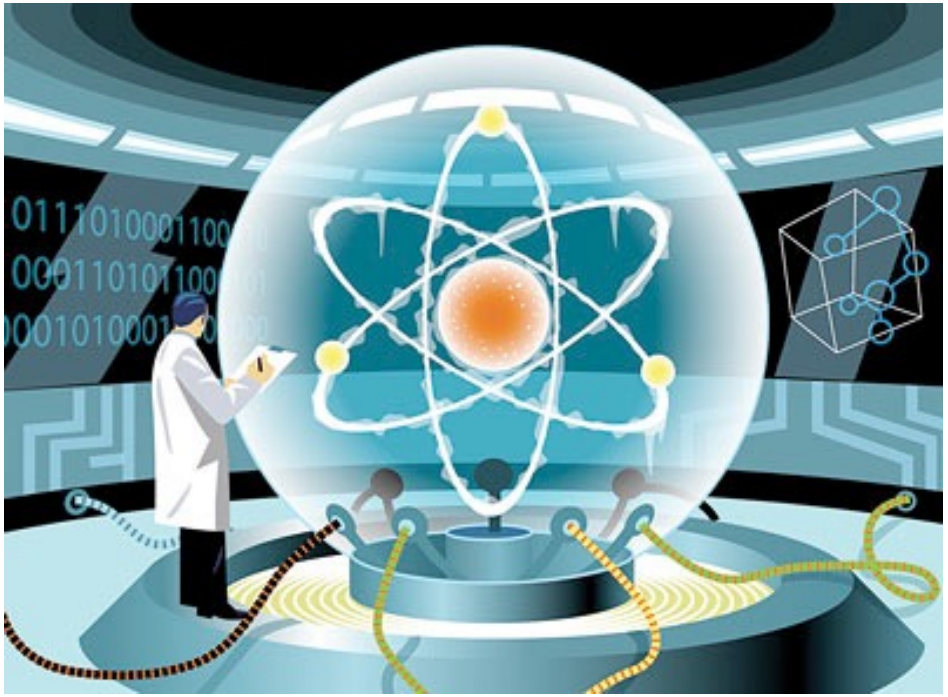
15-251
Great Theoretical Ideas in Computer Science

Lecture 25:
Quantum Computation: A very gentle introduction



November 24th, 2015

NOTE

This lecture is completely for fun.

It contains very little technical content.

The plan

Classical computers and classical theory of computation

Quantum physics (what the fuss is all about)

Quantum computers
(practical, scientific, and philosophical perspectives)

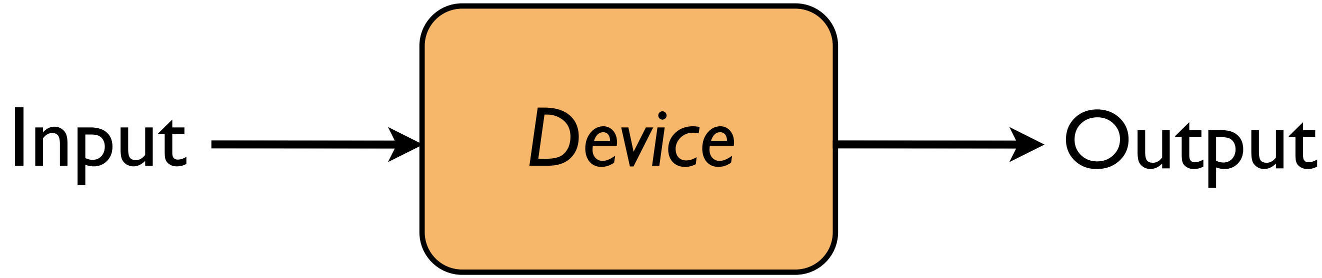
The plan

Classical computers and classical theory of computation

What is a computer?

A device that manipulates/processes data (information)

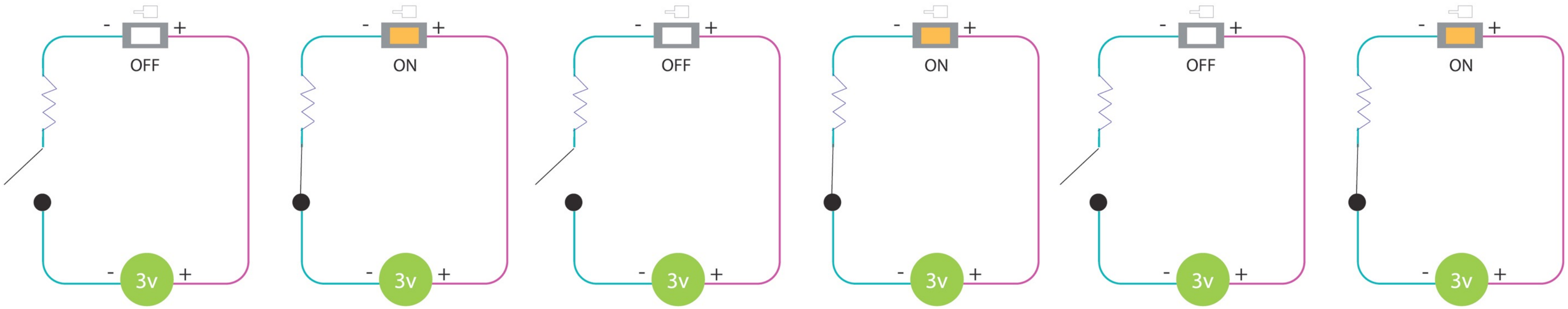
Usually



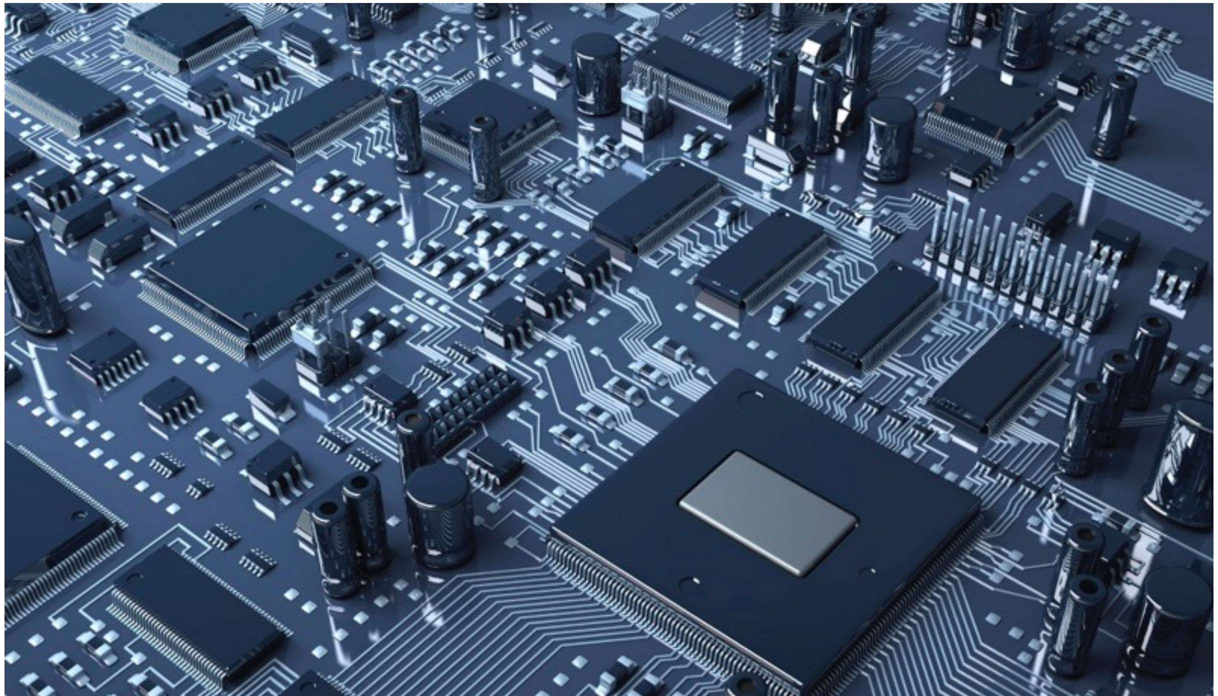
Examples:

How is data stored and processed ?

Data can be represented using a sequence of switches.



A sequence of bits (0s and 1s)

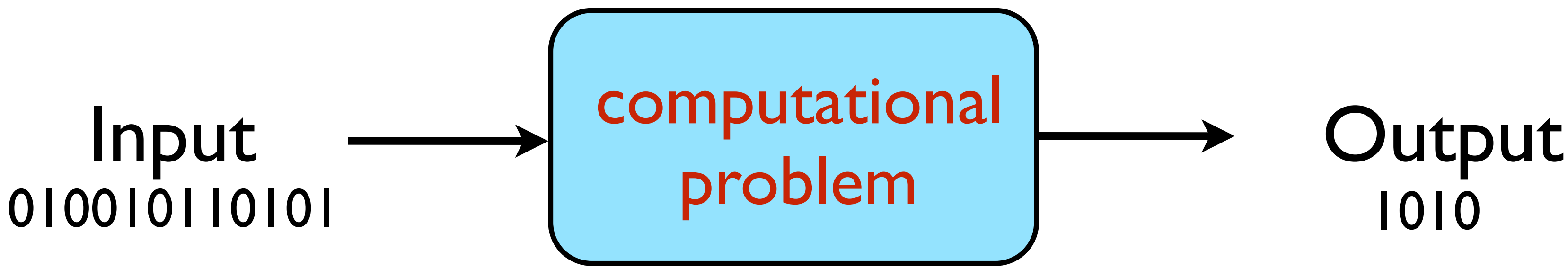


Circuits implement basic operations / instructions.

Everything follows classical laws of physics.

Theory of computation

We want to solve (efficiently) computational problems:



<u>Examples:</u>

Sorting
Sort a list of numbers.

Traveling Salesman Problem
Given a list of cities and distances between each pair, find the shortest route that travels each city once.

Factoring
Given an integer, find its prime factors.

Theory of computation

Computability

Is the computational problem computable?

Complexity

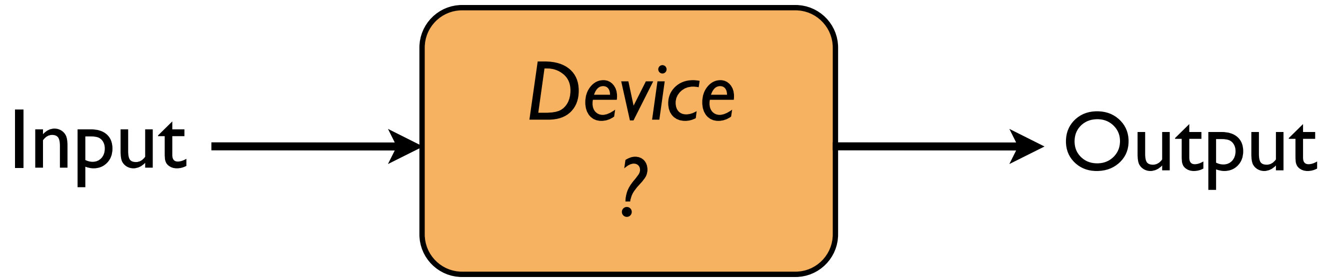
How complex is the computational problem
(with respect to *time* and *space/memory* required)

Factor

`2037035976334486086268445688409378161051468393665936250636140449354381299763336706183397`

Theory of computation

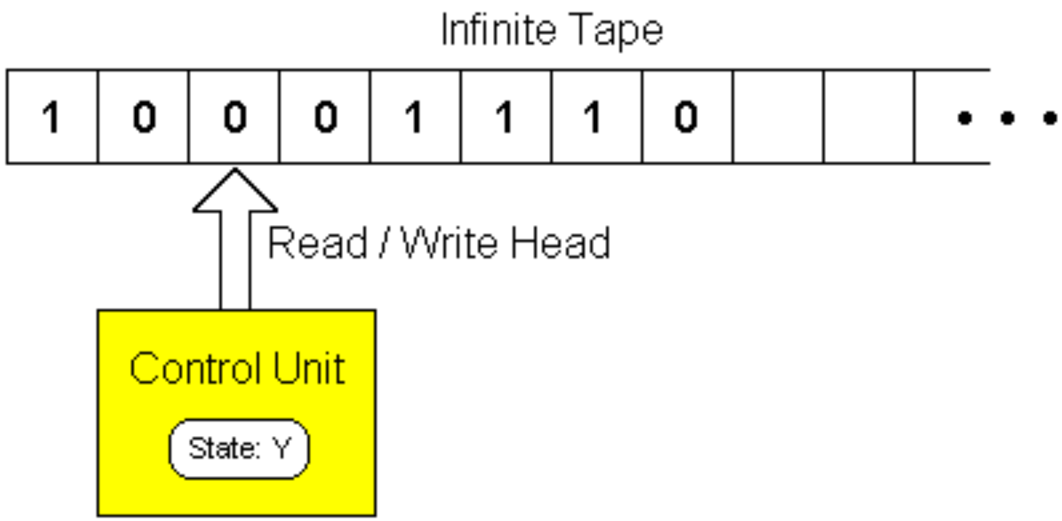
Which computer are we using ?
(MacBook Pro, MacBook Air, Dell, Samsung, Sony?)



To study computability and complexity rigorously:
need a universal mathematical model of a computer.

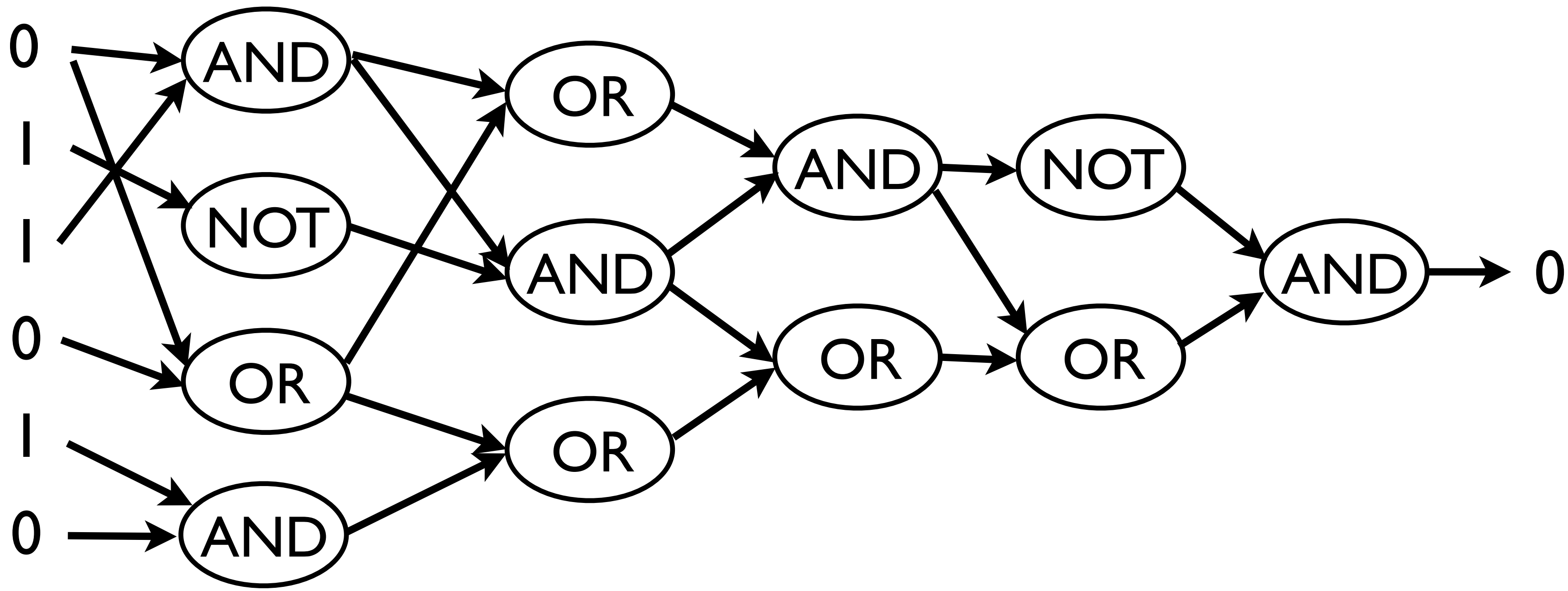
Turing Machines ~ **Boolean Circuits**

Turing Machines



Theory of computation

Boolean Circuits



Complexity:

How many <u>local</u> operations do we need to do in order to compute the problem/function?

~ how much time do we need to compute it?

(Physical) Church-Turing Thesis

Turing Machines ~ (Uniform) Boolean Circuits

universally capture all of computation.

(Physical) Church Turing Thesis

Any computational problem that can be solved by a physical device, can be solved by a Turing Machine.

Strong version

Any computational problem that can be solved *efficiently* by a physical device, can be solved *efficiently* by a Turing Machine.

The plan

Classical computers and classical theory of computation

Quantum physics (what the fuss is all about)

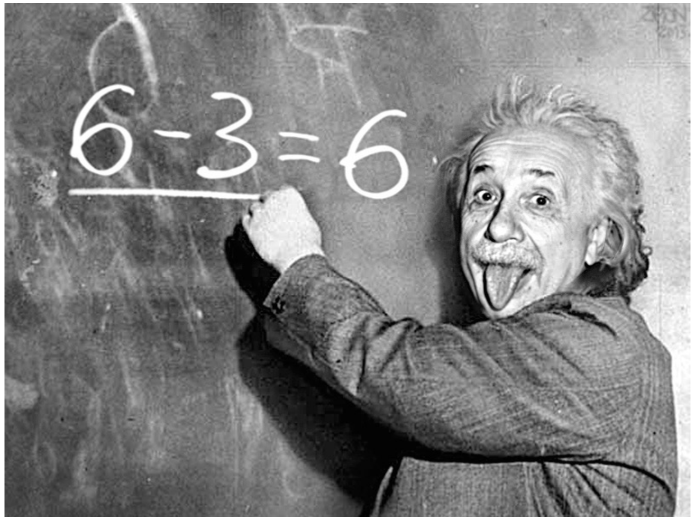
Quantum computers
(practical, scientific, and philosophical perspectives)

The plan

Quantum physics (what the fuss is all about)

One slide course on physics

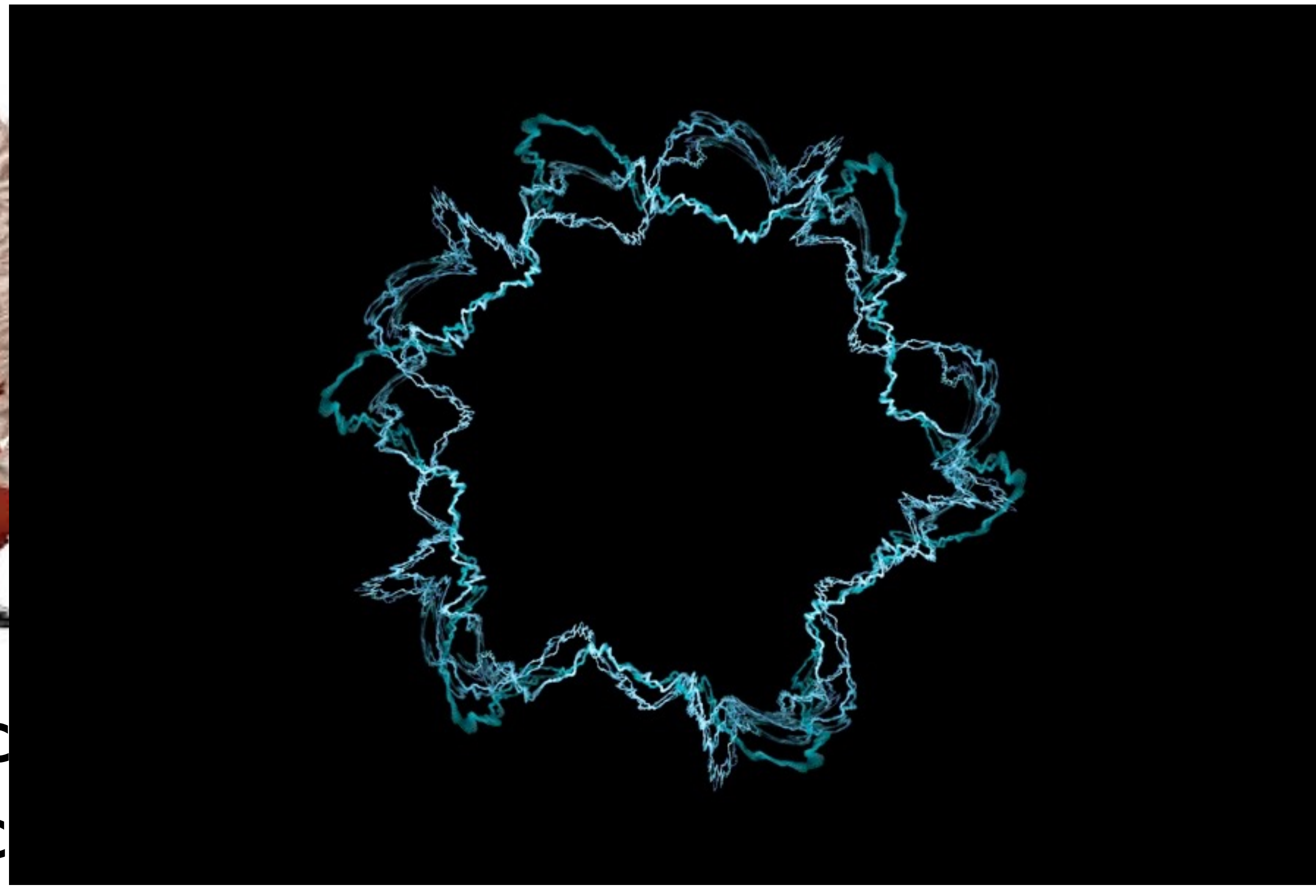
Classical
Physics

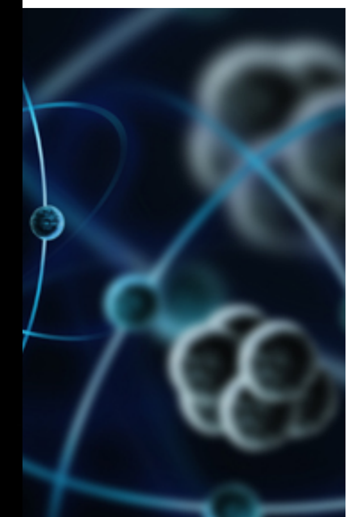


General Theory
of Relativity

Quantum
Physics

One slide course on physics





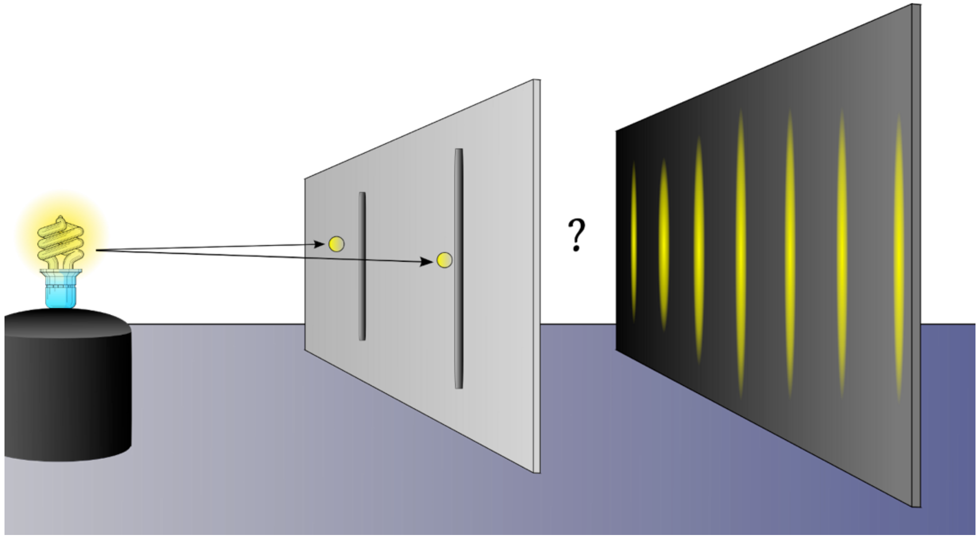
Classic
Physic

antum
ysics

String Theory (?)

Video: Double slit experiment

http://www.youtube.com/watch?v=DfPeprQ7oGc



Keep in mind:

Nature has no obligation to conform to your intuitions.

Video: Double slit experiment

Two interesting aspects of quantum physics

Having multiple states simultaneously

Example: electrons can have states
spin "up" or spin "down". $|\mathrm{up}\rangle$ or $|\mathrm{down}\rangle$

In reality, they can be in both states at the same time.

A superposition of two states.

Measurement

Quantum property is **very** sensitive/fragile !

If it interacts with the outside world, magic is gone.

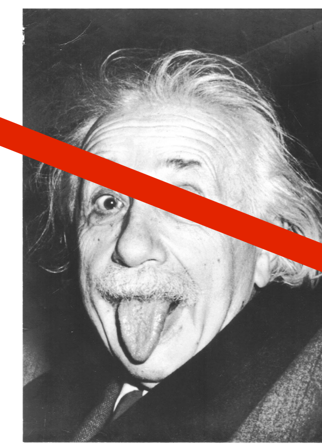
So you'll never see $|\mathrm{up}\rangle$ and $|\mathrm{down}\rangle$ simultaneously.

It must be just our ignorance

- There is no way that in reality, the electron has two states simultaneously.
- We don't know its state, so we say it is in *superposition*.
- In reality, it is always in one of the two states.
- This is why when we measure/observe the state, we find it in one state.

God does not play dice with the world.

- *Albert Einstein*



Einstein, don't tell God what to do.

- *Niels Bohr*

How should we fix our intuitions
to put it in line with experimental results ?

Removing physics from quantum physics

mathematics underlying quantum physics

=

generalization/extension of probability theory

(allow "negative probabilities")

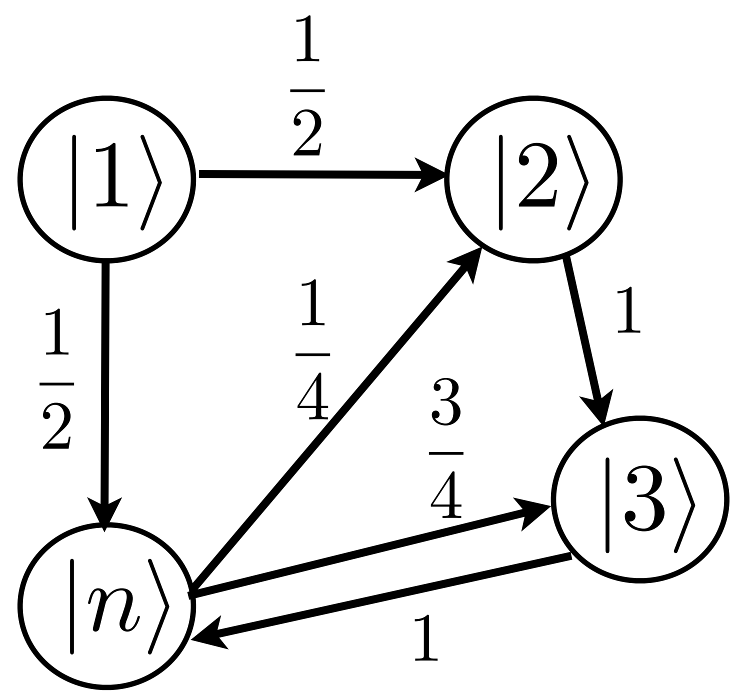
Probabilistic states

Suppose an object can have n possible states:

$$|1\rangle, |2\rangle, \cdots, |n\rangle$$

At each time step, the state can change.

What happens if we start at state $|1\rangle$ and evolve?



Initial state:

$$\begin{array}{c} |1\rangle \\ |2\rangle \\ |3\rangle \\ \\ |n\rangle \end{array} \begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

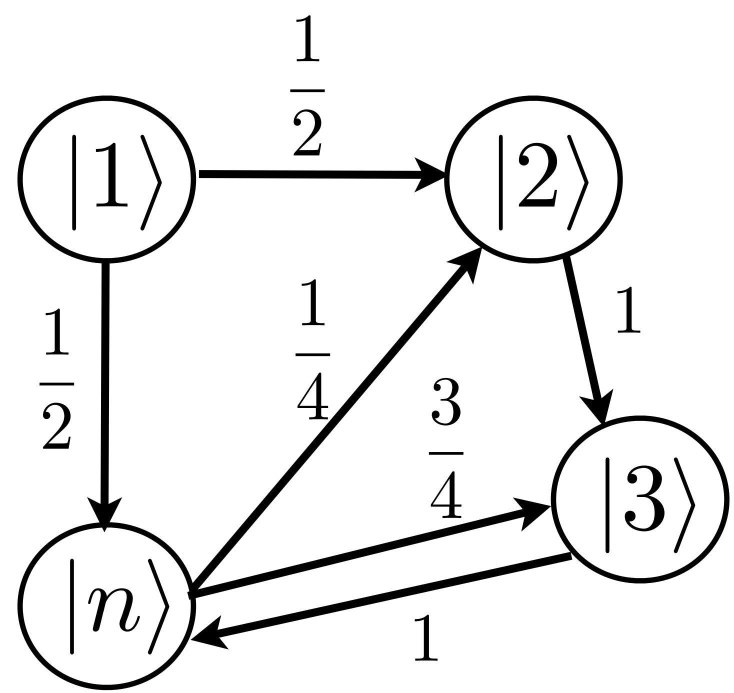
Probabilistic states

Suppose an object can have n possible states:

$$|1\rangle, |2\rangle, \cdots, |n\rangle$$

At each time step, the state can change.

What happens if we start at state $|1\rangle$ and evolve?



After one time step:

$$\begin{bmatrix}\text{Transition}\\ \text{Matrix}\end{bmatrix}\begin{array}{c}|1\rangle\\ |2\rangle\\ |3\rangle\\ \\ |n\rangle\end{array}\begin{bmatrix}1\\ 0\\ 0\\ \vdots\\ 0\end{bmatrix} = \begin{bmatrix}0\\ 1/2\\ 0\\ \vdots\\ 1/2\end{bmatrix}$$

Probabilistic states

$$\begin{bmatrix} \\ \text{Transition} \\ \text{Matrix} \\ \\ \end{bmatrix} \begin{array}{c} |1\rangle \\ |2\rangle \\ |3\rangle \\ \\ |n\rangle \end{array} \begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1/2 \\ 0 \\ \vdots \\ 1/2 \end{bmatrix}$$

the new state (probabilistic)

A general probabilistic state:

$$\begin{bmatrix} p_1 \\ p_2 \\ \vdots \\ p_n \end{bmatrix}$$

$p_i = \text{ the probability of being in state } i$

$p_1 + p_2 + \cdots + p_n = 1$

$(\ell_1 \text{ norm is } 1)$

Probabilistic states

$$\begin{bmatrix} \\ \text{Transition} \\ \text{Matrix} \\ \\ \end{bmatrix} \begin{array}{c} |1\rangle \\ |2\rangle \\ |3\rangle \\ \\ |n\rangle \end{array} \begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1/2 \\ 0 \\ \vdots \\ 1/2 \end{bmatrix}$$

the new state (probabilistic)

A general probabilistic state:

$$\begin{bmatrix} p_1 \\ p_2 \\ \vdots \\ p_n \end{bmatrix} = p_1 \underset{\begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}}{|1\rangle} + p_2 \underset{\begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix}}{|2\rangle} + \cdots + p_n \underset{\begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}}{|n\rangle}$$

Probabilistic states

Evolution of probabilistic states

$$\begin{bmatrix} \text{Transition} \\ \text{Matrix} \\ \\ \end{bmatrix}$$

It can be any matrix that maps probabilistic states to probabilistic states.

In general we won't restrict ourselves to just one transition matrix.

$$\pi_0 \xrightarrow{K_1} \pi_1 \xrightarrow{K_2} \pi_2 \xrightarrow{K_3} \cdots$$

Quantum states

$$\begin{bmatrix} p_1 \\ p_2 \\ \vdots \\ p_n \end{bmatrix}$$

p_i's can be negative.

Quantum states

α_i's can be negative.

α_i 's are called amplitudes.

$$\begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix} = \alpha_1|1\rangle + \alpha_2|2\rangle + \cdots + \alpha_n|n\rangle$$

$$\alpha_1^2 + \alpha_2^2 + \cdots + \alpha_n^2 = 1 \quad (\ell_2 \text{ norm is } 1)$$

(α_i can be a complex number)

$$\begin{bmatrix} \text{Unitary} \\ \text{Matrix} \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix} = \begin{bmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{bmatrix} \qquad \beta_1^2 + \beta_2^2 + \cdots + \beta_n^2 = 1$$

any matrix that preserves the "quantumness"

Quantum states

Evolution of quantum states

$$\begin{bmatrix} \\ \text{Unitary} \\ \text{Matrix} \\ \\ \end{bmatrix}$$

It can be any matrix that maps quantum states to quantum states.

In general we won't restrict ourselves to just one unitary matrix.

$$\psi_0 \xrightarrow{U_1} \psi_1 \xrightarrow{U_2} \psi_2 \xrightarrow{U_3} \cdots$$

Quantum states

Measuring quantum states

$$\begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix} = \alpha_1|1\rangle + \alpha_2|2\rangle + \cdots + \alpha_n|n\rangle$$

$$\alpha_1^2 + \alpha_2^2 + \cdots + \alpha_n^2 = 1$$

When you measure the state, you will see

state i with probability α_i^2 .

Probabilistic states vs Quantum states

Suppose we have just 2 possible states: $|0\rangle$ and $|1\rangle$

$$\begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1/2 \\ 1/2 \end{bmatrix}$$

$$\begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1/2 \\ 1/2 \end{bmatrix}$$

randomize a random state

$\longrightarrow$ random state

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

$$\frac{1}{2}\left(\frac{1}{2}|0\rangle + \frac{1}{2}|1\rangle\right) \qquad \frac{1}{2}\left(\frac{1}{2}|0\rangle + \frac{1}{2}|1\rangle\right)$$

$$\frac{1}{4}|0\rangle + \frac{1}{4}|1\rangle \quad + \quad \frac{1}{4}|0\rangle + \frac{1}{4}|1\rangle$$

Probabilistic states vs Quantum states

Suppose we have just 2 possible states: $|0\rangle$ and $|1\rangle$

$$\begin{bmatrix} 1/\sqrt{2} & -1/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{bmatrix}$$

$$\begin{bmatrix} 1/\sqrt{2} & -1/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2} \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} -1/\sqrt{2} \\ 1/\sqrt{2} \end{bmatrix}$$

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

$$\frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) \qquad \frac{1}{\sqrt{2}}\left(-\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)$$

$$\cancel{\frac{1}{2}|0\rangle} + \frac{1}{2}|1\rangle \quad + \quad -\cancel{\frac{1}{2}|0\rangle} + \frac{1}{2}|1\rangle = |1\rangle$$

Probabilistic states vs Quantum states

To find the probability of an event:

add the probabilities of every possible way it can happen

Probabilistic states vs Quantum states

Quantum

To find the probability of an event:

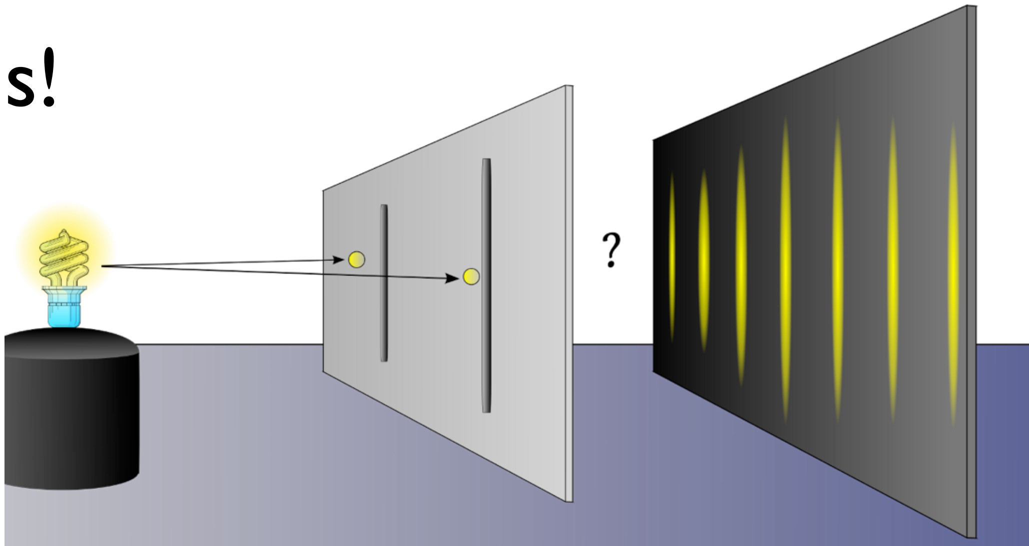
add the amplitudes of every possible way it can happen

square to get a positive probability value

one way has positive amplitude

other way has negative amplitude

event never happens!



Probabilistic states vs Quantum states

A final remark

Quantum states are an <u>upgrade</u> to:

2-norm (Euclidean norm) and algebraically closed fields.

Nature seems to be choosing the mathematically more elegant option.

The plan

Classical computers and classical theory of computation

Quantum physics (what the fuss is all about)

Quantum computers
(practical, scientific, and philosophical perspectives)

The plan

Quantum computers
(practical, scientific, and philosophical perspectives)

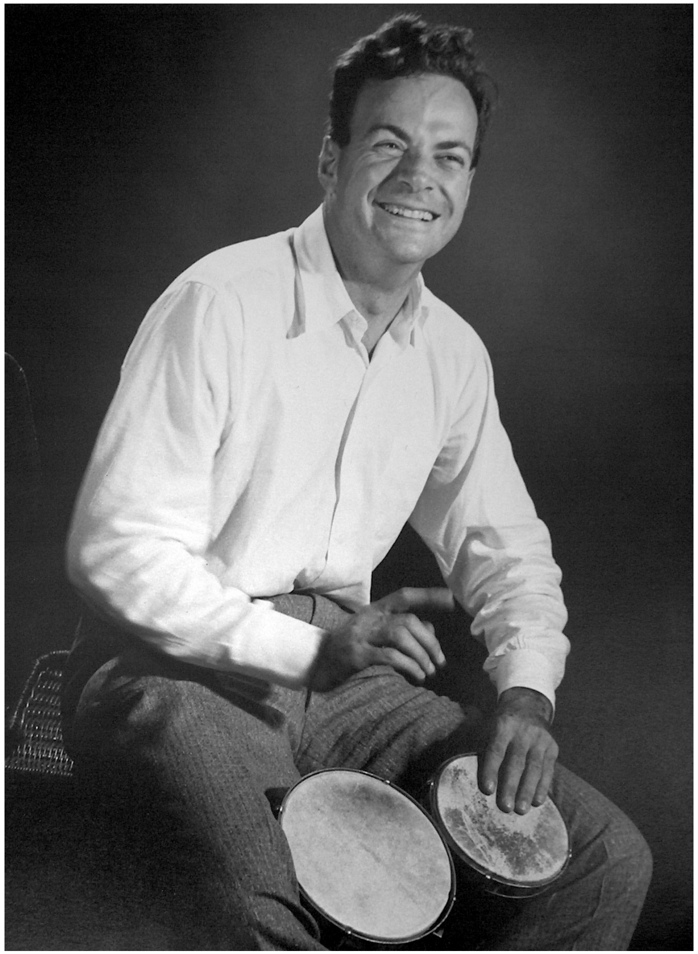
Two beautiful theories

Theory of computation

Quantum physics

Quantum Computation:

Information processing using laws of quantum physics.



Richard Feynman
(1918 - 1988)

It would be super nice to be able to simulate quantum systems.

With a classical computer this is extremely inefficient.

n state system $\longrightarrow$ complexity exponential in n

Why not view the quantum particles as a computer simulating themselves?

Why not do computation using quantum particles (quantum physics)?

Representing data

Recall: electrons can have states spin "up" or spin "down".

$|\mathrm{up}\rangle$ or $|\mathrm{down}\rangle$ ~ $|0\rangle$ or $|1\rangle$

A quantum bit: $\underline{\alpha_0|0\rangle + \alpha_1|1\rangle}$, $\alpha_0^2 + \alpha_1^2 = 1$
(qubit)

↓

A superposition of $|0\rangle$ and $|1\rangle$.

When you measure:

With probability α_0^2 it is $|0\rangle$.

With probability α_1^2 it is $|1\rangle$.

Representing data

<u>Recall</u>: electrons can have states spin "up" or spin "down".

$$|\mathrm{up}\rangle \quad \text{or} \quad |\mathrm{down}\rangle \qquad \sim \qquad |0\rangle \quad \text{or} \quad |1\rangle$$

A quantum bit: $\alpha_0|0\rangle + \alpha_1|1\rangle,$ $\qquad \alpha_0^2 + \alpha_1^2 = 1$
(qubit)

Two qubits:

$$\alpha_{00}|0\rangle|0\rangle + \alpha_{01}|0\rangle|1\rangle + \alpha_{10}|1\rangle|0\rangle + \alpha_{11}|1\rangle|1\rangle$$

we actually write it as:

$$\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

$$\alpha_{00}^2 + \alpha_{01}^2 + \alpha_{10}^2 + \alpha_{11}^2 = 1$$

Representing data

Recall: electrons can have states spin "up" or spin "down".

$$|\mathrm{up}\rangle \quad \text{or} \quad |\mathrm{down}\rangle \qquad \sim \qquad |0\rangle \quad \text{or} \quad |1\rangle$$

A quantum bit: $\alpha_0|0\rangle + \alpha_1|1\rangle,$ $\qquad \alpha_0^2 + \alpha_1^2 = 1$
(qubit)

Three qubits:

$$\alpha_{000}|000\rangle + \alpha_{001}|001\rangle + \alpha_{010}|010\rangle + \alpha_{011}|011\rangle +$$
$$\alpha_{100}|100\rangle + \alpha_{101}|101\rangle + \alpha_{110}|110\rangle + \alpha_{111}|111\rangle$$

$$\alpha_{000}^2 + \alpha_{001}^2 + \alpha_{010}^2 + \alpha_{011}^2 + \alpha_{100}^2 + \alpha_{101}^2 + \alpha_{110}^2 + \alpha_{111}^2 = 1$$

Processing data

What will be our model?

In the classical setting, we had:

Turing Machines

Boolean circuits

In the quantum setting, it is more convenient to use the circuit model.

Processing data: quantum gates

A qubit: $\alpha_0|0\rangle + \alpha_1|1\rangle, \qquad \alpha_0^2 + \alpha_1^2 = 1$

The only non-trivial gate for a single classical bit is

$$0 \longrightarrow \boxed{\text{NOT}} \longrightarrow 1$$

$$1 \longrightarrow \boxed{\text{NOT}} \longrightarrow 0$$

There are many non-trivial quantum gates for a single qubit.

<u>One famous example:</u> **Hadamard gate**

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

$$|1\rangle \longrightarrow \boxed{H} \longrightarrow \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

Can figure out how
it transforms
an arbitrary qubit

$$\alpha_0|0\rangle + \alpha_1|1\rangle$$

Processing data: quantum gates

A qubit: $\alpha_0|0\rangle + \alpha_1|1\rangle, \qquad \alpha_0^2 + \alpha_1^2 = 1$

The only non-trivial gate for a single classical bit is

$$0 \longrightarrow \boxed{\text{NOT}} \longrightarrow 1$$

$$1 \longrightarrow \boxed{\text{NOT}} \longrightarrow 0$$

There are many non-trivial quantum gates for a single qubit.

<u>One famous example:</u> **Hadamard gate**

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

$$|1\rangle \longrightarrow \boxed{H} \longrightarrow \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

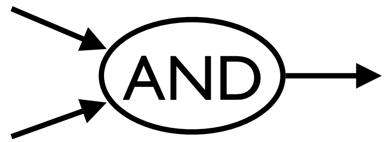
The "transition" matrix:

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

Processing data: quantum gates

A qubit: $\alpha_0|0\rangle + \alpha_1|1\rangle, \qquad \alpha_0^2 + \alpha_1^2 = 1$

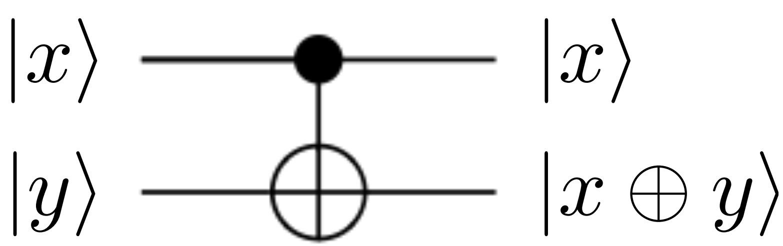
An example of a classical gate on <u>two</u> classical bits:



<u>A famous example of a quantum gate on 2 qubits:</u>

controlled NOT

For
$x, y \in \{0, 1\}$



<u>Notice:</u>

Input: 2 qubits

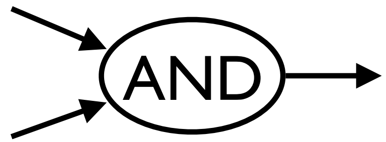
Output: 2 qubits

<u>Fact</u>: quantum operations must be "reversible".
(gates)

Processing data: quantum gates

A qubit: $\alpha_0|0\rangle + \alpha_1|1\rangle, \qquad \alpha_0^2 + \alpha_1^2 = 1$

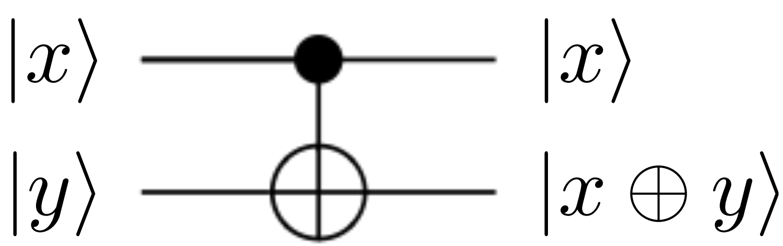
An example of a classical gate on <u>two</u> classical bits:



<u>A famous example of a quantum gate on 2 qubits:</u>

controlled NOT

For
$x, y \in \{0, 1\}$



"transition" matrix:

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

<u>**Fact**</u>: quantum operations must be "reversible".
(gates)

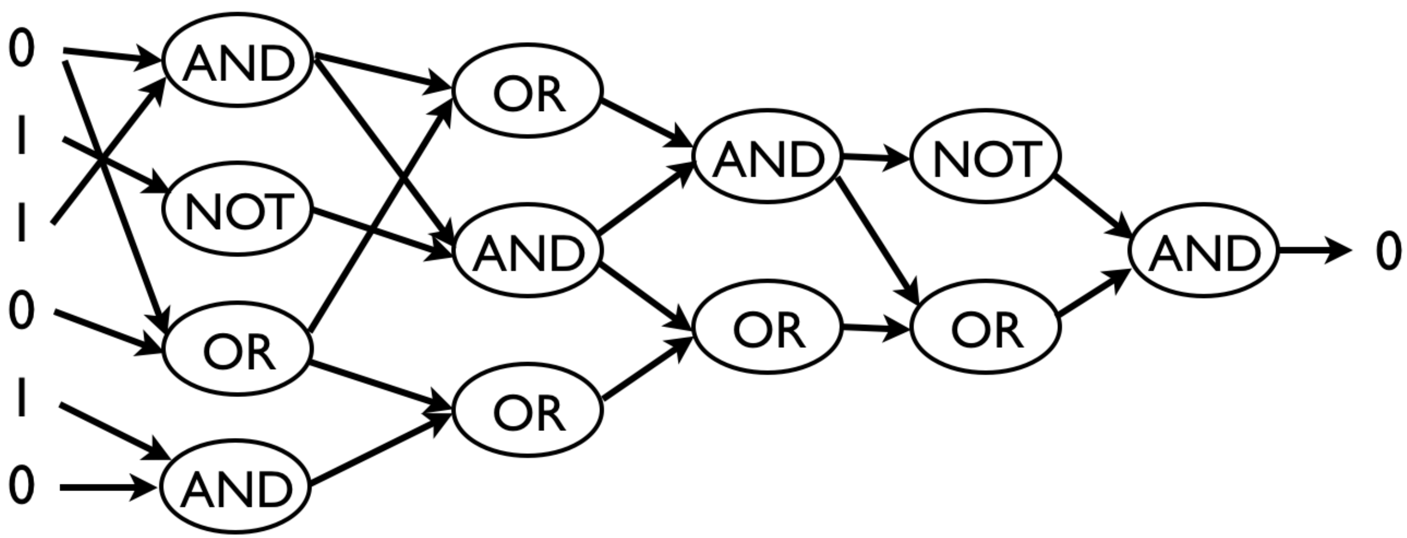
Processing data: quantum circuits

A classical circuit

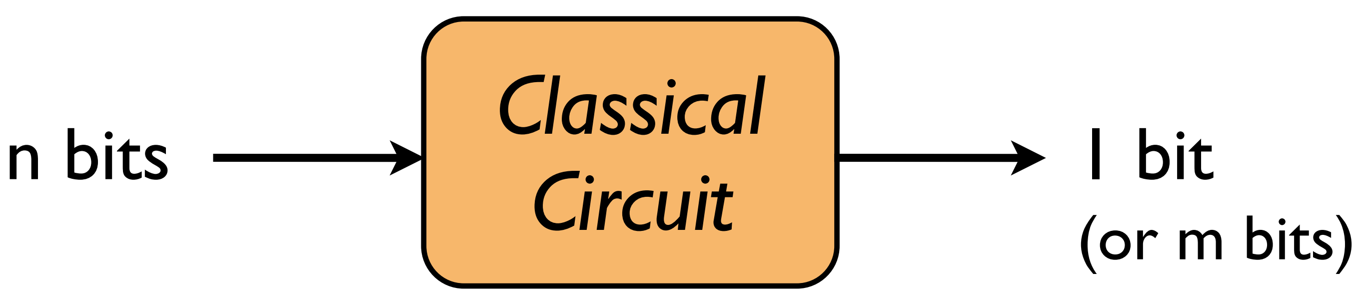
INPUT

OUTPUT

n bits



1 bit

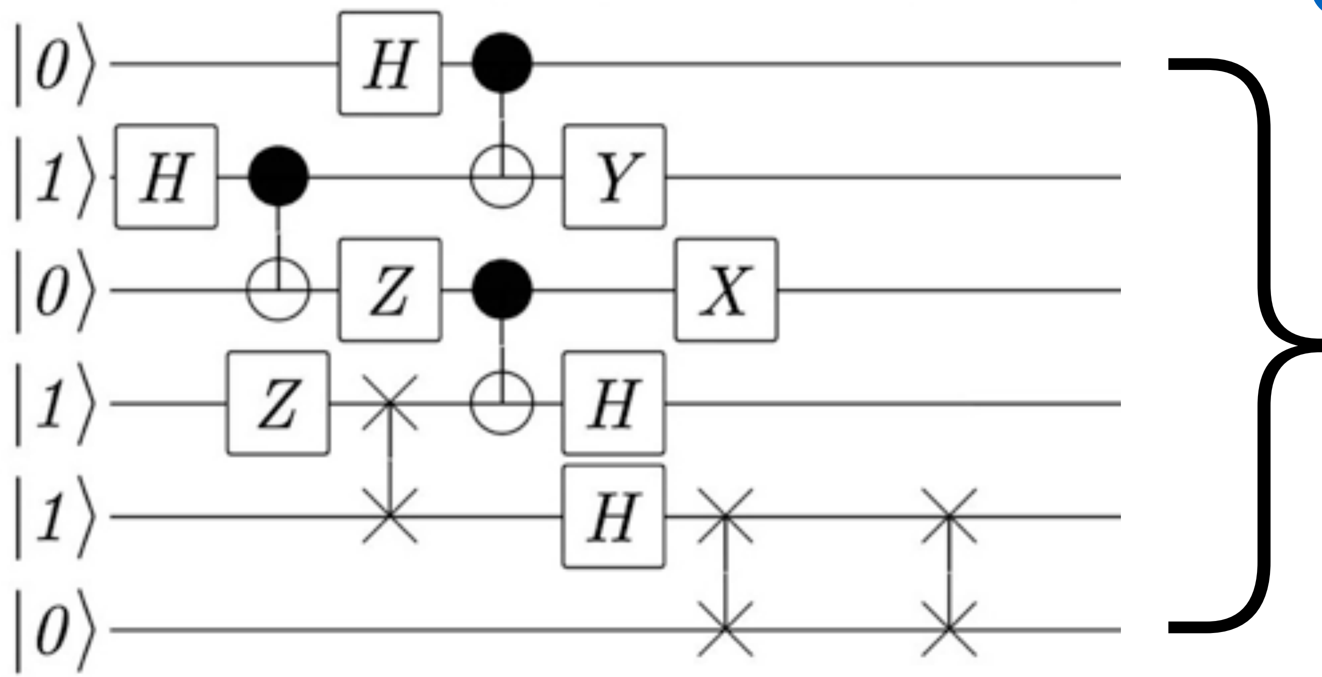


Processing data: quantum circuits

A quantum circuit

INPUT

n qubits



OUTPUT

n qubits

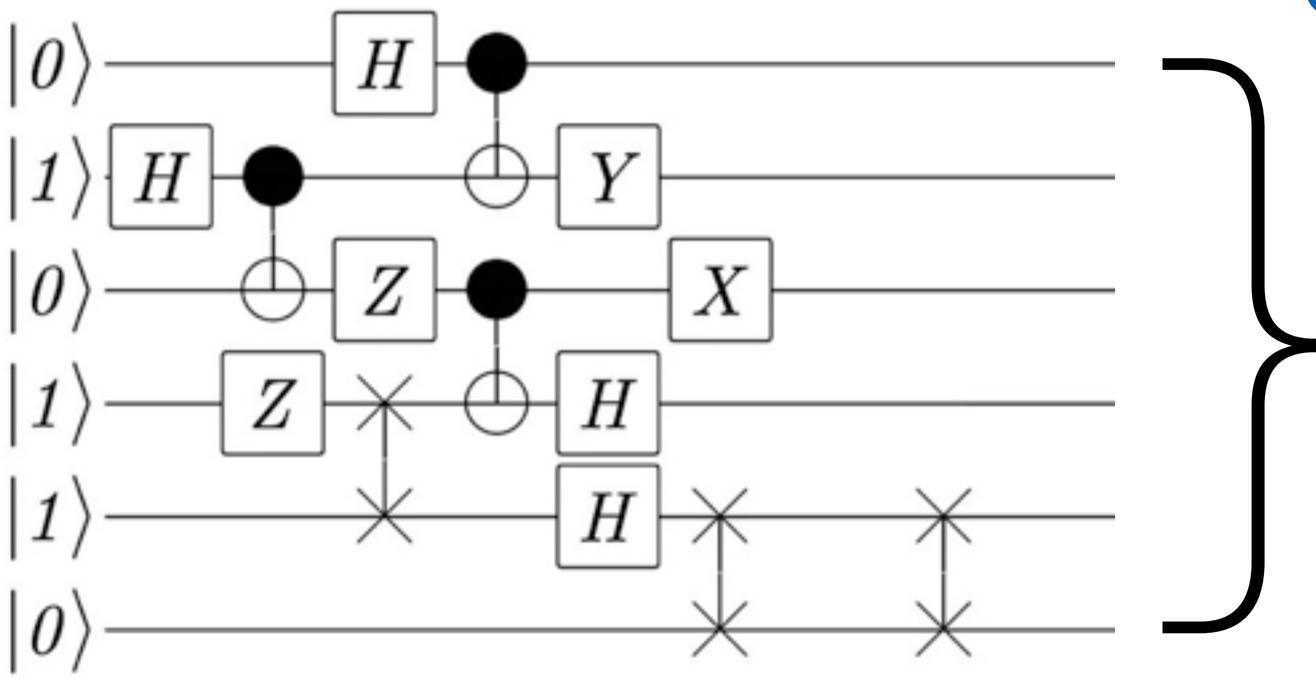
quantum gates

Processing data: quantum circuits

A quantum circuit

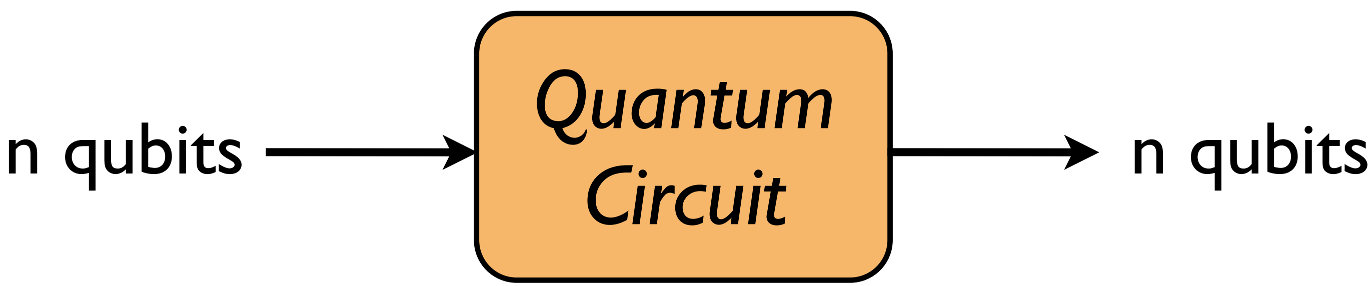
INPUT

n qubits



OUTPUT

n qubits



<u>Fact</u>: quantum operations must be "reversible".

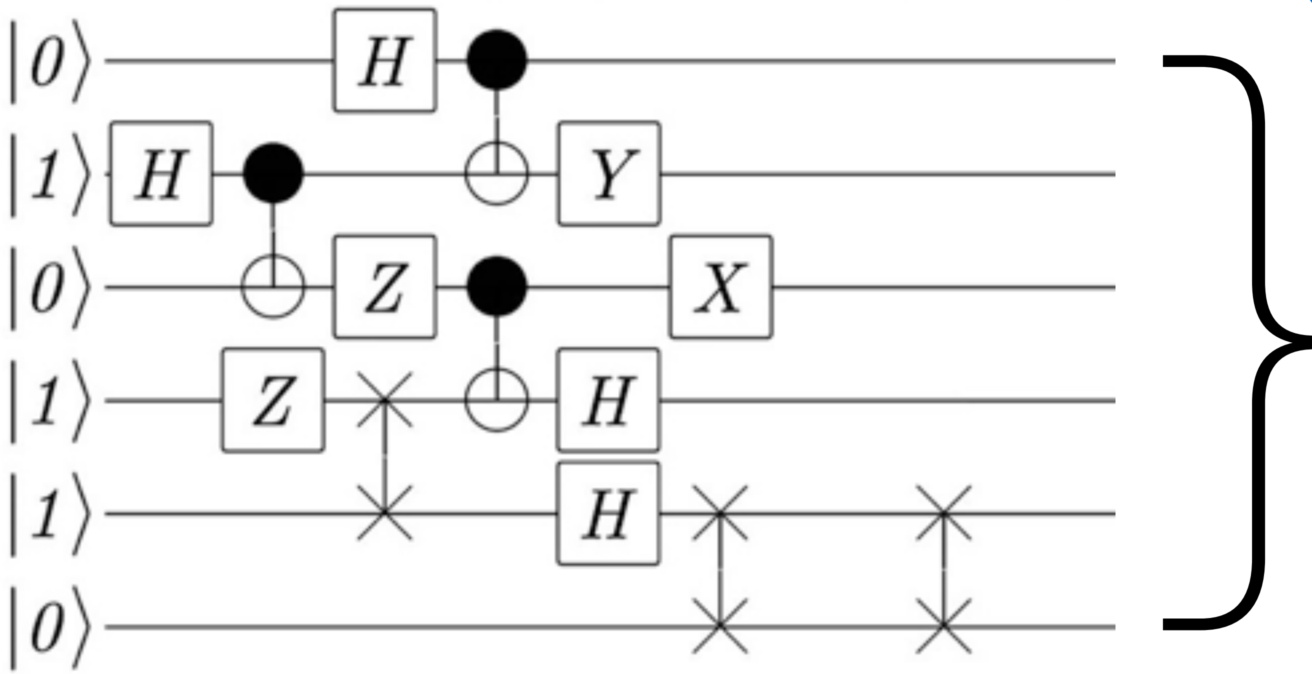
(gates) (circuits)

Processing data: quantum circuits

A quantum circuit

INPUT

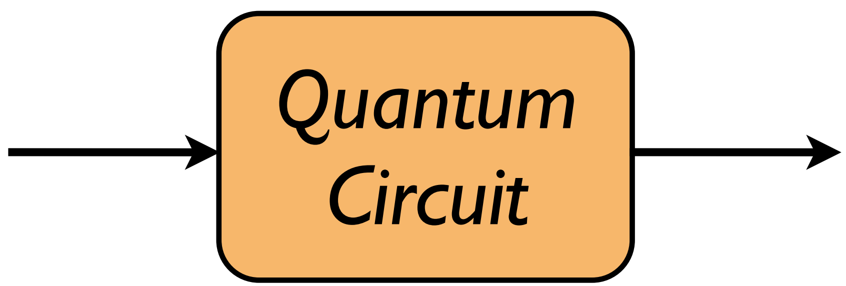
n qubits



OUTPUT

n qubits

$|0\rangle|1\rangle|0\rangle|1\rangle|1\rangle|0\rangle$



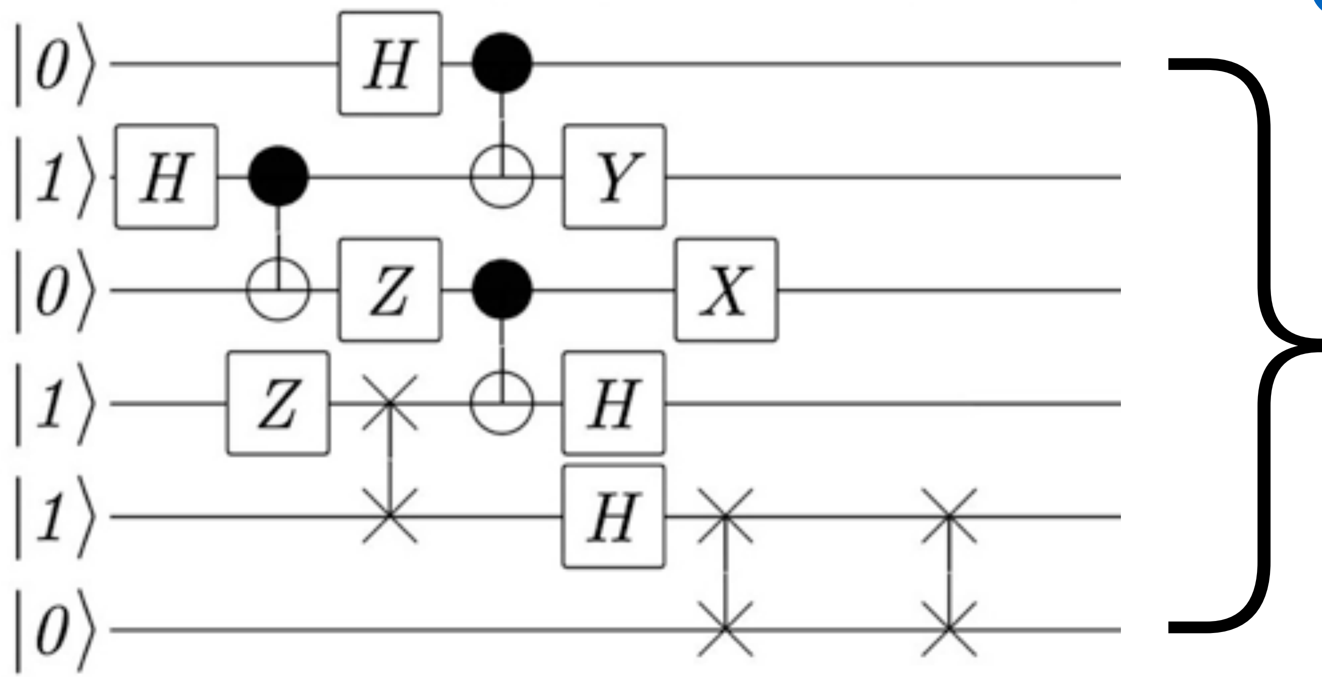
Processing data: quantum circuits

A quantum circuit

INPUT

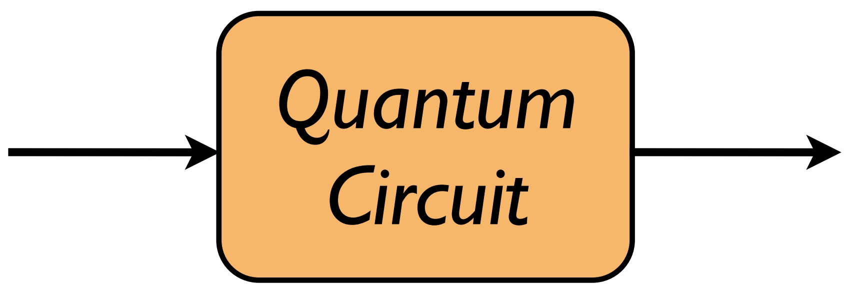
OUTPUT

n qubits



n qubits

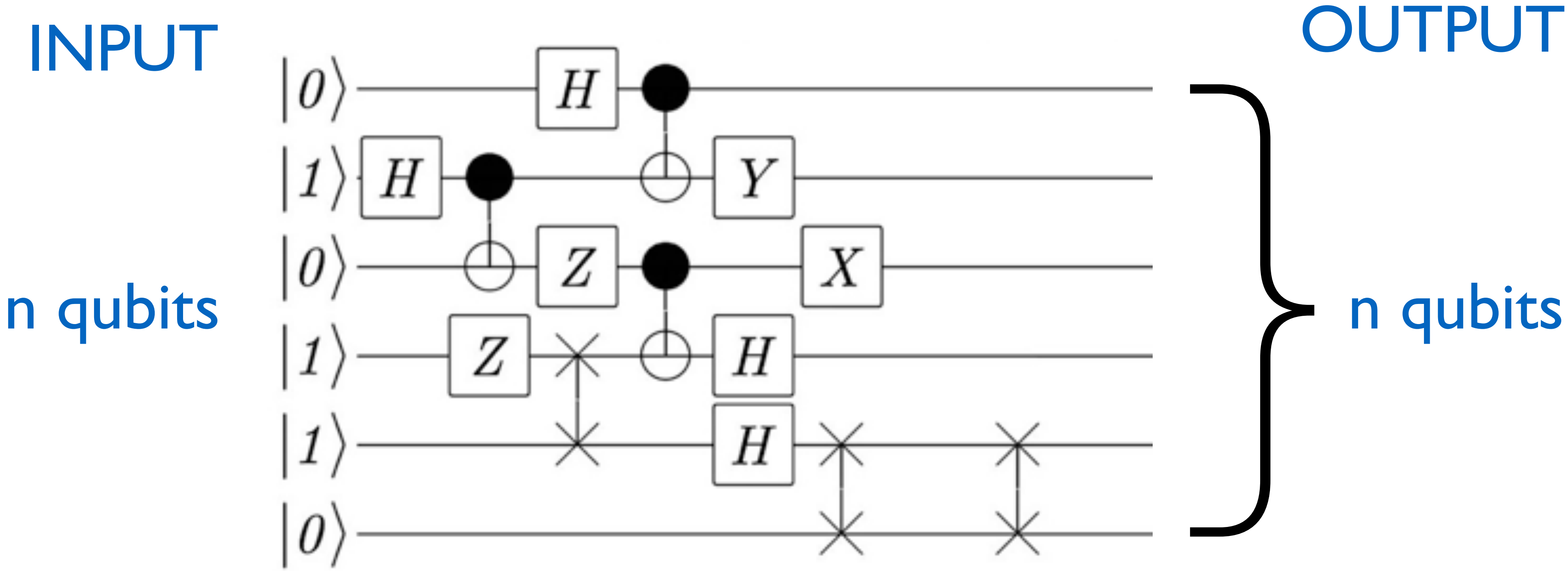
$|010110\rangle$

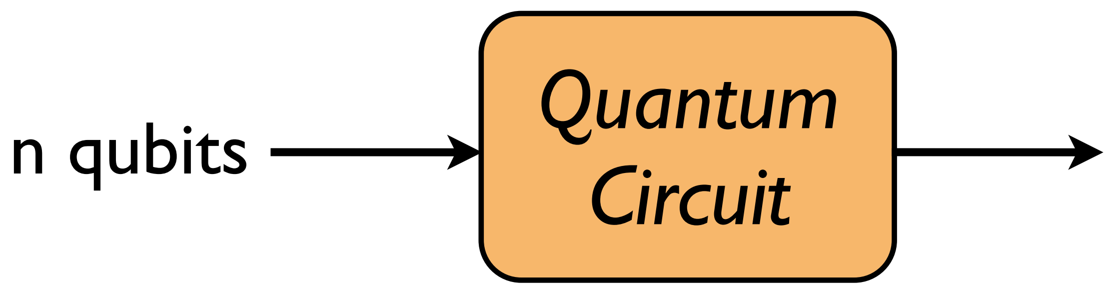


$$\alpha_{000000}|000000\rangle + \alpha_{000001}|000001\rangle + \alpha_{000010}|000010\rangle + \cdots \alpha_{111111}|111111\rangle$$

Processing data: quantum circuits

A quantum circuit





superposition of 2^n possible states.

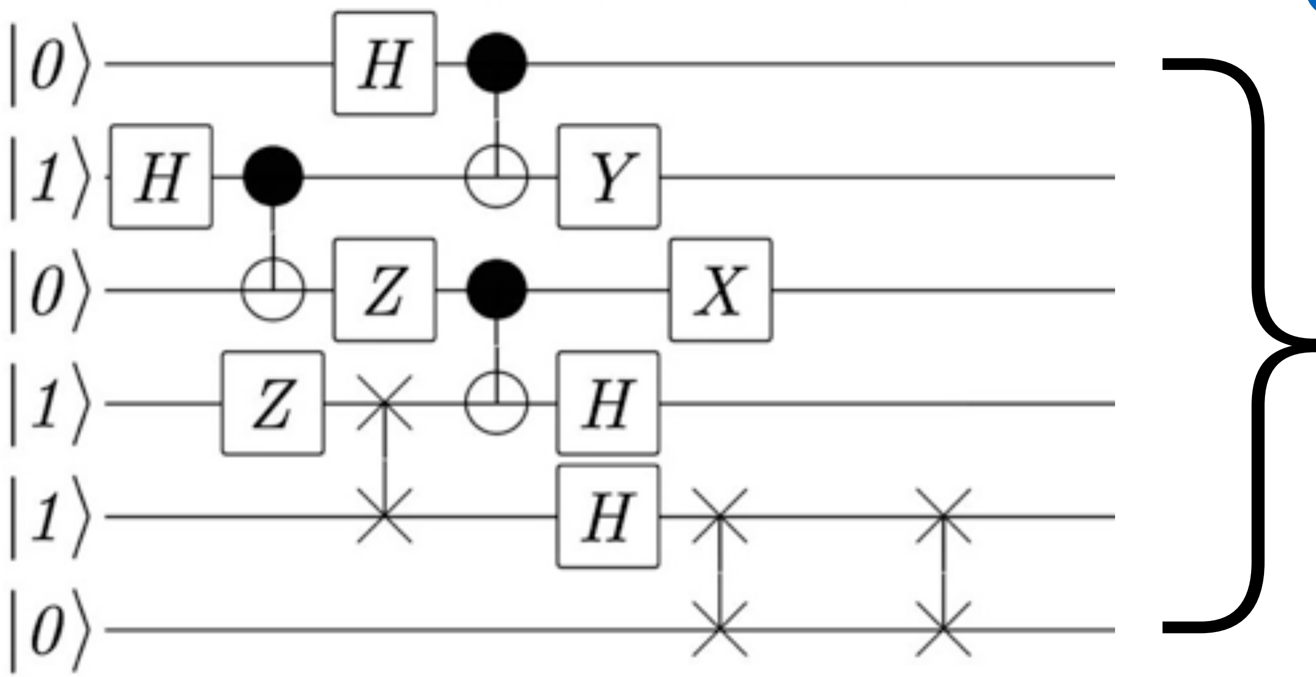
2^n amplitudes.

Processing data: quantum circuits

A quantum circuit

INPUT

n qubits



OUTPUT

n qubits

How do we get classical information out of the circuit?

We measure the output qubit(s). I.e., we measure:

$$\alpha_{000000}|000000\rangle + \alpha_{000001}|000001\rangle + \cdots + \alpha_{111111}|111111\rangle$$

Or we can measure the first qubit.

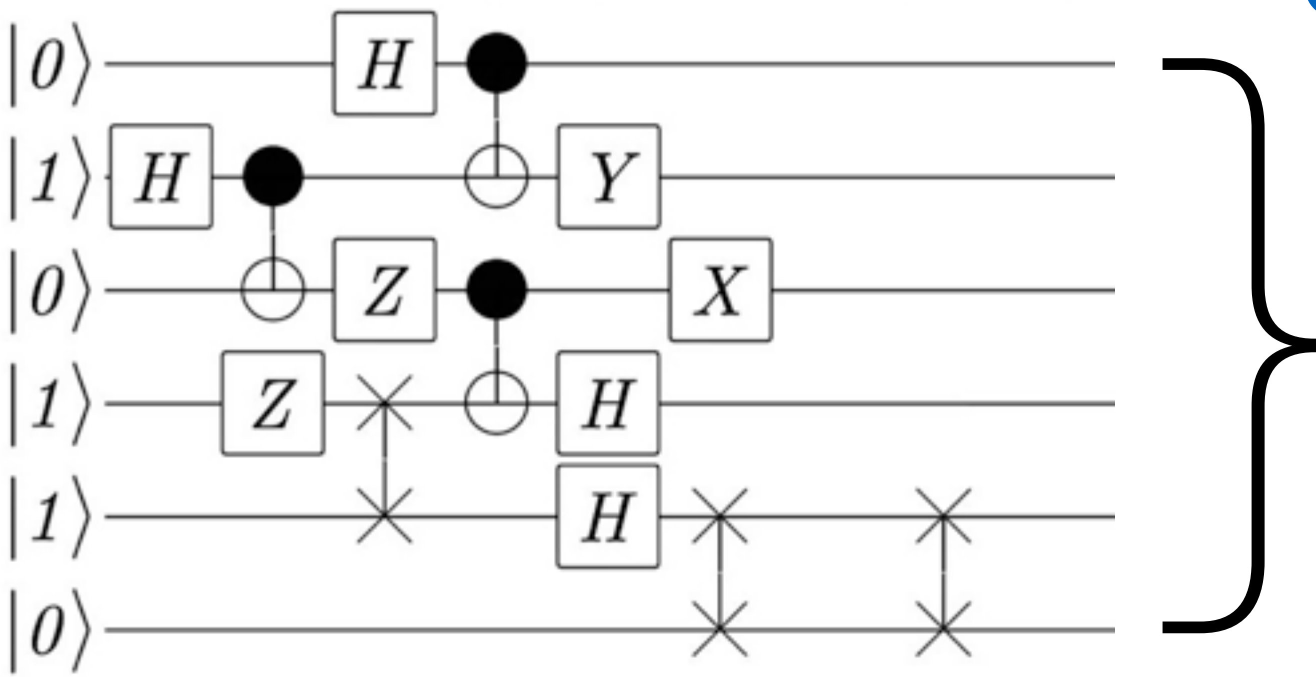
Processing data: quantum circuits

A quantum circuit

INPUT

OUTPUT

n qubits



n qubits

Which quantum gates can we use?

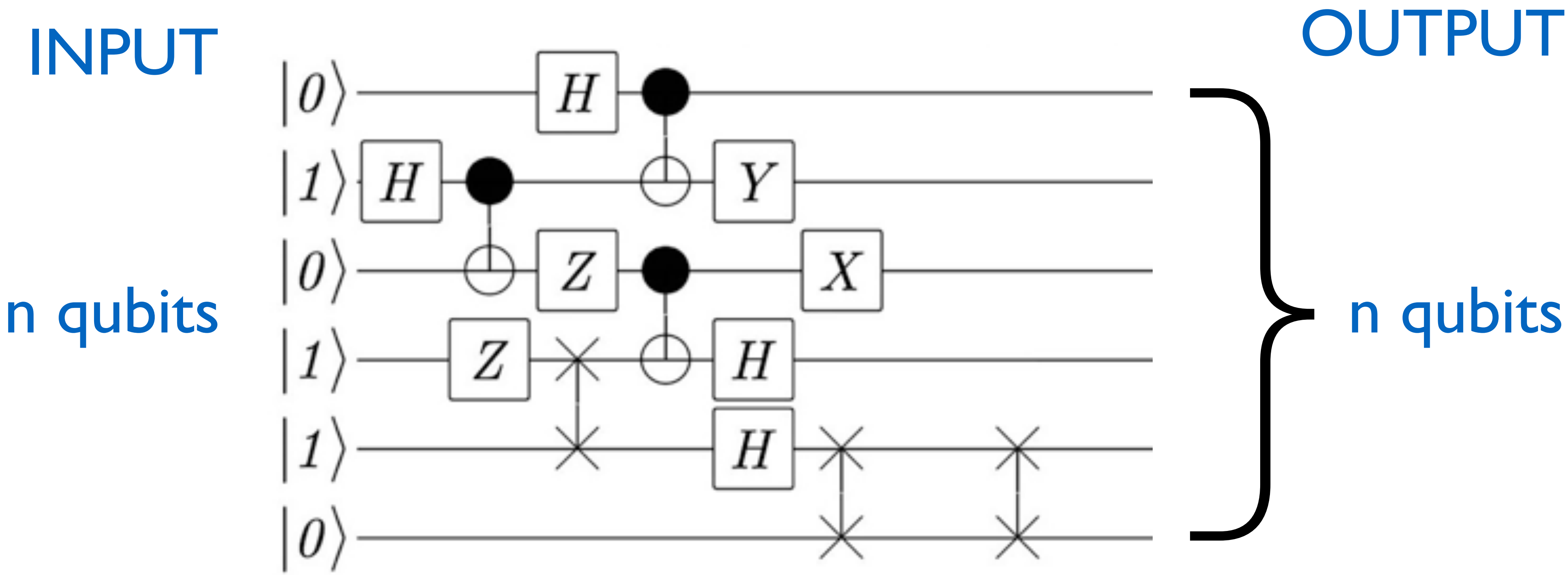
The choice doesn’t matter as long as they are “universal”.

(and they act on a small number of qubits.)

Any unitary operation can be reduced to a finite sequence of the gates.

Processing data: quantum circuits

A quantum circuit



Complexity?

How many local operations do we need to compute the problem.   i.e. number of gates.

~ how much time we need to compute it.

Quantum computers: practical perspective

What useful things can we do with a quantum computer?

Factoring: Given an integer, find its prime factors.

We can factor large numbers efficiently !

2037035976334486086268445688409378161051468393665936250636140449354381299763336706183 39

So what?

Can break cryptographic systems !!!

Can we solve every problem efficiently?

No !

Quantum computers: practical perspective

What useful things can we do with a quantum computer?

Can simulate quantum systems efficiently !

Areas where you need to understand the quantum behavior of atoms and molecules :

- nanotechnology
- microbiology
- pharmaceuticals
- superconductors.

...

Quantum computers: scientific perspective

(Physical) Church Turing Thesis

Any computational problem that can be solved by a physical device, can be solved by a Turing Machine.

Strong version

Any computational problem that can be solved *efficiently* by a physical device, can be solved *efficiently* by a Turing Machine.

Strong version doesn't seem to be true.

Quantum computers: scientific perspective

One of the great scientific advances of our time.

To know the limits of efficient computation:

Incorporate actual facts about physics.

Quantum computers: philosophical perspective

Is the universe deterministic ?

How does nature keep track of all the numbers ?

$$1000 \text{ qubits } \rightarrow 2^{1000} \text{ amplitudes}$$

Does quantum physics have anything to say about the human mind and consciousness ?

Can quantum physics say anything about free will ?

Quantum AI ?

Where are we at building quantum computers?

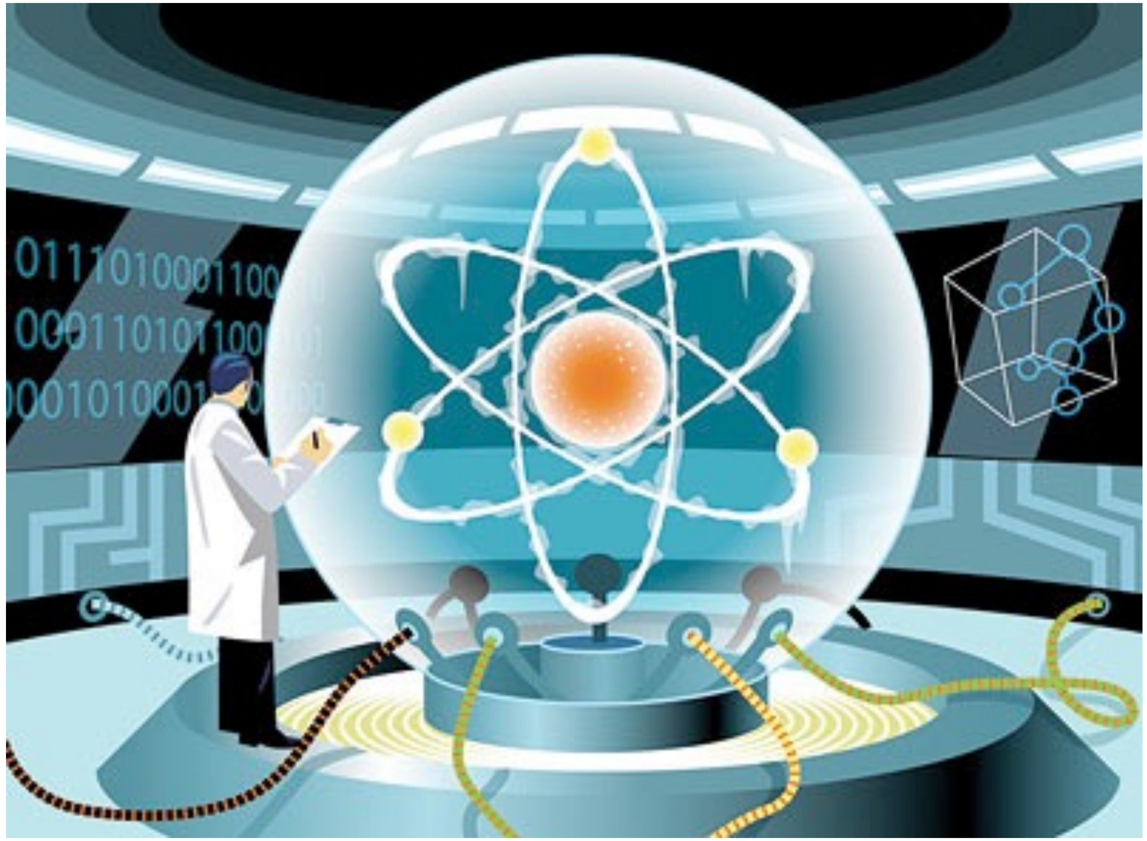
When can I expect a quantum computer on my desk ?

<u>Two points of view:</u>

- After about 20 years and 1 billion dollars of funding :
  Can factor 21 into 3 x 7. (with high probability)

- We already have a quantum computer: D-Wave.
  In the near future, we'll all have one.

Challenge: Interference with the outside world.



A whole new exciting world of computation.

Potential to fundamentally change how we view computers and computation.