Classifying Modular Categories

Eric Rowell

Texas A&M University

UT Tyler, October 2009

Outline

Outline

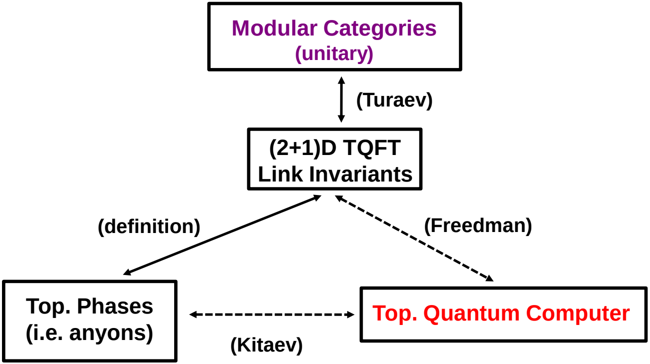
Outline

Outline

Collaborators and References

- Zhenghan Wang, Microsoft Station Q
- Richard Stong, CCR West
- Seung-moon Hong, U. Toledo (Ohio)
- R., Stong, Wang: *On classification of modular tensor categories.* Comm. Math. Phys. (2009) math.QA/0712.1377.
- Hong, R.: *On the classification of non-self-dual modular categories* preprint (on arxiv).

Relevance to Quantum Computing: Overview



Topological States

Definition (Das Sarma, et al)

a system is in a topological phase if its low-energy effective field theory is a *topological quantum field theory.*

Algebraic part: modular category.

Some Axioms

Definition

A fusion category is a monoidal category $(\mathcal{C}, \otimes, \mathbf{1})$ that is:

- $\mathbb{C}$-linear: $\mathrm{Hom}(X, Y)$ f.d. vector space
- abelian: $X \oplus Y$
- finite rank: simple objects $\{X_0 := \mathbf{1}, X_1, \ldots, X_{m-1}\}$
- semisimple: $Y \cong \bigoplus_i c_i X_i$
- rigid: duals X^*, $b_X : \mathbf{1} \to X \otimes X^*$, $d_X : X^* \otimes X \to \mathbf{1}$
- compatibility...

First Example

Example

$\mathcal{V}$ the category of f.d. $\mathbb{C}$-vector spaces.

- $\mathbf{1} = \mathbb{C}$
- $\mathbf{1}$ is the only simple object: rank 1
- $V^* \otimes V \xrightarrow{d_V} \mathbf{1}$: $d_V(f \otimes v) = f(v)$
- $\mathbf{1} \xrightarrow{b_V} V \otimes V^*$: $b_V(x) = x \sum_j v_j \otimes v^j$

Braiding and Twists

Definition

A braided fusion (BF) category has isomorphisms:

$$c_{X,Y} : X \otimes Y \to Y \otimes X$$

satisfying, e.g.

$$c_{X,Y \otimes Z} = (\mathrm{Id}_Y \otimes c_{X,Z})(c_{X,Y} \otimes \mathrm{Id}_Z)$$

Definition

A *ribbon* category has compatible $*$ and $c_{X,Y}$. Encoded in "twists" $\theta_X : X \to X$ inducing $V \cong V^{**}$.

The Braid Group

Definition

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

$$\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}$$
$$\sigma_i \sigma_j = \sigma_j \sigma_i \text{ if } |i-j| > 1$$

Braid Group Representations

Fact

Braiding on $\mathcal{C}$ induces:

$$\Psi_X : \mathbb{C}\mathcal{B}_n \to \mathrm{End}(X^{\otimes n})$$

$$\sigma_i \to \mathrm{Id}_X^{\otimes i-1} \otimes c_{X,X} \otimes \mathrm{Id}_X^{\otimes n-i-1}$$

- X is *not* always a vector space
- $\mathrm{End}(X^{\otimes n})$ semisimple algebra (multi-matrix).
- simple $\mathrm{End}(X^{\otimes n})$-mods $V_k = \mathrm{Hom}(X^{\otimes n}, X_k)$ become $\mathcal{B}_n$ reps.

Modular Categories

Ribbon categories have:

- Consistent *graphical calculus*: braiding, twists, duality maps represented by "braid-like" diagrams
- canonical trace: $tr_{\mathcal{C}} : End(X) \to \mathbb{C} = End(\mathbf{1})$
- $tr_{\mathcal{C}}(Id_X) := \dim(X) \in \mathbb{R}^{\times}$ (generally not in $\mathbb{Z}_{\geq 0}$).
- Invariants of links: given L with each component labelled by an object X find a braid $\beta \in \mathcal{B}_n$ s.t. $\hat{\beta} = L$ then $K_X(L) := tr_{\mathcal{C}}(\Psi_X(\beta))$.

Definition

Let $S_{i,j} = tr_{\mathcal{C}}(c_{X_j,X_i} c_{X_i,X_j})$, $0 \leq i,j \leq m-1$. $\mathcal{C}$ is modular if $\det(S) \neq 0$.

Grothendieck Semiring

Definition

$Gr(\mathcal{C}) := (Obj(\mathcal{C}), \oplus, \otimes, \mathbf{1})$ a unital based ring.

- Define matrices
  $(N_i)_{k,j} := \dim \mathrm{Hom}(X_i \otimes X_j, X_k)$

$$\text{So: } X_i \otimes X_j = \bigoplus_{k=0}^{m-1} N_{i,j}^k X_k$$

- Rep. $\varphi : Gr(\mathcal{C}) \to \mathrm{Mat}_m(\mathbb{Z})$

$$\varphi(X_i) = N_i$$

- Respects duals: $\varphi(X^*) = \varphi(X)^T$ (self-dual $\Rightarrow$ symmetric)
- If $\mathcal{C}$ is braided, $Gr(\mathcal{C})$ is commutative

Frobenius-Perron Dimensions

Definition

- $\mathrm{FPdim}(X)$ is the largest eigenvalue of $\varphi(X)$
- $\mathrm{FPdim}(\mathcal{C}) := \sum_{i=0}^{m-1} \mathrm{FPdim}(X_i)^2$

(a) $\mathrm{FPdim}(X) > 0$

(b) $\mathrm{FPdim} : Gr(\mathcal{C}) \to \mathbb{C}$ is a unital homomorphism

(c) FPdim is unique with (a) and (b).

If $\mathrm{FPdim}(X) = \dim(X)$ for all X, $\mathcal{C}$ is pseudo-unitary.

Integrality

Definition

$\mathcal{C}$ is

- integral if $\mathrm{FPdim}(X) \in \mathbb{Z}$ for all X
- weakly integral if $\mathrm{FPdim}(\mathcal{C}) \in \mathbb{Z}$

Not Quite an Example

Example

Let G be a finite group. Rep(G) category of f.d. $\mathbb{C}$ reps. of G is ribbon (not modular).

- $\mathrm{FPdim}(V) = \dim_{\mathbb{C}}(V)$.
- $Gr(\mathrm{Rep}(G))$ is the *representation ring*.
- Let $\{V_i\}$ be the irreps. $x_i := \dim(V_i)$, $V_0 = \mathbb{C}$ trivial rep.
- $S = \begin{pmatrix} 1 & x_1 & \cdots & x_m \\ x_1 & \ddots & \cdots & x_1 x_m \\ \vdots & \vdots & x_i x_j & \vdots \\ x_m & x_m x_1 & \cdots & x_m^2 \end{pmatrix}$ $\det(S) = 0$ (rank 1 in fact).
- twists: $\theta_i = 1$ for all i.

Some Sources of Modular Categories

Example

Quantum group $U = U_q\mathfrak{g}$ with $q = e^{\pi \mathrm{i}/\ell}$.

- subcategory of *tilting modules* $\mathcal{T} \subset \mathrm{Rep}(U)$
- quotient $\mathcal{C}(\mathfrak{g}, \ell)$ of $\mathcal{T}$ by *negligible morphisms* is modular.

Example

G a finite group, ω a 3-cocyle

- semisimple quasi-triangular quasi-Hopf algebra $D^\omega G$
- $\mathrm{Rep}(D^\omega G)$ is a BF category (modular).

Conjecture (Folk)

All modular categories come from these 2 families.

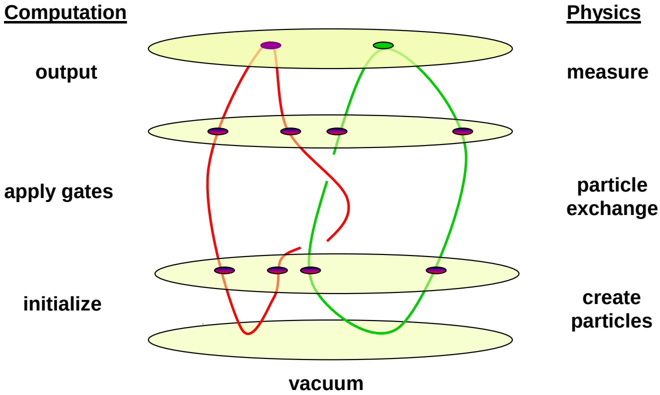
Everyone's Favorite Example

Example (Fibbonaci)

quantum group category $\mathcal{C}(\mathfrak{g}_2, 15)$

- Two simple objects $\mathbf{1}$, X
- $\mathrm{FPdim}(X) = \tau = \frac{1+\sqrt{5}}{2}$
- $S = \begin{pmatrix} 1 & \tau \\ \tau & -1 \end{pmatrix}$
- $\theta_0 = 1$, $\theta_X = e^{4\pi i/5}$
- $X \otimes X = \mathbf{1} \oplus X$

Topological Quantum Computation: Schematic



Dictionary

Categories	Physics
Simple objects X_i	Indecomposable particle types t_i
$\mathbf{1}$	vacuum type
dual objects X^*	Antiparticles
$\mathrm{End}(X)$	State space
$c_{X,Y}$	particle exchange
$\det(S) \neq 0$	particle types distinguishable
$X_i \otimes X_j = \bigoplus_k N_{i,j}^k X_k$	fusion channels $t_i \star t_j \to t_k$
$\frac{N_{i,j}^k \dim(X_k)}{\dim(X_i)\dim(X_j)}$	$Prob(t_i \star t_j \to t_k)$

Link Invariants

Recall: $\mathcal{C}$ ribbon, $X \in \mathcal{C}$, L a link: get invariant $K_X(L)$.

Question

Is computing (randomized approximation) $K_X(L)$ easy: FPRASable or hard: $\#P$-hard, not FPRASable, assuming $P \neq NP$?

Appears to coincide with: *Is* $\Psi_X(\mathcal{B}_n)$ *finite or infinite?*
Related to topological quantum computers: weak or powerful?

Conjecture (Algebraic)

$\Psi_X(\mathcal{B}_n)$ finite iff $\mathrm{FPdim}(\mathcal{C}) \in \mathbb{Z}$

See proceedings of 2007 conf.

Landscape of Modular Categories

Question

- Are there "exotic" (not quantum group or Hopf algebra) modular categories?
- How many modular categories are there?

General Problem

Problem

Classify all modular categories, up to equivalence.

- For physicists: a classification of algebraic models for FQH liquids
- For topologists: a classification of (most? all?) quantum link invariants
- For algebraists (David): a classification of (all?) factorizable Hopf algebras.
- would include a classification of finite groups...too ambitious!

First Reduction

Theorem (Ocneanu Rigidity)

Fix a unital based ring R. There are at most finitely many (fusion, ribbon) modular categories $\mathcal{C}$ with $Gr(\mathcal{C}) \cong R$.

Up to finite ambiguity, enough consider:

Problem

Classify all unital based rings R such that $R \cong Gr(\mathcal{C})$ for some modular category $\mathcal{C}$.

Definition

$\mathcal{C}$ and $\mathcal{D}$ are Grothendieck equivalent if $Gr(\mathcal{C}) \cong Gr(\mathcal{D})$.

Wang's Conjecture

More bad news:

Conjecture

Fix $m \geq 1$. There are finitely many modular categories of rank m.

Only verified in the following situations:

- $m \leq 4$
- $\mathcal{C}$ is weakly integral.
- $\text{FPdim}(\mathcal{C})$ (hence $\text{FPdim}(X_i)$ and $N_{i,j}^k$) bounded.

$m = 2$: true for *fusion* cats., $m = 3$: true for *ribbon* cats.

More Modest Goal

Problem

Classify modular categories:

- that are pseudo-unitary (so $\dim(X_i) \geq 1$)
- up to Grothendieck equivalence
- for small ranks m (say ≤ 12).

Symmetries of $N_{i,j}^k$

Denote by i^* the label of X_i^*. Then:

- $N_{i,j}^k = N_{j,i}^k = N_{i,k^*}^{j^*} = N_{i^*,j^*}^{k^*}$
- $N_{i,i^*}^0 = 1$, $N_{i^*} = N_i^T$
- $N_i N_j = N_j N_i$

Diophantine equations.

Symmetries of S and T

Define $T_{i,j} = \theta_i \delta_{i,j}$. S and T satisfy:

- $S = S^T$ (symmetric, but $\mathbb{C}$-entries!)
- $SS^\dagger = \alpha I$, $S^4 = \alpha^2 I$ (Projectively Unitary)
- $T^N = I$ for some N, $\theta_{i^*} = \theta_i$.
- $(ST)^3 = \gamma S^2$
- $\dim(\mathcal{C}) = (\sum_i \theta_i \dim(X_i)^2)(\sum_i \dim(X_i)^2/\theta_i)$

Note: $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \to S$ and $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \to T$ give rep. of $PSL(2,\mathbb{Z})$.

Relationship between N_i and S

Verlinde formula:

$$N_{i,j}^{k} = \sum_{r} \frac{S_{i,r} S_{j,r} \overline{S_{k,r}}}{\dim(\mathcal{C}) \dim(X_r)}.$$

So enough to classify S-matrices...
Moreover, $\Phi_j(X_i) := S_{i,j} / \dim(X_j)$ are characters of $Gr(\mathcal{C})$.

Relationship Among N_i, S and T

The balancing axiom:

$$S_{i,j}\theta_i\theta_j = \sum_k N_{i^*,j}^k \dim(X_k)\theta_k.$$

Definition

A triple $(\{N_i\}, S, T)$ satisfying symmetries, balancing, Verlinde, is a modular data.

Galois Theory

Preliminary Facts:

- $S_{i,j}$ are algebraic integers and θ_i are roots of 1.
- Denote $p_i(x) := char_{N_i}(x)$.
- roots of p_i are $S_{i,j}/\dim(X_j)$
- $K = \mathbb{Q}(S_{i,j})$ is Galois extension $(|Aut_{\mathbb{Q}}(K)| = \dim_{\mathbb{Q}}(K))$
- K is splitting field of $\{p_i\}$.

Harder Results

Denote by $G = Gal(K/\mathbb{Q}) = Gal(\mathcal{C})$.

Theorem (Coste, Gannon)

(a) *G is abelian*

(b) *G permutes characters Φ_j, get injective homomorphism: $G \to S_m$.*

(c) *Let $\sigma \in G < S_m$: $S_{i,j} = \pm S_{\sigma(i),\sigma^{-1}(j)}$*

New Strategy

Problem

Fix m and $G < S_m$ abelian. Classify modular categories $\mathcal{C}$ with $Gal(\mathcal{C}) = G$ (not just $\cong$).

Remarks

- j is G-fixed if and only if $S_{i,j}/\dim(X_j) \in \mathbb{Z}$ for all i.
- 0 is G-fixed if and only if $\mathcal{C}$ is integral.
- If G does not fix any j, lots of symmetries among the $S_{i,j}$.

Integral Cases

Lemma

Suppose $\mathcal{C}$ is an integral modular category of rank m. Let $d_1 \geq d_2 \geq \cdots \geq d_m = 1$ be the dimensions of simple objects. Then the integers $y_i := \dim(\mathcal{C})/(d_i)^2$ satisfy:

(a) $y_1 \leq y_2 \leq \cdots \leq y_m = \dim(\mathcal{C})$

(b) $\sum_{i=1}^{m} 1/y_i = 1$

(c) $i \leq y_i \leq (m - i + 1)u_i$ *where* $u_1 := 1$ *and* $u_{k+1} := u_k(u_k + 1)$.

$u_k + 1$ is Sylvester's sequence: $2, 3, 7, 43, 1807, \ldots$ (double-exponential).

Algorithm

To classify integral modular categories of rank m:

1. Solve for integers $y_1 \leq \cdots \leq y_m$ such that:
   1. $\sqrt{y_m/y_i} \in \mathbb{Z}$
   2. $\sum_i 1/y_i = 1$
   3. $x_i \leq u_m$
2. Set $d_i = \sqrt{y_m/y_i}$. solve $d_i d_j = \sum_k N_{i,j}^k d_k$, $N_{i,j}^k \leq \max(d_i)^2$.
3. solve for S and T, look for realizations...

Example: $m = 5$

- so $y_i \leq 43$
- Only solutions: $(5, 5, 5, 5, 5)$ and $(2, 8, 8, 8, 8)$.
- Gives dimensions: $(1, 1, 1, 1, 1)$ and $(1, 1, 1, 1, 2)$
- $(1, 1, 1, 1, 1)$ is realized, $(1, 1, 1, 1, 2)$ is not (no S matrix).
- $(1, 1, 1, 1, 2)$ *is* realized as $\text{Rep}(D_8)$...

Non-integral Strategy

Fix m and $G < S_m$. Assume $|G(0)| > 1$ (otherwise integral)

- Use G-action and $SS^\dagger \propto I$
- compute $char_{X_i}(x)$ two ways: from N_i and roots: $S_{i,j}/\dim(X_j)$.
- gives more Diophantine equations in $N_{i,j}^k$.
- Use balancing to bound $M > [\mathbb{Q}(\theta_i) : \mathbb{Q}] = [\mathbb{Q}(\theta_i) : K][K : \mathbb{Q}]$.
- So $\varphi_n(\theta_i) = 0$, φ_n cyclotomic degree $n < M$.
- Usually, implies Diophantine eqn *in each* $N_{i,j}^k$ (finitely many solutions)

A rank 3 example

Let $S = \begin{pmatrix} 1 & d_1 & d_2 \\ d_1 & s_{1,1} & s_{1,2} \\ d_2 & s_{1,2} & s_{2,2} \end{pmatrix}$, suppose $G = \langle (012) \rangle$

G-symmetries imply:

$s_{1,1} = \pm d_2$, $s_{1,2} = \pm 1$ and $s_{2,2} = \pm d_1$ ($\pm$ independent).

S unitary and $d_i > 1$ (not integral) imply:

$$S = \begin{pmatrix} 1 & d_1 & \frac{d_1}{d_1-1} \\ d_1 & \frac{-d_1}{d_1-1} & 1 \\ \frac{d_1}{d_1-1} & 1 & -d_1 \end{pmatrix}.$$

Observe: implies $\det(N_1) = \det(N_2) = -1$.

e.g. $d_1 (\frac{-1}{d_1-1})(\frac{d_1-1}{d_1}) = -1$

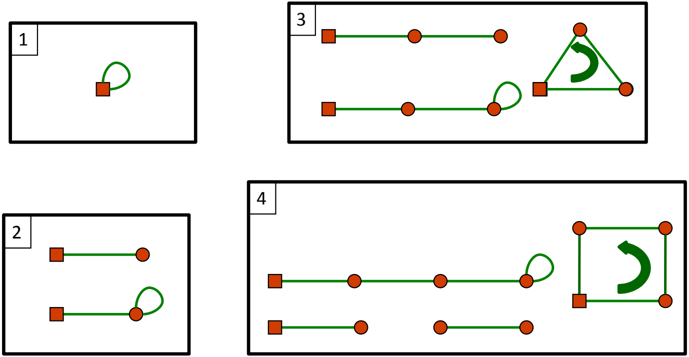
example, continued

$$N_1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & n_1 & n_2 \\ 0 & n_2 & n_3 \end{pmatrix}, N_2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & n_2 & n_3 \\ 1 & n_3 & n_4 \end{pmatrix}$$

$N_1 N_2 = N_2 N_1$ and $\det(N_1) = \det(N_2) = -1$ imply:
$n_2 = n_3 = 1$ and $n_1 + n_4 = 1$, so up to $X_1 \leftrightarrow X_2$, $n_1 = 1$, $n_4 = 0$.
This is realized (subcategory of $\mathcal{C}(\mathfrak{sl}_2, 7)$).

Rank ≤ 4 Classification

Fusion graph of X_i: m labels $N_{i,j}^k$ edges from j to k.



Non-self-dual approach

Complex conjugation $c = (1\ 1^*) \cdots (i\ i^*) \cdots \in G$
$c \neq 1$ if $X_i \ncong X_{i^*}$ for some i.
G abelian, so this gives significant reduction. For example:

Theorem

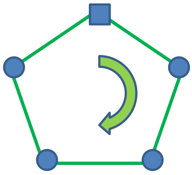
Suppose $\mathcal{C}$ is an odd rank, maximally non-self-dual modular category (i.e. only $\mathbf{1}$ is self-dual simple). Then $\mathcal{C}$ is integral.

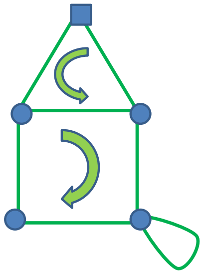
Proof.

After relabeling, $c = (1\ 2) \cdots (m-2\ m-1) \in G$. No $\sigma \in G$ with $\sigma(0) \neq 0$ commutes with c. So $G(0) = \{0\}$, hence integral. □

Non-self-dual Rank 5

Fusion graph classification:





Thank You!