Quantum Computing

Lecture $|0\rangle$

PROF. PAOLO ZULIANI

DIPARTIMENTO DI INFORMATICA

UNIVERSITÀ DI ROMA “LA SAPIENZA”

SAPIENZA
UNIVERSITÀ DI ROMA

Outline

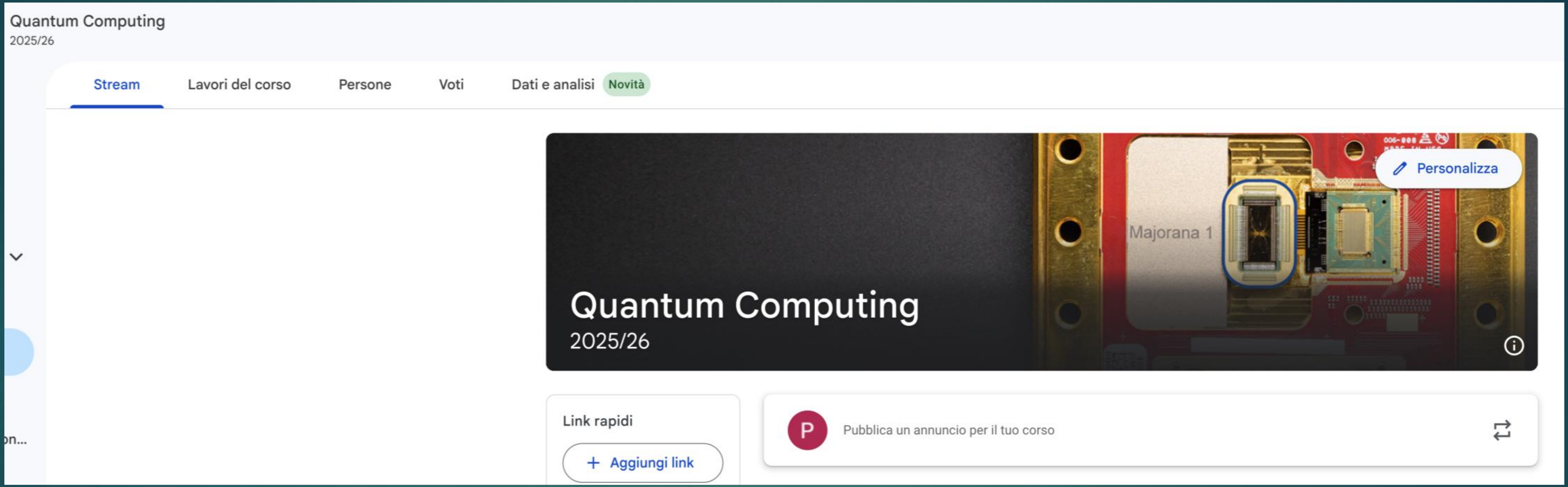
- Course info
- Debunking myths about quantum computing
- A brief history of quantum mechanics and quantum computing

Disclaimer

- This is a **BASIC** course
  - You might find it boring if you already have some quantum knowledge
- We will go slowly, and try to be as precise as possible
- Time permitting, we will try to cover some practical use of quantum computers

Course Info

- Google Classroom code: **2slubu2q**

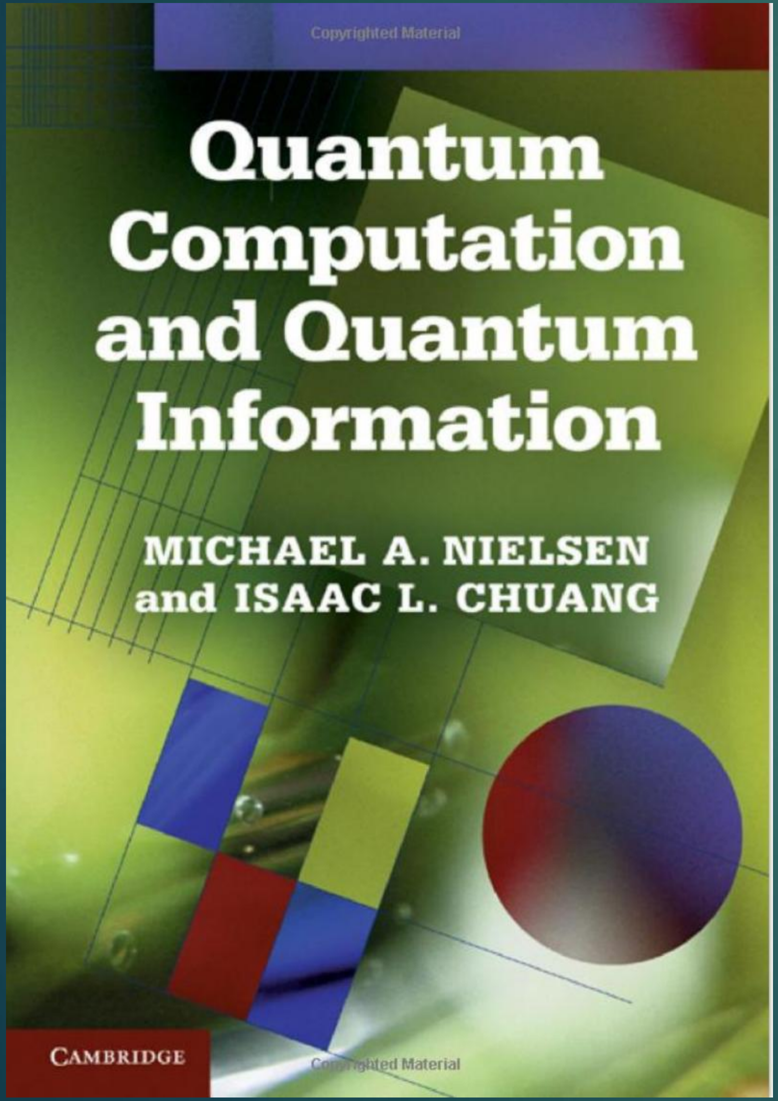


- Lectures in room T1, building E, viale Regina Elena 295:
  - **Tuesdays 14:00-16:00**
  - **Wednesdays 14:00-17:00**

Course Topics

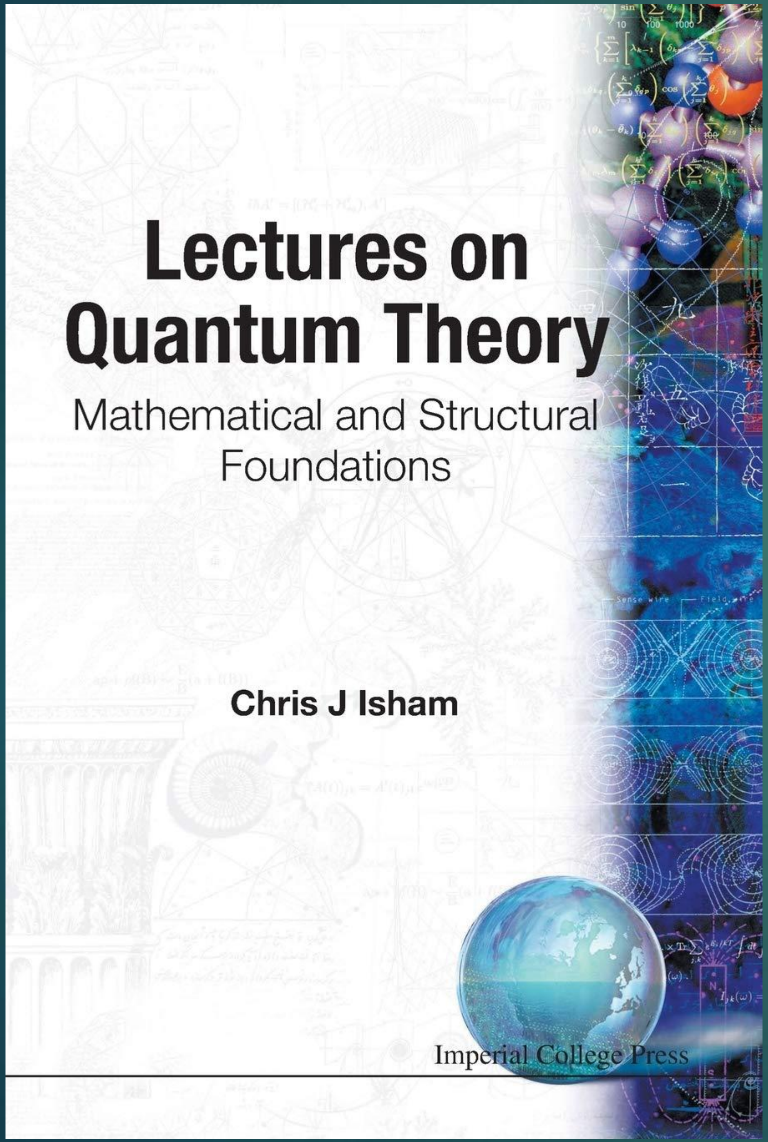
- Status of the quantum computing field
- Review of complex linear algebra
- Qubits and measurements
- Single-qubit unitary operations (NOT, Hadamard, Pauli matrices)
- Approximation of single-qubit unitaries
- Quantum registers (tensor products)
- Entangled states and EPR paradox
- Two-qubit operations (CNOT)
- Tensor product of unitary operations
- No cloning theorem and teleportation protocol
- Deutsch-Jozsa’s, Grover’s, and Shor’s algorithms
- Approximation of general unitaries (Solovay-Kitaev theorem)
- The BB84 and E91 quantum key-exchange protocols
- Basics of quantum information theory (density matrices, superoperators)
- Holevo's bound
- Post-quantum cryptography

Reading List



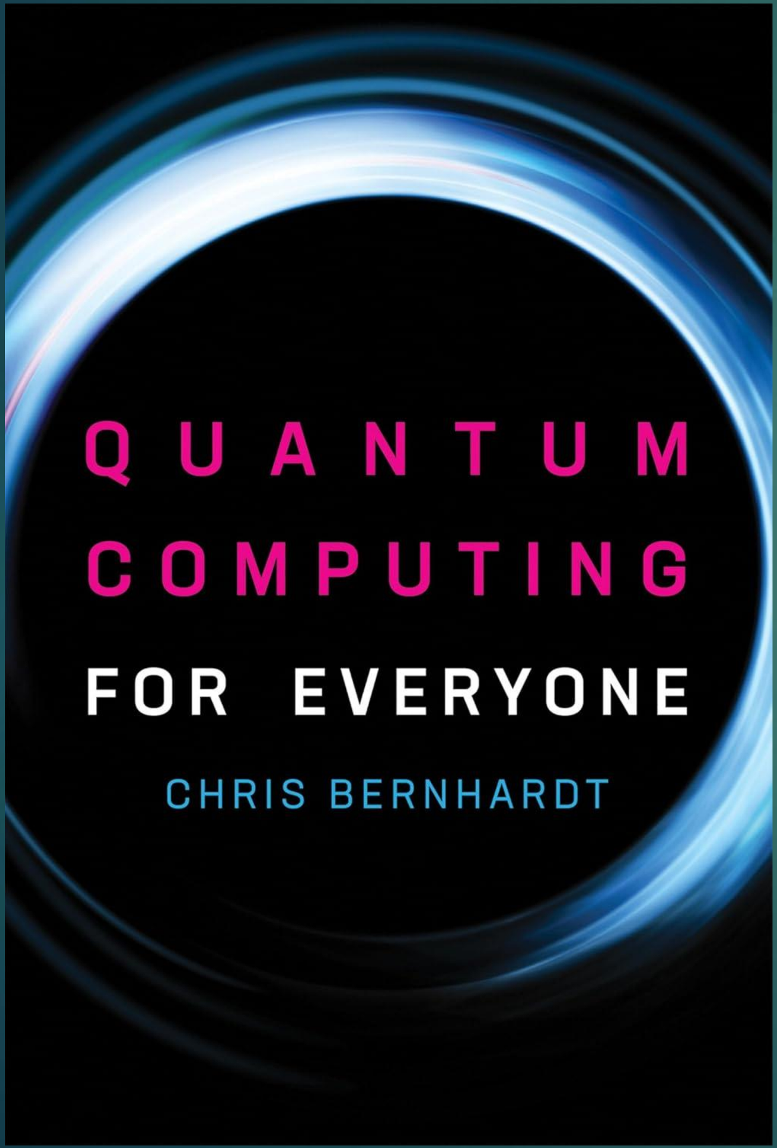
- *Quantum Computation and Quantum Information* M. Nielsen & I. L. Chuang, 10th ann. ed., 2010
  - We will cover material from chapters 1-6.
  - Still the most comprehensive book on quantum computing and information.

Reading List



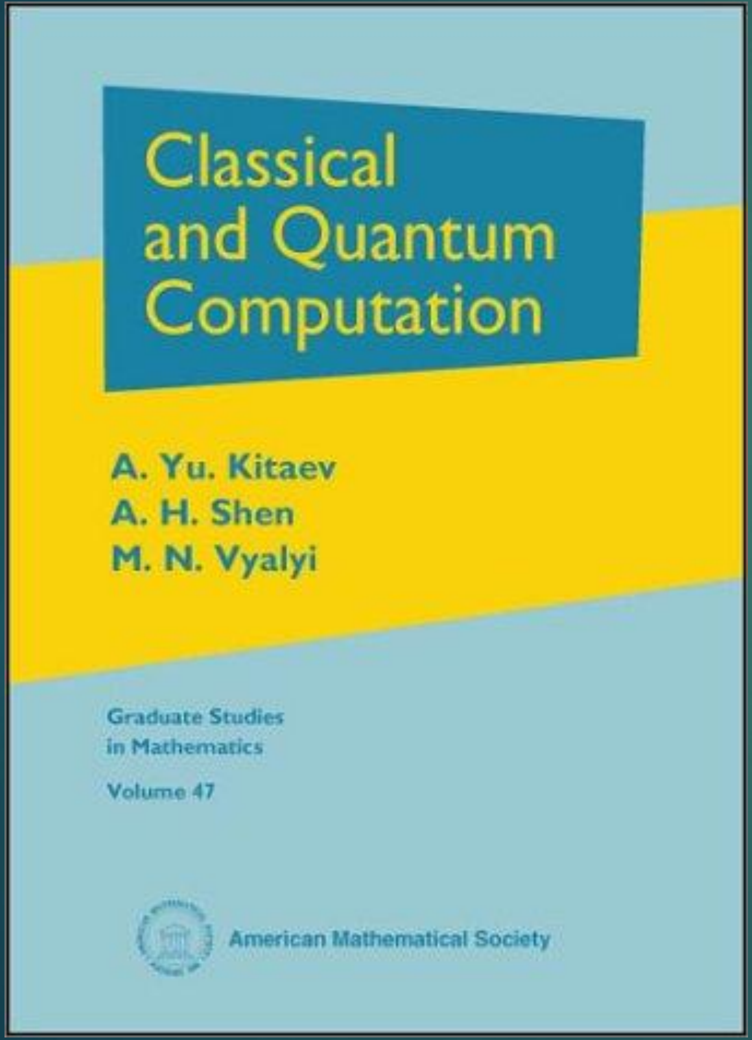
- *Lectures On Quantum Theory: Mathematical And Structural Foundations.*
  C. J. Hisham, 1995.
  - Hilbert spaces (finite-dimensional), unitary and self-adjoint operators, *etc*.
  - Excellent book for the mathematical details of quantum physics.

Reading List



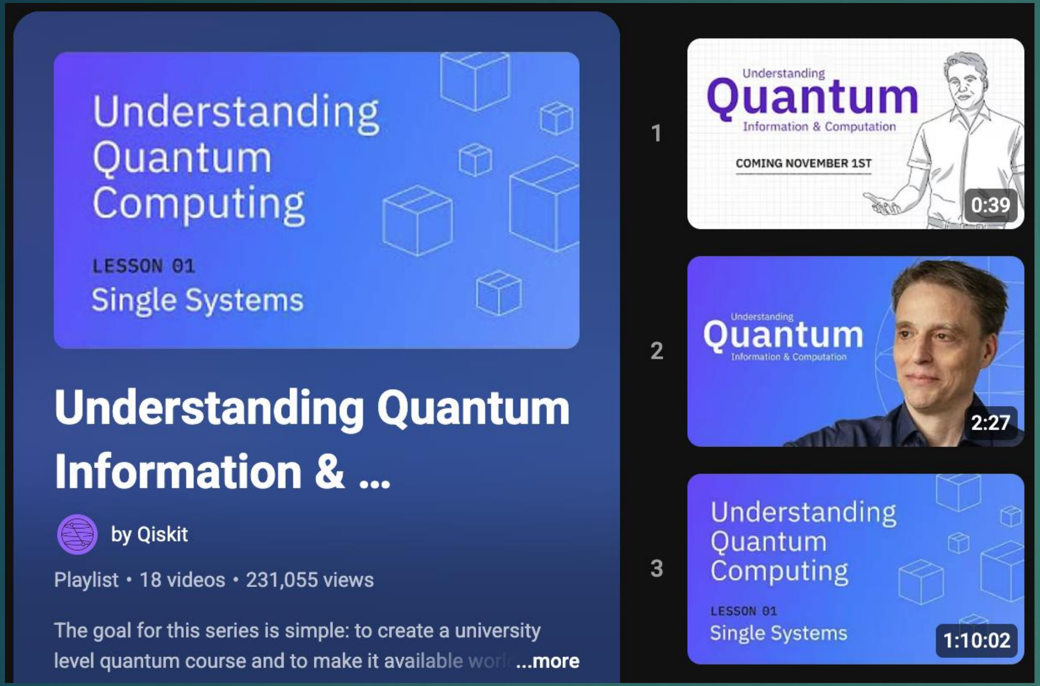
- *Quantum Computing for Everyone*
  C. Bernhardt, 2020.
  - Excellent book with <u>as little maths</u> as possible.
  - Super-clear, but skips many topics.

Reading List



- *Classical and Quantum Computation*
  A. Yu. Kitaev, A. H. Shen, M. N. Vyalyi, 2002.
  - Excellent coverage of the fundamentals without sparing the maths.
  - Covers some more advanced topics, *e.g.*, quantum error correction.

Reading/Viewing List



- *Understanding Quantum Information & Computation*
  - Excellent video lectures by John Watrous (IBM).
  - Lectures notes are available, too: https://arxiv.org/abs/2507.11536
- IBM's Qiskit textbook
  - Available at https://qiskit.org/learn/
  - Hands-on examples with IBM's quantum computers
- More pointers as needed, throughout the course

Exam

- Written: exercises and questions
- I will distribute exam examples later in the course

(A selection of)
Myths about quantum computing

Myth #1

- Quantum computers will solve NP-complete problems efficiently
- **WRONG!**
- As of today, there is no efficient classical or quantum algorithm for NP-complete problems
- Future: again no, unless *major* (and unlikely) advances in theory

Myth #2

- Quantum computers are so complicate that they will never be built

- **WRONG!**

- There are fully working (with some caveats) quantum computers (IBM, Quantinuum, QuEra, *etc.*)
  - Noisy Intermediate-Scale Quantum (NISQ) computers: small, noisy

- IBM has recently presented a 1,121-qubit system

Myth #3

- Quantum computing is just another fast hardware architecture such as GPUs, multi-core, *etc*.
- **NO!**
- Quantum computing exploits (quantum) phenomena that have no classical counterpart:
  - No one knows how to simulate *efficiently* such phenomena on a classical computer
- The theory of quantum computation is quite different from that of standard computation

Myth #4

- Quantum computing is hard (and one needs to know quantum physics)
- **Kind of true!**
- Fortunately, the mathematical theory of quantum physics is well developed (John von Neumann)
  - Based on complex linear algebra
- But today's “quantum programming languages” are merely circuit description notations:
  - We need ‘proper’ quantum programming abstractions

Myth #5

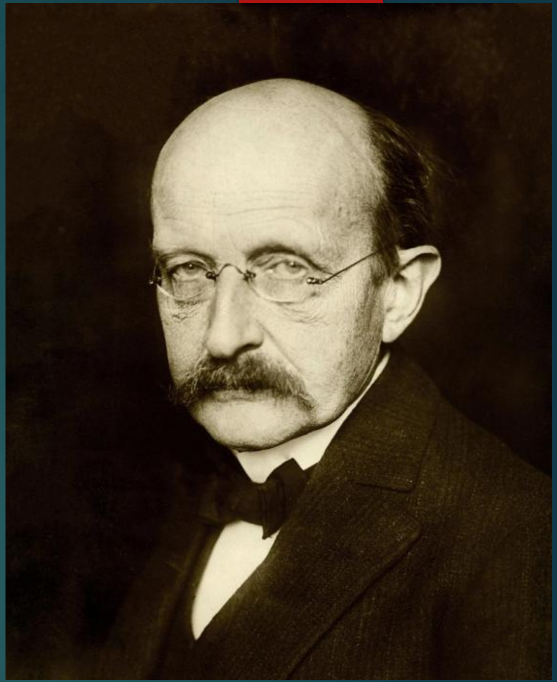
- Quantum computers and classical computers can solve the same problems
- **True!**
- A quantum computer can simulate a classical computer, and *vice versa:*
  - We don't know how to simulate *efficiently* quantum physics on a classical computer
  - For *some* problems there are *exponentially* more efficient quantum algorithms

Quantum Computers, Explained With Quantum Physics

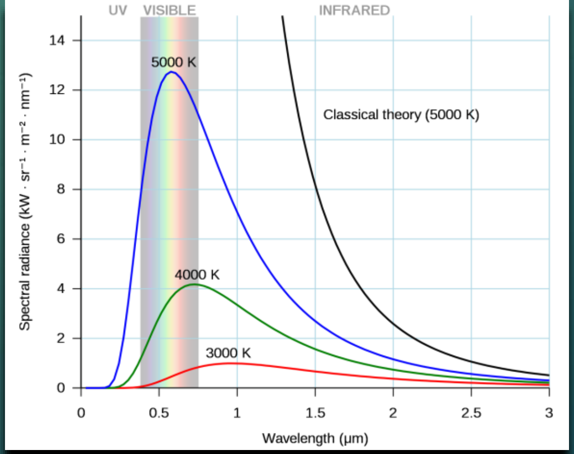
- https://youtu.be/jHoEjvuPoB8

A Brief History of Quantum Computing

- 1900: Max Planck's study of 'black-body' radiation
- An object in thermal equilibrium with its environment emits (mostly infrared) electromagnetic radiation (waves)
- The radiation intensity depends on the temperature of the object
- Planck: the energy released by the radiation comes in 'packets' (*quanta*)



Max Planck
(1933, public domain)

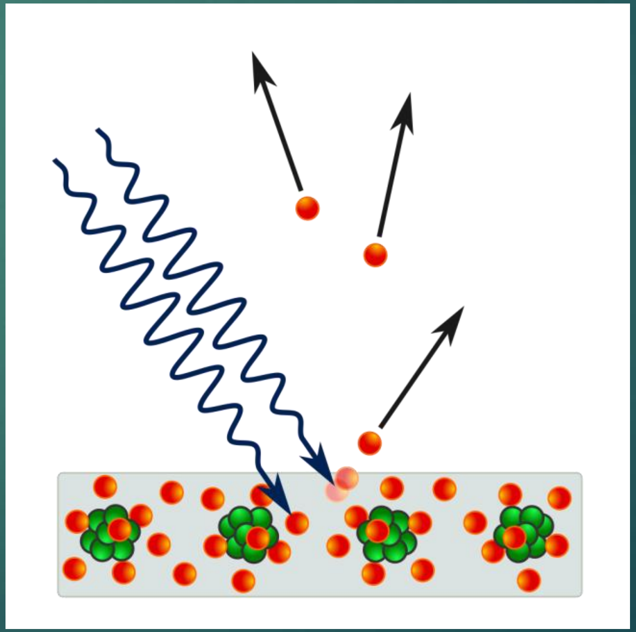


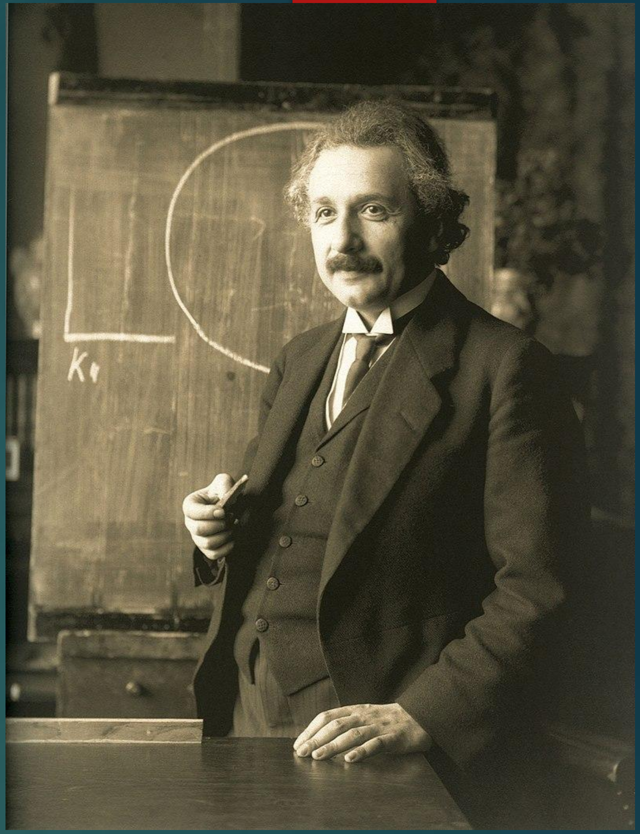
Public domain

Public domain

A Brief History of Quantum Computing

- 1905: Albert Einstein explained the photoelectric effect by assuming that light is absorbed in 'packets' (*quanta*)
- Einstein: light propagates through space as massless particles called *photons*
- Einstein got his Nobel prize for this work





Albert Einstein
(1921, public domain)

A Brief History of Quantum Computing

- 1926: Erwin Schrödinger’s equation describes the temporal evolution of an isolated quantum system

Time-dependent Schrödinger equation *(general)*

$$i\hbar\frac{d}{dt}|\Psi(t)\rangle = \hat{H}|\Psi(t)\rangle$$

Time-independent Schrödinger equation *(general)*

$$\hat{\mathrm{H}}\,|\Psi\rangle = E|\Psi\rangle$$

Erwin Schrödinger
(1933, public domain)

A Brief History of Quantum Computing

- 1927: Werner Heisenberg's uncertainty principle

- "Some things cannot be measured precisely"

$$\sigma_x \sigma_p \geq \frac{h}{2}$$

Position precision

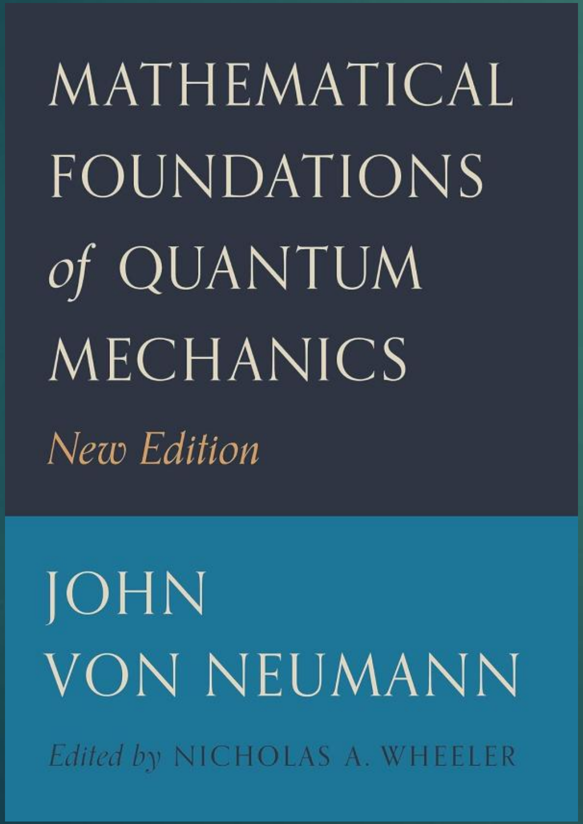
Momentum precision

Planck's constant (~10^{-34})

Werner Heisenberg
(1933, Bundesarchiv, Bild 183-R57262 / Unknown author / CC-BY-SA 3.0)

A Brief History of Quantum Computing

- 1932: John von Neumann’s book *Mathematical Foundations of Quantum Mechanics*



- Basically, the theoretical underpinnings of quantum computing!

John von Neumann
(Los Alamos)

Dr. Strangelove (Columbia Pictures)

A Brief History of Quantum Computing

- 1963: Yves Lecerf
- 1973: Charles Bennett

Charles Bennett
(https://www.flickr.com/photos/ibm_research_zurich/51002548905/)

- Reversible Turing machines
- An isolated quantum computer must be reversible! (Follows from Schrödinger's equation.)

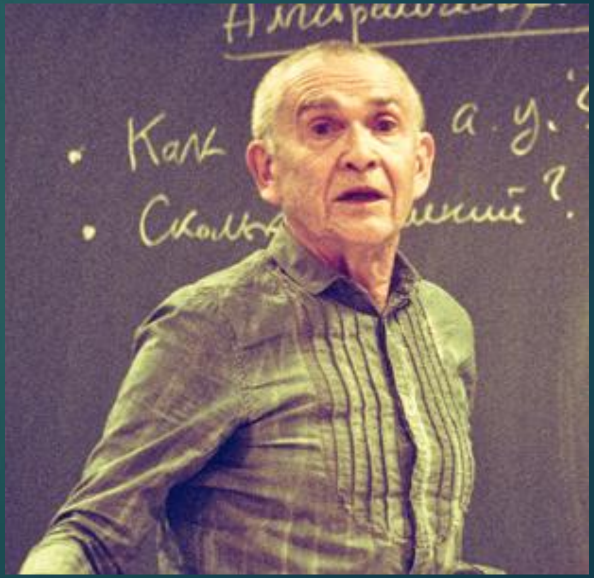
A Brief History of Quantum Computing

- 1980: Paul Benioff, Yuri Manin
- 1982: Richard Feynman

- First ideas about quantum computers
- *“Nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy.”* (Feynman)

Richard Feynman
(The Nobel Foundation)

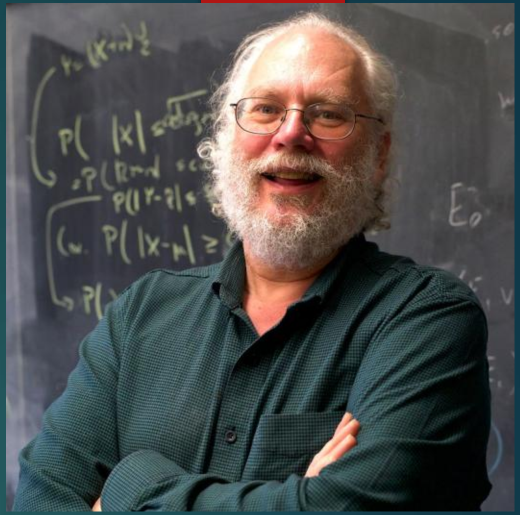
Paul Benioff
(Argonne National Lab)



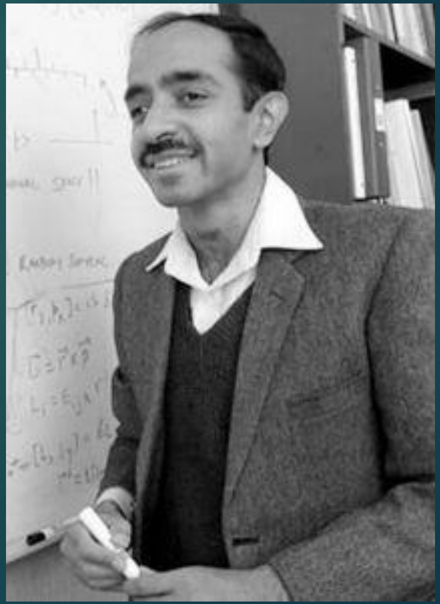
Yuri Manin
(Denis Mironov, CC BY-NC-ND)

A Brief History of Quantum Computing

- 1994: Peter Shor's quantum algorithm for integer factoring
  - **Exponential** speed-up over *current* classical algorithms
  - The Story of Shor's Algorithm, Straight from the Source
- 1996: Lov Grover's quantum algorithm for search
  - **Quadratic** speed-up over *best possible* classical algorithm



Peter Shor
(BBVA Foundation)



Lov Grover
https://datascience.columbia.edu/event/dr-lov-grover-is-quantum-searching-a-universal-property-of-nature/

Today: Public Sector

Major public investments in quantum technologies (QT):

- UK ~£1bn (likely more as QT are explicitly mentioned in the ***AUKUS*** pact https://www.gov.uk/government/news/uk-us-and-australia-launch-new-security-partnership)
- EU 1bn euro (***Quantum Flagship***)
- US similar amount as EU (plus unknown military spending)
- Germany (the state of Bavaria - automotive) a few hundred millions euro
- China: I don't know any figures, but from what they publish in scientific journals they are field leader

Today: Private Sector

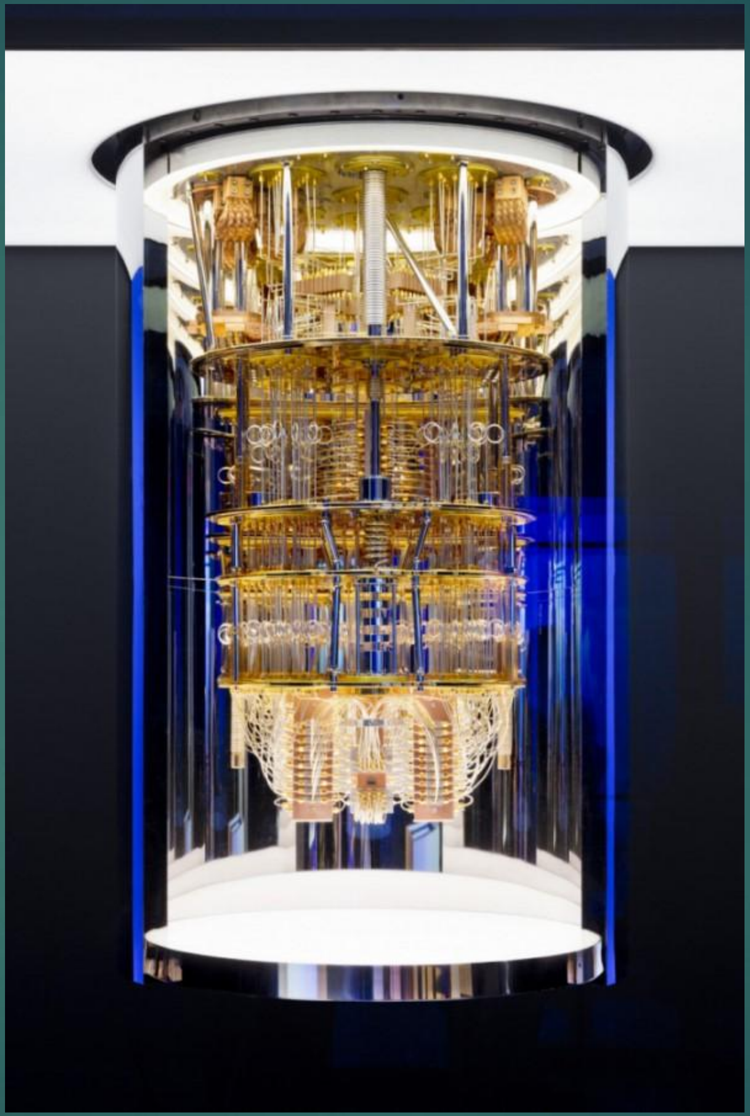
- **IBM, IonQ, IQM, Pasqal, QuERA** and **Quantinuum** build and sell their own quantum computers
- **Intel** and **Google** currently only build private machines
- **Microsoft** employs ~100 researchers and engineers in quantum computing
- **Amazon** have recently opened their quantum computing centre at Caltech
- Much interest and activity in financial institutions:
  - Quantum machine learning
  - Quantum simulation

Today

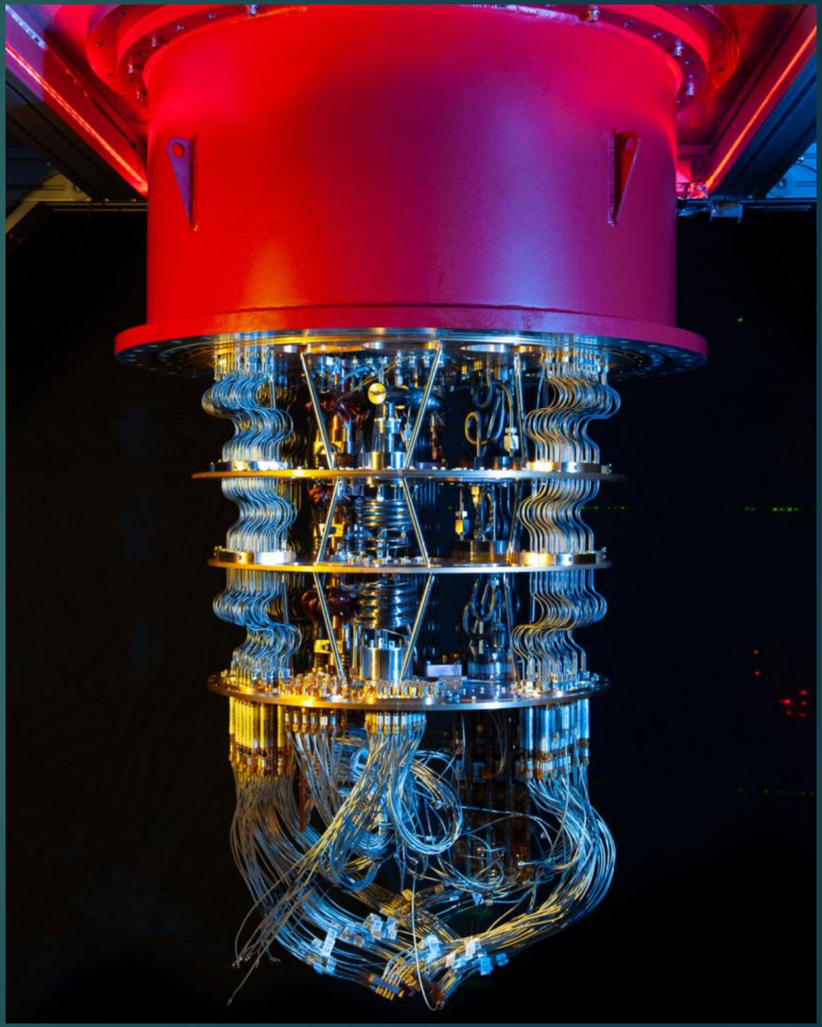
- We are in the **NISQ** (Noisy Intermediate-Scale Quantum) computer era.
- **IBM**: currently 156-qubit systems publicly available; 1,121-qubit system arrived in 2023.
- **Google**: ‘quantum supremacy’ demonstrated in Oct 2019 with a 54-qubit system.

https://quantumai.google/

https://research.ibm.com/blog/quantum-development-roadmap



https://commons.wikimedia.org/wiki/File:IBM_logo.svg

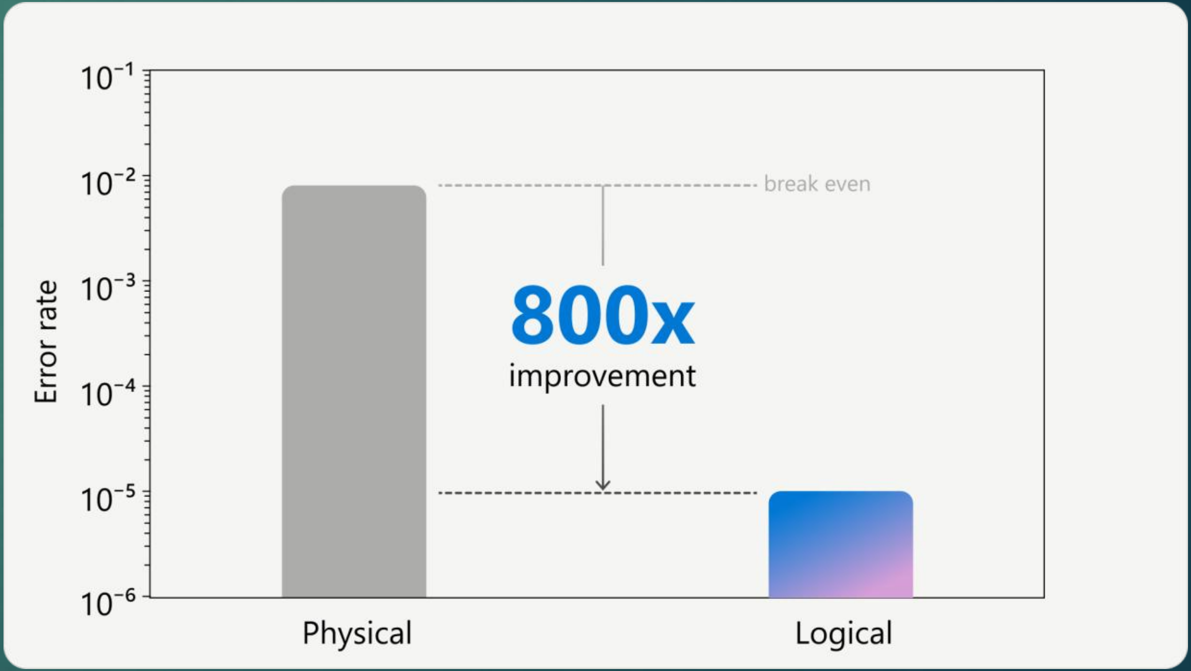


Google’s Sycamore

Today

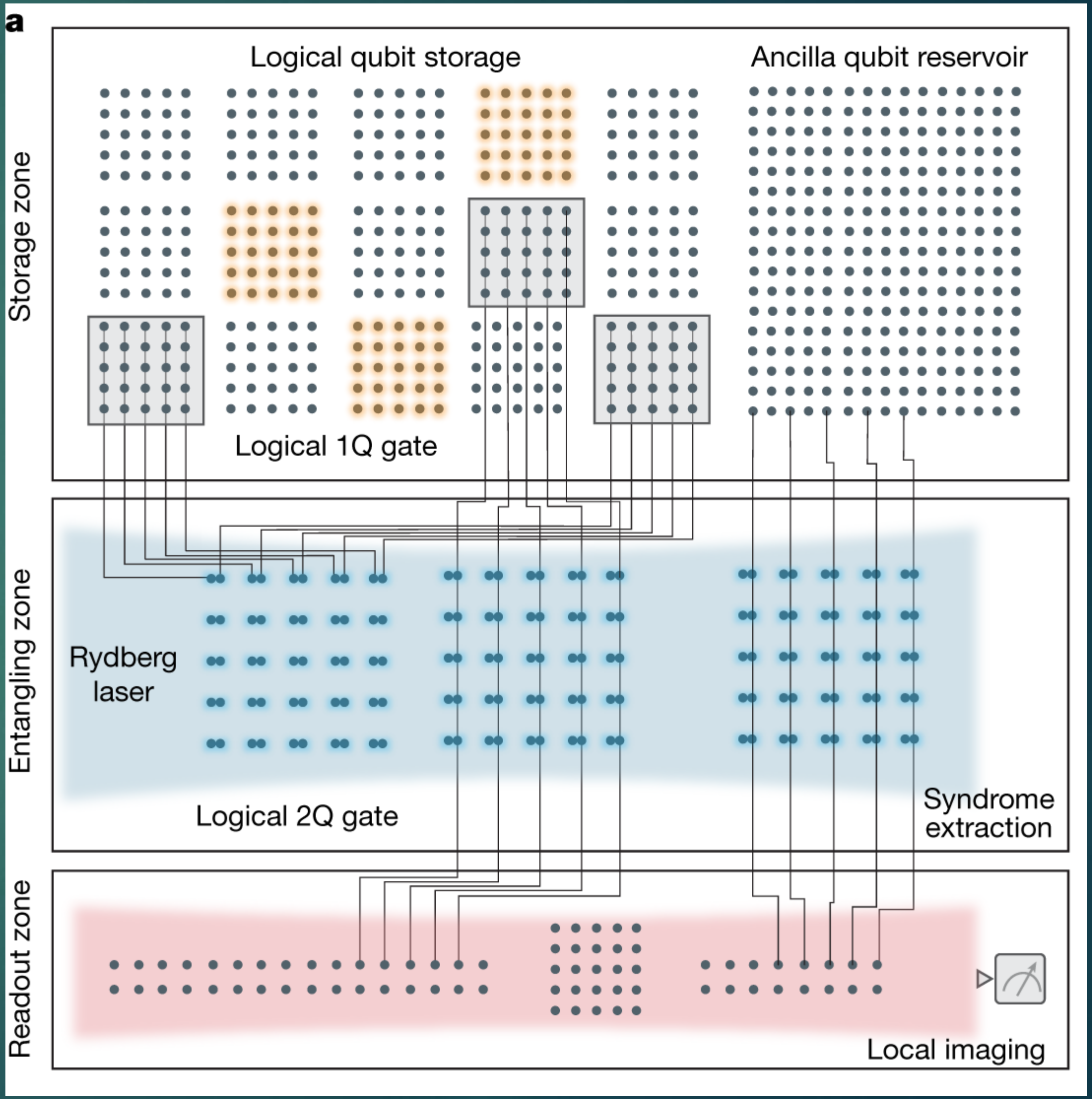
- **April 2024.** *Microsoft and Quantinuum demonstrate the most reliable logical qubits on record with an error rate 800x better than physical qubits*

- Created ***four*** (very reliable) logical qubits from 30 physical qubits
  - ~99.8% fidelity
- 800x error rate reduction:
  - Although by postselection …
- Technical details here



Today

- **December 2023. Harvard/MIT/QuEra:** *Error-Corrected Quantum Algorithms on 48 Logical Qubits*.
- Created up 48 logical qubits from ~300 physical qubits, and ran non-trivial quantum programs on them.
- Showed that quantum ECC gets better with increasing code size.
- High-level presentation (watch the part where they shuttle qubits around!)
- *Nature* paper and another seminar.



Today

- **February 2025. Microsoft announces the [Majorana 1 chip](#).**
  - First chip based on a topoconductor, utilizing Majorana particles.
  - Could be revolutionary for implementing fault-tolerant quantum computers.
  - https://quantum.microsoft.com/

Ettore Majorana
1906-1938?
(Public domain)

Photo by John Brecher for Microsoft