Lecture 28:
Quantum Computation: A gentle introduction
Announcements

Please fill out the Faculty Course Evaluations (FCEs).

https://cmu.smartevals.com
Announcements

As a “thank you” for filling it out:

You can vote to eliminte 2 topics from the final exam:

- Cake Cutting
- Stable Matchings
- Boolean Circuits
- Social Choice
- Approximation Algorithms
Announcements

The Last Lecture on Thursday

Daniel Sleator
Mor Harchol-Balter
Nihar Shah

Rashmi Vinayak
Anupam Gupta
Ryan O’Donnell
Announcements

The Last Lecture on Thursday
Quantum Computation
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 computer/computation?

A device that **manipulates** data (information)
Mathematical model of a computer:

Turing Machines ~ Boolean Circuits
Theory of computation

Turing Machines

Infinite Tape

1 0 0 0 1 1 1 0

Read / Write Head

Control Unit

State: Y
Theory of computation

Boolean Circuits

AND
OR
NOT

gates

AND
OR
NOT
Physical Realization

Circuits implement basic operations / instructions.

Everything follows classical laws of physics!
(Physical) Church-Turing Thesis

Turing Machines $\sim$ (uniform) Boolean Circuits

universally capture all of computation.
(Physical) Church-Turing Thesis

Turing Machines \sim (\text{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 \textit{efficiently} by a physical device, can be solved \textit{efficiently} by a TM.
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

Classical Physics

General Theory of Relativity

Quantum Physics

String Theory (?)
Video: Double slit experiment

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

Nature has no obligation to conform to your intuitions.
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”: $|\text{up}\rangle$ or $|\text{down}\rangle$

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

2. Measurement

   Quantum property is very sensitive/fragile!

   If you measure it (interfere with it), it “collapses”.

   So you either see $|\text{up}\rangle$ or $|\text{down}\rangle$. 
It must be just our ignorance

- There is no such thing as superposition.
- We don’t know the state, so we say it is in a 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 and evolution

vs

Quantum states and evolution
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:

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

Diagram:

- $|1\rangle$ to $|2\rangle$: $\frac{1}{2}$
- $|1\rangle$ to $|n\rangle$: $\frac{1}{2}$
- $|2\rangle$ to $|3\rangle$: $\frac{3}{4}$
- $|2\rangle$ to $|n\rangle$: $\frac{1}{4}$
- $|3\rangle$ to $|2\rangle$: $1$
- $|3\rangle$ to $|n\rangle$: $1$
- $|n\rangle$ to $|1\rangle$: $1$
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:

\[
\begin{bmatrix}
|1\rangle & 1 \\
|2\rangle & 0 \\
|3\rangle & 0 \\
\vdots & \vdots \\
|n\rangle & 0
\end{bmatrix}
\begin{bmatrix}
0 \\
1/2 \\
0 \\
\vdots \\
1/2
\end{bmatrix}
= 
\begin{bmatrix}
1/2 \\
1/4 \\
3/4 \\
\vdots \\
1
\end{bmatrix}
\]
**Probabilistic states**

Transition Matrix

\[
\begin{bmatrix}
|1\rangle & |2\rangle & |3\rangle & \cdots & |n\rangle \\
1 & 0 & 0 & \cdots & 0 \\
0 & 1/2 & 0 & \cdots & 0 \\
0 & 0 & \ddots & \ddots & 0 \\
0 & 0 & \cdots & 0 & 1/2
\end{bmatrix}
\]

the new state (probabilistic)

A general probabilistic state:

\[
\begin{bmatrix}
p_1 \\
p_2 \\
\vdots \\
p_n
\end{bmatrix}
\]

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

\[p_1 + p_2 + \cdots + p_n = 1\]

(\(\ell_1\) norm is 1)
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

Any matrix that maps probabilistic states to probabilistic states.

We won’t restrict ourselves to just one transition matrix.

\[
\begin{bmatrix}
\text{Transition Matrix}
\end{bmatrix}
\]

\[
\pi_0 \xrightarrow{K_1} \pi_1 \xrightarrow{K_2} \pi_2 \xrightarrow{K_3} \cdots
\]
Quantum states

$p_i$’s can be negative.
Quantum states

\[ \begin{bmatrix}
\alpha_1 \\
\alpha_2 \\
\vdots \\
\alpha_n
\end{bmatrix} \]

\( \alpha_i \)’s can be negative. \((\alpha_i \)’s are called amplitudes.\)

\[ \alpha_1 |1\rangle + \alpha_2 |2\rangle + \cdots + \alpha_n |n\rangle \]

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

\((\alpha_i \) can be a complex number)
Quantum states

Evolution of quantum states

Any matrix that maps quantum states to quantum states.

We won’t restrict ourselves to just one unitary matrix.

\[
\begin{bmatrix}
\text{Unitary Matrix}
\end{bmatrix}
\]

\[\Psi_0 \xrightarrow{U_1} \Psi_1 \xrightarrow{U_2} \Psi_2 \xrightarrow{U_3} \ldots\]
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 see state \( i \) with probability \( \alpha_i^2 \).
Suppose we have just 2 possible states:  \( |0\rangle \) and  \( |1\rangle \)

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

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

\[
|0\rangle \rightarrow \frac{1}{2} |0\rangle + \frac{1}{2} |1\rangle
\]

\[
\frac{1}{2} \left( \frac{1}{2} |0\rangle + \frac{1}{2} |1\rangle \right)
\]

\[
\frac{1}{4} |0\rangle + \frac{1}{4} |1\rangle + \frac{1}{4} |0\rangle + \frac{1}{4} |1\rangle
\]
Probabilistic states vs Quantum states

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

\[
\begin{bmatrix}
\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\
\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}
\end{bmatrix}
\begin{bmatrix}
1 \\
0
\end{bmatrix}
= \begin{bmatrix}
\frac{1}{\sqrt{2}} \\
\frac{1}{\sqrt{2}}
\end{bmatrix}
\]

\[
\begin{bmatrix}
\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\
\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}
\end{bmatrix}
\begin{bmatrix}
0 \\
1
\end{bmatrix}
= \begin{bmatrix}
-\frac{1}{\sqrt{2}} \\
\frac{1}{\sqrt{2}}
\end{bmatrix}
\]

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

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

\[
\frac{1}{2} |0\rangle + \frac{1}{2} |1\rangle + -\frac{1}{2} |0\rangle + \frac{1}{2} |1\rangle = |1\rangle
\]
Classical Probability

To find the probability of an event:

- add the probabilities of every possible way it can happen
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.

one way has positive amplitude
the other way has equal negative amplitude

event never happens!
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 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.
It would be super nice to be able to simulate quantum systems. With a classical computer this is extremely inefficient.\[ \text{n state system} \quad \xrightarrow{\text{complexity exponential in n}} \]

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.

\[ |\text{up}\rangle \quad \text{or} \quad |\text{down}\rangle \quad \sim \quad |0\rangle \quad \text{or} \quad |1\rangle \]

A quantum bit: (qubit) \[ \alpha_0 |0\rangle + \alpha_1 |1\rangle, \quad \alpha_0^2 + \alpha_1^2 = 1 \]

A superposition of \[ |0\rangle \] and \[ |1\rangle \].

When you measure: With probability \[ \alpha_0^2 \] it is \[ |0\rangle \].
With probability \[ \alpha_1^2 \] it is \[ |1\rangle \].
Representing data/information

An electron can be in “spin up” or “spin down” state.

\[ |\text{up}\rangle \quad \text{or} \quad |\text{down}\rangle \quad \sim \quad |0\rangle \quad \text{or} \quad |1\rangle \]

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

2 qubits:

\[ \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{10} |10\rangle + \alpha_{11} |11\rangle \]

\[ \alpha_{00}^2 + \alpha_{01}^2 + \alpha_{10}^2 + \alpha_{11}^2 = 1 \]
Representing data/information

An electron can be in “spin up” or “spin down” state.

\[ |\text{up}\rangle \quad \text{or} \quad |\text{down}\rangle \quad \sim \quad |0\rangle \quad \text{or} \quad |1\rangle \]

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

(qubit)

3 qubits:

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

\[ \alpha_{000}^2 + \alpha_{001}^2 + \alpha_{010}^2 + \alpha_{011}^2 + \alpha_{100}^2 + \alpha_{101}^2 + \alpha_{110}^2 + \alpha_{111}^2 = 1 \]
An electron can be in “spin up” or “spin down” state.

\[ |\text{up}\rangle \quad \text{or} \quad |\text{down}\rangle \sim |0\rangle \quad \text{or} \quad |1\rangle \]

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

For \( n \) qubits, how many amplitudes are there?
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.
One non-trivial classical gate for a single classical bit:

\[
\begin{align*}
0 & \rightarrow \text{NOT} \rightarrow 1 \\
1 & \rightarrow \text{NOT} \rightarrow 0
\end{align*}
\]

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

One famous example: **Hadamard gate**

\[
\begin{align*}
|0\rangle & \rightarrow H \rightarrow \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle \\
|1\rangle & \rightarrow H \rightarrow \frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle
\end{align*}
\]

“transition” matrix:

\[
\begin{bmatrix}
\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\
\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}
\end{bmatrix}
\]
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 \( x, y \in \{0, 1\} \)

\[
\begin{align*}
|x\rangle &\quad \text{controlled NOT} \quad |x\rangle \\
|y\rangle &\quad |x \oplus y\rangle
\end{align*}
\]

“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

n bits

0
1
1
1
1
0
0
1
1
0

AND

OR

AND

OR

AND

NOT

AND

OR

OR

AND

0

1 bit

OUTPUT

1 bit

n bits

Classical Circuit

n bits

1 bit
(or m bits)
Processing data: quantum circuits

A quantum circuit

INPUT

\[ |0\rangle \quad H \quad |0\rangle \quad Z \quad |1\rangle \quad Z \quad |1\rangle \quad H \quad |0\rangle \]

quantum gates

\[ |1\rangle \quad Z \] (acts on 1 qubit)

\[ |0\rangle \quad H \quad |1\rangle \] (acts on 2 qubits)

OUTPUT

\[ |0\rangle \quad Y \quad |1\rangle \quad H \quad |1\rangle \]

n qubits

n qubits
Processing data: quantum circuits

A quantum circuit

INPUT

$|0\rangle$

$|1\rangle$

$|0\rangle$

$|1\rangle$

$|1\rangle$

$|0\rangle$

OUTPUT

Quantum Circuit

$n$ qubits

$n$ qubits

$n$ qubits

$n$ qubits
A quantum circuit

INPUT

|0⟩, |1⟩

|0⟩, |1⟩

|0⟩, |1⟩

|0⟩, |1⟩

|0⟩

OUTPUT

Quantum Circuit

|010110⟩
Processing data: quantum circuits

A quantum circuit

\[\begin{array}{c}
|0\rangle \\
|1\rangle \\
|0\rangle \\
|1\rangle \\
|0\rangle \\
|1\rangle \\
\end{array}\]

Quantum Circuit

\[\begin{array}{c}
\alpha_{000000}|000000\rangle + \\
\alpha_{000001}|000001\rangle + \\
\alpha_{000010}|000010\rangle + \\
\ldots \\
\alpha_{111111}|111111\rangle
\end{array}\]
Processing data: quantum circuits

A quantum circuit

INPUT

$|0\rangle$ $H$ $|H\rangle$
$|1\rangle$ $Z$ $|Y\rangle$
$|0\rangle$ $X$
$|1\rangle$ $H$

OUTPUT

$n$ qubits

Quantum Circuit

superposition of $2^n$ possible states.
$(2^n$ amplitudes)
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

\[ |0\rangle \]
\[ |1\rangle \]
\[ |0\rangle \]
\[ |1\rangle \]
\[ |0\rangle \]

OUTPUT

\[ |0\rangle \]
\[ |1\rangle \]
\[ |1\rangle \]
\[ |1\rangle \]

Complexity?

number of gates \( \sim \) computation time
Physical Realization

?
Practical, Scientific and Philosophical Perspectives
What useful things can we do with a quantum computer?

We can factor large numbers efficiently!

2037035976334486086268445688409378161051468393665936250636140449354381299763336706183398445688409378161051468393665936250636140449354381299763336706183392834719747982982750348795478978952789024138794327890432736783553789507821378582549871

So what?

Can break RSA!

Can we solve every problem efficiently?

No!
Practical perspective

What useful things can we do with a quantum computer?

Can simulate quantum systems efficiently!

Better understand behavior of atoms and molecules.

Applications:
- nanotechnology
- microbiology
- pharmaceuticals
- superconductors.
...
To know the limits of efficient computation:

Incorporate actual facts about physics.
Any computational problem that can be solved by a physical device, can be solved by a Turing Machine.

(Physical) Church Turing Thesis

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 qubits $\rightarrow 2^{1000}$ amplitudes

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

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

Quantum AI?
Where are we at building quantum computers?

When can I expect a quantum computer on my desk?

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

**Challenge:** Interference with the outside world.

“quantum decoherence”
A whole new exciting world of computation.

Potential to fundamentally change how we view computers and computation.