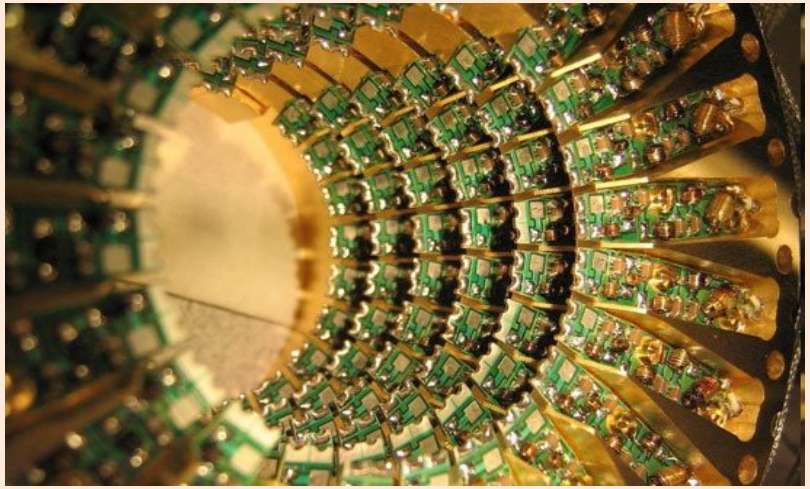
Introduction to Quantum Computing

Debajyoti Bera, IIIT-Delhi

Quantum Computing Community

IBM Almaden Research Center , 2001



Q.C. at D-Wave Systems Inc., 2006

Quantum Physics

Quantum Information & Quantum Computation

Cryptography

Information Theory

Computer Science

Communication Theory

Quantum Comp. for Comp. Science

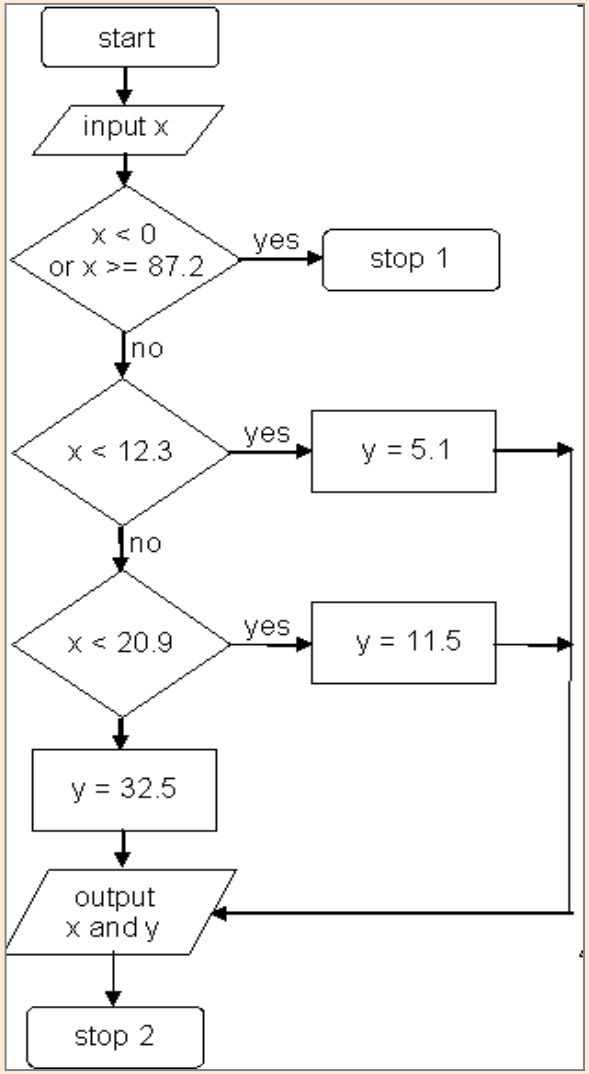
Computation in which
the operands and operators
follow the laws of quantum mechanics

1. Studying models of quantum computing
2. Design and analyse algorithms to efficiently solve problems

Overview

1. Computation
2. Quantum Mechanics
3. Quantum Computing
4. Progress & Challenge

What is Computation?



A sequence of steps,

Performed by a system

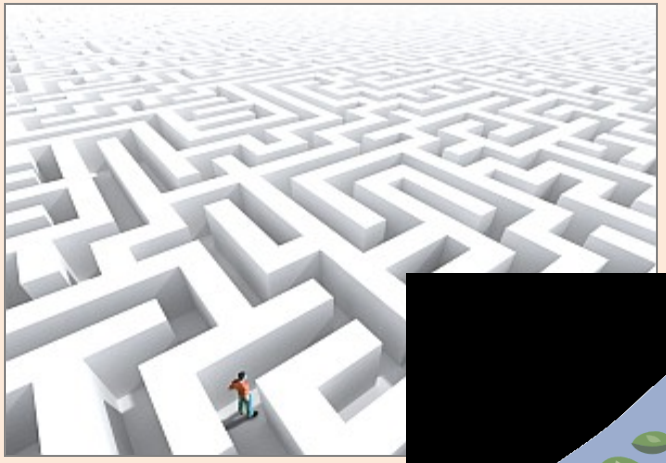
Which, given an input,

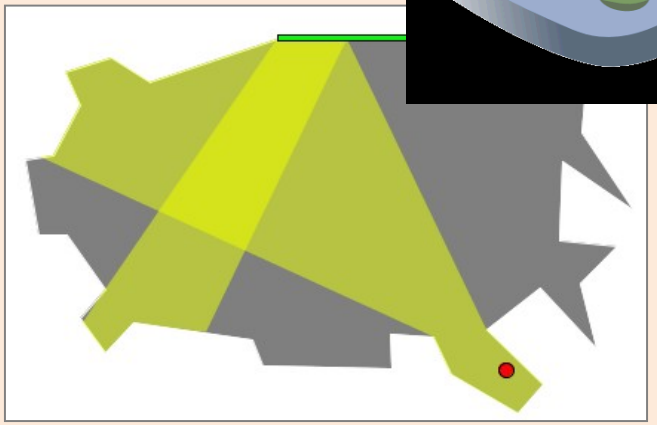
Produces output

Where, each step involves

Operation on values

What is Computation?





A sequence of steps,

Performed by a system

Which, given an input,

Produces output

Where, each step involves

Operation on values

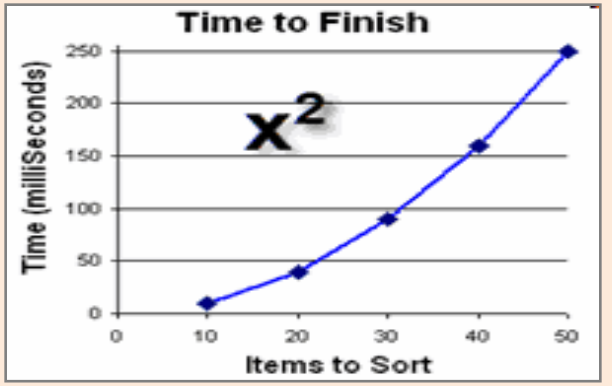
Analysis of Computation

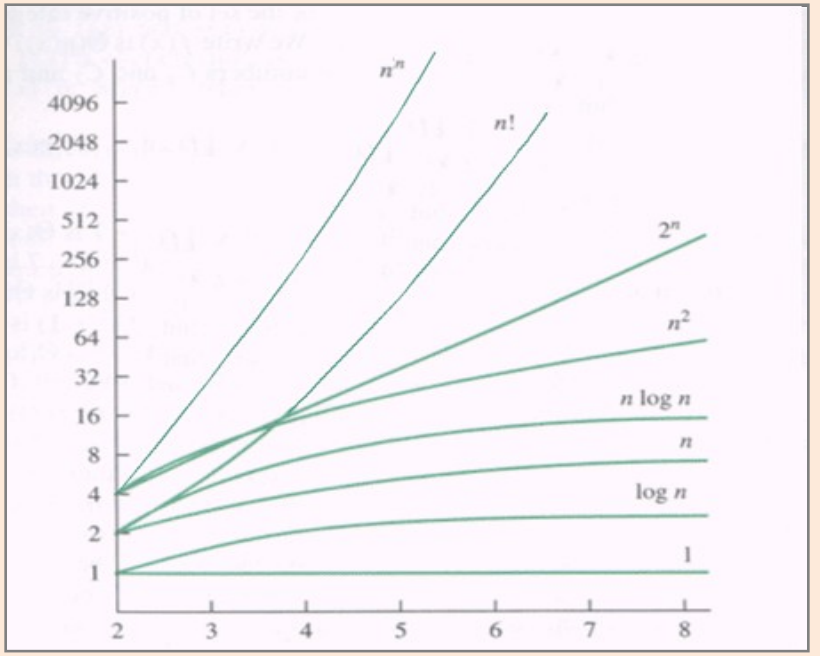
Models of Classical Computation

- Boolean Circuit
- Turing Machine
- Cellular Automata
- Genetic Algorithm, …

Metrics for Analysis

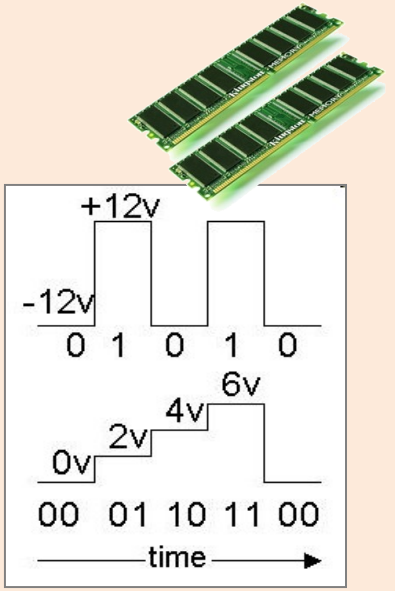
- Time to perform operations
- Space to store operands, …

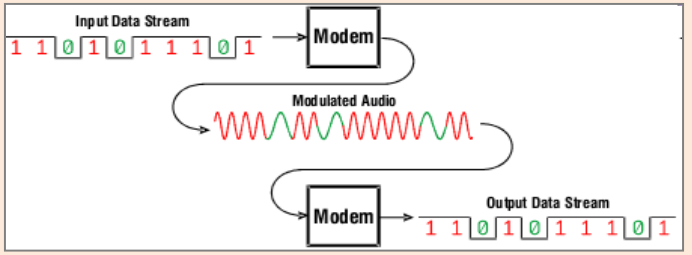




Operations & Operands

Operations on Operands	=	Change of state of "Some Thing"

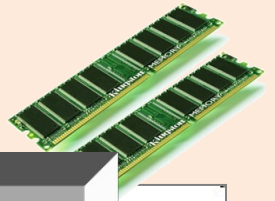


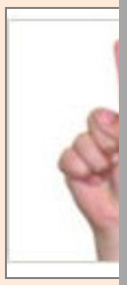


Operations & Operands

Operations

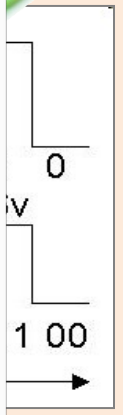
Change of state

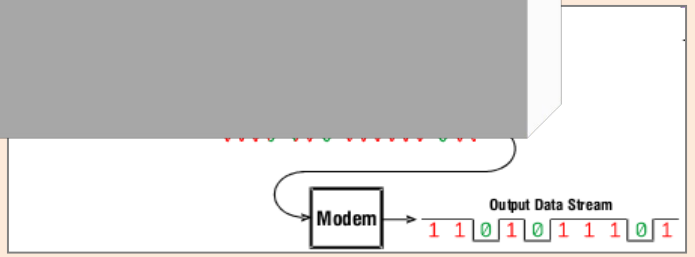




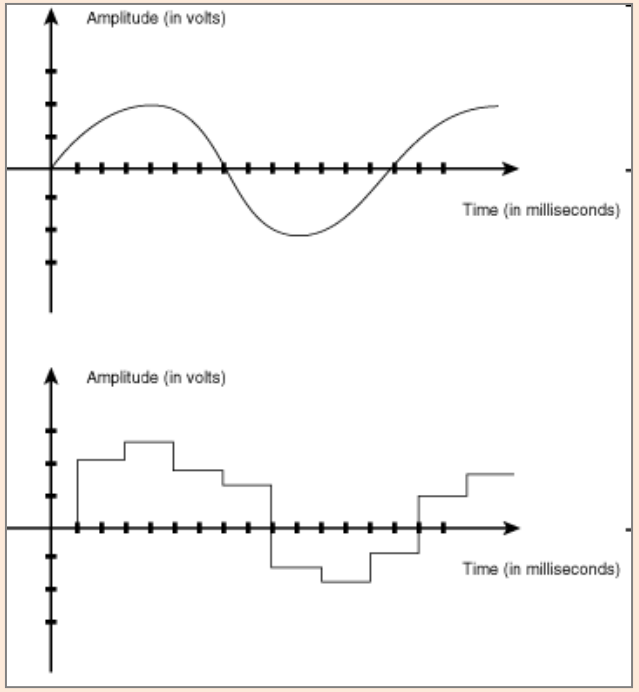
(Classical) Data/Value

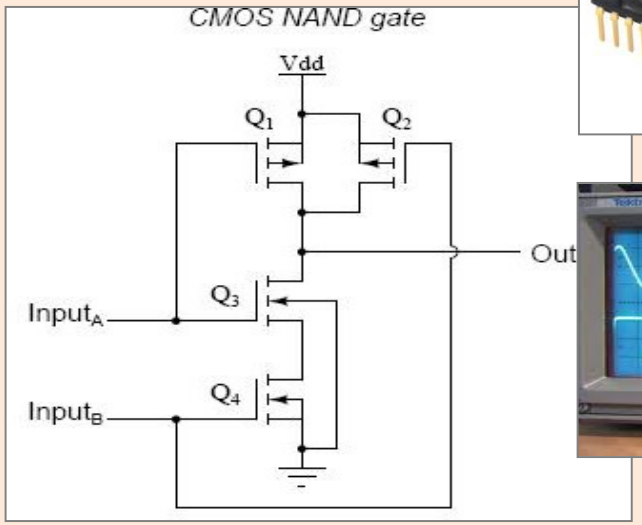
measurable property observable using macroscopic methods

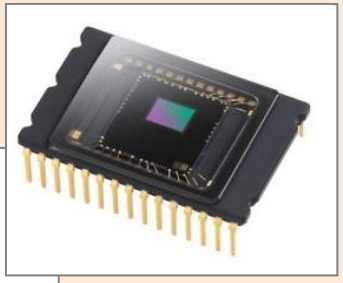


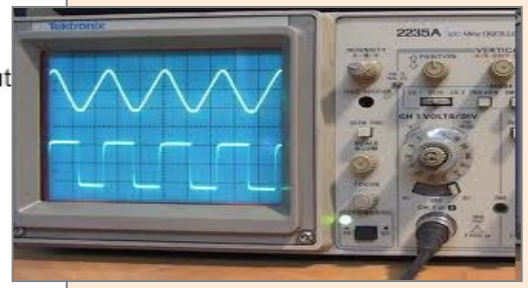


Classical Computation









"Bit" : 0 or 1

digital signal ±12V

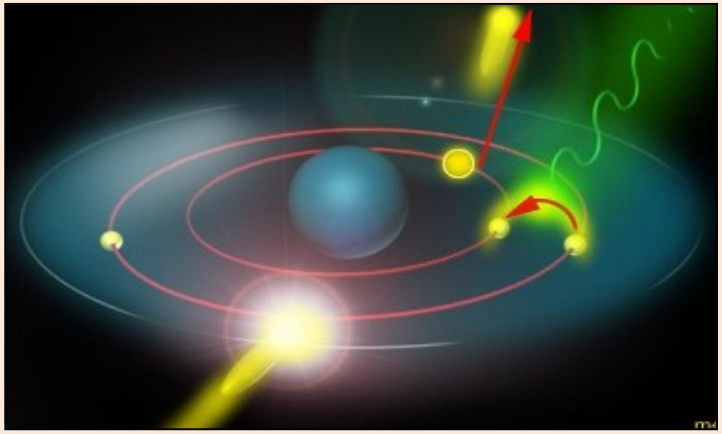
Operations – Boolean functions

Digital circuits & logic gates

Macroscopic CMOS transistors

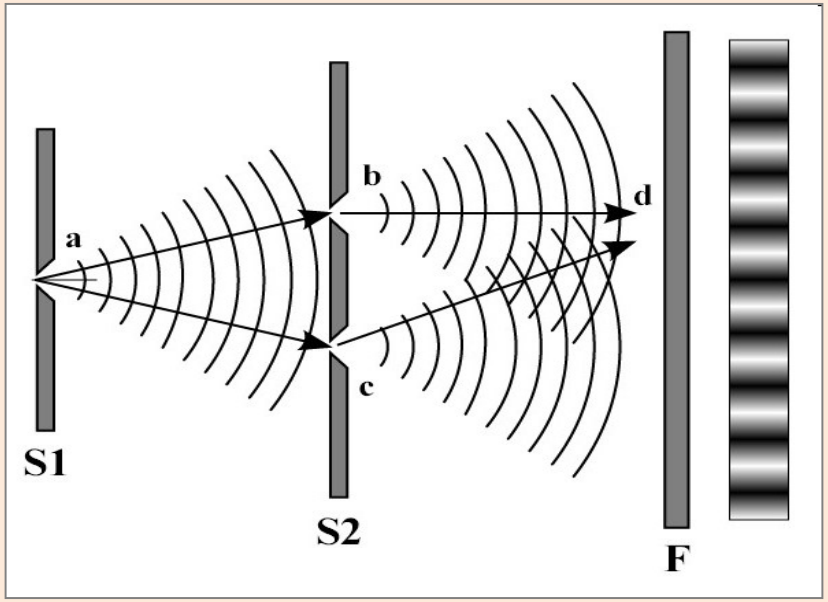
Quantum Mechanics

A proposed theory of nature (reality) that seems to be able to explain many facts about small particles which couldn't be (easily) explained using other theories.

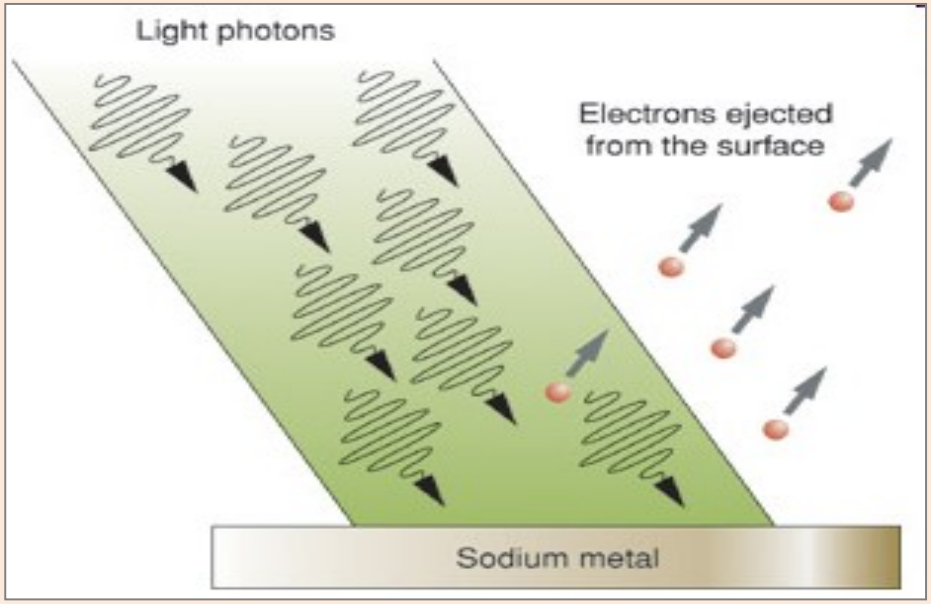


Reality of LIGHT?

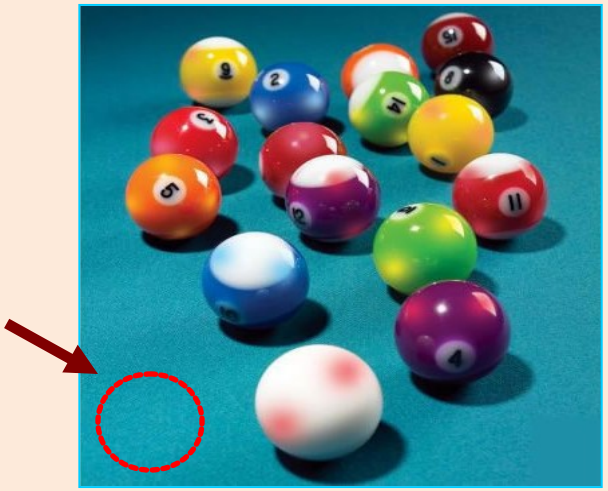
1803
Light behaves like wave
(Double slit expt.)



1905
Light made of photons
(Photoelectric effect)

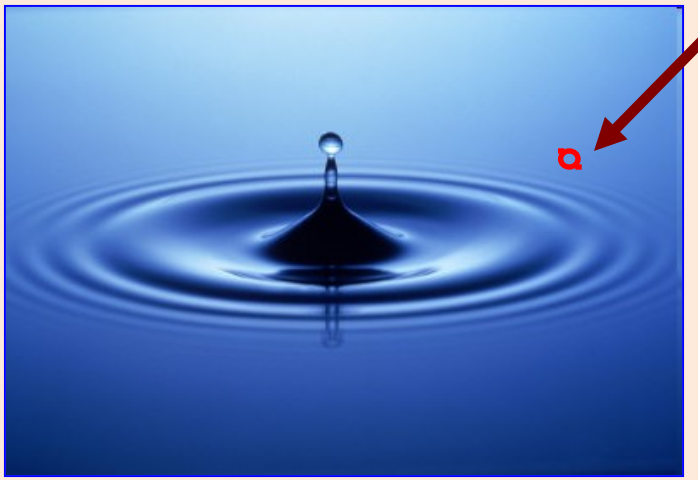


Existence: Particle -vs- Wave



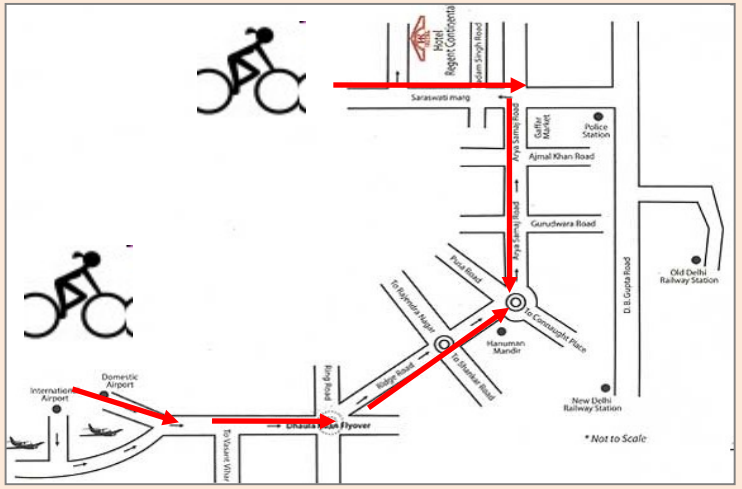
P
A
R
T
I
C
L
E

W
A
V
E

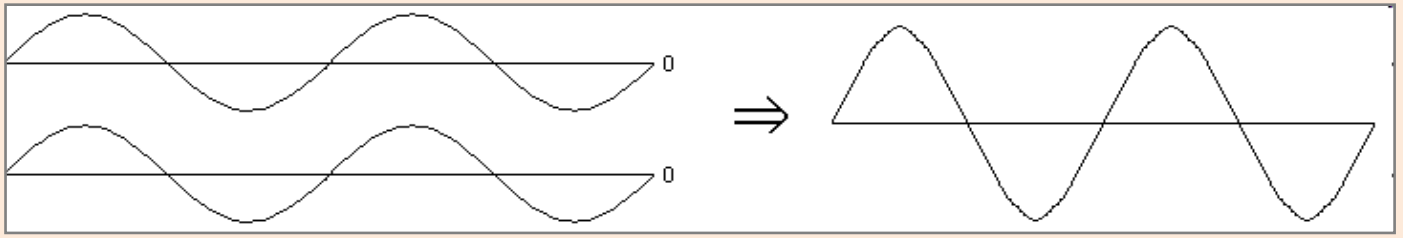


Existence: Particle -vs- Wave

PARTICLE



WAVE



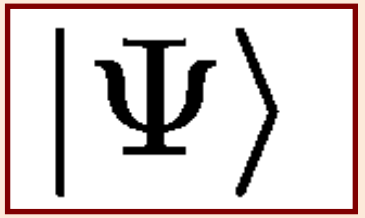
constructive interference

destructive interference

Quantum Mechanical Properties of "very small" objects

Both Particle & Wave

- Behaves like a particle whose "presence" follows a wave pattern (wavefunction)
- Has interference & other properties of waves…
- Simultaneously possesses multiple values
- "Collapses" to one value upon observation



Quantum Mechanical Properties

Possessed by atomic & sub-atomic particles

Particle	Property	Ket $\|0\rangle$	Ket $\|1\rangle$
Photon	Polarisation	Horizontal	Vertical
Photon	Time of arrival	Early	Late
Electron	Spin	Up	Down
Atom/Nucleus	Spin	Up	Down
Superconducting circuit	Energy state	Ground state	First excited state

2008: ~2 secs lifetime of a qubit
2013: ~39 mins lifetime of a qubit (room temp.)

Quantum Computing

Assuming ...

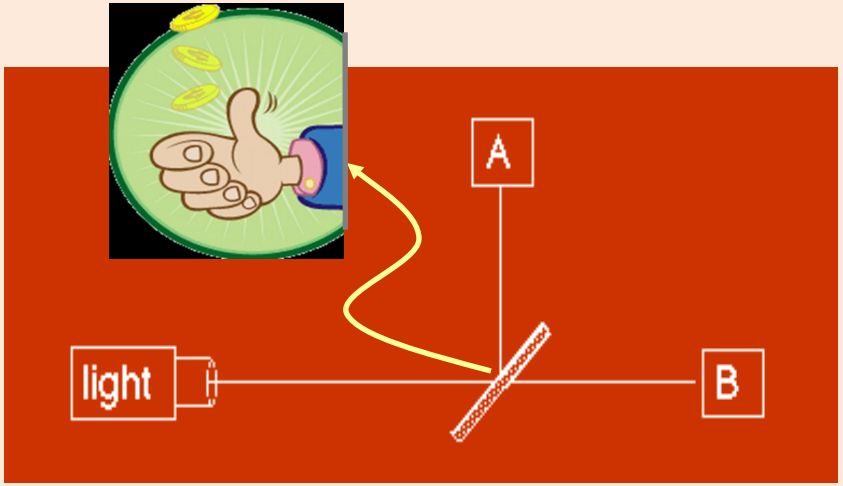
Machines which follow principles of quantum mechanics…

… Can we compute more effectively?

- Less time
- More space
- Fewer error

Quantum is <u>better than</u> Classical

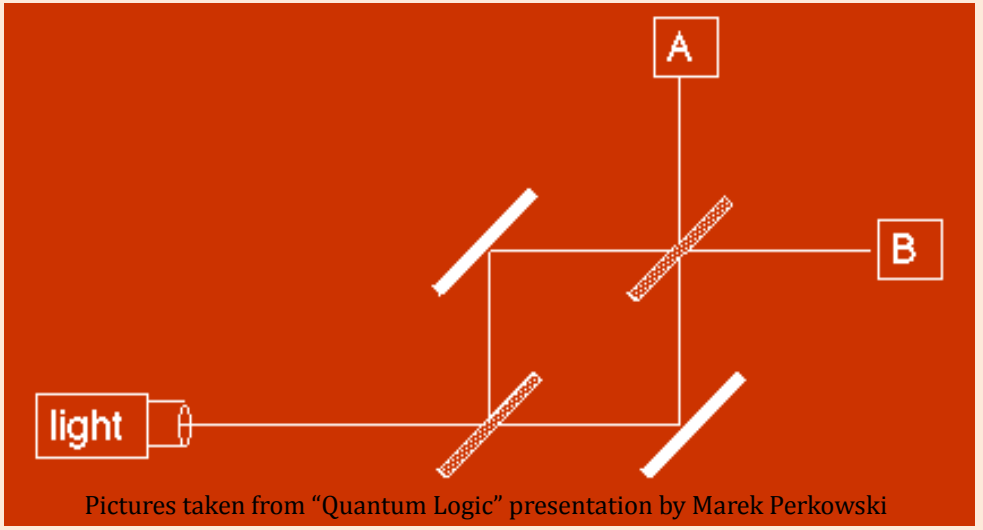
Using Photons for Data



1. 50% photons leaving the light source arrive at detector A
2. Rest 50% arrive at B

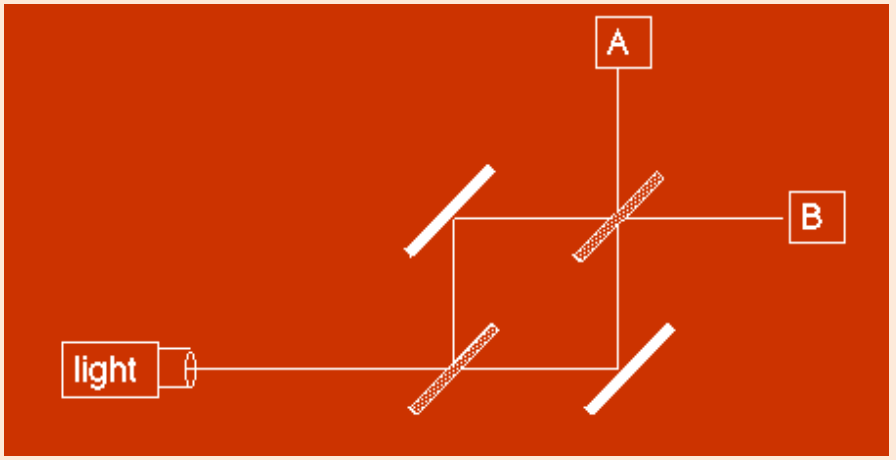
<u>All photons</u> leaving the source arrive at A !!!

Expt. setup: Equal path lengths, rigid mirrors, only one photon in the apparatus at a time.



Pictures taken from "Quantum Logic" presentation by Marek Perkowski

Quantum Bits – "qubits"



Mathematically…

A state with k possibilities is a unit-vector in $\mathbb{C}^k$

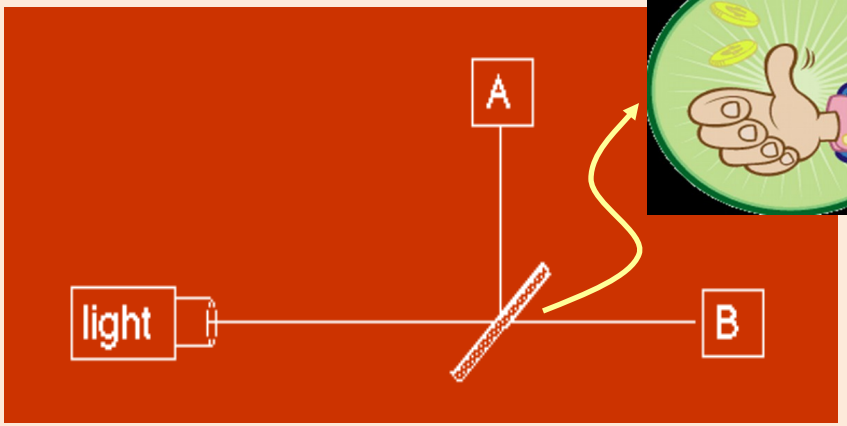
Combined State/ Wavefunction

Individual States / Possibilities

$$|\Psi\rangle = \alpha_1|S_1\rangle + \alpha_2|S_2\rangle + \alpha_3|S_3\rangle + \cdots$$

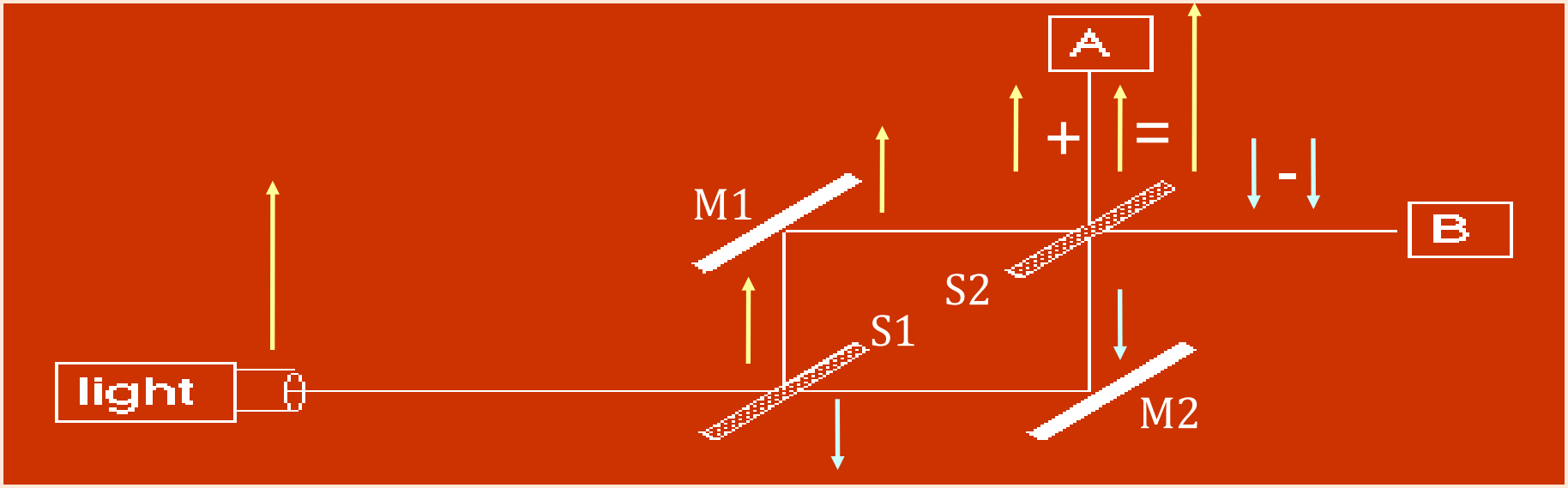
Amplitude (value of possibility) — can be –ve (interference)

Operations on Photons



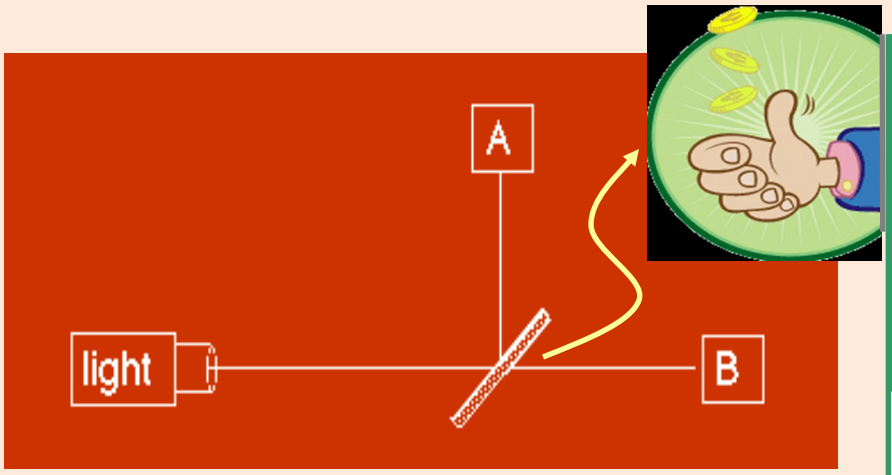
$$|\uparrow\rangle \rightarrow \frac{1}{\sqrt{2}}|\uparrow\rangle + \frac{1}{\sqrt{2}}|\downarrow\rangle$$

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



Pictures taken from “Quantum Logic” presentation by Marek Perkowski

Operations on Photons



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

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

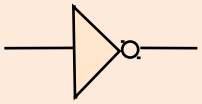
Hadamard Operator

Unitary operators (length-preserving, over complex numbers)

- NMR
- Optical Lattice
- Trapped Ion QC
- Cavity QED

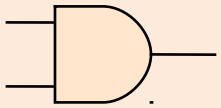
Pictures taken from “Quantum Logic” presentation by Marek Perkowski

Classical Boolean Gates



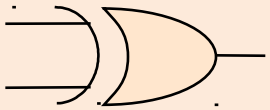
Not

x	NOT(x)
0	1
1	0



And

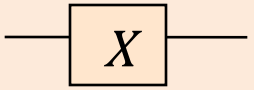
x	y	AND(x,y)
0	0	1
1	0	0
0	1	0
1	1	1



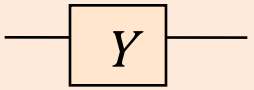
Xor

x	y	XOR(x,y)
0	0	0
1	0	1
0	1	1
1	1	0

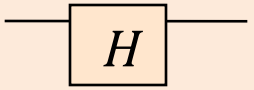
Common Quantum Gates



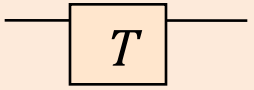
Pauli X (Not) $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$



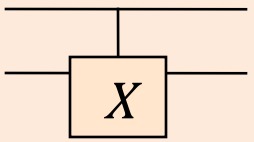
Pauli Y $\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$



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

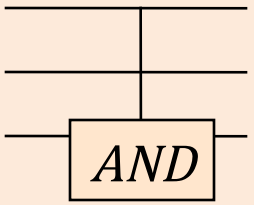


π/8 Rotation $\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$



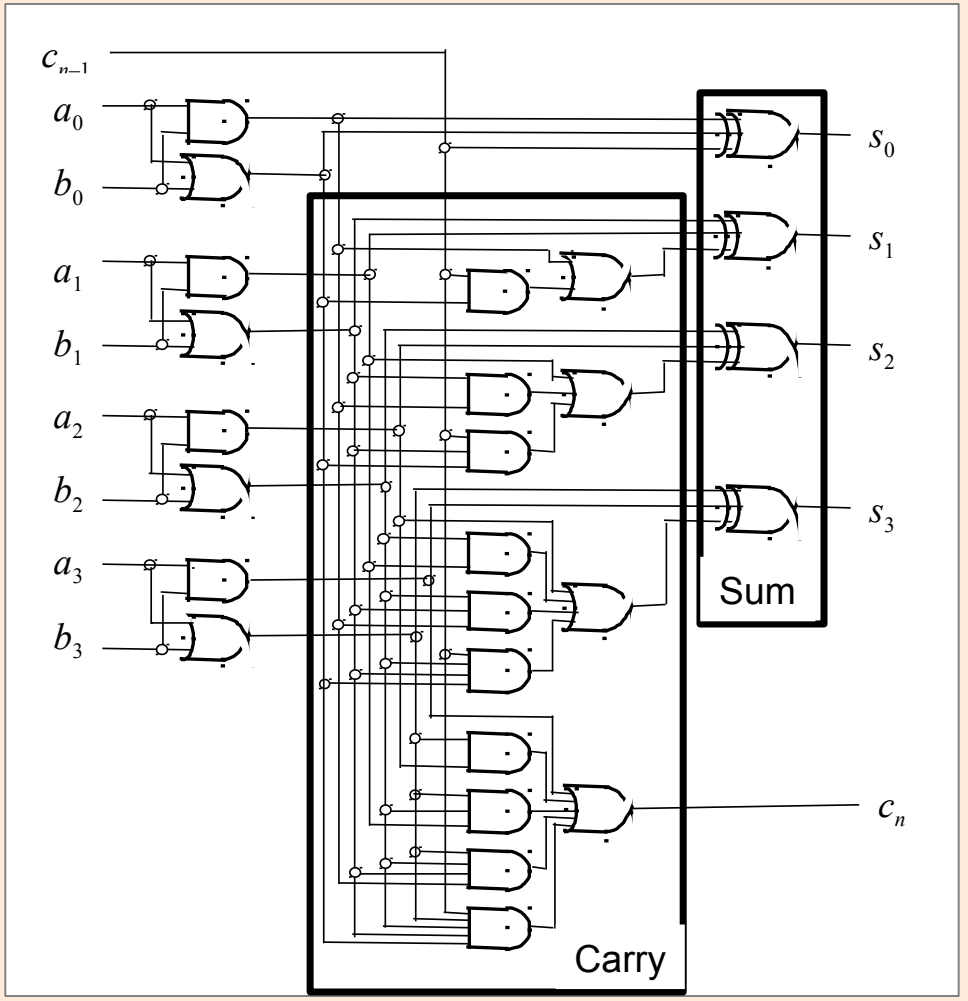
Controlled NOT

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

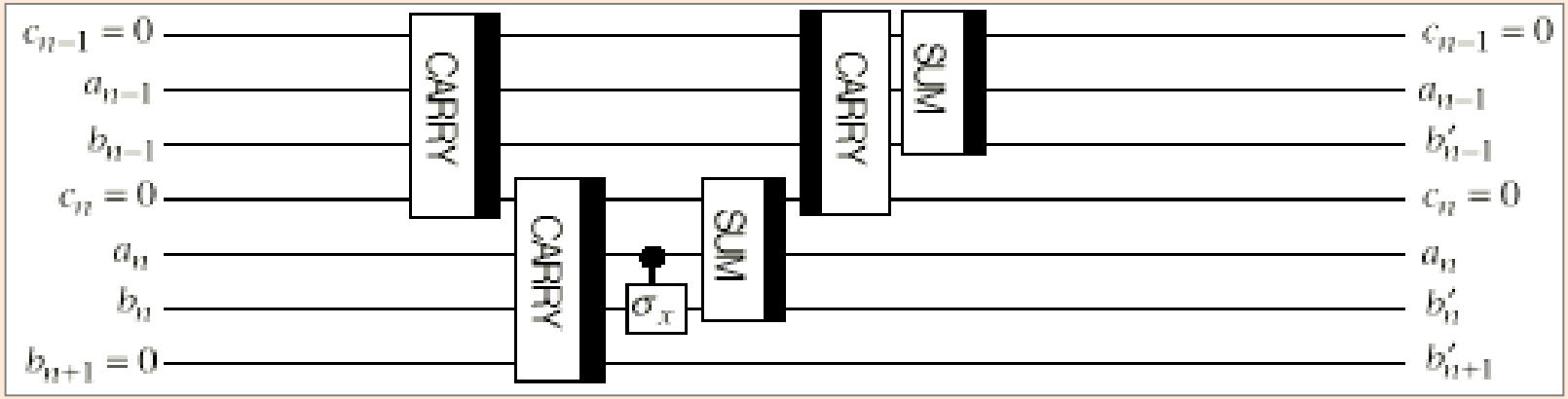


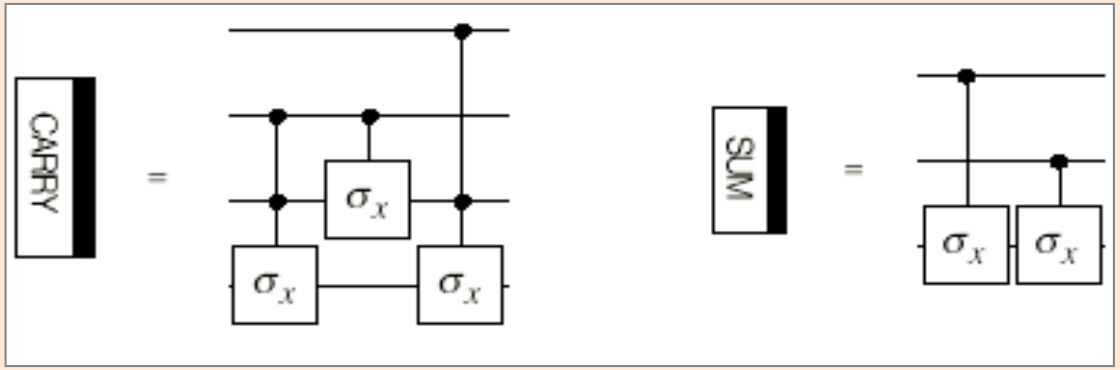
Toffoli

Classical Adder



Quantum Adder





σ_x :Pauli rotation

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Unlike Classical …

- ✓ Superposition
- ✓ Measurement
- ✓ Interference
- ✓ No copying
- ✓ Entanglement (multi qubit)

<u>At the same time, both 0 & 1</u>

vs.

At the same time, either 0 OR 1

Unlike Classical …

- ✓ Superposition
- ✓ Measurement
- ✓ Interference
- ✓ No copying
- ✓ Entanglement (multi qubit)

Reality is independent of observation

VS

Reality changes after observation

Unlike Classical …

- ✓ Superposition
- ✓ Measurement
- ✓ Interference
- ✓ No copying
- ✓ Entanglement (multi qubit)

Multiple occurrence increases probability

vs.

Multiple occurrence may decrease probability

Unlike Classical …

- ✓ Superposition
- ✓ Measurement
- ✓ Interference
- ✓ No copying
- ✓ Entanglement (multi qubit)

Cannot duplicate a state (qubit)

vs.

Can create arbitrary copies of data

Unlike Classical …

- ✓ Superposition
- ✓ Measurement
- ✓ Interference
- ✓ No copying
- ✓ Entanglement (multi qubit)

Value affected by far-off operations

vs.

Value affected by only local operations

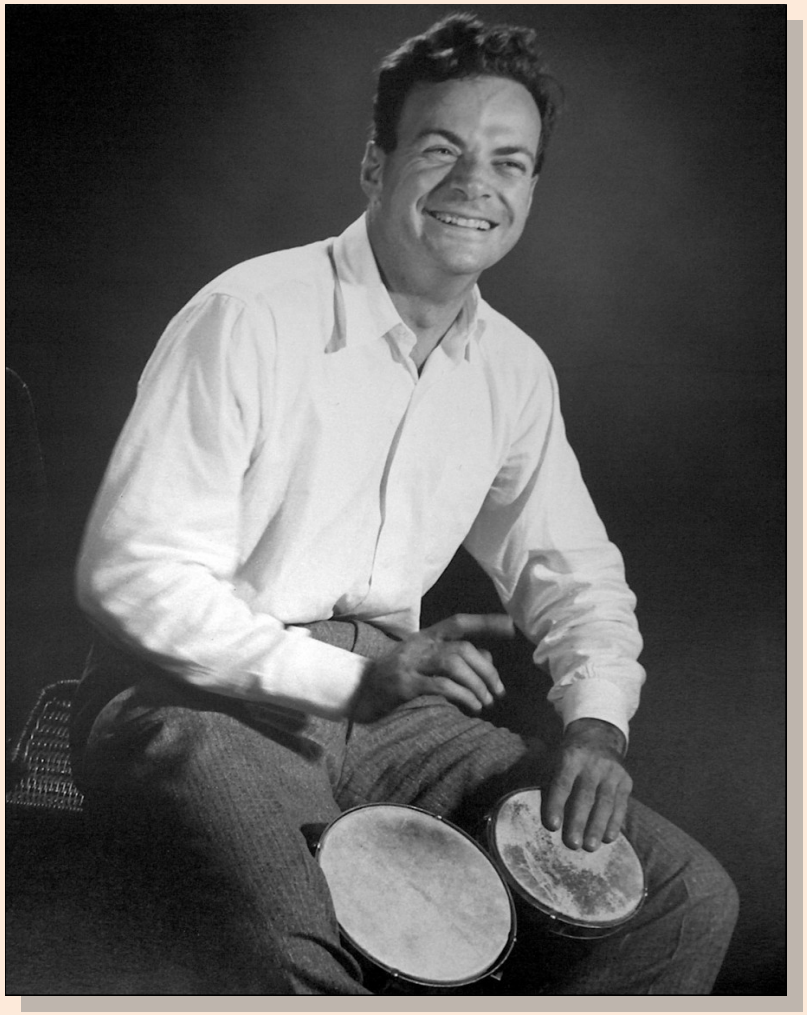
Secret Recipe

- In quantum systems possibilities count, even if they never happen!
- Each of exponentially many possibilities can be used to perform a part of a computation at the same time.
- It may be possible to cancel out "bad" possibilities during computation.

Pitfalls!

- Gates and circuits must be reversible (lossless computation)
- During measurement, all possible computations except only one are destroyed
- Temporary copies of intermediate results cannot be made
- Interference with environment completely changes computation (decoherence)

Quantum Computing: 1982 ...



1982

Simulating Physics with Computers

- *Richard Feynman*

“Nature isn't classical, dammit, and if you want to make a simulation of Nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy.”

… 1985 …

Church-Turing thesis (1930-1950): Anything that can be computed (by a mechanical process) can be computed by a Turing machine.

Church-Turing-Deutsch thesis: Anything that can be computed by a physical process can be computed by a universal computing device (Universal Quantum Turing Machine).

$\frac{198}{5}$

… 1993 …

1985: Deutsch – (inefficient) universal quantum Turing machine

1993

- Bernstein-Vazirani / Yao – efficient universal quantum Turing machine
- Equivalence of quantum computing models: quantum Turing machine & quantum circuit

… 1994 – 1996 …

1994 - Peter Shor came up with a quantum algorithm to factor very large numbers incredibly fast.

1997 - Lov Grover developed a quantum search algorithm which takes significantly lesser time to search unstructured database.

Both better than known classical algorithm!

… 1998 – 2001 …

Experimental demonstrations

- 2-qubit NMR quantum computer to solve Deutsch's problem (Oxford University, IBM-Stanford-MIT)
- 3-qubit, 5-qubit, 7-qubit NMR computer
- Execution of Grover’s algorithm on an NMR computer
- Execution of Shor’s algorithm to factor 15

Models for Quantum Computing

- Quantum Circuits
- Quantum Turing Machine
- Quantum Cellular Automata
- Quantum Query
- Quantum Communication
- Quantum Adiabatic Algorithms

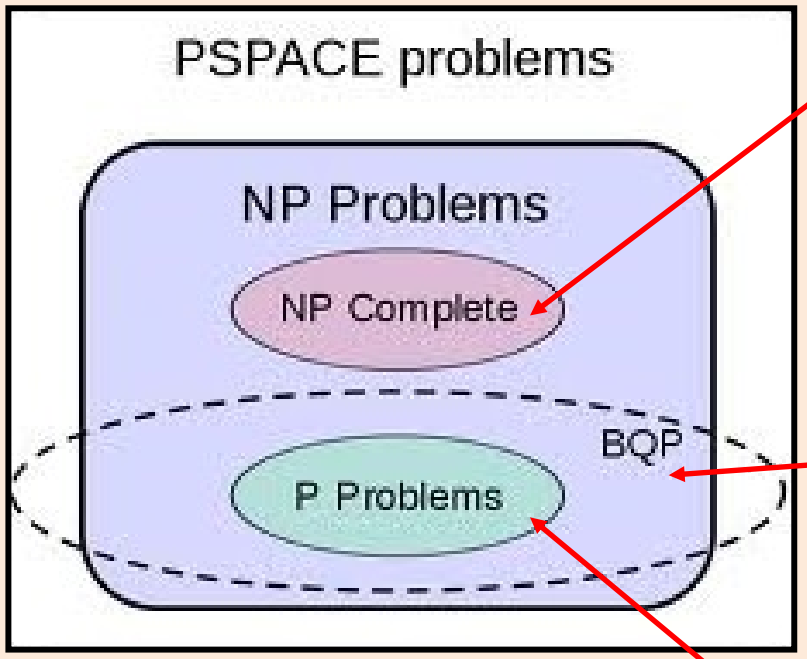
…

Mathematical models of computing which can be analysed without knowledge of quantum mechanics

Theory of Quantum Computing

- ✓ Efficient quantum circuits
  - Smaller size, lesser time, fewer faults
- ✓ Efficient quantum algorithms
  - Lesser storage, lesser time, fewer error
- ✓ Efficient quantum communication protocols
  - Lesser communication
- ✓ Also! Problems for which quantum algorithm provably cannot do significantly better than classical algorithms

Challenges



Possibly hard for classical computers

Timetable scheduling for large school

Easy for quantum computers ?

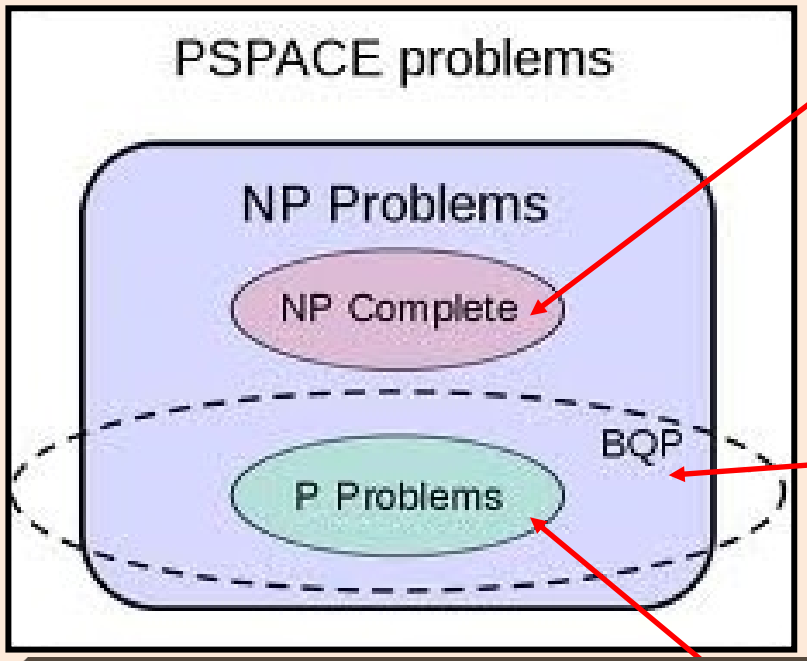
Easily solved by quantum computers

Factoring a very large number

Easily solved by classical computers

Testing if a number is prime

Challenges



Possibly hard for classical computers

Timetable scheduling for large school

Easy for quantum computers ?

Easily solved by quantum computers

Factoring a very large number

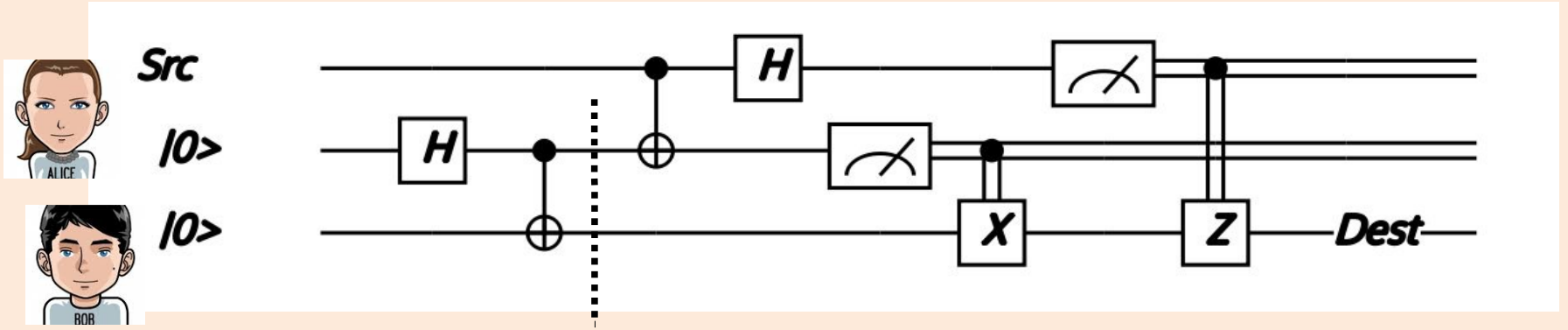
- Find efficient solutions for hard problems
- Understand which problems are still hard
- Make solutions robust to errors and failures

Microsoft LIQUi

Language-Integrated Quantum Operations

- Software platform for quantum computing
- Includes optimized classical simulation of q. circuits.
- Written in F#
- Vast repository of (C#) libraries
- Can create images of quantum circuits, LaTeX, PDF, etc.
- Available for Windows, Linux, Mac

Quantum Teleportation




```
// Define an EPR function
let EPR (qs:Qubits) =
    H qs; CNOT qs

let teleport (qs:Qubits) =
    let q0,q1,q2    = qs.[0],qs.[1],qs.[2]      // Extract 3 qubits

    // Give names to the first three qubits
    LabelL "Src" [q0]
    LabelL "\\ket{0}" [q1]
    LabelL "\\ket{0}" [q2]

    EPR[q1;q2]; CNOT qs; H qs                   // EPR 1,2, then CNOT 0,1 and H 0
    M[q1]; BC X [q1;q2]                         // Conditionally apply X
    M[q0]; BC Z [q0;q2]                         // Conditionally apply Z
    LabelR "Dest" [q2]                          // Label output
```

Project

- Given two distributions on Head and Tails, ...
  - D1 = HHHHTTTHTHHTHTHTHT... (Pr[H] = p1)
  - D2 = THHTHTTTTTHTHTTTHTHT... (Pr[H] = p2)
- A coin following either D1 or D2
  - Tossing coin gives lots of samples from D1 or D2 ...

- Identify if distribution of coin is D1 or D2
  - With error ~ 0.1, 0.01, 0.001, ...
  - Without error !!!

Using quantum techniques

Sampling Complexity

D0 = {Enc(x,k1), Enc(x,k2), Enc(x,k3), ... }
D1 = {Enc(y,k1), Enc(y,k2), Enc(y,k3), ... }
Given multiple encryptions of m (either x or y), identify m?

Output from a good PRG cannot be distinguished from the output of a true random generatior by a polynomial-time adv.

Important problem in hypothesis testing

Project Plan

- 1-2 student
  - comfortable with Linear Algebra
  - NO knowledge of Quantum Mechanics required
- Learn mathematical foundation of Quantum Computing ~ 2-3 wks
- Learn F# ~ 1 wk
- Read and implement various techniques

On leave for the next week (20-28th May).

Limited email response: dbera@iiitd.ac.in