

Topological Quantum Computing

Zhenghan Wang
Indiana University
Microsoft Project Q

Microsoft Project Q at Santa Barbara (visiting KITP/CNSI)

C. Nayak



M. Freedman

K. Walker



A. Kitaev

Eddy
Ardonne



Adrian Feiguin



Joost Slingerland

Simon
Trebst



Topological Quantum Computing:

1981 Jones---UNITARY rep of the braid groups

**1982 Stormer, Tsui, Gossard---FQHE
Nobel Prize 1998, Stormer, Tsui, Laughlin**

1989 Witten---Jones polynomial using TQFT

**1991 Welsh, Jaeger, Vertigan---exact computation
of $\{J(L,q), q=e^{2\pi i/r}\}$ of all links is # P hard for
 $r \neq 1,2,3,4,6$, while $r=1,2,3,4,6$ is poly-time**

**1990? Condensed matter physicists proposed
Chern-Simons theory as the effective theory for FQHE**

**1991 Moore, Read---propose non-abelian anyons
in FQHE using conformal field theory**

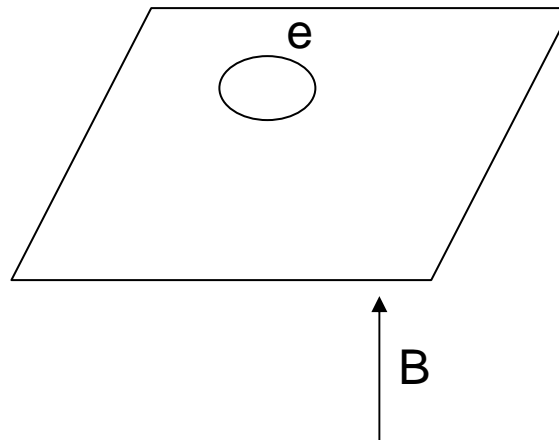
- 1997** Freedman suggested TQFT computers.
Kitaev proposed anyonic QC as an inherently
fault-tolerant quantum computing model
- 1999** Freedman, Kitaev, Larsen, Wang:
Computation based on TQFT is poly-equivalent to QCM
- 1998?** Preskill's Caltech group---topological quantum
computing mostly based on "weak" TQFTs
- 2005** Microsoft Project Q:
Nexus among quantum topology, quantum physics
and quantum computing
Searching for non-abelian anyons in Nature

2D Electron Systems

$N \sim 10^{11} \text{ cm}^{-2}$

$B \sim 10 \text{ T}$

$T \sim 9 \text{ mK}$



Depending on $N/B = \nu$, the Landau filling fraction
electron crystals, IQHE liquids, FQHE liquids

Realistic Hamiltonian:

$$H = \sum_j [\nabla_j + A(r_j)]^2 + \sum_{j < k} V(r_i - r_j)$$

What are the electrons doing?

**But for $\nu=1/3$ FQHE, guessed by Laughlin:
dancing collectively following the distribution
given by the norm squared of the Laughlin
wavefunction:**

$$|\Psi\rangle \sim \prod_{i<j} (z_i - z_j)^3 e^{-1/4l^2 \sum_i |z_i|^2},$$

**where z_i is the position of the i -th electron.
Furthermore, elementary excitations are
anyons, carrying charge $e/3$. (vortices in the
electron liquids)**

Effective Description of FQHE

Electron crystals, IQHE liquids fit into existing framework, and U(1)-Chern-Simons theory explains many FQHE liquids with abelian anyons. Anyons are elementary collective excitations.

But there are exceptions: believed to have non-abelian anyons, and to be related to SU(2)-Chern-Simons theory. (High T_c superconductors)

Project Q is an effort to understand those quantum systems as TQFTs and use them for quantum computing.

The Framework of Quantum Mechanics:

1. A state of a quantum system is represented by a non-zero vector in a Hilbert space V up to non-zero scalars.
---Superposition
2. Evolution is given by a unitary transformation of the Hilbert space V .
---Schrodinger
3. An observable such as position, momentum, energy, spin... is represented by an Hermitian operator H .
When H is measured in a state $|\psi\rangle$, then $|\psi\rangle$ collapses to an eigenstate of H with probability $|a_\lambda|^2$:
$$V = \bigoplus_{\lambda \in \text{spec}(H)} V_\lambda, \quad |\psi\rangle = \sum a_\lambda |e_\lambda\rangle$$

where $|e_\lambda\rangle$'s form an orthonormal basis of V .
---Uncertainty
4. If V_1, V_2 are the Hilbert spaces of two quantum systems, then the Hilbert space of the composite system is the tensor product $V_1 \otimes V_2$.
---Entanglement

Quantum information science:

---Storage, processing and communicating information using quantum systems.

Three milestones in QIS:

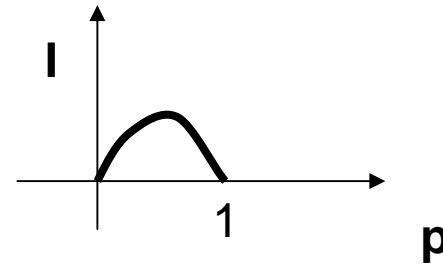
- 1. Shor's poly-time factoring algorithm (1994)**
- 2. Error-correcting code, thus fault-tolerant quantum computing (1996)**
- 3. Security of private key exchange (BB84 protocol)**

- **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

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

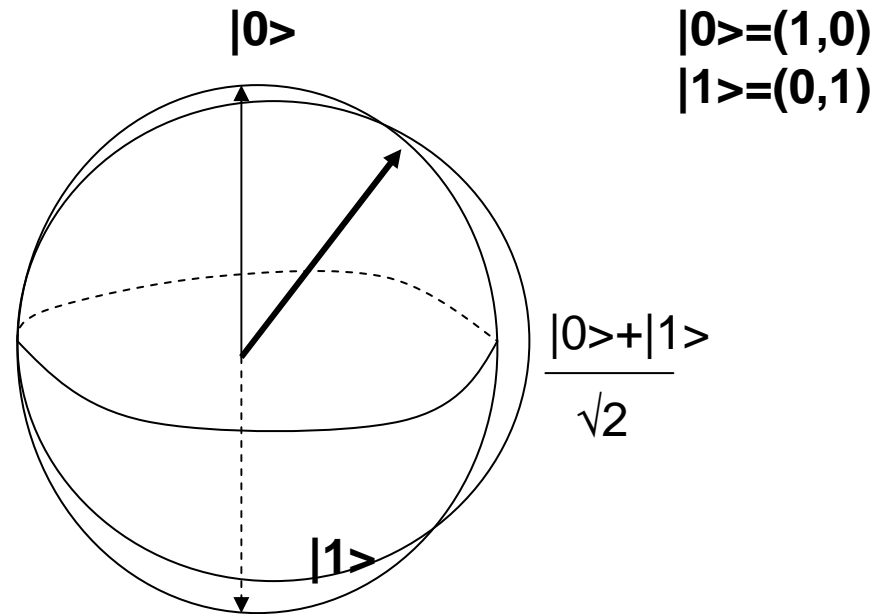


- **A state of a quantum system is an information source**

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

The states of a qubit is parameterized by the Bloch sphere:

$$S^2 = CP^1$$



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 $\{0,1\}^n \rightarrow \{0,1\}^{m(n)}$

Name: Factoring

Instance: an integer $N > 0$

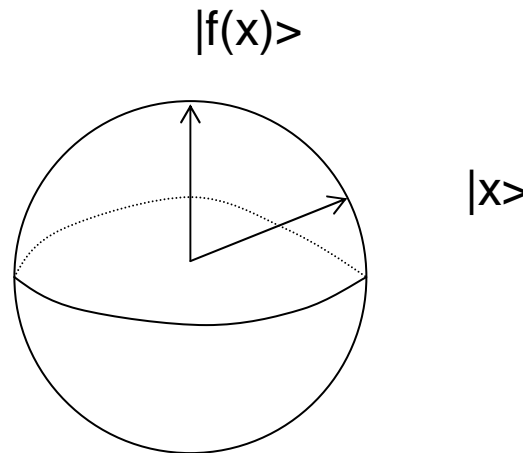
Question: Find the largest prime factor of N

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

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

How a quantum computer works

**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 gates:

e.g. $\sigma_z^{\pm 1/4} = \begin{pmatrix} 1 & 0 \\ 0 & e^{\pm \pi i/4} \end{pmatrix}$ $H = 2^{-1/2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ Hadamard

CNOT = $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ $|00\rangle \rightarrow |00\rangle$
 $|01\rangle \rightarrow |01\rangle$
 $|10\rangle \rightarrow |11\rangle$
 $|11\rangle \rightarrow |10\rangle$

$$\mathbf{C}^2 \otimes \mathbf{C}^2 \rightarrow \mathbf{C}^2 \otimes \mathbf{C}^2$$

Universality

Theorem 1: Any matrix in $U(2^m)$ is a finite composition of $U(2)$ and CNOT matrices (tensoring with identities).

Theorem 2: Finite compositions of $\sigma_z^{\pm 1/4}$ and Hadamard matrix H are dense in $SU(2)$.

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 (bounded error quantum polynomial-time)
Fix a universal gate set

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

1) there exists an efficient classical algorithm (i.e. a Turing machine) that computes a function $x \rightarrow D_x$, where $x \in \{0,1\}^n$, and D_x encodes a poly(n)-qubit circuit U_L .

2) when the state $U_L|0 \dots 0\rangle$ is measured in the standard basis $\{|i_1 \dots i_{p(n)}\rangle\}$, 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 can be efficiently computed by a TM can be computed efficiently by a QC, i.e. $BPP \subseteq BQP$

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

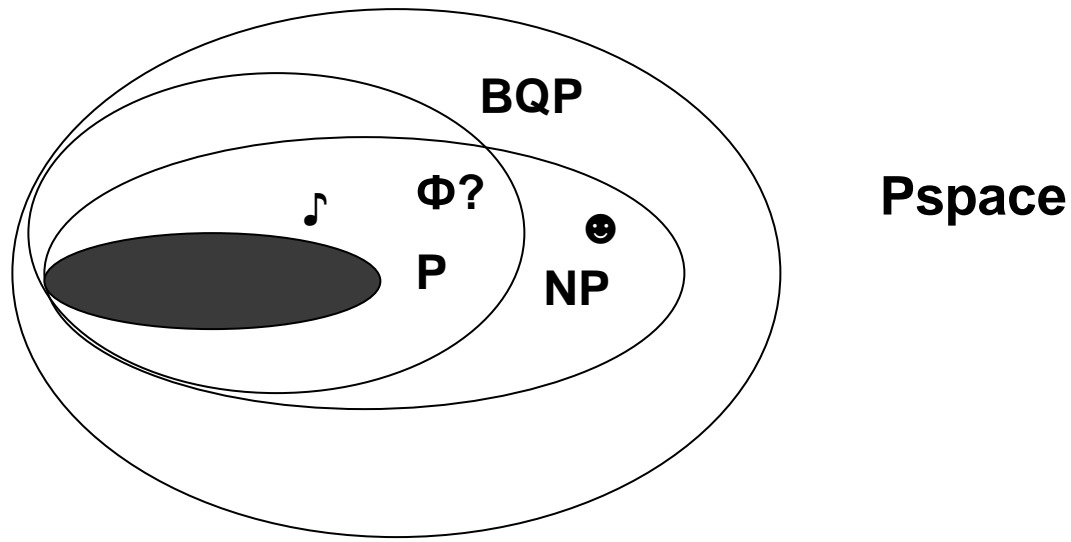
Given an n bit integer $N \sim 2^n$

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

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

For $N=2^{400}$, classically \sim billion years

Quantum computer \sim 1 second



Hidden subgroup problem

H a hidden subgroup of a finite group G , and $f: G \rightarrow X$ (X some set) such that a) f is constant on left cosets, and b) f takes different values on different cosets.

Find a generating set of H using only poly ($\log |G|$) many evaluations.

- 1. Simon's algorithm: $G = \mathbb{Z}_2^n$, $X = \mathbb{Z}_2^n$, $H = \mathbb{Z}_2\{a\}$**
- 2. Shor's algorithm: $G = \mathbb{Z}_{\phi(N)}$**
- 3. True for finitely generated abelian group**
- 4. Open for non-abelian groups
(Graph Isomorphism Problem: S_n)**

Can we build a large scale universal QC?

The obstacle is mistakes and errors (decoherence)

Error correction by simple redundancy

$0 \rightarrow 000, 1 \rightarrow 111$

Not available due to the No-cloning theorem:

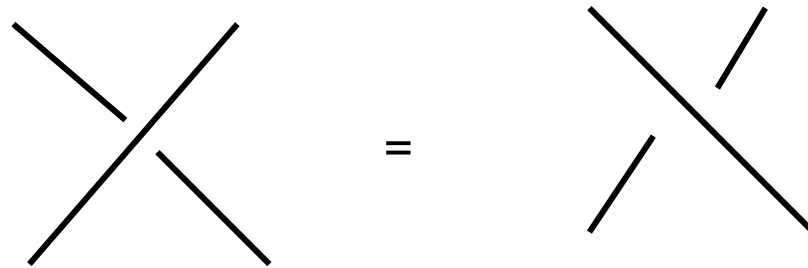
The cloning map $|\psi\rangle \otimes |0\rangle \rightarrow |\psi\rangle \otimes |\psi\rangle$ is not linear.

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

QC with non-abelian anyons

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

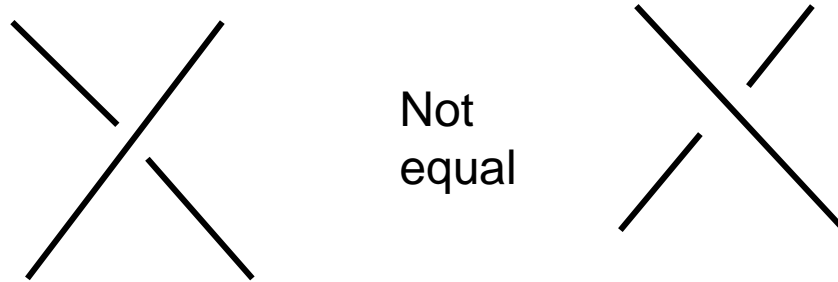
Worldlines (curves in $\mathbb{R}^3 \times \mathbb{R}$) exchanging two identical particles depend only on permutations



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 $\lambda: B_n \rightarrow U(1)$

**If not 1 or -1, but $e^{i\theta}$, abelian
anyons**

Non-abelian anyons

Suppose the ground state of n identical particles is degenerate, and has a basis $\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_k$

Then after braiding some particles:

$$\mathbf{e}_1 \rightarrow a_{11}\mathbf{e}_1 + a_{21}\mathbf{e}_2 + \dots + a_{k1}\mathbf{e}_k$$

•
•

Particle statistics is $\lambda: \mathbf{B}_n \rightarrow \mathbf{U}(k)$

Particles with $k > 1$ are called non-abelian anyons

Do non-abelian anyons exist?

Mathematically, are there unitary braid group representations?

Burau reps, 1936 (Squier 1984)

Alexander polynomial (Det, poly time)

Jones reps indexed by r , 1981

**Jones polynomial (Markov trace,
#P-hard unless $r=1,2,3,4,6$)**

Non-abelian anyons physically???

The elementary excitations (= vortices) in FQHE liquids are anyons.

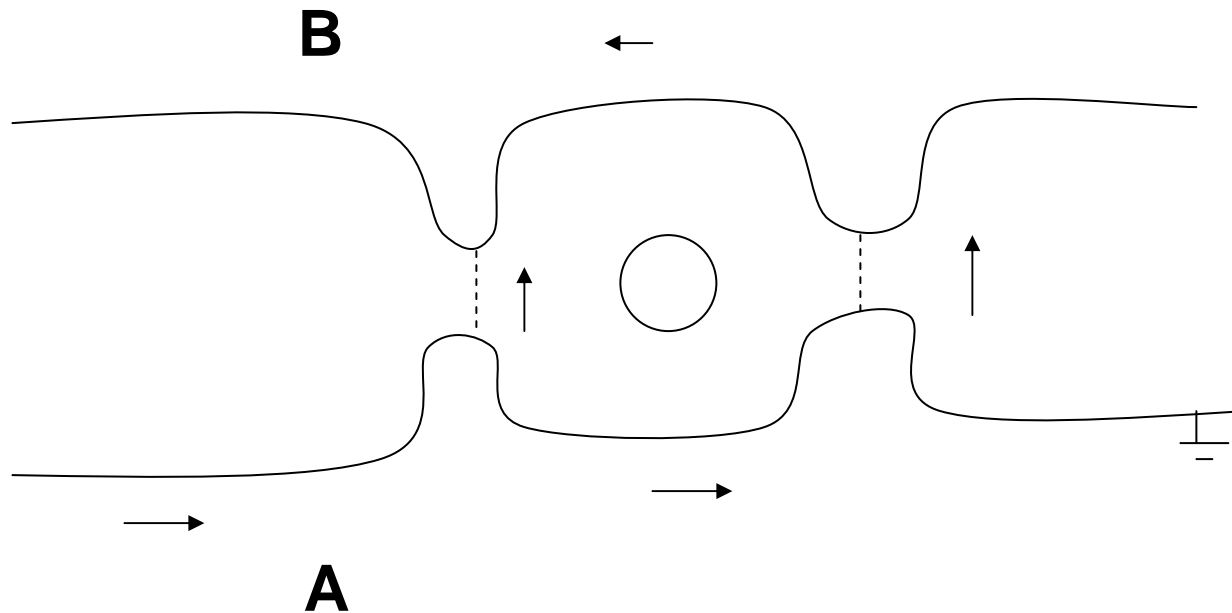
Let V be the ground states of the electron system with n anyons at certain positions in the plane.

If $\dim V > 1$, those anyons will be non-abelian anyons.

Read-Rezayi conjecture:

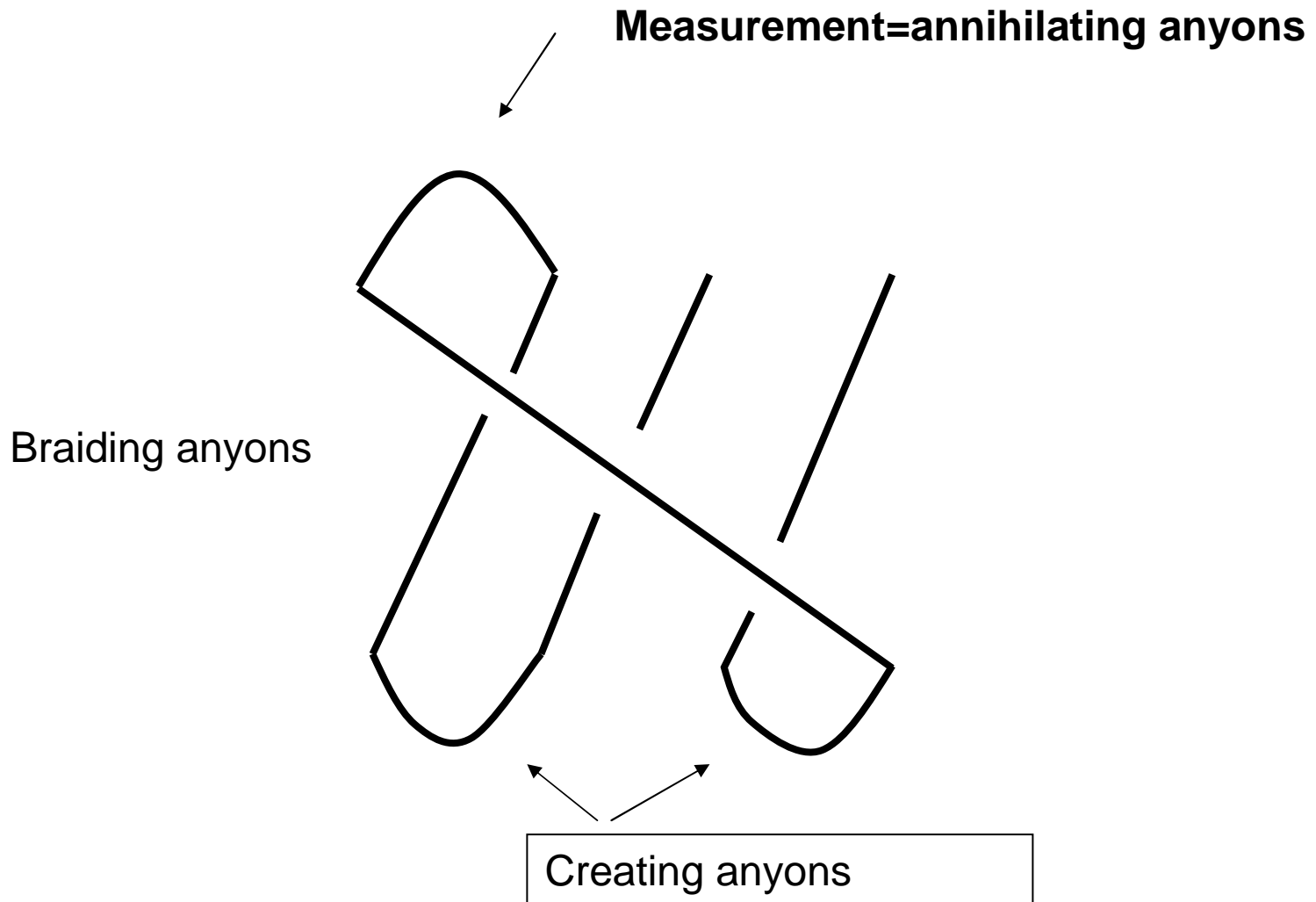
$\nu=1/3$ or $2/3$	\longleftrightarrow	Jones rep at $r=3$ (Abelian, Laughlin)
$\nu=5/2$	\longleftrightarrow	Jones rep at $r=4$ (Not Universal)
$\nu=13/5$ (or $12/5$)	\longleftrightarrow	Jones rep at $r=5$ (Universal QC)

Confirmation



Inject quasi-particles at A along the lower edge, and measure the current at B, which depends on the Jones polynomial of a link such as the Hopf link.

Hypothetical Topological Quantum Computers

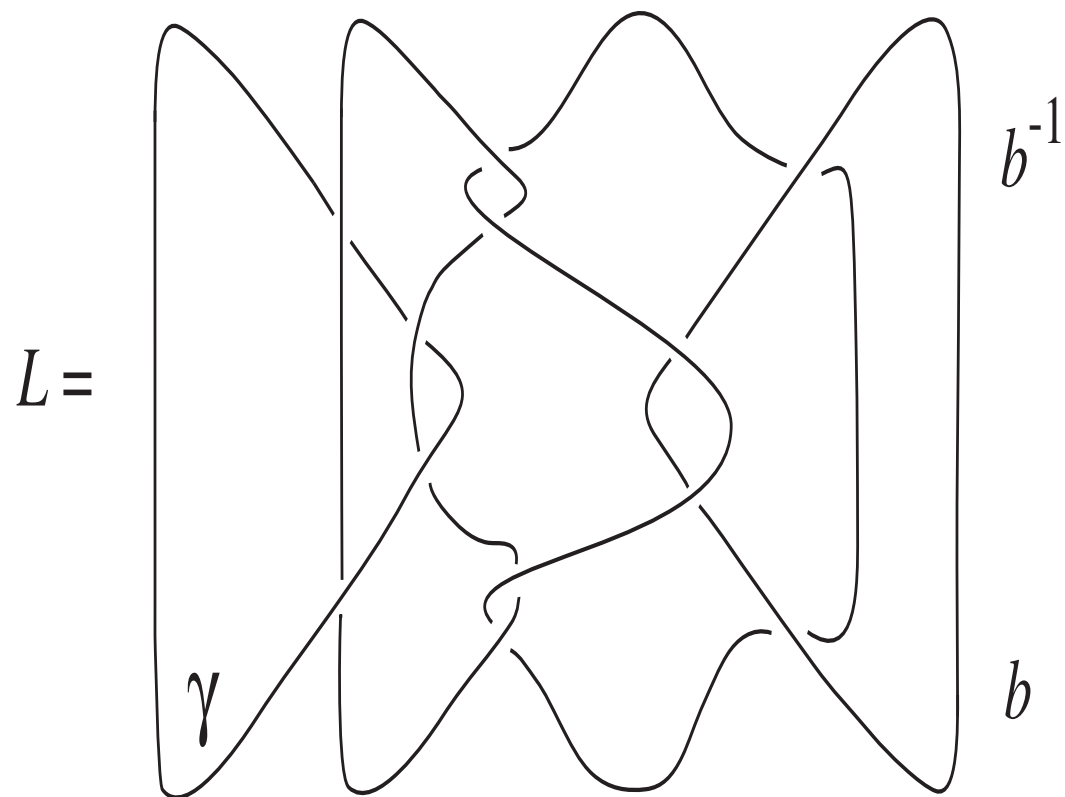


What TQC computes?

Start with the cup state $|\text{cup}\rangle$, braid as b , and annihilate the two leftmost particles, and record the resulting particle type. Repeat the process to get an approximation of the probability of observing any particle type.

The probability to observe the particle type 0 is $\langle \text{cap} | \rho^+(b) \Pi_0 \rho(b) | \text{cup} \rangle$, which is the link invariant for the following link L , hence TQC approximates link invariants.

γ is labeled by a projector onto 0, and b by the braided particle type



Main Theorems

Theorem 1 (FKW): Any unitary TQFT can be efficiently simulated by quantum computers.

Hence the related quantum invariants can be efficiently approximated by quantum computers.

Theorem 2 (FLW): Topological quantum computers based on the Jones rep of the braid groups (or SU(2)-Chern-Simons theory) are universal except $r=1,2,3,4,6$.

Hence the approximation of the Jones poly at 5th root of unity is a BQP complete problem.

Work in progress:

1. Mathematics

Classifications of TQFTs

2. Physics

**Model and search for topological
phases of matter**

•Error correction and fault tolerance will be essential in the operation of large scale quantum computers.

The “brute force” approach to fault-tolerant quantum computing uses clever circuit design to overcome the deficiencies of quantum hardware. It works in principle, but achieving it in practice will be challenging.

•Topological quantum computing is a far more elegant approach, in which the “hardware” is intrinsically robust due to principles of local quantum physics (if operated at a temperature well below the mass gap).

The topological approach also looks daunting from the perspective of current technology. But it is an attractive and promising long-term path toward realistic quantum computing. As a bonus, there are fascinating connections with deep issues in quantum many-body physics!

John Preskill

and mathematics.