Locality in Quantum Computation, II

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

September 2012
mostly based on arXiv:1009.0241 (Comm. Math. Phys. 2012)
and arXiv:1105.5048 (Inter. Math. Res. Not. 2012)

What is a Quantum Computer?

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

Definition

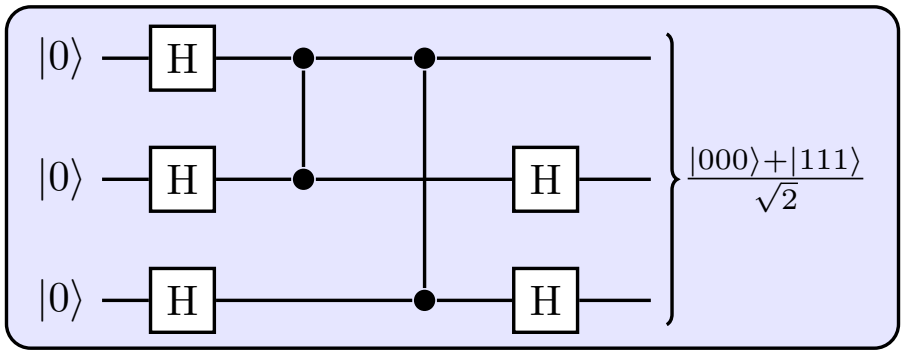
Quantum Computation is any computational model based upon the theoretical ability to manufacture, manipulate and measure quantum states.

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 $|a_i|^2$.

Quantum Circuit Model



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 $U_i \in \mathbf{U}(\mathcal{M}_{n_i})$ (n_i-local) usually $n_i \leq 4$.

Quantum Circuits

Definition

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

- $G_1 \cdot G_2 \cdots G_m \in \mathbf{U}(\mathcal{M}_n)$
- where $G_j = I_V^{\otimes a} \otimes U_i \otimes I_V^{\otimes b}$
- Given $U \in \mathbf{U}(\mathcal{M}_n)$ can only reasonably hope to approximate U as $G_1 \cdot G_2 \cdots G_m$

Remarks on QCM

Remarks

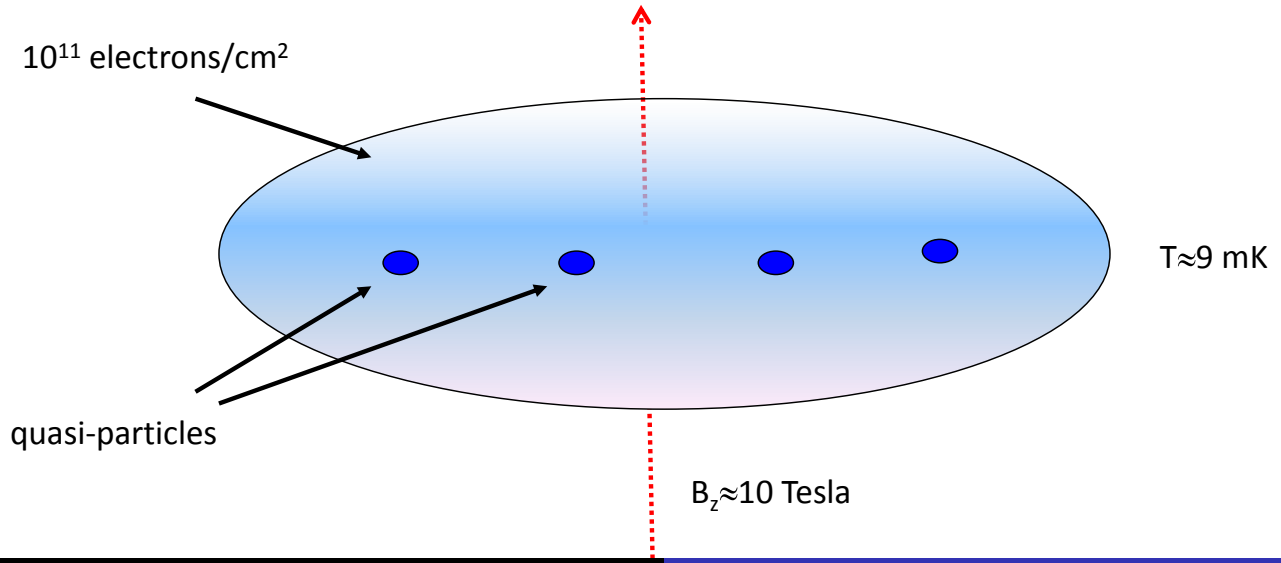
- Typical physical realization: composite of n identical d-level systems. E.g. $d = 2$: spin-$\frac{1}{2}$ arrays.
- The setting of most quantum algorithms: e.g. Shor's integer factorization algorithm
- QCM gates are algebraically local: the G_i act non-trivially on a few adjacent qudits.
- Main nemesis: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

Topological Phases of Matter (anyons)

Definition

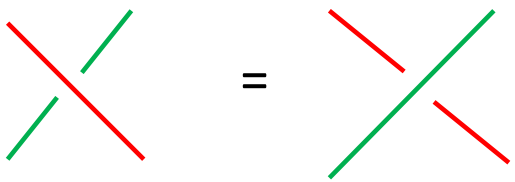
Topological Quantum Computation (TQC) is a computational model built upon systems of anyons (topological phases).

Fractional Quantum Hall Liquid

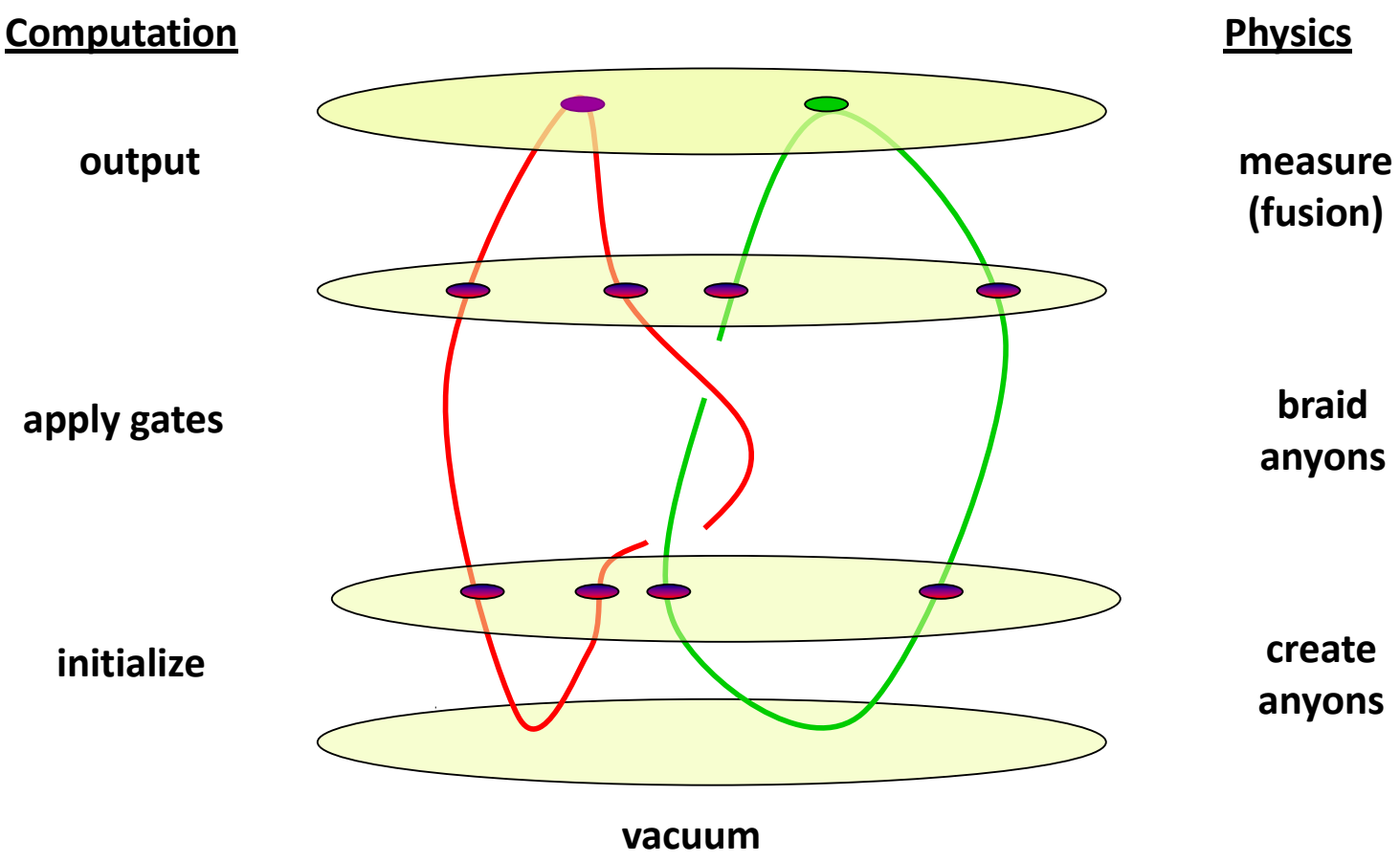


Anyons?!

- 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)



The Braid Group

A key role is played by the braid group:

Definition

$\mathcal{B}_n$ has generators σ_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 $|i - j| > 1$

Mathematical Model for Anyons

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

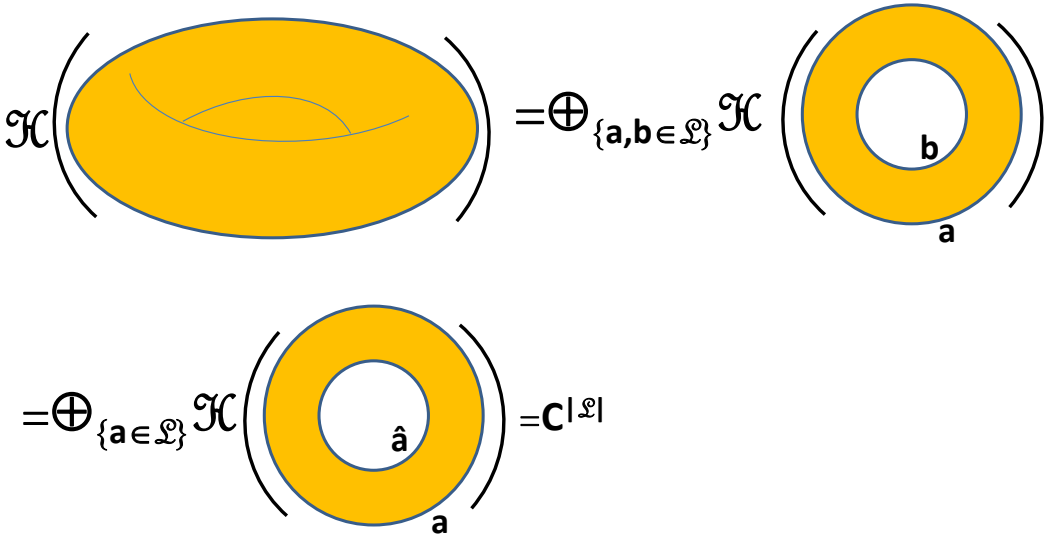
Most (known, useful) $(2+1)$-TQFTs come from the Reshetikhin-Turaev construction via modular categories.

Braided and Ribbon Categories

Definition (Heuristic)

- A braided category has a commutative tensor product:

  (up to isomorphisms) $c_{X,Y} : X \otimes Y \to Y \otimes X$
- A ribbon category allows one to "do topology"



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

Irrational Dimensions?!

Remark

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

Definition

A fusion category $\mathcal{C}$:

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

Dictionary

Modular Category	Anyonic System
Simple objects X_i	anyons
$\mathbf{1}$	vacuum type
dual objects X^*	antiparticles
$\mathrm{Hom}(X, Y)$	state spaces
$c_{X,Y}$	particle exchange
$\det(S) \neq 0$	anyons distinguishable
$X_i \otimes X_j = \bigoplus_k N_{i,j}^k X_k$	ground state degeneracy

Sources of Modular Categories

Example

- $\mathcal{C}(\mathfrak{g}, \ell)$: semisimple subquotient of quantum group $\mathrm{Rep}(U_q\mathfrak{g})$ at $q = e^{\pi i/\ell}$. Typically $\mathrm{FPdim}(X) \notin \mathbb{Z}$.
- $\mathrm{Rep}(DG)$: quantum double DG of finite group G $\mathrm{FPdim}(X) \in \mathbb{Z}$ for $X \in \mathrm{Rep}(DG)$.

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:

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

Universality?

Question

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

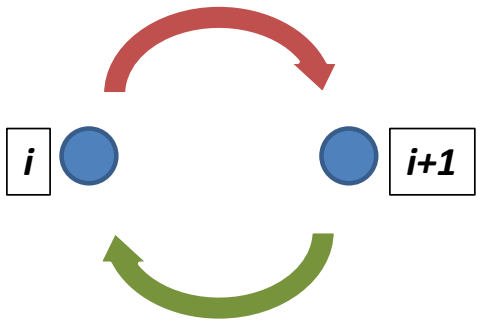
Remarks

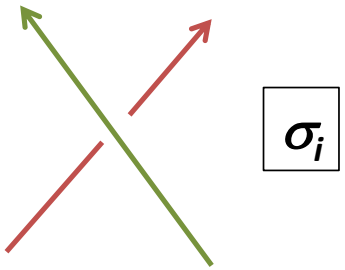
- A universal quantum computer can efficiently solve B(ounded error)Q(uantum resource)P(olynomial time) problems.
- The quantum circuit model is universal.

Topological Model

Remarks

- state space for n particles of type $X \in \mathcal{C}$: $\mathcal{H}_n^i := \mathrm{Hom}(X_i, X^{\otimes n})$
- Physically, gates are "particle exchanges" (braiding) acting on $\mathcal{H}_n := \bigoplus_i \mathcal{H}_n^i$.
- Mathematically, gates are $\{\varphi_n^X(\sigma_i)\}$ where $\varphi_n^X : \mathcal{B}_n \to \mathbf{U}(\mathcal{H}_n)$
- Topological protection from decoherence





Mathematical Formulation: Braid Group Representations

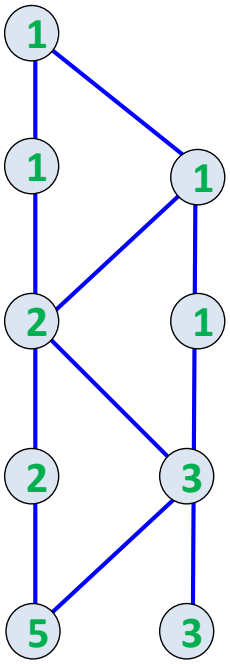
Fix $X \in \mathcal{C}$, and suppose decomp. of φ_n^X into irreps. is:

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

Fact

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

Example: $SU(2)_3$



$\varphi_n^5(\mathcal{B}_n)$ acts on:

$$\mathrm{Hom}_{\mathcal{C}}(\mathbf{1}, X^{\otimes n}) \oplus \mathrm{Hom}_{\mathcal{C}}(X, X^{\otimes n})$$

$$\dim(\mathrm{Hom}_{\mathcal{C}}(X_i, X^{\otimes n})) = Fib(n+i-1)$$

$$\overline{\varphi_n^5(\mathcal{B}_n)} \supset SU(Fib(n-1)) \times SU(Fib(n))$$

Algebraic Universality

Question

For $X \in \mathcal{C}$ (modular), when is $|\varphi_n^X(\mathcal{B}_n)| < \infty$?

Theorem (Jones '86)

For $X \in \mathcal{C}(\mathfrak{sl}_2, \ell)$ braid group image $\varphi_n^X(\mathcal{B}_n)$ infinite if and only if $\ell \notin \{3, 4, 6\}$.

Theorem (Etingof,R,Witherspoon '08)

For $X \in \mathrm{Rep}(DG)$ images $\varphi_n^X(\mathcal{B}_n)$ always finite.

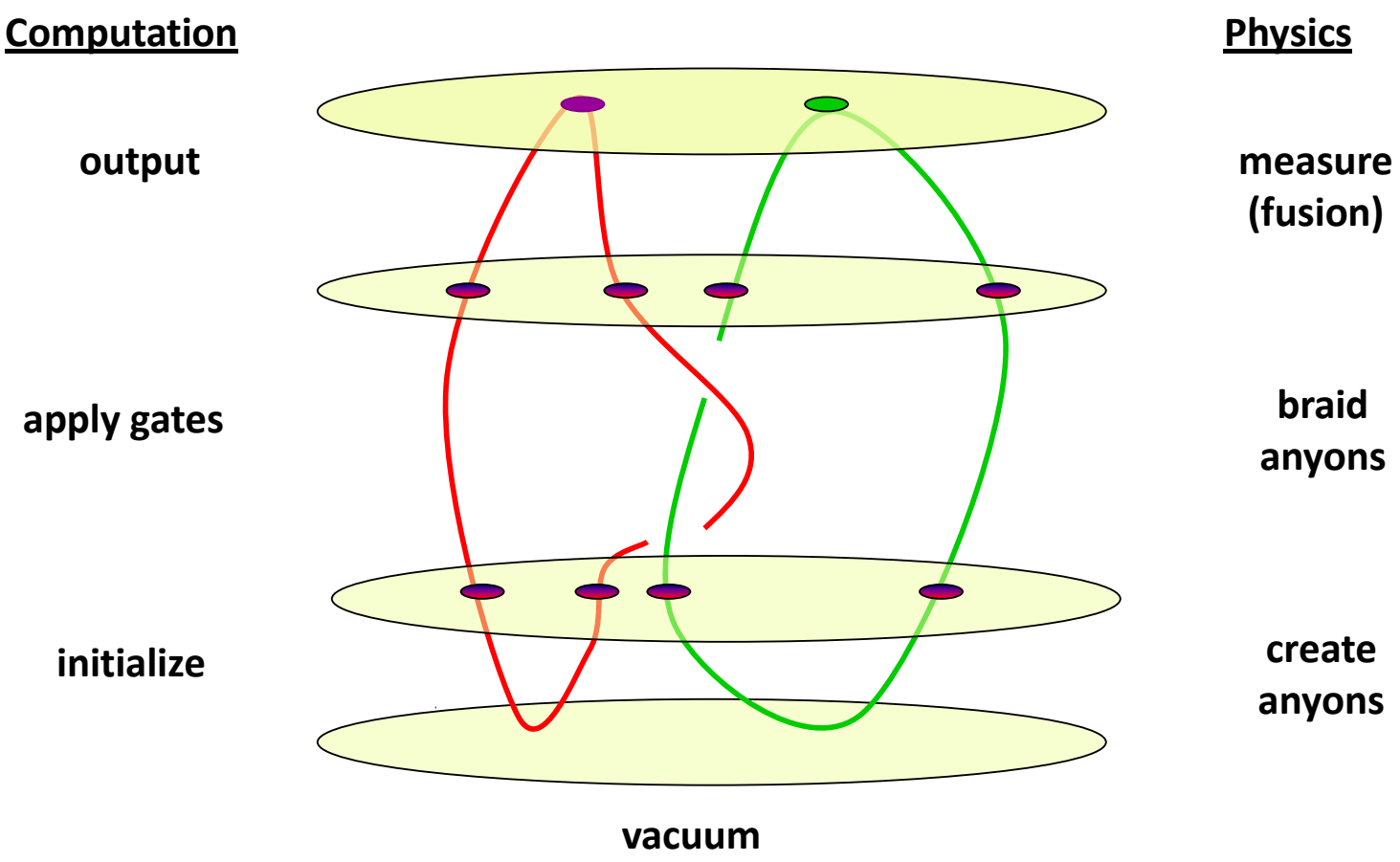
INTERMISSION

Enjoy some chocolate-coated qubits in the lobby!

Last time...

- Topological quantum computers: fault-tolerant due to invariance under (physically) local perturbations.
- Physical medium: topological phases. algebraically modeled by modular categories–generalizations of $Rep(G)$, 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)



Topological *and* Local?

Fact

Topological Models are not typically local.

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

Question

Can we uniformly "localize" $(\varphi_n^X, \mathcal{H}_n)$?

Recall: QCM has state spaces $\mathbb{C}^d \otimes \cdots \otimes \mathbb{C}^d$.

Simulating TQCs on QCM

Freedman *et al* showed that TQCs have a "hidden locality:" Let $U(\beta) \in \mathbf{U}(\mathcal{H}_n)$ be a unitary braiding matrix.
Goal: simulate U on $V^{\otimes k(n)}$ for some v.s. X.

- Set $V = \bigoplus_{(A,B,C)} \mathrm{Hom}(A, B \otimes C)$ 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...

Local $\mathcal{B}_n$ representations: Yang-Baxter eqn.

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 $\mathcal{B}_n$-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 $\mathcal{B}_n$-reps. (ρ_n, V_n) is a braided vector space (R, W) and injective algebra maps $\tau_n : \mathbb{C}\rho_n(\mathcal{B}_n) \to \mathrm{End}(W^{\otimes n})$ such that the following diagram commutes:

$$\begin{tikzcd} \mathbb{C}\mathcal{B}_n \arrow[d, "\rho_n"] \arrow[dr, "\rho^R"] & \\ \mathbb{C}\rho_n(\mathcal{B}_n) \arrow[r, "\tau_n"] & \mathrm{End}(W^{\otimes n}) \end{tikzcd}$$

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

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! $(\mathrm{FPdim}(X) = \sqrt{2})$ "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 $X \in \mathcal{C}(\mathfrak{sl}_2, \ell)$ $\mathcal{B}_n$-reps. $(\varphi_n^X, \mathcal{H}_n)$ localizable if and only if $\ell \in \{3, 4, 6\}$.

Theorem

For $X \in \mathrm{Rep}(DG)$, $\mathcal{B}_n$-reps. $(\varphi_n^X, \mathcal{H}_n)$ always localizable.

Remark

$\mathcal{B}_n$ acts on both $X^{\otimes n}$ and $\mathcal{H}_n := \bigoplus_i \mathrm{Hom}(X_i, X^{\otimes n})$. The first is local the second is merely localizable.

Some Improvements (Galindo, Hong, R)

We may relax localization definition to:

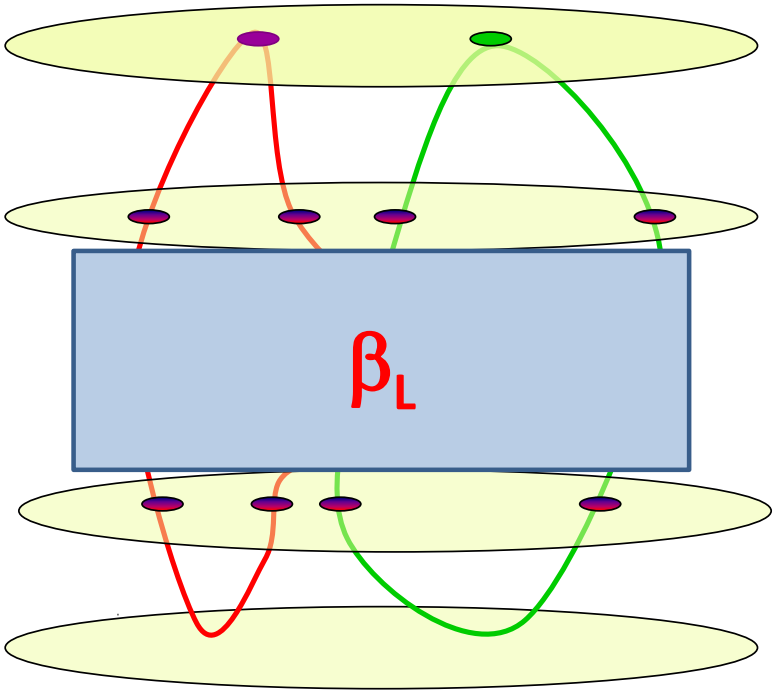
Definition

- a quasi-localization allows "re-coupling:" conjugation by associators.
- a generalized-localization allows solutions $R \in \mathrm{End}(V^{\otimes k})$ with $k > 2$ to Yang-Baxter equation.

What do TQCs compute?

Answer

(Approximations to) Link invariants!
Associated to $X \in \mathcal{C}$ is a link invariant $Inv_L(X)$ approximated by the corresponding Topological Model efficiently.



Prob( ) ~ x^{-t}|Inv_L( )|

Is TQC any better than classical computers?

Question

Suppose $\mathcal{C}$ models a TQC. What is the computational complexity of $Inv_L(X)$? (classical *and* quantum)?

Complexity of Jones Polynomial Evaluations

For $X \in \mathcal{C}(\mathfrak{sl}_2, \ell)$, $Inv_L(X) = V_L(q)$ 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:*
$$\begin{cases} FP & \ell = 3, 4, 6 \\ FP^{\sharp P} - complete & else \end{cases}$$
- *(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) $\mathrm{FPdim}(X)^2 \in \mathbb{Z}$

Some (Further) Evidence

Theorem (R,Wang)

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

Theorem (R,Naidu-R)

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

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

For $\mathcal{C}(\mathfrak{g}, \ell)$, Finite $|\varphi_n^X(\mathcal{B}_n)| \Rightarrow$ 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 $|\rho^R(\mathcal{B}_n)| < \infty$ (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.
- G. Collins: Computing with quantum knots *Sci. Amer.* March 2006.