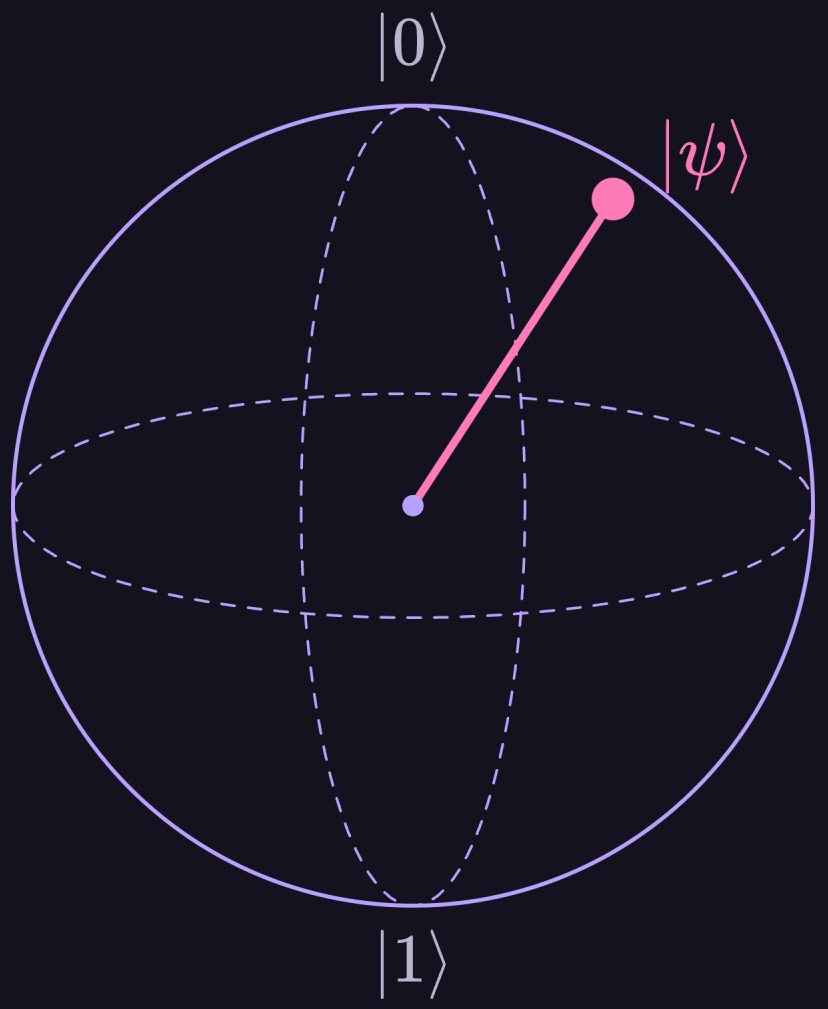
UCF · IBM QISKIT FALL FEST 2026

Quantum computing

An introduction for the curious — from postulates to circuits



Sumeet Shirgure

sumeetparameshwar.shirgure@ucf.edu

November 9, 2026 · Research Building 1

ROADMAP

The next 45 minutes

01
Origins
~4 min

02
Complex linear algebra
~13 min

03
Quantum postulates
~4 min

04
Qubits & hardware
~5 min

05
Algorithms
~10 min

06
Qiskit: Bell pair
~4 min

07
Stochastic Pauli noise
~5 min

→
Recap & questions
~3 min

01

Origins

How a theory of atoms became a theory of computation.

ORIGINS · PART 1

Quantum theory, 1900–1964

1900

Planck

Energy is exchanged in discrete quanta — the start of quantum theory.

1925–26

Heisenberg, Schrödinger

Matrix mechanics and wave mechanics: two faces of one theory.

1932

von Neumann

Quantum mechanics recast as linear algebra on Hilbert space.

1935

EPR · Schrödinger

Strange long-range correlations; Schrödinger names them entanglement.

1964

Bell

No local hidden-variable theory can reproduce those correlations — testably.

Every idea in this talk is already here: Hilbert spaces, measurement, entanglement. What was missing was the question “can we compute with it?”

ORIGINS · PART 2

Quantum computation, 1980–1996

1980

Benioff

A quantum-mechanical model of a Turing machine.

1981

Feynman

To simulate nature efficiently, build a computer out of quantum parts.

1985

Deutsch

The universal quantum computer, and the first quantum speed-up.

1994

Shor

Polynomial-time factoring — suddenly the field matters to cryptography.

1995–96

Shor, Steane, Lloyd, Grover

Error correction is possible; universal simulation; quadratic search.

Two motivations that still drive the field: **simulate physics** (Feynman) and **outperform classical algorithms** (Shor).

WHY QUANTUM COMPUTERS?

“Nature isn’t classical, dammit…”

— Richard Feynman, *Simulating Physics with Computers* (1981 talk, published 1982)

2^n

complex amplitudes are needed to write down the state of n qubits

≈ 18 PB

of memory to store a 50-qubit state at 16 bytes per amplitude

$2^{300} \approx 10^{90}$

amplitudes for 300 qubits — more than the roughly 10^80 atoms in the observable universe

ORIGINS · PART 3

From theory to hardware

1995

First quantum logic gate

CNOT on a trapped ion (NIST), months after the Cirac–Zoller proposal.

1997

Teleportation

Quantum teleportation of photon polarization demonstrated.

1999

Superconducting qubit

Coherent control of a superconducting circuit (NEC).

2016

Quantum in the cloud

IBM puts a 5-qubit processor online for anyone to use.

2017

Qiskit

IBM open-sources the Qiskit software development kit.

2019

Beyond classical?

Google samples random circuits on 53 qubits.

2023

Utility scale

IBM simulates dynamics on 127 qubits with error mitigation.

2024

Below threshold

Google shows logical errors falling as a surface code grows.

02

Complex linear algebra

Vectors, matrices and complex numbers — in finite dimensions only.

LINEAR ALGEBRA · STATES

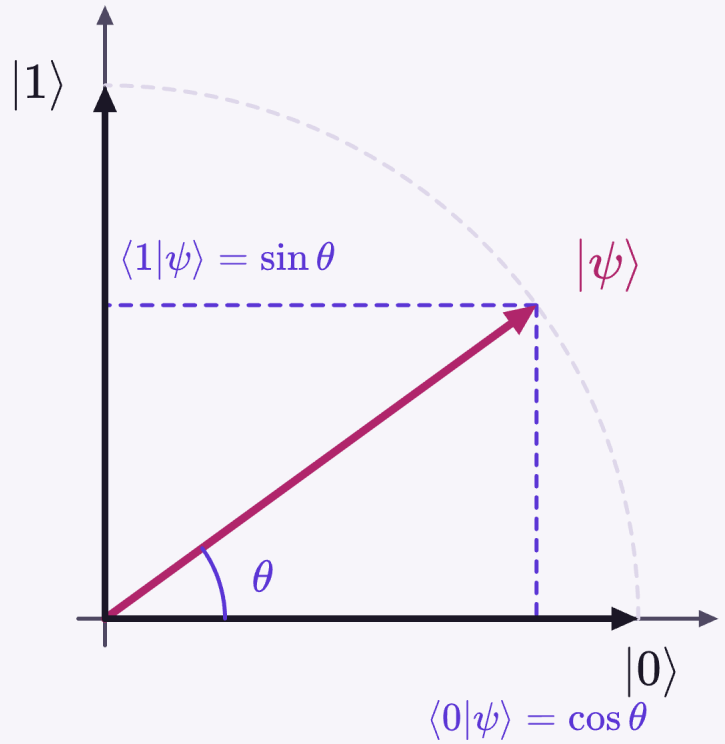
Bra-ket notation: states are vectors

- A **Hilbert space** here is just $\mathbb{C}^d$ with an inner product.
- A **ket** $|\psi\rangle$ is a column vector; a **bra** $\langle\psi| = |\psi\rangle^\dagger$ is its conjugate transpose.
- The bra-ket $\langle\phi|\psi\rangle = \sum_i \phi_i^* \psi_i$ is the inner product: an "overlap".
- States are normalized: $\langle\psi|\psi\rangle = 1$.

$$|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}, \quad |1\rangle = \begin{pmatrix}0\\1\end{pmatrix}, \quad |\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix}\alpha\\\beta\end{pmatrix}$$

$$\langle\psi| = (\alpha^* \quad \beta^*), \qquad \langle\psi|\psi\rangle = |\alpha|^2 + |\beta|^2 = 1$$

A real slice of the plane of qubit states: amplitudes are "shadows" on the basis directions.



LINEAR ALGEBRA · OPERATORS

Operators are machines built from kets and bras

OUTER PRODUCTS ARE OPERATORS

$$|1\rangle \longrightarrow \boxed{|0\rangle\langle 1|} \longrightarrow |0\rangle\,\langle 1|1\rangle = |0\rangle$$

the bra “reads” the input, the ket is written out

$$|0\rangle \longrightarrow \boxed{|0\rangle\langle 1|} \longrightarrow |0\rangle\,\langle 1|0\rangle = 0$$

zero overlap: nothing comes out

AS MATRICES

$$|0\rangle\langle 1| = \begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}0 & 1\end{pmatrix} = \begin{pmatrix}0 & 1\\0 & 0\end{pmatrix}$$

Any operator: $A = \sum_{ij} A_{ij}|i\rangle\langle j|$, $A_{ij} = \langle i|A|j\rangle$

Adjoint (conjugate transpose): $A^\dagger = (A^*)^T$

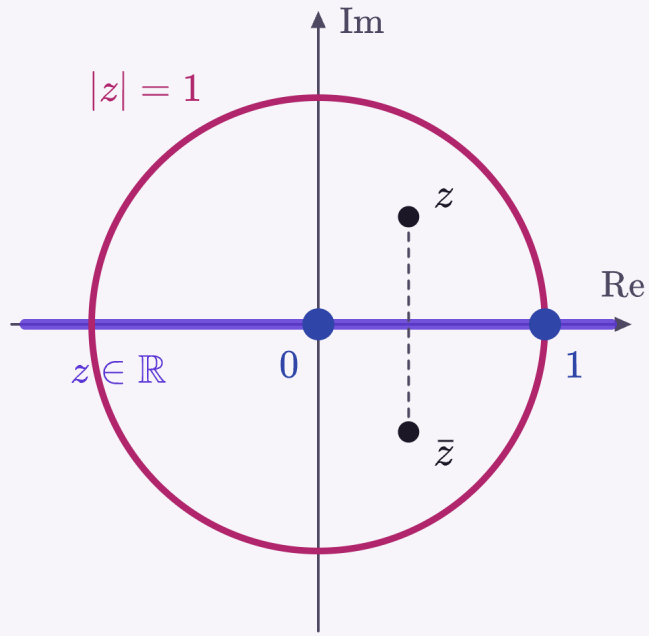
and $(|\psi\rangle\langle\phi|)^\dagger = |\phi\rangle\langle\psi|$

LINEAR ALGEBRA · INTUITION

Matrices behave like complex numbers

Kind	Definition	1 × 1 version	What it does to information
Adjoint	$A^\dagger$	$\bar{z}$	run it "backwards"
Projector	$P^2 = P = P^\dagger$	$z \in \{0, 1\}$	keep or discard — information is lost
Unitary	$U^\dagger U = I$	$\bar{z}z = 1,\ z = e^{i\theta}$	reversible relabeling — nothing is lost
Hermitian	$A = A^\dagger$	$z = \bar{z} \in \mathbb{R}$	real readings along perpendicular axes

Trick (as in Axler's *Linear Algebra Done Right*): to remember a property, check it on 1 × 1 matrices — they are just complex numbers.



Unitaries live on the circle, Hermitians on the line, projectors at 0 and 1.

LINEAR ALGEBRA · PROJECTORS

Projectors: keep one part, forget the rest

$$P^2 = P = P^\dagger$$

EXAMPLE

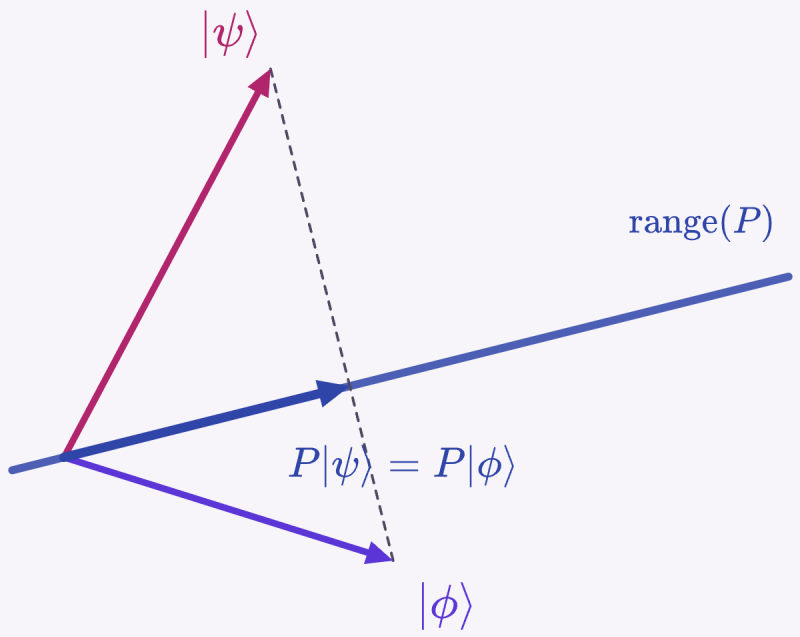
$P_0 = |0\rangle\langle 0|$ acting on $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$:

$$P_0|+\rangle = |0\rangle\,\langle 0|+\rangle = \frac{1}{\sqrt{2}}|0\rangle = P_0|-\rangle$$

Applying it twice changes nothing: $P_0^2 = |0\rangle\,\langle 0|0\rangle\langle 0| = P_0$

- Any unit vector gives one: $P_\psi = |\psi\rangle\langle\psi|$, and $I - P$ projects onto what is left.
- 1 × 1 check: $z^2 = z \Rightarrow z \in \{0, 1\}$ — keep or discard.

A projector casts a shadow onto a subspace. Different inputs can cast the same shadow: the rest is forgotten.



LINEAR ALGEBRA · UNITARIES

Unitaries: reversible moves that lose nothing

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

EXAMPLES

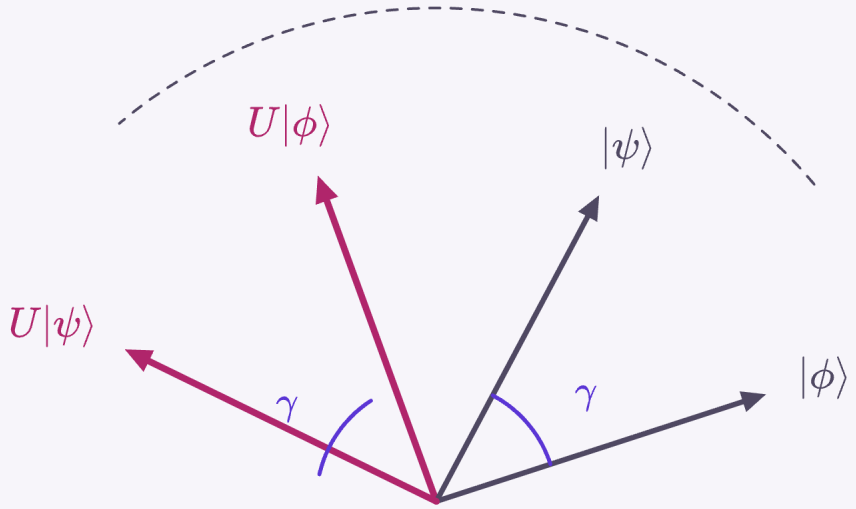
$$X = |0\rangle\langle 1| + |1\rangle\langle 0| : \quad X|0\rangle = |1\rangle\,\langle 0|0\rangle = |1\rangle$$

$$H = \tfrac{1}{\sqrt{2}}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|)$$

$$H|0\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle, \qquad H|1\rangle = |-\rangle$$

- Overlaps survive: $\langle U\phi|U\psi\rangle = \langle\phi|U^\dagger U|\psi\rangle = \langle\phi|\psi\rangle$
- Always reversible: $U^{-1} = U^\dagger$.
- 1 × 1 check: $|z| = 1$, a pure phase $e^{i\theta}$.

A unitary is a rigid rotation of state space: lengths and angles (overlaps) survive.



LINEAR ALGEBRA · OBSERVABLES

Hermitian operators: real stretches = observables

$$A = A^\dagger$$

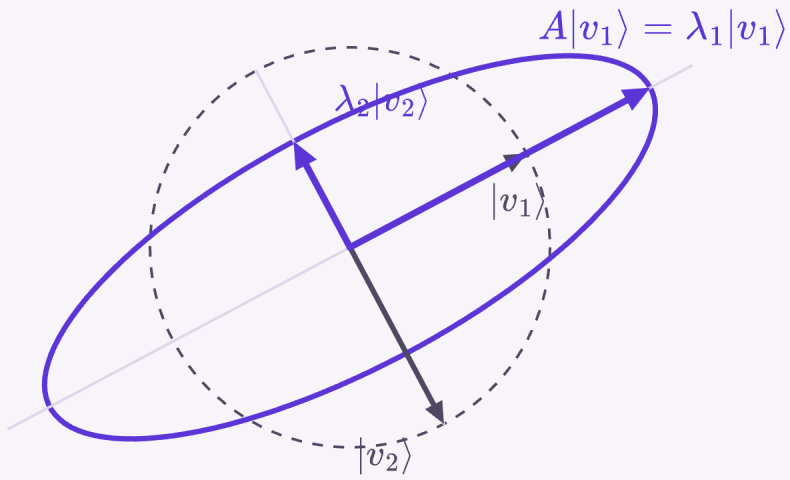
EXAMPLE: PAULI Z

$$Z = |0\rangle\langle 0| - |1\rangle\langle 1| : \qquad Z|0\rangle = |0\rangle, \quad Z|1\rangle = -|1\rangle$$

$$Z|+\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle, \qquad \langle +|Z|+\rangle = \langle +|-\rangle = 0$$

- Eigenvalues are real and eigenvectors for different eigenvalues are orthogonal.
- Eigenvalues = the possible **readings** of a measurement: these are **observables**.
- 1 × 1 check: $z = \bar{z}$ means $z \in \mathbb{R}$.

A Hermitian operator stretches space by real factors along perpendicular axes (a negative factor also flips).



LINEAR ALGEBRA · DECOMPOSITIONS

Resolution of the identity and spectral decomposition

RESOLUTION OF THE IDENTITY

$$\sum_i |i\rangle\langle i| = I$$

for any orthonormal basis. Why: expand any state, $|\psi\rangle = \sum_i |i\rangle \langle i|\psi\rangle$.

$$|0\rangle\langle 0| + |1\rangle\langle 1| = I = |+\rangle\langle +| + |-\rangle\langle -|$$

Trick: insert $I = \sum_i |i\rangle\langle i|$ anywhere in a calculation.

SPECTRAL DECOMPOSITION

$$A = \sum_k \lambda_k P_k$$

Hermitian (more generally normal) A with eigenvalues λ_k and orthogonal projectors P_k, $\sum_k P_k = I$.

$$Z = (+1)|0\rangle\langle 0| + (-1)|1\rangle\langle 1|, \qquad X = |+\rangle\langle +| - |-\rangle\langle -|$$

The analogy, made precise: Hermitian ⇔ all $\lambda_k \in \mathbb{R}$; unitary ⇔ all $|\lambda_k| = 1$; projector ⇔ all $\lambda_k \in \{0, 1\}$.

LINEAR ALGEBRA · FUNCTIONS OF OPERATORS

Exponentials and other functions of matrices

VIA THE SPECTRUM

If $A = \sum_k \lambda_k P_k$, then

$$f(A) = \sum_k f(\lambda_k)\, P_k$$

VIA POWER SERIES

$$e^A = \sum_{n \geq 0} \frac{A^n}{n!} = I + A + \frac{A^2}{2!} + \cdots$$

CONSEQUENCES

1. H Hermitian $\Rightarrow e^{-iHt} = \sum_k e^{-i\lambda_k t} P_k$
is unitary (all eigenvalues on the unit circle).

2. Careful: $e^{A+B} \neq e^A e^B$ unless $AB = BA$.
This is why we will need Trotterization.

3. Any P with $P^2 = I$
(e.g. a Pauli) has a closed form — next slide.

LINEAR ALGEBRA · DERIVATION

Deriving the exponential of a Pauli

ROUTE 1 · POWER SERIES

$$e^{-itP} = \sum_{n\geq 0} \frac{(-it)^n}{n!} P^n$$

Use $P^{2k} = I$ and $P^{2k+1} = P$ to split even and odd terms:

$$= \left(\sum_k \frac{(-1)^k t^{2k}}{(2k)!}\right) I - i\left(\sum_k \frac{(-1)^k t^{2k+1}}{(2k+1)!}\right) P$$

$$= \cos t\, I - i \sin t\, P$$

ROUTE 2 · SPECTRUM

$P^2 = I$ means eigenvalues ± 1: $P = P_+ - P_-$, $P_+ + P_- = I$.

$$e^{-itP} = e^{-it} P_+ + e^{it} P_-$$

$$= \cos t\,(P_+ + P_-) - i \sin t\,(P_+ - P_-)$$

$$= \cos t\, I - i \sin t\, P$$

Rotation gates: $R_P(\theta) = e^{-i\theta P/2}$.

LINEAR ALGEBRA · PAULI OPERATORS

The Pauli operators

I $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$|0\rangle\langle 0| + |1\rangle\langle 1|$

identity

X $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

$|0\rangle\langle 1| + |1\rangle\langle 0|$

bit flip

Y $\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$

$-i|0\rangle\langle 1| + i|1\rangle\langle 0|$

bit + phase flip

Z $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

$|0\rangle\langle 0| - |1\rangle\langle 1|$

phase flip

- Hermitian **and** unitary: $P^2 = I$, eigenvalues ± 1.
- $XY = iZ,\ YZ = iX,\ ZX = iY$; distinct Paulis anticommute: $XY = -YX$.
- A basis for 2 × 2 matrices: every Hermitian $A = a_0 I + a_1 X + a_2 Y + a_3 Z$ with real a_k.

LINEAR ALGEBRA · PAULI OPERATORS

Why “bit flip” and “phase flip”?

X Swaps the computational basis: a classical NOT on the bit value 0 ↔ 1.

$$X|0\rangle = |1\rangle, \quad X|1\rangle = |0\rangle$$

$$X\left(\alpha|0\rangle + \beta|1\rangle\right) = \beta|0\rangle + \alpha|1\rangle$$

$$X|\pm\rangle = \pm|\pm\rangle$$

Z Leaves the bit value alone but flips the sign of the $|1\rangle$ part: a relative phase $e^{i\pi} = -1$.

$$Z|0\rangle = |0\rangle, \quad Z|1\rangle = -|1\rangle$$

$$Z\left(\alpha|0\rangle + \beta|1\rangle\right) = \alpha|0\rangle - \beta|1\rangle$$

$$Z|+\rangle = |-\rangle, \quad Z|-\rangle = |+\rangle$$

- The two are mirror images: $HXH = Z$. A phase flip is a bit flip in the $|\pm\rangle$ basis, and vice versa.
- $Y = iXZ$ does both at once. On the Bloch sphere (part 4) each Pauli is a 180° rotation about its own axis.

LINEAR ALGEBRA · TENSOR PRODUCTS

Many qubits: tensor products

MATRICES: THE KRONECKER PRODUCT

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B \\ a_{21}B & a_{22}B \end{pmatrix}$$

An $m \times m$ and an $n \times n$ matrix give an $mn \times mn$ matrix. Example:

$$Z \otimes X = \begin{pmatrix} X & 0 \\ 0 & -X \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \end{pmatrix}$$

VECTORS: SAME RULE

$$|0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ 0 \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = |01\rangle$$

KEY RULES

$(A \otimes B)(|a\rangle \otimes |b\rangle) = A|a\rangle \otimes B|b\rangle$

$(A \otimes B)(C \otimes D) = AC \otimes BD$

n qubits live in $(\mathbb{C}^2)^{\otimes n} = \mathbb{C}^{2^n}$.

LINEAR ALGEBRA · TENSOR PRODUCTS

Pauli strings and entanglement

PAULI STRINGS

$Z \otimes Z \equiv ZZ, X \otimes I \equiv XI, \ldots$

The 4^n Pauli strings form a basis for all n -qubit operators, so every Hamiltonian is

$$H = \sum_j h_j P_j, \qquad P_j \in \{I, X, Y, Z\}^{\otimes n}$$

ENTANGLEMENT

Most vectors in $\mathbb{C}^2 \otimes \mathbb{C}^2$ are **not** products $|a\rangle \otimes |b\rangle$.

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \neq |a\rangle \otimes |b\rangle$$

Try it: a product has amplitudes $a_i b_j$, so $a_0 b_0 \, a_1 b_1 = a_0 b_1 \, a_1 b_0$ — here $\frac{1}{2} \neq 0$.

03

The postulates

Four rules that define the whole game.

POSTULATES

Quantum mechanics in four postulates

I · STATE

An isolated system is a unit vector $|\psi\rangle$ in a Hilbert space.

$|\psi\rangle$ and $e^{i\varphi}|\psi\rangle$ are the same physical state.

II · EVOLUTION

Closed systems evolve by unitaries:

$|\psi(t)\rangle = e^{-iHt/\hbar}|\psi(0)\rangle$

generated by the Hamiltonian H
(Schrödinger's equation).

III · MEASUREMENT

Projectors $\{P_m\}$, $\sum_m P_m = I$, give outcome m
with probability

$p(m) = \langle\psi|P_m|\psi\rangle$, leaving $P_m|\psi\rangle/\sqrt{p(m)}$.

IV · COMPOSITION

A joint system lives in the tensor product

$\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$.

POSTULATES · MEASUREMENT

Measurement in practice: the Born rule

BORN RULE IN THE Z BASIS

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

$$\Pr(0) = \langle\psi|0\rangle\,\langle 0|\psi\rangle = |\alpha|^2, \qquad \Pr(1) = |\beta|^2$$

Expectation value of an observable $A = \sum_k \lambda_k P_k$:

$$\langle A\rangle = \langle\psi|A|\psi\rangle = \sum_k \lambda_k \Pr(k)$$

SAME STATE, DIFFERENT QUESTIONS

$$|+\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

Measure Z: 0 or 1, each with probability ½.

Measure X (projectors $|\pm\rangle\langle\pm|$): always +.

After measuring, the state **is** the eigenvector you saw. Measurement is a projector: irreversible.

POSTULATES · COMPOSITION

Entanglement: correlations without a classical story

PRODUCT STATE

$$|0\rangle \otimes |+\rangle$$

Each qubit has a state of its own. Measuring one tells you nothing about the other.

ENTANGLED STATE

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

Each qubit alone is a fair coin, but outcomes always agree — in the Z basis **and** in the X basis.

- **Bell (1964), CHSH (1969):** any local classical model obeys $S \leq 2$; entangled qubits reach $2\sqrt{2} \approx 2.83$.
- **No signalling:** entanglement alone cannot send a message — you still need a classical channel.

04

Qubits

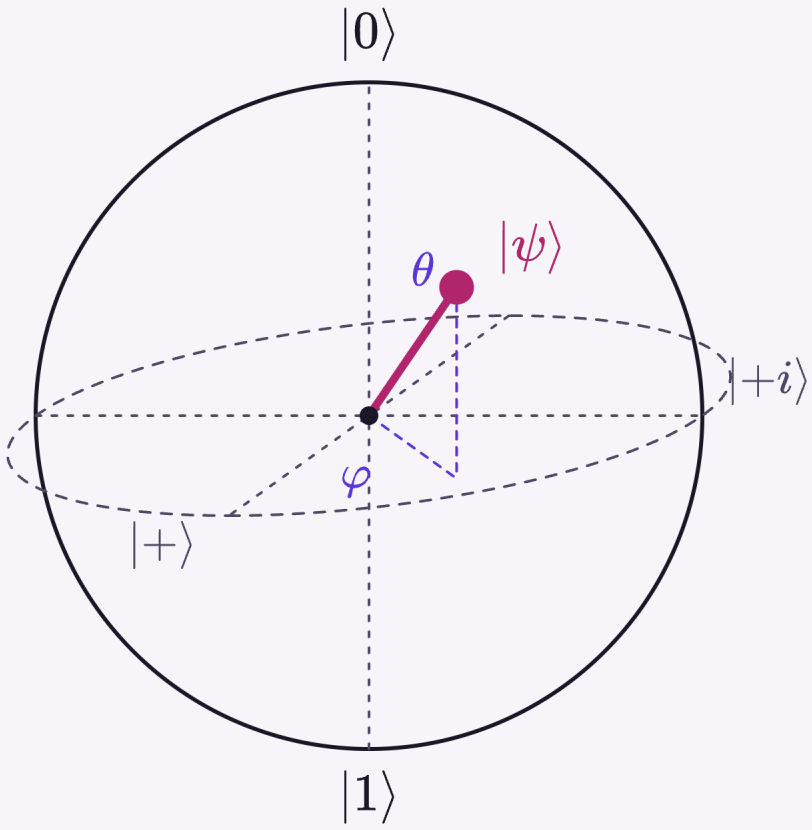
Any well-controlled two-level quantum system can store one.

QUBITS · GEOMETRY

One qubit, one sphere

$$|\psi\rangle = \cos\tfrac{\theta}{2}|0\rangle + e^{i\varphi}\sin\tfrac{\theta}{2}|1\rangle$$

- Normalization and an unobservable global phase leave two real numbers (θ, φ): a point on a sphere.
- Poles $|0\rangle, |1\rangle$. Equator $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$, $|\pm i\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle)$.
- Bloch vector $\vec{r} = (\langle X\rangle, \langle Y\rangle, \langle Z\rangle)$.
- Gates are rotations: $R_P(\theta) = e^{-i\theta P/2}$ turns the sphere by θ about axis P.



QUBITS · GATES

Gates: the instruction set

Gate	Definition	What it does
X	$\|0\rangle\langle 1\| + \|1\rangle\langle 0\|$	Bit flip: $\|0\rangle \leftrightarrow \|1\rangle$
Z	$\|0\rangle\langle 0\| - \|1\rangle\langle 1\|$	Phase flip: $\|1\rangle \to -\|1\rangle$
H	$\frac{1}{\sqrt{2}}(X + Z)$	$\|0\rangle \to \|+\rangle$, $\|1\rangle \to \|-\rangle$: superposition
S, T	$\mathrm{diag}(1, i)$, $\mathrm{diag}(1, e^{i\pi/4})$	Relative phases of 90° and 45°
Rx, Ry, Rz	$e^{-i\theta P/2}$	Rotate the Bloch vector by θ
CNOT	$\|0\rangle\langle 0\| \otimes I + \|1\rangle\langle 1\| \otimes X$	$\|a, b\rangle \to \|a, a \oplus b\rangle$: flip target if control is 1
CZ	$\|0\rangle\langle 0\| \otimes I + \|1\rangle\langle 1\| \otimes Z$	Phase -1 on $\|11\rangle$ only

Universality: $\{H, T, \mathrm{CNOT}\}$ approximates any unitary to any accuracy — efficiently, by Solovay–Kitaev.

QUBITS · REQUIREMENTS

What a physical qubit needs

1. **Well-defined qubits**
   a scalable physical system with two addressable levels
2. **Initialization**
   reliably reset to a simple state such as all zeros
3. **Long coherence**
   quantum information survives much longer than a gate takes
4. **Universal gates**
   a set of controllable operations that generates all unitaries
5. **Measurement**
   read out individual qubits

DIVINCENZO, 2000

Plus two criteria for quantum networks: convert stationary qubits to “flying” ones (photons), and transmit them faithfully.

QUBITS · MODALITIES

Many ways to build a qubit

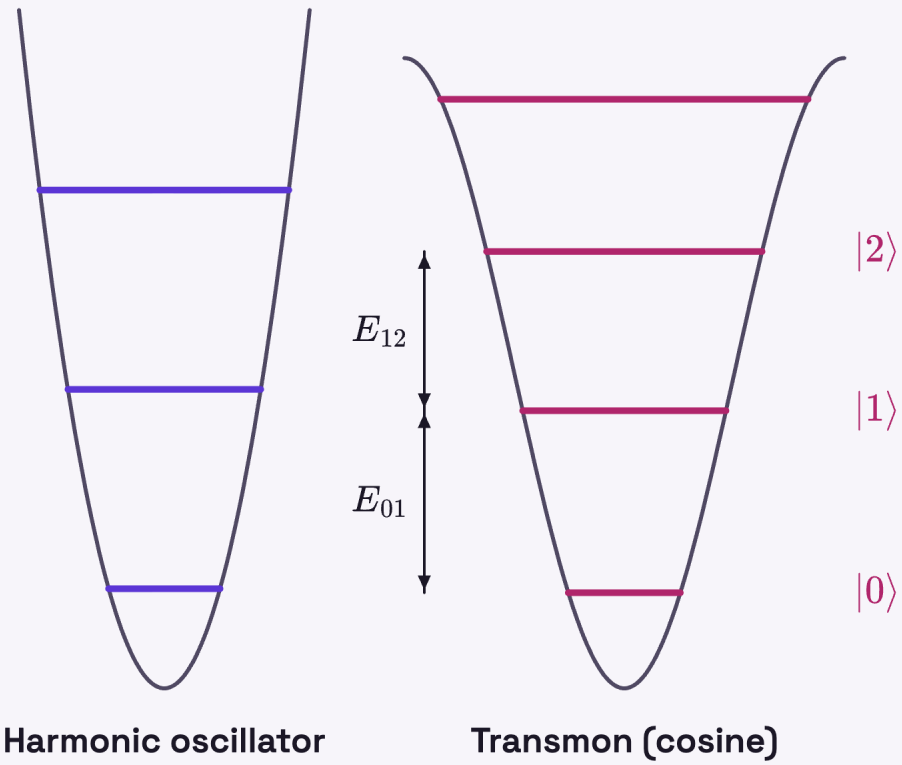
Modality	The qubit is...	Strengths	Challenges	Examples
Superconducting circuits	Lowest two levels of a nonlinear microwave circuit (transmon)	Fast gates; chip fabrication	Millikelvin cooling; wiring; crosstalk	IBM, Google, Rigetti
Trapped ions	Two internal levels of an ion held by electric fields	Very high fidelity; all-to-all coupling	Slower gates; scaling traps	Quantinuum, IonQ
Neutral atoms	Atoms in optical tweezers, coupled via Rydberg states	Large, reconfigurable arrays	Slower cycles; atom loss	QuEra, Pasqal, Atom Computing
Photons	Polarization, path or time-bin of single photons	Networking; little cooling of the qubits	Loss; probabilistic gates	PsiQuantum, Xanadu
Spins in silicon	Electron or nuclear spin in a quantum dot or donor	Tiny; CMOS-compatible	Device uniformity; control at scale	Intel, Diraq

QUBITS · IBM HARDWARE

Inside an IBM processor: the transmon

- A superconducting circuit: a capacitor plus a **Josephson junction**, a lossless nonlinear inductor.
- The cosine potential is softer than a parabola, so levels get **closer** going up: $E_{12} < E_{01}$.
- That negative anharmonicity α lets microwaves drive $|0\rangle \leftrightarrow |1\rangle$ without touching $|2\rangle$.
- Larger E_J/E_C means less charge noise but a smaller $|\alpha|/E_{01}$; devices sit near $|\alpha|/2\pi \approx 200\text{–}300\ \mathrm{MHz}$.
- Pulses of tens of ns; ~10–20 mK dilution refrigerator; coherence of order 100 µs.

$$E_{12} < E_{01}: \quad \alpha = E_{12} - E_{01} \approx -E_C$$



Levels computed numerically for E_J/E_C = 20 (exaggerated for visibility).

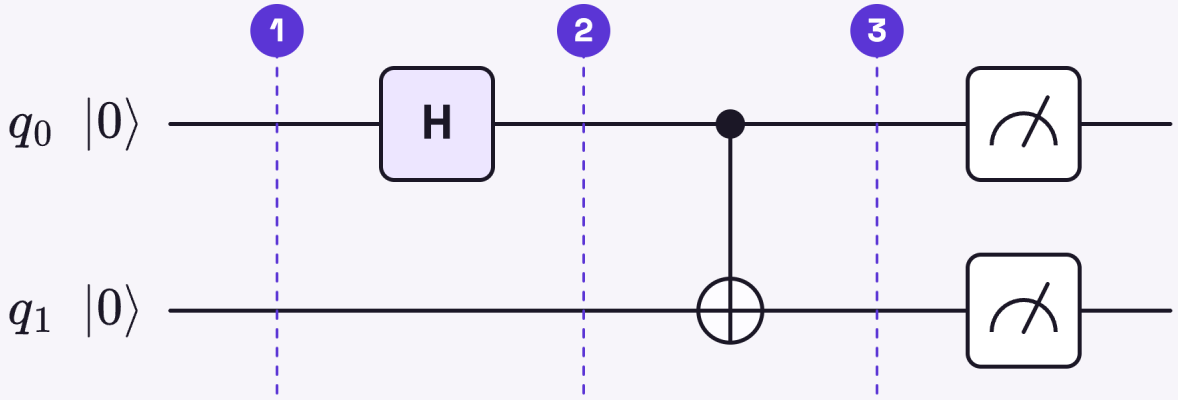
05

Algorithms

Small circuits, big ideas: entangle, teleport, simulate.

ALGORITHMS · BELL PAIR

Bell pair generation: two gates



Time flows left to right. Box: single-qubit gate. Dot joined to circled plus: CNOT (control, target). Meter: measurement.

1 · START

$|00\rangle$

2 · AFTER H ON QUBIT 0

$\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$

3 · AFTER CNOT

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

Measuring gives 00 or 11, each with probability ½ — never 01 or 10.

ALGORITHMS · BELL PAIR

The four Bell states

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

Circuit applied to $|00\rangle$ · Z outcomes always equal

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

Circuit applied to $|10\rangle$ · Z outcomes always equal

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

Circuit applied to $|01\rangle$ · Z outcomes always opposite

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Circuit applied to $|11\rangle$ · Z outcomes always opposite

- They form an orthonormal basis of two qubits: the **Bell basis**.
- **Bell measurement** = run the circuit backwards (CNOT, then H on the control) and measure in Z. This is the heart of teleportation.

ALGORITHMS · TELEPORTATION

Quantum teleportation: a qubit for two bits

Alice wants to give Bob an unknown state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ — without sending the qubit itself.

1

Share

Alice and Bob each hold half of a Bell pair $|\Phi^+\rangle$.

2

Measure

Alice Bell-measures her unknown $|\psi\rangle$ with her half: two random bits $m_1 m_2$.

3

Phone

She sends $m_1 m_2$ to Bob over an ordinary classical channel.

4

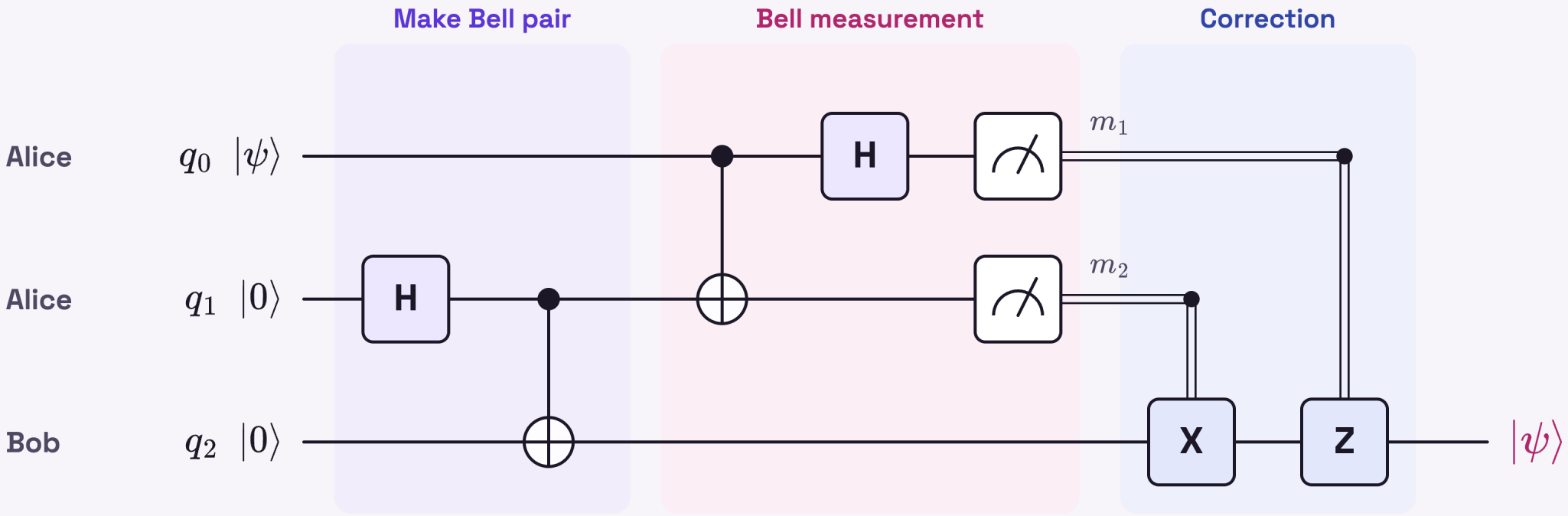
Fix

Bob applies X if $m_2 = 1$, then Z if $m_1 = 1$. His qubit is now $|\psi\rangle$.

Fine print: Alice's copy is destroyed (no-cloning holds), and nothing travels faster than light — Bob must wait for the bits. 1 Bell pair + 2 bits = 1 qubit.

ALGORITHMS · TELEPORTATION

The teleportation circuit



Double lines carry classical bits. In Qiskit the corrections use if_test on measured bits (dynamic circuits).

ALGORITHMS · TELEPORTATION

Why it works

After the Bell pair, $\mathrm{CNOT}_{q_0 \to q_1}$ and H on q_0, the state regroups by Alice's qubits:

$$\frac{1}{2}\Big[|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)\Big]$$

Alice's bits	Bob's qubit before fixing	Bob applies
`00`	$\alpha\|0\rangle + \beta\|1\rangle$	I
`01`	$\alpha\|1\rangle + \beta\|0\rangle$	X
`10`	$\alpha\|0\rangle - \beta\|1\rangle$	Z
`11`	$\alpha\|1\rangle - \beta\|0\rangle$	ZX (X first)

Each outcome has probability ¼ regardless of α and β — Alice learns nothing about the state.

ALGORITHMS · QUANTUM SIMULATION

Quantum simulation: Feynman's original application

THE TASK

Given H and $|\psi(0)\rangle$, prepare $|\psi(t)\rangle = e^{-iHt}|\psi(0)\rangle$ and measure observables.

1 · WRITE H IN PAULIS

$$H = \sum_j h_j P_j$$

Spin models already have this form; molecules need a fermion-to-qubit mapping.

2 · EXPONENTIATE EACH TERM

$$e^{-i\theta P_j}$$

A short circuit: basis change, a CNOT ladder, one Rz rotation.

3 · TROTTERIZE

$$e^{-i(A+B)t} \approx \left(e^{-iAt/n} e^{-iBt/n}\right)^n$$

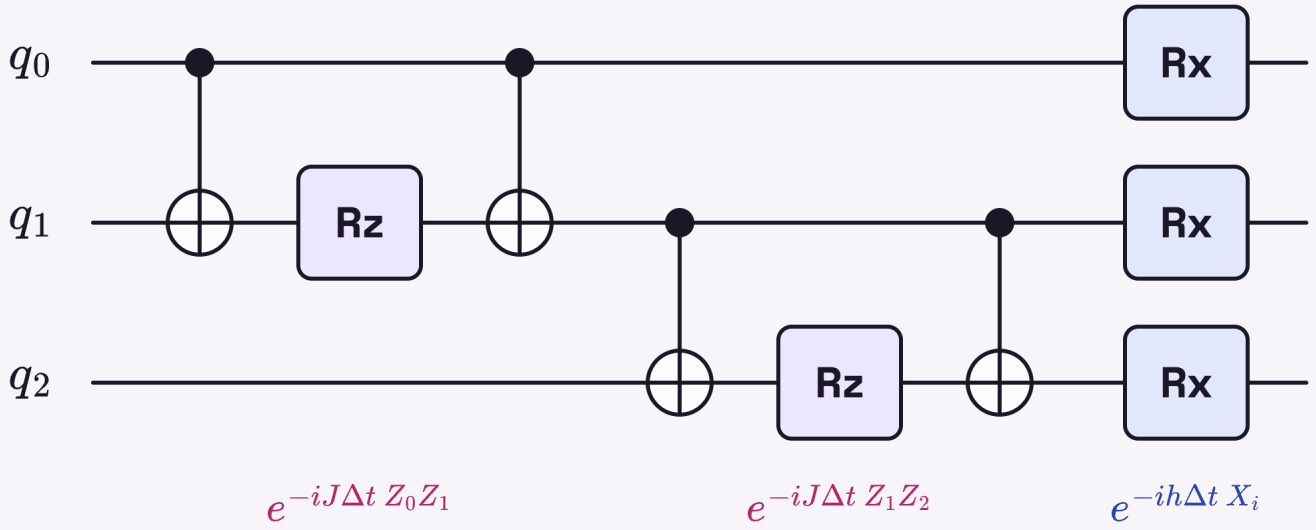
Error $\approx t^2 \|[A,B]\|/2n$:
more steps, more accuracy, deeper circuit.

ALGORITHMS · QUANTUM SIMULATION

Example: a 3-qubit Ising chain

$$H = J\left(Z_0 Z_1 + Z_1 Z_2\right) + h\left(X_0 + X_1 + X_2\right)$$

ZZ terms couple neighbouring spins; the transverse field X flips them. One Trotter step of length Δt:



BUILDING BLOCKS

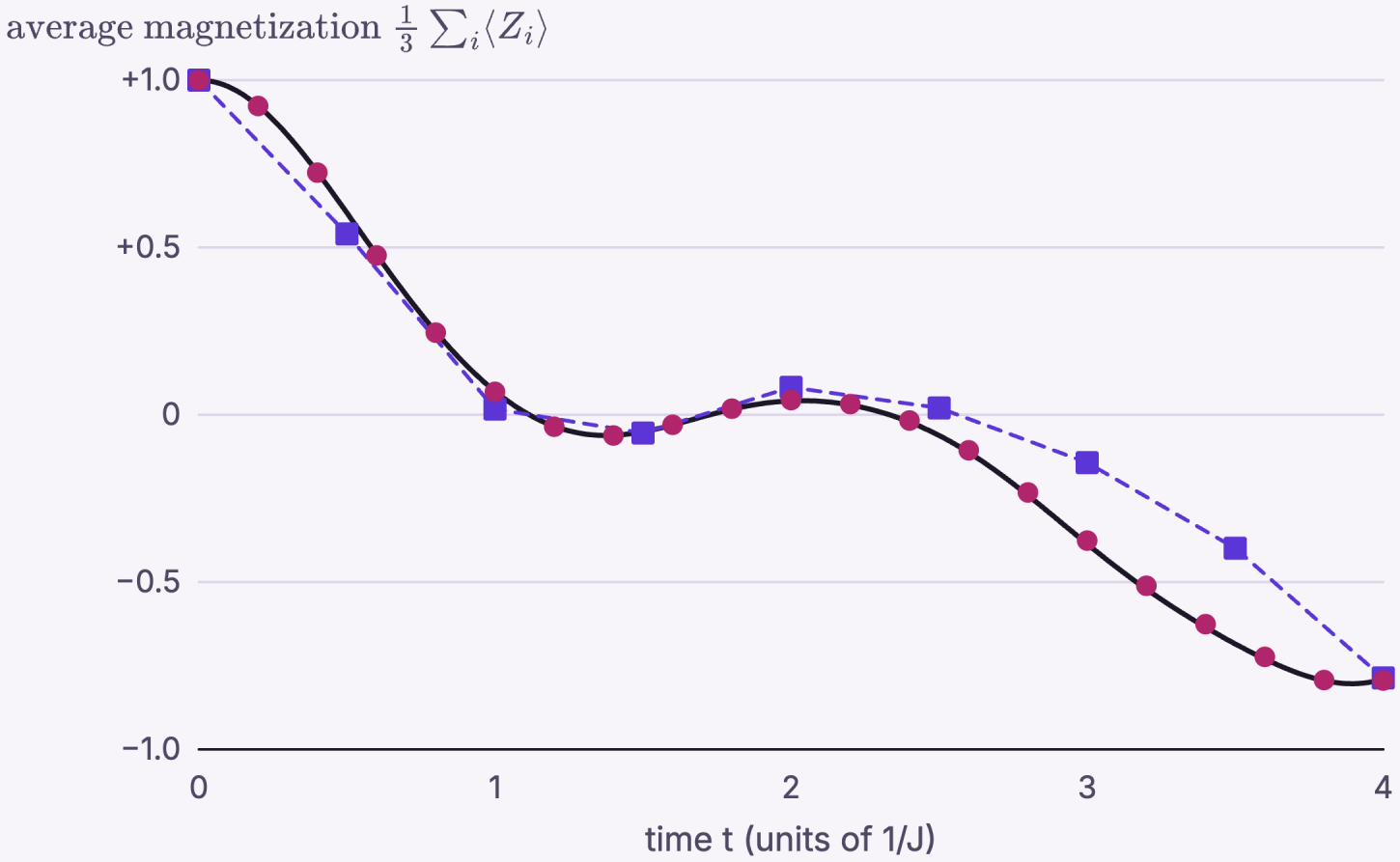
$$e^{-i\varphi X} = R_x(2\varphi)$$

$$e^{-i\varphi Z\otimes Z} = \mathrm{CNOT}\,(I \otimes R_z(2\varphi))\,\mathrm{CNOT}$$

Here $\varphi = J\Delta t$ or $h\Delta t$. Drop q_2 for the 2-qubit version.

ALGORITHMS · QUANTUM SIMULATION

Trotter in action: exact vs. approximate



LEGEND

- Exact evolution
- Trotter, Δt = 0.1 (40 steps)
- Trotter, Δt = 0.5 (8 steps)

J = h = 1, start in all zeros. Computed by exact state-vector simulation.

Small steps track the exact curve; big steps drift. But every extra step adds gates — and on hardware, more gates means more noise.

ALGORITHMS · IN PASSING

Further on: the QFT and Shor's algorithm

QUANTUM FOURIER TRANSFORM

$$|x\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i\, xy/N} |y\rangle, \quad N = 2^n$$

$O(n^2)$ gates versus $O(n2^n)$ for a classical FFT on the same 2^n numbers — but the amplitudes can't be read out directly. It shines inside algorithms that extract a **period**.

SHOR'S ALGORITHM (1994)

Factor N by finding the period r of $a^x \bmod N$; the QFT finds r.

Polynomial time versus the best known sub-exponential classical methods. It breaks RSA and elliptic-curve crypto — hence NIST's post-quantum standards (2024).

Needs a large **fault-tolerant** machine: a 2025 estimate puts RSA-2048 at under a million noisy qubits running for under a week.

Also worth a look: Grover search ($\sqrt{N}$ queries instead of N), phase estimation, VQE, QAOA.

06

Programming with Qiskit

From an idea to a circuit running on IBM quantum hardware.

QISKIT · WORKFLOW

The Qiskit pattern

1

Map

Turn the problem into circuits and observables.

2

Optimize

Transpile to the backend's native gates, qubit layout and connectivity.

3

Execute

Run with a primitive: Sampler (bitstrings) or Estimator (expectation values).

4

Post-process

Analyse counts or expectation values; apply error mitigation.

```
pip install qiskit qiskit-ibm-runtime   # SDK + access to IBM hardware
```

QISKIT · STEP 1

Build the Bell circuit

```
from qiskit import QuantumCircuit

qc = QuantumCircuit(2)   # two qubits, both start in state 0
qc.h(0)                  # Hadamard on qubit 0
qc.cx(0, 1)              # CNOT: control 0, target 1
qc.measure_all()         # measure into register "meas"

qc.draw("mpl")           # or print(qc) for text art
```

MAPPING TO THE MATH

qc.h(0) $\rightarrow H$ on q_0

qc.cx(0, 1) $\rightarrow \mathrm{CNOT}_{q_0 \rightarrow q_1}$

Six lines for the circuit on the Bell-pair slide.

QISKIT · STEP 2

Run it on a local simulator

```
from qiskit.primitives import StatevectorSampler

sampler = StatevectorSampler()
job = sampler.run([qc], shots=1024)
counts = job.result()[0].data.meas.get_counts()
print(counts)   # e.g. {'00': 517, '11': 507}
```

READING THE OUTPUT

Only 00 and 11 appear — the Bell-state correlation.

Qiskit bitstrings are little-endian: the rightmost bit is qubit 0.

The exact split varies from run to run: shot noise.

QISKIT · STEP 3

Run it on an IBM quantum computer

```
from qiskit_ibm_runtime import QiskitRuntimeService, SamplerV2 as Sampler
from qiskit.transpiler import generate_preset_pass_manager

service = QiskitRuntimeService()   # after saving your IBM Quantum API key once
backend = service.least_busy(operational=True, simulator=False)

pm = generate_preset_pass_manager(optimization_level=1, backend=backend)
isa_qc = pm.run(qc)                # rewrite into the device's native gates

result = Sampler(mode=backend).run([isa_qc], shots=4096).result()
print(result[0].data.meas.get_counts())
```

Expect mostly 00 and 11 — plus a few percent of 01 and 10. Where do those come from?

QISKIT · BONUS

The Ising simulation in 15 lines

```
from qiskit import QuantumCircuit
from qiskit.circuit.library import PauliEvolutionGate
from qiskit.quantum_info import SparsePauliOp
from qiskit.synthesis import LieTrotter
from qiskit.primitives import StatevectorEstimator

J, h, t, n = 1.0, 1.0, 2.0, 20
H = SparsePauliOp.from_sparse_list(
    [("ZZ", [0, 1], J), ("ZZ", [1, 2], J),
     ("X", [0], h), ("X", [1], h), ("X", [2], h)], num_qubits=3)
qc = QuantumCircuit(3)
qc.append(PauliEvolutionGate(H, time=t, synthesis=LieTrotter(reps=n)), range(3))

mz = SparsePauliOp.from_sparse_list([("Z", [i], 1/3) for i in range(3)], 3)
print(StatevectorEstimator().run([(qc, mz)]).result()[0].data.evs)
```

07

Noise

Real qubits are open systems. Errors are the rule, not the exception.

NOISE · SOURCES

Where errors come from

Decoherence

Energy relaxation (T_1: $|1\rangle$ decays to $|0\rangle$) and dephasing (T_2: the relative phase randomizes).

Control errors

Miscalibrated pulses over- or under-rotate; frequencies drift over time.

Crosstalk & leakage

Driving one qubit disturbs its neighbours; population escapes to $|2\rangle$.

Readout errors

A 0 is recorded as 1 or vice versa, typically around a percent.

Good two-qubit gates today fail roughly once in a few hundred to a few thousand uses. A 1,000-gate circuit almost certainly contains errors.

NOISE · MODEL

Stochastic Pauli noise: the simplest error model

THE MODEL

After each gate, independently at random:

apply X with probability p_X, Y with p_Y, Z with p_Z
— otherwise nothing.

We now know only a probability mixture, described by a density matrix $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$:

$$\rho \;\to\; (1-p)\,\rho + p_X X\rho X + p_Y Y\rho Y + p_Z Z\rho Z$$

with $p = p_X + p_Y + p_Z$.

Bit flip

X with probability p

r_y, r_z shrink by $1 - 2p$

Phase flip

Z with probability p

r_x, r_y shrink by $1 - 2p$

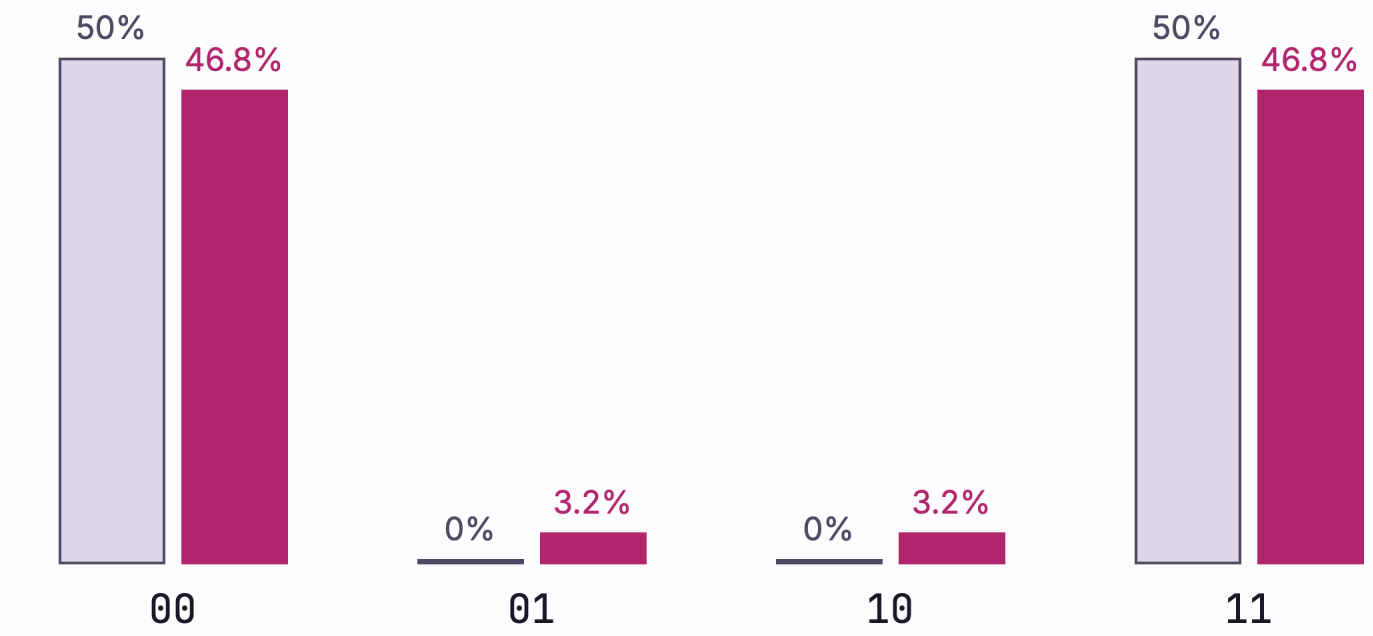
Depolarizing

X, Y, Z each with $p/3$

whole sphere shrinks by $1 - \frac{4p}{3}$

NOISE · EFFECT

Noise on a Bell pair



WHAT THE COUNTS SHOW

X or Y
errors flip a Z outcome: each qubit flips with
$q = 2p/3$.

Mismatch probability
$2q(1-q) \approx 6.4\%$
→ the stray 01 and 10.

Z
errors are invisible in these counts — measure in the X basis too to catch them.

NOISE · WHY PAULI?

Why the Pauli model is the workhorse

Tailor it

Pauli twirling (randomized compiling) turns general gate noise into Pauli noise — Qiskit Runtime can do this for you.

Simulate it

Pauli errors in Clifford circuits can be sampled efficiently on a classical computer.

Correct it

Paulis span every operator, so codes that fix X and Z errors fix any error: errors become digital.

Mitigate it

Learn the Pauli noise, then cancel its bias (PEC) or extrapolate it to zero (ZNE).

NOISE · OUTLOOK

From mitigation to error correction

3-QUBIT REPETITION CODE

$$|0\rangle \to |000\rangle, \qquad |1\rangle \to |111\rangle$$

Measure parities Z_0Z_1 and Z_1Z_2
(via an extra qubit) to locate a single bit flip without disturbing the encoded state.

Failure: $3p^2 - 2p^3$ instead of p. At $p = 1\%$: $\approx 0.03\%$.

SCALING UP

Protect against X **and** Z with surface codes and quantum LDPC codes (IBM's roadmap uses bivariate-bicycle codes).

Below a threshold error rate, adding qubits makes logical errors shrink exponentially.

That is the road from today's noisy devices to running Shor.

RECAP

Six things to remember

1. States are unit vectors, gates are unitaries, measurement is a probabilistic projection.
2. n qubits $\leftrightarrow$ 2^n amplitudes: the source of power and of difficulty.
3. Think of matrices as numbers: projectors ~ {0, 1}, unitaries ~ unit circle, Hermitian ~ real line.
4. Entanglement + measurement + two classical bits = teleportation.
5. Simulation: write H in Pauli strings, exponentiate, Trotterize.
6. Noise is real; Pauli noise is the model to know; error correction is the way out.

Thank you — questions?

LEARN

- IBM Quantum Platform: Qiskit documentation and Learning courses
- Nielsen & Chuang, *Quantum Computation and Quantum Information*
- Sheldon Axler, *Linear Algebra Done Right*
- John Preskill, Ph219 lecture notes (Caltech)

BUILD THIS WEEK

Hackathon: November 9–16 · teams of up to 5 (solo welcome)

Warm-ups: run the Bell pair on hardware; add feed-forward to teleportation; Trotterize the Ising chain and compare with exact results.

`neerpatel125.github.io/UCF-Qiskit-Fall-Fest`

Sumeet Shirgure `sumeetparameshwar.shirgure@ucf.edu`