# Meeting 13.2 TQC and 3-manifold invariants

I. "Accept probability of circuit" = "Normalized quantum invariant"

II. Approximating quantum invariants w/ quantum computers

IPAM Summer School (UCLA) on Mathematics of Topological Phases
8/29 - 9/3

http://www.ipam.ucla.edu/programs/summer-schools/graduate-summer-school-mathematics-of-topological-phases-of-matter/

Deadline: 5/29

# Lightning review of last time

Given:

- extended unitary (2+1)-dim TQFT $Z$
- a "self-dual color" $X$ (secretly, a self-dual object in unitary modular tensor category determined by $Z$)
- two planar matchings $T, S$ of $2k$ points

such that:

- quantum representation

$$Z : B_{4k} \longrightarrow U(Z(4k; X, 1))$$

has dense image

- $|T\rangle, |S\rangle$ linearly independent in $Z(2k; X, 1)$

then:

can "lift" quantum circuit $C$ (over favorite universal gate set) acting on $n$ qubits to a braid diagram $b_C \in B_{2nk}$ such that $b_C$ acts on subspace

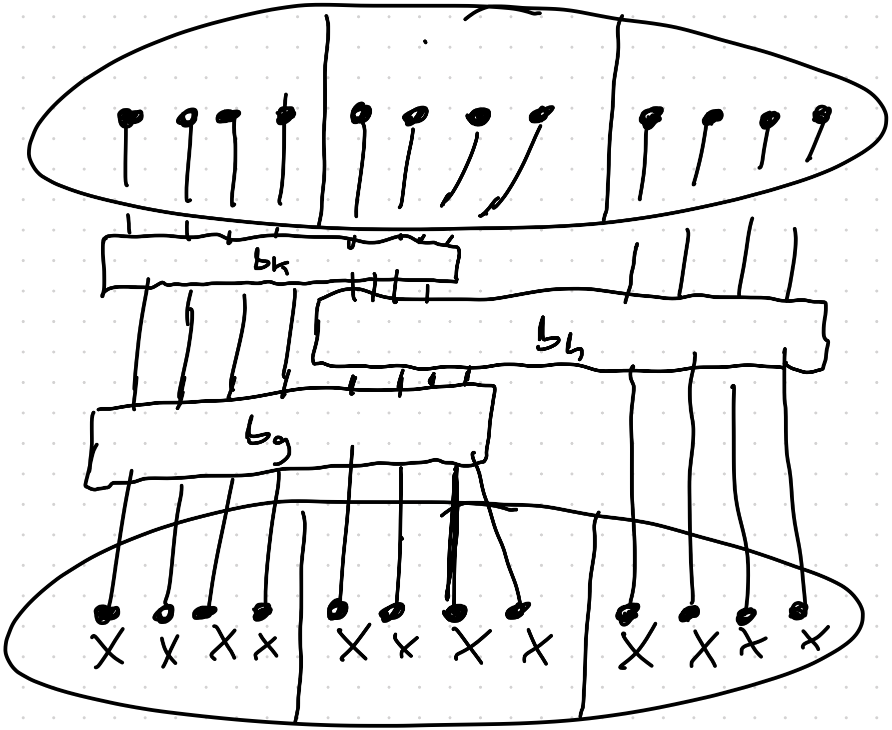
$$\underbrace{H_k \otimes H_k \otimes \cdots \otimes H_k}_{n} \subseteq Z(2nk; X, 1),$$

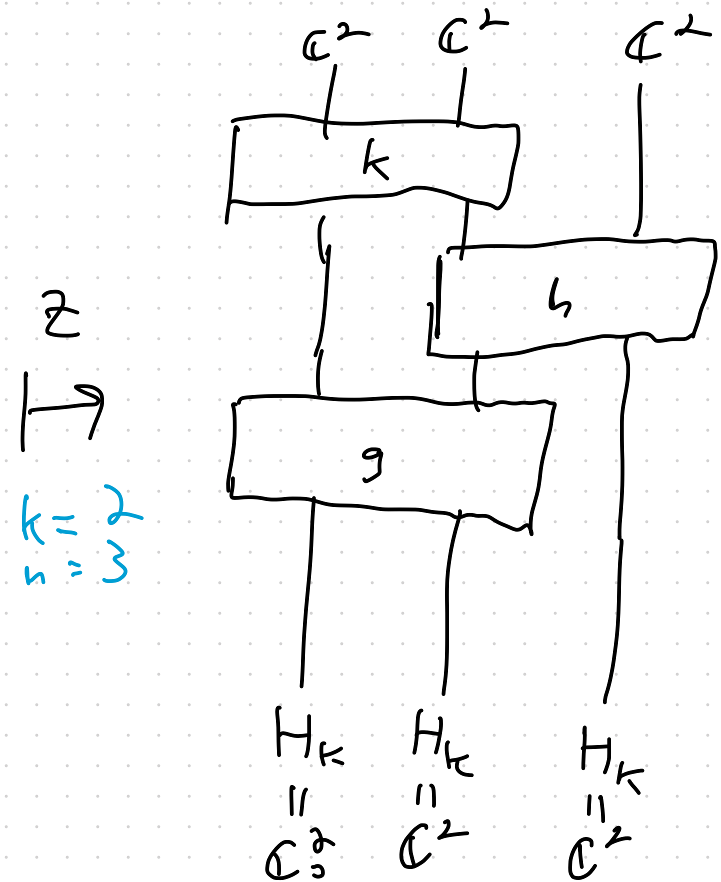
where $H_k = \mathrm{span}\{|T\rangle, |S\rangle\}$, in the same way $C$ acts on $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2$. Moreover, the isomorphism $\mathbb{C}^2 \cong H_k$ identifies

$$|0\rangle = \frac{|T\rangle}{\sqrt{\langle T | T\rangle}}$$

For concreteness, we use

$T =$ 




$g, h, k \in \mathcal{G} \leq U(\mathbb{C}^2 \otimes \mathbb{C}^2)$

$b_g, b_h, b_k \in B_8$

The encoding $C \mapsto b_C$ is linear time.

We might call this topological quantum computing
b/c circuits can be encoded inside a TQFT

However, there's an even better reason to call it TQC:
if we are using $C$ to answer a Yes/No question,
then the probability of a Yes outcome is closely
related to $X$-colored link invariant of $b_C$
"closed up" with copies of $T$.

In particular, we call it TQC b/c of the answer we now give to question asked at end of previous meeting:

How do topological invariants of knots/links/3-manifolds derived from & relate to this model of computation?

## I. "Accept probability of circuit" = "Normalized quantum invariant"

Notice we haven't actually used the identity

$$|0\rangle = \frac{|T\rangle}{\sqrt{\langle T|T\rangle}}.$$

Here's why it matters:

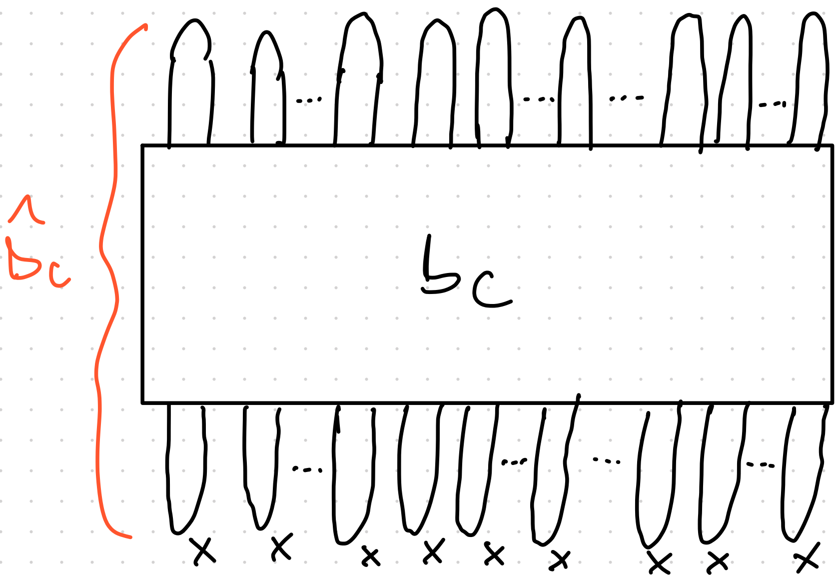
$$\langle 00\cdots 0|C|00\cdots 0\rangle = \frac{\langle TT\cdots T|b_C|TT\cdots T\rangle}{(\langle T|T\rangle)^n}$$

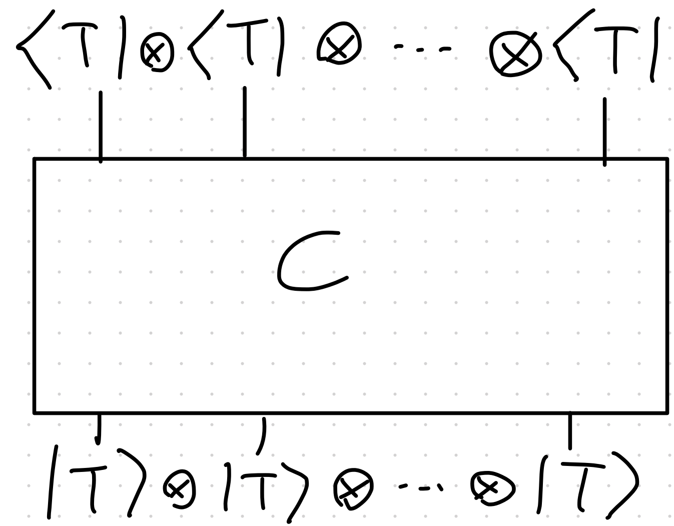
$|\langle 0^n|C|0^n\rangle|^2$ is probability
C outputs $|0^n\rangle$ when input $|0^n\rangle$

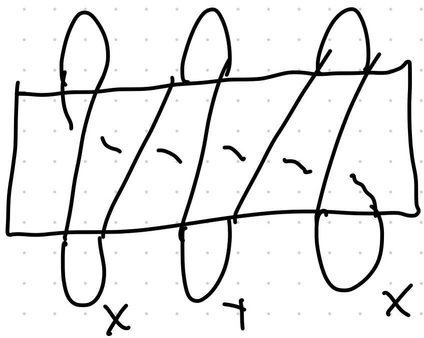
and numerator and denominator of RHS both have topological interpretation, thanks to TQFT axioms.

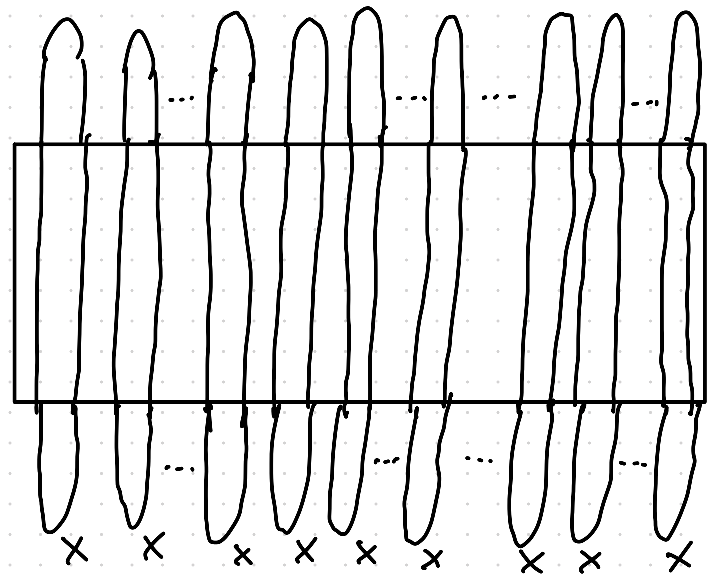
$\langle TT\cdots T | b_c | TT \cdots T\rangle = Z(\hat{b}_c)$ where $\hat{b}_c$ is

X-colored ~~link~~ ribbon diagram as follows:







$$Z(K_1 \sqcup K_2) = Z(K_1) \cdot Z(K_2)$$

$$(\langle\!\langle T \mid T \rangle\!\rangle)^n = (\langle\!\langle T \mid \overbrace{\mathrm{id}}^{\in B_{2k}} \mid T \rangle\!\rangle)^n = Z(O_X^k)^n = Z(O_X)^{nk}$$

where $O_X$ is $X$-colored trivially framed ribbon unknot and

$O_X^k$ is $X$-colored trivially framed ribbon unlink w/ $k$-components.

Thus,

$$\langle 00\cdots 0 | C | 00\cdots 0\rangle = \frac{Z(\hat{b}_c)}{Z(\bigcirc_X)^{nk}}$$

Example: Jones-Kauffman TQFT w/ $\mathcal{C} = U_q sl_2$-mod, $X = V$ the defining representation of $U_q sl_2$, and $q = e^{2\pi i/k}$, then $Z(\hat{b}_c)$ is value of Jones polynomial of $\hat{b}_c$ at $q$, and

$$Z(\bigcirc_V) = q + q^{-1}.$$

$$e^{2\pi i/100} + e^{-2\pi i/100} = 1 - \varepsilon$$

Reminder: BQP$(\mathcal{G}, 1/3)$

$\mathcal{G}$: gate set

Decision problem $F: \{0,1\}^* \to \{0,1\} = \{No, Yes\}$ is in BQP if:

exists a classical poly time algorithm that converts bit string $x \in \{0,1\}^n$ to a $\mathcal{G}$-circuit $C_x$ such that

$$\langle F(x), x, 0^{m-1} | C_x | x, 0^m \rangle \geq 2/3 .$$

Note: here I'm letting $C_x$ depend on $x$, and not just $|x| = n$.

Variation: $BQP(\mathcal{G}, 1/3)$

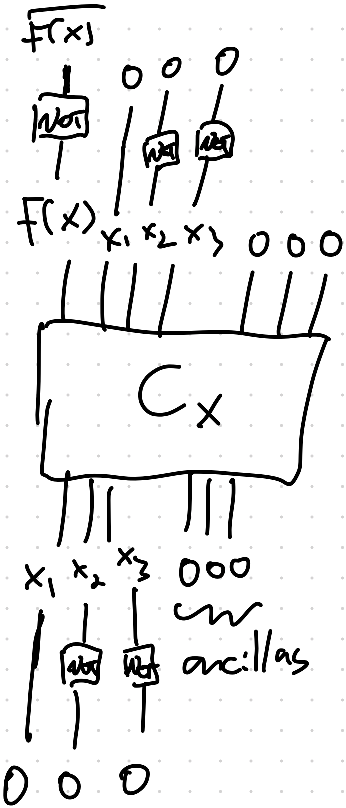
$\mathcal{G}$: gate set

Decision problem $F: \{0,1\}^* \to \{0,1\} = \{No, Yes\}$ is in BQP if:

exists a classical poly time algorithm that converts bit string $x \in \{0,1\}^n$ to a $\mathcal{G}$-circuit $C_x$ such that

$$\langle \overline{F(x)}, 0^n, 0^{m-1} | C_x | 0^n, 0^m \rangle \geq 2/3 .$$

So: We might as well allow $x$ to prepare $x$ from $00\cdots0$. We negate $F(x)$ for contrived reason.


$\overline{f(x)}$
NOT
0 0 0
NOT NOT
$f(x)$ $x_1$ $x_2$ $x_3$ 0 0 0
$C_x$
$x_1$ $x_2$ $x_3$ 000
ancillas
NOT NOT
0 0 0

If $x=011$

A reference:

**Proposition 2.3.** $D \in \mathsf{BQP}$ *if and only if there is a quantum circuit* $C = C(x)$ *with* $\mathrm{poly}(|x|)$ *unitary gates acting on* $n = \mathrm{poly}(|x|)$ *qubits, such that* $C$ *itself can be generated in deterministic polynomial time* $\mathsf{FP}$, *and such that the probability*

$$p(x) = |\langle 0^n | C | 0^n \rangle|^2 \tag{2.1}$$

*is at least* $2/3$ *if* $D(x) = \text{yes}$ *and at most* $1/3$ *if* $D(x)$ *is* no.

[Kuperberg, "How hard is it to approximate the Jones polynomial?"]

<u>Theorem</u> (Topological quantum computing)

Suppose $Z$ and $X$ satisfy conditions above. Then the decision problem

$$f : \{0,1\}^* \to \{0,1\} = \{\text{No}, \text{Yes}\}$$

is in BQP if and only if there exists a polynomial time (classical) algorithm that takes $y \in \{0,1\}^*$ to a braid diagram $b_y$ such that

$$\left[\frac{Z(\hat{b}_y)}{Z(\bigcirc_X)^{nk}}\right]^{\alpha} \geq \frac{2}{3} \quad \text{if} \quad f(y) = \text{Yes}$$

and $$\left[\frac{Z(\hat{b}_y)}{Z(\bigcirc_X)^{nk}}\right]^{\alpha} \leq \frac{1}{3} \quad \text{if} \quad f(y) = \text{No}.$$

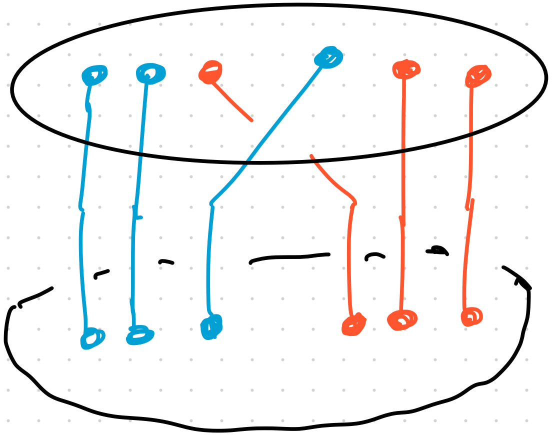
## Remarks

1. Conditions on $X$ can be relaxed (e.g. not self dual, use multiple colors to build a qubit, etc...). Unclear what precise level of generality ought to be.

2. I don't know examples of $Z$ + $X$ such that

$$Z : B_k \longrightarrow U(Z(k; X, 1))$$

has infinite image for all $k \gg 0$ BUT is NEVER dense



No homeo, b/c these are two different Hilbert spaces

Instead, use "color preserving subgroup" $B_{3,3}$ of $B_6$