

# A Taste of Theoretical Quantum Computing

## CMSC5719 Seminar (2026 Fall)

---

Xiao Liang

 <https://xiao-liang.github.io>

Department of Computer Science and Engineering  
The Chinese University of Hong Kong

# What Is Quantum Computing? — From Newton to Schrödinger

# Core Idea: Computing Follows Physics

- Our computational power is bounded—and enabled—by our understanding of physics.
- Different physical laws suggest different ways to represent and process information.
- We will travel from classical mechanics (Newton) to electromagnetism (Maxwell) to quantum mechanics (Schrödinger).

# Era I: Classical Mechanics and Mechanical Computing

Governing law for classical mechanics: Newton's second law

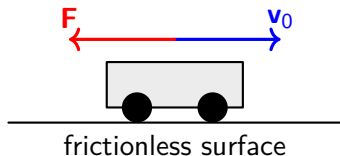
$$\mathbf{F} = m \cdot \mathbf{a} = \frac{d\mathbf{p}}{dt}$$

- **F**: Force vector. The net force acting on an object (magnitude and direction).
- **m**: Mass (scalar). A measure of an object's inertia; how much it resists changes in motion.
- **a**: Acceleration vector. The time rate of change of velocity:  $\mathbf{a} = \frac{d\mathbf{v}}{dt}$ .
- **p**: Momentum vector. Defined as  $\mathbf{p} = m\mathbf{v}$  for a particle with constant mass  $m$  and velocity  $\mathbf{v}$ .
- $\frac{d\mathbf{p}}{dt}$ : Time derivative of momentum. How momentum changes with time; equals the net force.

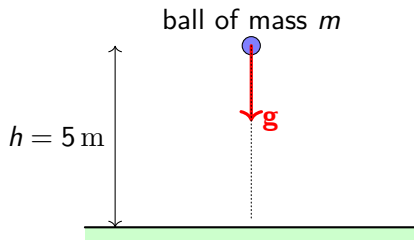
Governing law for classical mechanics: Newton's second law

$$\mathbf{F} = m \cdot \mathbf{a} = \frac{d\mathbf{p}}{dt}$$

Exemplary systems we can solve:



(a) Cart on a frictionless surface



(b) Ball dropped from height

If we can build gears, levers, and pulleys, we can compute with them.

# Mechanical Computing Devices: Abacus

Abacus:

- rods with beads represent digits;
- compute by moving beads according to rules.

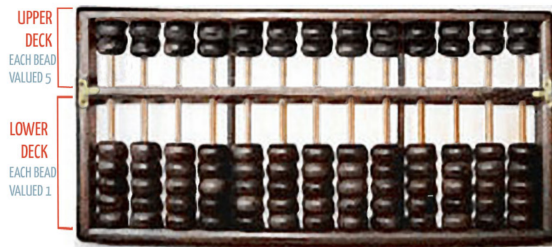
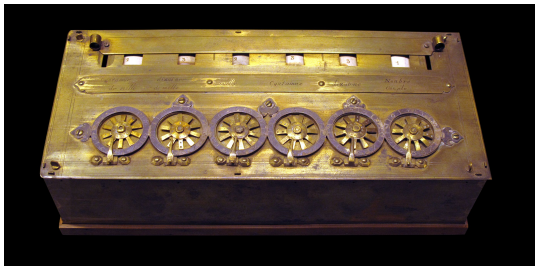


Figure: Abacus

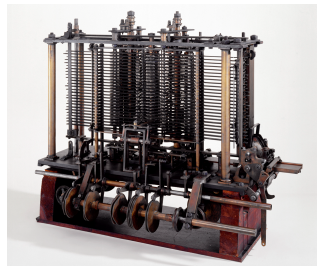
# Mechanical Computing Devices: Gear calculators

Gear calculators (e.g., Pascaline, Babbage's analytical engine ):

- gear positions encode numbers;
- addition/subtraction via gear rotations and carries.



(a) Pascaline



(b) Babbage's analytical engine

## Era II: Electromagnetism and Electronic Computing

Governing laws: Maxwell's equations (unifying electricity and magnetism):

$$\nabla \cdot \mathbf{E} = \frac{\rho}{\epsilon_0} \quad (\text{Gauss's law})$$

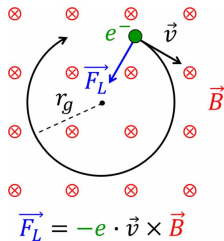
$$\nabla \cdot \mathbf{B} = 0 \quad (\text{Gauss's law for magnetism})$$

$$\nabla \times \mathbf{E} = -\frac{\partial \mathbf{B}}{\partial t} \quad (\text{Faraday's law})$$

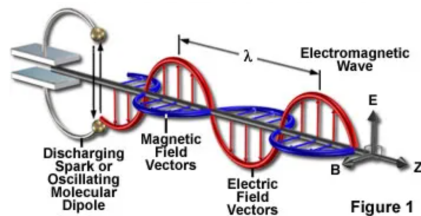
$$\nabla \times \mathbf{B} = \mu_0 \mathbf{J} + \mu_0 \epsilon_0 \frac{\partial \mathbf{E}}{\partial t} \quad (\text{Ampère–Maxwell law})$$

Where  $\mathbf{E}$  is the electric field,  $\mathbf{B}$  is the magnetic field,  $\rho$  is the electric charge density,  $\mathbf{J}$  is the current density,  $\epsilon_0$  is the vacuum permittivity, and  $\mu_0$  is the vacuum permeability.

## Exemplary systems we can solve using Maxwell's equations:



(a) An electron in a magnetic field



(b) Propagation of an electromagnetic wave

If we can harness fields and waves (wires, antennas, circuits), we can compute with electrons and light.

# Electronic Computing Devices

State-of-the-art devices: calculators, desktops, smartphones, cloud servers.

Encoding:

- Bits as high/low voltage levels.
- Wires carry bits; memory stores them as charge states or magnetic domains.

Computing:

- Logic gates (AND, OR, NOT, NAND, etc.) built from transistors implement Boolean functions.
- Synchronous circuits orchestrated by clocks compose gates into processors.
- Algorithms = sequences of logic operations on registers of bits.

# Mechanical Computing vs Electronic Computing

Mechanical calculators are great for a few coupled motions (gears, cams, analog integrators). They struggle when a task needs:

- exploring an enormous number of possibilities,
- processing very large datasets with high precision,
- running millions to billions of steps quickly,
- flexible memory and branching logic.

Electronics handle these via fast arithmetic, memory, and massive parallelism. E.g.,

- High-Dimensional PDEs and Large-Scale Simulation
- Large-Scale Linear Algebra and Optimization
- Symbolic Computation and Automated Reasoning
- Data-Intensive Analytics

# Era III: Quantum Mechanics and Quantum Computing

## A New Revolution: **Quantum Mechanics**

- At microscopic scales, classical laws fail to explain experiments.
- Quantum mechanics provides new rules for how systems evolve and how measurements behave.

## **Concrete examples:**

- Atoms and molecules (about 0.1–1 nanometer): Explains why elements have colors and why chemicals bond.
- Tunneling through thin barriers (a few nanometers): Used in flash memory and scanning tunneling microscopes.
- Quantum dots (1–10 nanometers): Tiny crystals that glow different colors in modern TV screens.

# Shrödinger's Equation

Quantum Mechanics is ruled by Shrödinger's equation

$$i\hbar \frac{\partial}{\partial t} |\psi(t)\rangle = \hat{H} |\psi(t)\rangle$$

where

- $i$ : the imaginary root  $i := \sqrt{-1}$ ; (we'll discuss more on why complex numbers are necessary later)
- $\hbar$ : Planck's reduced constant<sup>1</sup>. You just need to know that it is some physics constant of the magnitude  $\approx 1.055 \times 10^{-34} J \cdot s$ .
- $|\psi(t)\rangle$ : It's a vector (more discussion later)
- $\hat{H}$ : It's a matrix (more discussion later)

---

<sup>1</sup>This is named after the renowned physicist [Max Planck](#), recipient of the Nobel Prize in Physics in 1918.

## An Inaccurate-yet-Helpful Analogy (1/3)

We don't need a fully rigorous understanding of this equation—this isn't a quantum mechanics course. But it helps to have an intuitive feel for it. We'll build that intuition by drawing an analogy with classical mechanics.

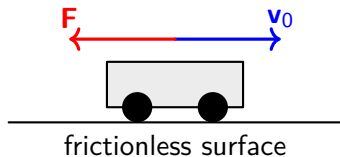


Figure: Cart on a frictionless surface

- You have a cart, an initial speed  $v_0$ , and a force  $F$  acting.
- If you know the setup, you can predict **where the cart will be** at time  $t$ .
- In short: knowing the rule  $\mathbf{F} = m \cdot \mathbf{a}$  and the starting point lets us predict motion.

## An Inaccurate-yet-Helpful Analogy (2/3)

We can use Schrödinger's equation (instead of Newton's) to solve the system as well:

$$i\hbar \frac{\partial}{\partial t} |\psi(t)\rangle = \hat{H} |\psi(t)\rangle$$

- $|\psi(t)\rangle$ : think of this as a **vector** that describes the system's overall state at time  $t$ .
- $\hat{H}$  (Hamiltonian): think of this as a **big rule-book or matrix** encoding how the system behaves (energies, forces, boundaries).
- The equation says: **change in the system's state over time** is determined by **the rule-book acting on the state**.

## An Inaccurate-yet-Helpful Analogy (3/3)

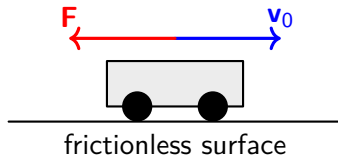


Figure: Cart on a frictionless surface

In more details:

- $|\psi(t)\rangle$ : Think it as “where/what the system is like right now.” It’s like a vector you update over time.
- $\hat{H}$ : Think it as “all the ingredients of the system”—mass, potential energy, constraints, fields, etc. It acts like a matrix that “pushes” the system’s state forward in time.
- $i\hbar \frac{\partial}{\partial t}$ : It reads as “how fast the state changes with time,” scaled by a constant  $i$  times  $\hbar$ .

# Today's Agenda

Our goal is to understand how the Schrödinger equation enables us to:

- encode information, and
- perform computation.

In particular:

- ① Schrödinger equation  $\Rightarrow$  4 math postulates
- ② 4 math postulates  $\Rightarrow$  quantum computing
- ③ Unique quantum phenomena:
  - No-Cloning Theorem;
  - Elitzur–Vaidman bomb tester
- ④ Some discussion on the interpretation of quantum mechanics (i.e., the four postulates)

## The 4 Postulates (simplified)

## Postulate 1: A qubit is a unit vector

A qubit state is a **unit vector** in  $\mathbb{C}^2$ :

$$\text{state} = a_0 \cdot \mathbf{e}_0 + a_1 \cdot \mathbf{e}_1, \quad |a_0|^2 + |a_1|^2 = 1.$$

Here,

$$\mathbf{e}_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad \mathbf{e}_1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad a_0, a_1 \in \mathbb{C}.$$

## Postulate 1: A qubit is a unit vector

A qubit state is a **unit vector** in  $\mathbb{C}^2$ :

$$\text{state} = a_0 \cdot \mathbf{e}_0 + a_1 \cdot \mathbf{e}_1, \quad |a_0|^2 + |a_1|^2 = 1.$$

Here,

$$\mathbf{e}_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad \mathbf{e}_1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad a_0, a_1 \in \mathbb{C}.$$

We use **Dirac notation**:

$$|0\rangle = \mathbf{e}_0, \quad |1\rangle = \mathbf{e}_1.$$

Thus, we can write the same state as

$$|\psi\rangle = a_0 |0\rangle + a_1 |1\rangle.$$

### Intuition

A qubit is described by two complex coefficients, called **amplitudes**, whose squared magnitudes sum to 1.

## The notation is just linear algebra

If

$$|\psi\rangle = \begin{pmatrix} a_0 \\ a_1 \end{pmatrix},$$

then its conjugate transpose is

$$\langle\psi| = (a_0^* \ a_1^*).$$

For another vector  $|\phi\rangle = b_0 |0\rangle + b_1 |1\rangle$ , the inner product is

$$\langle\psi|\phi\rangle = a_0^* b_0 + a_1^* b_1.$$

In particular,

$$\langle\psi|\psi\rangle = |a_0|^2 + |a_1|^2 = 1.$$

The same notation works in larger spaces

In a  $d$ -dimensional space, write

$$|k\rangle = \mathbf{e}_k, \quad k \in \{0, 1, \dots, d-1\}.$$

# From a classical bit to a qubit

## A classical one-bit register

A classical computer stores a bit with value

0      or      1.

These are the two possible states of a one-bit register.

# From a classical bit to a qubit

## A classical one-bit register

A classical computer stores a bit with value

0 or 1.

These are the two possible states of a one-bit register.

## The quantum analogue

A one-qubit register has two corresponding **computational basis states**:

classical 0  $\longleftrightarrow$   $|0\rangle$ ,      classical 1  $\longleftrightarrow$   $|1\rangle$ .

Thus,  $|0\rangle$  and  $|1\rangle$  represent the quantum versions of storing a definite classical bit.

# What is new?

A qubit can also be in a **superposition**

$$|\psi\rangle = a_0 |0\rangle + a_1 |1\rangle, \quad |a_0|^2 + |a_1|^2 = 1.$$

This is not another classical bit value: the coefficients are amplitudes, not stored classical bits.

## Postulate 2: Put registers together

Putting two qubits together gives a new space with **four basis vectors**:

$$|00\rangle, \quad |01\rangle, \quad |10\rangle, \quad |11\rangle.$$

The labels record the basis value of each qubit.

In this order, a joint state is a unit vector in  $\mathbb{C}^4$ :

$$|\psi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle,$$

where

$$|a_{00}|^2 + |a_{01}|^2 + |a_{10}|^2 + |a_{11}|^2 = 1.$$

## Postulate 2: More possibilities

This idea extends to  $n$  qubits

With  $n$  qubits, there are  $2^n$  basis labels:

$$|00 \cdots 0\rangle, \quad |00 \cdots 1\rangle, \quad \dots, \quad |11 \cdots 1\rangle.$$

Any **unit** vector in  $\mathbb{C}^{2^n}$  is valid  **$n$ -qubit** state.

Importantly, this allows us to encode data!

Remark: We are skipping the formal construction

Mathematically, combining these spaces uses a **tensor product**. Our basis-label explanation is informal; we will not develop tensor products or formal separability criteria due to the time limit.

## Postulate 3: Evolution uses unitary matrices

Between measurements, an ideal isolated quantum state evolves as

$$|\psi\rangle \longrightarrow U|\psi\rangle,$$

where  $U$  is a **unitary matrix**.

A unitary matrix is a square complex matrix satisfying

$$UU^\dagger = U^\dagger U = I.$$

Equivalently,

$$U^{-1} = U^\dagger.$$

## Postulate 3: These are our rules for manipulating data

Classically, we manipulate data using operations such as addition, multiplication, and division. In our simplified quantum model:

Manipulate the state using unitary matrices.

- We cannot arbitrarily overwrite or duplicate amplitudes.
- Measurement is a separate operation: it is described by Postulate 4.

## Postulate 4: Measurement gives an outcome I

Suppose the state is

$$|\psi\rangle = a_0 |0\rangle + a_1 |1\rangle + \cdots + a_{2^n-1} |2^n - 1\rangle.$$

Measuring in this basis gives outcome  $k$  with probability

$$\Pr[k] = |a_k|^2, \quad k \in \{0, 1, \dots, 2^n - 1\}.$$

After observing  $k$ , the state “collapses” to

$$|k\rangle.$$

Remember both parts

Measurement produces a classical outcome and changes the quantum state.

## Postulate 4: Measurement gives an outcome II

Why normalization matters

The probabilities sum to 1:

$$\sum_{k=0}^{2^n-1} |a_k|^2 = 1.$$

## Postulate 4: Two examples

### One qubit

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}.$$

- Outcome 0: probability 1/2; state becomes  $|0\rangle$ .
- Outcome 1: probability 1/2; state becomes  $|1\rangle$ .

### Two qubits

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

Measuring both qubits:

- Outcome 00: probability 1/2.
- Outcome 11: probability 1/2.
- Outcomes 01 and 10: probability 0.

## Quiz: Apply the rules

Suppose

$$|\psi\rangle = \frac{1}{\sqrt{3}}|0\rangle + \sqrt{\frac{2}{3}}|1\rangle.$$

- 1 Is this a valid state?
- 2 What are the measurement probabilities?
- 3 What is the state after observing 0?

## No-Cloning Theorem

# Can we copy a qubit?

Classically, copying a bit means

$$(b, 0) \longmapsto (b, b).$$

Can we do the same thing for a qubit? That is,

$$(|\psi\rangle, |0\rangle) \longmapsto (|\psi\rangle, |\psi\rangle).$$

## A Surprising Answer

No! **No-cloning theorem**: There is no (universal) copying algorithm for qubits.

## Combining independently prepared states

Before discussing copying, we need one simple notation rule.

If we independently prepare

$$|\psi\rangle = a_0 |0\rangle + a_1 |1\rangle, \quad |\phi\rangle = b_0 |0\rangle + b_1 |1\rangle,$$

we write their joint state as  $|\psi\rangle |\phi\rangle$ .

It is defined by multiplying coefficients:

$$\begin{aligned} |\psi\rangle |\phi\rangle &= (a_0 |0\rangle + a_1 |1\rangle)(b_0 |0\rangle + b_1 |1\rangle) \\ &= a_0 b_0 |00\rangle + a_0 b_1 |01\rangle + a_1 b_0 |10\rangle + a_1 b_1 |11\rangle. \end{aligned}$$

### Remark

This is an implication of Postulate 2, the **tensor product** that we omitted earlier.

# The no-cloning theorem

## No universal perfect copying machine

There is no single unitary operation  $U$  that satisfies

$$U(|\psi\rangle |0\rangle) = |\psi\rangle |\psi\rangle$$

for **every** qubit state  $|\psi\rangle$ .

## Why might copying fail?

A matrix acts linearly:

$$U(a|v\rangle + b|w\rangle) = aU|v\rangle + bU|w\rangle.$$

# Proof of the No-Cloning Theorem I

Let us first recall the following special qubit

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}.$$

If we put  $|+\rangle$  adjacent to  $|0\rangle$ , we have

$$|+\rangle |0\rangle = \frac{|00\rangle + |10\rangle}{\sqrt{2}}.$$

If we put  $|+\rangle$  adjacent to itself, we have

$$|+\rangle |+\rangle = \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2}.$$

## Proof of the No-Cloning Theorem II

Suppose  $U$  copies every qubit state. Then

$$U(|0\rangle |0\rangle) = |00\rangle, \quad U(|1\rangle |0\rangle) = |11\rangle.$$

By linearity,

$$U(|+\rangle |0\rangle) = U\left(\frac{|00\rangle + |10\rangle}{\sqrt{2}}\right) = \frac{U|00\rangle + U|10\rangle}{\sqrt{2}} = \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

However, from the last slide

$$|+\rangle |+\rangle = \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2}.$$

### Contradiction

These vectors are different. Therefore, the proposed universal copier cannot exist.

## Elitzur–Vaidman Bomb Tester

## The setup: An unattended suitcase

Imagine an unattended suitcase at an airport. You may send a bit  $b \in \{0, 1\}$  into its input wire.



There are two possible kinds of suitcase:

### An innocent suitcase

There is no bomb.

The suitcase simply forwards the input:

$$b \mapsto b.$$

### A malicious suitcase

A meter reads the input:

- If  $b = 0$ , return 0.
- If  $b = 1$ , trigger the bomb.

Explosion means **game over**.

## Why classical queries cannot solve this safely

| Query | Innocent suitcase | Malicious suitcase |
|-------|-------------------|--------------------|
| 0     | Return 0          | Return 0           |
| 1     | Return 1          | Explosion          |

### Querying with 0

This is safe, but the two suitcases behave identically. We learn nothing about whether a bomb is present.

### Querying with 1

This distinguishes the two possibilities, but triggers the bomb if one is present.

# The quantum game: Send a qubit instead

Now we may send a qubit

$$|\psi\rangle = a_0 |0\rangle + a_1 |1\rangle, \quad |a_0|^2 + |a_1|^2 = 1.$$

## An innocent suitcase

The suitcase returns the qubit unchanged:

$$|\psi\rangle \mapsto |\psi\rangle.$$

No measurement occurs.

## A malicious suitcase

The meter measures in the basis  $\{|0\rangle, |1\rangle\}$ :

- Outcome 0: no explosion; return the post-measurement state  $|0\rangle$ .
- Outcome 1: trigger the bomb. Game over.

## Check the rules: What happens to this query?

Suppose we send

$$|\psi\rangle = \frac{1}{\sqrt{3}}|0\rangle + \frac{\sqrt{2}}{\sqrt{3}}|1\rangle.$$

### Your turn

For each kind of suitcase:

- 1 What can happen?
- 2 What is the probability of each possibility?
- 3 What state is returned if there is no explosion?

## Check the rules: What happens to this query?

Suppose we send

$$|\psi\rangle = \frac{1}{\sqrt{3}}|0\rangle + \frac{\sqrt{2}}{\sqrt{3}}|1\rangle.$$

### Your turn

For each kind of suitcase:

- 1 What can happen?
- 2 What is the probability of each possibility?
- 3 What state is returned if there is no explosion?

### Malicious suitcase

$$\Pr[\text{survive}] = \frac{1}{3}, \quad \Pr[\text{explode}] = \frac{2}{3}.$$

On survival, the returned state is  $|0\rangle$ .

## Our tool: A small quantum rotation

Consider the matrix

$$R_\epsilon = \begin{pmatrix} \cos \epsilon & -\sin \epsilon \\ \sin \epsilon & \cos \epsilon \end{pmatrix}.$$

- For real coordinate vectors, it rotates counterclockwise by angle  $\epsilon$ .
- It is unitary:

$$R_\epsilon^\dagger R_\epsilon = I.$$

- Therefore, Postulate 3 allows us to apply it to a quantum state.

In particular,

$$R_\epsilon |0\rangle = \cos \epsilon |0\rangle + \sin \epsilon |1\rangle.$$

### Intuition

A small rotation creates a small amplitude on  $|1\rangle$ .

# The idea: Many small rotations

Start with  $|0\rangle$ .

- 1 Rotate the state by a small angle.
- 2 Send the state into the suitcase.
- 3 Repeat.

If there is no bomb

Nothing measures the state.

The small rotations can accumulate until the state reaches  $|1\rangle$ .

If there is a bomb

Each query measures the state.

Whenever we survive, the state returns to  $|0\rangle$ .  
The rotations do not accumulate.

The tradeoff

Each query carries a small risk. Can the **total** risk also be made small?

Parameters: Make the total angle approximately  $\pi/2$

Fix a small angle  $\epsilon \in (0, 1]$ . For example,  $\epsilon = 0.0001$ .

Set

$$T = \left\lceil \frac{\pi}{2\epsilon} \right\rceil.$$

So

$$T\epsilon \approx \frac{\pi}{2}.$$

A simplifying assumption

For the rest of the discussion, we simply assume

$$T\epsilon = \frac{\pi}{2}.$$

There are ways to correct this small rounding error, but we will not bother with them here.

# The Elitzur–Vaidman testing algorithm

## Parameters

Choose  $\epsilon \in (0, 1]$ , and set

$$T = \left\lceil \frac{\pi}{2\epsilon} \right\rceil.$$

We assume  $T\epsilon = \pi/2$ , ignoring the small rounding error.

## Algorithm

- ① Initialize the current state to  $|0\rangle$ .
- ② For rounds  $i = 1, \dots, T$ :
  - Apply  $R_\epsilon$ .
  - Query the suitcase with the resulting state.
  - If it explodes, stop. Otherwise, keep the returned state.
- ③ If still alive, measure in  $\{|0\rangle, |1\rangle\}$ :
  - Outcome 1: report “no bomb.”
  - Outcome 0: report “live bomb.”

## No bomb: The rotations accumulate

An innocent suitcase does not change the state.

After  $i$  rounds,

$$|\psi_i\rangle = R_\epsilon^i |0\rangle = \cos(i\epsilon) |0\rangle + \sin(i\epsilon) |1\rangle.$$

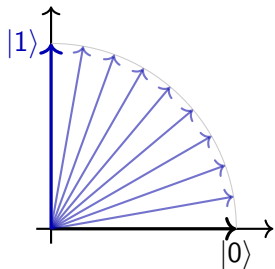
After all  $T$  rounds, using our assumption  $T\epsilon = \pi/2$ ,

$$\begin{aligned} |\psi_T\rangle &= R_\epsilon^T |0\rangle \\ &= R_{T\epsilon} |0\rangle \\ &= R_{\pi/2} |0\rangle = |1\rangle. \end{aligned}$$

### Conclusion

Under our simplifying assumption, with no bomb, the final outcome is 1 with probability 1.

## Geometric picture: No bomb



### No intermediate measurement

Each small rotation continues from where the previous one ended.

$$|0\rangle \longrightarrow \dots \longrightarrow |1\rangle.$$

We assume the total angle is

$$T\epsilon = \frac{\pi}{2}.$$

### What this picture represents

The axes are the real amplitudes of  $|0\rangle$  and  $|1\rangle$ . This is an amplitude-plane picture, not a physical path or a Bloch sphere. The steps are enlarged for visibility.

## Live bomb: Every surviving query resets the state

Suppose we have survived all previous rounds. The current state is  $|0\rangle$ .  
In every round,

$$|0\rangle \xrightarrow{R_\epsilon} \cos \epsilon |0\rangle + \sin \epsilon |1\rangle .$$

The meter then measures this state:

### Outcome 0: Survival

Probability:

$$\cos^2 \epsilon .$$

Returned state:

$$|0\rangle .$$

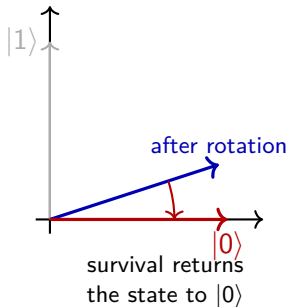
### Outcome 1: Explosion

Probability:

$$\sin^2 \epsilon .$$

The protocol ends.

## Geometric picture: A live bomb



Repeat

$$|0\rangle \xrightarrow{\text{small rotation}} \text{small tilt} \xrightarrow{\text{survival}} |0\rangle.$$

The small tilts never accumulate on surviving runs.

If all rounds are survived, the final state is  $|0\rangle$ .

### Conclusion

For a live bomb, every surviving run ends with outcome 0.

# Why frequent checks can inhibit change

## No bomb

- Small rotations.
- No intermediate measurements.
- The state reaches  $|1\rangle$  under our simplifying assumption.

## Live bomb

- Small rotations.
- Measurement after each rotation.
- Survival returns the state to  $|0\rangle$ .

## The remaining question: What is the total risk?

For a live bomb, every reached round has explosion probability

$$\sin^2 \epsilon.$$

But there are  $T$  rounds

A small risk per round does not automatically imply a small total risk.

We will use two tools:

- 1 The **union bound**, from probability.
- 2 For a small angle in radians,

$$\sin^2 \epsilon \approx \epsilon^2.$$

## A probability tool: The union bound

For any events  $A_1, \dots, A_T$ ,

$$\Pr \left[ \bigcup_{i=1}^T A_i \right] \leq \sum_{i=1}^T \Pr[A_i].$$

In words

The probability that **at least one** event happens is at most the sum of the individual probabilities.

## Apply the union bound to the bomb I

Fix the case of a **live bomb**.

Let  $A_i$  be the event

$$A_i = \{\text{the bomb explodes in round } i\}.$$

Since every round uses the angle  $\epsilon$ ,

$$\begin{aligned}\Pr[A_i] &= \Pr[\text{reach round } i] \Pr[\text{explode in } i \mid \text{reach } i] \\ &= \Pr[\text{reach round } i] \sin^2 \epsilon \\ &\leq \sin^2 \epsilon.\end{aligned}$$

## Apply the union bound to the bomb II

Therefore,

$$\begin{aligned}\Pr[\text{the bomb explodes}] &= \Pr \left[ \bigcup_{i=1}^T A_i \right] \\ &\leq \sum_{i=1}^T \Pr[A_i] \\ &\leq \boxed{T \sin^2 \epsilon}.\end{aligned}$$

## Small angles make the total risk small

For small  $\epsilon$ ,

$$\sin^2 \epsilon \approx \epsilon^2.$$

Thus, intuitively,

$$T \sin^2 \epsilon \approx T \epsilon^2 \approx \frac{\pi}{2} \epsilon.$$

### An actual upper bound

Using  $\sin \epsilon \leq \epsilon$  and  $T \leq \frac{\pi}{2\epsilon} + 1$ ,

$$\Pr[\text{the bomb explodes}] \leq T \sin^2 \epsilon \leq T \epsilon^2 \leq \boxed{\frac{\pi}{2} \epsilon + \epsilon^2}.$$

### We control $\epsilon$

As  $\epsilon$  decreases, the explosion risk goes to 0, but the number of queries increases.

## A concrete numerical example

Choose

$$\epsilon = 0.0001.$$

Then

$$T = \left\lceil \frac{\pi}{2(0.0001)} \right\rceil = 15,708.$$

For a live bomb,

$$\begin{aligned}\Pr[\text{the bomb explodes}] &\leq T\epsilon^2 \\ &= 15,708 \cdot (0.0001)^2 \\ &= 0.00015708.\end{aligned}$$

### Interpretation

The explosion probability is at most

$$0.015708\%.$$

The probability of safely identifying a live bomb is therefore at least 99.984292%.

# What the algorithm guarantees

Under our simplifying assumption  $T\epsilon = \pi/2$ :

## Innocent suitcase

- No explosion.
- Final state:  $|1\rangle$ .
- Report “no bomb” with probability 1.

## Malicious suitcase

- Explosion probability at most  $T\epsilon^2$ .
- If we survive, final state:  $|0\rangle$ .
- Every surviving run correctly reports “live bomb.”

## The quantum advantage in this game

We can identify a live bomb without detonating it, with success probability approaching 1.

Why the Four Postulates?  
— “You cannot keep asking why.”

# Inherent Tension for CS-oriented Quantum Computing

**Tension:** limited time for underlying quantum mechanics.

- Pedagogical stance: adopt an axiomatic approach.
- Core idea: accept the four postulates as the foundation.

# Why an Axiomatic Approach?

## Reason 1: Breadth vs. Time

- Many quantum computing topics to cover.
- Finite lecture time prevents deep QM detours.

## Reason 2: Limits of Understanding

- Humanity does not fully understand the “why” behind QM.
- Physicists (only) know what it predicts and how to apply it.
- But the postulates’ ultimate justification remains an open question about reality’s structure.  
(More discussion later: interpretations of quantum mechanics.)

## Suggested Viewing: Feynman on Boundaries of Explanation

Watch: [Interview with Richard Feynman \(14:54–22:27\)](#)

- Theme: respecting the limits when probing “what really happened.”
- Takeaway: why we accept the four postulates as foundational for quantum computing without demanding deeper “whys” in this course.

### Who is Richard Feynman?

Richard P. Feynman (1918–1988) was an American theoretical physicist known for his path integral formulation of quantum mechanics, development of quantum electrodynamics (for which he shared the 1965 Nobel Prize in Physics), and the invention of Feynman diagrams. He was also a renowned educator, author of the Feynman Lectures on Physics, and a pioneer in articulating the idea of quantum computation.

## Beyond the Clip

- The full one-hour interview is engaging and inspiring.
- Valuable for creativity, curiosity, and research in any field.
- Recommended if you have time: [watch the entire interview](#).

# Summary

In summary:

- We adopt the four postulates to build quantum computing rigorously.
- We (computer scientists) focus on design and analysis of quantum algorithms, not the underlying physics.
- Deeper “why” questions touch active frontiers of physics.