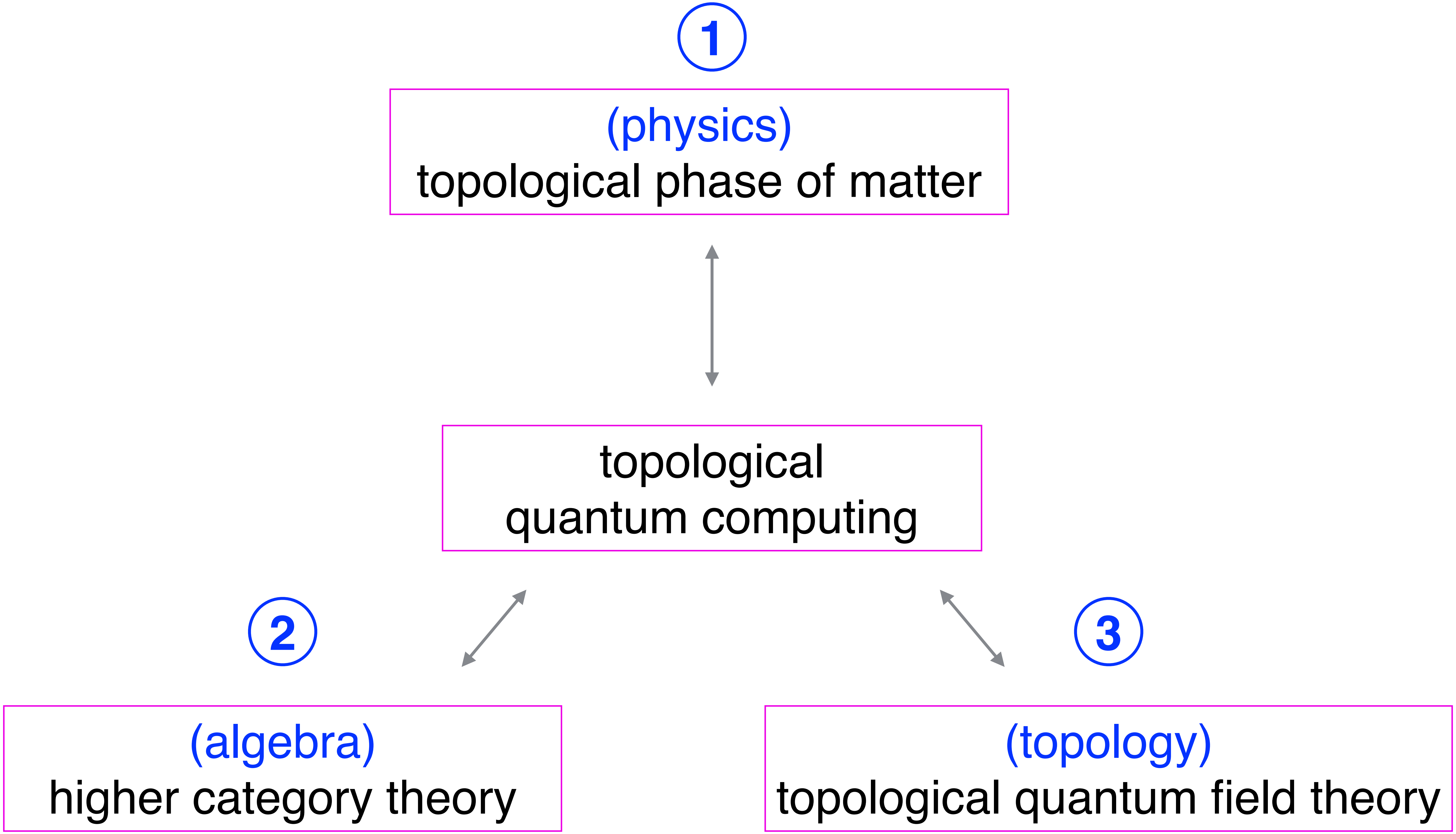
An introduction to Topological Quantum Computing

Shawn Xingshan Cui
Dept. of Mathematics
Dept. of Physics and Astronomy
Purdue University

Mini course for
Algebraic structures in topology 2026

University of Puerto Rico, Río Piedras, July 10-17, 2026


1
(physics)
topological phase of matter
topological
quantum computing
2
(algebra)
higher category theory
3
(topology)
topological quantum field theory

Part III: Outline

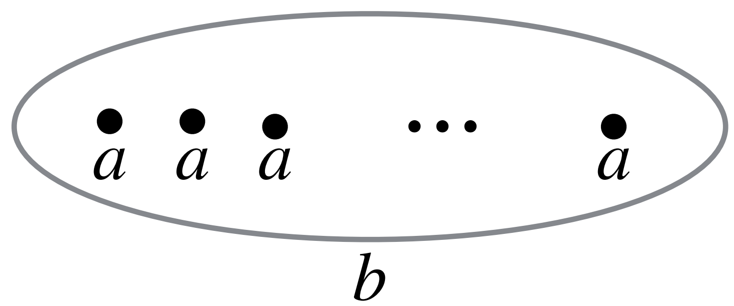
- TQC Setup
- Universality of anyons
- Quantum invariants from anyons

TQC Setup

Fix an anyon system or UMTC $\{L,\ N_{ab}^{c},\ F_{d,ef}^{abc}, R_c^{ba}\}$

★ Qubit spaces and computational bases

$V_c^{a,\cdots,a} \equiv V_b^{a^{\otimes n}}$: space of physical processes of splitting b into n anyons of type a; space of n type-a anyons with total type b

$V_b^{a^{\otimes n}}$ $=$ 

- a must be a non-Abelian anyon

$$\dim V_b^{a^{\otimes n}} \sim (\dim_q a)^n$$

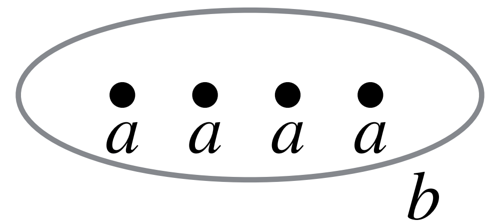
- In general, $V_b^{a^{\otimes n}}$ does not have a tensor product structure. To encode *k* qubits, choose *n* large enough so that

$$(\mathbb{C}^2)^k \hookrightarrow V_b^{a^{\otimes n}}$$

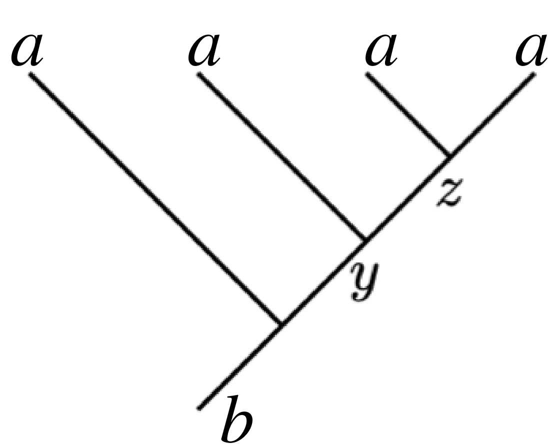
Practically: want a systematic way to choose the embedding

- Choose the `computing' anyon $a$, `total-type' anyon b, and a fixed integer m, such that $V_b^{a^{\otimes m}}$ is the desired qubit/qudit.

e.g. $m = 4$



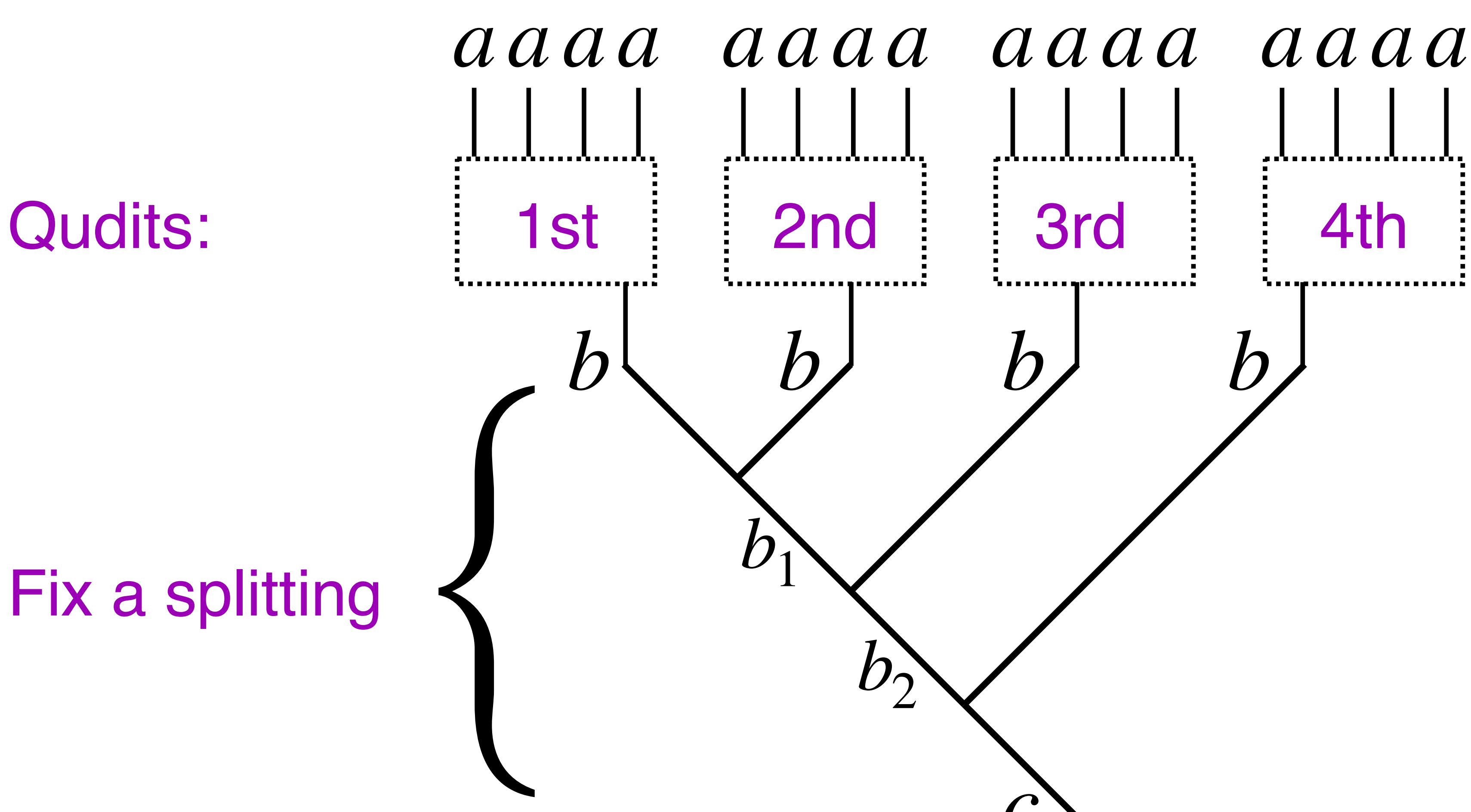
Choose a splitting-tree basis as the computational basis:

$\Bigg\{$ 

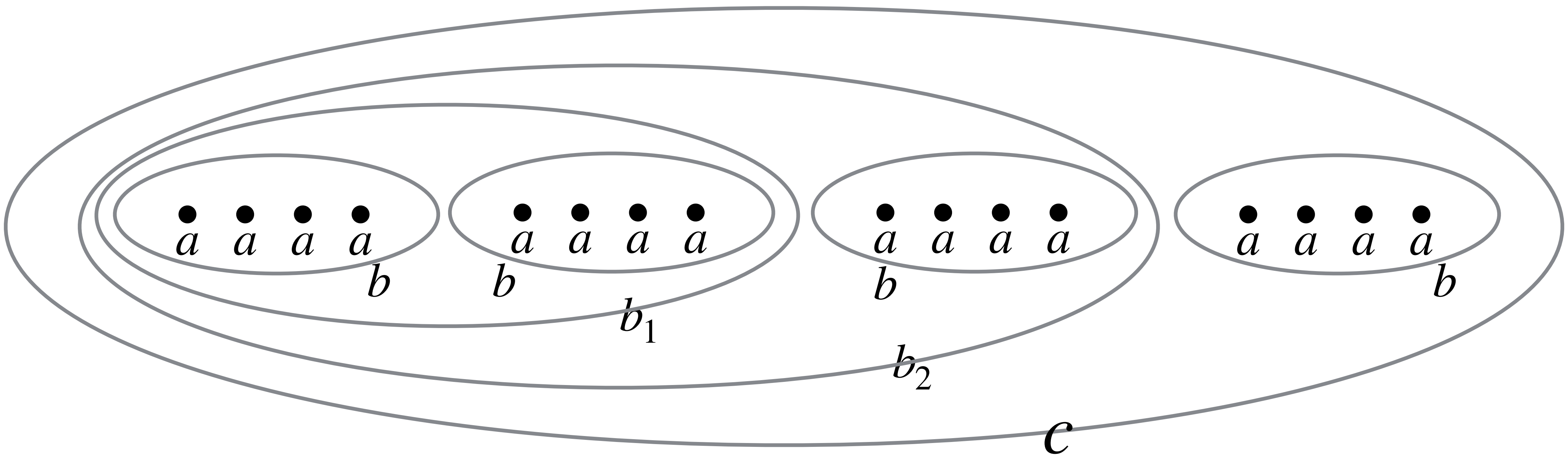
: $(a, a; z), (a, z; y), (a, y; b)$ admissible $\Bigg\}$

- To encode *k* qudits, choose anyon c such that $V_c^{b^{\otimes k}} \neq 0$

$$\underbrace{V_b^{a^{\otimes m}} \otimes \cdots \otimes V_b^{a^{\otimes m}}}_{k} \hookrightarrow V_c^{a^{\otimes mk}}$$



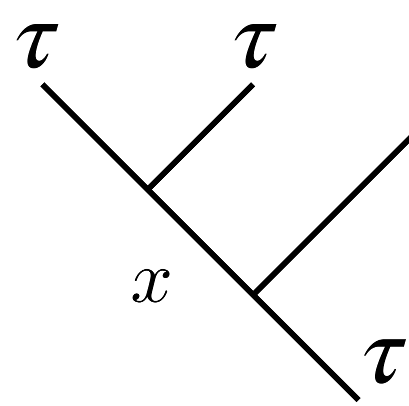
2D picture:



Example: Fib

$$\tau \otimes \tau = \mathbf{1} \oplus \tau$$

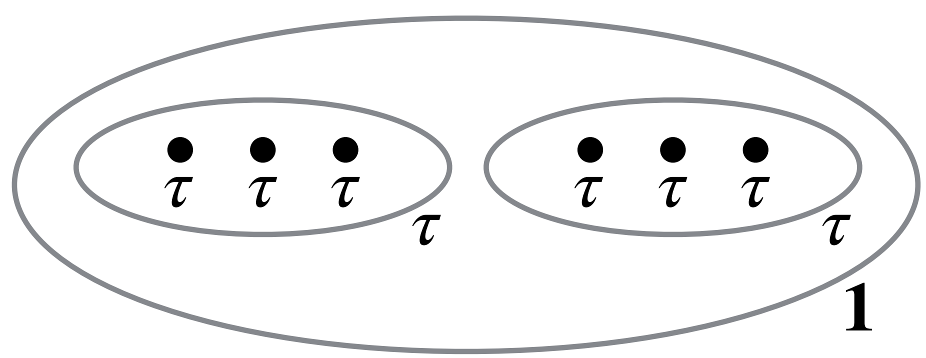
$V_\tau^{\tau\tau\tau}$ has a basis:



$$x = \mathbf{1}, \tau$$

Hence $V_\tau^{\tau\tau\tau}$ is a qubit.

Two qubits: $V_\tau^{\tau^{\otimes 3}} \otimes V_\tau^{\tau^{\otimes 3}} \quad \hookrightarrow \quad V_{\mathbf{1}}^{\tau^{\otimes 6}}$



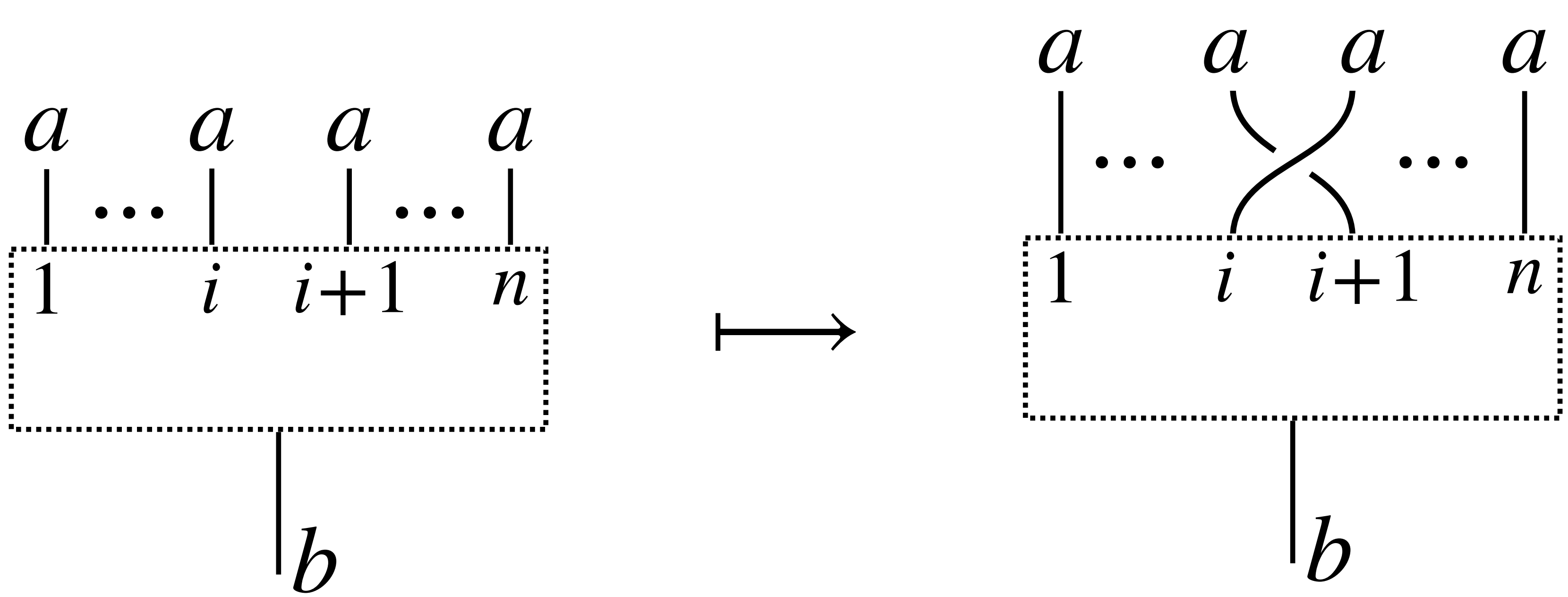
Note $\dim V_\tau^{\tau^{\otimes 6}} = F_5 = 5$

★ Quantum gates from braiding

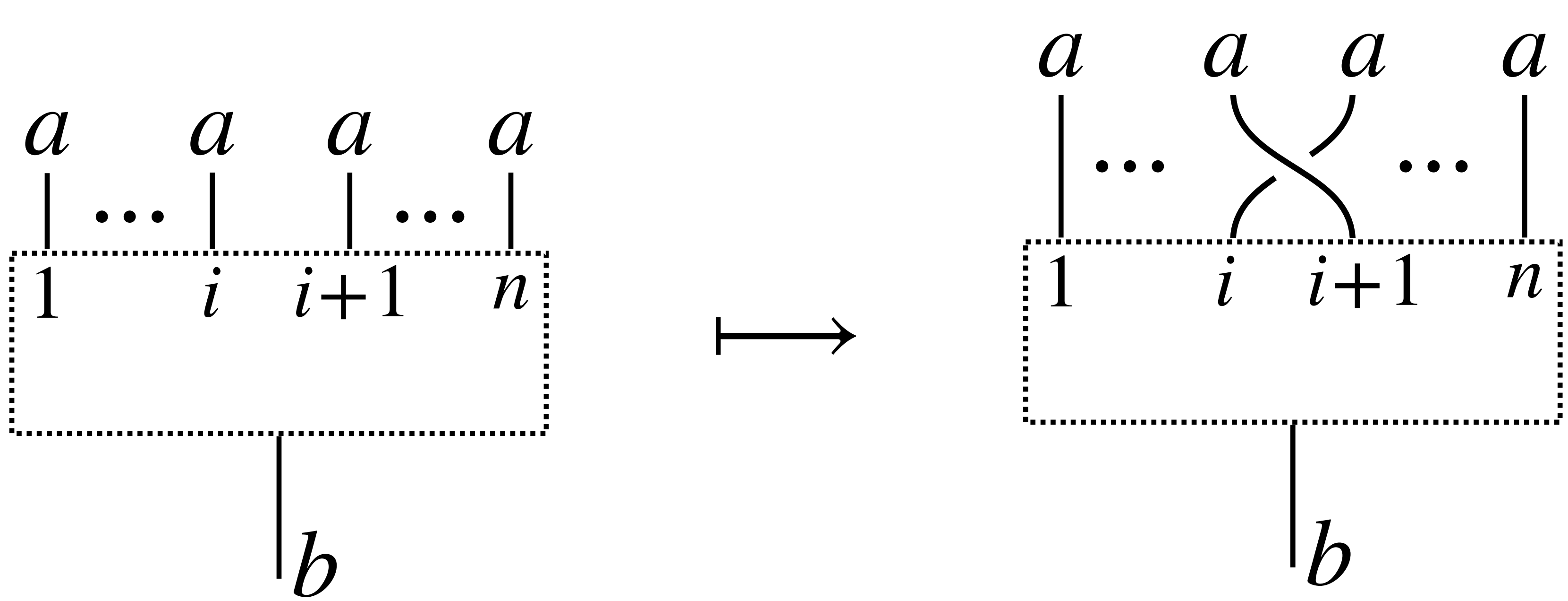
Recall: braiding induces unitary representation of braid groups

$$\rho \equiv \rho_b^{a,n} : B_n \longrightarrow U(\, V_b^{a^{\otimes n}} \,)$$

$\rho(\sigma_i)$:

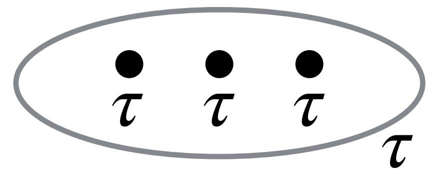


$\rho(\sigma_i^{-1})$:



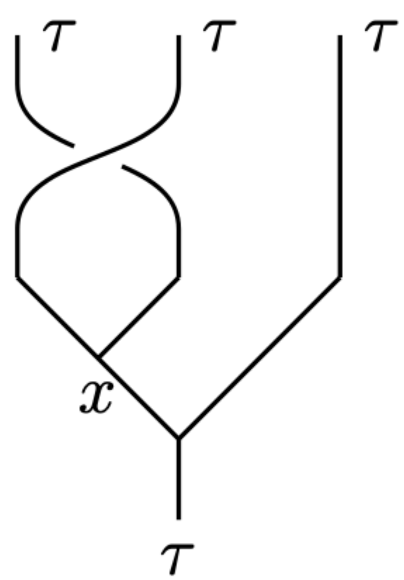
Example: Fib

- 1-qubit gates

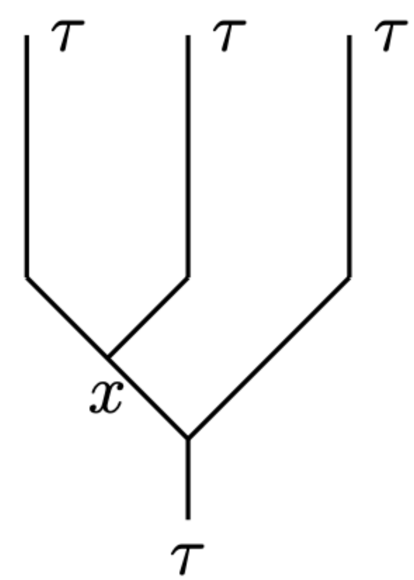


$$\rho : B_3 = \langle \sigma_1, \sigma_2 \rangle \longrightarrow U(\, V_\tau^{\tau^{\otimes 3}} \,)$$

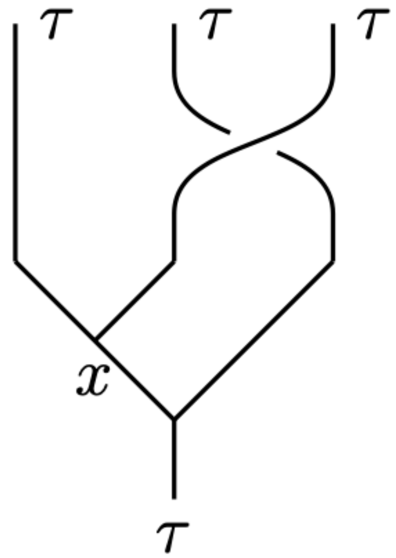
$x = \mathbf{1}, \tau$



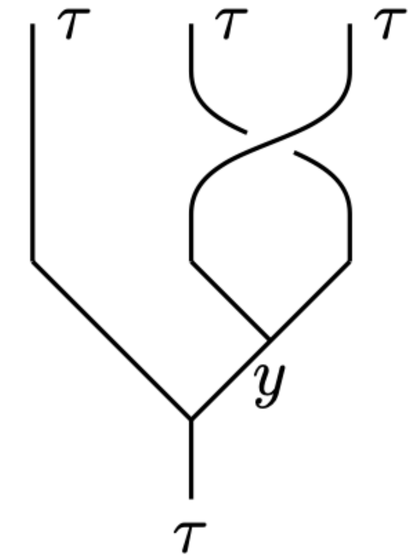
$= R_x^{\tau\tau}$



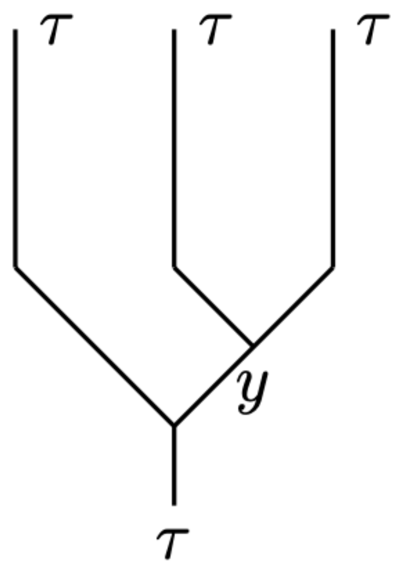
$$\rho(\sigma_1) = \begin{pmatrix} R_{\mathbf{1}}^{\tau\tau} & 0 \\ 0 & R_\tau^{\tau\tau} \end{pmatrix} = \begin{pmatrix} e^{-4\pi i/5} & 0 \\ 0 & e^{3\pi i/5} \end{pmatrix}$$



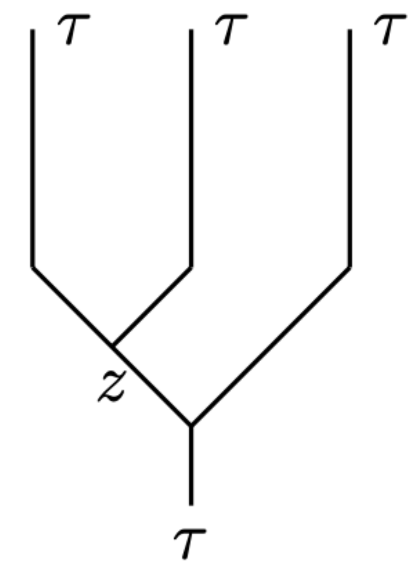
$$= \sum_{y=\mathbf{1},\tau} F^{\tau\tau\tau}_{\tau;yx}$$



$$= \sum_{y=\mathbf{1},\tau} F^{\tau\tau\tau}_{\tau;yx} R^{\tau\tau}_{y}$$



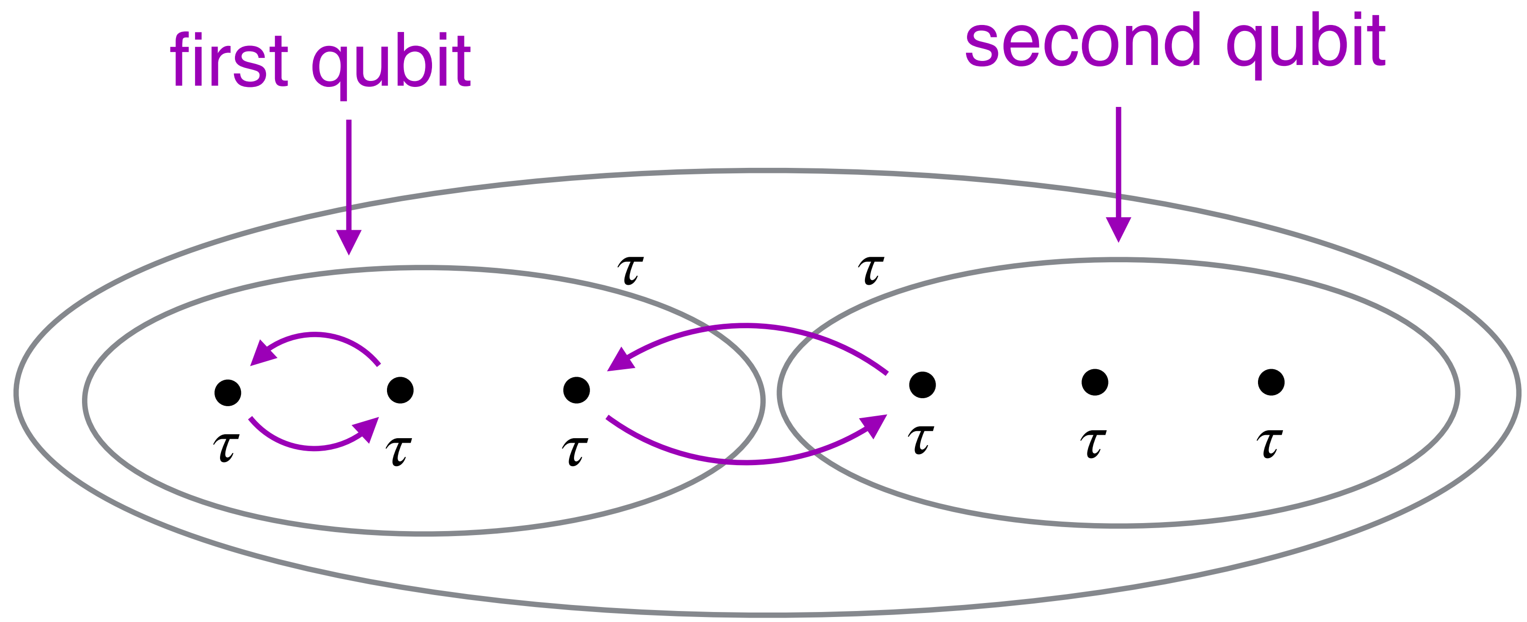
$$= \sum_{y,z=\mathbf{1},\tau} F^{\tau\tau\tau}_{\tau;yx} R^{\tau\tau}_{y} (F^{\tau\tau\tau}_{\tau})^{-1}_{zy}$$



$$\rho(\sigma_2)_{zx} = \sum_{y=\mathbf{1},\tau} F^{\tau\tau\tau}_{\tau;yx}\, R^{\tau\tau}_{y}\, (F^{\tau\tau\tau}_{\tau})^{-1}_{zy}$$

$$\rho(\sigma_2) = (F^{\tau\tau\tau}_{\tau})^{\dagger}\, \rho(\sigma_1)\, F^{\tau\tau\tau}_{\tau}$$

- Multi-qubit gates are computed similarly



2 qubits $\quad V_\tau^{\tau^{\otimes 3}} \otimes V_\tau^{\tau^{\otimes 3}} \subset V_{\mathbf{1}}^{\tau^{\otimes 6}}$

A general braiding acts on $V_{\mathbf{1}}^{\tau^{\otimes 6}}$, not necessarily preserve $V_\tau^{\tau^{\otimes 3}} \otimes V_\tau^{\tau^{\otimes 3}}$

Conjecture

In the above encoding, there is no leakage-free entangling braiding gates.

- A braiding on $V_{\mathbf{1}}^{\tau^{\otimes 6}}$ that preserves $V_\tau^{\tau^{\otimes 3}} \otimes V_\tau^{\tau^{\otimes 3}}$, and
- On $V_\tau^{\tau^{\otimes 3}} \otimes V_\tau^{\tau^{\otimes 3}}$, is not of the form $A \otimes B$ or $\mathrm{SWAP} \circ (A \otimes B)$

Universality of anyons

An anyon a is braiding universal if for some anyon b and for all N large enough, the image of $\mathrm{Im}\,\rho_b^{a,N}$ of the braid group is dense in $U(V_b^{a^{\otimes N}})$.

Theorem (Freedman-Larsen-Wang, 2002)

The τ anyon in Fib is braiding universal.

Theorem (Freedman-Larsen-Wang, 2002)

For the anyon theory SU$(2)_k$ arising from the quantum group $U_q(\mathfrak{sl}_2), \quad q = e^{2\pi i/(k+2)}$, if k is not 0,1,2,4, then the non-Abelian anyons are braiding universal. (Fib $\sim$ SU$(2)_3$)

Property F Conjecture (Naidu-Rowell, 2011)

An anyon has finite braid group image if and only if its quantum dimension squared is an integer. (True for all known cases)

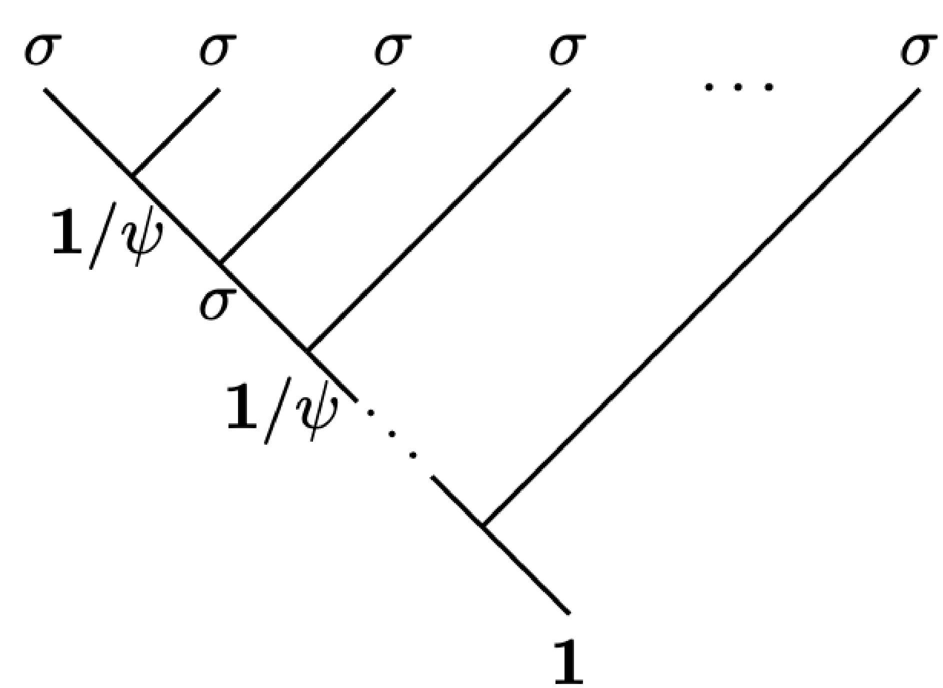
Example: Ising $=$ SU$(2)_2$

- Label set: $L = \{\mathbf{1}, \psi, \sigma\}$; $\bar{a} = a$.
- Fusion rules: $\psi \otimes \psi = \mathbf{1}$, $\psi \otimes \sigma = \sigma$, $\sigma \otimes \sigma = \mathbf{1} \oplus \psi$.
- F-matrices:

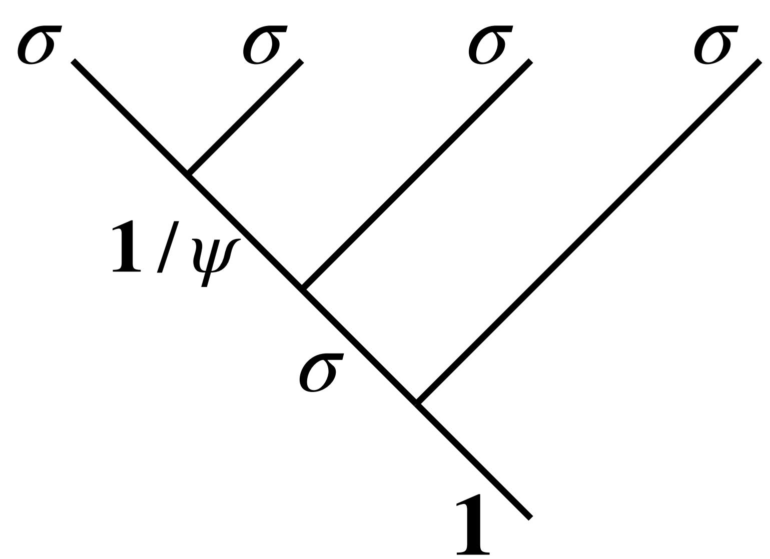
$$F_\sigma^{\sigma\sigma\sigma} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad F_\sigma^{\psi\sigma\psi} = F_\psi^{\sigma\psi\sigma} = (-1).$$

- R-symbols: $R_\mathbf{1}^{\psi\psi} = -1, \quad R_\sigma^{\psi\sigma} = R_\sigma^{\sigma\psi} = -i, \quad R_\mathbf{1}^{\sigma\sigma} = e^{-\pi i/8}, \quad R_\psi^{\sigma\sigma} = e^{3\pi i/8}.$

$\dim V_{\mathbf{1}}^{\sigma^{\otimes 2n}} = 2^{n-1}$, a rare case!



Qubit $V_{\mathbf{1}}^{\sigma\sigma\sigma\sigma}$:



$$\rho(\sigma_1) = \rho(\sigma_3) = e^{-\frac{\pi i}{8}} \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix},$$

$$\rho(\sigma_2) = e^{-\frac{\pi i}{8}} \begin{pmatrix} \frac{1-i}{2} & \frac{1+i}{2} \\ \frac{1+i}{2} & \frac{1-i}{2} \end{pmatrix}$$

Fact: $\mathrm{Im}\,\rho_{\mathbf{1}}^{\sigma,2n}$ is the Clifford group generated by $\{\mathrm{CNOT}, H, P, X\}$

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad P = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \mathrm{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Theorem (Gottesman–Knill)

Quantum gates in the Clifford group can be simulated efficiently on a classical computer.

A quantum computer built from the Ising anyons have no quantum advantage.

Example: SU$(2)_4$

Anyon types $L = \{0,1,2,3,4\}$

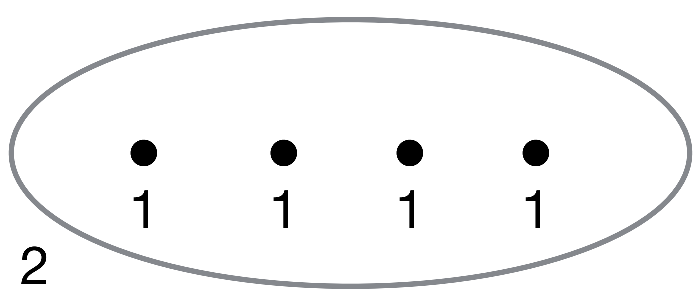
vacuum

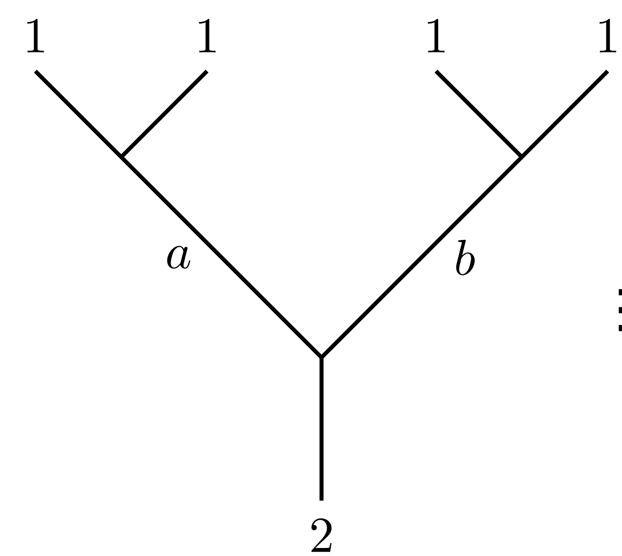
Partial fusion rules:

$$1 \otimes 1 = 0 \oplus 2$$

$$2 \otimes 2 = 0 \oplus 2 \oplus 4$$

- qutrit model



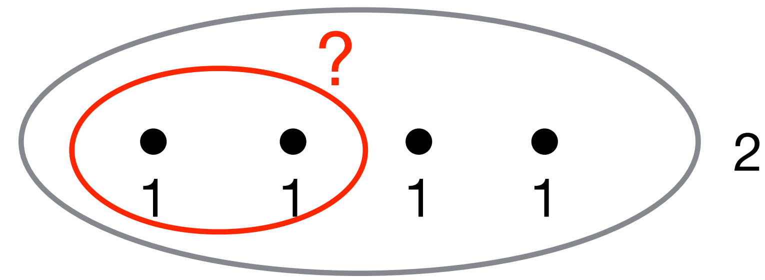


$\equiv |a, b\rangle$

$$(a, b) = (0,2),\ (2,0),\ (2,2)$$

The braid group has finite image — not braiding universal

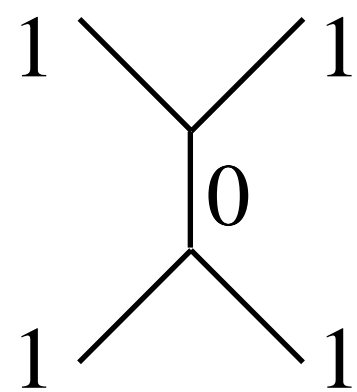
- Measurement of total type



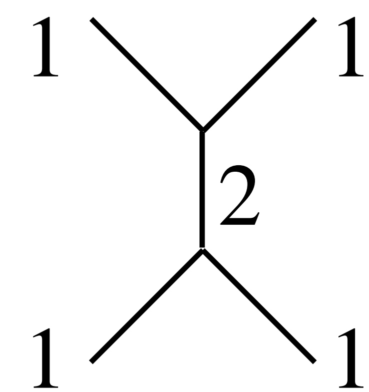
$$1 \otimes 1 = 0 \oplus 2$$

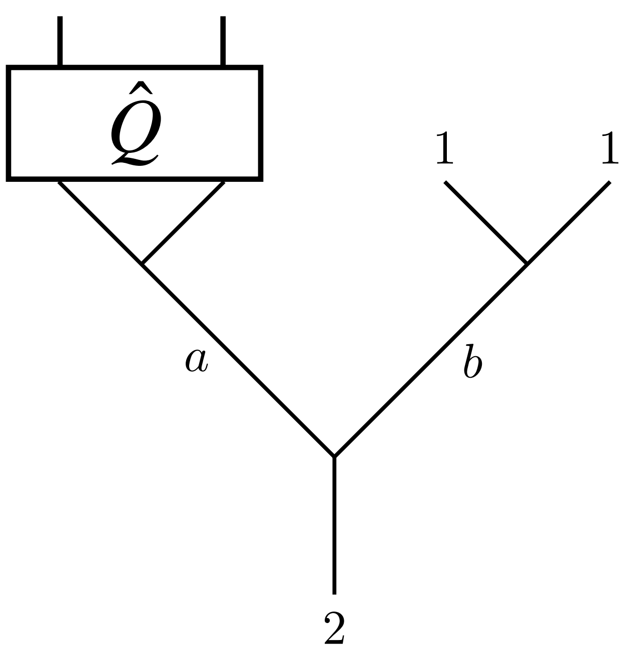
For some $\lambda_0 \neq \lambda_2 \in \mathbb{R}$

$\hat{Q} \;:=\; \lambda_0$

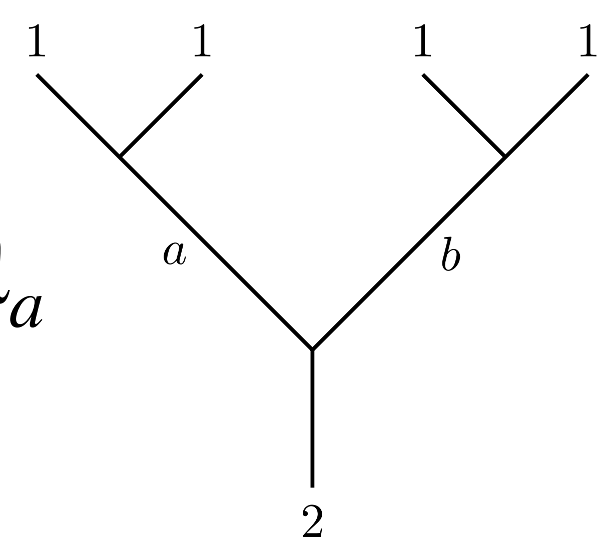


$+ \quad \lambda_2$

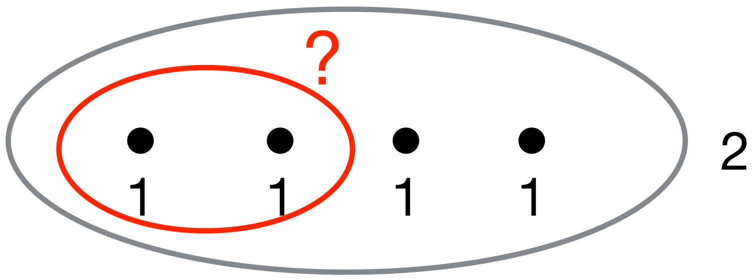




$= \quad \lambda_a$



$(a, b) = (0,2),\ (2,0),\ (2,2)$



Effect of measuring the total type of the two type-1 anyons, i.e. $\hat{Q}$:

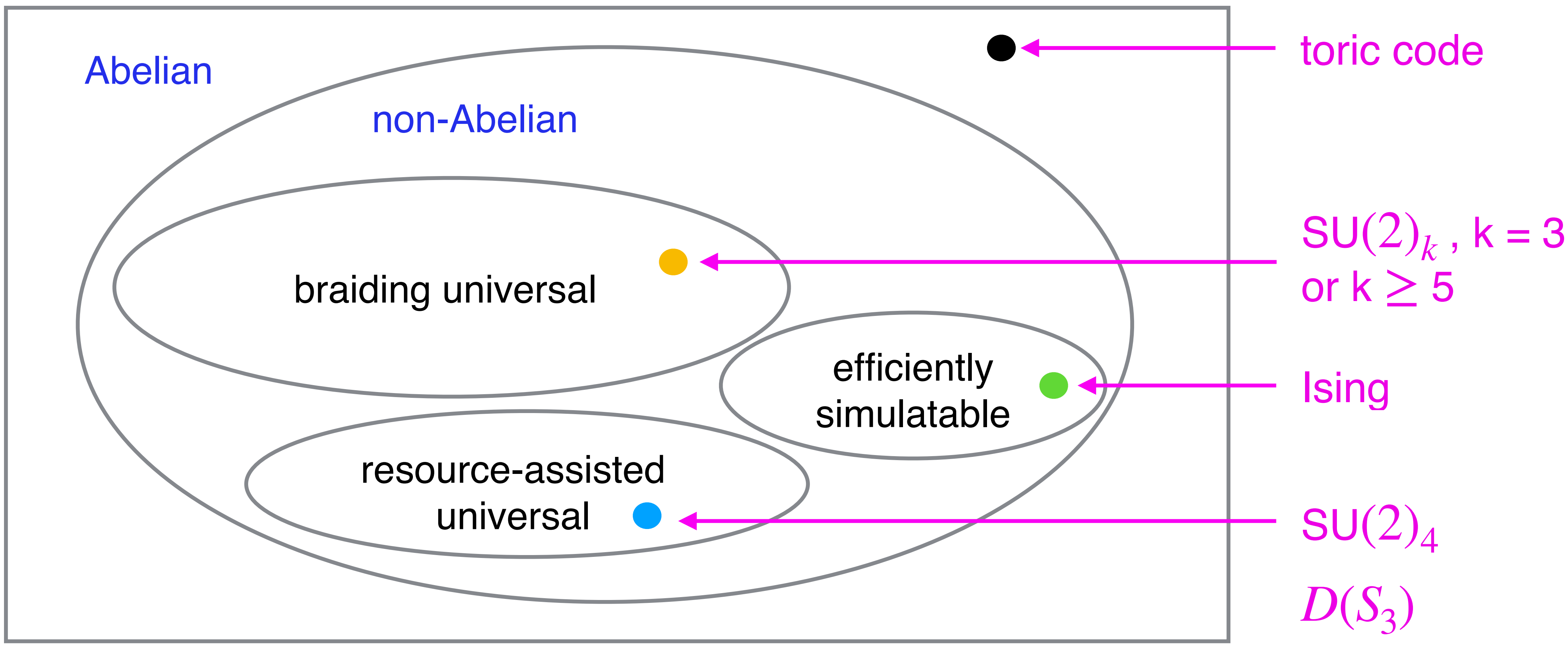
$$\alpha|0,2\rangle + \beta|2,0\rangle + \gamma|2,2\rangle \quad \begin{cases} \nearrow \ |0,2\rangle & \text{Prob} = |\alpha|^2 \\ \searrow \ \dfrac{\beta|2,0\rangle + \gamma|2,2\rangle}{|\beta|^2 + |\gamma|^2} & \text{Prob} = |\beta|^2 + |\gamma|^2 \end{cases}$$

$$|\alpha|^2 + |\beta|^2 + |\gamma|^2 = 1$$

Theorem **(Cui - Wang, '14)**

In $\mathrm{SU}(2)_4$ with the above encoding, braiding supplemented with the measurement of the total type of two anyons, is universal —

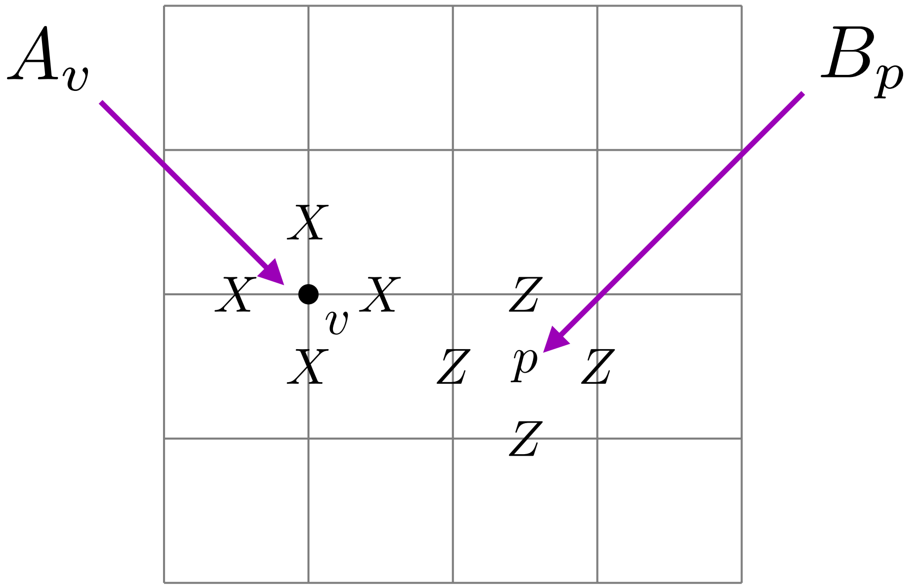
Resource-Assisted Universality



Problem

How to characterize each class of anyons?

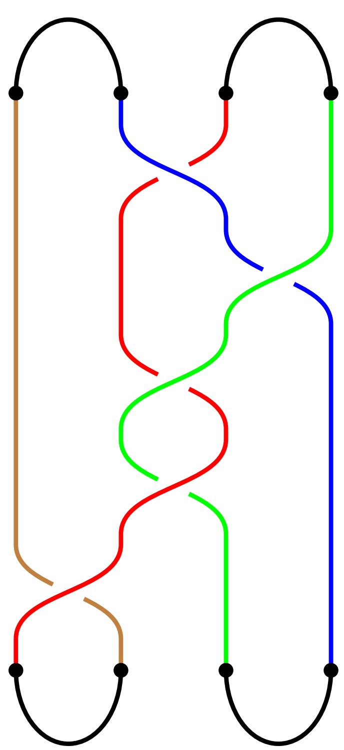
Topological quantum field theory (TQFT)



Put the system on a general surface

$$\Sigma \longmapsto V(\Sigma)$$

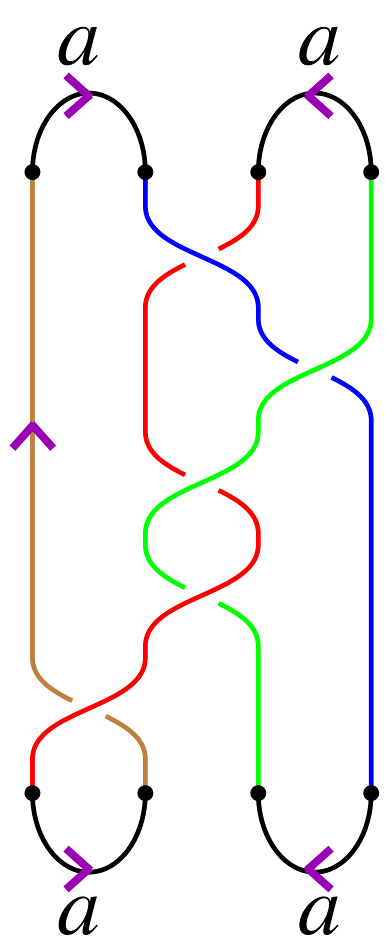
vector space of states



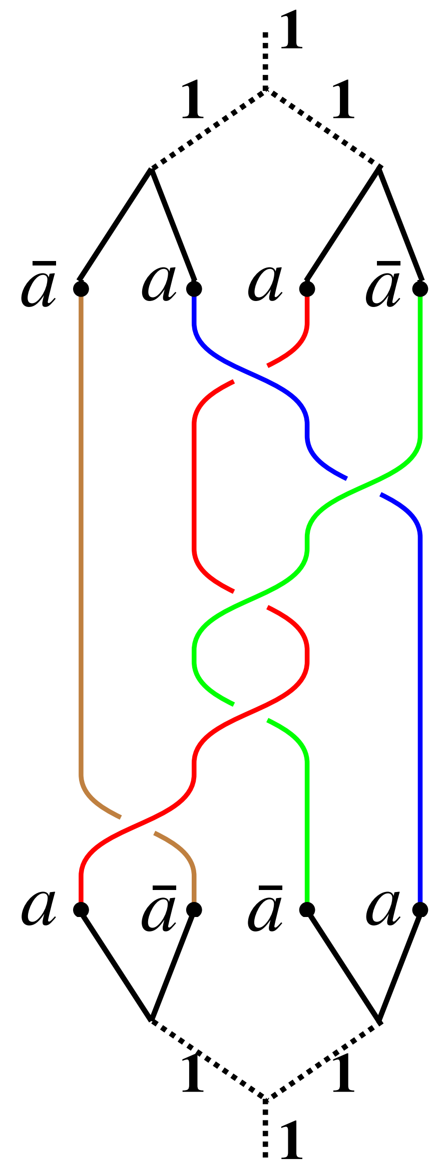
$$(M;K) \longmapsto Z(M;K)$$

Knot in a 3-manifold — Knot invariant

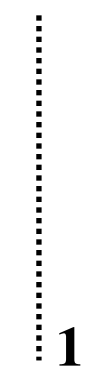
For an oriented knot/link K labelled by anyon a



$=$ $(\dim_q a)^2$



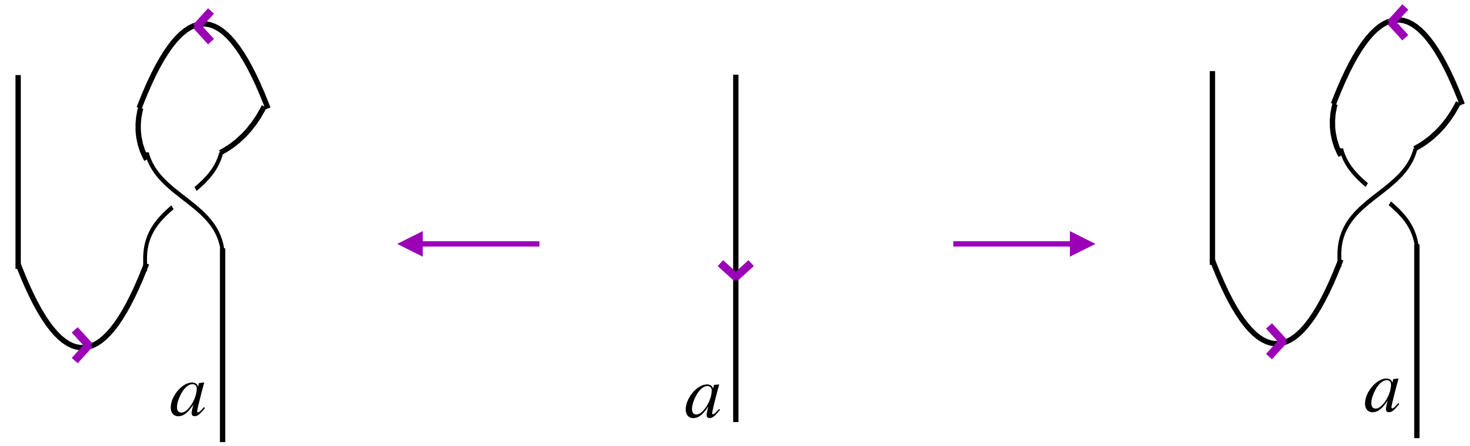
$=: \langle K; a \rangle$



- Can be computed using *F*- and *R*-symbols.
- Invariant under Reidemeister II and III moves.

$\langle K; a \rangle$ is an invariant of framed oriented links — Reshetikhin-Turaev invariant

- Reidemeister I move:



$$\theta_a \langle K;a\rangle \longleftarrow \langle K;a\rangle \longrightarrow \overline{\theta_a}\,\langle K;a\rangle$$

topological twist

Let $lk(K)$ be the linking number of K,

$$J(K;a) := \theta_a^{-lk(K)}\,\langle K;a\rangle$$

is an invariant of un-framed oriented links

Fact: for the Fibonacci anyon, $J(K;\tau)$ is (a version of) of the Jones polynomial of K evaluated at 5-th root of 1.

$\mathsf{Vec}_{\mathbb{C}}$: category of vector spaces

objects: vector spaces, $V_1, V_2, \cdots$

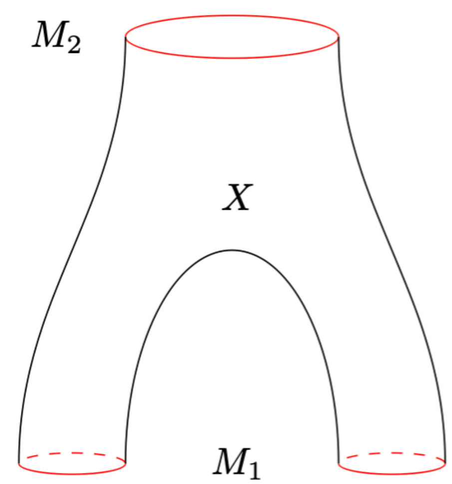
morphisms: linear maps $f : V_1 \to V_2$

$\mathsf{Cob}(d+1)$: category of cobordisms

objects: closed d-dim manifolds, $M_1, M_2, \cdots$

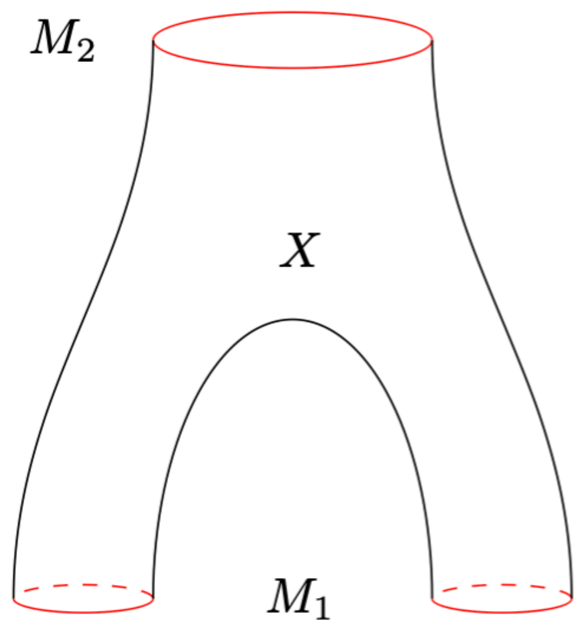
morphisms: $(d+1)$-dim cobordisms $X : M_1 \to M_2$

i.e. $\partial X = M_1 \sqcup M_2$



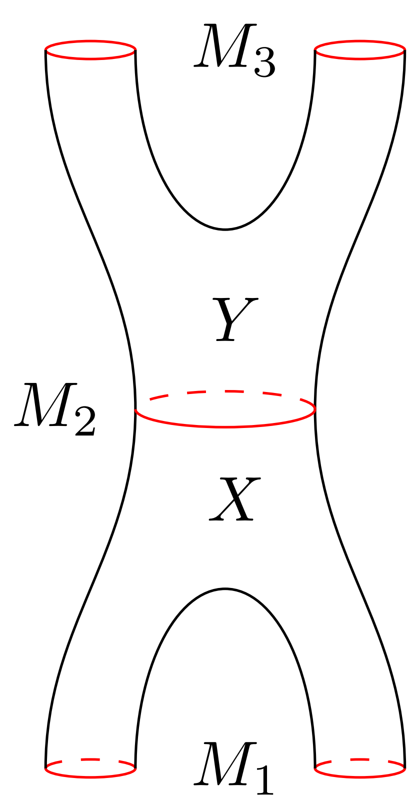
A $(d+1)$-dim topological quantum field theory (TQFT) is a symmetric functor

$$(V, Z) : \mathsf{Cob}(d+1) \ \to \ \mathsf{Vec}_{\mathbb{C}}$$



$$\begin{tikzcd} V(M_2) \\ V(M_1) \arrow[u, "Z(X)"] \end{tikzcd}$$

Subject to (for instance)



$$\begin{tikzcd} V(M_3) \\ V(M_2) \arrow[u, "Z(Y)"] \\ V(M_1) \arrow[u, "Z(X)"] \arrow[uu, bend right, "Z(X \cup_{M_2} Y)"'] \end{tikzcd}$$

- If X is closed, i.e., no boundary,

$$X : \varnothing \to \varnothing,$$

$$Z(X) : \mathbb{C} \to \mathbb{C}, \qquad Z(X) \in \mathbb{C}$$

$Z(\,\cdot\,)$ is an invariant of closed (d+1)-manifolds — quantum invariants

- Given $\phi : M \xrightarrow{\sim} M$, let M_ϕ be the mapping cylinder,

$$M_\phi : M \to M$$

$$Z(M_\phi) : V(M) \to V(M)$$

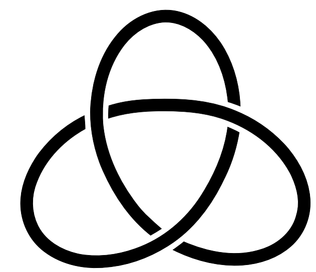
representation of the mapping class group: $\mathrm{MCG}(M) \to \mathrm{GL}(\ V(M)\ )$

$$\phi \quad \mapsto \quad Z(M_\phi)$$

(2+1)-dim TQFTs

Modular tensor category $\mathscr{C}$ $\longrightarrow$ Witten-Reshetikhin-Turaev $Z_{\mathscr{C}}(\,\cdot\,)$

Let *M* be a 3-manifold and *L* be a surgery link for *M*

$$Z_{\mathscr{C}}(M) \;=\; \sum \quad \dim_q(x) \quad \Big\langle$$  $$^{x} \Big\rangle$$

anyon types $x \in \mathscr{C}$ weight Reshetikhin-Turaev invariant

Volume Conjectures (Chen-Yang, '15)

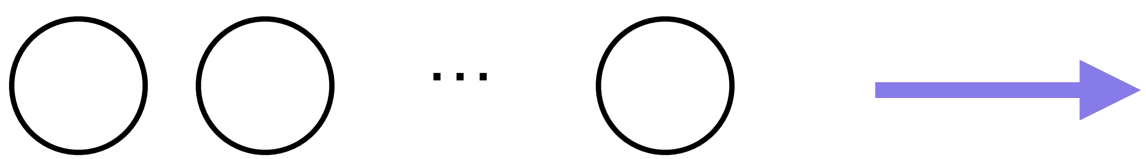
Let $\mathrm{TLJ}(r)$ be the Temperley-Lieb-Jones category with the Kauffman variable $A = e^{\frac{\pi i}{r}}$, *M* be a closed oriented hyperbolic 3-manifold. Then for r odd,

$$\lim_{r\to\infty} \frac{4\pi}{r} \log|Z_{\mathrm{TLJ}(r)}(M)| \;=\; \mathrm{Vol}(M)\,.$$

(3+1)-dimensions

Topological phases of matter:

- Anyons (point-like excitations) can only be fermions/bosons
- More interesting excitations are string-like. Motions of strings lead to representations of the motion groups of links.



N-component unlink

Loop braid group LB_n

$$\langle \sigma_1, \cdots, \sigma_{n-1}, s_1, \cdots s_{n-1} \mid \cdots \rangle$$

Algebraic theories: monoidal/braided 2-categories

Special cases: ribbon fusion categories, group-crossed braided fusion, spherical fusion 2-categories, etc.

(3+1)-TQFTs:

Construct TQFTs to distinguish smooth structures of 4-manifolds.

- Turaev-Viro type based on fusion 2-categories [Douglous-Reutter, ’18]

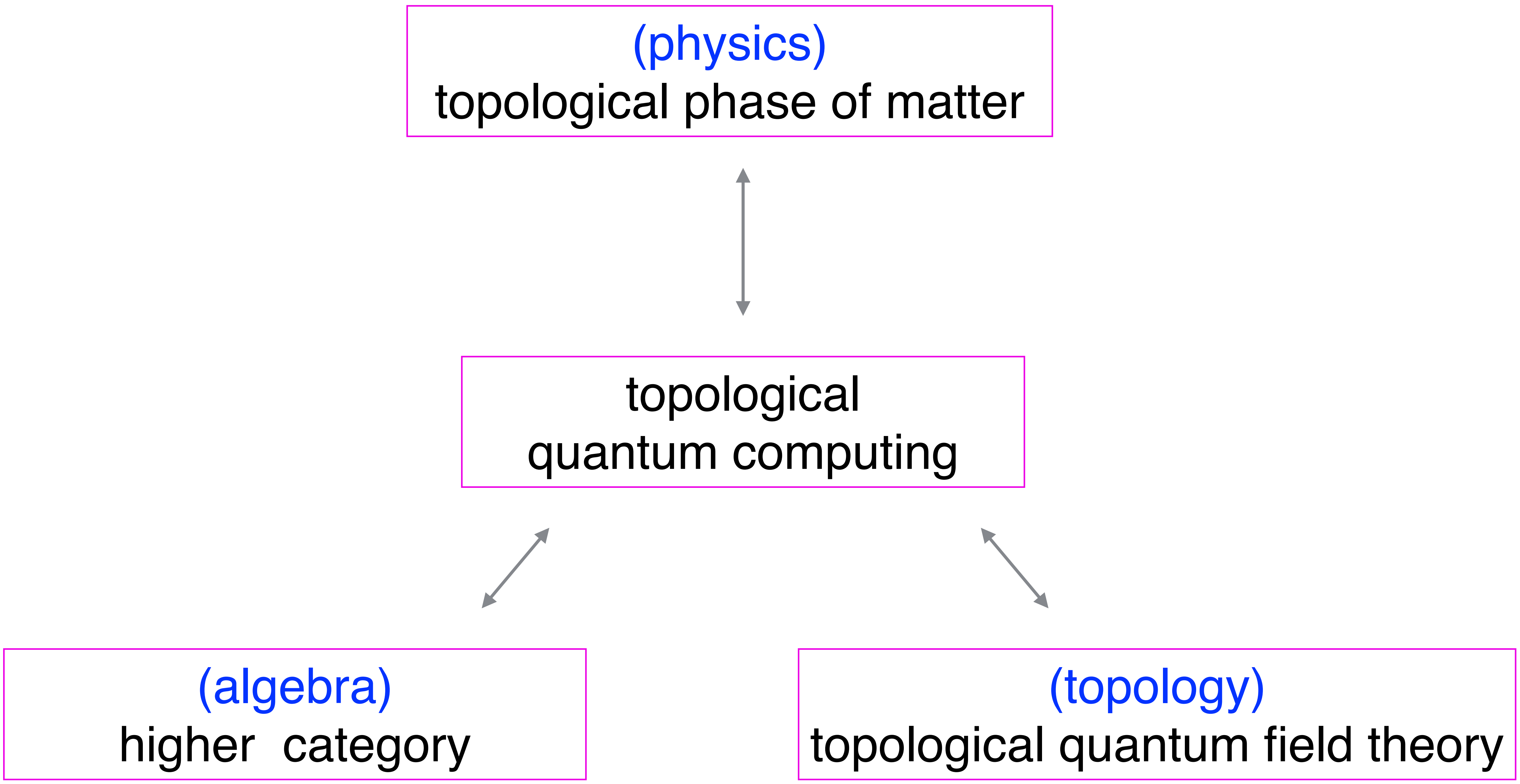
No-go theorem:

Semisimple TQFTs cannot distinguish smooth structures [Reutter, ’20]

Non-semisimple efforts:

- Trisection invariant based on Hopf algebras [Chaidez-Cotler-Cui, ’19, ’23]
- Skein TQFTs from ribbon categories [Costantino-Geer-Haïoun-Patureau-Mirand, ’23]
- Invariants of 4D 2-handlebodies under 2-equivalence from ribbon cats [Beliakova-De Renzi-Faes, ’25; Beliakova-De Renzi, 22’]
- Khovanov homology and skein lasagna modules [Morrison-Walker-Wedrich, ’22; Ren-Willis, '24]

can distinguish smooth structures


(physics)
topological phase of matter
topological
quantum computing
(algebra)
higher category
(topology)
topological quantum field theory