(Topological) Quantum Computing

Agenda:

- Computability and Physics
- Quantum Computing Basics
- Operational Theory of Anyons
- Topological Quantum Computing

References:

- Deutsch : Proc. R. Soc. Lond. A 400 (1985)
- Lloyd : PRL 75 (1995)
- Lahtinen and Pachos, 1705.04103 (review 1)
- Field and Simula, 1802.06176 (review 2)

1. Computability and Physics:

- These days, computation seems inextricably tied to physics. In this first section, I want to give a more philosophical take as to why, which will channel nicely (I hope!) into talking about different physical models of computation.

Def. An <u>alphabet</u> Σ is a finite collection of symbols; a <u>Σ-string</u> is a finite string of letters from Σ.

Ex.
- $\Sigma = \{0, 1\}$, 1001, 0111
- $\Sigma = \{a, b, \dots, z\}$, physics, azqbhf
- $\Sigma = \{\ddot\smile, \ddot\frown, \ddot-\}$, $\ddot\smile\ddot-\ddot\smile\ddot\frown$

Def. $\Sigma^* := \{\text{all } \Sigma\text{-strings}\}$.

Def. A function $f : \Sigma^* \longrightarrow \Gamma^*$ is <u>computable</u> iff $\exists$ a "reasonable effective procedure" $A_f : \Sigma^* \to \Gamma^*$

$$\forall \sigma \in \mathrm{dom}(f) : f(\sigma) = A_f(\sigma).$$

• One is left wondering what constitutes a "reasonable effective procedure".

Turing's Idea:

Human working by rule w/ unlimited pens and paper

$$\Updownarrow$$

Turing machine

Church-Turing Thesis:

A is a reasonable effective procedure

$$\Longleftrightarrow$$

A is simulable on a Turing machine

Thus,

$$f \text{ computable} \Longleftrightarrow A_f \text{ simulable on TM}.$$

Corollary: Countably many computable $f:\Sigma^* \to \Gamma^*$ (whereas uncountably many $f:\Sigma^* \to \Gamma^*$).

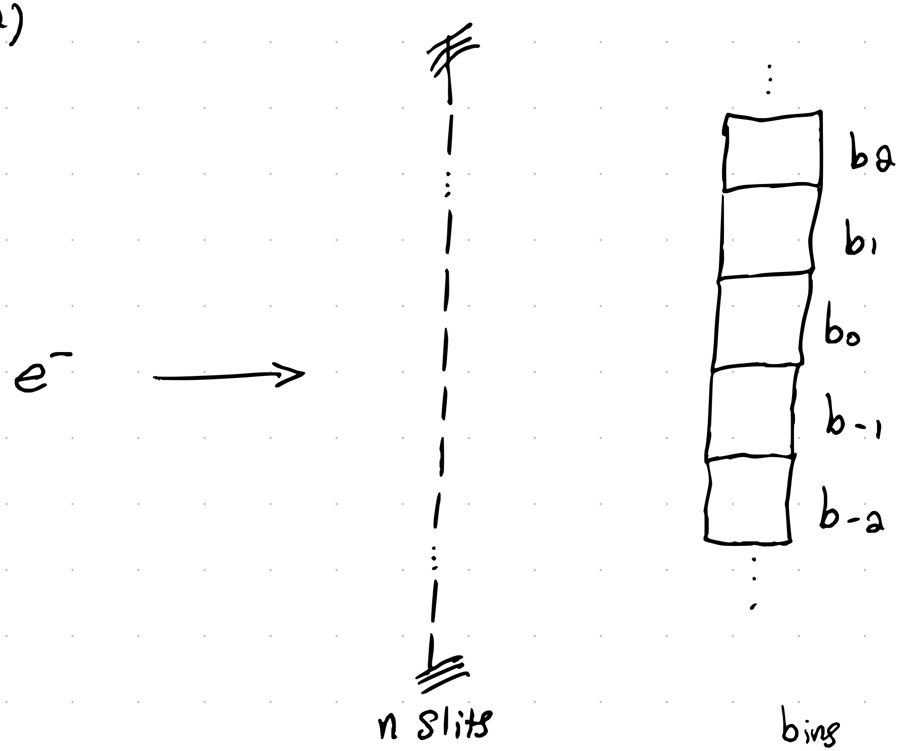
Ex:

(1) $f : n \longmapsto$ nth Fib. #

A_f:

```
if n=1:
    return 1
else:
    return n+f(n-1)
```

(2)



Let

$f_k : n \longmapsto$ bin(s) b_i where electron is kth-most probable to be seen

→ This <u>is</u> computable (one can simulate this on a computer!)

→ Why should it be? Not clear, but elevate to postulate!

Physical CTT (Deutsch):

$\mathcal{A}$ physically realizable effective procedure

$\Longleftrightarrow$

$\mathcal{A}$ simulable on TM

Therefore,

$$f \text{ computable} \Longleftrightarrow \mathcal{A}_f \text{ physically realizable effective procedure.}$$

$$\Longleftrightarrow \mathcal{A}_f \text{ simulable on TM}$$

Upshot: No physical model of computing can "compute more" than the garden-variety TM.

→ only countably many physically computable functions!

→ Let's now consider two physical models of computation, quantum circuits and the topological quantum computer.

→

2. Quantum Computing Basics.

Def. A finite set $G \subseteq SU(n)$ is <u>computationally universal</u> iff G^* is dense in $SU(n)$.

→ Thus, require G to be able to approximate any unitary

→ This is generically possible because of a theorem by Lloyd.

Thm (Lloyd): All $G \subseteq SU(n)$ are computationally universal except a set of measure zero.

Idea: See if e-vals of gates in G are irrationally related to π (occurs w/ prob.$=1$), then take powers to approximate.

→ Is such quantum compilation efficient?

Thm (Solovay-Kitaev): Fix $\varepsilon > 0$ and let $G \subseteq SU(n)$. Then, $\exists c \leq 4 : \forall \mathcal{U} \in SU(d)$, $\exists$ sequence $S \in G^*$ of length $\mathcal{O}(\log^c(1/\varepsilon))$ s.t.

$$\|S - \mathcal{U}\|_{op} \leq \varepsilon.$$

→ In original SK theorem G needed to be closed under inversion, however a recent result by Bouland removed that requirement.

Def. The Clifford + T gate set is

Can exclude S but easier to implement than T?

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

$$\underbrace{\text{CNOT} \qquad H \qquad S}_{\text{Clifford}} \qquad \underbrace{T}_{T}$$

Thm: The Clifford + T set is computationally universal. In fact, Clifford + $\tilde{T}$ set, $\tilde{T} \notin$ Clifford group, is universal.

→ For proof, see, e.g. Nielsen and Chuang.

Upshot:

- If in some other computational model one can simulate the Clifford + $\tilde{T}$ gates for some $\tilde{T}$, one can simulate a general purpose quantum computer!
- **Question:** How to do this on a topological quantum computer?

3. Operational Theory of Anyons:

Assumptions:

- Anyons exist
- Microscopic details incidental
  - → I.e., all we care about are the anyons themselves, not how they are made or the system in which they live.

Thus, anyons evolve via:

(i) Pairwise creation or annihilation,

(ii) fusion (to form other anyons),

(iii) adiabatic exchange.

→ Let's build a general anyon model.

Let $A = \{1, a, b, c, \ldots\}$ be collection of distinct anyons.

$\uparrow$

Vacuum

→ $a, b, \ldots$ can be seen as topological charges of anyons in model.

→ As charges, they satisfy conservation rules, here called <u>fusion rules</u>

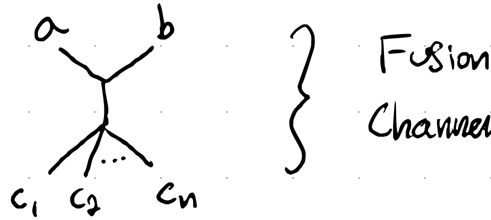
→

Def. For anyons $a, b \in M$, the <u>fused anyon (ab)</u> satisfies the <u>fusion rule</u>

$$a \times b = \sum_{c \in M} N_{ab}^{c}\, c,$$

where $N_{ab}^{c} \in \{0, 1, 2, \dots\}$ are the <u>fusion coefficients</u>. These specify the <u>fusion channels</u> that (ab) can take.

→ Intuitively, fusion channels specify what (ab) can become:



→ Mention Hardy's Paradox?

Def. • An <u>operational anyon model</u> M is a pair $(A, A^{\times})$, where

$$A^{\times} = \{a \times b \mid a, b \in A\}.$$

→ Yes there is more to specify (the F and R matrices). Get to this later.

• M is <u>abelian</u> iff

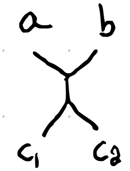
$$\forall a, b \in A, \ \exists! c \in A : N_{ab}^{c} \neq 0.$$

→ Thus, every a, b fuses to unique outcome:

- M is <u>non-abelian</u> iff

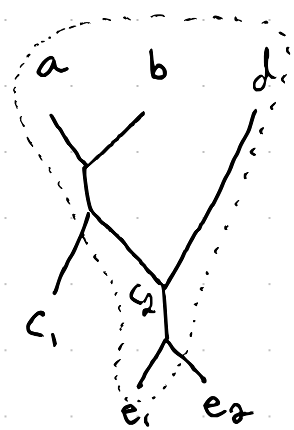
$$\exists a, b, c_1, c_2 \in A : N_{ab}^{c_1}, N_{ab}^{c_2} > 0 .$$

→ So multiple fusion channels:



$\Big\}$ ≥ 2 fusion channels

→ Thus, repeated fusion in non-abelian model leads to repeated branching:



(→ Assuming fusion rule:

$c_2 \times d = e_1 + e_2$)

<u>Notation:</u> For encircled branch (with only one leaf), associate a state

$$|(a\, b)\, d : c_2 d : e_1\rangle$$

for the particular fusion channel.

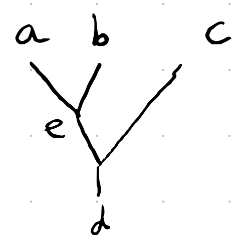
→

→ One could try to define this notation more generally (I did) but it gets hairy fast.

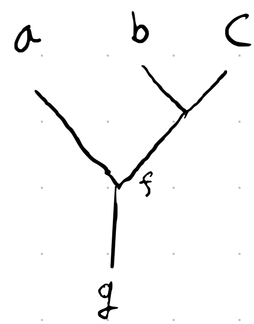
→ Instead, let's see a few examples.

→ For three anyons:

$$|(a\,b)c : ec : d\rangle \equiv$$



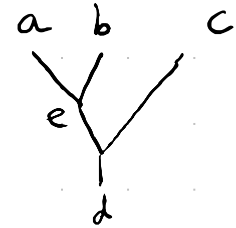
$$|a(bc) : af : g\rangle \equiv$$

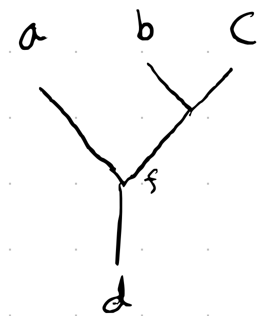


→ Collection of all such states forms the fusion space:

$$\text{fusion space} = \{\text{all fusion channel states in model } M\}.$$

→ Consider now the previous two channels, but in a model where the total charge turns out to be the same:

$$|(a\,b)\,c : ec : d\rangle \equiv$$  (1)

$$|a(b\,c) : af : d\rangle \equiv$$  (2)

→ Different channels lead to same anyon d.

→ These sectors can be superposed (same charge sector), and thus are related:

$$|(ab)\,c : ec : d\rangle = \sum_{\substack{f \\ N_{ab}^{f} \neq 0}} \left(F_{abc}^{d}\right)_{ef} |a(bc) : af : d\rangle$$

→ "F-matrix". Describes structure of fusion space (how all states in given charge sector relate).

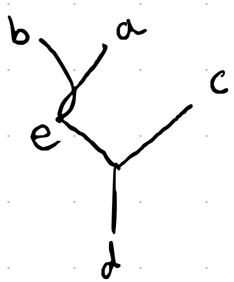
→ Ultimately (1) and (2) represent the 2D basis of the d-charge sector with 3 anyons.

→ These will later represent logical states.

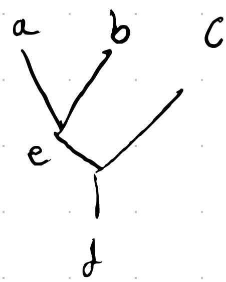
→ Notice, in this transformation w/ F matrix, no cutting or crossing of the diagram occurred.

→ We now go to braiding.

<u>M abelian:</u>

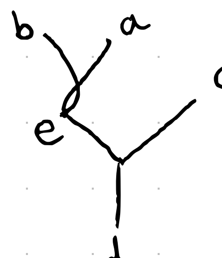


$$= e^{i\theta_{ab}}$$

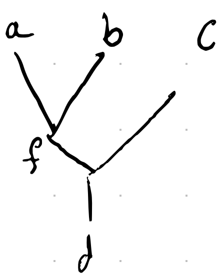


→ However, for non-abelian M, a, b may fuse to multiple different particles, so, in general

<u>M non-abelian:</u>



$$= \sum_{\substack{f \\ N_{ab}^{f} \neq 0}} e^{i\theta_{ab}^{f}}$$



One writes $R_{ab}^{f} = e^{i\theta_{ab}^{f}}$, "R matrix".

→ Collectively, these specify braiding rules, and they realize the unitary transformations in the fusion space.

→

4. TQC with Ising Anyons:

→ Recall, suffices to simulate Clifford + T gateset.

→ Unfortunately, natural models like the Ising anyon model can only simulate Clifford topologically but whatever let's at least try to understand that!

→ There are other models, such as the Fibonacci anyon model, that is universal, however it has many quirks, such as not scaling (on adding another anyon) like a tensor products but by the Fibonacci sequence!

<u>Def.</u> The Ising anyon model $\mathcal{I} = (A, A^\times)$ has

$$A = \{1, \sigma, \psi\}$$

$$\underbrace{1}_{\text{vacuum}} \quad \underbrace{\sigma}_{\text{anyon}} \quad \underbrace{\psi}_{\text{fermion}}$$

$$A^\times = \left\{ \begin{array}{l} 1\times 1 = 1,\ 1\times\psi = \psi,\ 1\times\sigma = \sigma, \\ \psi\times\psi = 1,\ \psi\times\sigma = \sigma,\ \sigma\times\sigma = 1+\psi \end{array} \right\}.$$

<u>Note:</u> Nonabelian because $\sigma\times\sigma = 1+\psi$.

Note:

$$\sigma \times \sigma \times \sigma = 2\sigma$$

$$\sigma \times \sigma \times \sigma \times \sigma = 2\cdot 1 + 2\cdot \psi$$

$$\sigma \times \sigma \times \sigma \times \sigma \times \sigma = 4\sigma$$

I.e., dimension of fusion space doubles for every σ-pair added — akin to tensor product!

→ suggests to use σ as encoding logical information. Indeed:

Initialization:

In vacuum sector,

$$|00\rangle := |\sigma\sigma:1\rangle\,|\sigma\sigma:1\rangle\,|\sigma\sigma:1\rangle$$ ← Initialize anyons here!

$$|10\rangle := |\sigma\sigma:\psi\rangle\,|\sigma\sigma:\psi\rangle\,|\sigma\sigma:1\rangle$$

$$|01\rangle := |\sigma\sigma:1\rangle\,|\sigma\sigma:\psi\rangle\,|\sigma\sigma:\psi\rangle$$

$$|11\rangle := |\sigma\sigma:\psi\rangle\,|\sigma\sigma:1\rangle\,|\sigma\sigma:\psi\rangle$$

→ ($\psi \times \psi = 1$ consistent with this, because always even number of ψs).

Quantum Gates:

Ising anyons have

$$F = F^{\sigma}_{\sigma\sigma\sigma} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$= H \quad \text{(Hadamard!)}$$

E.g., the state acquires -1 phase whenever exchanged σ-pair fuses to become ψ

and

$$R = \begin{pmatrix} R^{1}_{\sigma\sigma} & 0 \\ 0 & R^{\psi}_{\sigma\sigma} \end{pmatrix} = e^{-i\pi/8}\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

$$= e^{-i\pi/8} S \quad \text{(S-gate!)}$$

→ Single qubit logic gates!

→ Implement these on logical qubits.

→ As we have six σ anyons in the logical basis,

Let $R_{ij} = R$ exchange matrix for anyons σ_i and σ_j.

Upshot (Lahtinen et. al):

$$H \otimes \mathbb{I} = R_{12} R_{23} R_{12} = RF^{-1}RFR \otimes \mathbb{I}$$

$$\mathbb{I} \otimes H = R_{56} R_{45} R_{56} = \mathbb{I} \otimes RF^{-1}RFR$$

$$\text{CNOT} = R^{-1}_{12} R_{34} R^{-1}_{56}$$

• One can verify these algebraically (the math is hairy).

→

Q: How to implement T topologically.

- Unfortunately, cannot do so w/ Ising anyons.
- Can with Fibonacci anyons, but those scale weirdly.
- In principle you can interact anyons, which will then implement, but then ruins fault-tolerance!

The Final Step — Measurement:

Recall the basis states:

$$|00\rangle := |\sigma\sigma:1\rangle\,|\sigma\sigma:1\rangle\,|\sigma\sigma:1\rangle$$

$$|10\rangle := |\sigma\sigma:\psi\rangle\,|\sigma\sigma:\psi\rangle\,|\sigma\sigma:1\rangle$$

$$|01\rangle := |\sigma\sigma:1\rangle\,|\sigma\sigma:\psi\rangle\,|\sigma\sigma:\psi\rangle$$

$$|11\rangle := |\sigma\sigma:\psi\rangle\,|\sigma\sigma:1\rangle\,|\sigma\sigma:\psi\rangle$$

- These correspond to distinct patterns of pairwise fusion outcomes.

Since $\sigma\times\sigma = 1+\psi$, each pairwise fusion gives either 1 or ψ. Thus, readout is just pairwise fusion!

//

Questions? (Ananth!)