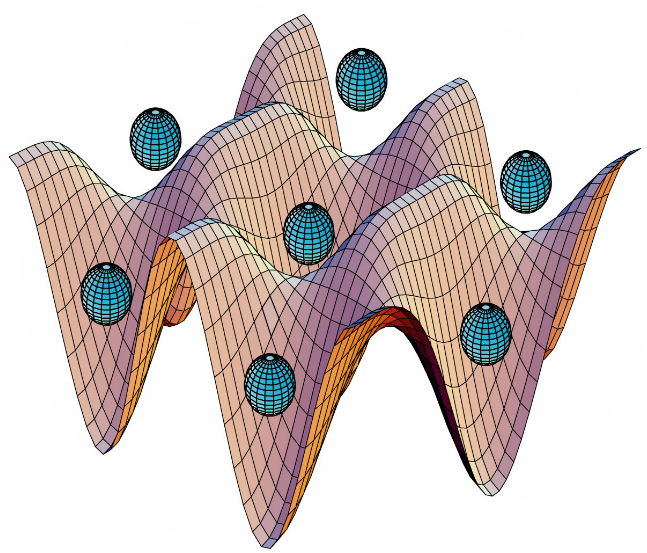
Петербургский электротехнический университет
"ЛЭТИ"
Факультет электроники

The World of Quantum Information



Marianna Safronova
Department of Physics and Astronomy

May 22, 2012

University of Delaware

Outline

- Quantum Information: fundamental principles

  (and how it is different from the classical one).
  - Bits & Qubits
  - Quantum weirdness: entanglement, superposition & measurement
  - Logic gates & Quantum circuits
- Cryptography & quantum information
- A brief introduction to quantum computing
- Real world: what do we need to build a quantum computer/quantum network?
- Current status & future roadmap

Why quantum information?

Information is physical!

Any processing of information

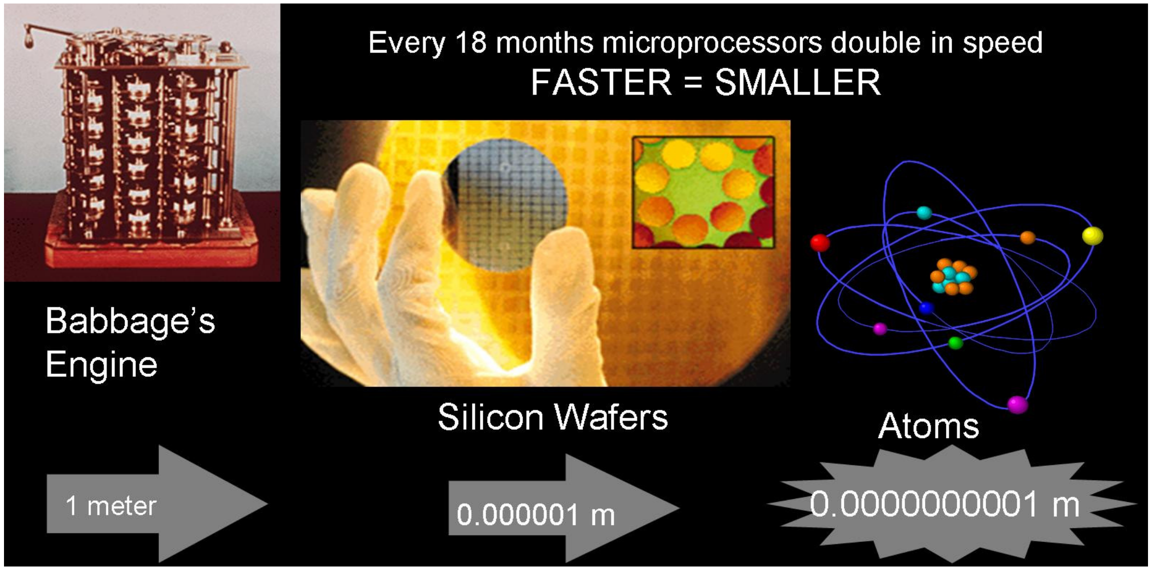
is always performed by physical means

Bits of information obey laws of classical physics.

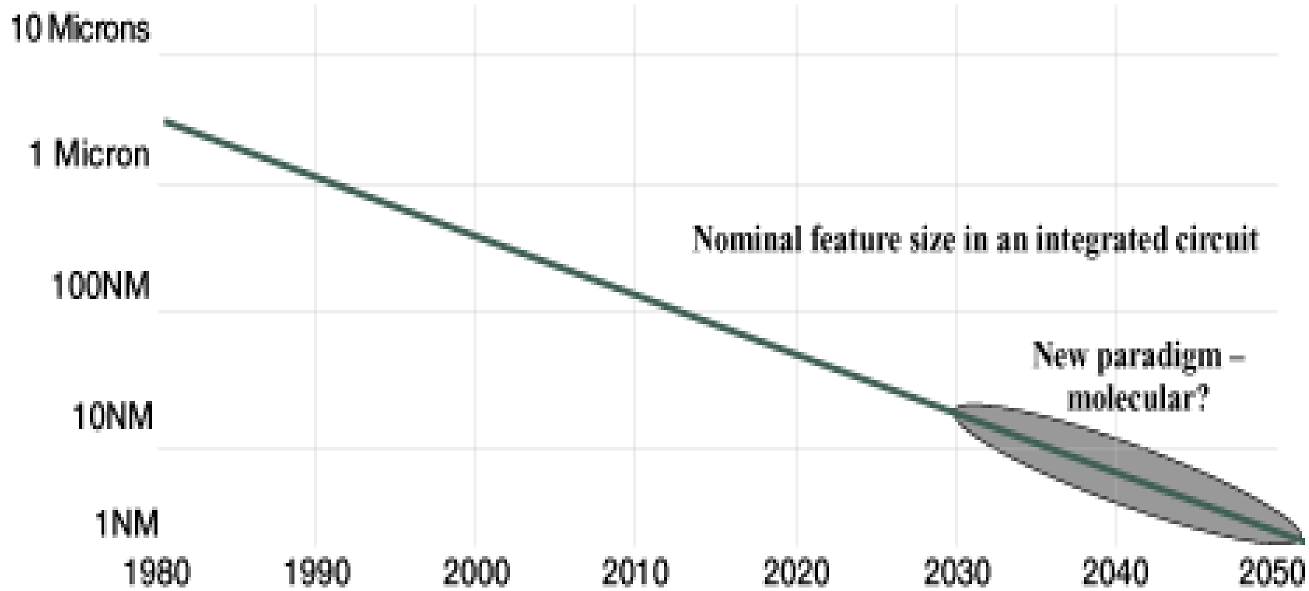
Why quantum information?

Information is physical!
Any processing of information
is always performed by physical means

Bits of information obey laws of classical physics.



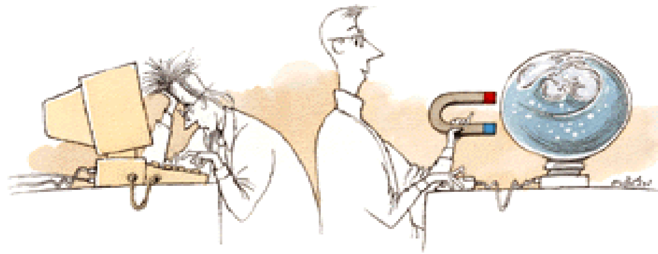
Why Quantum Computers?



Computer technology is making devices smaller and smaller…

…reaching a point where classical physics is no longer a suitable model for the laws of physics.

Bits & Qubits



Fundamental building blocks of classical computers:

BITS

STATE:

Definitely

0 or 1

Fundamental building blocks of quantum computers:

Quantum bits

or

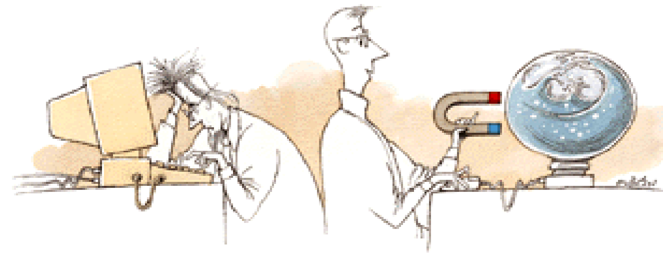
QUBITS

Basis states: $|0\rangle$ and $|1\rangle$

Superposition:

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

Bits & Qubits



Fundamental building blocks of classical computers:

BITS

STATE:

Definitely

0 or 1

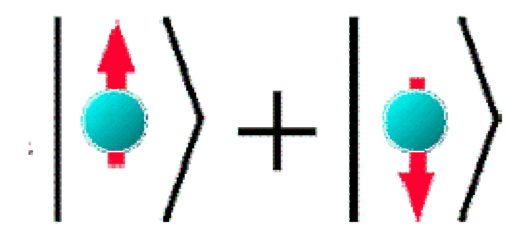
Fundamental building blocks of quantum computers:

Quantum bits

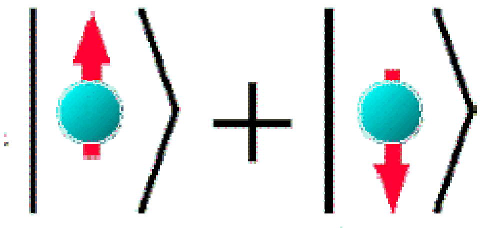
or

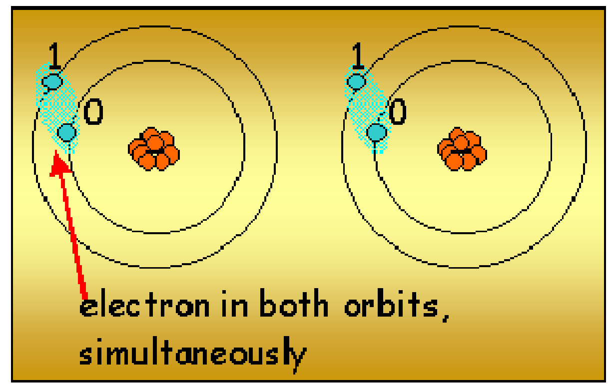
QUBITS

Basis states: $|0\rangle$ and $|1\rangle$

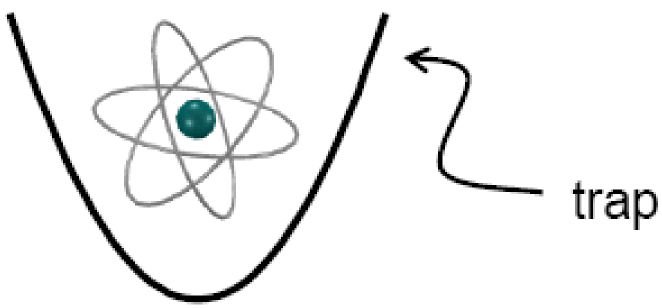


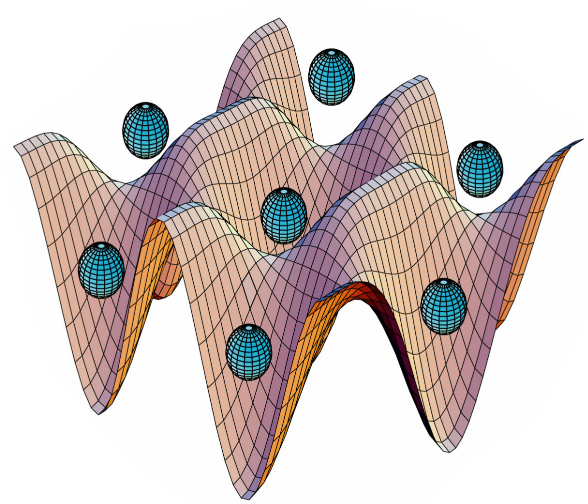
Qubit: any suitable two-level quantum system





single trapped atom:

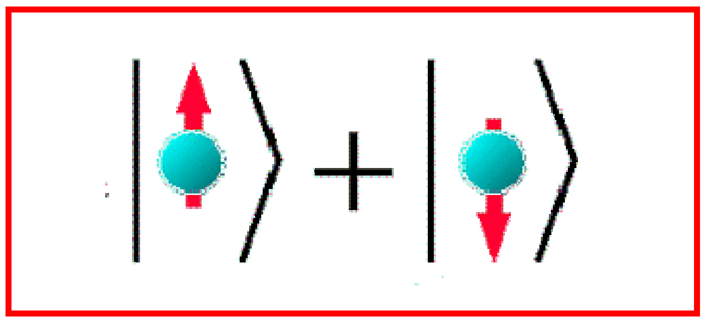




Bits & Qubits: primary differences

Superposition

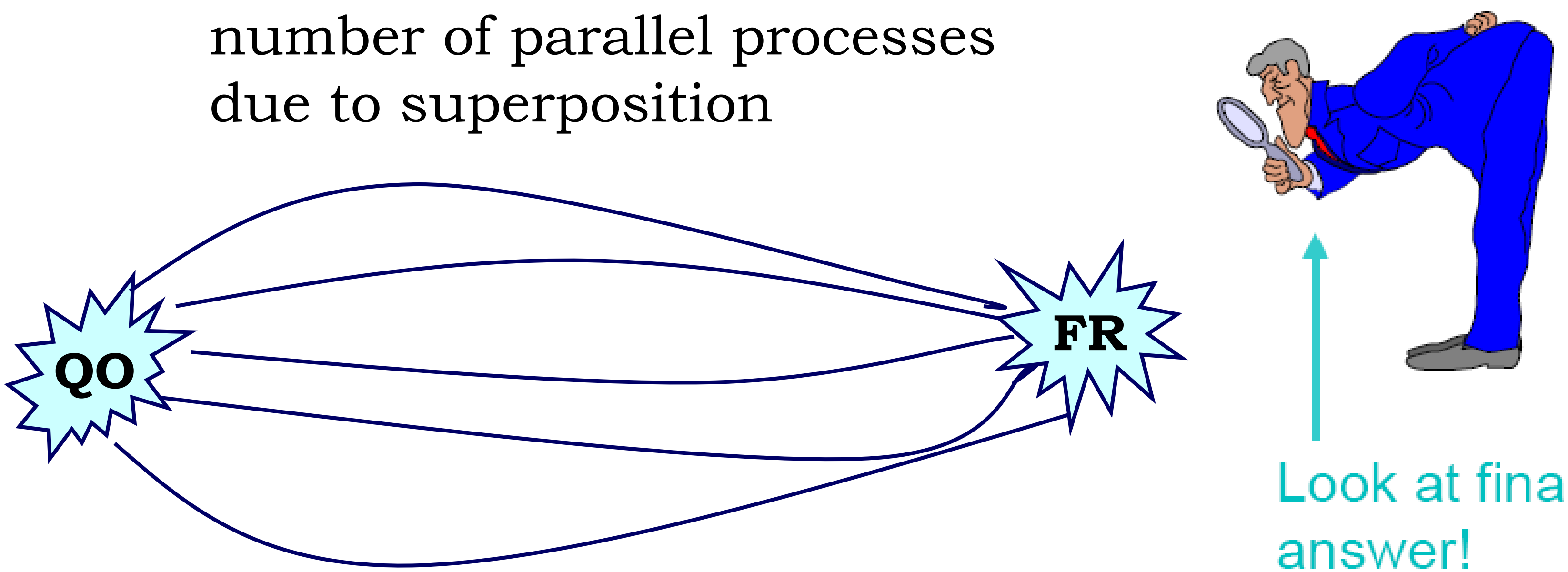
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$



Bits & Qubits: primary differences

Measurement

- Classical bit: we can find out if it is in state 0 or 1 and the measurement will not change the state of the bit.
- Qubit: Quantum calculation: number of parallel processes due to superposition



Bits & Qubits: primary differences

- Superposition
- Measurement

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

- Classical bit: we can find out if it is in state 0 or 1 and the measurement will not change the state of the bit.
- Qubit: we cannot just measure α and β and thus determine its state! We get either $|0\rangle$ or $|1\rangle$ with corresponding probabilities $|\alpha|^2$ and $|\beta|^2$.

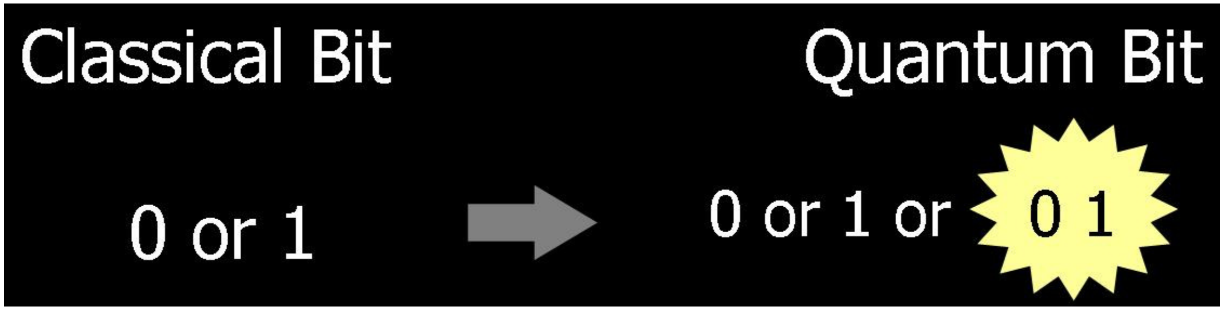
$$|\alpha|^2 + |\beta|^2 = 1$$

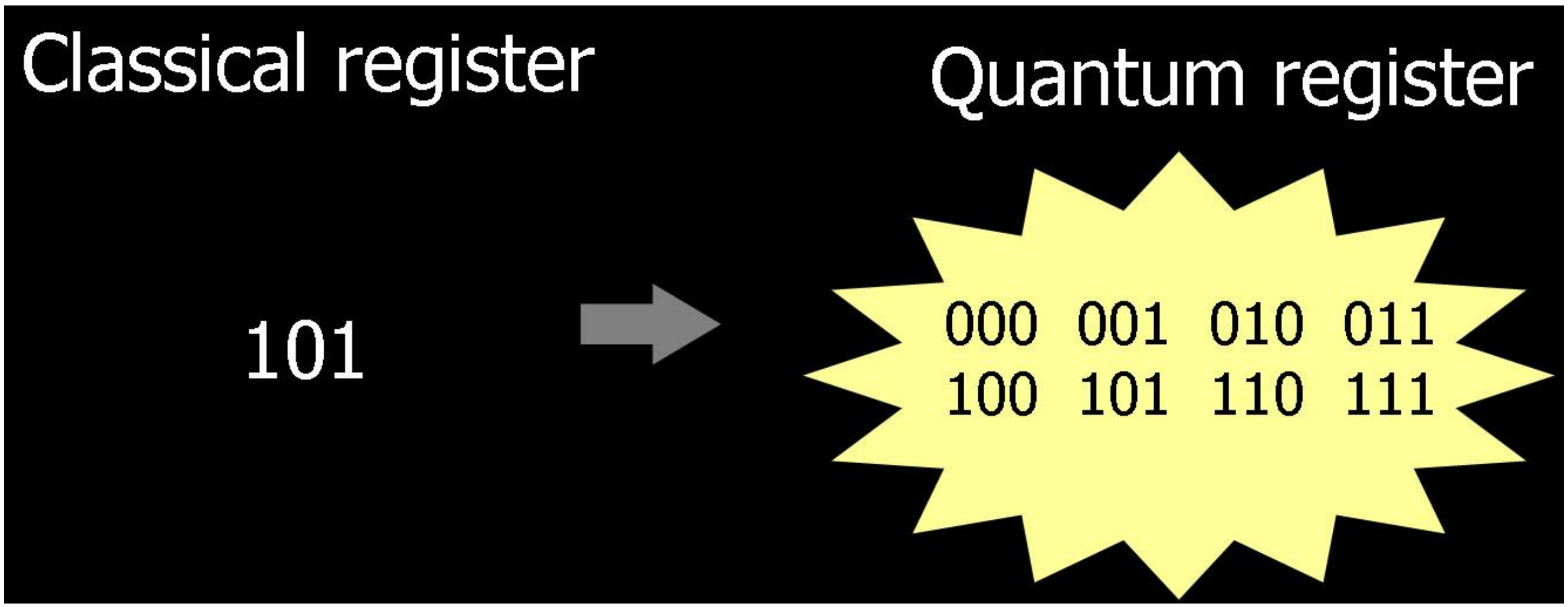
- The measurement changes the state of the qubit!

Hilbert space is a big place!

- Carlton Caves

Multiple qubits





Hilbert space is a big place!

- Carlton Caves

Multiple qubits

- Two bits with states 0 and 1 form four definite states 00, 01, 10, and 11.
- Two qubits: can be in superposition of four computational basis set states.

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$$

2 qubits	4 amplitudes
3 qubits	8 amplitudes
10 qubits	1024 amplitudes
20 qubits	1 048 576 amplitudes
30 qubits	1 073 741 824 amplitudes
500 qubits	**More amplitudes than our estimate of number of atoms in the Universe!!!**

Entanglement

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

Results of the measurement

First qubit	0	1
Second qubit	0	1

$$|\psi\rangle \neq |\alpha\rangle \otimes |\beta\rangle \longrightarrow \boxed{\text{Entangled states}}$$

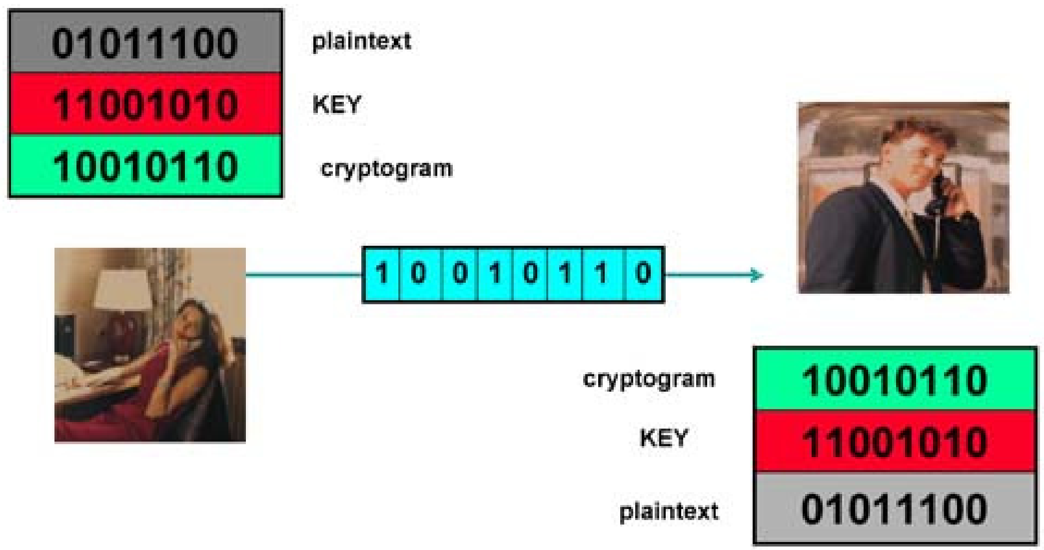
Quantum cryptography

Classical cryptography

Scytale - the first known mechanical device to implement permutation of characters for cryptographic purposes

Classical cryptography

Private key cryptography



How to securely transmit a private key?

Key distribution

A central problem in cryptography:
the key distribution problem.

1) Mathematics solution: public key cryptography.
2) Physics solution: quantum cryptography.

Public-key cryptography relies on the computational difficulty of certain hard mathematical problems (computational security)

Quantum cryptography relies on the laws of quantum mechanics (information-theoretical security).

Quantum key distribution

- Quantum mechanics: quantum bits cannot be copied or monitored.

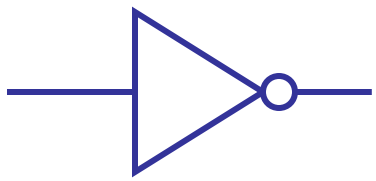
- Any attempt to do so will result in altering it that can not be corrected.

- Problems
  - Authentication
  - Noisy channels

Quantum logic gates

Logic gates

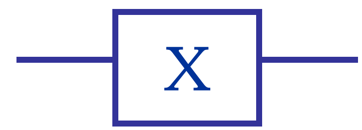
Classical NOT gate

A  NOT A

A	NOT A
0	1
1	0

The only non-trivial single bit gate

Quantum NOT gate (X gate)

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

Matrix form representation

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

$$X \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix}$$

More single qubit gates

Any unitary matrix U will produce a quantum gate!

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$\alpha|0\rangle + \beta|1\rangle \;—\boxed{Z}—\; \alpha|0\rangle - \beta|1\rangle$$

Hadamard gate:

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

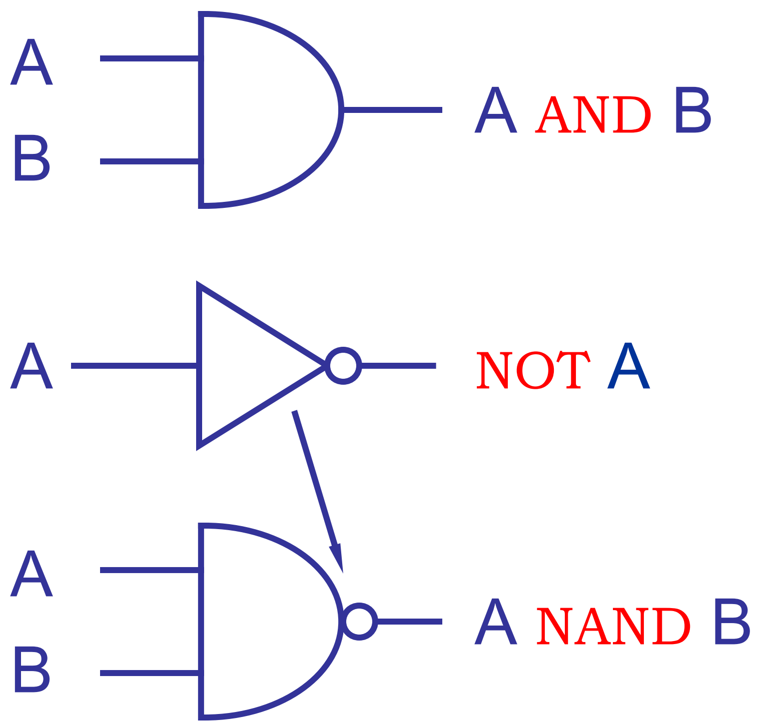
$$\alpha|0\rangle + \beta|1\rangle \;—\boxed{H}—\; \alpha\frac{|0\rangle + |1\rangle}{\sqrt{2}} + \beta\frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Single qubit gates, two-qubit gates, three-qubit gates …

- How many gates do we need to make?
- Do we need three-qubit and four-qubit gates?
- Where do we find such physical interactions?
- Coming up with one suitable controlled interaction for physical system is already a problem!

Universality:
classical computation

Only one classical gate (NAND) is needed to compute any function on bits!



A	B	A AND B	A NAND B
0	0	0	1
0	1	0	1
1	0	0	1
1	1	1	0

Universality: quantum computation

How many quantum gates do we need to build any quantum gate?

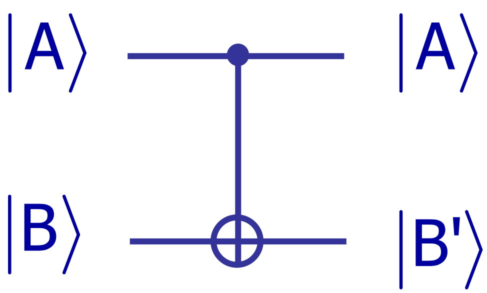
Any n-qubit gate can be made from 2-qubit gates.
(Since any unitary nxn matrix can be decomposed to product of two-level matrices.)

Only one two-qubit gate is needed!

Example: CNOT gate

Universal set of gates

CNOT



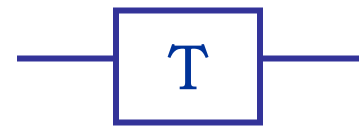
$\vert AB\rangle$	$\vert AB'\rangle$
$\vert 00\rangle$	$\vert 00\rangle$
$\vert 01\rangle$	$\vert 01\rangle$
$\vert 10\rangle$	$\vert 11\rangle$
$\vert 11\rangle$	$\vert 10\rangle$

Hadamard gate:

$\vert A\rangle$	$\vert A'\rangle$
$\vert 0\rangle$	$\frac{\vert 0\rangle+\vert 1\rangle}{\sqrt{2}}$
$\vert 1\rangle$	$\frac{\vert 0\rangle-\vert 1\rangle}{\sqrt{2}}$

$$H=(X+Z)/\sqrt{2}$$

π/8 gate:



$$T=\begin{bmatrix}1 & 0\\ 0 & e^{i\pi/4}\end{bmatrix}$$

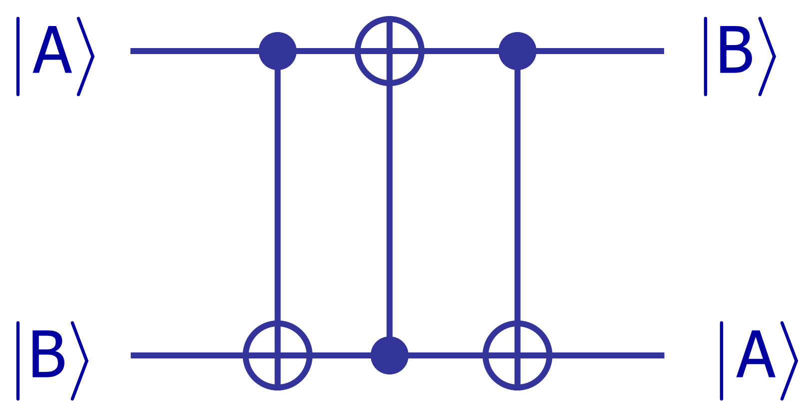
Phase gate S:

$$S=\begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}$$

$$S=T^2$$

From gates to circuits

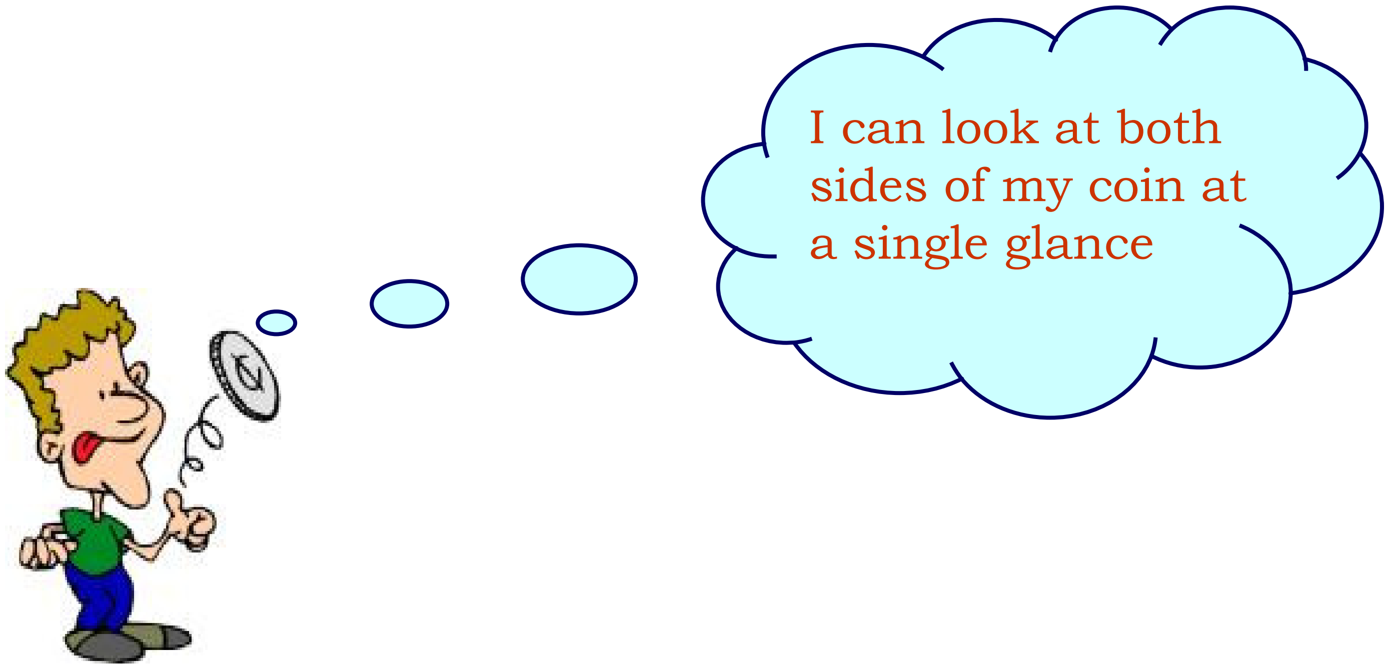
Example: swap circuit



Differences with classical circuits

- No loops - no feedback from one part of circuit to another.
- No wires joined together since it is not reversible.
- No "copy a qubit" operation (forbidden by quantum mechanics).

Quantum parallelism



Quantum parallelism

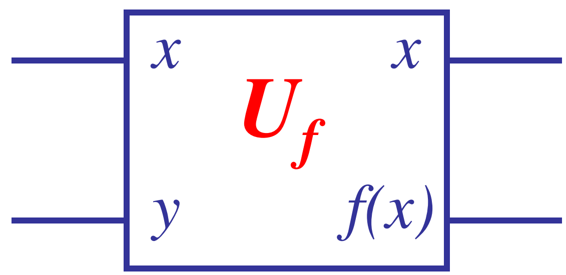
$$f(x):\{0,1\}\rightarrow\{0,1\}$$

$$|x,y\rangle \xrightarrow{U_f} |x, y\oplus f(x)\rangle$$

Superposition

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

$$|0\rangle$$

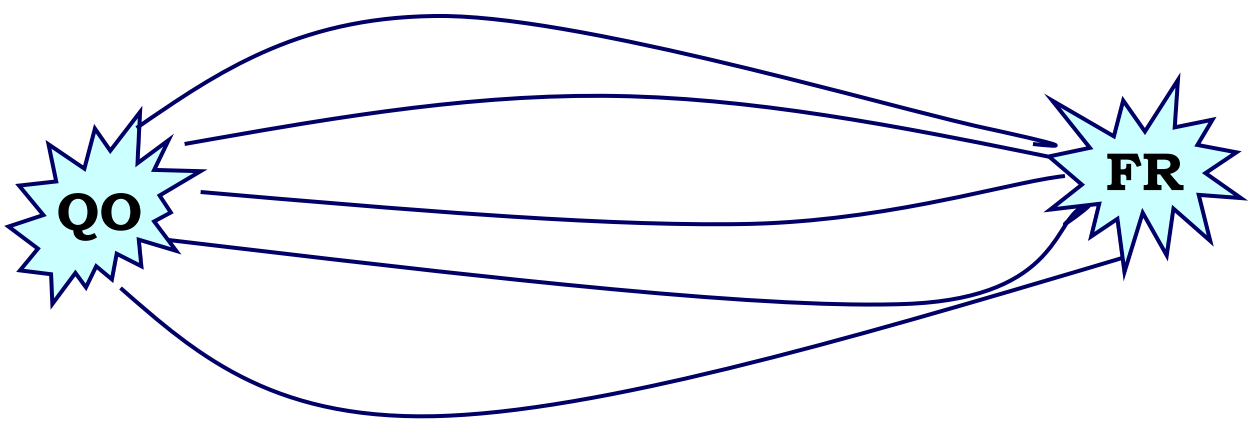


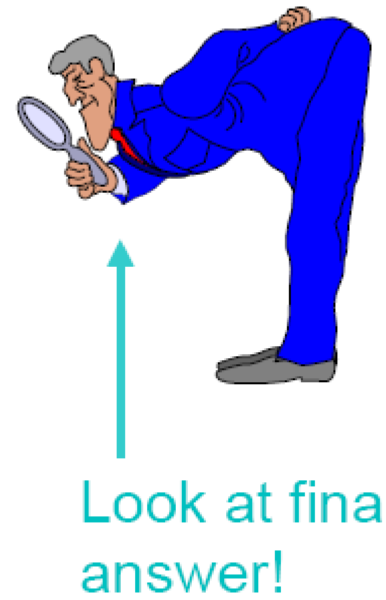
$$\frac{|0,f(0)\rangle+|1,f(1)\rangle}{\sqrt{2}}$$

Single circuit just evaluated ***f(x)*** for **both** x=0 and 1 simultaneously!

Quantum parallelism:
a major problem

- So we can evaluate functions for all values of x at the same time using just one circuit!
- Need only n+1 qubits to evaluate 2^n values of x.
- But we still get only one answer when we measure the result: it collapses to x,f(x)!!!





Quantum algorithms

Unique features of quantum computation

- Superposition: n qubits can represent 2^n integers.
- Problem: if we read the outcome we lose the superposition and we can't know with certainty which one of the values we will obtain.

- Entanglement: measurements of states of different qubits may be highly correlated.

Current advantages of quantum computation

- Shor's quantum Fourier transform provides exponential speedup over known classical algorithms.
- Applications: solving discrete logarithm and factoring problems which enables a quantum computer to break public key cryptosystems such as RSA.
- Quantum searching (Grover's algorithm) allows quadratic speedup over classical computers.
- Simulations of quantum systems.

How to factor 15?

- Pick a number less then 15: 7
- Calculate 7^n mod 15:

n	7^n	15×A	7^n mod 15
1	7	1	7
2	49	45	4
3	343	330	13
4	2401	2400	1

R=4

- Calculate $\gcd\left\{7^{R/2} \pm 1, 15\right\}$
- $\gcd\{48,15\} = 3,\ \gcd\{50,15\} = 5$

Shor's algorithm for N=15

- Choose n such as 2^n<15: n=4
- Choose y: y=7
- Initialize two four-qubit register $|\psi_0\rangle = |0000\rangle|0000\rangle$
- Create a superposition of states of the first register
- Compute the function $f(k)=7^k$ mod 15 on the second register.
- Operate on the first register by a Fourier transform
- Measure the state of the first register: u=0, 4, 8, 12 are only non-zero results.
- Two cases give period R=4, therefore the procedure succeeds with probability 1/2 after one run.

Back to the real world:

What do we need to build a quantum computer?

- **Qubits** which retain their properties.

  Scalable array of qubits.

- **Initialization:** ability to prepare one certain state repeatedly on demand. Need continuous supply of $|0\rangle$.

- **Universal set of quantum gates.** A system in which qubits can be made to evolve as desired.

- **Long relevant decoherence times.**

- Ability to efficiently **read out the result.**

The Mid-Level Quantum Computation Roadmap: Promise Criteria

QC Approach	The DiVincenzo Criteria						
	Quantum Computation					QC Networkability	
	#1	#2	#3	#4	#5	#6	#7
NMR	🔴	🟡	🟡	🟢	🟡	🔴	🔴
Trapped Ion	🟡	🟢	🟡	🟢	🟢	🟡	🟡
Neutral Atom	🟡	🟢	🟡	🟡	🟡	🟡	🟡
Cavity QED	🟡	🟢	🟡	🟡	🟢	🟡	🟡
Optical	🟡	🟡	🟢	🟡	🟡	🟡	🟢
Solid State	🟡	🟡	🟡	🟡	🟡	🔴	🔴
Superconducting	🟡	🟢	🟡	🟡	🟡	🔴	🔴
Unique Qubits	This field is so diverse that it is not feasible to label the criteria with "Promise" symbols.						

Legend: 🟢 = a potentially viable approach has achieved sufficient proof of principle

🟡 = a potentially viable approach has been proposed, but there has not been sufficient proof of principle

🔴 = no viable approach is known