Topological Quantum Computation (TQC)

References:
[Wang; TQC]
[Turaev; Quantum invariants...]
[Bakalov-Kirillov; Lectures on Tensor Cats...]
[arXiv:math/0103200]

1) Quantum Computation

Classically, information is stored, processed and read out using bits.

Bit: $\mathbb{Z}_2 = \{0,1\}$

n-Bit: $\mathbb{Z}_2^n$

Quantum Computation: Qubit $\mathbb{C}^2 = \mathbb{C}[\mathbb{Z}_2]$

w. basis $|0\rangle, |1\rangle$.

n-Qubit $(\mathbb{C}^2)^{\otimes n} = \mathbb{C}[\mathbb{Z}_2^n]$ (n-bits give basis)

A computational problem f is a collection of Boolean maps

$\{f_n : \mathbb{Z}_2^n \to \mathbb{Z}_2^{m(n)}\}$

Examples: Primality, Factoring...

A gate set S is a set consisting of unitary operators $(\mathbb{C}^2)^{\otimes n} \to (\mathbb{C}^2)^{\otimes n}$ for any n. (usually for $n \leq 2$)

Example:

$$\hat{S} = \left\{ \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & e^{\pm i\pi/4} \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \right\}$$

Hadamard matrix — phase gate — CNOT

- An n-quantum circuit over gate set S is a map $U : (\mathbb{C}^2)^{\otimes n} \to (\mathbb{C}^2)^{\otimes n}$ that is a composition of maps of the form $\mathrm{id} \otimes g \otimes \mathrm{id}$, $g \in S$.
- A gate set is called universal if $\{n\text{-qubit circuit}\}$ is dense in $SU(\mathbb{Z}^n)$ $\forall n$.

Example: The gate set $\hat{S}$ is a universal gate set.

To solve a problem f, we would like to have an algorithm which finds us an operator U_x s.t. $U_x|x\rangle = |f(x)\rangle$

Definition: A computational problem $\{f_n : \mathbb{Z}_2^n \to \mathbb{Z}_2^{m(n)}\}$ is in BQP (bounded-error quantum polynomial time) if there exist polynomials $a(n), g(n) \in \mathbb{N}$ (ancilla, garbage) s.t. $n + a(n) = m(n) + g(n)$ and a classical efficient algorithm that gives bit string $S(n)$ encoding a unitary operator $U_{S(n)}$ s.t.:

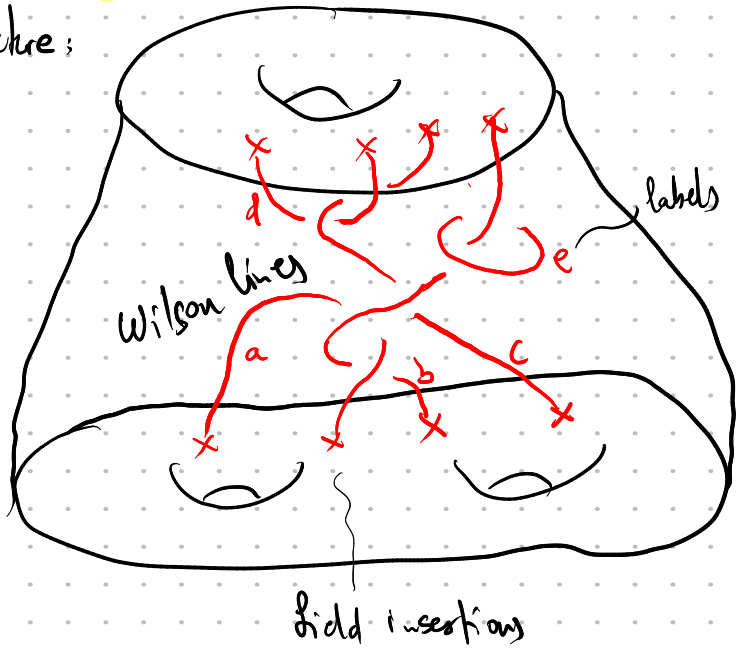
$$U_{S(n)}|x, 0^{a(n)}\rangle =: \sum_y a_y |y\rangle$$

$$\sum_{y = f(x)z} |a_y|^2 \geq 3/4 \qquad (z \in \mathbb{Z}_2^{g(n)})$$

Example:
- Factoring is in BQP (Shor's algorithm)
- Approximation of Jones polynomials at certain roots of unity is in BQP.

2) Modular functors

TQFT picture:



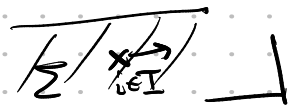
(In Reshetikhin-Turaev labels are given by objects in the associated modular category $\mathcal{C}$)

Def: A label set is a finite pointed set $(I, 0)$ together with an involution map $\hat{(\,)} : I \to I; i \mapsto \hat{i}$ s.t. $\hat{0} = 0$.

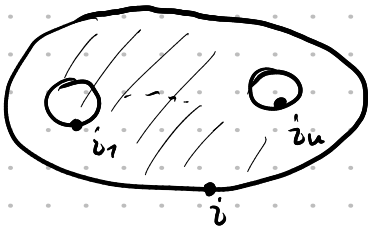
(**Example:** The isomorphism classes of a fusion category form a label set w. $0 = [\mathbb{1}]$ and involution by duals.)

Def: A labeled surface is a oriented compact surface Σ w. boundary s.t. each boundary component has a marked point and is labeled by an element in I (and a Lagrangian subsp. $\lambda \subset H_1(\Sigma; \mathbb{R})$).

Equivalently,



Example: $E(i; i_1, \dots, i_n) \equiv$



planar surface

Def: A modular functor w. label set I is a symmetric monoidal functor $V : \mathrm{Mod}(I) \to \mathrm{Vect}_\phi$

$$\left[\begin{array}{c}\Sigma \\ \text{labeled} \\ \text{surface}\end{array}\right] \longmapsto \begin{array}{c}V(\Sigma) \\ \text{fin dim} \\ \text{vec. sp.}\end{array} \quad \text{"state space"}$$

$$[f : \Sigma \xrightarrow{\sim} \Sigma'] \mapsto V(f) : V(\Sigma) \xrightarrow{\sim} V(\Sigma')$$

s.t. $V(fg) = V(f) \circ V(g)$ etc]

s.t. 1) (Disk axiom) $V\left(\right.$  $\left.\right) \cong \begin{cases} \phi, & i = 0 \\ 0, & \text{else} \end{cases}$

2) (Annulus axiom) $V\left(\right.$  $\left.\right) \cong \begin{cases} \phi, & i = \hat{j} \\ 0, & \text{else} \end{cases}$

3) (Self-dual axiom) $\exists$ non-deg bil. pairing $d_\Sigma : V(\Sigma) \times V(-\Sigma) \to \phi$ natural, compatible w. rest.

4) (Gluing Axiom)

Let γ be a pointed simple closed curve in Σ.

Define $\Sigma^\gamma := \overline{\Sigma \setminus \gamma}$ to be the cut surface.

Gluing isomorphism:

$$V(\Sigma) \xrightarrow{\sim} \bigoplus_{i \in I} V(\Sigma^\gamma; \hat{i}, i)$$

satisfying conditions...

A modular functor encodes (projective) representations of the mapping class group.

- A unitary modular functor is a modular functor, where each state space is equipped w. positive def. Hermitian form $\langle , \rangle_\Sigma : V(\Sigma) \times V(\Sigma) \to \mathbb{C}$ natural and compatible w. the other axioms.

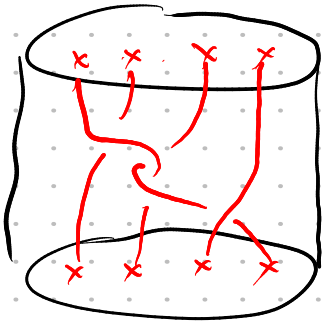
  $\rightsquigarrow$ Unitary representations of the mapping class group. (In particular representations of the braid group B_n)

Fix a label $i \in I$. Define:

$$V_n^j := V(E(j; i, \dots, i))$$

Then, $B_n \curvearrowright V_n^j$

TQFT picture



To use Topological quantum Computation, one wants to implement quantum circuits using the modular functor.

Idea: Given a quantum circuit $U : (\mathbb{C}^2)^{\otimes n} \to (\mathbb{C}^2)^{\otimes n}$, find a braid $b \in B_n$ s.t.

$$\begin{array}{ccc} (\mathbb{C}^2)^{\otimes n} & \hookrightarrow & V_n^d \\ \downarrow U & & \downarrow V(b) \\ (\mathbb{C}^2)^{\otimes n} & \hookrightarrow & V_n^d \end{array} \quad \text{"commutes"}$$

Universality: Find braids implementing a universal gate set efficiently.

$\rightsquigarrow$ Braid group reps have dense image in $SU(V_n^d)$

Example
- Fibonacci Computer is universal.
  [label set $I = \{1, \tau\}$
- Kitaev's toric code is not universal.