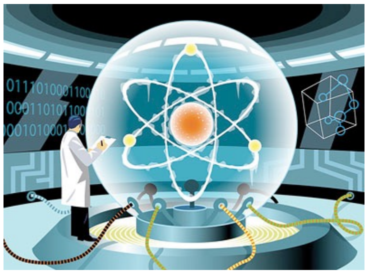
15-251: Great Ideas in Theoretical Computer Science

Lecture 24: A Gentle Intro to Quantum Computation



Nov 20th, 2018

The plan

Classical computers and classical theory of computation

Quantum physics (what the fuss is all about)

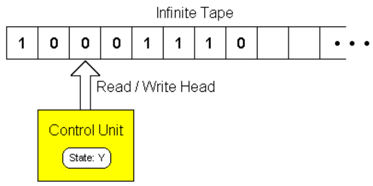
Quantum computation
(practical, scientific, and philosophical perspectives)

Theory of computation

Mathematical model of a computer:

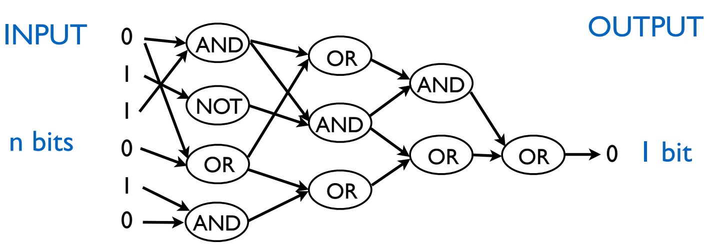
Theory of computation

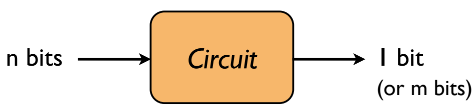
Turing Machines



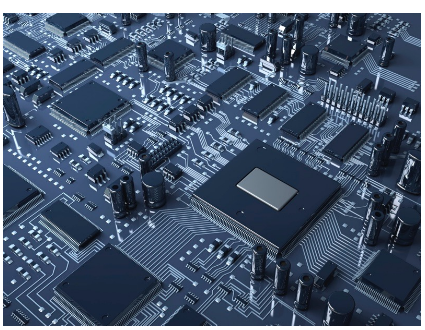
Theory of computation

Boolean Circuits





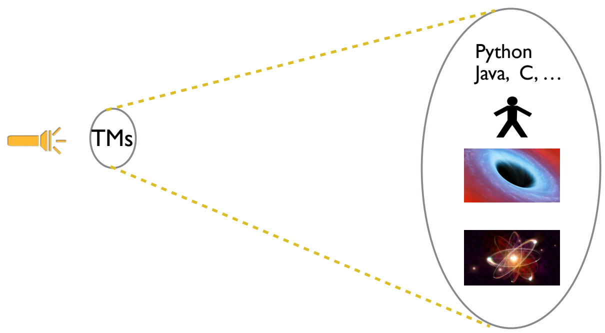
Physical Realization



Circuits implement basic operations / instructions.

(Physical) Church-Turing Thesis

Turing Machines ~ (uniform) **Boolean Circuits**
universally capture all of computation.



All types of computation

(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 ___________ by a physical device, can be solved ___________ by a TM.

The plan

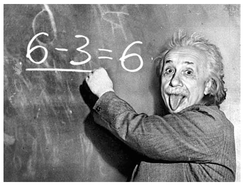
Classical computers and classical theory of computation

Quantum physics (what the fuss is all about)

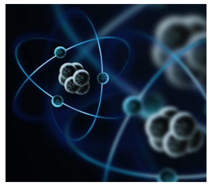
Quantum computation
(practical, scientific, and philosophical perspectives)

One slide course on physics

Classical
Physics

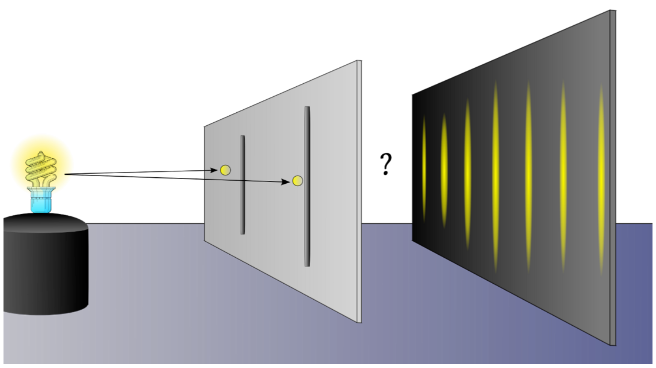


General Theory
of Relativity



Quantum
Physics

Video: Double slit experiment



2 interesting aspects of quantum physics

1. Having multiple states "simultaneously"

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

In reality, they can be in a ____________ of two states.

2. Measurement

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

If you measure it (interfere with it), it "collapses".

So you either see $|\mathrm{up}\rangle$ or $|\mathrm{down}\rangle$.

Removing physics from quantum physics

mathematics underlying quantum physics

=

Probabilistic states and evolution

vs

Quantum states and evolution

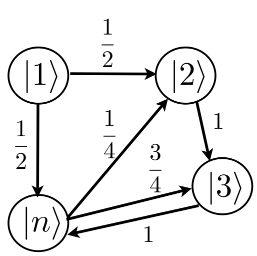
Probabilistic states

Suppose an object can have n possible states:

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

At each time step, the state can change probabilistically.

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



Initial state:

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

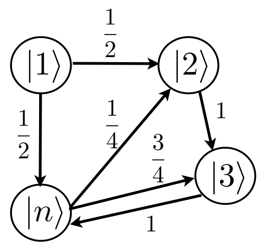
Probabilistic states

Suppose an object can have n possible states:

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

At each time step, the state can change probabilistically.

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



After one time step:

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

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:

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

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:

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

Probabilistic states

Evolution of probabilistic states

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

Any matrix that maps probabilistic states to probabilistic states.

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

α_i's can be negative. (α_i's are called __________.)

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

$$\begin{bmatrix} \text{Unitary} \\ \text{Matrix} \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix} = \begin{bmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{bmatrix}$$

any matrix that preserves "quantumness"

Quantum states

Evolution of quantum states

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

Any matrix that maps quantum states to quantum states.

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

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

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 $|1\rangle$

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

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

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

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

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

Probabilistic states vs Quantum states

Classical Probability

To find the probability of an event:

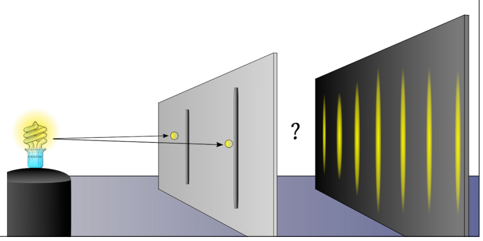
add the probabilities of every possible way it can happen

Probabilistic states vs Quantum states

Quantum

To find the probability of an event:

add the amplitudes of every possible way it can happen, then square the value to get the probability.



Probabilistic states vs Quantum states

A final remark

Quantum states are an **upgrade** to:

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

Nature seems to be choosing the mathematically more elegant option.

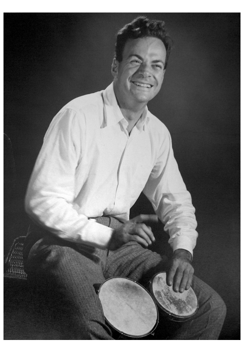
The plan

Classical computers and classical theory of computation

Quantum physics (what the fuss is all about)

Quantum computation
(practical, scientific, and philosophical perspectives)

Quantum Computation:



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 quantum system $\longrightarrow$ complexity exponential in **n**

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

Why not do computation using quantum particles/physics?

Representing data/information

An electron can be in "spin up" or "spin down" state.

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

A quantum bit:
(qubit)

When you measure:

Representing data/information

An electron can be in "spin up" or "spin down" state.

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

2 qubits:

Representing data/information

An electron can be in "spin up" or "spin down" state.

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

3 qubits:

Processing data

What will be our model?

In the classical setting, we had:

- Turing Machines
- Boolean circuits

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

Processing data: quantum gates

One non-trivial classical gate for a single classical bit:

$$0 \to \text{NOT} \to 1$$
$$1 \to \text{NOT} \to 0$$

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

One famous example: **Hadamard gate**

$$|0\rangle \to \boxed{H} \to$$
$$|1\rangle \to \boxed{H} \to$$

"transition" matrix:

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

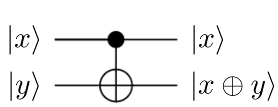
Processing data: quantum gates

Examples of classical gates on 2 classical bits:

A famous example of a quantum gate on 2 qubits:

controlled NOT

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



"transition" matrix:

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

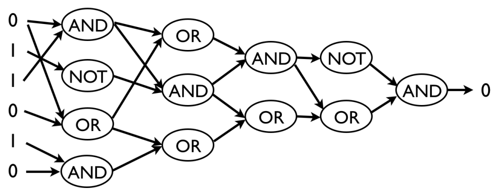
Processing data: quantum circuits

A classical circuit

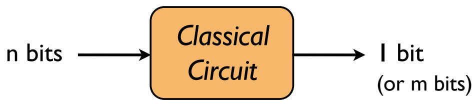
INPUT

OUTPUT

n bits



1 bit



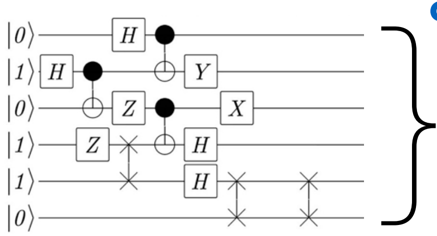
Processing data: quantum circuits

A quantum circuit

INPUT

OUTPUT

n qubits



n qubits

quantum gates

(acts on 1 qubit) (acts on 2 qubits)

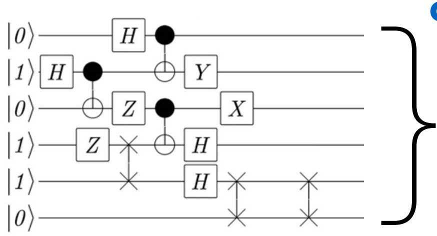
Processing data: quantum circuits

A quantum circuit

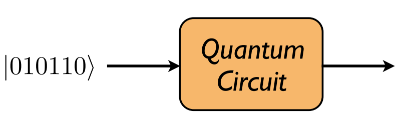
INPUT

OUTPUT

n qubits



n qubits

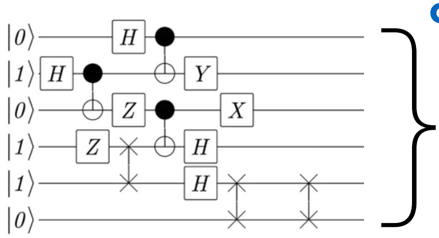


Processing data: quantum circuits

A quantum circuit

INPUT

n qubits



OUTPUT

n qubits

How do we get "classical information" from the circuit?

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

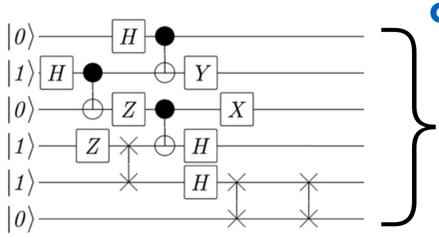
$$\alpha_{000000}|000000\rangle + \alpha_{000001}|000001\rangle + \cdots + \alpha_{111111}|111111\rangle$$

Processing data: quantum circuits

A quantum circuit

INPUT

n qubits



OUTPUT

n qubits

Complexity?

Practical, Scientific and Philosophical Perspectives

Practical perspective

What useful things can we do with a quantum computer?

We can factor large numbers efficiently!

203703597633448608626844568840937816105146839366593625063614044935438129976333670618339
844568840937816105146839366593625063614044935438129976333670618339928374928729109198341
992834719747982982750348795478978952789024138794327890432736783553789507821378582549871

So what?

Can we solve every problem efficiently?

Practical perspective

What useful things can we do with a quantum computer?

Can simulate quantum systems efficiently!

Better understand behavior of atoms and moleculues.

Applications:
- nanotechnology
- microbiology
- pharmaceuticals
- superconductors.

...

Scientific perspective

To know the limits of efficient computation:

Incorporate actual facts about physics.

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 TM.

Strong version doesn't seem to be true!

Philosophical perspective

Is the universe deterministic ?

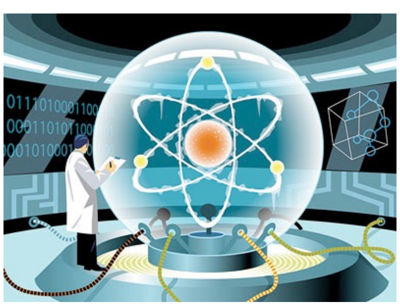
How does nature keep track of all the numbers ?

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

How should we interpret quantum measurement?
(the measurement problem)

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

Quantum AI?



A whole new exciting world of computation.

Potential to fundamentally change how we view computation.