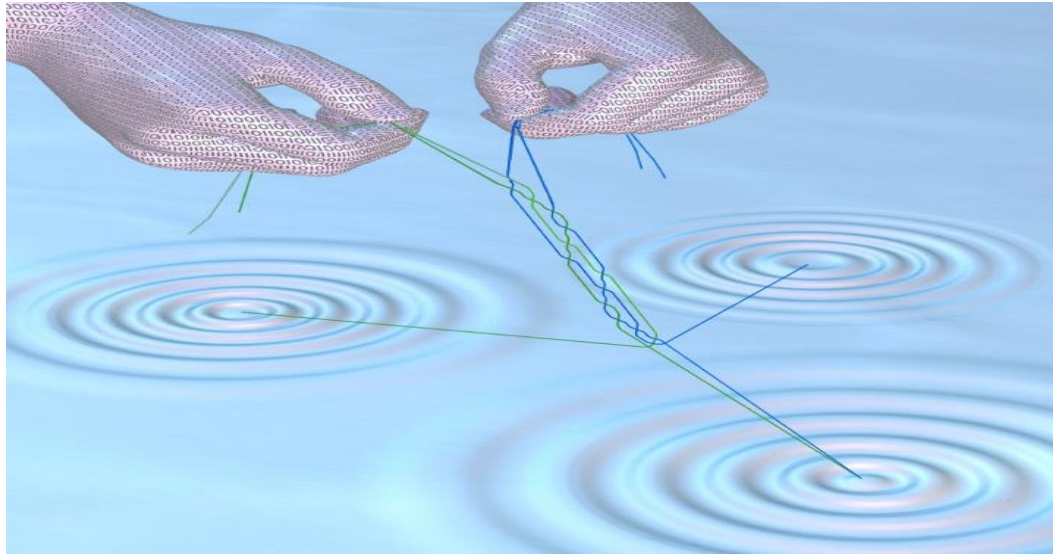


Topological Quantum Computation



Zhenghan Wang
Microsoft Station Q & UC Santa Barbara
Texas, March 26, 2015

P/NP, and the quantum field computer

MICHAEL H. FREEDMAN



Classical Physics	Turing Model
Quantum Mechanics	Quantum Computing
Quantum Field Theory	???
String Theory	??????

Fault-tolerant quantum computation by anyons

A.Yu. Kitaev 🍷 🟩 🟩



Quantum field computing is the same as quantum computing.

True for TQFTs
(Freedman, Kitaev, Larsen, W.)

Quantum Computation

- There is a serious prospect for quantum physics to change the face of information science.
- Theoretically, the story is quite compelling:
 - Shor's factoring algorithm (1994)
 - Fault tolerance ~1996-1997 independently
 - **P. Shor**
 - **A. M. Steane**
 - **A. Kitaev**
- But for the last twenty years the most interesting progress has been to build a quantum computer.

Why Quantum More Powerful?

- Superposition

A (classical) **bit** is given by a physical system that can exist in one of two distinct states:

0 or 1

A **qubit** is given by a physical system that can exist in a linear combination of two distinct quantum states: $|0\rangle$ or $|1\rangle$

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$$

$$\alpha, \beta \in \mathbb{C}$$

$$|\alpha|^2 + |\beta|^2 = 1 \quad |\psi\rangle \in \mathbb{C}P^1$$

- Entanglement

Quantum states need not be products. For example:

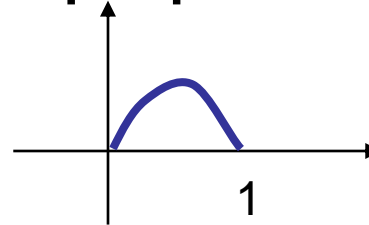
$$\begin{aligned} |\Psi_{AB}\rangle &= \frac{1}{\sqrt{2}} (|0_A 0_B\rangle + |1_A 1_B\rangle) \\ &\neq |\psi_A\rangle \otimes |\phi_B\rangle \end{aligned}$$

This is the property that enables quantum state teleportation and Einstein's "spooky action at a distance."

- Classical information source is modeled by a **random variable** X

The bit---a random variable $X \in \{0,1\}$ with equal probability.
Physically, it is a switch

$$I_X(p) = - \sum_{i=1}^n p_i \log_2 p_i ,$$



- A **state** of a quantum system is an information source

The qubit---a quantum system whose states given by non-zero vectors in \mathbb{C}^2 up to non-zero scalars.
Physically, it is a 2-level quantum system.

Paradox: A qubit contains both more and less than 1 bit of information.

The average amount information of a qubit is $\frac{1}{2 \ln 2}$.

A **computing** problem is given by a family of **Boolean** maps $\{0,1\}^n \longrightarrow \{0,1\}^{m(n)}$

Name: Factoring

Instance: an integer $N > 0$

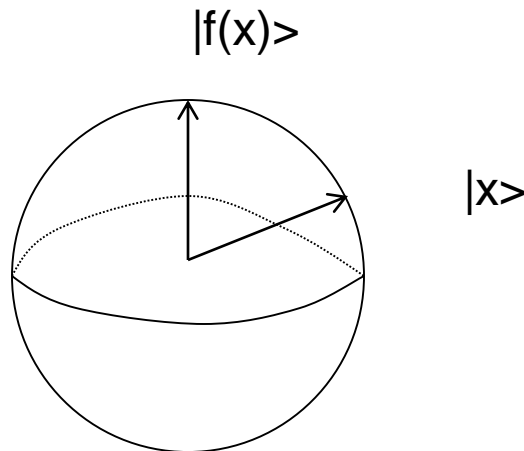
Question: Find the largest prime factor of N

Encode N as a bit string of length $n \sim \log_2 N$,
the factoring problem is a family of Boolean functions
 $f_n: \{0,1\}^n \longrightarrow \{0,1\}^{m(n)}$

e.g. $n=4$, $f_4(1111) = 101$, i.e., $f_4(15) = 5$

How Quantum Computers Work

Given a Boolean map $f: \{0,1\}^n \rightarrow \{0,1\}^n$,
for any $x \in \{0,1\}^n$, represent x as a basis
 $|x\rangle \in (\mathbb{C}^2)^{\otimes n}$, then find a unitary matrix U so
that $U(|x\rangle) = |f(x)\rangle$.



Basis of $(\mathbb{C}^2)^{\otimes n}$ is in 1-1 correspondence with n-bit strings or $0, 1, \dots, 2^n - 1$

Problems

- x , $f(x)$ does not have same # of bits
- $f(x)$ is not reversible
- The final state is a linear combination
- ...
- **Not every U_x is physically possible**

Gate Set

Fix a collection of unitary matrices (called **gates**) and use only compositions of local unitaries from this gate set

e.g. **standard gate set**

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \text{--- Hadmard,} \quad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{\pi i/4} \end{pmatrix} \text{--- } \frac{\pi}{8} \text{ gate}$$

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, |i, j\rangle \rightarrow |i, (i + j) \bmod 2\rangle, i, j = 0 \text{ or } 1$$

Universality

- Fix a gate set S , a **quantum circuit** on n -qubits $(\mathbb{C}^2)^{\otimes n}$ is a composition of finitely many matrices g_i , where each g_i is of the form $\text{id} \otimes g \otimes \text{id}$, where each $g \in S$ is a gate.
- **Universality**: A gate set S is **universal** if the collection of all quantum circuits form a **dense** subset of the union $\bigcup_{n=1}^{\infty} \text{PSU}(2^n)$.

The class **BQP** (**b**ounded **e**rror **q**uantum **p**olynomial-time)
Fix a **physical** universal gate set

A computing problem $f_n: \{0,1\}^n \rightarrow \{0,1\}^{m(n)}$ is in **BQP** if

- 1) there exists a classical algorithm of time $\text{poly}(n)$ (i.e. a Turing machine) that computes a function $x \rightarrow D_x$, where $x \in \{0,1\}^n$, and D_x encodes a $\text{poly}(n)$ -qubit circuit U_x .
- 2) when the state $U_x|0 \cdots 0\rangle$ is measured in the standard basis $\{|i_1 \cdots i_{p(n)}\rangle\}$, the **probability** to observe the value $f_n(x)$ for any $x \in \{0,1\}^n$ is at least $3/4$.

Remarks:

- 1) Any function that can be computed by a QC can be computed by a TM.
- 2) Any function that can be efficiently computed by a TM can be computed efficiently by a QC, i.e. $\text{BPP} \subseteq \text{BQP}$

Factoring is in **BQP** (Shor's algorithm), but not known in **FP** (although **Primality** is in **P**).

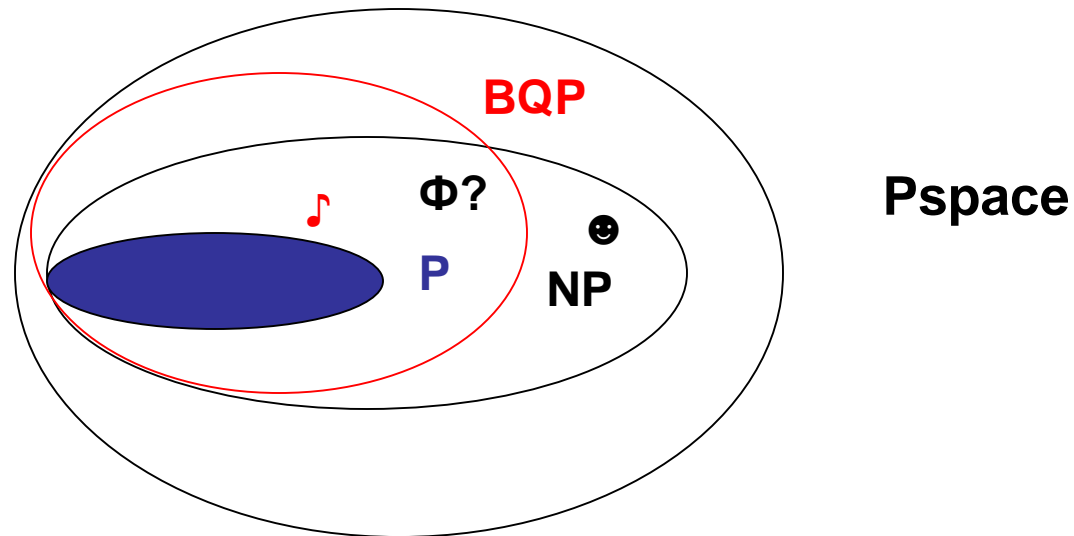
Given an n bit integer $N \sim 2^n$

Classically $\sim e^c n^{1/3} \text{ poly}(\log n)$

Quantum mechanically $\sim n^2 \text{ poly}(\log n)$

For $N=2^{500}$, classically \sim billion years

Quantum computer \sim few days



Can We Build a Large Scale Universal QC?

Yes theoretically. Fault-tolerant quantum computation theory shows if hardware can be built up to the accuracy threshold $\sim 10^{-4}$, then a scalable QC can be built.

But in reality, the obstacle is mistakes and errors (decoherence)

Classical error correction by redundancy

$$0 \rightarrow 000, 1 \rightarrow 111$$

Not available due to the **No-cloning** theorem:

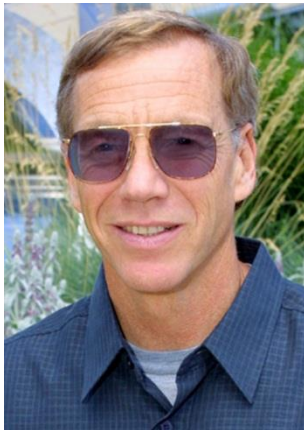
The cloning map $|\psi\rangle \otimes |0\rangle \rightarrow |\psi\rangle \otimes |\psi\rangle$ is not linear.

Key “Post-Shor” Idea



Peter Shor
Shor's Factoring Algorithm

To use topology to protect quantum information



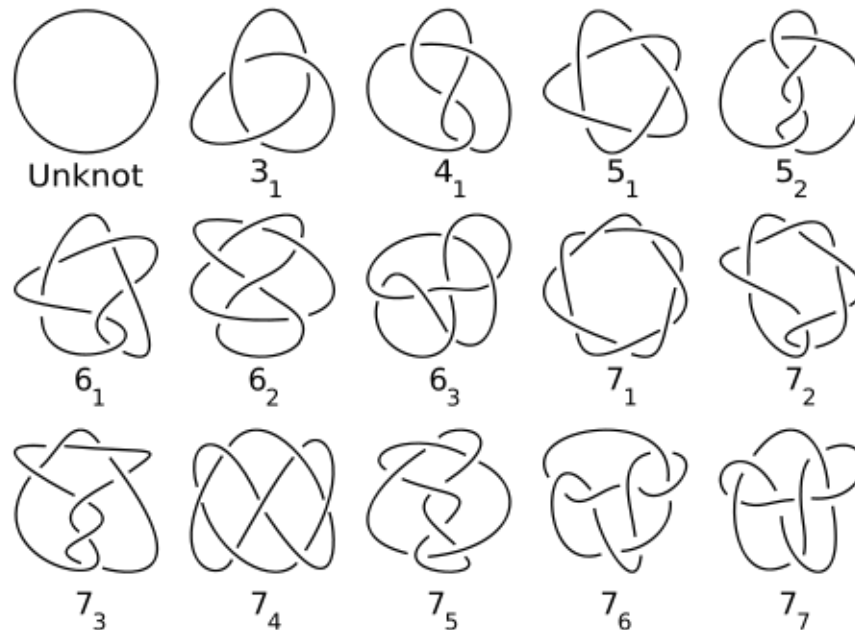
Michael Freedman



Alexei Kitaev

Why Topology?

- **Topology** is usually conceived of as that part of geometry which survives deformation.



- But, equally, **topology** is that part of quantum physics which is robust to deformation (error).

A Revolutionary New Idea

If a physical system were to have quantum *topological* (necessarily nonlocal) degrees of freedom, which were *insensitive to local probes*, then information contained in them would be *automatically protected against errors caused by local interactions with the environment*.

This would be fault tolerance guaranteed by physics at the hardware level, with no further need for quantum error correction, i.e. topological protection.

Alexei Kitaev

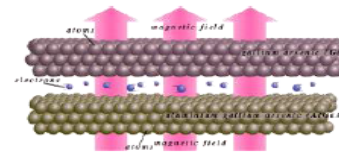
Topological Phases of Matter

A **topological quantum phase** is represented by a quantum theory whose low energy physics in the thermodynamic limit is modeled by a **stable unitary topological quantum field theory (TQFT)**.

2D Topological Phases in Nature

- Quantum Hall States

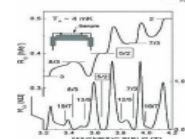
1980 Integral Quantum Hall Effect ---
von Klitzing (1985 Nobel)



1982 Fractional QHE---Stormer, Tsui, Gossard at $\nu = \frac{1}{3}$
(1998 Nobel for Stormer, Tsui, and Laughlin)

1987 Non-abelian FQHE???"---R. Willett et al at $\nu = \frac{5}{2}$

- Topological superconductors
- Topological insulators
- ...



$$R_H = \nu^{-1} \frac{h}{e^2}$$

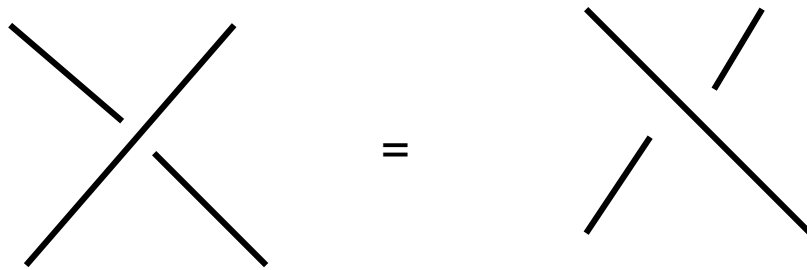
Anyons

- **Anyons:** quasi-particles or **topological excitations** in topological phases of matter. Their statistics are more general than bosons/fermions, can be even non-abelian--- $k \times k$ matrices.
- **Models:** **Simple objects** in unitary modular tensor categories.

Statistics of Particles

In \mathbb{R}^3 , particles are either bosons or fermions

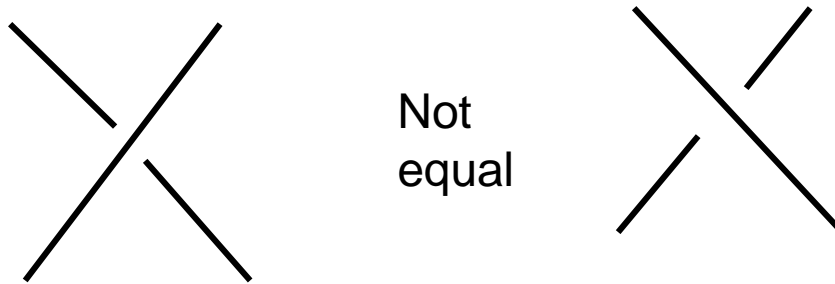
Worldlines (curves in $\mathbb{R}^3 \times \mathbb{R}$) exchanging two **identical** particles depend only on permutations



Statistics is $\lambda: \mathbf{S}_n \rightarrow \mathbf{Z}_2$

Braid Statistics

In \mathbb{R}^2 , an exchange is of infinite order



Braids form groups B_n

Statistics is $\lambda: B_n \rightarrow U(k)$

If $k > 1$, non-abelian anyons

Non-abelian Statistics

If the ground state is not unique, and has a basis $\psi_1, \psi_2, \dots, \psi_k$

Then after braiding some particles:

$$\psi_1 \longrightarrow a_{11}\psi_1 + a_{12}\psi_2 + \dots + a_{k1}\psi_k$$

$$\psi_2 \longrightarrow a_{12}\psi_1 + a_{22}\psi_2 + \dots + a_{k2}\psi_k$$

.....

$$\lambda: B_n \longrightarrow U(k)$$

Do non-abelian anyons exist?

The search for Majoranas or the Jones rep of the braid group at 4th root of unity in the real world

Of all exotic excitations believed to exist in topological quantum physics, we are the closest to detecting and harnessing Majoranas.

perspective

Majorana returns

F. Wilczek, Nature Physics'09



Physics Today / Volume 64 / Issue 3 / SEARCH AND DISCOVERY

Physics Today - March 2011

The expanding search for Majorana particles

Barbara Goss Levi

Science, April (2011)



NEWS

Search for Majorana Fermions Nearing Success at Last?

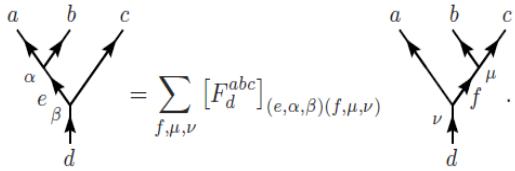
Researchers think they are on the verge of discovering weird new particles that borrow a trick from superconductors and could give a big boost to quantum computers

Anyon Models

- **Label set:** a finite set $L=\{a,b,c,\dots\}$ of anyon types or labels with an involution and a trivial type. E.g. any finite group G .
- **Fusion rules:** $\{N_{ab}^c, a,b,c\in L\}$. The fusion rules determine when two anyons of types a,b are fused, whether or not anyons of type c appear, i.e. if N_{ab}^c is ≥ 1 or $=0$.
- The Frobenius-Perron eigenvalue of the matrix N_a is the quantum dimension of a .
- Others

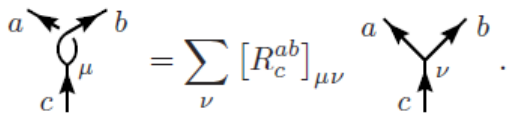
Anyon Model $\mathcal{C} = \text{UMTC}$

A modular tensor category = a non-degenerate braided spherical fusion category: a collection of numbers $\{L, N_{ab}^c, F_{d;nm}^{abc}, R_c^{ab}\}$ that satisfy some polynomial constraint equations.



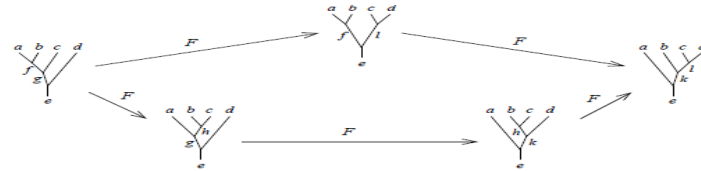
$$\begin{array}{c} a \\ \swarrow \\ \alpha \\ \searrow \\ e \end{array} \begin{array}{c} b \\ \swarrow \\ \beta \\ \searrow \\ e \end{array} \begin{array}{c} c \\ \swarrow \\ \beta \\ \searrow \\ e \end{array} = \sum_{f, \mu, \nu} [F_d^{abc}]_{(e, \alpha, \beta)(f, \mu, \nu)} \begin{array}{c} a \\ \swarrow \\ \nu \\ \searrow \\ d \end{array} \begin{array}{c} b \\ \swarrow \\ f \\ \searrow \\ d \end{array} \begin{array}{c} c \\ \swarrow \\ \mu \\ \searrow \\ d \end{array} .$$

6j symbols for recoupling

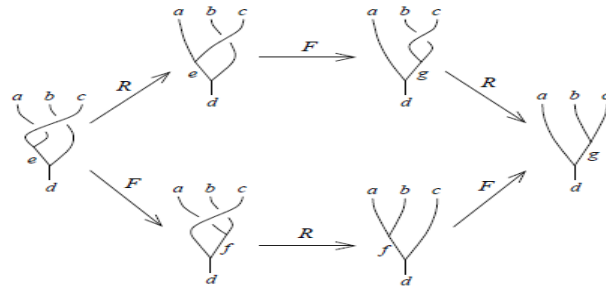


$$\begin{array}{c} a \\ \swarrow \\ \mu \\ \searrow \\ c \end{array} \begin{array}{c} b \\ \swarrow \\ \mu \\ \searrow \\ c \end{array} = \sum_{\nu} [R_c^{ab}]_{\mu \nu} \begin{array}{c} a \\ \swarrow \\ \nu \\ \searrow \\ c \end{array} \begin{array}{c} b \\ \swarrow \\ \nu \\ \searrow \\ c \end{array} .$$

R-symbol for braiding



Pentagons for 6j symbols



Hexagons for R-symbols

Ising Theory

Ising=M(3,4) minimal model
=TL at 4th root

Particle types: $\{1, \sigma, \psi\}$

q-dimensions: $\{1, \sqrt{2}, 1\}$

Fusion rules:

1---ground state

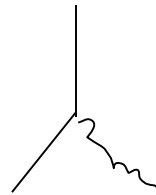
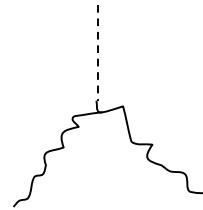
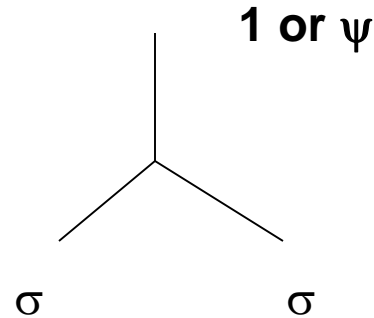
ψ ---Majorana fermion

σ ---Ising anyon

$$\sigma^2 \cong 1 + \psi,$$

$$\psi^2 \cong 1,$$

$$\sigma \psi \cong \psi \quad \sigma \cong \sigma$$

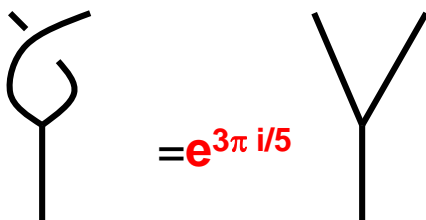


Fibonacci Theory

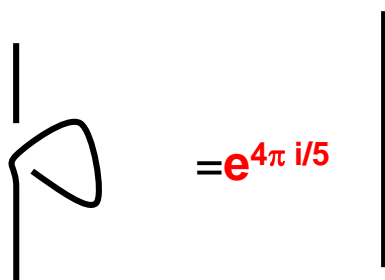
G_2 level=1 CFT, $c=14/5 \pmod 8$

- Particle types: $\{1, \tau\}$, τ ---Fib anyon
- Quantum dimensions: $\{1, \phi\}$, ϕ =golden ratio
- Fusion rules: $\tau^2=1 \oplus \tau$

- Braiding:



- Twist:



Topological Quantum Computation

Freedman 97, Kitaev 97, FKW 00, FLW 00

Computation

Physics

readout

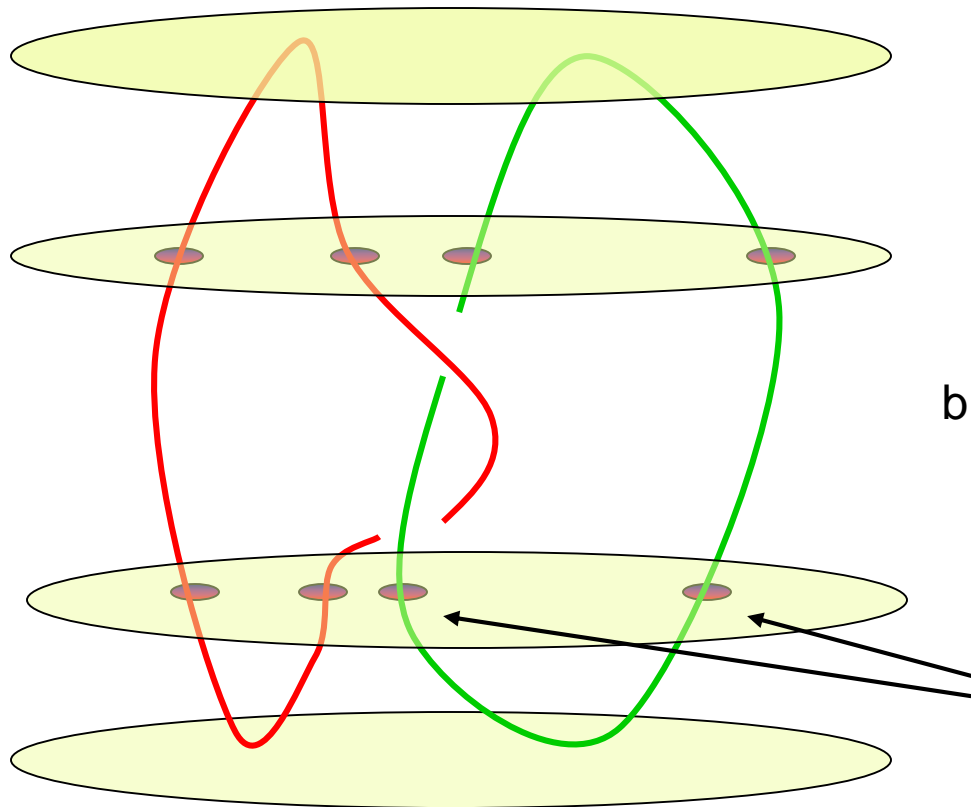
fusion

applying gates

braiding particles

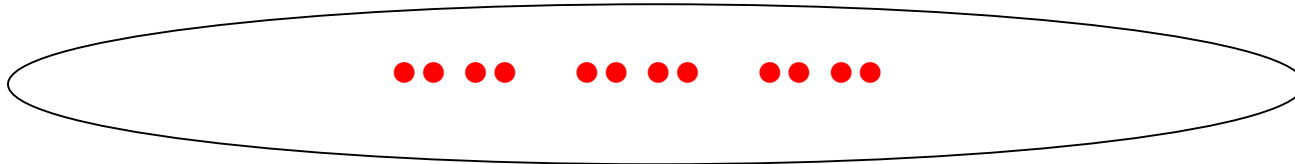
initialize

create
anyons



Anyonic Quantum Computer

For n qubits, consider the $4n$ anyons
 $\rho: \mathbf{B}_{4n} \rightarrow \mathbf{U}(N_{4n})$, e.g. $N_{4n} \sim 4n-2$ Fib number



Given a quantum circuit on n qubits

$$U_L: (\mathbb{C}^2)^{\otimes n} \longrightarrow (\mathbb{C}^2)^{\otimes n}$$

Topological compiling: find a braid $b \in \mathbf{B}_{4n}$ so that the following commutes for any U_L :

$$\begin{array}{ccc}
 (\mathbb{C}^2)^{\otimes n} & \xrightarrow{\quad} & V_{4n} \\
 U_L \downarrow & & \downarrow \rho(b) \\
 (\mathbb{C}^2)^{\otimes n} & \xrightarrow{\quad} & V_{4n}
 \end{array}
 \qquad V_{4n}\text{-gs of } 4n \text{ anyons}$$

Mathematical Theorems

Theorem 1 (Freedman-Kitaev-W.): Any unitary (2+1)-TQFT can be efficiently simulated by the quantum circuit model.

There are efficient additive approximation algorithms of quantum invariants by the quantum circuit model.

Theorem 2 (Freedman-Larsen-W.): Anyonic quantum computers based on RT/WCS $SU(2)$ -TQFTs at level k are braiding universal except $k = 1, 2, 4$.

The approximation of Jones poly of links at the $(k + 2)^{\text{th}}$ root of unity ($k \neq 1, 2, 4$) is a BQP-complete problem.

Theorem 3 (Cui-W., Levaillant-Bauer-Bonderson-Freedman-W.): Anyonic model based on $SU(2)$ at level $k = 4$ is universal for quantum computation if braidings are supplemented with (projective or interferometric) measurements in the middle of computation.

Universality of Braiding Gates

In 1981, Jones proved that the images of his unitary representation $\rho_{r,a}(B_n)$ of the braid groups are infinite

(same as anyon statistics in Reshetikhin-Turaev/Witten-Chern-Simons $SU(2)_k$ -TQFTs for $k=r-2$)

if $r \neq 1, 2, 3, 4, 6$, $n \geq 3$ or $r = 10$, $n \neq 4$,
and asked:

What are the closed images of $\rho_{r,a}(B_n)$ in the unitary groups?

Density Theorem (FLW):

Always contain $SU(N_{r,a})$ if $r \neq 1, 2, 3, 4, 6$ and $n \geq 3$ or $r=10$, also $n \neq 4$.

Others are finite groups which can be identified.

Proof is a general solution of 2-eigenvalue problem and generalized to 3-eigenvalue by Larsen-Rowell-W.

Computational Power of Braiding Gates

- Ising anyon σ does not lead to universal braiding gates, but Fib anyon τ does
- Quantum dimension of Ising anyon σ has quantum dimension $=\sqrt{2}$, while Fib anyon τ has quantum dimension $\phi=(\sqrt{5}+1)/2$ ---golden ratio
- Given an anyon type x , when does it lead to universal braiding gate sets?

Rowell conjecture: **Braid universal iff $d_x^2 \neq \text{integer}$**

Quantum Mathematics:

Quantization and Categorification

TQFT and Higher Category

