Tutorial on dagger categories

Peter Selinger

Dalhousie University Halifax, Canada

FMCS 2018

Part I: Quantum Computing

Quantum computing: States

• state of one qubit:
$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \neq 0$$
.

• state of two qubits:

$$\left(\begin{array}{c} \alpha \\ \beta \\ \gamma \\ \delta \end{array}\right).$$

• separable:
$$\begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix}$$
.

• otherwise *entangled*.

Notation

•
$$|\mathbf{0}\rangle = \begin{pmatrix} 1\\ 0 \end{pmatrix}, |\mathbf{1}\rangle = \begin{pmatrix} 0\\ 1 \end{pmatrix}.$$

• $|\mathbf{i}\mathbf{j}\rangle = |\mathbf{i}\rangle \otimes |\mathbf{j}\rangle$ etc.

Quantum computing: Operations

- unitary transformation
- measurement

Some standard unitary gates

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$
$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{i} \end{pmatrix},$$
$$CNOT = \begin{pmatrix} \frac{1}{0} & 0 \\ 0 & X \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ \frac{0 & 1 & 0 & 0}{0 & 0 & 1} \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Measurement



Mixed states

A *mixed state* is a (classical) probability distribution on quantum states.

Ad hoc notation:

$$\frac{1}{2}\left\{ \left(\begin{array}{c} \alpha \\ \beta \end{array} \right) \right\} + \frac{1}{2}\left\{ \left(\begin{array}{c} \alpha' \\ \beta' \end{array} \right) \right\}$$

Note: A mixed state is a description of our *knowledge* of a state. An actual closed quantum system is always in a (possibly unknown) "pure" (= non-mixed) state.

Density matrices (von Neumann)

Represent the pure state $v = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \in \mathbb{C}^2$ by the matrix

$$u v^{\dagger} = \left(\begin{array}{cc} \alpha \overline{\alpha} & \alpha \overline{\beta} \\ \beta \overline{\alpha} & \beta \overline{\beta} \end{array} \right) \in \mathbb{C}^{2 \times 2}.$$

Represent the mixed state $\lambda_1\left\{\nu_1\right\}+\ldots+\lambda_n\left\{\nu_n\right\}$ by

$$\lambda_1 \nu_1 \nu_1^{\dagger} + \ldots + \lambda_n \nu_n \nu_n^{\dagger}.$$

This representation is not one-to-one, e.g.

$$\frac{1}{2}\left\{ \left(\begin{array}{c}1\\0\end{array}\right)\right\} + \frac{1}{2}\left\{ \left(\begin{array}{c}0\\1\end{array}\right)\right\} = \frac{1}{2}\left(\begin{array}{c}1&0\\0&0\end{array}\right) + \frac{1}{2}\left(\begin{array}{c}0&0\\0&1\end{array}\right) = \left(\begin{array}{c}.5&0\\0&.5\end{array}\right)$$

$$\frac{1}{2} \left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\} + \frac{1}{2} \left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\} = \frac{1}{2} \begin{pmatrix} .5 & .5 \\ .5 & .5 \end{pmatrix} + \frac{1}{2} \begin{pmatrix} .5 & -.5 \\ -.5 & .5 \end{pmatrix} = \begin{pmatrix} .5 & 0 \\ 0 & .5 \end{pmatrix}$$

But these two mixed states are indistinguishable.

Quantum operations on density matrices

Unitary:

$\nu \mapsto U \nu$	$vv^{\dagger} \mapsto Uvv^{\dagger}U^{\dagger}$	$A \mapsto UAU^{\dagger}$

Measurement:



Quantum operations

A *quantum operation* is a map from mixed states to mixed states that is physically possible.

Mathematically, it is a function from density matrices to density matrices that is:

(1) linear

- (2) *positive:* A positive \Rightarrow F(A) positive
- (3) completely positive: $F \otimes id_n$ positive for all n
- (4) trace non-increasing: A positive $\Rightarrow tr F(A) \leq tr(A)$

Theorem: The above conditions are necessary and sufficient for **F** to be physically possible. In particular, unitary transformations and measurements are both special cases.

Characterization of completely positive maps

Let $F:\mathbb{C}^{n\times n}\to\mathbb{C}^{m\times m}$ be a linear map. We define its characteristic matrix as

$$\chi_{F} = \begin{pmatrix} F(E_{11}) & \cdots & F(E_{1n}) \\ \vdots & \ddots & \vdots \\ F(E_{n1}) & \cdots & F(E_{nn}) \end{pmatrix}.$$

Theorem (Characteristic matrix; Choi's theorem). F is completely positive if and only if χ_F is positive.

Another, better-known characterization is the following:

Theorem (Kraus representation theorem): F is completely positive if and only if it can be written in the form

$$F(A) = \sum_{i} B_{i}AB_{i}^{\dagger}$$
, for some matrices B_{i} .

Part II: Dagger categories

"Untyped" quantum mechanics All countably-based Hilbert spaces are isomorphic. Therefore, in physics, one often works in a single fixed Hilbert space \mathcal{H} . Let

 $\mathsf{f} \; : \; \mathcal{H} \; \to \mathcal{H}.$

Then one also has:

f^{\dagger} :	${\cal H}$	\rightarrow	${\cal H}$	(the	adjoint)
f*:	\mathcal{H}^*	\rightarrow	\mathcal{H}^*	(the	transpose)
f :	\mathcal{H}^*	\rightarrow	\mathcal{H}^*	(the	conjugate)

Objects

Hilbert spaces form a category. Recognizing more than one object makes the notation much clearer.

Examples:

- a self-adjoint operator $(f^{\dagger} = f)$ must be of type $A \rightarrow A$
- a unitary operator $(f^{\dagger} = f^{-1})$ can be of type $A \to B$
- an *idempotent* $(f \circ f = f)$ must be of type $A \rightarrow A$

Dagger categories

Definition. A *dagger category* is a category C together with an involutive, identity-on-objects, contravariant functor $\dagger : C \to C$.

Concretely:

• operation:

$$\frac{f: A \to B}{f^{\dagger}: B \to A}$$

• equations:

$$\mathsf{id}_A^\dagger = \mathsf{id}_A, \qquad (g \circ f)^\dagger = f^\dagger \circ g^\dagger, \qquad f^{\dagger\dagger} = f$$

This notion has appeared in the literature many times, e.g., [Puppe 1962], [Doplicher and Roberts 1989]. More recently popularized by [Abramsky and Coecke 2004].

In a dagger category:

- A morphism $f : A \to B$ is called *unitary* if $f^{\dagger} \circ f = id_A$ and $f \circ f^{\dagger} = id_B$.
- A morphism $f: A \to A$ is called *self-adjoint* or *hermitian* if $f = f^{\dagger}$.
- A morphism $f : A \to A$ is called *positive* if there exists C and $h : A \to C$ such that $f = h^{\dagger} \circ h$.

Dagger symmetric monoidal categories

Definition. A dagger symmetric monoidal category is a symmetric monoidal category with a dagger structure, satisfying the following additional equations: for all $f : A \rightarrow B$, $g : B \rightarrow C$, and $h : C \rightarrow D$:

$$\begin{array}{ll} (f\otimes h)^{\dagger} = f^{\dagger}\otimes h^{\dagger} : B\otimes D \to A\otimes C, \\ \alpha^{\dagger}_{A,B,C} = \alpha^{-1}_{A,B,C} & : A\otimes (B\otimes C) \to (A\otimes B)\otimes C, \\ \lambda^{\dagger}_{A} = \lambda^{-1}_{A} & : I\otimes A \to A, \\ \sigma^{\dagger}_{A,B} = \sigma^{-1}_{A,B} & : B\otimes A \to A\otimes B. \end{array}$$

Examples: Sets and relations, Hilbert spaces and linear functions.

Dagger traced monoidal categories

Definition. A *dagger traced monoidal category* is a dagger symmetric monoidal category with a natural family of *trace operators*

$$\operatorname{Tr}^X : (A \otimes X, B \otimes X) \to (A, B),$$

satisfying the usual three trace axioms and:

$$\mathsf{Tr}^{\mathsf{X}}(\mathsf{f}^{\dagger}) = (\mathsf{Tr}^{\mathsf{X}}\,\mathsf{f})^{\dagger}.$$

Examples: Sets and relations; Hilbert spaces and linear functions.

Compact closed categories

A *compact closed category* is a symmetric monoidal category with the following additional structure:

• a new operations on objects:

A^*

• additional morphisms:

$$\begin{array}{ll} \eta_A: \ I \to A^* \otimes A & (\text{unit}) \\ \varepsilon_A: \ A \otimes A^* \to I & (\text{counit}) \end{array}$$

• equations:

$$\lambda_{A}^{-1} \circ (\epsilon_{A} \otimes \mathrm{id}_{A}) \circ \alpha_{A,A^{*},A}^{-1} \circ (\mathrm{id}_{A} \otimes \eta_{A}) \circ \rho_{A} = \mathrm{id}_{A}$$
$$\rho_{A^{*}}^{-1} \circ (\mathrm{id}_{A^{*}} \otimes \epsilon_{A}) \circ \alpha_{A^{*},A,A^{*}} \circ (\eta_{A} \otimes \mathrm{id}_{A^{*}}) \circ \lambda_{A} = \mathrm{id}_{A^{*}}.$$

From this, one can define: $f^* : B^* \to A^*$, given $f : A \to B$.

Dagger compact closed categories

Definition. A *dagger compact closed category* is a compact closed, dagger symmetric monoidal category also satisfying



Examples: Sets and relations, Hilbert spaces and linear functions.

Theorem (essentially Joyal, Street, and Verity): every dagger traced monoidal category can be fully and faithfully embedded in a dagger compact closed category. Conversely, any full an faithful subcategory of a dagger compact closed category is dagger traced monoidal.

Categorical quantum mechanics

A surprising amount of quantum mechanics can be done from the axioms of a dagger compact closed category (i.e., without assuming anything a priori about the complex numbers). One can express e.g. scalars and vectors, inner products, projections, unitary maps, and self-adjoint operators, measurement and the Born rule, quantum protocols, and much more. Graphical language of dagger traced monoidal categories



In the graphical language, the adjoint is the "mirror image" of a box (or diagram).

Graphical language, continued





 $\mbox{Counit} \quad \varepsilon_{\mathcal{A}}: \mathcal{A} \otimes \mathcal{A}^* \to I$

If $f : A \to B$, then f, $f^{\dagger} : B \to A$, $f_* : A^* \to B^*$, and $f^* : B^* \to A^*$ are graphically represented as follows:



Here $f_* = (f^{\dagger})^* = (f^*)^{\dagger}$.

Theorem [Kelly/Laplaza 1980, Joyal/Street/Verity 1996, Selinger 2005]. A well-typed equation between morphisms in the language of dagger traced monoidal (or dagger compact closed) categories follows from the axioms if and only if it holds, up to graph isomorphism, in the graphical language. Quantum mechanics, graphically

Let **C** be a dagger compact closed category.

Scalars. a *scalar* is a morphism $\phi : I \to I$, graphically ϕ Note that for scalars,

Vectors. A vector of type A is a morphism $f: I \to A$, graphically $f \to A$.

Inner product. Given two vectors $f, g : I \to A$, their *inner product* $\langle f | g \rangle$ is the scalar $f^{\dagger} \circ g$:

Matrices

An $(A \times B)$ -*matrix* is a morphism $I \to A^* \otimes B$.

The matrix of a map $f : A \to B$ is $\lceil f \rceil : I \to A^* \otimes B$, defined as follows:



Positive maps and matrices

A morphism $f : A \to A$ is *positive* if it is of the form $f = g^{\dagger} \circ g$, for some B and $g : A \to B$.



A *positive matrix* is the matrix of a positive map, i.e., it is of the form



where $k = g^{\dagger}$.

30

Completely positive map

By Choi's theorem, a morphism $f : A^* \otimes A \to B^* \otimes B$ in Hilbert spaces is *completely positive* if it is of the form



In an arbitrary dagger compact closed category, Choi's theorem becomes a definition.

Remark A completely positive map



applied to a positive matrix



yields a positive matrix.

The CPM contruction

Definition. Let C be a dagger compact closed category. The category CPM(C) of *completely positive maps over* C has:

- the same objects as C,
- a morphism $f : A \to B$ in **CPM**(**C**) is a completely positive map $f : A^* \otimes A \to B^* \otimes B$ in **C**.

For example, **CPM**(**Hilb**) is the usual category of completely positive maps.

Theorem. If C is dagger compact closed, then so is CPM(C).

Part III: Completeness

Introduction

Hasegawa, Hofmann, and Plotkin: an equation holds in all traced symmetric monoidal categories if and only if it holds in finite dimensional vector spaces.

Corollary: finite dimensional vector spaces are also complete for compact closed categories (using [Joyal/Street/Verity 1996]).

Here:

- we simplify Hasegawa, Hofmann, and Plotkin's proof;
- we extend it to *dagger* traced symmetric monoidal categories (therefore: dagger compact closed categories) and finite dimensional *Hilbert* spaces.

Evaluation of diagrams: summation over internal indices



Statement of the main result

Theorem 1. Let $M, N : A \to B$ be two terms in the language of dagger traced monoidal categories. Then [M] = [N] holds for every possible interpretation in finite dimensional Hilbert spaces if and only if M = N holds in the graphical language (and therefore, holds in all dagger traced monoidal categories).

Signature

A *signature* is a collection of object variables and morphism variables with domain and codomain information.

Example: $\{A, B, f: B \to A \otimes A, g: A \otimes B \to B \otimes A\}$.

Here is a diagram N over this signature:



Interpretation

An *interpretation* of a signature in finite-dimensional Hilbert spaces consists of the following data:

- for each object variable A, a chosen finite-dimensional Hilbert space [A];
- for each morphism variable $f: A_1 \otimes \ldots \otimes A_n \to B_1 \otimes \ldots \otimes B_m$, a chosen linear map $\llbracket f \rrbracket : \llbracket A_1 \rrbracket \otimes \ldots \otimes \llbracket A_n \rrbracket \to \llbracket B_1 \rrbracket \otimes \ldots \otimes \llbracket B_m \rrbracket$.

We define $\llbracket f^{\dagger} \rrbracket = \llbracket f \rrbracket^{\dagger}$.

Evaluation of diagrams

The *evaluation* of a diagram M under a given interpretation is a scalar that is defined by the usual "summation over internal indices" formula. Example:



$$\llbracket N \rrbracket = \sum_{a_1, b_2, b_3, a_4, a_5} \llbracket g \rrbracket_{b_3, a_1}^{a_1, b_2} \cdot \llbracket f \rrbracket_{a_5, a_4}^{b_3} \cdot \llbracket f^{\dagger} \rrbracket_{b_2}^{a_5, a_4}.$$

Main result

Theorem 1. Let $M, N : A \to B$ be two terms in the language of dagger traced monoidal categories. Then [M] = [N] holds for every possible interpretation in finite dimensional Hilbert spaces if and only if M = N holds in the graphical language (and therefore, holds in all dagger traced monoidal categories).

Reductions

Without loss of generality, it suffices to consider a special case:

- We may assume that $M, N : I \to I$, i.e., that both the domain and codomain of M and N are the tensor unit.
- It suffices to consider terms whose graphical representation does not contain any "trivial cycles".

Relative completeness

Theorem 1 is a consequence of the following lemma:

Lemma 2 (Relative completeness). Let M be a (closed simple dagger traced monoidal) diagram. Then there exists an interpretation $[-]_M$ in finite dimensional Hilbert spaces, depending only on M, such that for all N, $[N]_M = [M]_M$ holds if and only if N and M are isomorphic diagrams.

Right-to-left: trivial.

We call this interpretation the *M*-interpretation.

The M-interpretation

Suppose M is the following diagram:



The M-interpretation is defined as follows:

- [A]_M is a 3-dimensional Hilbert space with orthonormal basis {A₁, A₂, A₄};
- [B]_M is a 2-dimensional Hilbert space with orthonormal basis {B₃, B₅};

The M-interpretation, continued



Define three linear maps $F_x : \llbracket B \rrbracket_M \to \llbracket A \rrbracket_M \otimes \llbracket A \rrbracket_M$, $F_y : \llbracket A \rrbracket_M \otimes \llbracket A \rrbracket_M \to \llbracket B \rrbracket_M$, and $F_z : \llbracket A \rrbracket_M \otimes \llbracket B \rrbracket_M \to \llbracket B \rrbracket_M \otimes \llbracket A \rrbracket_M$.

$$(F_x)_{jk}^i = \begin{cases} x & \text{if } i = B_5, \ j = A_2, \ \text{and } k = A_1, \\ 0 & \text{else}, \end{cases}$$

$$(F_y)_k^{ij} = \begin{cases} y & \text{if } i = A_2, \ j = A_1, \ \text{and } k = B_3, \\ 0 & \text{else}, \end{cases}$$

$$(F_z)_{kl}^{ij} = \begin{cases} z & \text{if } i = A_4, \ j = B_3, \ k = B_5, \ \text{and } l = A_4 \\ 0 & \text{else}. \end{cases}$$

where x, y, z are fixed chosen algebraically independent transcendentals.

The M-interpretation, continued



Finally, define

$$\begin{bmatrix} \mathbf{f} \end{bmatrix}_{\mathcal{M}} = \mathbf{F}_{\mathbf{x}} + \mathbf{F}_{\mathbf{y}}^{\dagger} \\ \begin{bmatrix} \mathbf{g} \end{bmatrix}_{\mathcal{M}} = \mathbf{F}_{\mathbf{z}}.$$

Note: we took the adjoint of F_y .

Proof of the Lemma



Calculate the M-interpretation of N:

$$\llbracket N \rrbracket = \sum_{a_1, b_2, b_3, a_4, a_5} \llbracket g \rrbracket_{b_3, a_1}^{a_1, b_2} \cdot \llbracket f \rrbracket_{a_5, a_4}^{b_3} \cdot \llbracket f^{\dagger} \rrbracket_{b_2}^{a_5, a_4}.$$

This is an integer polynomial in $x, y, z, \overline{x}, \overline{y}, \overline{z}$.

Claim: The coefficient at xyz is non-zero iff $N \cong M$.

Proof of the Lemma, continued



In fact, the only non-zero contribution comes from the assignment $a_1 \mapsto A_4$, $b_2 \mapsto B_3$, $b_3 \mapsto B_5$, $a_4 \mapsto A_1$, and $a_5 \mapsto A_2$.

This corresponds exactly to the (in this case unique) isomorphism from N to M.

Corollary: the integer coefficient of p at xyz is equal to the *number* of different isomorphisms between N and M (usually 0 or 1, but could be more).

Generalization: other fields

- Theorem 1 works for any field k of characteristic 0 with a non-trivial involutive automorphism $x \mapsto \overline{x}$ (but not Lemma 2).
- if there aren't enough transcendentals, first pass to $k(x_1, \ldots, x_n)$.
- Pass from $k(x_1, \ldots, x_n)$ to k because in a field of characteristic 0, any non-zero polynomial has a non-root.

Open question: bounded dimension

- The M-interpretation uses Hilbert spaces of unbounded dimension.
- Does Theorem 1 remain true if the dimension of the Hilbert spaces is fixed to some n?
- Not true in dimension 2. Bob Paré's counterexample:

tr(AABBAB) = tr(AABABB)

holds for 2×2 -matrices, but not in the graphical language.

Proof: Cayley-Hamilton theorem: $A^2 = \mu A + \nu I$ for some scalars μ, ν . Therefore

 $tr(AABBAB) = \mu tr(ABBAB) + \nu tr(BBAB),$ $tr(AABABB) = \mu tr(ABABB) + \nu tr(BABB),$

• Unknown in dimension 3.