Introduction to Topological Quantum Computing

Zhenghan Wang
Microsoft Station Q & UC Santa Barbara

New Mexico State, Oct. 18, 2019
Why Quantum Computing?

More than 4000 years between Abacus and modern chip, but same principles and information unit---the **Bits**.

Quantum building blocks fundamentally different—the **Qubits**.

1. **Inevitability**: Moore’s law comes to an end
2. **Desirability**: Potential exponential speed-up
3. **Feasibility**: fault-tolerant computation possible
"As a generality, we propose that each physical theory supports computational models whose power is limited by the physical theory. It is well known that classical physics supports a multitude of the implementation of the Turing machine". Freedman further suggested that computational models based on some TQFTs might be more powerful than quantum computing—the computing model based on quantum mechanics. But when accuracy and measurement are carefully analyzed, the computing model based on TQFTs are polynomially equivalent to quantum computing $P/\text{NP}$, and the quantum field computer

Michael H. Freedman

Classical Physics

Quantum Mechanics

Quantum Field Theory

Topological Quantum Field Theories $=$ Quantum Mechanics

Freedman, Kitaev, W., 02

Freedman, Larsen, W., 02
QM 1: New States of Existence

• **Superposition:**
  In quantum world, all available classical states form a quantum definite state in a superposition with prescribed complex amplitudes.

• **Entanglement:**
  Sub-systems lost their pure states in entangled states ---only the whole system has definite states and subsystems have spooky action.
QM 2: New Dynamical Behavior

- All classical states in a quantum state evolve in parallel as time goes by.
- Classical impossible event forbidden by energy barrier could happen due to quantum tunneling.
- Quantum states can be teleported through reconstruction via entangled “DNA”.
Qubits

Modern name of a two-level quantum system such as electron spin and their composites. States of n-qubits are non-zero vectors in \( (\mathbb{C}^2)^\otimes n = \mathbb{C}[\mathbb{Z}_2^n] \)
Quantum Computing

Given

\[ f(x) = \{ f_n(x) : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^m \} \]
\[ x \in \mathbb{Z}_2^n \text{ a bit string} \]

- The initial input \( x \) is encoded onto some physical system.
- The evolution of the physical system processes \( x \).
- The computational result \( f(x) \) is read out through some measurement of the system.

Find \( U_x \) such that

\[ U_x |x\rangle = |f(x)\rangle \]
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 $|1\rangle$

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

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

$$|\alpha|^2 + |\beta|^2 = 1 \quad s \in CP^1$$

• **Entanglement**

Quantum states need not be products. For example:

$$|\Psi_{AB}\rangle = \frac{1}{\sqrt{2}} (|0_A0_B\rangle + |1_A1_B\rangle)$$

$$\neq |\psi_A\rangle \otimes |\phi_B\rangle$$

This is the property that enables quantum state teleportation and Einstein’s “spooky action at a distance.”
Can We Build a Useful Certifiable 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 decoherence.

Classical error correction by redundancy

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

Not available due to the No-cloning theorem:

The cloning map $|\psi> \otimes |0> \rightarrow |\psi> \otimes |\psi>$ is not linear.
Key “Post-Shor” Idea

To use topology to protect quantum information

Peter Shor
Shor’s Factoring Algorithm

Michael Freedman

Alexei Kitaev
\( P/\text{NP} \), 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.)
• **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).
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 Quantum Computation

Freedman 97, Kitaev 97, FLW 00

Computation
- readout
- applying gates
- initialize

Physics
- fusion
- braiding particles
- create anyons
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
  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
- ...
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 $\lambda: S_n \rightarrow \mathbb{Z}_2$.
Braid Statistics

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

\[ \not= \]

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 $\psi_1, \psi_2, \ldots, \psi_k$

Then after braiding some particles:

\[
\begin{align*}
\psi_1 &\rightarrow a_{11}\psi_1+a_{12}\psi_2+\ldots+a_{k1}\psi_k \\
\psi_2 &\rightarrow a_{12}\psi_1+a_{22}\psi_2+\ldots+a_{k2}\psi_k \\
&\ldots.
\end{align*}
\]

$$\lambda: B_n \rightarrow U(k)$$
X self-dual with fusion rule

\[ X \otimes X = 1 \oplus Y \oplus \cdots, \]

The braid \( b \) is non-trivial.

Anyon Models

• **Label set**: a finite set \( L = \{a, b, c, \ldots \} \) 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 \( \geq 1 \) 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.
Majorana Systems

Ising Anyon $\sigma$ and Majorana fermion

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

Quantum dim: $\{1, \sqrt{2}, 1\}$

Fusion rules:

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

1 --- ground state
$\psi$ --- self-conjugate
(Majorana) fermion
$\sigma$ --- Ising anyon (square root of electrons)

All self-conjugate
Majorana Qubit

Degeneracy and braiding of four Ising anyons $\sigma$ with fixed total charge or the fusion channels of a pair of Ising anyons (total charge not fixed).
Fibonacci Theory
G_2 level=1 CFT, c=14/5 mod 8

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

- Braiding:

- Twist:
Anyonic Quantum Computer (Sparse)

For \( n \) qubits, consider the \( n \) groups of 4 anyons
\[
\rho: B_{4n} \rightarrow U(V_{4n}),
\]

Given a quantum circuit on \( n \) qubits
\[
U_L: (C^2)^{\otimes n} \rightarrow (C^2)^{\otimes n}
\]

Topological compiling: find a braid \( b \in B_{4n} \) so that the following commutes for any \( U_L \):
\[
\begin{align*}
(C^2)^{\otimes n} & \xrightarrow{U_L} V_{4n} \\
(C^2)^{\otimes n} & \xrightarrow{\rho(b)} V_{4n}
\end{align*}
\]
Stingy Nature

• Jones:

Braid representation is finite for SU(2)_k (k = 1, 2, 4), infinite otherwise

• Freedman, Larsen, Wang (2001):

Actual density in PU when infinite

Mother nature seems to be forcing us to work with SU(2)_2/U(1)=Ising anyon, i.e. Majorana physics

Missing $\frac{\pi}{8}$-gate $T=\begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{\pi i}{4}} \end{pmatrix}$ from the standard gate set
Hierarchy of $SU(2)_k$ Computational Power

- $k=1$, abelian (semion)
- $k=2$, Ising non-abelian but classically efficiently simulable, good for memory
- $k=3$, Fibonacci braiding universal
- $k=4$, braiding non-universal, but can be made universal by supplementing braiding with measurement. $SU(2)_4$ is the first of a sequence of interesting anyon systems.
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 $\sigma$ does not lead to universal braiding gates, but Fib anyon $\tau$ does

• Quantum dimension of Ising anyon $\sigma$ has quantum dimension $=\sqrt{2}$, while Fib anyon $\tau$ has quantum dimension $\phi=(\sqrt{5}+1)/2$---golden ratio

• Given an anyon type $x$, when does it lead to universal braiding gate sets?

Property F conjecture: Braid universal iff $d_x^2 \neq \text{integer}$
New Qudit Gate Sets

• The standard qubit gate set: Hadamard, $\pi/8$ T-gate, and CNOT.

• The qudit generalization of Hadamard is the generalized Hadamard $H_d = \frac{1}{\sqrt{d}} (\omega_d^{ij})$

• The generalized “Pauli-gates” $Q_{d,j} = (\omega_d^{\delta_{ij}})$

• The generalized CNOT gate $SUM_d$:
  $SUM|i,j> = |i, i+j \mod d>$
Qubits, Qutrits and Qupits

• $d=2$, $Q_1$ is Pauli $Z$. For universality, $T$-gate is a 4$^{th}$ root of $Z$.
• $d=3$, any 2$^{nd}$ root $P_j = (-\omega_3^2)^{\delta_{ij}}$ of $Q_j$ will lead to a universal gate set.
• $d=p>3$ prime, all $Q_j$ suffice.
• For qubits, $H$, CNOT and Phase lead to Clifford circuits and for qutrits, $H_3$, $SUM_3$ and $Q_j$ lead to generalized Clifford circuits.
Metaplectic Anyon Systems

• An anyon system with fusion rules $SO(N)_2$.
• Weakly Integral and Property F, so braiding alone is not universal for quantum computation.
• Like Ising, more realistic, and computational power of braiding weak. But universal when braiding is supplemented with measurement.
(Joint work with Shawn Cui.)
\[ SU(2)_4 = SO(3)_2 \]

- The label set is \{1, x, y, x’, z\} with quantum dimensions \{1, \sqrt{3}, 2, \sqrt{3}, 1\}. Type x (or x’) anyons are metaplectic and type y metaplectic modes. Both have property F. So braidings alone are not universal.

- Surprisingly, x and y anyons are different that their associated link invariants potentially have very different computational complexity.
Fusion Rules

- $z$ is abelian: $zx = x'$, $zx' = x, zy = y$, $z^2 = 1$
- metaplectic anyon $x$ is weakly integral: $x^2 = 1 + y$
- metaplectic mode $y$ is integral: $y^2 = 1 + y + z$, $xy = x'y = x + x'$
- Consider 4 metaplectic anyons $x$ with total charge $= y$, it is a qutrit $C^3 = \{|1y>, |y1>, -|yy>\}$. 

\[ \text{Diagram:} \quad \begin{array}{c} \ \ / \ \ / \ \ / \\
\ x \quad x \quad x \quad x \\
\ 1/y \quad 1/y \\
\ y \\
\ \end{array} \]
Braiding Gates

- For 1-qutrit, the image of the 4-strand braid group $B_4$ is the generalized Clifford group of order 216, and there is a braid which leads to the $SUM_3$ gate (entangled).
- If we can get an extra gate to obtain all 1-qutrit gates, then we will have a universal gate set.
Measurement Primitive

• Add partial projective measurement to determine if the total charge of the first two metaplectic anyons in a qutrit is trivial or not.

• For $SU(2)_4$, braiding gates supplemented with this measurement are enough for universal quantum computation.
Second Quantum Revolution

New EE:
Emergence and entanglement

Information and Mathematics:
Shannon, Turing, Von Neumann, Shor, Freedman,…

Rich world of topological materials and quantum mathematics:

X.-G. Wen