probability

Unitary Matrix

- Square, entries are complex numbers;

  $UU^T = I$

  $U^{-1} = U^T$
- Examples
  - Rotation matrices in 2D and 3D
  - Reflections

$$\begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix}$$

Quantum Gates

- Hadamard gate H self-inverse

$$H(|0\rangle) = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$
$$H(|1\rangle) = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$
$$a_0 H(|0\rangle) + a_1 H(|1\rangle) = \frac{a_0 + a_1}{\sqrt{2}}|0\rangle + \frac{a_0 - a_1}{\sqrt{2}}|1\rangle$$

- Controlled not gate CNOT

$$CNOT(|00\rangle) = |00\rangle$$
$$CNOT(|01\rangle) = |01\rangle$$
$$CNOT(|10\rangle) = |11\rangle$$
$$CNOT(|11\rangle) = |10\rangle$$

11

Quantum Algorithms

- Fourier transform $O(n \log(n))$ vs. $O(\log^2(n))$
- Factoring $O(n^2)$ vs. $O(\log(n)^3 \log^2(n))$
- Class of algorithms with
  - Solved only by guess and verify
  - Each guess takes equally long to verify
  - No information which guess is better than others
  - so n answers must be checked
  - Can be done in $O(\sqrt{n})$ time

12

Issues

- Physical realization of qubits that scales
  - D-Wave says they have a 28-qubit prototype www.dwavesys.com
  - Want 1024 qubits by end of 2008
- Initialization
- Computation steps faster than decoherence; http://plato.stanford.edu/entries/qm-decoherence/
- Universal set of quantum gates
- Reading the final state conveniently

13