Category Theory for Quantum Computing

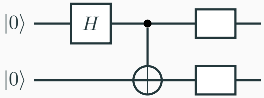
The Language Behind Diagrammatic Reasoning

Prerequisites for ZX-Calculus and Diagrammatic Reasoning

March 31, 2026

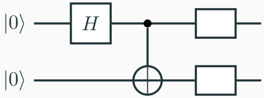
You Already Think Categorically

- When you compose gates in sequence, you use a category.



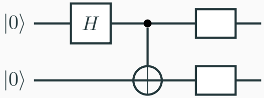
You Already Think Categorically

- When you compose gates in sequence, you use a category.
- When you put qubits side by side with $\otimes$, you use a monoidal category.



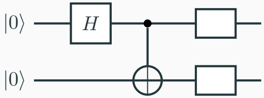
You Already Think Categorically

- When you compose gates in sequence, you use a category.
- When you put qubits side by side with $\otimes$, you use a monoidal category.
- When you draw a quantum circuit, you draw a string diagram.



You Already Think Categorically

- When you compose gates in sequence, you use a category.
- When you put qubits side by side with $\otimes$, you use a monoidal category.
- When you draw a quantum circuit, you draw a string diagram.



This talk gives names to what you already do — and shows why the names have teeth.

Categories

Composing Gates in Sequence

$$\mathbb{C}^2 \xrightarrow{H} \mathbb{C}^2 \xrightarrow{T} \mathbb{C}^2$$

Gate $H : \mathbb{C}^2 \to \mathbb{C}^2$ followed by $T : \mathbb{C}^2 \to \mathbb{C}^2$ gives $T \circ H$.

Two properties you always use:

- *Associative*: $(f \circ g) \circ h = f \circ (g \circ h)$
- *Identity*: the "do nothing" wire I satisfies $g \circ I = g = I \circ g$

These are the entire definition of a category.

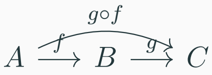
What Is a Category?

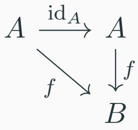
Definition (Category)

A *category* $\mathcal{C}$ consists of:

1. A collection of *objects* $\mathrm{ob}(\mathcal{C})$
2. *Morphisms* $f\colon A \to B$ between objects
3. A *composition* rule: $g \circ f$ for $A \xrightarrow{f} B \xrightarrow{g} C$
4. An *identity* $\mathrm{id}_A\colon A \to A$ for each object

Subject to *associativity* and *identity laws*.





FdHilb: The Category Where Quantum Computing Lives

The quantum category FdHilb

- *Objects*: finite-dimensional Hilbert spaces $\mathbb{C}^n$
- *Morphisms*: **all** linear maps (not just unitaries!)
- *Composition*: matrix multiplication
- *Identity*: the identity matrix I_n on $\mathbb{C}^n$

Includes gates, states, effects, measurements — everything.

Key insight: A quantum state $|\psi\rangle$ is a morphism $\mathbb{C} \to \mathbb{C}^2$, not a vector.

An effect $\langle\phi|$ is a morphism $\mathbb{C}^2 \to \mathbb{C}$.

Also: $\mathbf{Mat}$ (objects = natural numbers, morphisms = matrices) — the same category with coordinates.

Isomorphisms and Unitaries

Definition (Isomorphism)

A morphism $f\colon A \to B$ is an *isomorphism* if there exists $g\colon B \to A$ with $g \circ f = \mathrm{id}_A$ and $f \circ g = \mathrm{id}_B$. Write $A \cong B$.

In $\mathbf{FdHilb}$: isomorphisms = invertible linear maps.

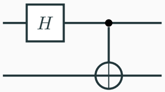
- The Hadamard gate satisfies $H^2 = I$, so H is an isomorphism (with $H^{-1} = H$).
- A measurement projector $|0\rangle\langle 0|$ is a morphism but **not** an isomorphism.

Unitary gates satisfy $U^\dagger U = I$ — they are *special* isomorphisms.

The difference between "invertible" and "unitary" will matter when we add the dagger (§6).

Functors

Same Physics, Different Languages

Circuit	Matrix	Hilbert space
	$\text{CNOT} \cdot (H \otimes I)$ $= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \cdot \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}$	$\mathbb{C}^2 \otimes \mathbb{C}^2 \xrightarrow{H \otimes \mathrm{id}} \mathbb{C}^2 \otimes \mathbb{C}^2 \xrightarrow{\text{CNOT}} \mathbb{C}^2 \otimes \mathbb{C}^2$

Each translation preserves composition and identities.

A structure-preserving map between categories is a functor.

Functors: Structure-Preserving Translations

Definition (Functor)

$F : \mathcal{C} \to \mathcal{D}$ maps objects to objects, morphisms to morphisms, preserving:

- Composition: $F(g \circ f) = F(g) \circ F(f)$
- Identities: $F(\mathrm{id}_A) = \mathrm{id}_{F(A)}$

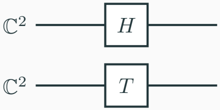
Key examples

- $\dim : \mathbf{FdHilb} \to \mathbf{Mat}$
  (Hilbert space $\mapsto$ dimension, map $\mapsto$ matrix)
- Forgetful: $\mathbf{FdHilb} \to \mathbf{Vect}$
  (forget the inner product)
- $\mathbb{C}[\text{-}] : \mathbf{Set} \to \mathbf{Vect}$
  (classical bits $\{0, 1\} \mapsto$ basis states)

When Qiskit compiles your circuit to a unitary matrix, it is applying a functor.

Monoidal Categories

Parallel Wires = Tensor Product



$$H \otimes T : \mathbb{C}^2 \otimes \mathbb{C}^2 \to \mathbb{C}^2 \otimes \mathbb{C}^2$$

One qubit: $\mathbb{C}^2$. Two qubits: $\mathbb{C}^2 \otimes \mathbb{C}^2 \cong \mathbb{C}^4$.

The tensor product $\otimes$ combines systems in parallel:

- *States*: $|\psi\rangle \otimes |\phi\rangle$ is the joint state
- *Gates*: $U \otimes V$ applies U to first, V to second
- *Wires*: parallel wires = tensor product

We need a category with *two* operations: sequential ($\circ$) and parallel ($\otimes$).

Monoidal Category = Category + Tensor Product

Definition (Monoidal Category)

$(\mathcal{C}, \otimes, I, \alpha, \lambda, \rho)$:

- Bifunctor $\otimes \colon \mathcal{C} \times \mathcal{C} \to \mathcal{C}$
- Unit object I ("empty system")
- Coherence isomorphisms:
  - $(A \otimes B) \otimes C \cong A \otimes (B \otimes C)$
  - $I \otimes A \cong A \cong A \otimes I$

Subject to pentagon + triangle axioms.

Mac Lane's Coherence Theorem

Every monoidal category is equivalent to a strict one.

You never worry about parenthesizing three qubits: $(\mathbb{C}^2 \otimes \mathbb{C}^2) \otimes \mathbb{C}^2 = \mathbb{C}^2 \otimes (\mathbb{C}^2 \otimes \mathbb{C}^2)$.
Coherence says you were right not to!

The Monoidal Unit Gives You States and Scalars

The unit object $I = \mathbb{C}$ is the "no qubit" system. It gives us:

Concept	Morphism	Quantum
State	$\psi\colon I \to A$	$\lvert\psi\rangle\colon \mathbb{C} \to \mathbb{C}^2$
Effect	$\phi\colon A \to I$	$\langle\phi\rvert\colon \mathbb{C}^2 \to \mathbb{C}$
Scalar	$c\colon I \to I$	$\langle\phi\vert\psi\rangle \in \mathbb{C}$

The Born rule:

probability $= \lvert\text{scalar}\rvert^2$

$= \lvert\langle 0\vert H\vert 1\rangle\rvert^2 = \frac{1}{2}$

Aha: A quantum state is not a vector — it is a *morphism from the trivial system*.

FdHilb: Putting It All Together

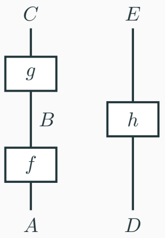
Category theory	FdHilb	Quantum computing
Object	$\mathbb{C}^n$	System of qubits
Morphism $A \to B$	Linear map	Gate / channel
Composition $g \circ f$	Matrix multiplication	Sequential gates
Tensor $A \otimes B$	Tensor product	Parallel wires
Tensor $f \otimes g$	Kronecker product	Parallel gates
Unit I	$\mathbb{C}$	Trivial (no-qubit) system
State $I \to A$	Ket $\|\psi\rangle$	State preparation
Effect $A \to I$	Bra $\langle\phi\|$	Measurement outcome
Scalar $I \to I$	Complex number	Probability amplitude

String Diagrams

Your Circuit Diagrams Are Already String Diagrams

Dictionary

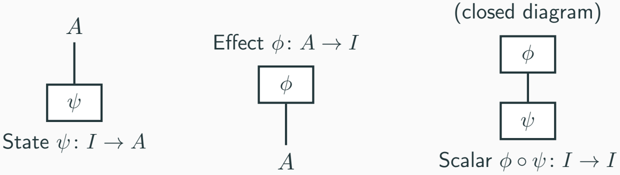
Cat. theory		Diagram
Object A	$\leftrightarrow$	Wire
$f : A \to B$	$\leftrightarrow$	Box
id_A	$\leftrightarrow$	Plain wire
$g \circ f$	$\leftrightarrow$	Vertical stack
$f \otimes g$	$\leftrightarrow$	Side by side
Unit I	$\leftrightarrow$	No wire



$$= (g \circ f) \otimes h$$

Quantum circuit notation is a *special case* of string diagrams, restricted to qubits and unitaries.

States, Effects, and the Born Rule — Diagrammatically

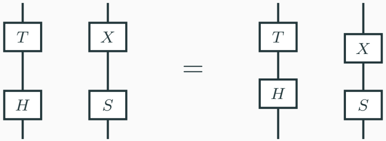


State $|\psi\rangle$: wire out, no input
Effect $\langle\phi|$: wire in, no output

Inner product $\langle\phi|\psi\rangle$:
plug state into effect $\rightarrow$ closed diagram $=$ scalar

The Interchange Law (You Use It Every Day)

$$(g \otimes k) \circ (f \otimes h) = (g \circ f) \otimes (k \circ h)$$



Sliding boxes vertically on *independent wires* does not change the diagram.

This is why the order of gates on *different* qubits does not matter.

Soundness and Completeness: Only the Wiring Matters

Theorem (Joyal–Street)

Two morphisms in a monoidal category are equal if and only if their string diagrams are related by *planar isotopy* (continuous deformation preserving connectivity).

Translation: you can **stretch, bend, and slide** boxes along wires freely.

Only the *connectivity* matters, not the geometry.

Aha: Every time you redraw a circuit to "look cleaner" without changing what it computes, you are applying the Joyal–Street theorem.

This is the mathematical foundation that makes circuit optimization *rigorous*.

Symmetric Monoidal Categories

The SWAP Gate and Braiding

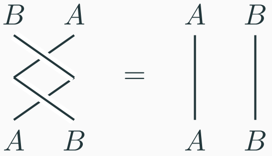
SWAP: $|a\rangle \otimes |b\rangle \mapsto |b\rangle \otimes |a\rangle$

In string diagrams — a *crossing* of wires:

$= \sigma_{A,B}$

Symmetric = swapping twice is identity:

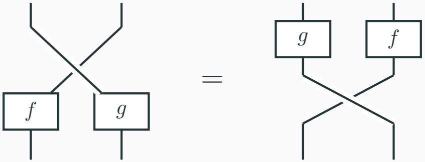
$\sigma_{B,A} \circ \sigma_{A,B} = \mathrm{id}$



$\mathbf{FdHilb}$ is symmetric monoidal. In a *braided* (not symmetric) category, overcrossings $\neq$ undercrossings — like anyons in topological quantum computing.

You Can Slide Gates Through a SWAP

Naturality: $(g \otimes f) \circ \sigma = \sigma \circ (f \otimes g)$



In circuit optimization, moving a single-qubit gate past a SWAP is a standard simplification.

This is the *naturality* of σ.

Dagger Categories

The Dagger (†): What Makes Quantum *Quantum*

Every linear map $f\colon H \to K$ has an adjoint $f^\dagger\colon K \to H$.

Definition (Dagger Category)

A category with an operation † sending $f\colon A \to B$ to $f^\dagger\colon B \to A$:

1. $\mathrm{id}_A^\dagger = \mathrm{id}_A$
2. $(g \circ f)^\dagger = f^\dagger \circ g^\dagger$ (reverses order!)
3. $(f^\dagger)^\dagger = f$ (involutive)

If a circuit runs U_1, U_2, U_3, its adjoint runs $U_3^\dagger, U_2^\dagger, U_1^\dagger$.

This is exactly how you build $U^\dagger$ in practice.

$\mathbf{Set}$ has no canonical dagger — this distinguishes quantum from classical.

Unitaries ($U^\dagger U = I$) and Observables ($H^\dagger = H$)

Unitary morphism

$f^\dagger \circ f = \mathrm{id}_A$ and $f \circ f^\dagger = \mathrm{id}_B$

= quantum gates, norm-preserving

Self-adjoint morphism

$f^\dagger = f$

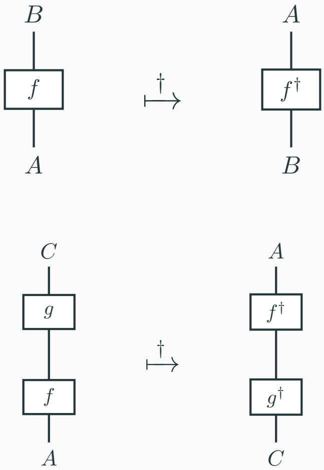
= observables / Hermitian operators

Examples:

- $H^\dagger = H$ (self-adjoint *and* unitary)
- $T^\dagger = \left(\begin{smallmatrix} 1 & 0 \\ 0 & e^{-i\pi/4} \end{smallmatrix}\right) \neq T$ (unitary, not self-adjoint)
- Pauli X, Y, Z: both unitary *and* self-adjoint
- $|0\rangle\langle 0|$: self-adjoint, not unitary

Category theory distinguishes *isomorphism* (has inverse) from *unitary* (inverse = dagger).

The Dagger = Reflect the Diagram



$(g \circ f)^\dagger = f^\dagger \circ g^\dagger$ is *automatic*: reflecting a vertical stack reverses the order.

Compact Closed Categories

Bell States and the Categorical Structure of Entanglement

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

- Creates entanglement from nothing
- Categorically: a **cup** (coevaluation) $\eta\colon I \to A \otimes A^*$

Bell measurement $\langle\Phi^+|$:

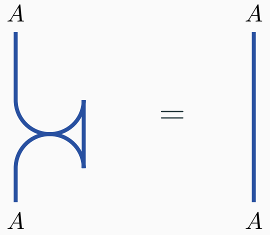
- Consumes entanglement
- Categorically: a **cap** (evaluation) $\varepsilon\colon A^* \otimes A \to I$

Every object having a dual with cups and caps gives a compact closed category.

Snake Equations: Bending Wires Straight

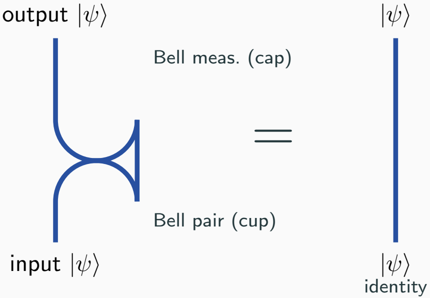
The snake (zig-zag) equations:

$$(\varepsilon \otimes \mathrm{id}) \circ (\mathrm{id} \otimes \eta) = \mathrm{id}_A \qquad (\mathrm{id} \otimes \varepsilon) \circ (\eta \otimes \mathrm{id}) = \mathrm{id}_{A^*}$$



A bent wire can be pulled straight. These are **not** trivial identities — they encode deep physics.

Quantum Teleportation **is** the Snake Equation



The snake equation $(\varepsilon \otimes \mathrm{id}) \circ (\mathrm{id} \otimes \eta) = \mathrm{id}$ is the *proof* that teleportation works.

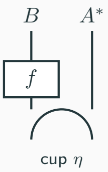
Teleportation is a topological fact: a bent wire can be pulled straight.

Choi–Jamiołkowski: Channels $\leftrightarrow$ States

In a compact closed category:

$$\mathrm{Hom}(A, B) \cong \mathrm{Hom}(I, B \otimes A^*)$$

Every quantum channel $f : A \to B$ corresponds to a bipartite state (its *Choi state*).



$=$ Choi state of f

Construction: feed half a Bell pair through the channel.

Channel tomography — reconstructing f from its Choi state — is a *structural consequence* of compact closure.

Building Up to a Dagger Compact Category

+ Compact Closed	entanglement, teleportation
+ Dagger	adjoint ($\dagger$), unitaries
+ Symmetric	SWAP gate
+ Monoidal	parallel composition ($\otimes$)
Category	sequential composition

FdHilb is a dagger compact category — the natural home of quantum computing.

Each layer captures a distinct physical feature. None is redundant.

Monoids & Comonoids

Copying and Deleting: Where Classical and Quantum Part Ways

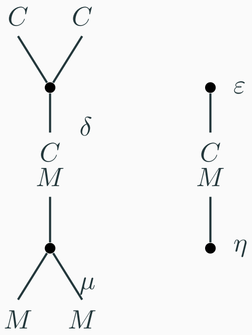
Comonoid on object C

- Copy: $\delta\colon C \to C \otimes C$
- Delete: $\varepsilon\colon C \to I$

Satisfying coassociativity + counitality.

Monoid on object M (dual)

- Merge: $\mu\colon M \otimes M \to M$
- Create: $\eta\colon I \to M$



The CNOT gate (with ancilla $|0\rangle$) IS the comultiplication: $|b\rangle|0\rangle \mapsto |b\rangle|b\rangle$.

No-Cloning = No Universal Comonoid in $\mathbf{FdHilb}$

Theorem (No-Cloning)

There is no linear map $\delta \colon \mathbb{C}^2 \to \mathbb{C}^2 \otimes \mathbb{C}^2$ that copies all states: $\delta(|\psi\rangle) = |\psi\rangle \otimes |\psi\rangle$ for all $|\psi\rangle$.

Proof in one line: if $\delta|0\rangle = |00\rangle$ and $\delta|1\rangle = |11\rangle$, then by linearity:

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

Trying to copy a superposition produces *entanglement*, not a copy!

In $\mathbf{Set}$: $\delta(x) = (x, x)$ copies *everything*.
Every object has a universal comonoid.
$\mathbf{Set}$ is *cartesian* monoidal.

In $\mathbf{FdHilb}$: copying is **basis-dependent**.
$|i\rangle \mapsto |i\rangle \otimes |i\rangle$ works for one basis only.
Each basis $\to$ a different comonoid.

Each Orthonormal Basis → a Frobenius Algebra

For any orthonormal basis $\{|i\rangle\}$, the four operations:

Copy:	$\delta(|i\rangle) = |i\rangle \otimes |i\rangle$	Delete:	$\varepsilon(|i\rangle) = 1$
Merge:	$\mu(|i\rangle \otimes |j\rangle) = \delta_{ij}|i\rangle$	Create:	$\eta(1) = \sum_i |i\rangle$

form a **special commutative Frobenius algebra** (SCFA).

Computational basis $\{|0\rangle, |1\rangle\}$

Z-spider

Hadamard basis $\{|+\rangle, |-\rangle\}$

X-spider

This is the bridge to ZX-calculus: green spiders = computational SCFA, red spiders = Hadamard SCFA.

Looking Ahead

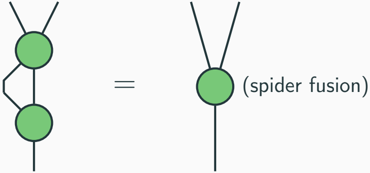
Your New Toolkit

You already knew...	Now you can call it...
Sequential gate composition	Category (morphism composition)
Switching circuit $\leftrightarrow$ matrix	Functor
Tensor product / parallel wires	Monoidal category
Circuit diagrams	String diagrams
SWAP gate	Symmetric braiding
Adjoint / $U^\dagger$	Dagger
Bell states / teleportation	Compact closure (cups, caps, snakes)
Copying classical data / no-cloning	Comonoids / no universal comonoid
Basis-dependent copying	Frobenius algebra

Coming Up Next: The ZX-Calculus

Everything in this talk was the *foundation*. The ZX-calculus builds on it:

- **Spider fusion**: any connected network of same-color spiders fuses into one
- **Bialgebra rule**: governs how Z and X spiders interact
- **Completeness**: *every* equation between quantum circuits can be derived diagrammatically



With today's vocabulary, the ZX rules are not mysterious — they are natural consequences of complementary Frobenius algebras in a dagger compact category.

Why This Matters

1. Category theory is not abstract nonsense imposed on quantum computing. It is the structure that was already there, given a name.

2. String diagrams are not just pictures. They are a rigorous proof system (Joyal–Street), and every deformation is a valid equation.

3. The ZX-calculus turns this into a practical tool: circuit optimization, error correction, compilation — all by diagram rewriting.

You have been doing category theory all along.

Now you know.