Locality in Quantum Computation, II

Eric Rowell\textsuperscript{1} with
Z. Wang\textsuperscript{2}, C. Galindo\textsuperscript{3}, S.-M. Hong\textsuperscript{4}


September 2012
What is a Quantum Computer?

From [Freedman-Kitaev-Larsen-Wang ’03]:

**Definition**

*Quantum Computation* is any computational model based upon the theoretical ability to *manufacture, manipulate* and *measure* quantum states.
Primer on Quantum Mechanics

Basic Principles

- **Superposition**: a state is a vector in a Hilbert space $|\psi\rangle \in \mathcal{H}$
- **Schrödinger**: Evolution of the system is unitary $U \in \mathbf{U}(\mathcal{H})$
- **Entanglement**: Composite system state space is $\mathcal{H}_1 \otimes \mathcal{H}_2$
- **Wave-function collapse**: Measuring $|\psi\rangle = \sum_i a_i |e_i\rangle$ gives $|e_i\rangle$ with probability $|a_i|^2$. 
Fix $d \in \mathbb{Z}$ and let $V = \mathbb{C}^d$.

**Definition**

The *$n$-qudit state space* is the $n$-fold tensor product:

$$\mathcal{M}_n = V \otimes V \otimes \cdots \otimes V.$$  

A *quantum gate set* is a collection $S = \{U_i\}$ of unitary operators $U_i \in U(\mathcal{M}_{n_i})$ ($n_i$-local) usually $n_i \leq 4$. 

---


Locality in Quantum Computation, II
Quantum Circuits

Definition

A quantum circuit on $S = \{U_i\}$ is:

- $G_1 \cdot G_2 \cdots G_m \in U(M_n)$
- where $G_j = I_V^\otimes a \otimes U_i \otimes I_V^\otimes b$
- Given $U \in U(M_n)$ can only reasonably hope to approximate $U$ as $G_1 \cdot G_2 \cdots G_m$
Remarks on QCM

- Typical physical realization: composite of \( n \) identical \( d \)-level systems. E.g. \( d = 2 \): spin-\( \frac{1}{2} \) arrays.
- The setting of most quantum algorithms: e.g. Shor’s integer factorization algorithm
- QCM gates are algebraically local: the \( G_i \) act non-trivially on a few adjacent qudits.
- Main nemesis: decoherence—errors due to interaction with surrounding material. Requires expensive error-correction...
**Topological Phases of Matter (anyons)**

**Definition**

Topological Quantum Computation (TQC) is a computational model built upon systems of anyons (topological phases).

**Fractional Quantum Hall Liquid**

- $10^{11}$ electrons/cm$^2$
- $B_z \approx 10$ Tesla
- $T \approx 9$ mK
- quasi-particles

---

Anyons?!

- In \( \mathbb{R}^3 \): bosons or fermions: \( \psi(z_1, z_2) = \pm \psi(z_2, z_1) \)
- Particle exchange \( \rightsquigarrow \) reps. of symmetric group \( S_n \)
- In \( \mathbb{R}^2 \): anyons: \( \psi(z_1, z_2) = e^{i\theta} \psi(z_2, z_1) \)
- Particle exchange \( \rightsquigarrow \) reps. of braid group \( \mathcal{B}_n \)
- Mathematically: \( \mathbb{R}^3 \setminus \{z_i\} \) (dull) vs. \( \mathbb{R}^2 \setminus \{z_i\} \) (interesting)
Topological Model (non-adaptive)

**Computation**

- initialize
- apply gates
- output

**Physics**

- create anyons
- braid anyons
- measure (fusion)

vacuum

---

Eric Rowell\(^1\) with Z. Wang\(^2\), C. Galindo\(^3\), S.-M. Hong\(^4\) 1:Texas A&M U.; 2:Microsoft; 3:U. de los Andes; 4:U. Toledo

Locality in Quantum Computation, II
The Braid Group

A key role is played by the braid group:

Definition

$\mathcal{B}_n$ has generators $\sigma_i$, $i = 1, \ldots, n - 1$ satisfying:

(R1) $\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}$

(R2) $\sigma_i \sigma_j = \sigma_j \sigma_i$ if $|i - j| > 1$
Definition (Nayak, et al ’08)

A system is in a topological phase if its low-energy effective field theory is a topological quantum field theory (TQFT).

Fact

Most (known, useful) \((2 + 1)\)-TQFTs come from the Reshetikhin-Turaev construction via modular categories.
Definition (Heuristic)

- A **braided** category has a commutative tensor product:
  
  $c_{X,Y} : X \otimes Y \rightarrow Y \otimes X$

- A **ribbon** category allows one to “do topology”

$$
\mathcal{K}
\begin{pmatrix}
\text{ } & \text{ } & \text{ } \\
\text{ } & \text{ } & \text{ } \\
\text{ } & \text{ } & \text{ } \\
\end{pmatrix}
= \bigoplus_{\{a,b \in \mathcal{L}\}} \mathcal{K}
\begin{pmatrix}
\text{ } & \text{ } & \text{ } \\
\text{ } & \text{ } & \text{ } \\
\text{ } & \text{ } & \text{ } \\
\end{pmatrix}
$$

$$
= \bigoplus_{\{a \in \mathcal{L}\}} \mathcal{K}
\begin{pmatrix}
\text{ } & \text{ } & \text{ } \\
\text{ } & \text{ } & \text{ } \\
\text{ } & \text{ } & \text{ } \\
\end{pmatrix}
= C_{\mathcal{L}}
$$
Modular Categories

Definition (Heuristic)

A modular category is a ribbon category with a non-degenerate braiding and a manageable (finite) number of simple objects.

Example

- $Rep(G)$ (G a Lie algebra or finite group). boring braiding: $(\sigma_V, V)^2 = ld_{V \otimes V}$ bosons/fermions
- $Rep(A)$ (A a quantum Lie algebra or quantum double of a group). exciting braiding: $c^2_{X, X} \neq ld_{X \otimes X}$ anyons.
Remark

Key fact: in a modular category objects might not be vector spaces, but still have dimensions: $\text{FPdim}(X) \in \mathbb{R}_{>0}$, but not always $\mathbb{Z}$!

Definition

A fusion category $\mathcal{C}$:

- is weakly integral if $\text{FPdim}(X)^2 \in \mathbb{Z}$ for all $X$ simple
- and integral if $\text{FPdim}(X) \in \mathbb{Z}$ for all $X$ simple.
### Dictionary

<table>
<thead>
<tr>
<th>Modular Category</th>
<th>Anyonic System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simple objects $X_i$</td>
<td>anyons</td>
</tr>
<tr>
<td>$1$</td>
<td>vacuum type</td>
</tr>
<tr>
<td>dual objects $X^*$</td>
<td>antiparticles</td>
</tr>
<tr>
<td>$\text{Hom}(X, Y)$</td>
<td>state spaces</td>
</tr>
<tr>
<td>$c_{X, Y}$</td>
<td>particle exchange</td>
</tr>
<tr>
<td>$\det(S) \neq 0$</td>
<td>anyons distinguishable</td>
</tr>
<tr>
<td>$X_i \otimes X_j = \bigoplus_k N_{i,j}^k X_k$</td>
<td>ground state degeneracy</td>
</tr>
</tbody>
</table>
Sources of Modular Categories

Example

- $\mathcal{C}(g, \ell)$: semisimple subquotient of quantum group $\text{Rep}(U_q g)$ at $q = e^{\pi i/\ell}$. Typically $\text{FPdim}(X) \notin \mathbb{Z}$.

- $\text{Rep}(DG)$: quantum double $DG$ of finite group $G$. $\text{FPdim}(X) \in \mathbb{Z}$ for $X \in \text{Rep}(DG)$. 
Extended Read-Rezayi Conjecture

FQH Liquids distinguished by filling fraction $\nu = p/q$.

Conjecture

The TQFTs modelling FQH liquids at $\nu = 2 + \frac{k}{k+2}$ is the SU(2) level $k$ Chern-Simons TQFT.

Remarks

- $SU(2)_2$ is the “Ising theory”
- $SU(2)_3$ contains the “Fibonacci theory”
Example: $\mathcal{C}(\mathfrak{sl}_2, \ell) = SU(2)_{\ell-2}$

Example

$\mathcal{C}(\mathfrak{sl}_2, \ell)$ has simple objects $\{X_0, \ldots, X_{\ell-2}\}$ and:

- $\text{FPdim}(X_k) = \frac{\sin\left(\frac{(k+1)\pi}{\ell}\right)}{\sin\left(\frac{\pi}{\ell}\right)}$
- $X_1 \otimes X_k = X_{k-1} \oplus X_{k+1}$
- is weakly integral iff $\ell \in \{3, 4, 6\}.$
Universality?

Question
How powerful is a given TQC relative to a universal quantum computer?

Remarks
- A universal quantum computer can efficiently solve B(ounded error)Q(uantum resource)P(olynomial time) problems.
- The quantum circuit model is universal.
Topological Model

Remarks

- state space for $n$ particles of type $X \in \mathcal{C}$:
  $$\mathcal{H}_n^i := \text{Hom}(X_i, X \otimes n)$$

- Physically, gates are “particle exchanges” (braiding) acting on
  $$\mathcal{H}_n := \bigoplus_i \mathcal{H}_n^i.$$  

- Mathematically, gates are \( \{ \varphi_X^n(\sigma_i) \} \) where \( \varphi_X^n : \mathcal{B}_n \rightarrow \text{U}(\mathcal{H}_n) \)

- **Topological** protection from decoherence

$$
\begin{align*}
\text{Hubbard Model} & \quad \text{Hubbard Model} \\
\text{State Space} & \quad \text{State Space} \\
\text{Physically} & \quad \text{Physically} \\
\text{Mathematically} & \quad \text{Mathematically} \\
\text{Topological} & \quad \text{Topological}
\end{align*}
$$
Fix $X \in \mathcal{C}$, and suppose the decomposition of $\varphi_n^X$ into irreps. is:

$$\mathcal{H}_n \cong \bigoplus_j V_n^j$$

**Fact**

- For TQC to be universal, $\varphi_n^X(\mathcal{B}_n)$ must be dense in $\prod_j \text{SU}(V_n^j)$.
- Usually, enough that $|\varphi_n^X(\mathcal{B}_n)| = \infty$. 

Eric Rowell$^1$ with Z. Wang$^2$, C. Galindo$^3$, S.-M. Hong$^4$ 1:Texas, Locality in Quantum Computation, II
Example: $SU(2)_3$

$\varphi^5_n(B_n)$ acts on:

$$\text{Hom}_C(1, X^\otimes n) \oplus \text{Hom}_C(X, X^\otimes n)$$

$$\dim(\text{Hom}_C(X_i, X^\otimes n)) = \text{Fib}(n + i - 1)$$

$\varphi^5_n(B_n) \supset SU(\text{Fib}(n - 1)) \times SU(\text{Fib}(n))$
Quantum Computation Models
Foundational Problems
Qualitative Questions
Conjectural Answer to All Questions

Computational Power

Algebraic Universality

Question
For $X \in \mathcal{C}$ (modular), when is $|\varphi^n_X(B_n)| < \infty$?

Theorem (Jones ’86)
For $X \in \mathcal{C} (\mathfrak{sl}_2, \ell)$ braid group image $\varphi^n_X(B_n)$ infinite if and only if $\ell \not\in \{3, 4, 6\}$.

Theorem (Etingof, R, Witherspoon ’08)
For $X \in \text{Rep}(DG)$ images $\varphi^n_X(B_n)$ always finite.
INTERMISSION
Enjoy some chocolate-coated qubits in the lobby!
Topological quantum computers: fault-tolerant due to invariance under (physically) local perturbations.

Physical medium: topological phases. algebraically modeled by modular categories—generalizations of $\text{Rep}(G)$, $G$ a finite group.

Topological gates: braid group representations induced by adiabatic particle exchange.

Universality: encoded in density of braid group image.
Topological Model (non-adaptive)

Initialize

Create anyons

Apply gates

Braid anyons

Output

Measure (fusion)

Vacuum

Computation

Physics
Topological and Local?

Fact

Topological Models are not typically local.

- $\mathcal{H}_n = \bigoplus_i \text{Hom}(X_i, X^\otimes n) \neq V^\otimes f(n)$
- $\varphi^X_n(\sigma_i)$ smeared across all of $\mathcal{H}_n$.

Question

Can we uniformly “localize” $(\varphi^X_n, \mathcal{H}_n)$?

Recall: QCM has state spaces $\mathbb{C}^d \otimes \cdots \otimes \mathbb{C}^d$. 
Freedman *et al* showed that TQCs have a “hidden locality:” Let $U(\beta) \in U(\mathcal{H}_n)$ be a unitary braiding matrix. Goal: simulate $U$ on $V \otimes k(n)$ for some v.s. $X$.

- Set $V = \bigoplus_{(A,B,C)} \text{Hom}(A, B \otimes C)$ and $W = V \otimes (n-1)$
- TQFT axioms (gluing, disjoint union) imply: $\mathcal{H}_n \hookrightarrow W$

**Remark**

$V$ can be quite large and $U(\beta)$ only acts on the subspace $\mathcal{H}_n$. Forced to project, etc...
Definition

$(R, V)$ is a **braided vector space** if $R \in Aut(V \otimes V)$ satisfies

$$(R \otimes I_V)(I_V \otimes R)(R \otimes I_V) = (I_V \otimes R)(R \otimes I_V)(I_V \otimes R)$$

Induces a sequence of local $B_n$-reps $(\rho^R, V^\otimes n)$ by

$$\rho^R(\sigma_i) = I_V^\otimes i-1 \otimes R \otimes I_V^\otimes n-i-1$$

$v_1 \otimes \cdots \otimes v_i \otimes v_{i+1} \otimes \cdots \otimes v_n \xrightarrow{\rho^R(\sigma_i)} v_1 \otimes \cdots \otimes R(v_i \otimes v_{i+1}) \otimes \cdots \otimes v_n$

Idea: “braided QCM” gate set \{R\}
Square Peg, Round Hole?

Definition (R, Wang)

A **localization** of a sequence of $B_n$-reps. $(\rho_n, V_n)$ is a braided vector space $(R, W)$ and injective algebra maps $\tau_n : \mathbb{C}\rho_n(B_n) \to \text{End}(W \otimes^n)$ such that the following diagram commutes:

\[
\begin{array}{ccc}
\mathbb{C}B_n & \xrightarrow{\rho^R} & \mathbb{C}\rho_n(B_n) \\
\downarrow{\rho_n} & & \downarrow{\tau_n} \\
\mathbb{C}\rho_n(B_n) & \xrightarrow{\tau_n} & \text{End}(W \otimes^n)
\end{array}
\]

Idea: Push (non-local) braiding gates inside a braided QCM.

Eric Rowell\textsuperscript{1} with Z. Wang\textsuperscript{2}, C. Galindo\textsuperscript{3}, S.-M. Hong\textsuperscript{4} 1:Texas A&M U.; 2:Microsoft; 3:U. de los Andes; 4:U. Toledo

Locality in Quantum Computation, II
Example $\mathcal{C}(\mathfrak{sl}_2, 4)$

Let $R = \alpha \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & -1 & 0 \\ 0 & 1 & 1 & 0 \\ -1 & 0 & 0 & 1 \end{pmatrix}$

Theorem (Franko, R, Wang '06)

$(R, \mathbb{C}^2)$ localizes $(\rho_n^X, \mathcal{H}_n)$ for $X = X_1 \in \mathcal{C}(\mathfrak{sl}_2, 4)$

Remark

Notice: $X$ is not a vector space! ($\text{FPdim}(X) = \sqrt{2}$) "hidden locality" has $\dim(V) = 10$, $\dim(W) = 10^{n-1}$ while $\dim(\mathcal{H}_n) \in O(2^n)$. 
Some Answers

Theorem (R, Wang)

For $X \in C(\mathfrak{sl}_2, \ell)$ $B_n$-reps. $(\phi_n^X, \mathcal{H}_n)$ localizable if and only if $\ell \in \{3, 4, 6\}$.

Theorem

For $X \in \text{Rep}(DG)$, $B_n$-reps. $(\phi_n^X, \mathcal{H}_n)$ always localizable.

Remark

$B_n$ acts on both $X \otimes^n$ and $\mathcal{H}_n := \bigoplus_i \text{Hom}(X_i, X \otimes^n)$. The first is local the second is merely localizable.
We may relax localization definition to:

**Definition**

- a **quasi-localization** allows “re-coupling:” conjugation by associators.
- a **generalized-localization** allows solutions $R \in \text{End}(V^\otimes k)$ with $k > 2$ to Yang-Baxter equation.
What do TQCs compute?

**Answer**

(Approximations to) Link invariants!
Associated to $X \in C$ is a link invariant $\text{Inv}_L(X)$ approximated by the corresponding Topological Model efficiently.
Is TQC any better than classical computers?

**Question**

Suppose $C$ models a TQC. What is the computational complexity of $\text{Inv}_L(X)$? (classical and quantum)?
For $X \in C(\mathfrak{sl}_2, \ell)$, $\text{Inv}_L(X) = V_L(q)$ Jones polynomial at $q = e^{2\pi i/\ell}$

**Theorem (Vertigan,Freedman-Larsen-Wang)**

- *(Classical) exact computation of $V_L(q)$ at $q = e^{2\pi i/\ell}$ is:*
  - $FP$ if $\ell = 3, 4, 6$
  - $FP^{\#P}$ – complete else

- *(Quantum) approximation of $|V_L(q)|$ at $q = e^{2\pi i/\ell}$ is BQP

Essentially: one can quantum approximate $V_L(q)$ efficiently, but no efficient exact classical algorithm unless $\ell \in \{3, 4, 6\}$ or $P=NP$!
Localization Conjecture

Conjecture (R, Wang and Galindo, Hong, R)

For \((\varphi_n^X, \mathcal{H}_n)\) associated with \(X \in \mathcal{C}\) TFAE:

(F) \(|\varphi_n^X(B_n)| < \infty\)

(L) \((\varphi_n^X, \mathcal{H}_n)\) has a quasi- or generalized-localization

(P) \(Inv_K(X)\) efficiently computable on Turing Machine \(K\) a Knot.

(W) \(FPdim(X)^2 \in \mathbb{Z}\)
Some (Further) Evidence

**Theorem (R,Wang)**

Suppose that each $\mathcal{H}_n$ is irreducible for all $n \gg 0$. Then \textbf{Localizable} $\Rightarrow$ \textbf{Weakly Integral}.

**Theorem (R,Naidu-R)**

For $X \in C(\mathfrak{g}, \ell)$, $\text{FPdim}(X) \in \mathbb{Z} \Rightarrow |\varphi^X_n(\mathcal{B}_n)| < \infty$

**Theorem (Jones,Freedman-Larsen-Wang,Larsen-R-Wang,R)**

For $C(\mathfrak{g}, \ell)$, \textbf{Finite} $|\varphi^X_n(\mathcal{B}_n)| \Rightarrow $ \textbf{Weakly Integral}.
Consequences

Main Consequence

If Localization conjecture holds, then **Universality** and **Localizability** are incompatible in the non-adaptive topological model.

Conjecture implies:

Conjecture

If \((R, V)\) is a unitary, finite order solution to the Yang-Baxter eqn. then \(|\rho^R(B_n)| < \infty\) (perhaps modulo the center).

Question

Can you find a counterexample? Given \(U \in U((\mathbb{C}^d)^\otimes k)\) what does \(\{I_d^\otimes i \otimes U \otimes I_d^\otimes (n-i-k)\}\) generate in \(U((\mathbb{C}^d)^\otimes n)\)?
Further Reading

- J. Pachos: An Introduction to Topological Quantum Computing (e-version available from TAMU library)
- N. Read: Topological phases and quasiparticle braiding Physics Today July 2012.