Greg Kuperberg's Lectures on

Quantum Algebra and Fault Tolerance

Sanchayan Dutta
dutta@ucdavis.edu

Contents

1 Lecture 1 (4 March, 2023)

1.1 Bosons and Fermions

Precept: Certain families of particles are entirely identical, e.g., all electrons are identical. Meaning that if you switch the state of two electrons (say) or two photons, etc. you should get the exact same state.

So: If you have n identical particles, there is an action of S_n, the symmetric group, and totally identical means that S_n acts by a 1-dimension representation.

If every permutation sigma acts by a factor of 1, the particles are identical bosons. If every sigma acts by $(-1)^\sigma$, the particles are identical fermions.

You could call these semi-identical particles. This can happen, but you don't want just one representation for each n separately. Whatever those axioms are, there are other solutions, but they are all either parabosons or parafermions that can be re-described as ordinary bosons and fermions, together with extra hidden internal state.

Example: Quarks. Now seen as fermions, they are in effect semi-identical because they have a hidden 3-dimensional color Hilbert space.

If H is the Hilbert space for one boson, and respectively, fermion, then the Hilbert space for n bosons is $S_n(H)$, and for n fermions it is $\Lambda^n(H)$, not $H^{\otimes n}$ in either case.

If particles are localized in space, then it's more interesting to consider physical permutations of them, rather than simply relabelling. Say that we work in $d+1$ dimensions. If d is at least three, then $\pi_1(\text{n distinct points in } \mathbb{R}^3) = S^n$. If $d = 2$, then $\pi_1(\text{n distinct points in } \mathbb{R}^3) = B_n$ (the braid group), which is bigger and different from S_n, although it surjects to S_n.

1.2 Parastatistics theorem and implications

Instead of S_n, we want representations of B_n instead. Even if the n particles in 2D are manifestly different, you will still get an interesting braiding group, the pure braid group $PB_n :=$ The kernel of the homomorphism from B_n to S_n. There is no counterpart to the parastatistics theorem in this case.

What was first considered: Consistent families of 1-dimensional irreps of B_n. Switching two particles, say counterclockwise, can produce any phase factor $e^{i\theta}$, not necessarily ± 1. Particles like this are then called anyons. Actually, only roots of unity occur, for later mathematical reasons.

Since there is no parastatistics theorem in $2+1$-dimensions (with braid groups), higher semi-identical anyons have to be examined too. These are called non-abelian anyons because the braid groups acts by matrices that in general don't commute.

Consistency across particle # is best discussed in terms of fusion.

Generalizing the fusion rules in $d \geq 3$:

1. Boson + Boson = Fermion.
2. Boson + Fermion = Fermion.
3. Fermion + Fermion = Boson.

The topological part of a spacetime diagram of some anyons in a given physical system that can braid, fuse, annihilate, and un-annihilate, will in general be a tensor network – like a Feynman diagram – except tangled in $\mathbb{R}^3$.

A category that supports such tensor networks is called a ribbon category. A ribbon category is an object in quantum algebra, and even a single closed loop is a very interesting type of "tensor" network in this case, because it's a knot! Ribbon categories are an important explanation of, e.g., the Jones polynomial.

For anyons, certainly, the ribbon category must be unitary. Moreover, (for reasons...), there are only finitely many irreducible objects in a relevant ribbon category. Also, there is a non-singularity condition, so that you can expect anyons to be modelled by unitary modular tensor categories.

1. Anyon braiding can be useful or even universal for quantum computing. Example: Fibonacci anyons are known to produce braid group representations that are dense in Fibonacci-dimensional Hilbert spaces.

2. Kitaev defined surface codes, of multi-Pauli stabilizer type, and observed that point error syndromes behave as abelian anyons.

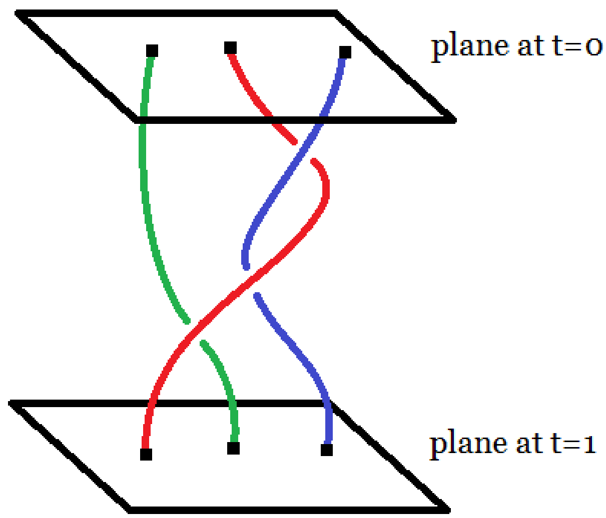
1.3 Fundamental Group of Configuration Space

Let X be a "nice" topological space (say, a manifold). Define $F_n(X)$ to be the subspace of X^n comprised of tuples with distinct coordinates. The symmetric group S_n acts on it freely, and we can form the n-configuration space as the quotient $SF_n(X)\colon = F_n(X)/S_n$. Then we define the braid group as $B_n(X) = \pi_1(SF_n(X))$. (Of course, $SF_n(X)$ should be path-connected...)

If you take $X = \mathbb{R}$ then the connected components of $F_n(X)$ are blocks for the action of S_n. Given any two tuples $(x_1, \cdots, x_n)$ and $(y_1, \cdots, y_n)$ with $x_1 < x_2 < \cdots < x_n$ and $y_1 < y_2 < \cdots < y_n$, these two tuples will be path-connected: first shift all coordinates of $\vec{y}$ uniformly enough to the right so that $x_n < y_1$, then shift y_1 back until it's x_1, then shift y_2 back until it's y_2, and so on. The space of all tuples $(x_1, \cdots, x_n)$ with increasing coordinates is homeomorphic to $\mathbb{R}^n$ which is simply connected. Similarly for any other tuples whose coordinates are "ranked" in a given order.

Now consider $X = \mathbb{C}$ with $n = 2$. We must delete the subspace $\{(z, z)\colon z \in \mathbb{C}\}$ from $\mathbb{C}^2$. (Keep in mind for now that C_2 acts on the carved-out space by transposing coordinates.) This subspace is a plane inside Euclidean 4-space, so it homeomorphic to $\mathbb{R} \times (\mathbb{R}^3 - L)$ for a line $L \subset \mathbb{R}^3$. Better yet, consider the obvious Euclidean structure on the space and take the orthogonal complement $\{(z, -z)\colon z \in \mathbb{C}\}$: there is an orthogonal projector given by $(z, w) \mapsto (z - w, w - z)/\sqrt{2}$ and then an isomorphism into the punctured plane given by $(u, -u) \mapsto u$. Thus, we have a deformation retract from $\mathbb{C}^2 - \text{diag}$ onto $\mathbb{C}^\times$, and we know $\pi_1(\mathbb{C}^\times)$ is infinite cyclic. (This is the pure braid group P_2.)

So what about $n > 2$? In configuration space (which has $2n$ real dimensions, so is hard to visualize) a single point, a "configuration," represents n distinct points in a plane (which is easy to visualize). And a path in configuration space represents each of the n points in the plane having a path in and out of it.



Thus, imagine a continuum (indexed by $[0,1]$) of copies of $\mathbb{C}$ (resting flat) piled on top of each other. If one lets the altitude represent time, then the paths traced out between the points represent strings, and if one looks at this picture from the side one sees braid diagrams!

Since we can choose our basepoint for π_1 to be anything, without loss of generality we may assume it is $\{1, 2, \cdots, n\} \subset \mathbb{C}$ for the purpose of visualization. Tuples in $\mathbb{C}^n$ with nondistinct coordinates represent two strings intersecting at the same point, which is why we must delete this subspace from $\mathbb{C}^n$: to prevent collisions.

A path in $\mathbb{C}^n$ ending where it started means each colored string above would have to go back to its original point, and this defines a pure braid. If we quotient by the action of S_n, we essentially allow the path in configuration space to go to any of the permuted configurations, which means the strings in the braid diagram can connect *different* dots.

2 Lecture 2 (13 March, 2023)

2.1 Monoidal Tensor Categories

A category is a "class" of objects, and (at least) a set of morphisms $\mathrm{Hom}(A, B)$ for every two objects, with associative composition and an identity in each $\mathrm{End}(A) = \mathrm{Hom}(A, A)$.

If the class of objects is merely a set, the category C is called "small". These categories of interest for us may as well be small.

Compositions in a category are "linear words". $f \circ g \circ h$ or just fgh means $f(g(h(x)))$, so h then g then f.

Goal: To enrich a category to make the allowed words graphs rather than linear words. These graphs can be called tensor networks.

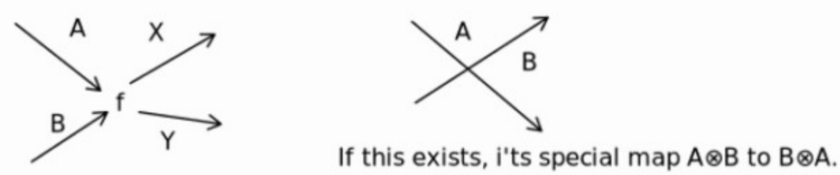
Easiest case is planar, acylic tensor networks that flow from left to right (say), or top to bottom.

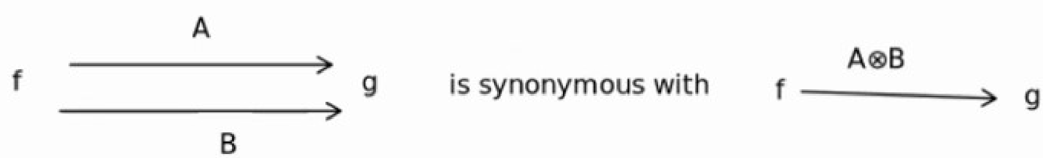
This is what a monoidal category achieves. The idea is to make a multiplication law on objects as morphism with suitable axioms. If A and B are objects, so $A \otimes B$ (new operation, not a universal property). If f and g are morphisms, so is $f \otimes g$. You may assume axioms so that $f\colon A \otimes B \otimes \cdots \to X \otimes Y \otimes \cdots$ can be a vertex in an acyclic tensor network that then has a well-defined value as a morphism. There is also a unit object I s.t. $I \otimes A = A$.

Why planar? Because no prior relationship between $A \otimes B$ and $B \otimes A$.

An important example: The category of vector spaces with "$\otimes$" is the usual tensor product.

Even the simplest thing, a just plain monoidal category, has "fusion" or bundling of edges.





A monoidal (or tensor) category is *symmetric* means that there is a distinguished switching isomorphism $s\colon A \otimes B \to B \otimes A$ for every A and B, with various axioms to make it do what you want. s_{AB} and s_{BA} should be inverses, and more subtly

$$(A \otimes B) \otimes C \to C \otimes (A \otimes B)$$

should do the same thing as $A \otimes B \otimes C \to A \otimes C \otimes B \to C \otimes A \otimes B$.

Example: Again, vector spaces.

A victory: You can always interpret tensor networks as circuits in the sense of computer science. The three most popular models of computers – deterministic, randomized and quantum – are all expressible with symmetric tensor categories.

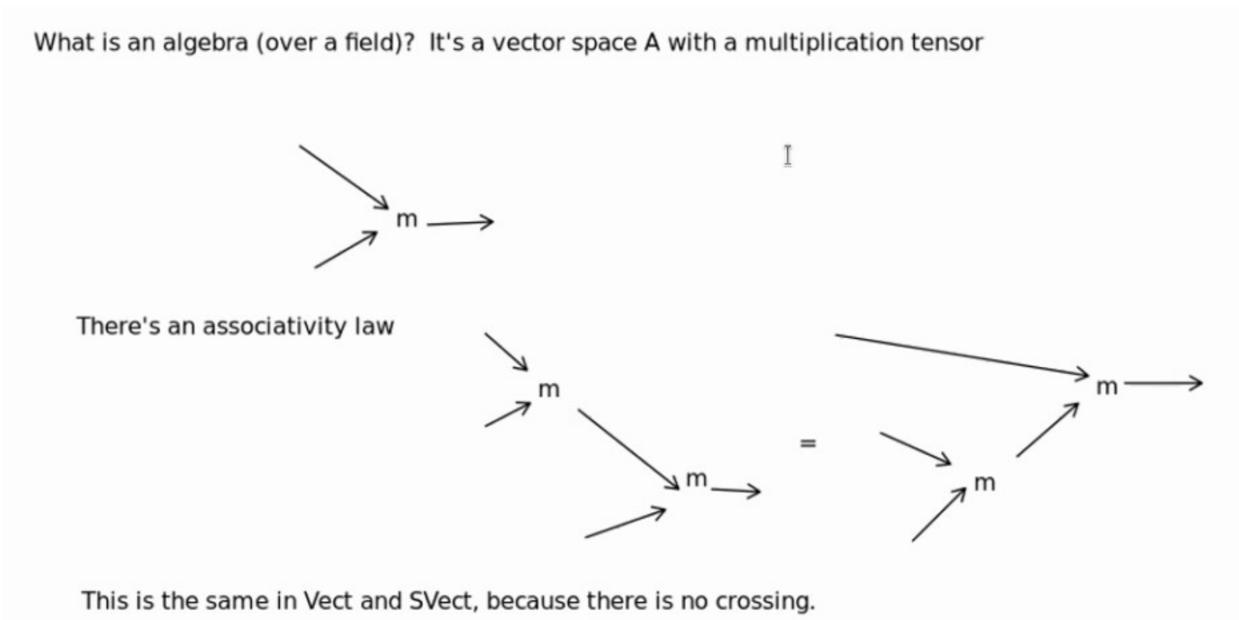
For deterministic computation, the category is set (finite sets) and functions, and $\otimes = \times$. For randomized computation, the objects are finite sets, the morphisms are stochastic maps and $\otimes = \otimes$ for the map.

For quantum computation, the objects are finite-dimensional Hilbert spaces (or sums of matrix algebras) and the morphisms are TPCPs.

2.2 $\otimes$ category Vect of vector spaces

Take graded (or at least $\mathbb{Z}/2$-graded) vector spaces. Then $V \otimes W$ is also naturally graded (or binary graded) and that is a very similar category to Vect. Now there is an alternating switching map that is just as good as the normal one.

$$(v \otimes w) \to (-1)^{(\deg v)(\deg w)} w \otimes v$$



(Binary graded is better actually.) Then you get a new category, SVect, super vector spaces.

The commutativity law has a cross, so that supercommutative algebras are more general than commutative algebras.

Example: A poly algebra $F\{a_1, a_2, \ldots, a_n\}$ where the generators anticommute is supercommutative if the generators are odd-graded.

2.3 Braid Tensor Category

The Jacobi identity for a Lie algebra (and the asymmetry $[x, y] = -[y, x]$) has crossings. So you can define a Lie superalgebra, and it's more general than a Lie algebra.

A symmetric tensor category has a subtle generalization, called braid tensor category. We assume two switching isomorphisms from $A \otimes B \to B \otimes A$, not just one, left and right half twist. The consistency axioms can be adapted to this.

End result: Valid tensor networks can but don't have to be planar. If they're not planar, they are tangled in $\mathbb{R}^3$. So far they still have to be left-to-right acyclic.

Symmetric monoidal is a degenerate special case of braided monoidal.

Left (half) twist from $A \otimes B$ to $B \otimes A$ is inverse to the right half twist from $B \otimes A$ to $A \otimes B$.

Sometimes, but not always, a braid tensor category is perfectly happy to be a subcategory of Vect (or often vect, just finite dimensional vector spaces) except with a variant $\otimes$.

If G is a group and $\mathbb{F}$ is a field ($\mathbb{C}$), then there is a category $\mathrm{rep}(G)$ of finite dimensional representations. In fact, a symmetric $\otimes$ category (and ultimately a subcategory of vect). If V and W are two representations of G, then (1) $\mathrm{Hom}(V, W)$ is just the G-linear maps. (2) $V \otimes W$ needs an action of G, not $G \times G$. For a group, you use the diagonal action $g(v \otimes w)\colon gv \otimes gw$.

If L is a Lie algebra, there is a similar construction of $\mathrm{Rep}(L)$, except:

$$a(v \otimes w)\colon = (av) \otimes w + v \otimes (aw)$$

$\mathsf{rep}(G)$ and $\mathsf{rep}(L)$ are in fact symmetric monoidal subcategories of vect.

An amazing discovery: If G is a complex simple (or compact simple) Lie group, then $\mathsf{rep}(G)$ which is symmetric monoidal, has a braided monoidal deformation. $\mathsf{rep}_q(G)$ where q is a complex number and $q = 1$ is the starting "classical" case. $\mathsf{rep}(G) = \mathsf{rep}_1(G)$. You can work over $\mathbb{C}[q, q^{-1}]$ or you can let q be non-zero in $\mathbb{C}$. You can actually keep "$\otimes$" the same, morally it moves too, but certainly s_{AB} get deformed, so that s_{AA} no longer has order 2.

s_{AB} is the usual switching map with an adjustment called and R-matrix which is actually a 4-index tensor. You can flatten a native tensor network in $\mathsf{rep}_q(G)$ into a planar tensor network in vect, but you have to replace each crossing by R or R^{-1} composed with the usual switching map.

The most popular way to set this up is to work at the Lie algebra level, and replace $U(L)$ by a deformed algebra $U_q(L)$, which is officially called a "quantum group".

There is a universal R is some version of $U_q(L) \otimes U_q(L)$.

If L is a Lie algebra, it has a fellow travelling associative algebra, the universal enveloping algebra, given by reinterpreting $z = [x, y]$ as $z = xy - yx$. Theorem: (PBW) $U(L)$ is a deformed polynomial algebra. If L is abelian so that $[x, y] = 0$ always, then $U(L)$ is exactly the algebra of polynomials in $\dim L$ variables.

The Jones polynomial of a knot can be realized as the value of a tensor network in $\mathsf{rep}_q(\mathsf{SL}(2, \mathbb{C}))$ or $\mathsf{rep}_q(\mathsf{sl}(2, \mathbb{C}))$ or $\mathsf{rep}_q(SU(2))$, where the network is just K itself labeled by the 2-dimensional representation of $\mathrm{sl}_2(2, \mathbb{C})$, etc.

$\mathsf{rep}_q(G)$ or $\mathsf{rep}_q(L)$ both live as monoidal subcategories of vect, only changing the crossing maps s_{AB}. So, the objects all still have integer dimensions which multiply when you tensor, and add when you take direct sums. Whatever you get, it can't be the Fibonacci category, which has an object F where

$F \otimes F = F \oplus I$ implies that $\dim \mathrm{Inv}(F^{\otimes n})$ is a Fibonacci number.

However, close. $\mathrm{rep}_q(SU(2))$, when q is a 5th root of unity, develops an ideal as a linear tensor category. You can quotient $\mathrm{rep}_q(SU(2))$ by its ideal, which then destroys its chance to live in vect, but the Fibonacci category lives inside of it afterward.

The formulation, where you (1) deform $\mathrm{rep}(G)$ into $\mathrm{rep}_q(G)$, (2) let q be a root of unity, and (3) quotient by the negligible ideal. This is an important source of fusion and modular tensor categories.