Quantum Information Processing

Lecture 1

Dr. Ahmad Khonsari

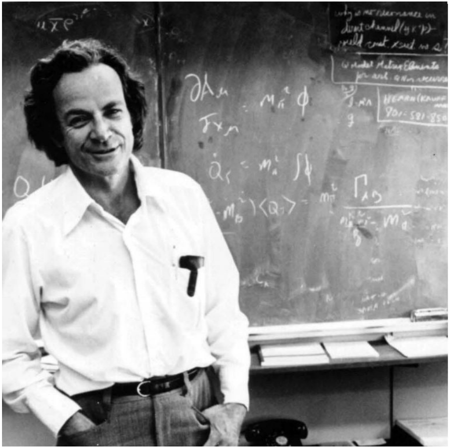
Uiversity of Tehran

Fall 2022

December 16, 2022

Slides Prepared by Mahdi Dolati

What is quantum computing? (1)



Source: Wikipedia

... trying to find a computer simulation of physics seems to me to be an excellent program to follow out. ... the real use of it would be with quantum mechanics.
... Nature isnt classical ... and if you want to make a simulation of Nature, youd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesnt look so easy.
Richard Feynman

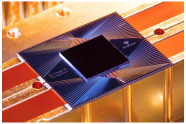
What is quantum computing? (2)

Source: www.globalinfluence.world

The theory of computation has traditionally been studied almost entirely in the abstract, as a topic in pure mathematics. This is to miss the point of it. Computers are physical objects, and computations are physical processes. What computers can or cannot compute is determined by the laws of physics alone, and not by pure mathematics.
David Deutsch

Why study quantum computing?

Quantum Supremacy Using a Programmable Superconducting Processor
(Wednesday, October 23, 2019)
Posted by John Martinis, Chief Scientist Quantum Hardware and Sergio Boixo, Chief Scientist Quantum Computing Theory, Google AI Quantum
Today we published the results of this quantum supremacy experiment in the Nature article,"Quantum Supremacy Using a Programmable Superconducting Processor". We developed a new 54-qubit processor, named "Sycamore", that is comprised of fast, high-fidelity quantum logic gates, in order to perform the benchmark testing. Our machine performed the target computation in 200 seconds, and from measurements in our experiment we determined that it would take the worlds fastest supercomputer $10,000$ years to produce a similar output.



Photograph of the Sycamore processor.

Why study quantum computing in computer science?

- Quantum software development
- Quantum algorithm design
- Quantum machine learning
- Quantum computer architecture and compiler design
- Quantum information theory research
- Quantum communication system development
- Quantum security system development

Scope of the course

- Theoretical basis for quantum computing.
- Practical basis for quantum computing.
- Near-term potential of quantum computing.
- Other applications of quantum information.

What the course isn't:

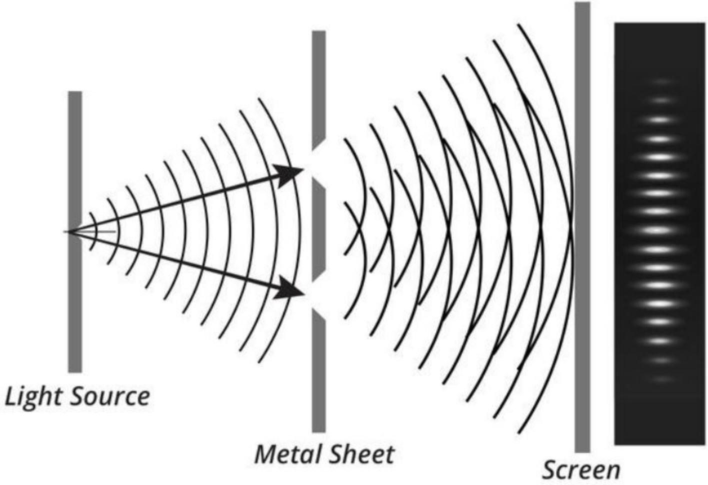
- Philosophy
- .. and physics is quite minimal.

Course outline

1	Bits and qubits	Introduction
2	Linear algebra	Fundamentals
3	Postulates of quantum mechanics	
4	Concepts in quantum mechanics	
5	The quantum circuit model	
6	Applications of quantum information	Quantum information
7	Deutsch-Jozsa algorithm	Theoretical QC
8	Quantum search	
9	QFT & QPE	
10	QFT & QPE: Factoring	
11	QFT & QPE: Quantum Chemistry	
12	Quantum complexity	
13	Quantum error correction	Practical QC
14	Fault tolerant quantum computing	
15	Adiabatic quantum computing	Near-term QC
16	Case studies in quantum computation	

A little bit of physics

The double-slit experiment



Source: www.curiosity.com

The qubit

An information theoretic way to represent superposition

A classical bit is an intuitive concept, it is either equal to:

$$0 = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle \qquad 1 = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle$$

Even if we are uncertain about whether a classical bit, B, is in state 0 or 1, we can characterise it by a probability mass function, or a mixture

$$p(B = 0) = p_0 \ ; \ p(B = 1) = p_1$$

where $p_0 + p_1 = 1$. A qubit, $|\psi\rangle$, is quite different, it can be in a superposition of the 0 and 1 states:

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

where α and β are complex numbers such that $|\alpha|^2 + |\beta|^2 = 1$.

Measuring a qubit

Any attempt to measure the state

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

results in $|0\rangle$ with probability $|\alpha|^2$, and $|1\rangle$ with probability $|\beta|^2$.
After the measurement, the system is in the measured state! That is, the post-measurement state, $|\psi^{'}\rangle$, will be:

$$|\psi^{'}\rangle = |0\rangle \text{ or } |\psi^{'}\rangle = |1\rangle$$

Further measurements will always yield the same value. We can only extract one bit of information from the state of a qubit.

The state of a qubit describes more than just its measurement probabilities

The superposition of $|0\rangle$ and $|1\rangle$ states describes a physical structure, and not merely a probability mass function over possible measurement outcomes. For example:

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

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

all have a 50% chance of being in either in the $|0\rangle$ or $|1\rangle$ state if measured, but all correspond to different superpositions, which will evolve differently. **It is crucial to appreciate this point to grasp the essence of quantum computing.**

The Hadamard gate, H, has the following function on the state $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$:

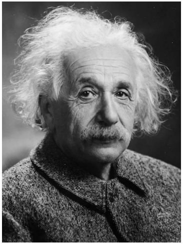
$$H|+\rangle \rightarrow |0\rangle$$

and also the function on the state $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$:

$$H|-\rangle \rightarrow |1\rangle$$

- This is an example of 'interfering' two states in superposition, to yield a deterministic outcome.
- It is also an example of a fundamental difference between two states with the same measurement outcome probabilities ($|+\rangle$ and $|-\rangle$).

Spooky action at a distance.
Albert Einstein



Source: www.space.com

No theory of reality compatible with quantum theory can require spatially separate events to be independent.
John Stewart Bell

Source: Wikipedia

The Bell state

An information theoretic way to represent entanglement

The (two-qubit) Bell state $|\Phi^+\rangle$ is defined:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

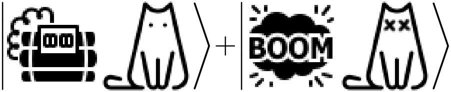
What this says is:

- Each of the two qubits are in an equal superposition of the $|0\rangle$ and $|1\rangle$ states.
- However, they are entangled, as soon as one qubit is measured (say the outcome is 1) then the second qubit collapses into the state $|1\rangle$.
- There is no requirement that the two qubits are local, in the spatial sense, in order for this to occur.

Schrödinger's cat

Source: www.researchgate.net

Erwin Schrödinger's famous thought experiment tells of a cat whose life has been entangled with a vial of deadly poison.



Source: www.icons8.com

Three things to remember

Quantum systems are distinguished from their classical counterparts by three phenomena:

- Superposition
- Interference
- Entanglement

These can be represented in information theoretical terms by a qubit, and the operations thereon, and throughout this course we will see how these three phenomena give rise to powerful quantum communication, security and computing systems.