



NITHeP Mini-school on quantum computing

# INTRODUCTION TO THE THEORY OF QUANTUM COMPUTING

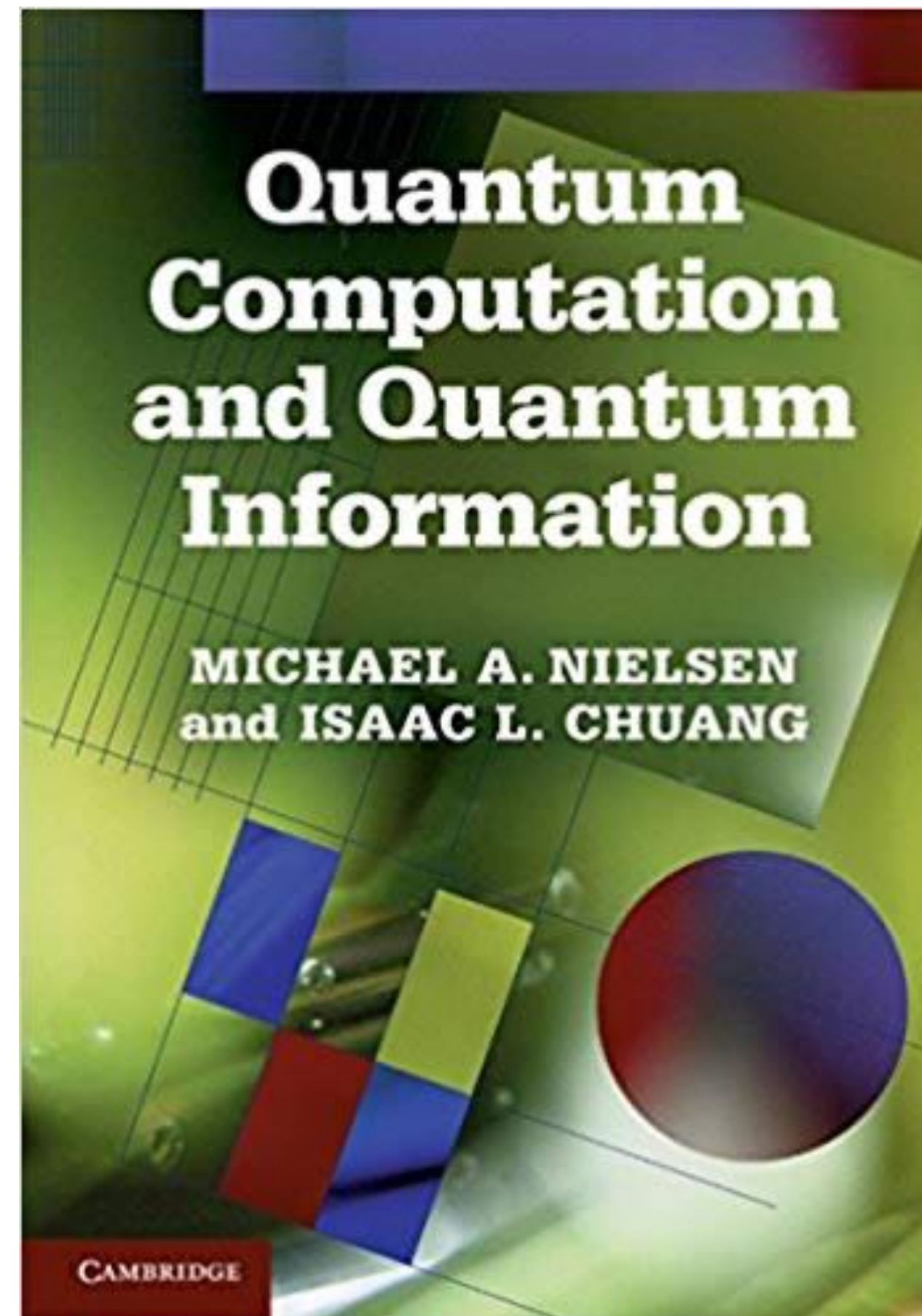
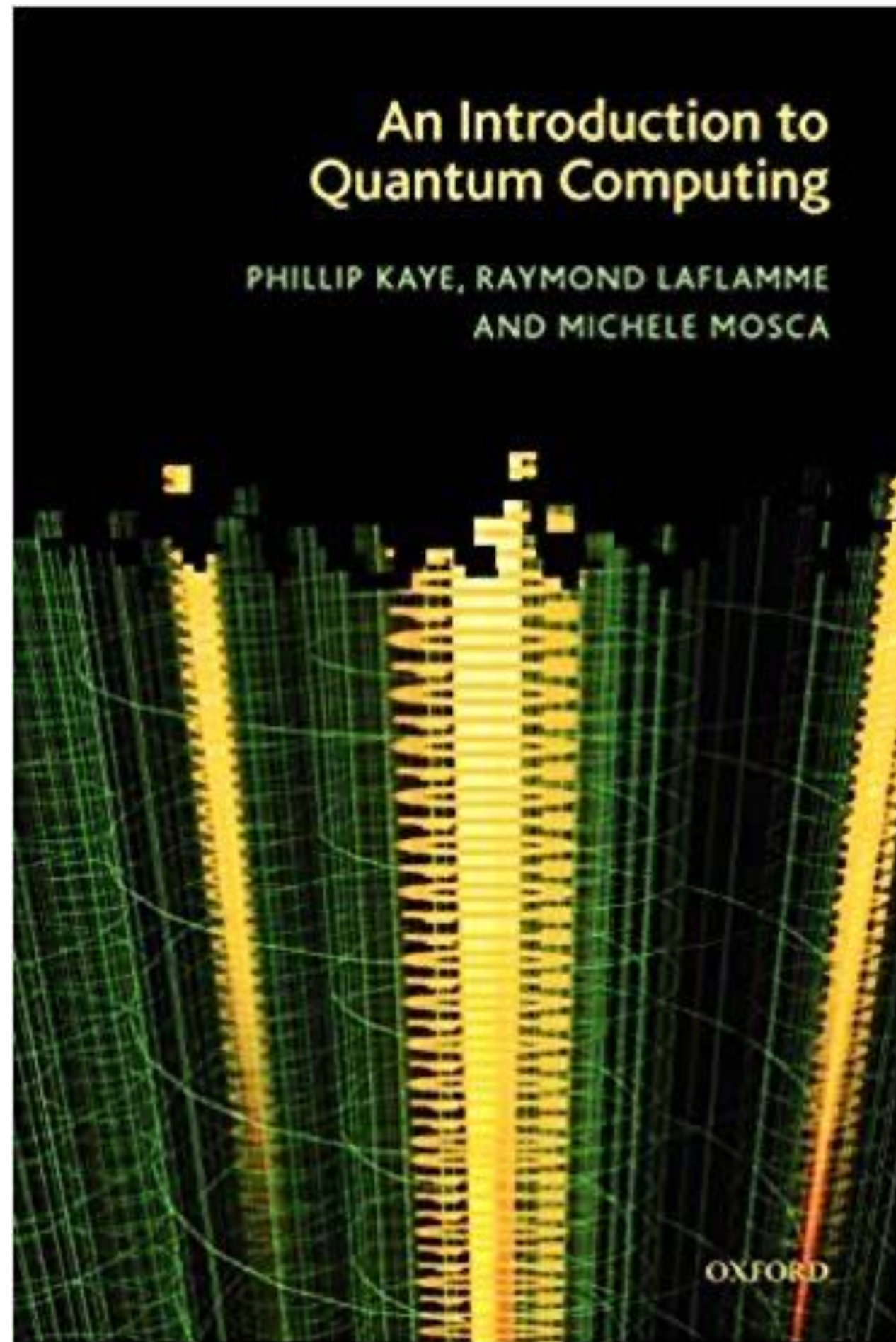
---

Daniel K. Park | [dkp.quantum@gmail.com](mailto:dkp.quantum@gmail.com)





# Some References



## Course Notes:

- John Preskill (Caltech)
- Umesh Vazirani (UC Berkeley)
- Scott Aaronson (UT Austin)
- John Watrous (U Waterloo)

## Part I: What & Why

- Introduction & Background

## Part II: How

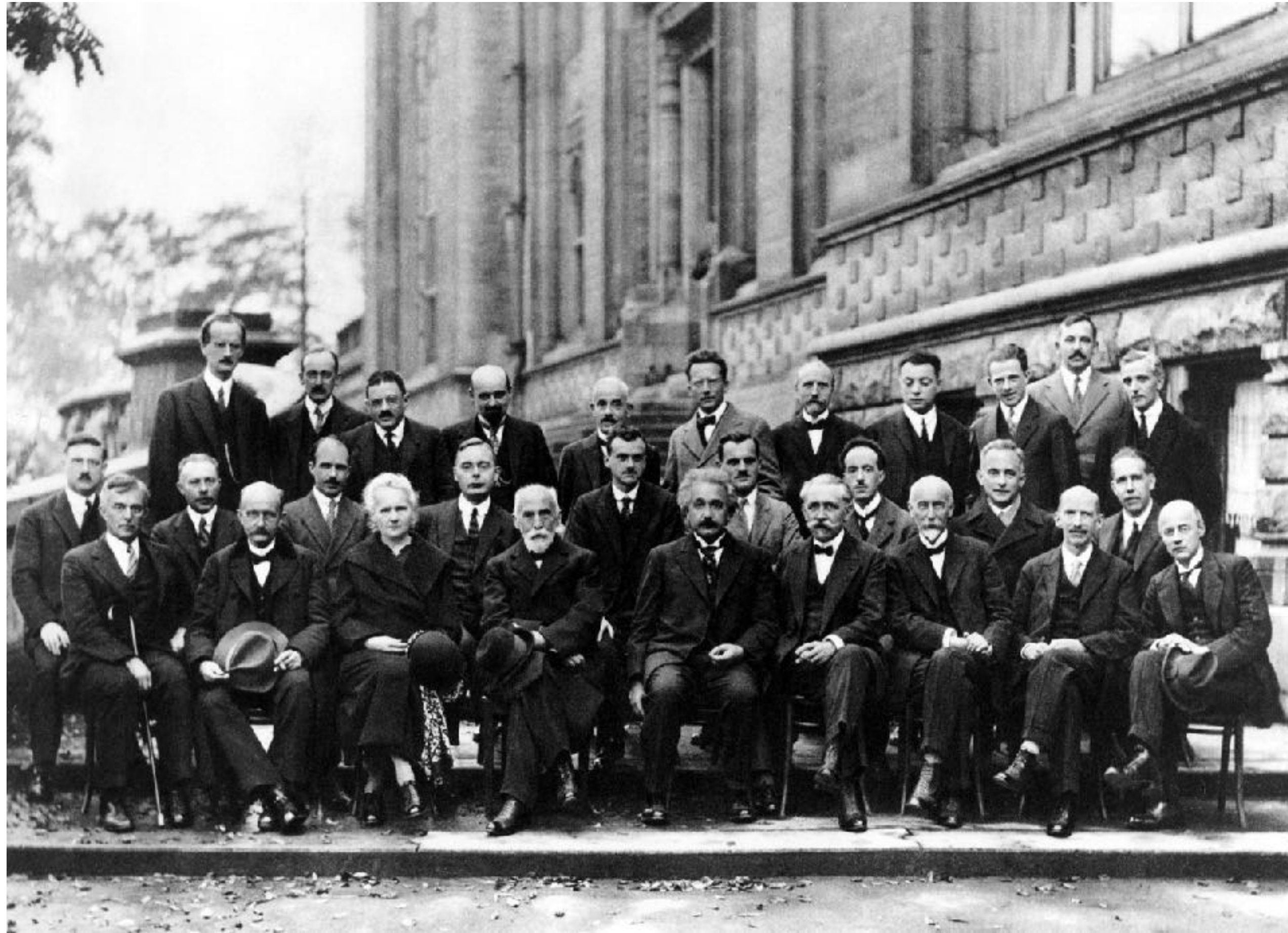
- Quantum Circuit
- Quantum Algorithms
- Quantum Error Correction

# I. Introduction & Background

---



# What is Quantum Information Processing?





# What is Quantum Information Processing?

“Quantum Information Processing is the result of using the laws of quantum physics to perform **information processing tasks** that were previously believed impossible or infeasible”

Here we focus on  
computation

Quantum Information Science

Physics

Computer  
Science

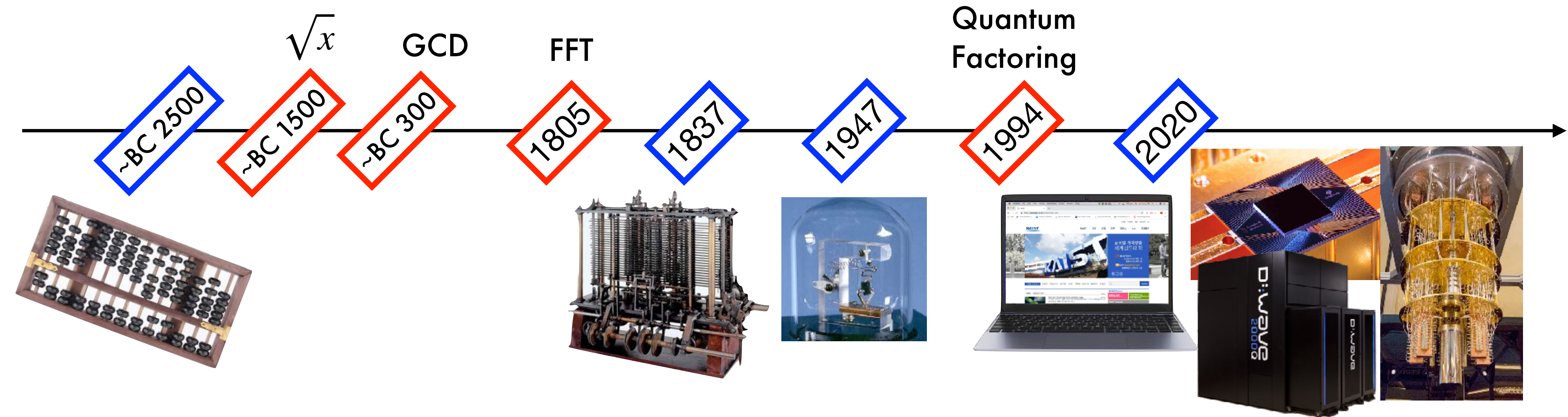
Math

Engineering

Philosophy

- For information to be useful, it must be stored in some physical medium and manipulated by some physical process.
- This implies that the laws of physics ultimately dictate the capabilities of any information-processing machine.
- Thus it is natural to consider the laws of physics when we study the theory of information processing and computation.
- Classical computation is based on classical mechanics. But classical mechanics emerges as a special limit of quantum mechanics. So quantum computers can only be better than classical computers, and it is a **natural attempt** to build a computer based on quantum mechanics.

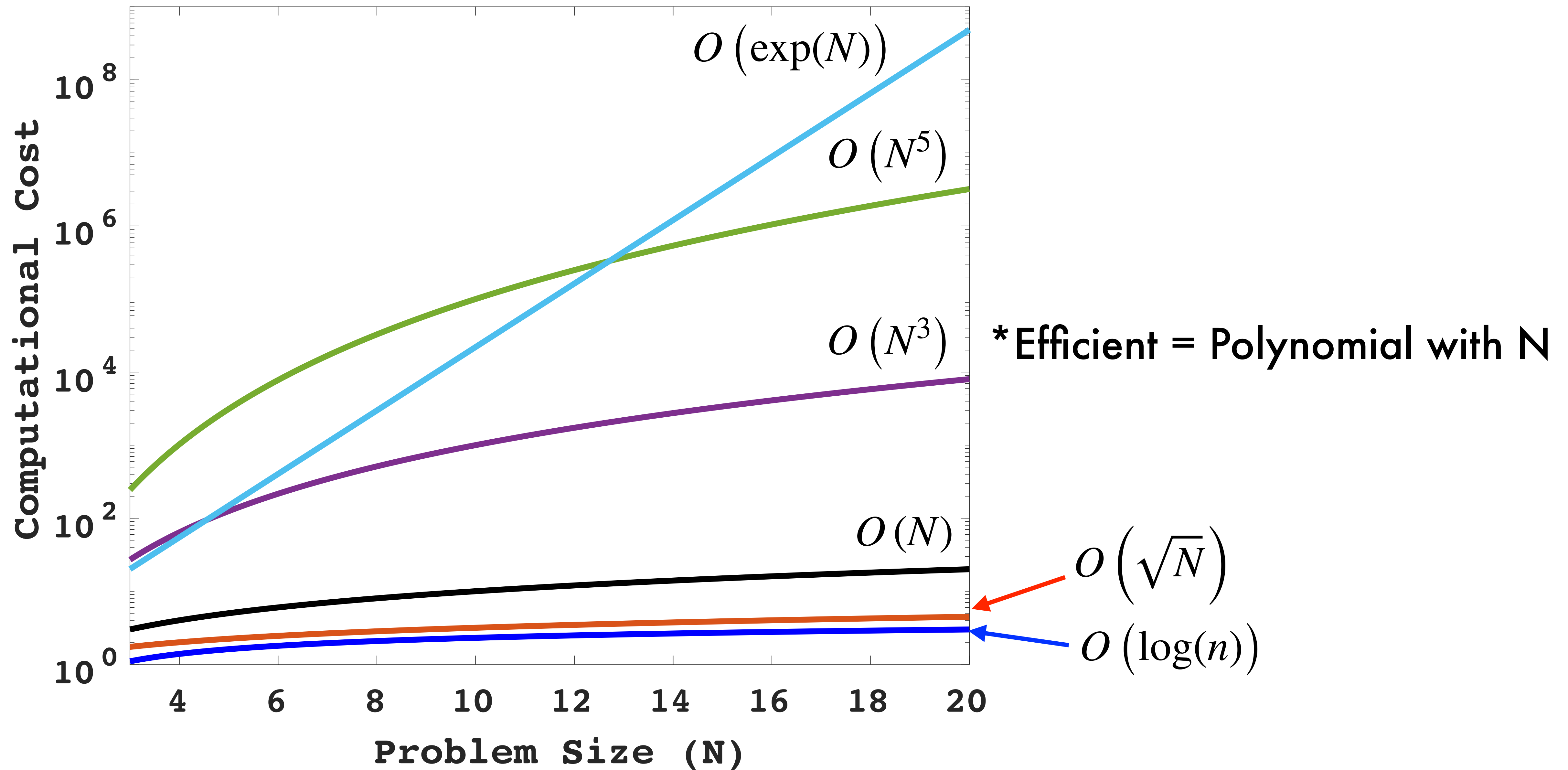
# Computability & Efficiency

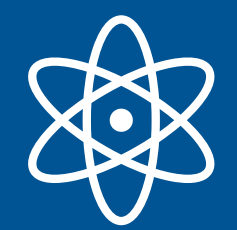


- Fundamental questions: Is a problem computable? How much resource?
- Strong Church-Turing Thesis: A probabilistic Turing machine (PTM) — Turing machine with a coin-flipper — can **efficiently** simulate any **realistic** model of computing.



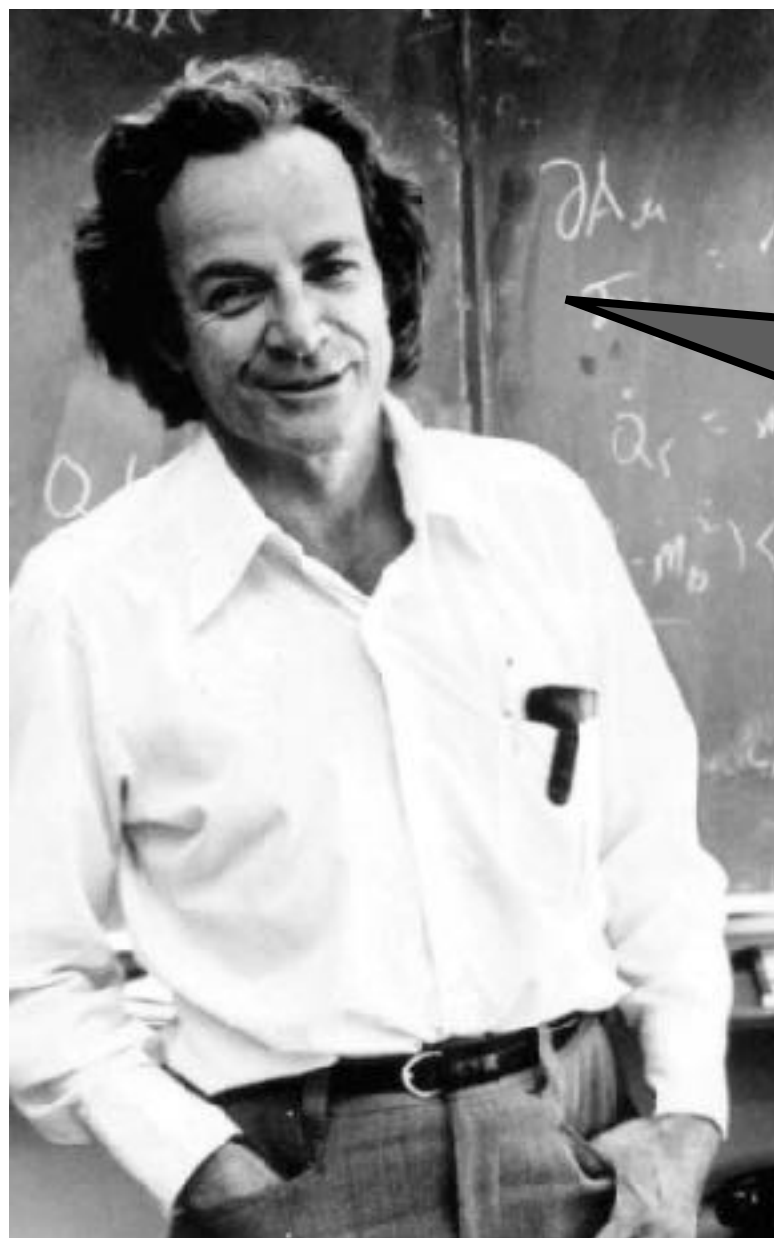
# Computability & Efficiency





# Fundamental Motivations

- Quantum computing challenges the strong Church-Turing thesis.
- Classical computer is not powerful enough to efficiently simulate quantum computer.  
→ Need a computing model capable of simulating arbitrary realistic physical devices.
- Is quantum computing realistic? In principle yes!

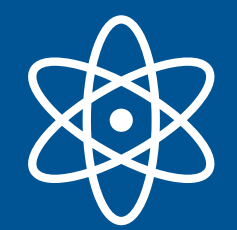


Nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical,...

Quantum physics should be a reference for computational complexity

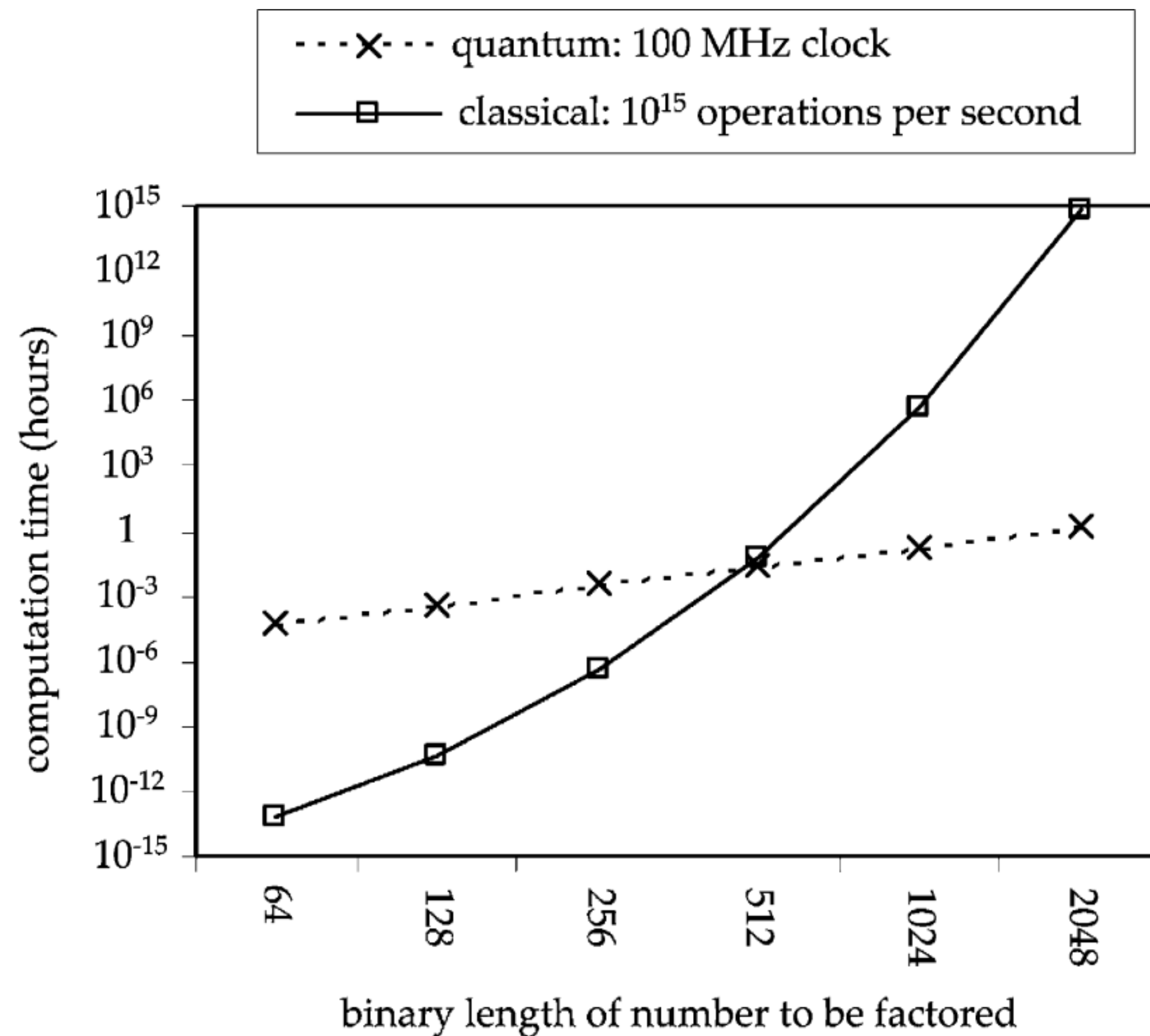






# Example: Shor's Factoring Algorithm

- Given  $N$ , find prime numbers  $p$  and  $q$  such that  $N = pq$
- Basis for commercially important cryptography.
- First quantum algorithm to tackle an important problem that is computationally hard classically.



Source: Proceedings of the IEEE 92(10):1630-1638 (2004)

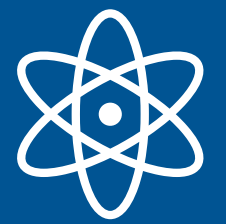
# Eye-Opening Speculations

One of the following scenarios should be correct.

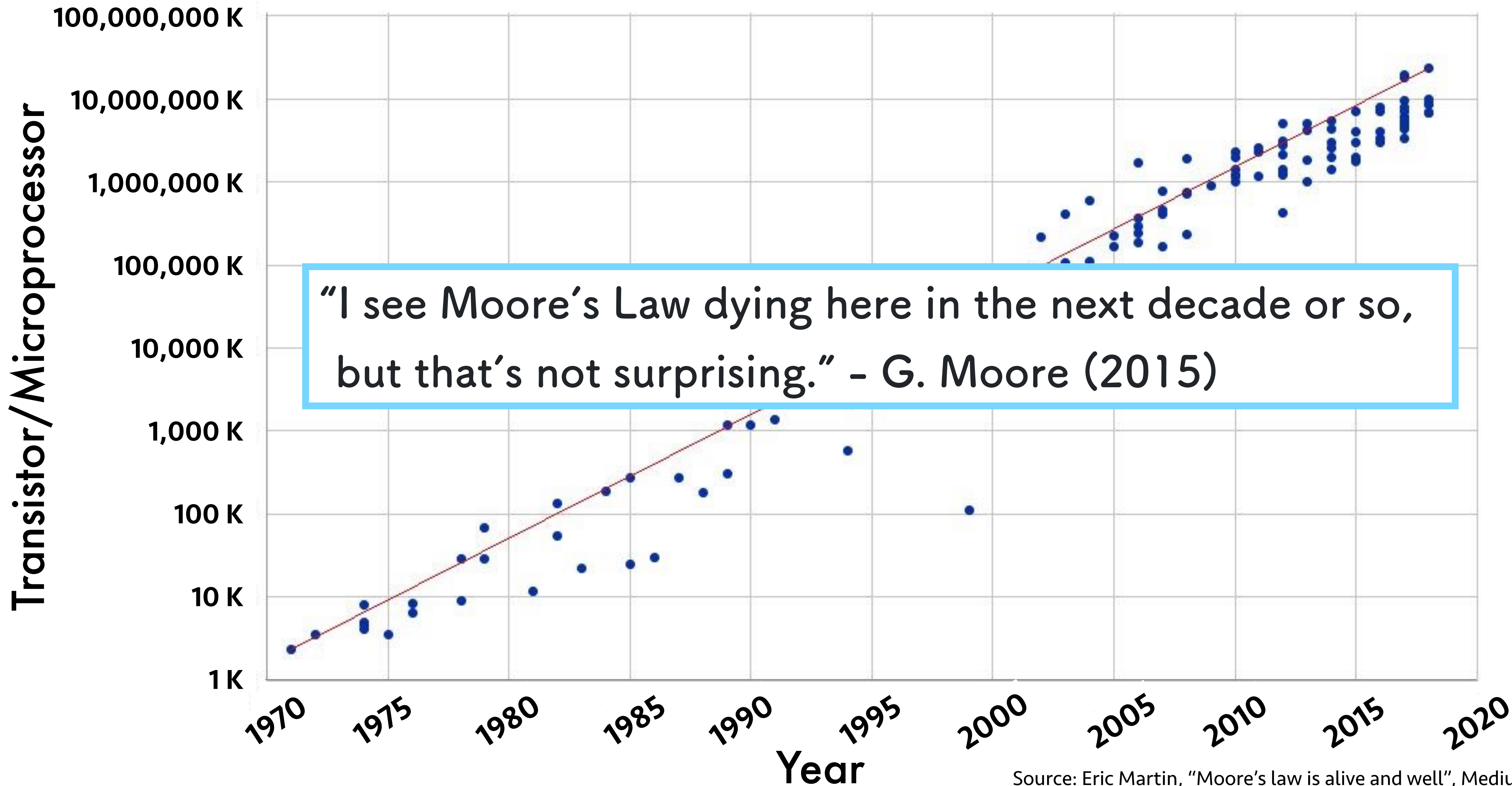
- Practical quantum computation is possible.
- Scalable quantum computing is fundamentally impossible.
  - ➔ Our understanding of quantum mechanics is wrong.
- Classical computing can efficiently simulate quantum mechanics.



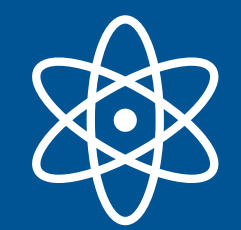




# Technological Motivation: Moore's Law

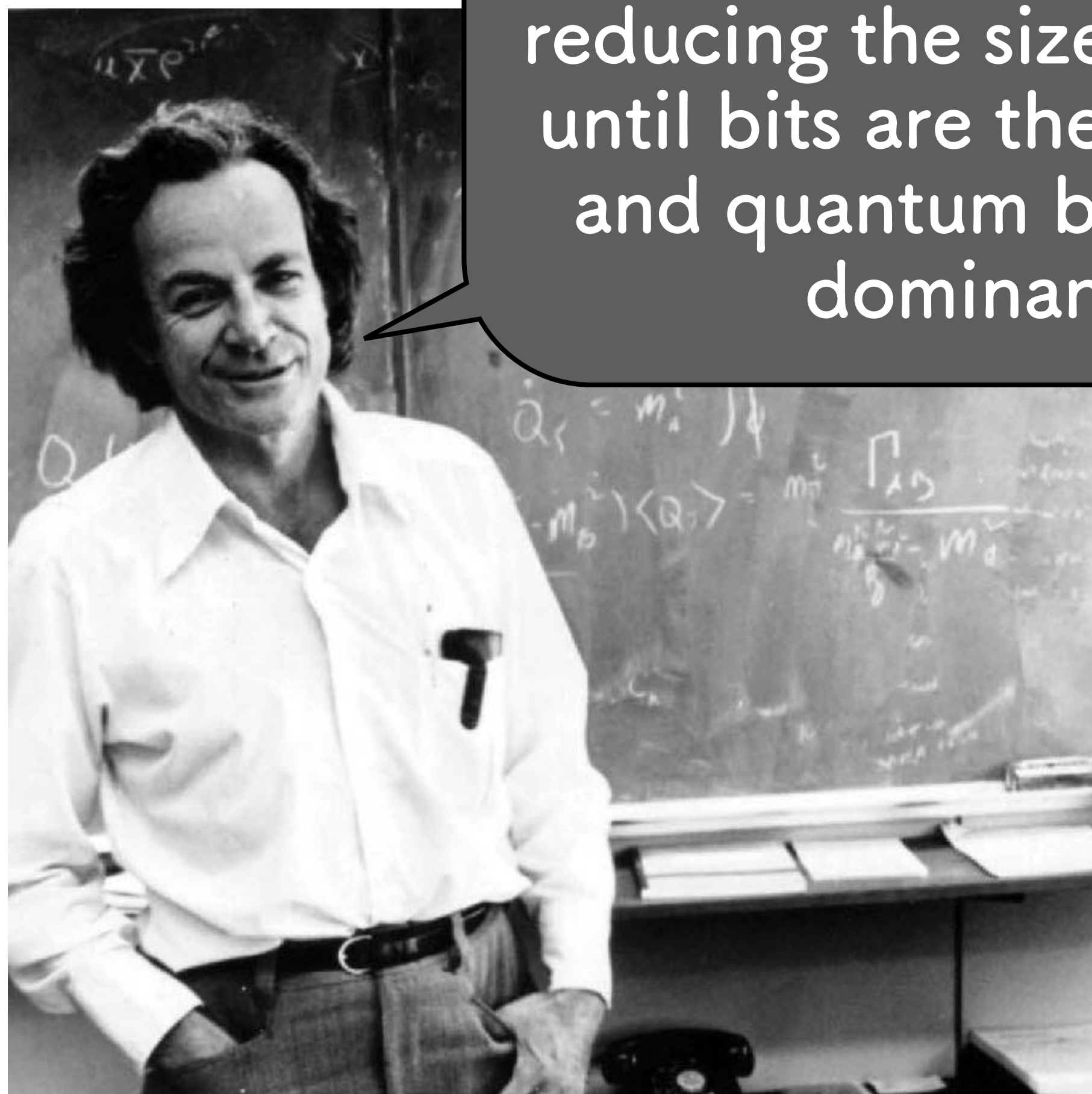




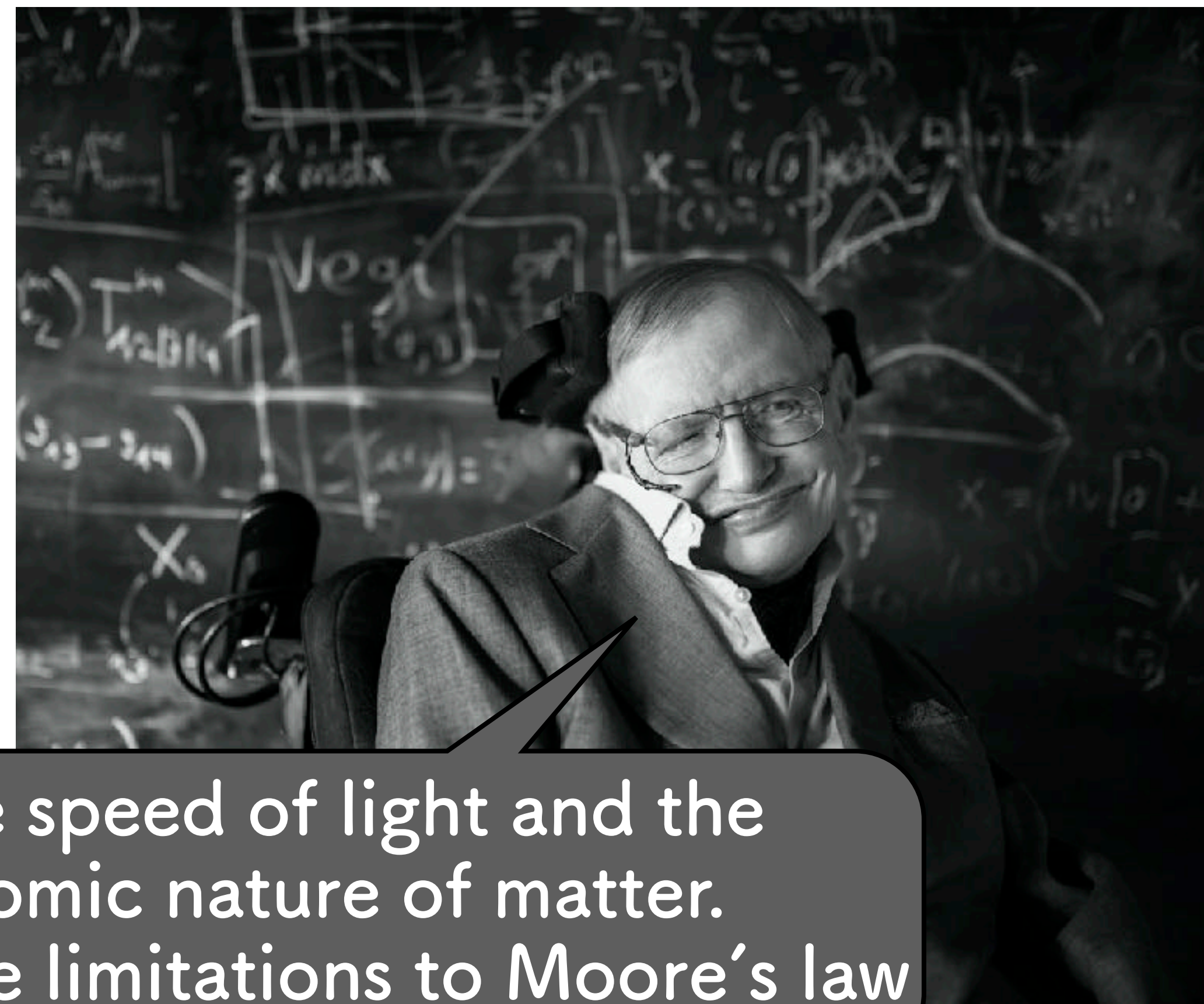


# Fundamental Limit to Current Technology

... it seems that the laws of physics present no barrier to reducing the size of computers until bits are the size of atoms, and quantum behavior holds dominant sway.



The speed of light and the atomic nature of matter.  
- On the limitations to Moore's law

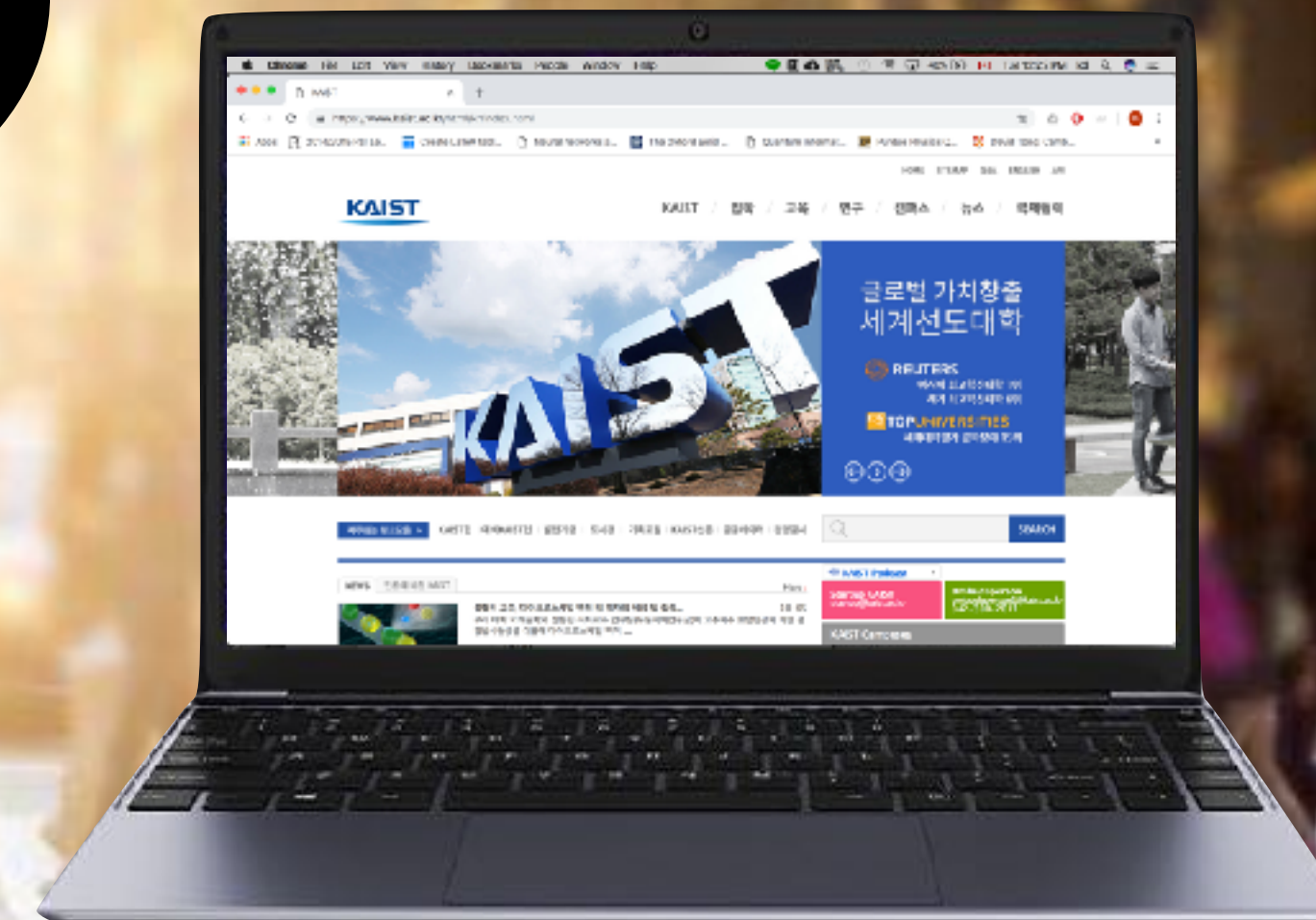




# Physics of What We See



Classical  
Physics





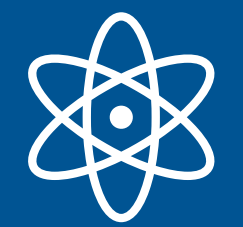
# Physics of What Atoms See



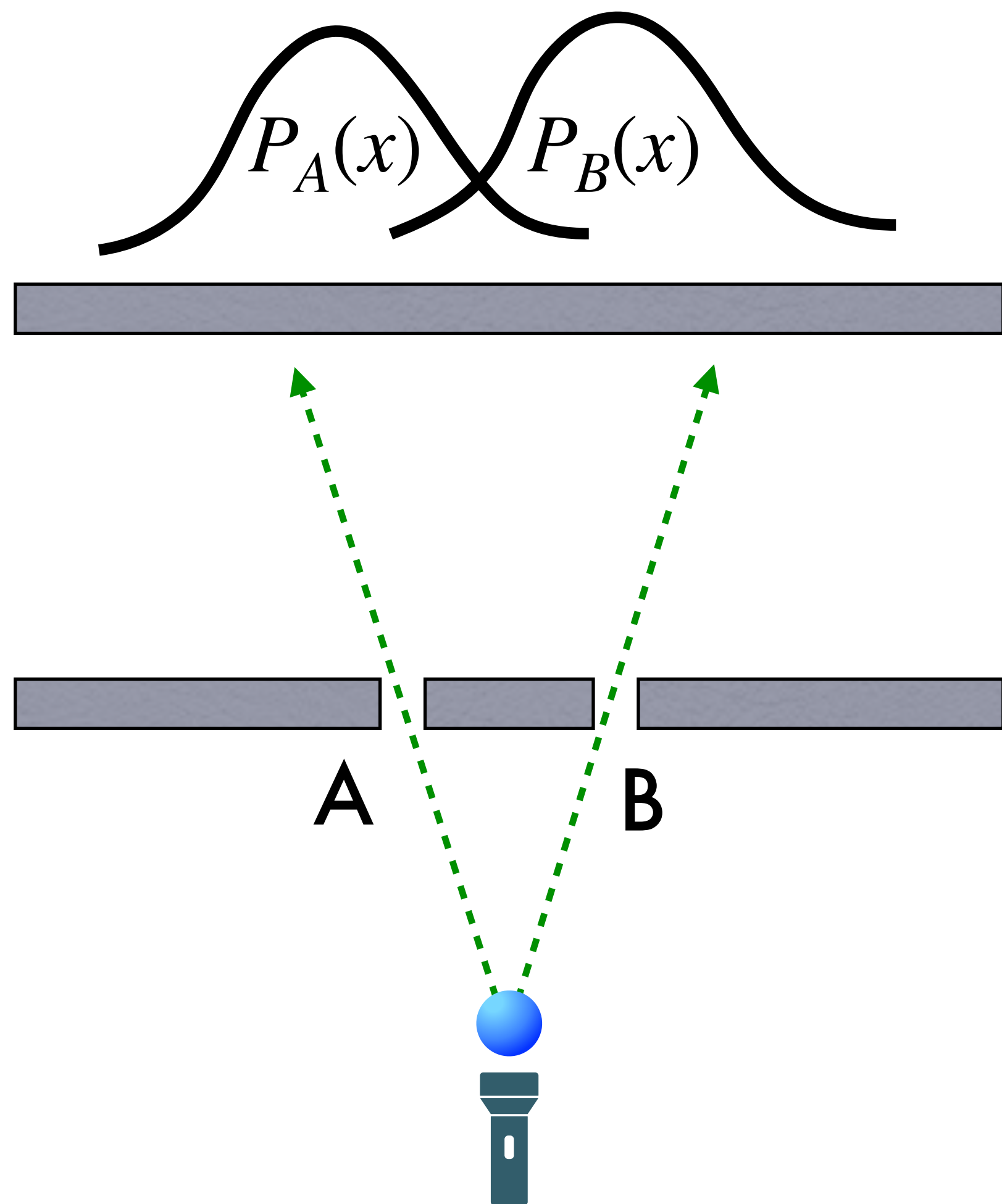
atomic  
scale



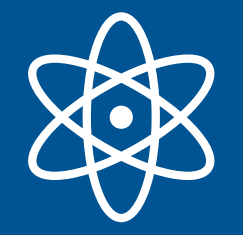




# Quantum: Beyond Our Usual Intuition

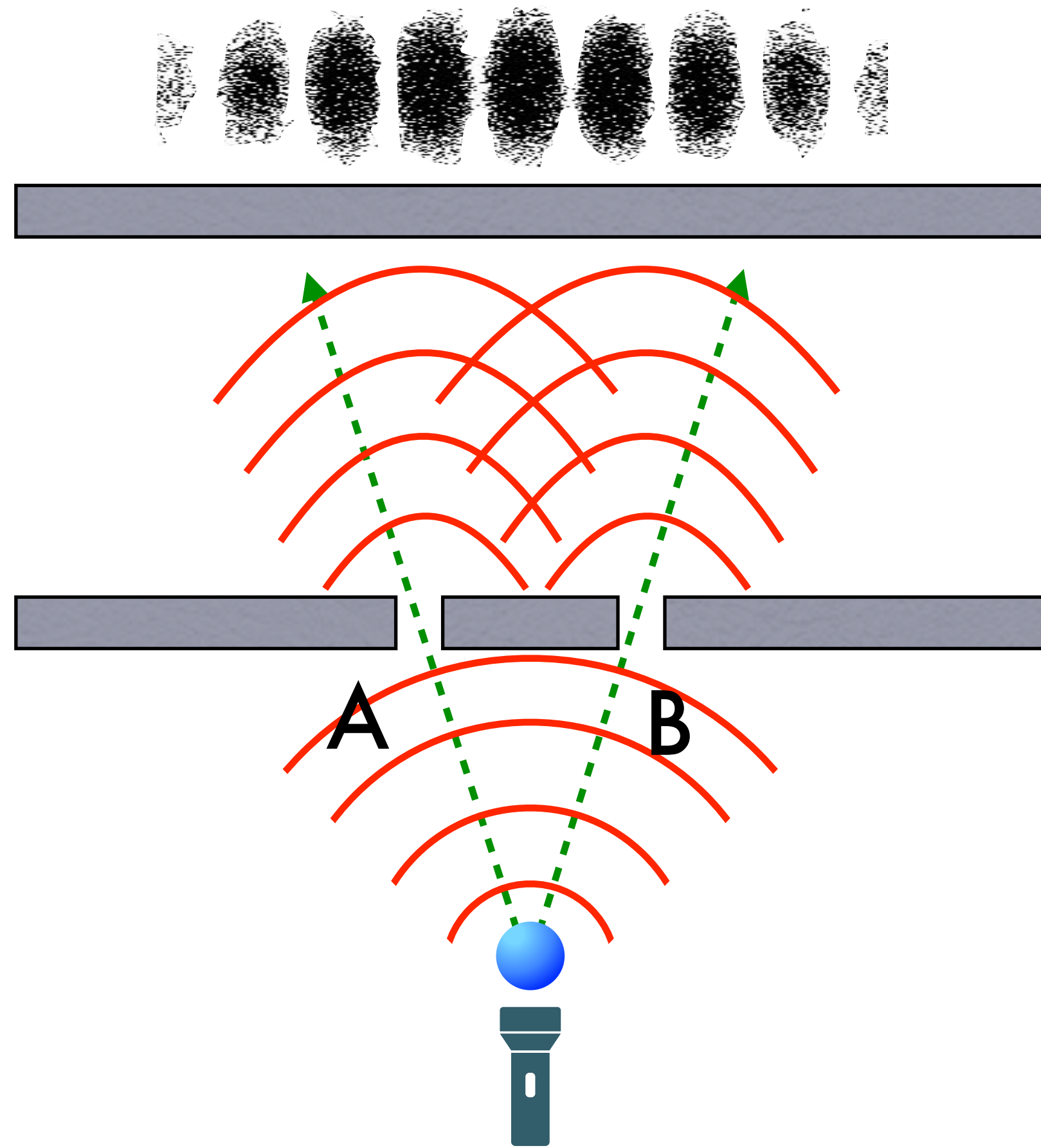


$$P(x) = P_A(x) + P_B(x)$$



# Quantum: Beyond Our Usual Intuition

Quantum interference

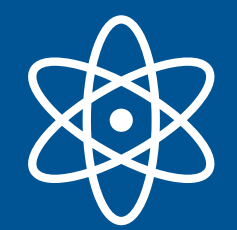


Quantum superposition

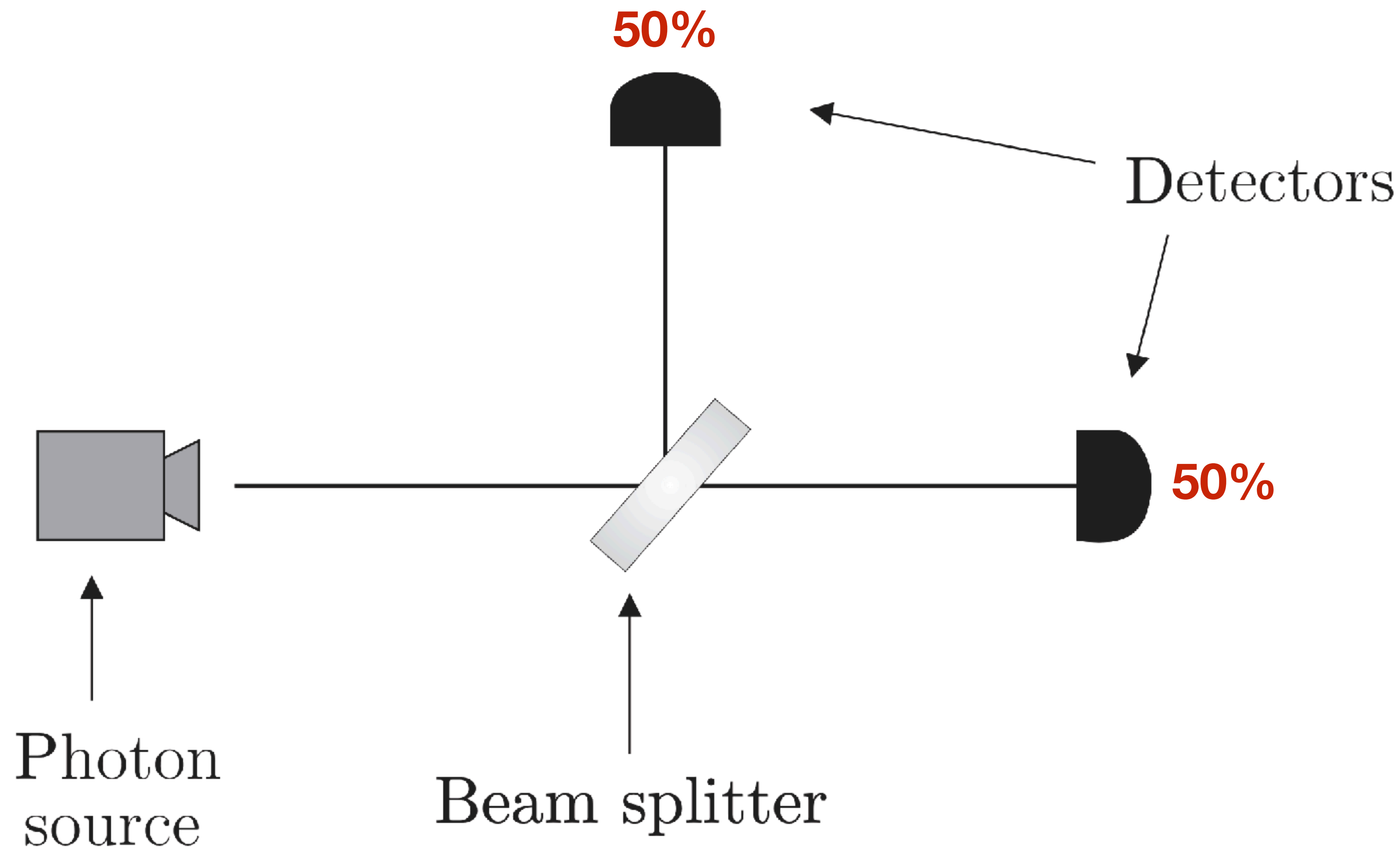
$$P(x) \neq P_A(x) + P_B(x)$$

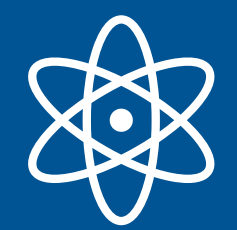
$$P(x) = P_A(x) + P_B(x) + I_{AB}(x)$$



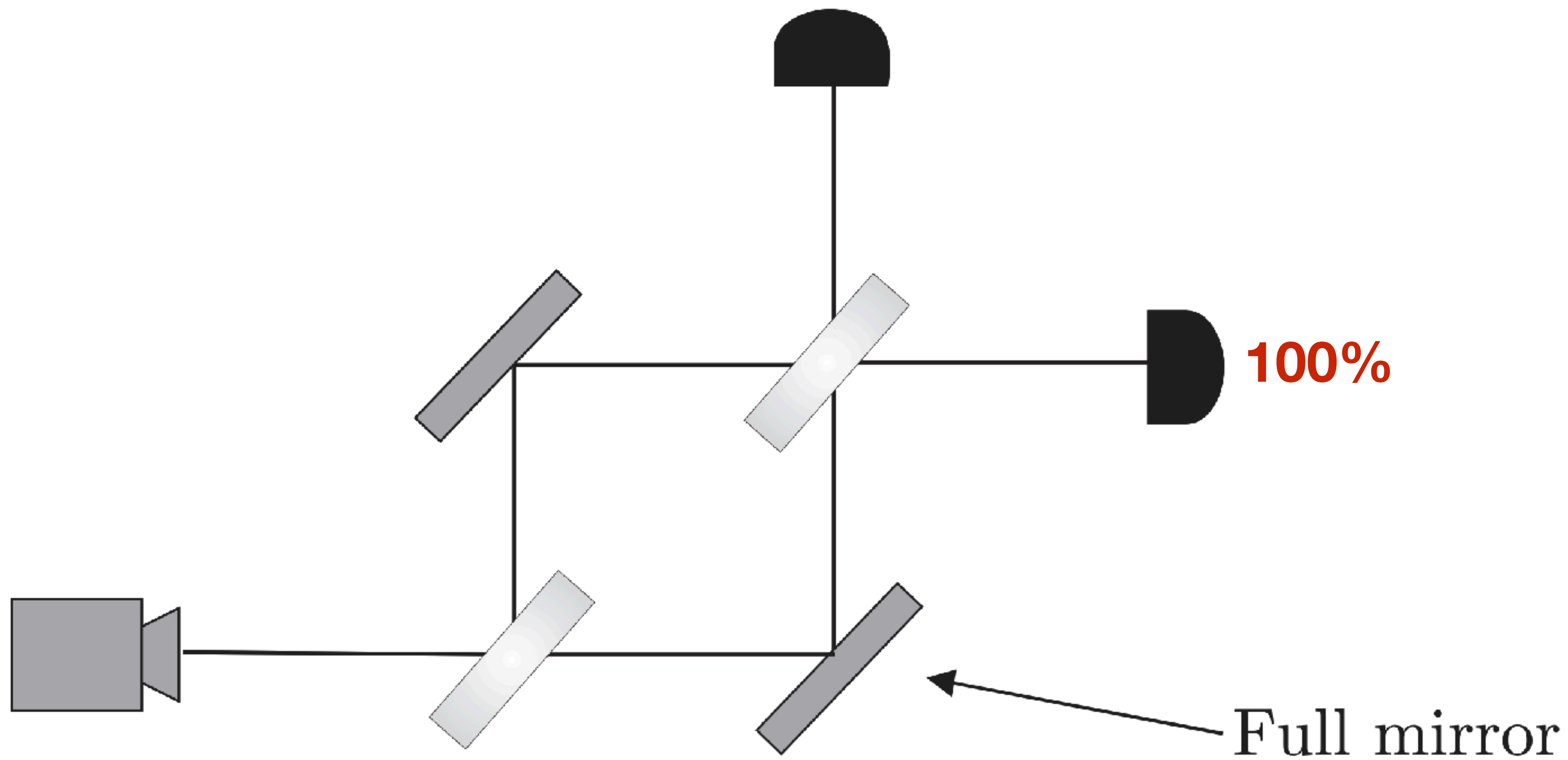


# Quantum: Beyond Our Usual Intuition

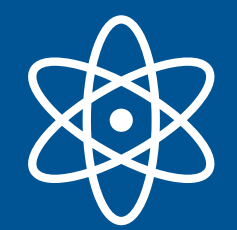




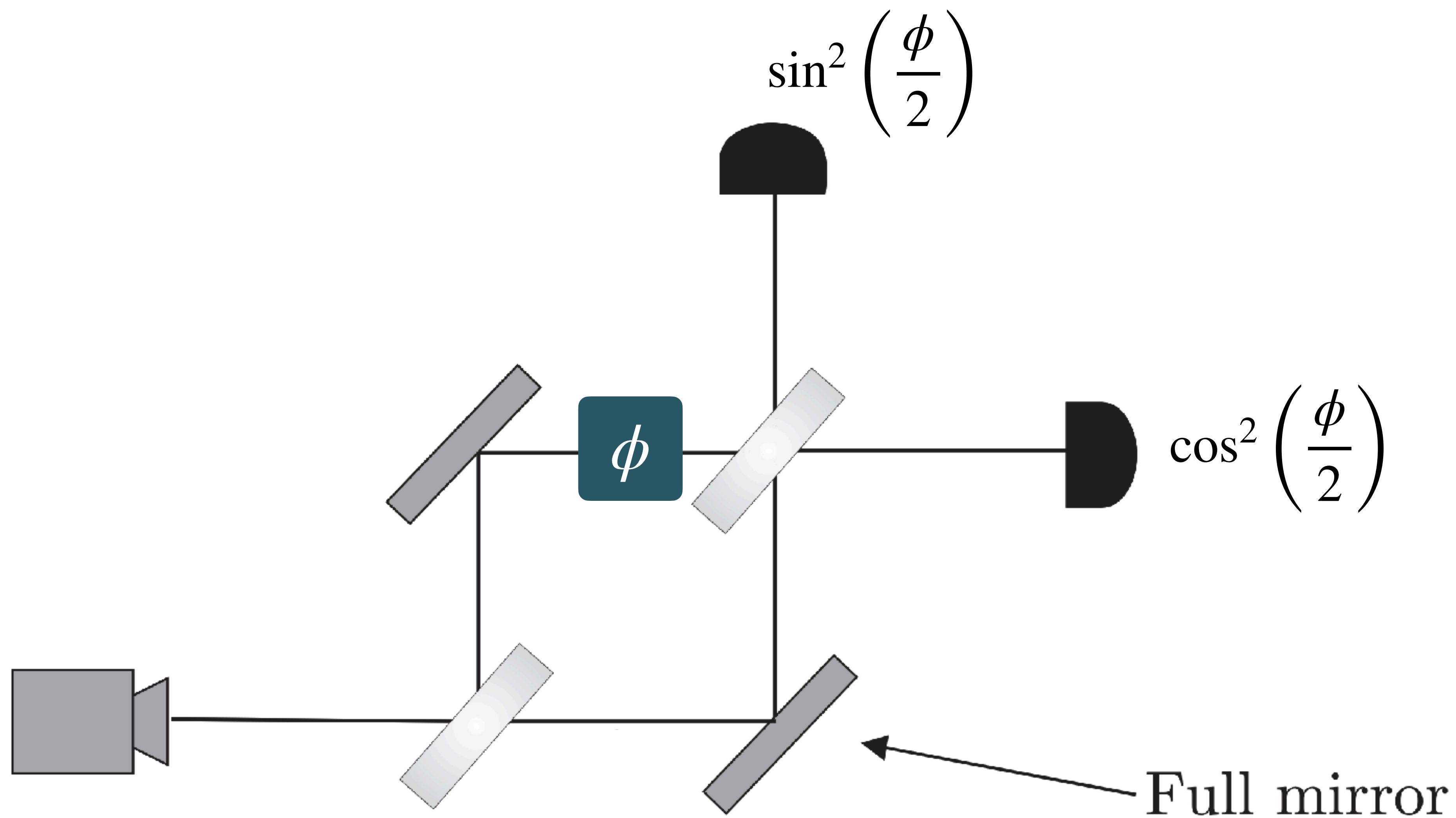
# Quantum: Beyond Our Usual Intuition

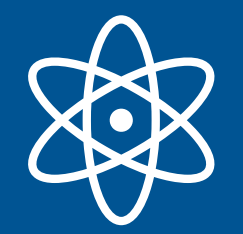






# Quantum: Beyond Our Usual Intuition

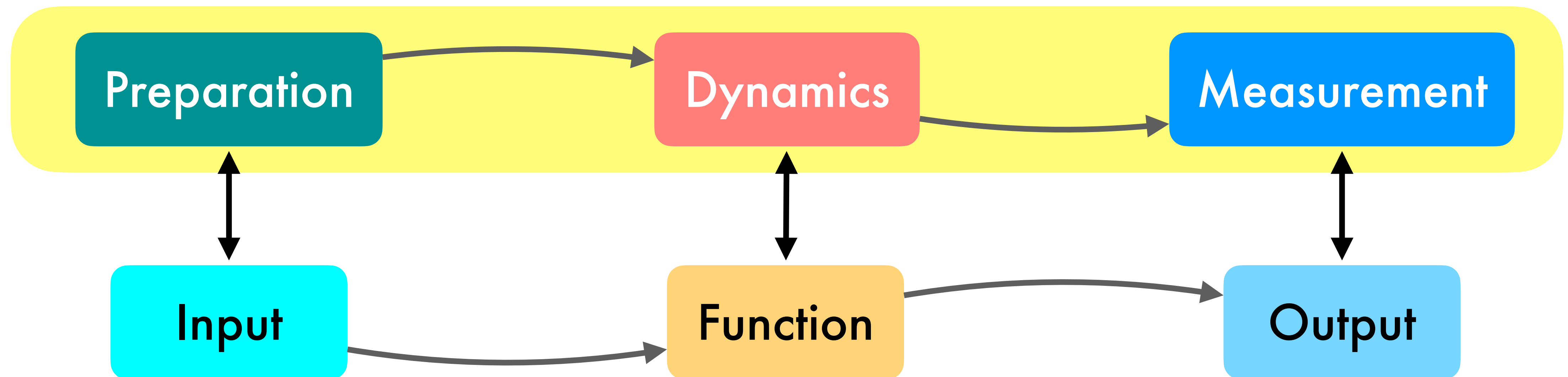




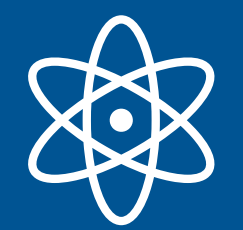
# Quantum Mechanics: Brief Review

- Quantum Mechanics is a mathematical theory that describes nature at the microscopic/atomic scale.
- Quantum Computing consists of:

## Postulates of QM

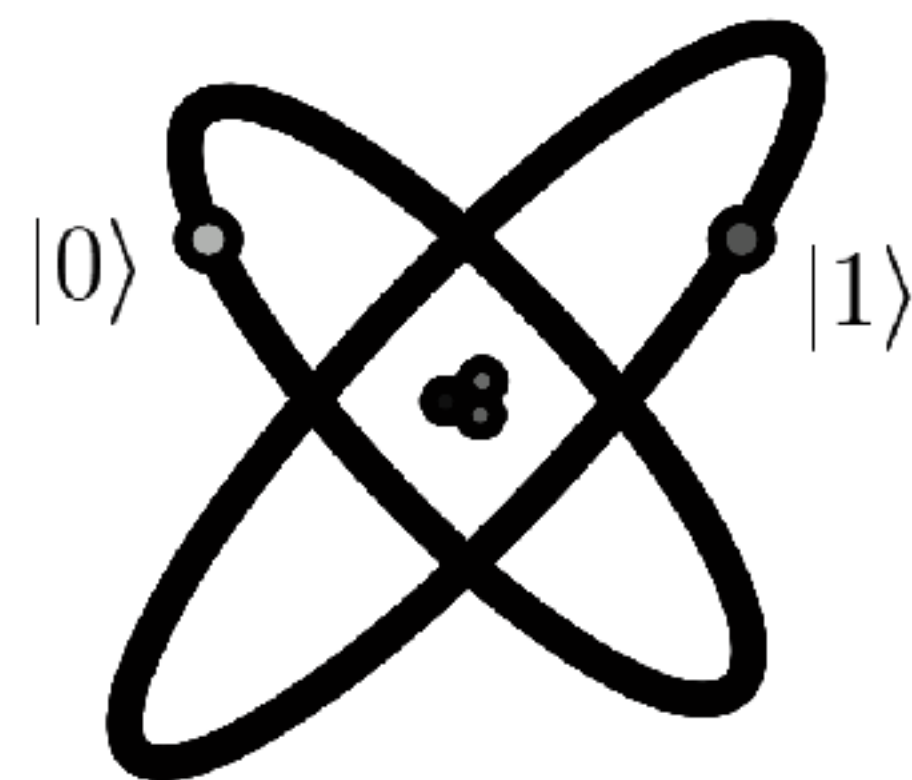




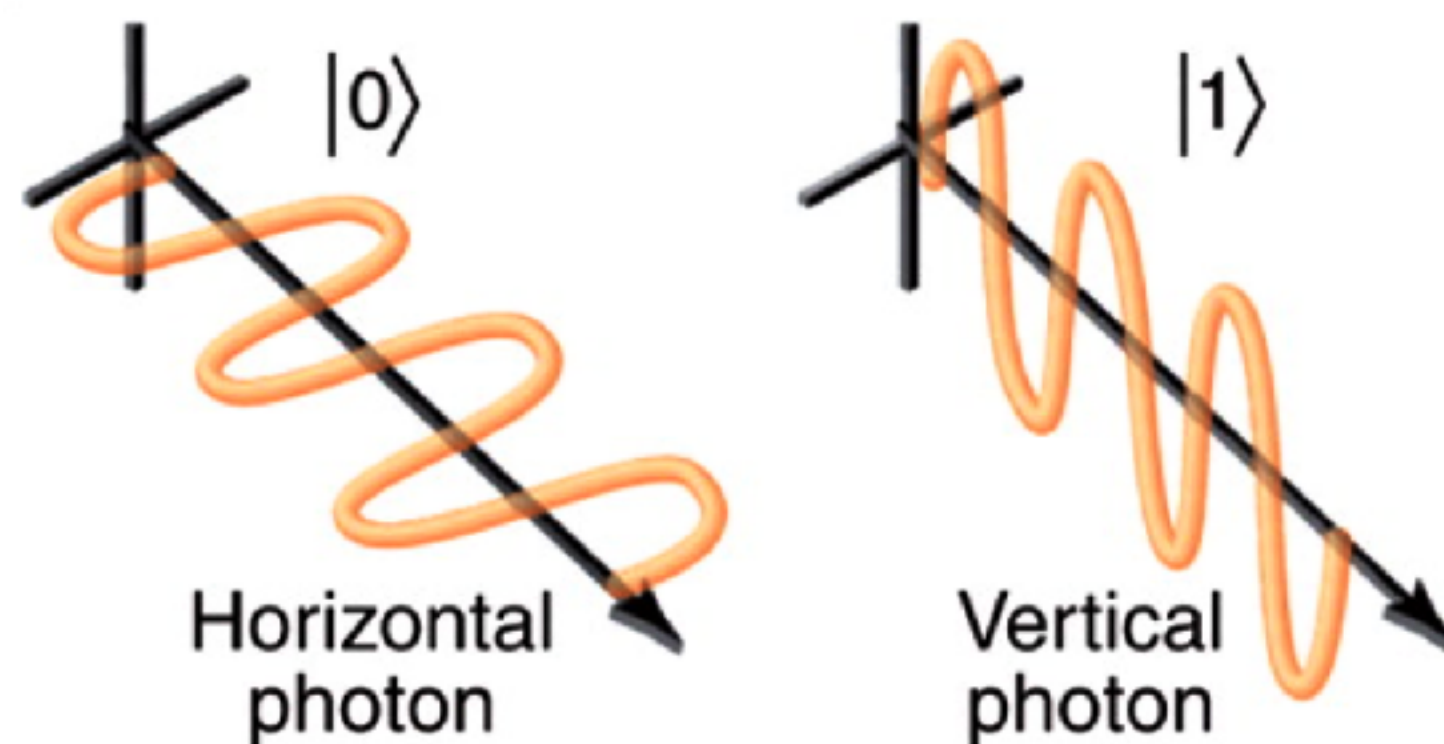


# Abstraction: Qubit

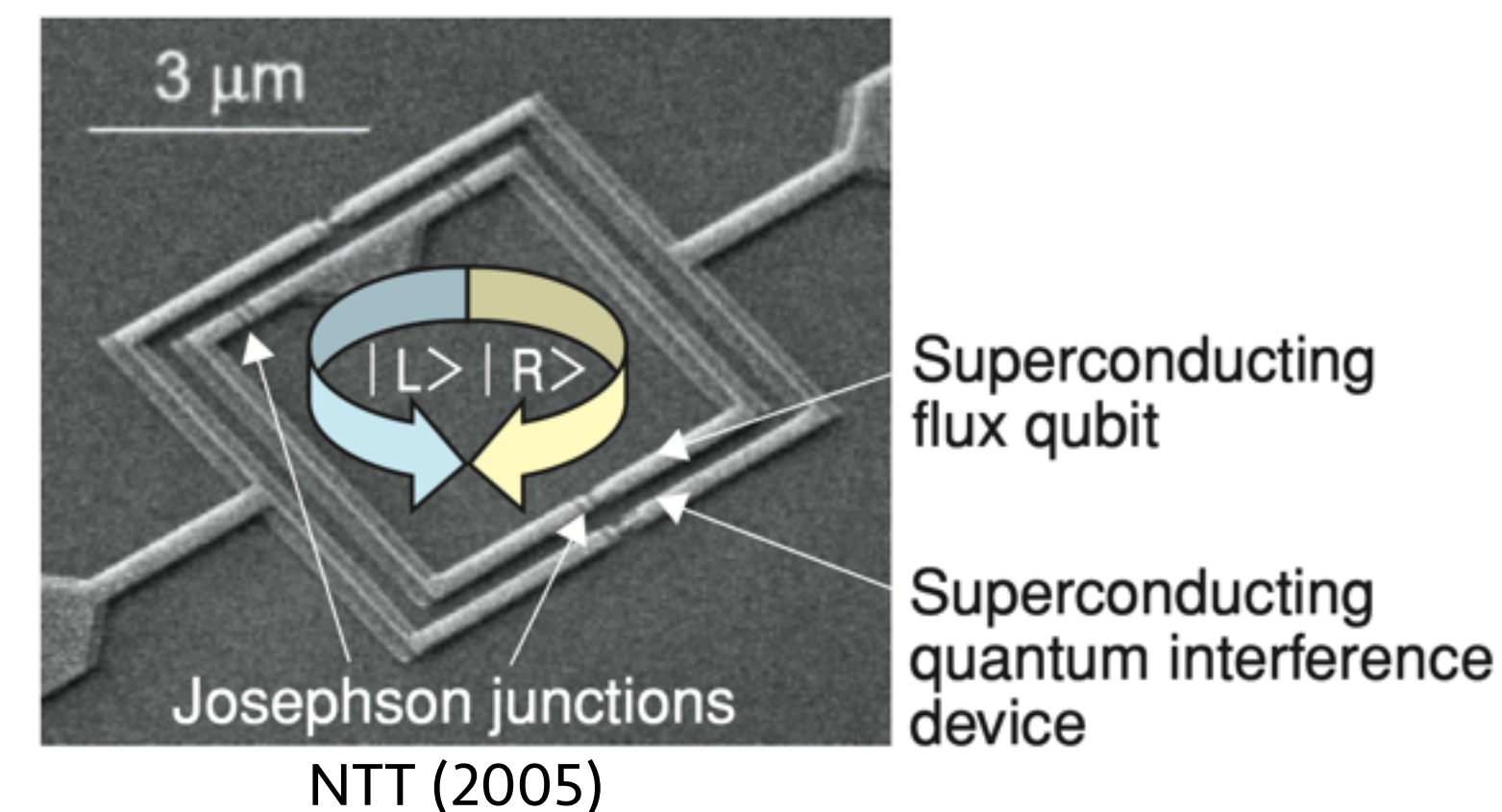
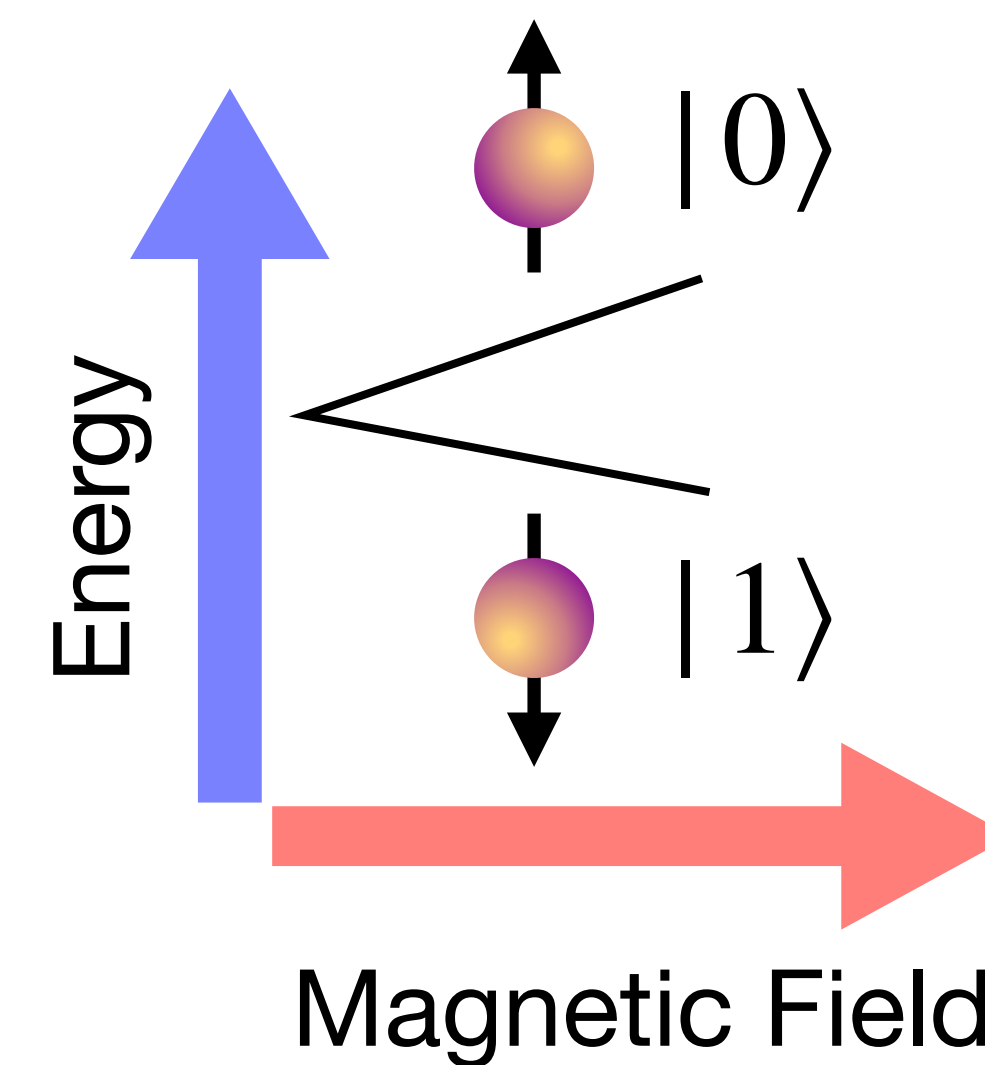
- Bit vs Qubit: Qubit is a unit of quantum information.
- Usually a two level quantum system

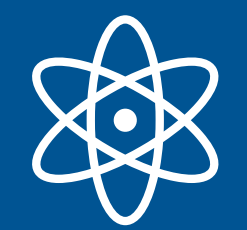


Quantum Computation and Quantum Information (2000)



Optical Quantum Computing, Science, **318**, 1567-1570 (2007)





# Postulates of QM: State

Any isolated physical system is completely described by a **state vector**, which is a unit vector in a complex vector space with inner product (i.e. **Hilbert space**)

$$|\psi\rangle \in \mathcal{H} \quad \langle\psi|\psi\rangle = 1 \quad \langle\phi|\psi\rangle \in \mathbb{C}$$

For  $d$ -dimensional quantum system:  $|\psi\rangle \in \mathbb{C}^d$

For  $n$  quantum bits:  $d = 2^n$



# Postulates of QM: State

Any isolated physical system is completely described by a **state vector**, which is a unit vector in a complex vector space with inner product (i.e. **Hilbert space**)

Dirac notation & computational basis:

$$\underbrace{|000\dots 0\rangle}_{n} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \left. \vphantom{\begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}} \right\} 2^n \quad |000\dots 1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \quad \dots \quad |11\dots 10\rangle = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ 0 \end{pmatrix} \quad |11\dots 11\rangle = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

**Example**  $n=1$ :  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$  and  $\alpha, \beta \in \mathbb{C}$ ,  $|\alpha|^2 + |\beta|^2 = 1$

# Postulates of QM: Dynamics

The time evolution of a closed quantum system is described by the Schrödinger equation

$$i\hbar \frac{d|\psi\rangle}{dt} = H|\psi\rangle,$$

where  $\hbar$  is the Planck's constant and  $H$  is a fixed Hermitian operator known as the Hamiltonian of the closed system.

Or equivalently:

The time evolution of a closed quantum system is described by a unitary transformation

$$|\psi(t_2)\rangle = U(t_2, t_1) |\psi(t_1)\rangle.$$



# Postulates of QM: Measurement

Quantum measurements are described by a set of measurement operators  $\{M_m\}$  that act on the state space of the system being measured. If the quantum state immediately before the measurement is  $|\psi\rangle$ , then the **probability that result  $m$  occurs** is

$$p(m) = \langle \psi | M_m^\dagger M_m | \psi \rangle, \quad \text{Probabilistic!}$$

and **the state after** the measurement is

$$\frac{M_m |\psi\rangle}{\sqrt{p(m)}}. \quad \text{Backaction!}$$

Since  $\sum_m p(m) = 1$ , the measurement operators must satisfy  $\sum_m M_m^\dagger M_m = I$ .

# Postulates of QM: Measurement

Example:  $M_0 = |0\rangle\langle 0|$ ,  $M_1 = |1\rangle\langle 1|$  **Measurement in the computational basis**

These are Hermitian and  $M_0^2 = M_0$ ,  $M_1^2 = M_1$ .  $\therefore M_0^\dagger M_0 + M_1^\dagger M_1 = I$

Suppose the state being measured is  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ .

The probability of obtaining 0:  $p(0) = \langle\psi|M_0^\dagger M_0|\psi\rangle = \langle\psi|0\rangle\langle 0|\psi\rangle = |\alpha|^2$

The state after obtaining 0:  $\frac{M_0|\psi\rangle}{|\alpha|} = \frac{\alpha}{|\alpha|}|0\rangle$  **Physically irrelevant Global phase**

Similarly,  $p(1) = \langle\psi|M_1^\dagger M_1|\psi\rangle = |\beta|^2$ , and the state after is  $\frac{M_1|\psi\rangle}{|\beta|} = \frac{\beta}{|\beta|}|1\rangle$



# Postulates of QM: Composite System

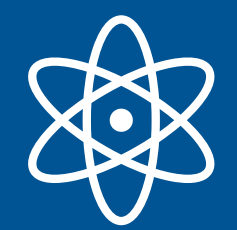
The state space of a composite physical system is the tensor product space  $\mathcal{H}_1 \otimes \dots \otimes \mathcal{H}_n$  of the state spaces of the component subsystems  $\mathcal{H}_1, \dots, \mathcal{H}_n$ .

**Example:**  $|\psi_1\rangle = \alpha_1|0\rangle + \beta_1|1\rangle \quad |\psi_2\rangle = \alpha_2|0\rangle + \beta_2|1\rangle$

**Concatenate:**

$$\alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle = \begin{pmatrix} \alpha_1\alpha_2 \\ \alpha_1\beta_2 \\ \beta_1\alpha_2 \\ \beta_1\beta_2 \end{pmatrix} = \begin{pmatrix} \alpha_1 \begin{pmatrix} \alpha_2 \\ \beta_2 \end{pmatrix} \\ \beta_1 \begin{pmatrix} \alpha_2 \\ \beta_2 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} \alpha_1 \\ \beta_1 \end{pmatrix} \otimes \begin{pmatrix} \alpha_2 \\ \beta_2 \end{pmatrix}$$

$$|\psi_1\rangle \otimes |\psi_2\rangle = (\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle)$$



# Entanglement

- Some composite quantum states cannot be written in the product form, i.e.  $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \dots \otimes |\psi_m\rangle$

Example:  $|\Phi_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$  cannot be written as  $|\psi_1\rangle \otimes |\psi_2\rangle$

- A quantum state that can be written in the product form is **separable**.
- A quantum state that is not separable is **entangled**.
- Entanglement describes correlations between quantum systems that cannot be described with classical physics.



# Composite system: Measurement

**General two-qubit state:**  $\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$ ,  $\sum |\alpha_{ij}|^2 = 1$

If we measure both bits, we get  $|ij\rangle$  with probability  $|\alpha_{ij}|^2$ .

What if we just measure one of them, e.g. the first qubit?

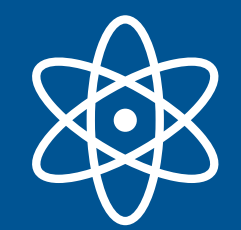
**Rewrite:** 
$$\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2} |0\rangle \left( \frac{\alpha_{00}|0\rangle + \alpha_{01}|1\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}} \right) + \sqrt{|\alpha_{10}|^2 + |\alpha_{11}|^2} |1\rangle \left( \frac{\alpha_{10}|0\rangle + \alpha_{11}|1\rangle}{\sqrt{|\alpha_{10}|^2 + |\alpha_{11}|^2}} \right)$$

What if we just throw away one of them, e.g. the first qubit?

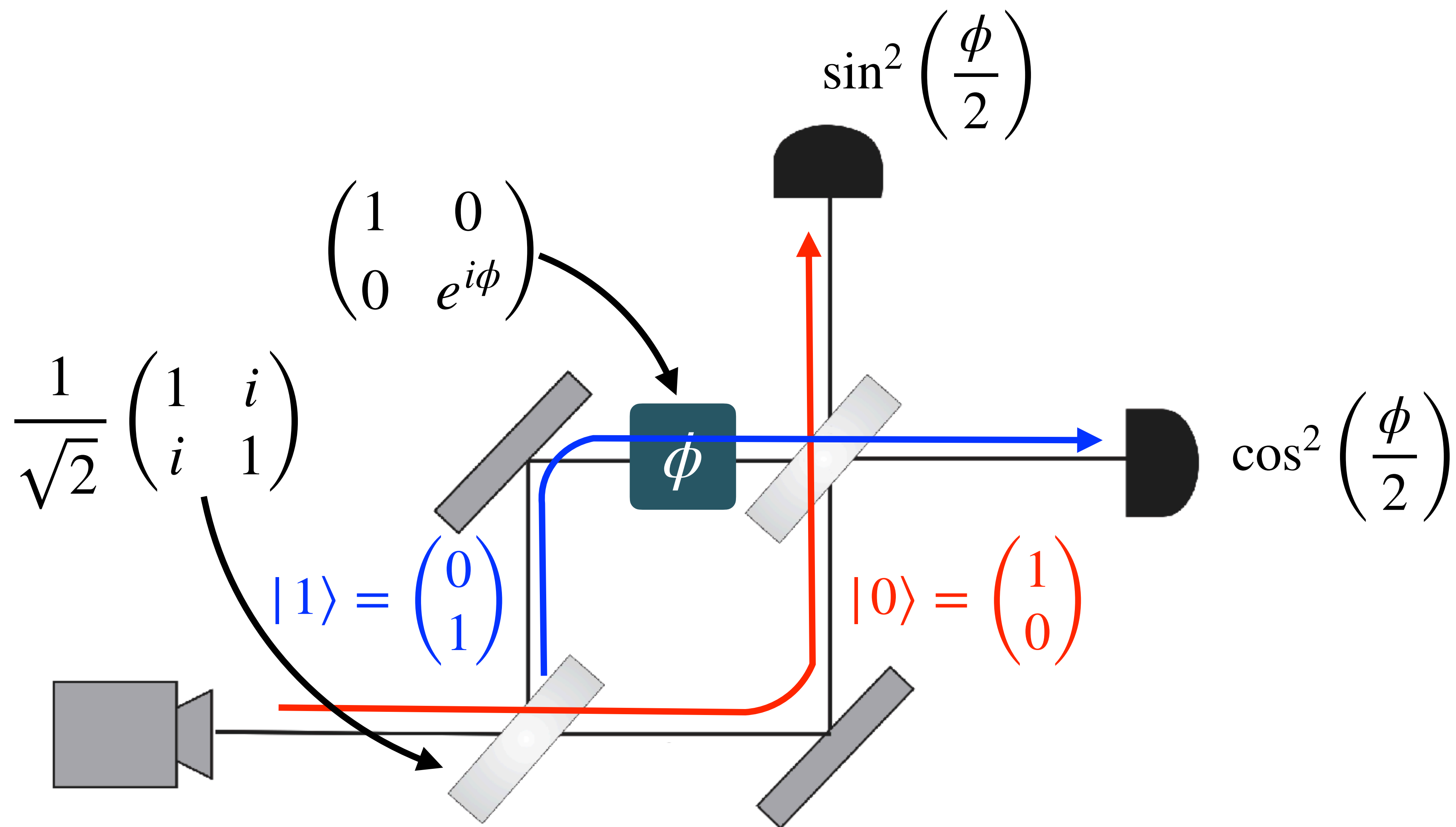
Probabilistic mixture of states  $\rightarrow$  Mixed State

**Example:**  $|\Phi_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$

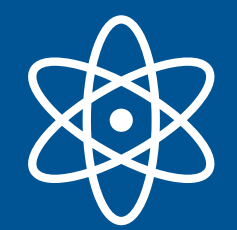
Throwing away one qubit leaves the other in a completely random state



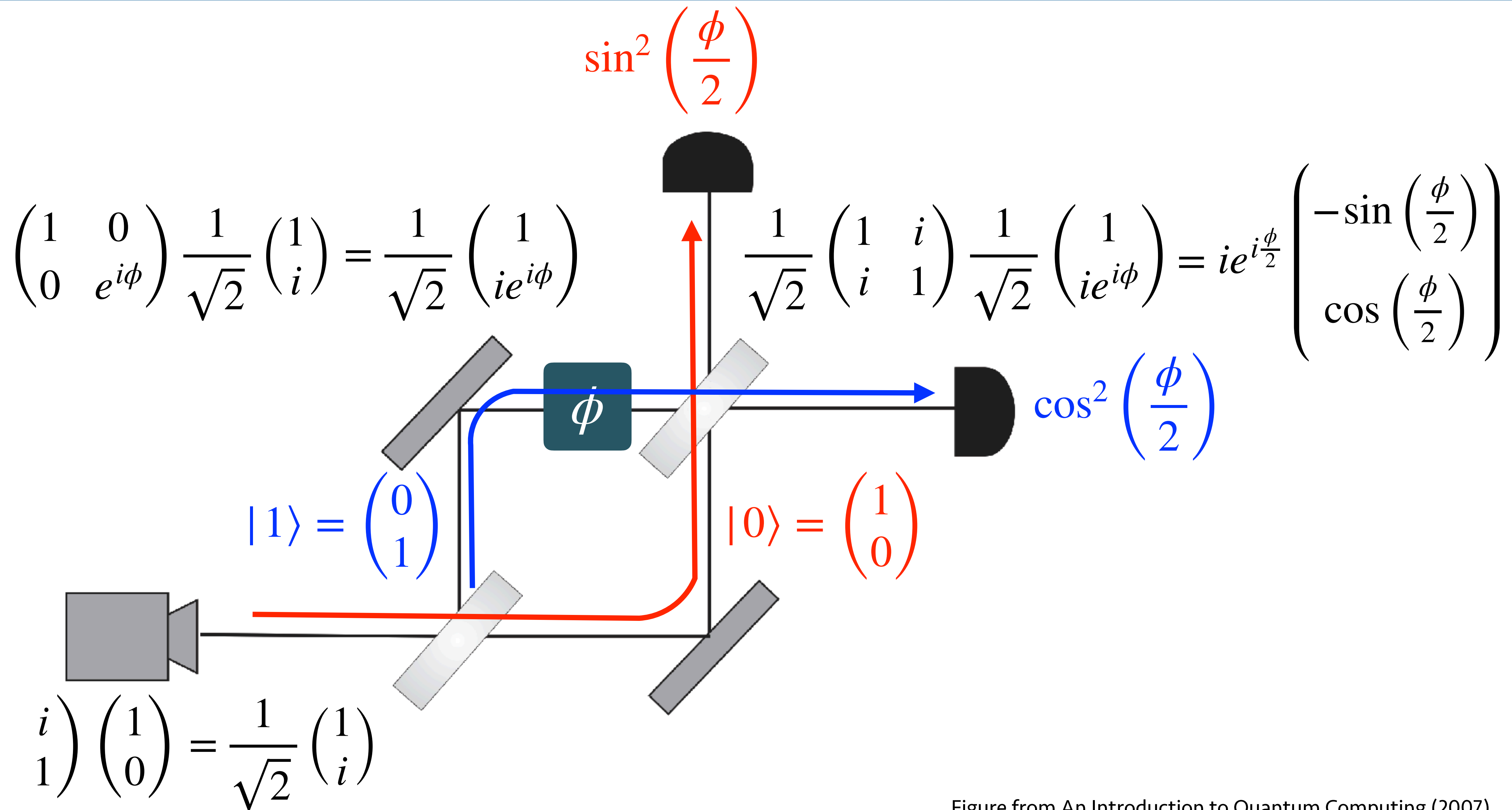
# Revisit Mach-Zehnder Interferometer

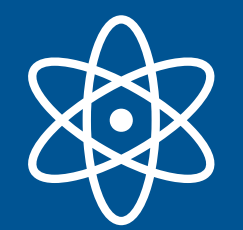






# Revisit Mach-Zehnder Interferometer



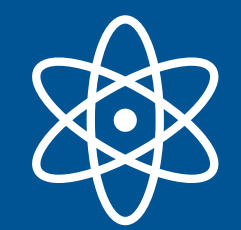


# Comparison to Classical Deterministic Bits

- The values of a two-state system are labeled with 0 or 1
- $n$  two-state systems have  $2^n$  possible values, labeled with binary strings. For example,  $n = 3$ : 000, 001, 010, 011, 100, 101, 110, 111.
- More redundant representation:

$$\underbrace{000\dots0}_n = \left( \begin{array}{c} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{array} \right) \left. \vphantom{\begin{array}{c} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{array}} \right\} 2^n \quad 000\dots1 = \left( \begin{array}{c} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{array} \right) \quad \dots \quad 11\dots10 = \left( \begin{array}{c} 0 \\ 0 \\ \vdots \\ 1 \\ 0 \end{array} \right) \quad 11\dots11 = \left( \begin{array}{c} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{array} \right)$$





# Comparison to Classical Probabilistic Bits

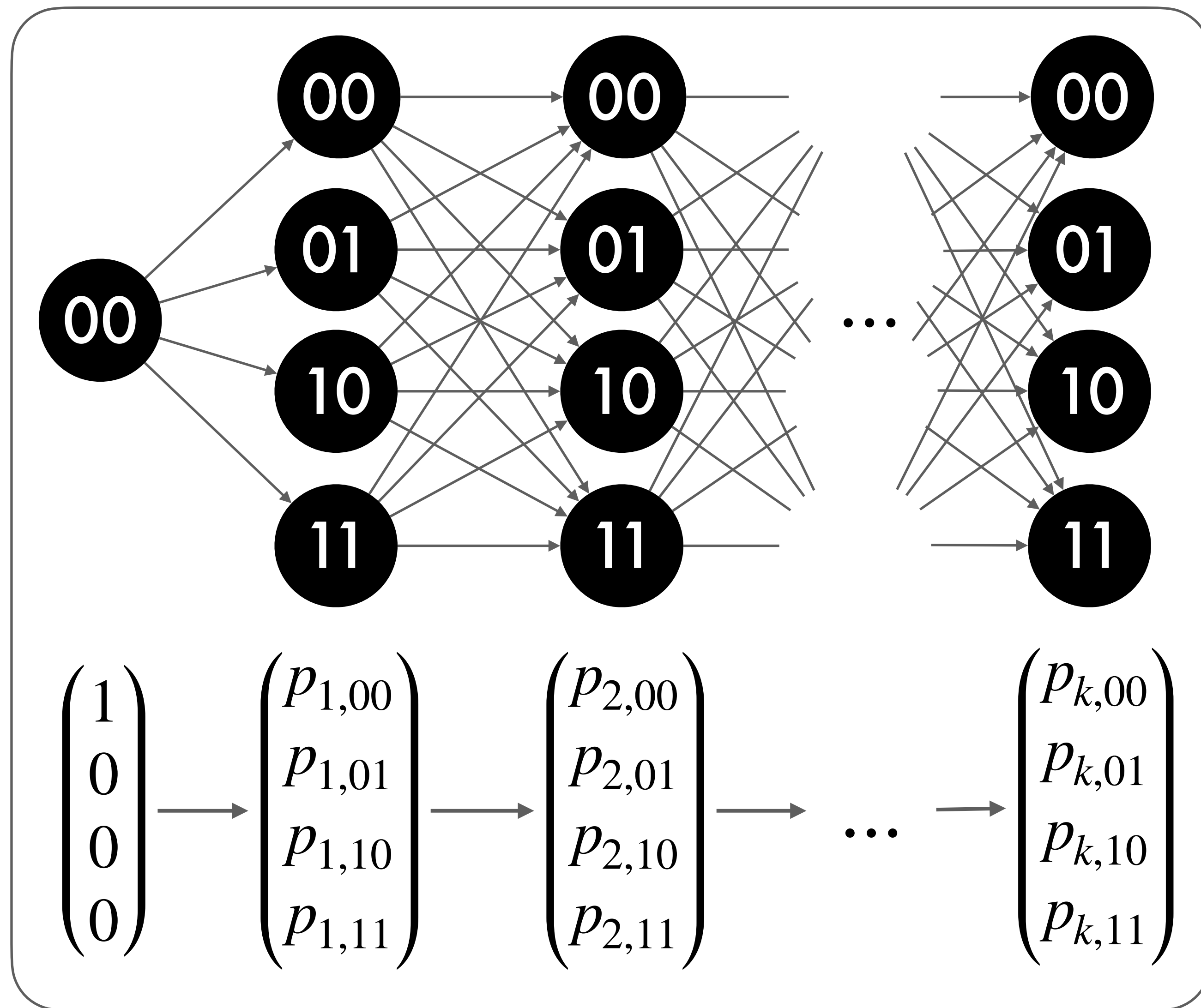
## Example: 2 bits

1st bit:  $\begin{pmatrix} \text{Pr}(0) \\ \text{Pr}(1) \end{pmatrix} = \begin{pmatrix} p_0 \\ p_1 \end{pmatrix}$

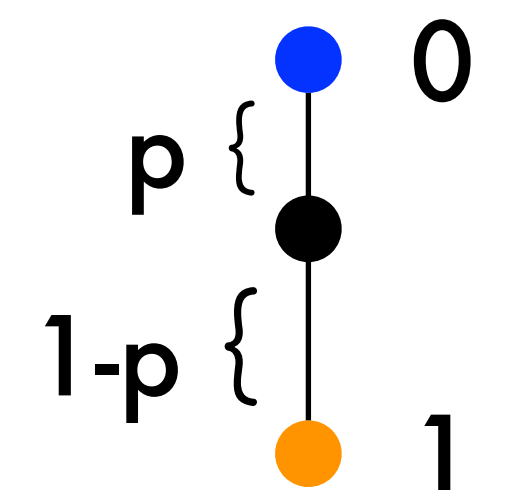
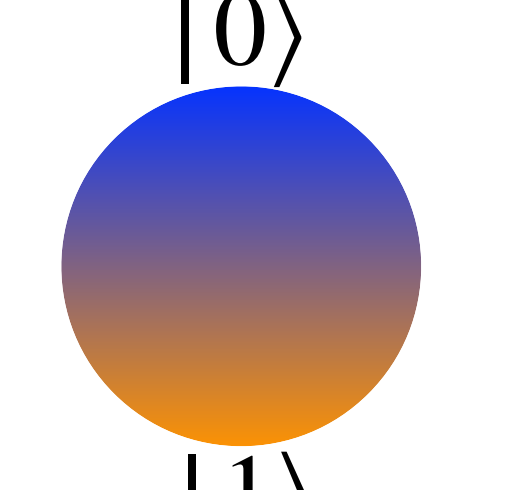
2nd bit:  $\begin{pmatrix} \text{Pr}(0) \\ \text{Pr}(1) \end{pmatrix} = \begin{pmatrix} q_0 \\ q_1 \end{pmatrix}$



$$\begin{pmatrix} \text{Pr}(00) \\ \text{Pr}(01) \\ \text{Pr}(10) \\ \text{Pr}(11) \end{pmatrix} = \begin{pmatrix} p_0 q_0 \\ p_0 q_1 \\ p_1 q_0 \\ p_1 q_1 \end{pmatrix} = \begin{pmatrix} p_0 \\ p_1 \end{pmatrix} \otimes \begin{pmatrix} q_0 \\ q_1 \end{pmatrix}$$



# Summary: Bit, Pbit, Qubit

	bit	probabilistic bit	quantum bit
Pictorial Representation	<div><div>● 0</div><div>● 1</div></div>		
Vector Representation	$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$	$\begin{pmatrix} p \\ 1 - p \end{pmatrix}, p \in \mathbb{R}$	$\begin{pmatrix} \alpha \\ \beta \end{pmatrix}, \alpha, \beta \in \mathbb{C}$
Observation	0	$\Pr(0) = p$ $\Pr(1) = 1 - p$	$\Pr(0) =  \alpha ^2$ $\Pr(1) =  \beta ^2$
Evolution	Deterministic	Stochastic	Unitary

Quantum mechanics: a mathematical generalization of the probability theory



# Quantum Mechanics for Computing

1 qubit

$\alpha_1 |0\rangle$

$\alpha_2 |1\rangle$

2 qubits

$\alpha_1 |00\rangle$

$\alpha_2 |01\rangle$

$\alpha_3 |10\rangle$

$\alpha_4 |11\rangle$

3 qubits

$\alpha_1 |000\rangle \quad \alpha_2 |001\rangle \quad \alpha_3 |010\rangle \quad \alpha_4 |011\rangle \quad \alpha_5 |100\rangle \quad \alpha_6 |101\rangle \quad \alpha_7 |110\rangle \quad \alpha_8 |111\rangle$

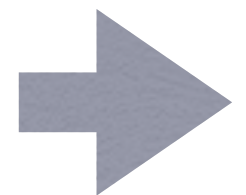
$\vdots$

$\vdots$

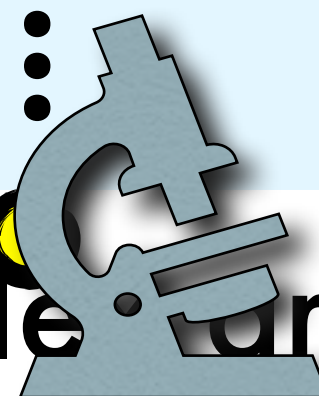
$\vdots$

$\vdots$

70 qubits



Process  $\sim 10^9$  amplitudes in parallel



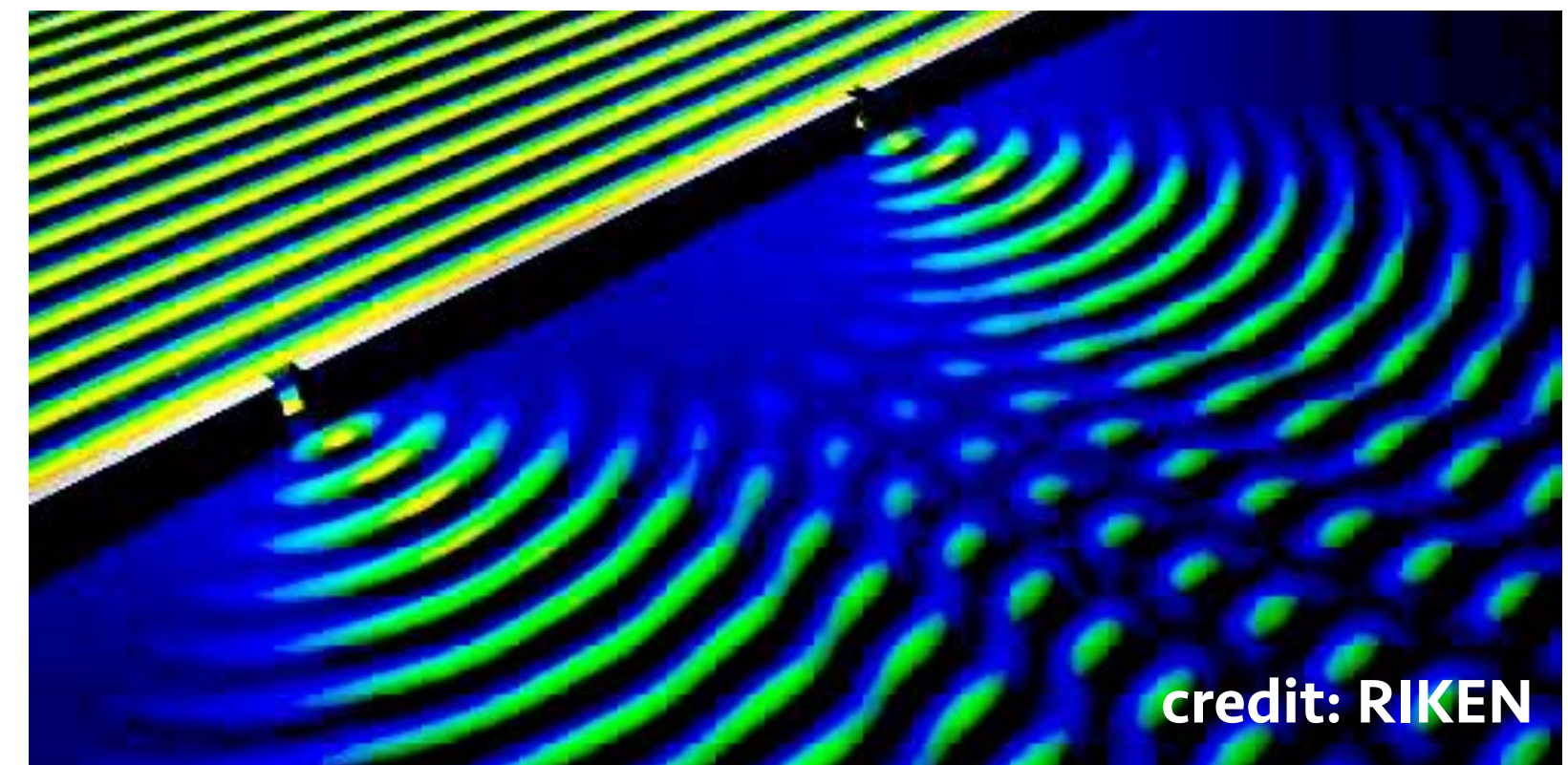
$\rightarrow \sim 10^9$  terabytes

But there is an enemy...

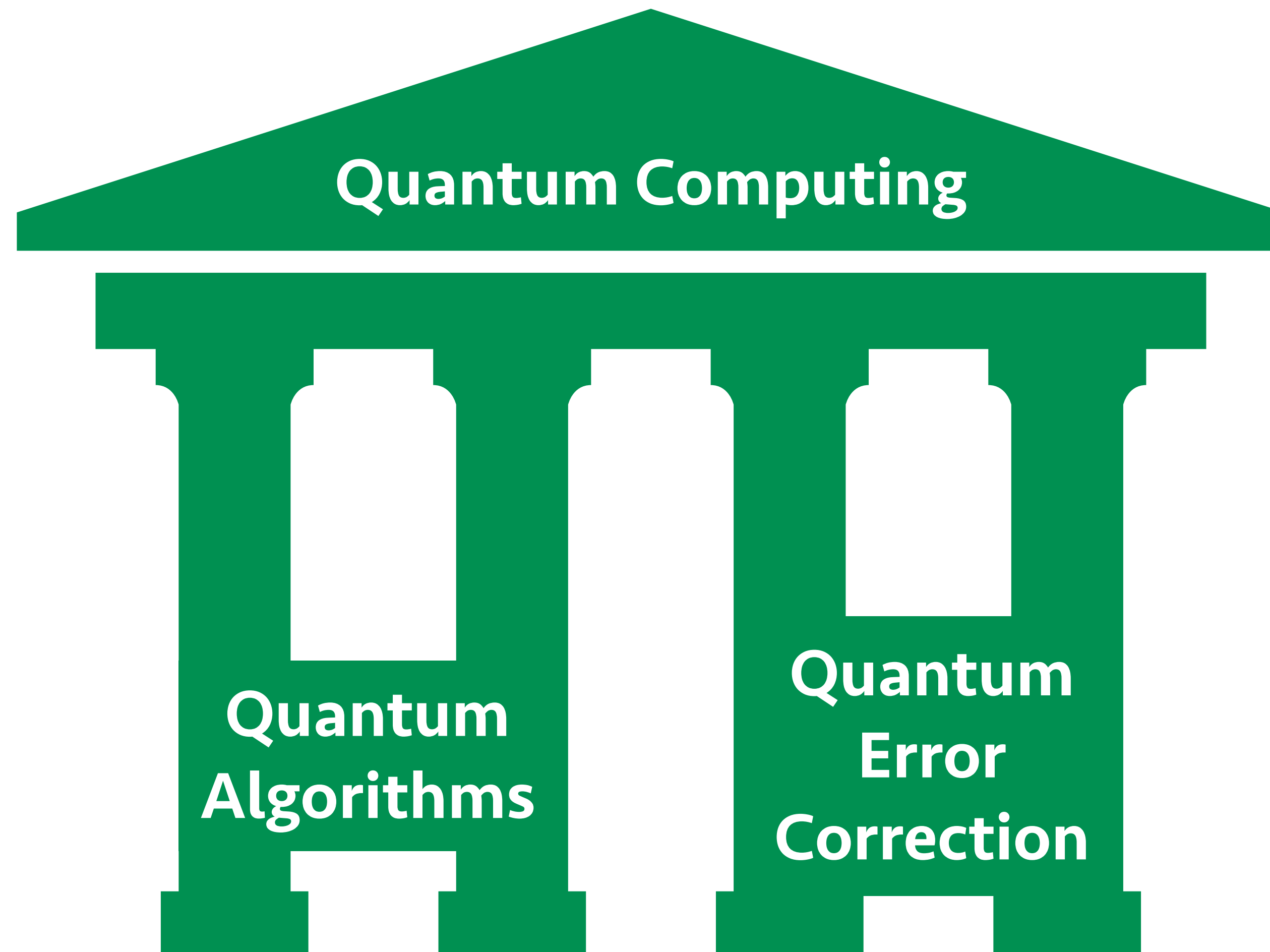
Measurement destroys quantum superposition!



**SOLUTION:** Quantum Interference!



# Theoretical Pillars for Quantum Computing



# Theoretical Pillars for Quantum Computing

Exponential or polynomial speed-up for some computational tasks, such as:

- Integer Factoring
- Solving a system of linear equations
- Finding eigenvectors and eigenvalues
- Support vector machine
- Principal component analysis

⋮



Quantum  
Error  
Correction



# Theoretical Pillars for Quantum Computing

Exponential or polynomial speed-up for some computational tasks, such as:

- Integer Factoring
- Solving a system of linear equations
- Finding eigenvectors and eigenvalues
- Support vector machine
- Principal component analysis

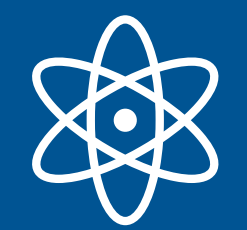
⋮



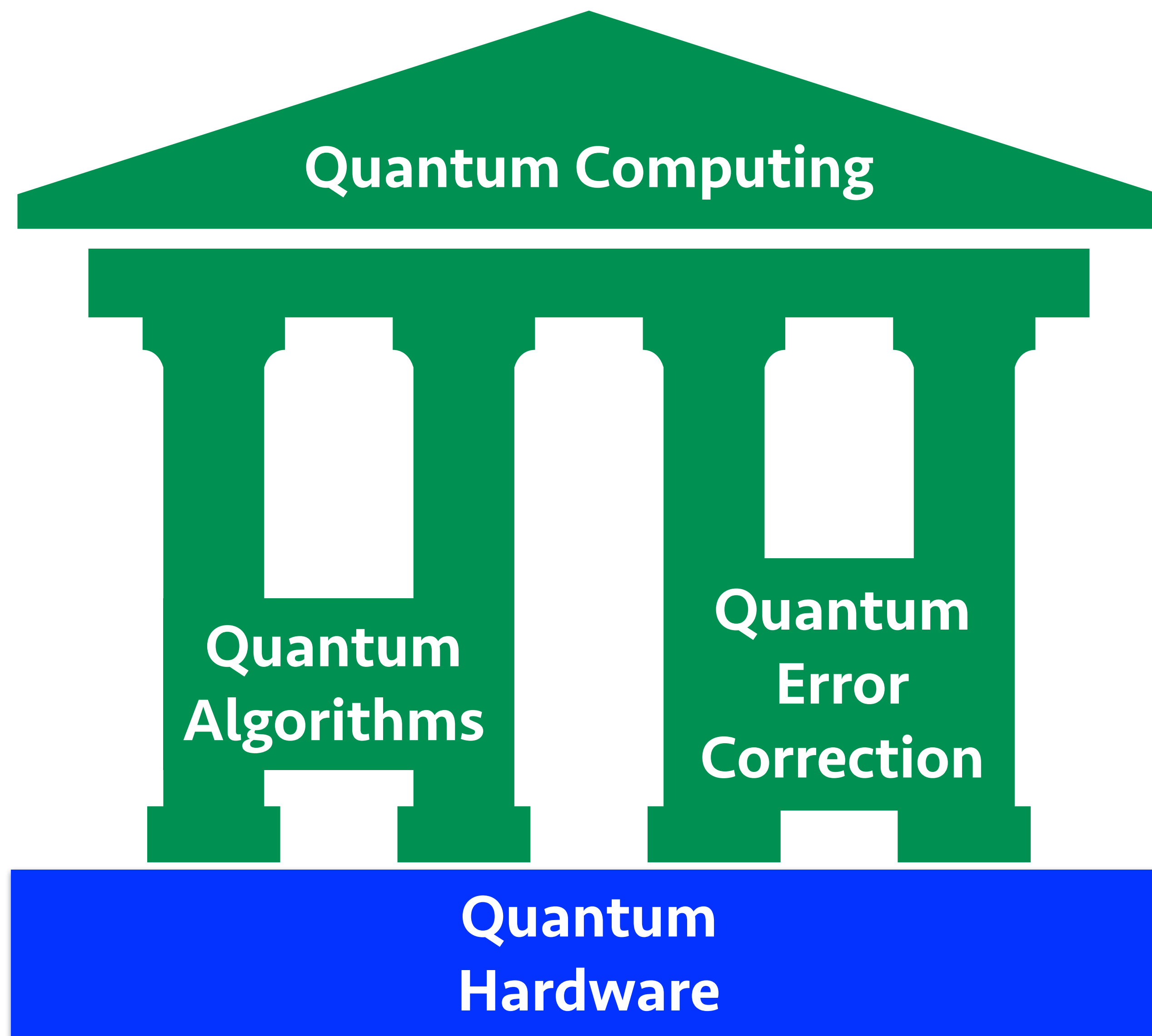
Quantum  
Algorithms

Quantum  
Error  
Correction

Imperfections are not the fundamental  
objections to quantum computation



# Theoretical Pillars for Quantum Computing



# Quantum Hardware Roadmap

