Meeting 14.1: Computational complexity of TQFT invariants

I. Approximating quantum invariants w/ quantum computers

II. Bad news.

ICES INSTRUCTOR + COURSE EVALUATION SYSTEM ONLINE

Please do an eval!

Deadline: 5/6

I. Approximating quantum invariants w/ quantum computers

So far:

- built model(s) of quantum computation using 2+1-dimensional once-extended unitary TQFTs
- normalized quantum invariants of knots/links are sometimes "important amplitudes" of quantum circuits

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

Special knot constructed from circuit

Note: there are flavors for closed 3-manifolds (instead of links in S^3) using quantum reps of MCG (closed surface)

Natural question:

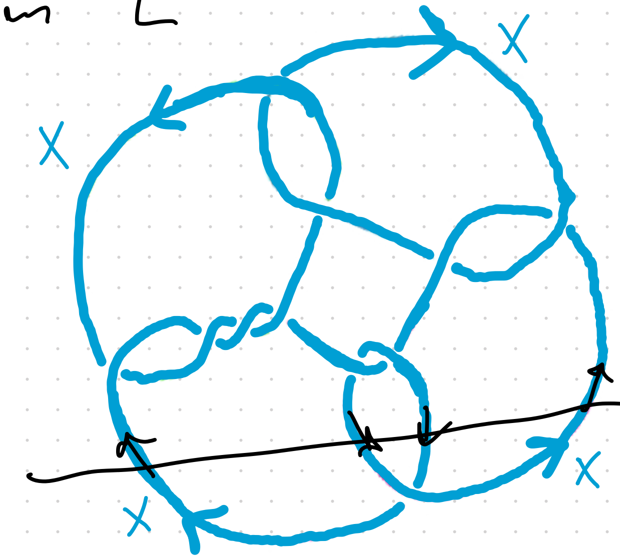
Is there a "converse"? Can quantum computers do something for topology?

Kind of. Suppose we have:

- once extend unitary TQFT Z and color X (not self-dual)
- an X-colored ribbon link diagram L

Then in linear time, we can convert L to a quantum circuit C_L such that

$$\langle 00\cdots 0 | C_L | 00\cdots 0 \rangle = \frac{Z(L)}{Z(\bigcirc_X)^{b(L)}}$$

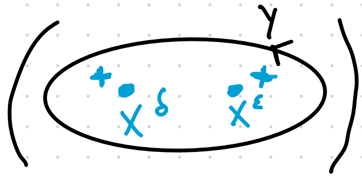


L11a420 from Knot Atlas

where $b(L)$ is the bridge number of diagram L.

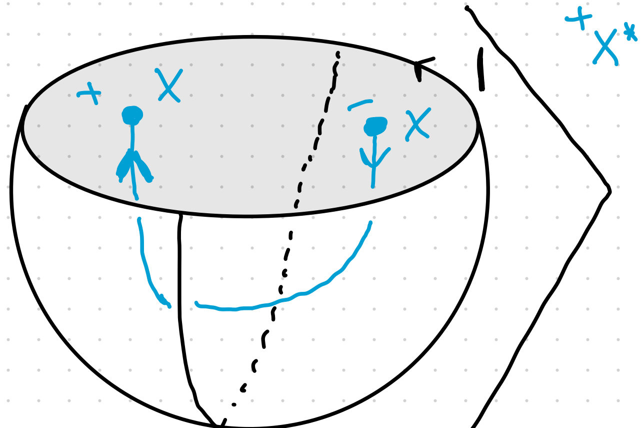
More precisely: to "have Z and X" means we have:

- an identification of Hilbert spaces

$Z(X^{\delta}, X^{\varepsilon}) = \bigoplus_{Y \in C} Z\Big($  $\Big) \xrightarrow{\cong} \mathbb{C}^{N(X^{\delta}, X^{\varepsilon})}$

qudits w/ $d = N(X^{\delta}, X^{\varepsilon})$

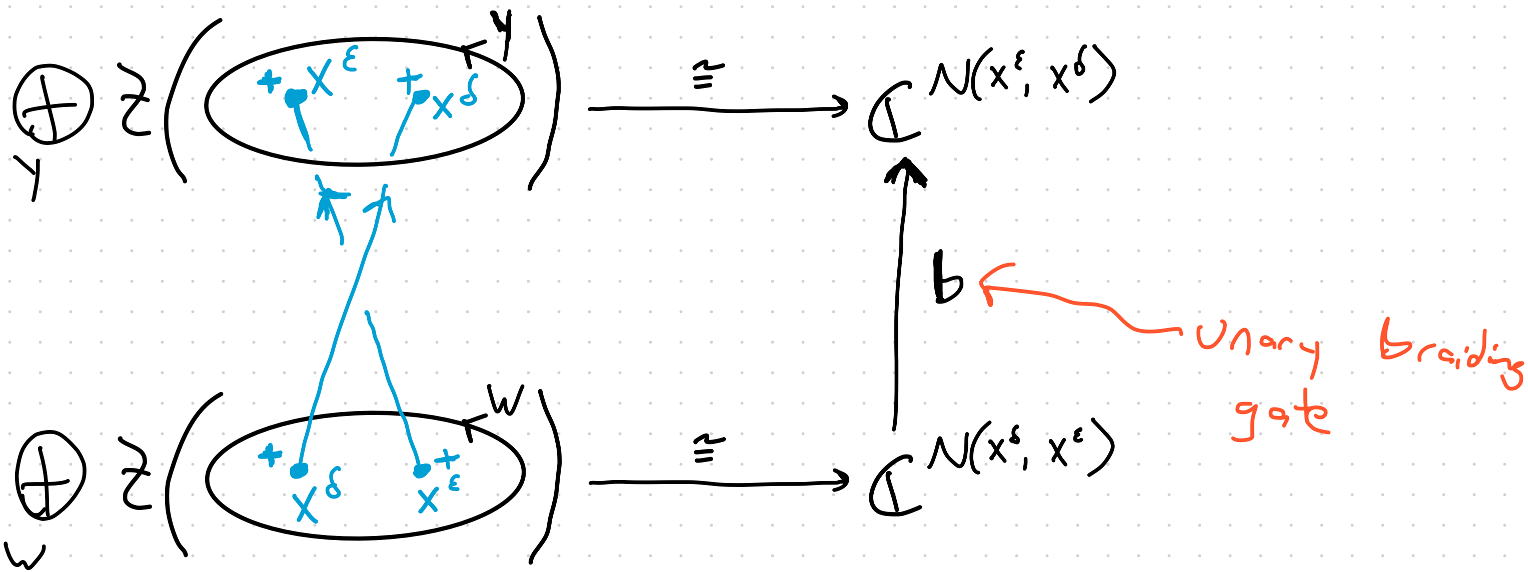
where $\delta, \varepsilon = \phi$ or $*$ such that

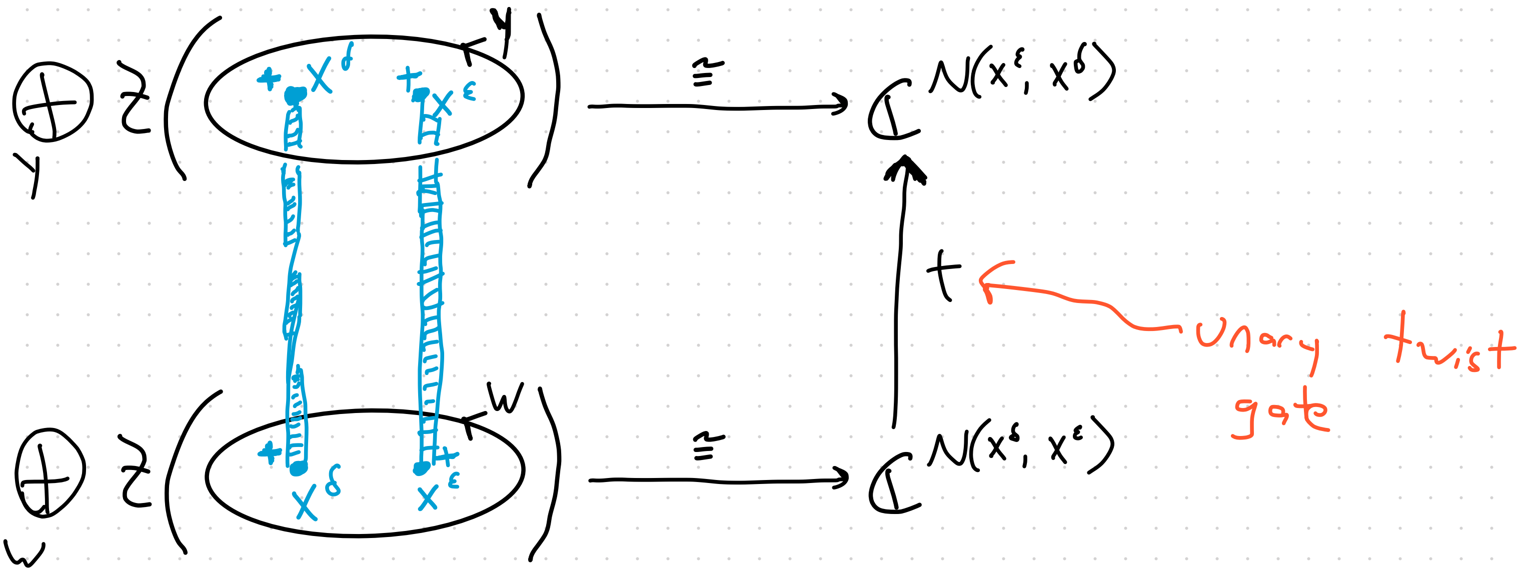
$Z(X, X^{*}; 1) \ni \Big|$  $\Big\rangle \mapsto |0\rangle \in \mathbb{C}^{N(X, X^{*})}$

$$\underline{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad}$$

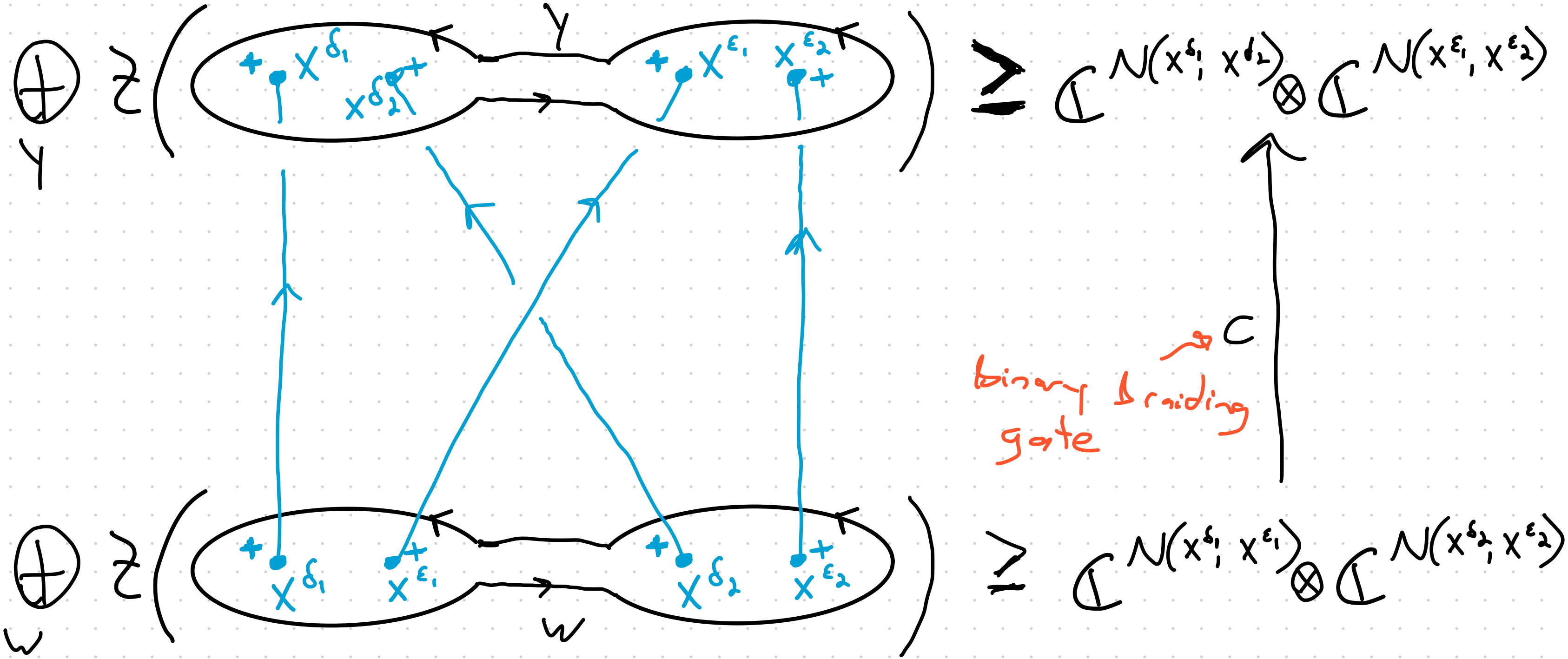
Normalization factor $= Z(\mathcal{O}_X)$

- descriptions (e.g. matrices w/ algebraic entries) of "braiding gates"





$\bigoplus_Y Z$
$\bigoplus_W Z$
x^δ
x^ε
Y
W
$\simeq$
$\mathbb{C}^{N(x^\varepsilon, x^\delta)}$
$\mathbb{C}^{N(x^\delta, x^\varepsilon)}$
t
unary twist gate


⊕_Y Z( ) ≅ ℂ^{N(x^{δ1}, x^{δ2})} ⊗ ℂ^{N(x^{ε1}, x^{ε2})}
⊕_W Z( ) ≅ ℂ^{N(x^{δ1}, x^{ε1})} ⊗ ℂ^{N(x^{δ2}, x^{ε2})}
Y
W
x^{δ1}
x^{δ2}
x^{ε1}
x^{ε2}
binary braiding gate
C

Note: the above local data should be considered as (part of) a combinatorial/finite algebraic definition of TQFT Z.

It needs to satisfy various compatibility conditions...

If we wanted to be more precise, should use a

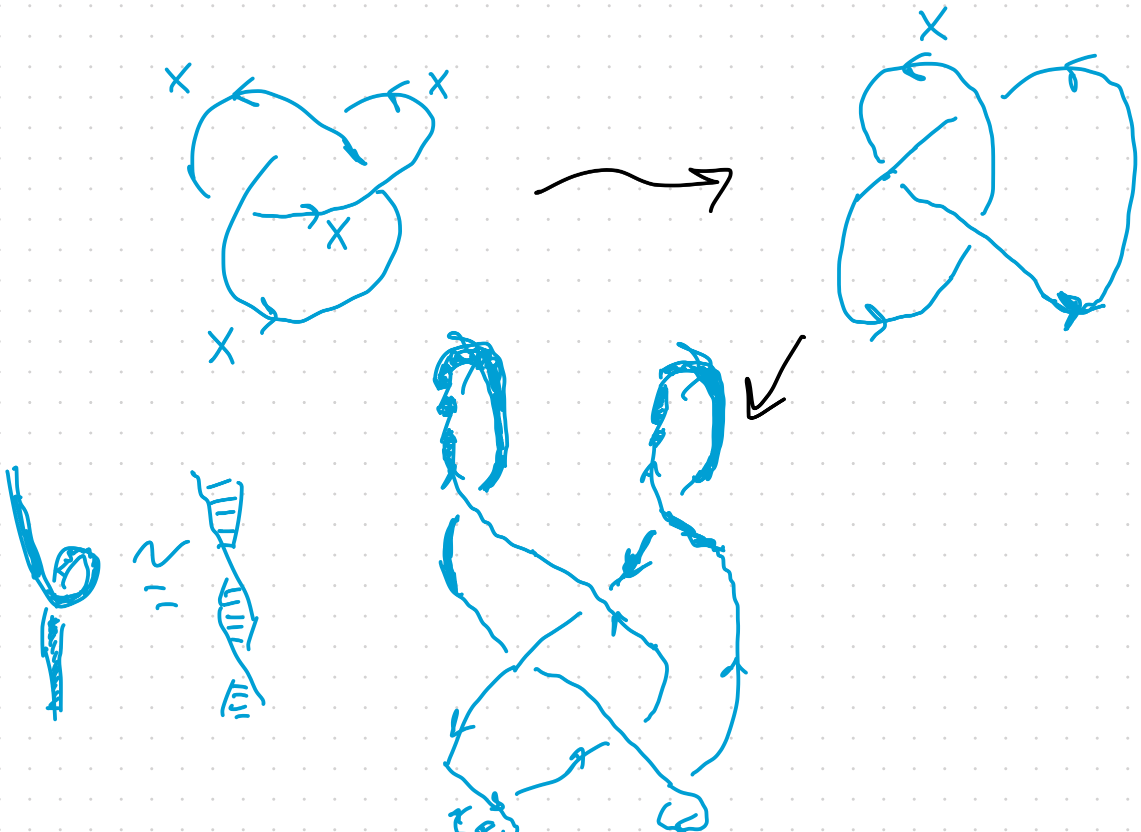
skeletalization of a

Unitary modular tensor

category.

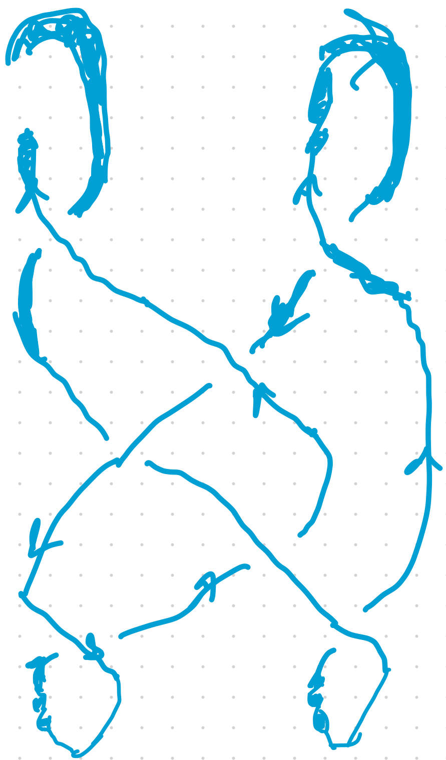
Converting L to c_L:

1. Put L in "standard bridge position:"

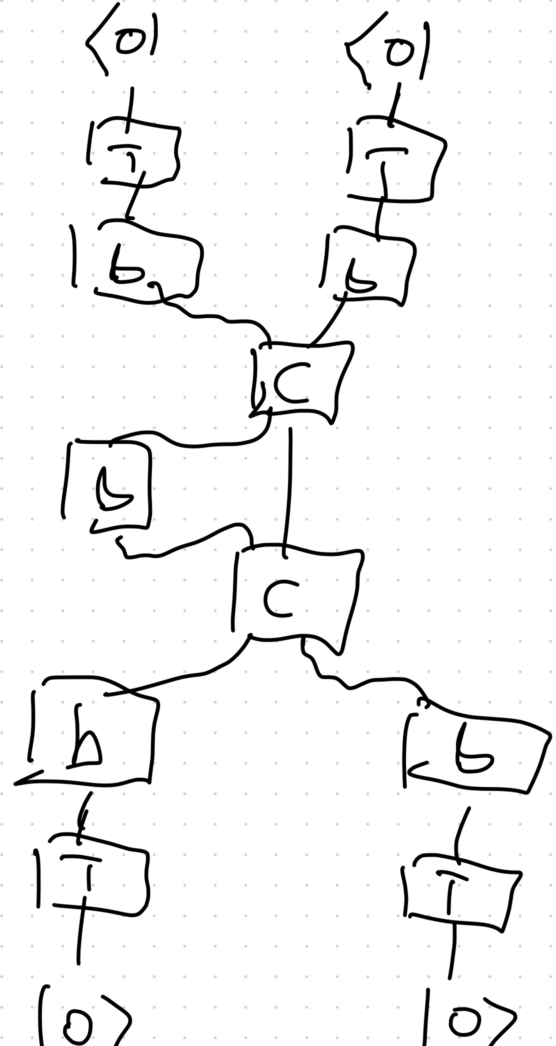


Arrows "wrong" at cups/caps

2



$\mapsto$



3. Easy to check using TQFT axioms

$$\langle 00\cdots0 | C_L | 00\cdots0 \rangle = \frac{Z(L)}{Z(\bigcirc_X)^{b(L)}}$$

where $b(L)$ is the bridge number of diagram L.

Now what?

We can approximate the probability

$$\left|\langle 00\cdots 0 | C_L | 00\cdots 0\rangle\right|^2$$

in usual way via repeated trials. In particular, given N, can find N-bit binary approximation in $O(\log N)$.

Suppose $\left| P - \left|\langle 00\cdots 0 | C_L | 00\cdots 0\rangle\right|^2\right| < \varepsilon$.

Then

$$\left| P - \left|\frac{Z(L)}{Z(\bigcirc_x)^{b(L)}}\right|^2\right| < \varepsilon$$

$$\Rightarrow \left| P \cdot |Z(\bigcirc_x)|^{2b(L)} - |Z(L)|^2 \right| < \varepsilon \cdot |Z(\bigcirc_x)|^{2b(L)}$$

Now what?

Want to compute an invariant of L.

Know:

$$\langle 00\cdots0 | C_L | 00\cdots0 \rangle = \frac{Z(L)}{Z(\bigcirc_x)^{b(L)}}$$

Not an invariant of L.

It is bridge number of DIAGRAM.

So, LHS is NOT invariant.

$$|Z(L)|^r$$

Summarizing:

Extracting an invariant of L, namely,

$$|Z(L)|^2$$

From the identity

$$\langle 00\cdots0|C_L|00\cdots0\rangle = \frac{Z(L)}{Z(\bigcirc_x)^{b(L)}}$$

has error that scales exponentially badly w/ $b(L)$. Error depends on diagram!

$$\left| P \cdot |\mathcal{Z}(\underset{X}{\circlearrowleft})^{2b(L)}| - |\mathcal{Z}(L)|^2 \right| < \varepsilon \cdot |\mathcal{Z}(\underset{X}{\circlearrowleft})|^{2b(L)}$$

If $|\mathcal{Z}(\underset{X}{\circlearrowleft})| \leq 1$, we're happy.

But this NEVER happens unless X is an "abelian anyon," in which case $\mathcal{Z}(L)$ is trivial.

Moral: if L is "wide," it takes a ton of work to overcome the error.

Can we rescue anything?

1. If we restricted L to $b(L) < 100$, we can compute $Z(L)$ in linear time on a classical computer!

No dice!

2. Can we "massage" L to make $b(L)$ small? For every $N > 0$, exists link L such that $b(D) > N$ for all diagrams D of L.

3. Can we massage C_L to get a thinner circuit C_L' that is useful?

No...

Freedman, Cui-Freedman-Wang

"Complexity Classes as Mathematical Axioms"

2. Bad News

Z any TQFT w/ $X = X^*$ w/ dense quantum reps of braid group

Theorem 1.2. *Let ~~$V(L,t)$~~ be the ~~Jones polynomial~~ of a link L described by a link diagram, and ~~let t be a principal, non-lattice root of unity.~~ Let $0 < a < b$ be two positive real numbers, and assume as a promise that either $|V(L,t)| < a$ or $|V(L,t)| > b$. Then it is #P-hard, in the sense of Cook-Turing reduction, to decide which inequality holds. Moreover, it is still #P-hard when L is a knot.*

[Kuperberg, "How hard is it to approximate...?"]

$$|Z(L)| < a \quad \text{or} \quad |Z(L)| > b$$

is NP-hard (even better, #P-hard) to distinguish.

"Proof"

PostBQP = "Linear circuits"

$\overset{\text{Aaronson}}{=}$ PP