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

<table>
<thead>
<tr>
<th>Infinite Tape</th>
<th>1</th>
<th>0</th>
<th>1</th>
<th>0</th>
<th>1</th>
<th>0</th>
</tr>
</thead>
</table>

Control Unit
State: Y

Physical Realization

Boolean Circuits

Circuits implement basic operations / instructions.
(Physical) Church-Turing Thesis

Turing Machines \sim (uniform) Boolean Circuits

universally capture all of computation.

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

Strong version

The plan

Classical computers and classical theory of computation

Quantum physics (what the fuss is all about)

Quantum computation

(practical, scientific, and philosophical perspectives)
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 ______ 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 \( |\text{down}\rangle \).
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:

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

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**

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

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**

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

\[
\begin{bmatrix}
\alpha_1 \\
\alpha_2 \\
\vdots \\
\alpha_n
\end{bmatrix}
= \begin{bmatrix}
\beta_1 \\
\beta_2 \\
\vdots \\
\beta_n
\end{bmatrix}
\]

Any matrix that preserves “quantumness”

---

**Quantum states**

**Evolution of quantum states**

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

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 \( |1\rangle \)

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

randomize a random state

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

\[
\frac{1}{4} |0\rangle + \frac{1}{4} |1\rangle + \frac{1}{4} |0\rangle + \frac{1}{4} |1\rangle
\]

Probabilistic states vs Quantum states

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

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

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

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

\[
\frac{1}{2} |0\rangle + \frac{1}{2} |1\rangle + \frac{1}{2} |0\rangle + \frac{1}{2} |1\rangle = |1\rangle
\]
Probabilistic states vs Quantum states

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.

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:

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

With a classical computer this is extremely inefficient.

$n$-state quantum system complexity exponential in $n$

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

Why not do computation using quantum particles/physics?
<table>
<thead>
<tr>
<th>Representing data/information</th>
</tr>
</thead>
<tbody>
<tr>
<td>An electron can be in “spin up” or “spin down” state.</td>
</tr>
<tr>
<td>$</td>
</tr>
</tbody>
</table>

**A quantum bit:**

(qubit)

**When you measure:**

<table>
<thead>
<tr>
<th>Representing data/information</th>
</tr>
</thead>
<tbody>
<tr>
<td>An electron can be in “spin up” or “spin down” state.</td>
</tr>
<tr>
<td>$</td>
</tr>
</tbody>
</table>

2 qubits:

<table>
<thead>
<tr>
<th>Representing data/information</th>
</tr>
</thead>
<tbody>
<tr>
<td>An electron can be in “spin up” or “spin down” state.</td>
</tr>
<tr>
<td>$</td>
</tr>
</tbody>
</table>

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:

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

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

One famous example: **Hadamard gate**

\[
\begin{align*}
|0\rangle & \rightarrow H |0\rangle \\
|1\rangle & \rightarrow H |1\rangle
\end{align*}
\]

“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:

- **AND**
- **OR**

A famous example of a quantum gate on 2 qubits:

**controlled NOT**

For \(x, y \in \{0, 1\}\)

\[
\begin{align*}
|x\rangle & \rightarrow (|x\rangle \\
|y\rangle & \rightarrow |x \oplus y\rangle
\end{align*}
\]

“transition” matrix:

\[
\begin{bmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0
\end{bmatrix}
\]
A classical circuit

INPUT

\[ \begin{array}{cccc}
0 & 1 & 0 & 1 \\
\text{AND} & \text{OR} & \text{AND} & \text{NOT} \\
0 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 \\
\end{array} \]

OUTPUT

\[ \begin{array}{cccc}
1 \\
\end{array} \]

Classical Circuit

\[ \begin{array}{c}
n \text{ bits} \quad \rightarrow \quad 1 \text{ bit} \\
\text{(or m bits)}
\end{array} \]

A quantum circuit

INPUT

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

\[ \begin{array}{c}
H \\
Y \\
Z \\
X \\
H \\
\end{array} \]

Quantum gates

INPUT

Quantum Circuit

\[ \begin{array}{c}
|010110\rangle \\
\end{array} \]

OUTPUT

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

(n acts on 1 qubit) (acts on 2 qubits)
How do we get “classical information” from the circuit? We measure the output qubit(s). e.g. we measure:
\[ \alpha_{000000}|000000\rangle + \alpha_{000001}|000001\rangle + \cdots + \alpha_{111111}|111111\rangle \]
Practical perspective

What useful things can we do with a quantum computer?

We can factor large numbers efficiently!

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 molecules.

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 qubits → $2^{1000}$ amplitudes

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

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

Quantum AI!

A whole new exciting world of computation.

Potential to fundamentally change how we view computation.