A Categorical Approach to Quantum Computing

Ross Duncan

Attributions

The categorical presentation of quantum mechanics is due to Samson Abramsky and Bob Coecke (see *Proc. LiCS 2004*)

The associated quantum logic is joint work with Samson Abramsky (see *Proc QPL 2004*)

Motivation

We are interested in *types* for quantum mechanics

- to design nice quantum programming languages
- to prove correctness of quantum protocols and algorithms
- discover new models for quantum computation?
- perhaps learn something new about physics?

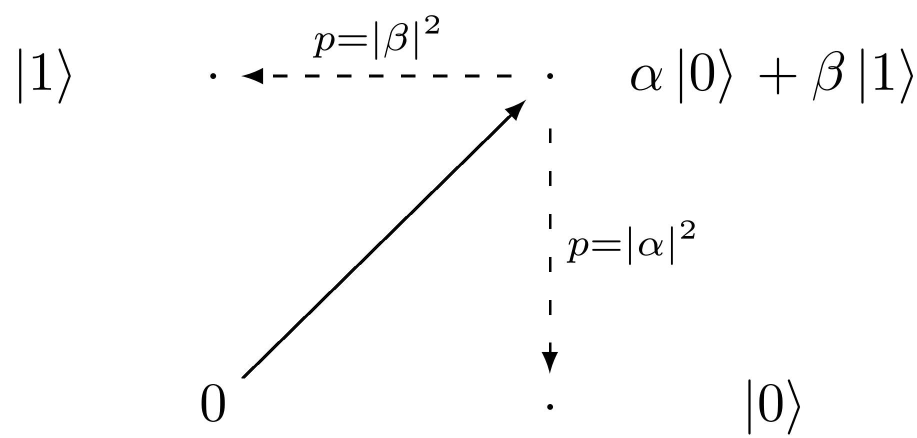
Most current work on quantum programming languages treats the quantum realm as a *black box*... but we know this is wrong!

- Teleportation protocol (+ many others) show *information flow* along quantum parts of the system.
- Josza proved that quantum speedup is due to *increasing entanglement* between subsystems.

Want to reveal and describe this informatic structure.

Quantum Behaviour

- *Quantum states* are complex (unit) vectors (upto phase)
- Often think of *qubits*: vectors in $\mathbb{C}^2$ with standard basis $|0\rangle, |1\rangle$.
- Compounds systems formed by *tensor product*: can't always separate components.
- *Measurement* involves projection onto a basis:



Entanglement

- *Entangled* states cannot be separated into components, e.g. $\forall \psi, \phi$:

$$|00\rangle + |11\rangle \neq |\psi\rangle \otimes |\phi\rangle$$

- Measurement at one component causes collapse at the other:

$$\begin{tikzcd} & {|00\rangle + |11\rangle} \arrow[dl] \arrow[dr] & \\ {|00\rangle} & \text{or} & {|11\rangle} \end{tikzcd}$$

More on Entanglement

For finite dimensional Hilbert spaces A, B we have an isomorphism

$$\begin{array}{rcl} A \otimes B & \cong & A \to B \\ \sum_{ij} z_{ij} \cdot (a_i \otimes b_j) & \cong & (a_i \mapsto \sum_j z_{ij} b_j) \end{array}$$

We can see that under this isomorphism

$$|00\rangle + |11\rangle \quad \cong \quad \begin{array}{l} |0\rangle \mapsto |0\rangle \\ |1\rangle \mapsto |1\rangle \end{array} \quad = \quad \mathrm{id}_Q$$

In general, maximally entangled states correspond to unitary maps and separable states correspond to “constants”.

Example: Bell States

Let $\beta_i : Q \to Q$ be the the following linear maps

$$\beta_1 : \begin{array}{l} |0\rangle \mapsto |0\rangle \\ |1\rangle \mapsto |1\rangle \end{array} \qquad \beta_2 : \begin{array}{l} |0\rangle \mapsto |0\rangle \\ |1\rangle \mapsto -|1\rangle \end{array}$$

$$\beta_3 : \begin{array}{l} |0\rangle \mapsto |1\rangle \\ |1\rangle \mapsto |0\rangle \end{array} \qquad \beta_4 : \begin{array}{l} |0\rangle \mapsto |1\rangle \\ |1\rangle \mapsto -|0\rangle \end{array}$$

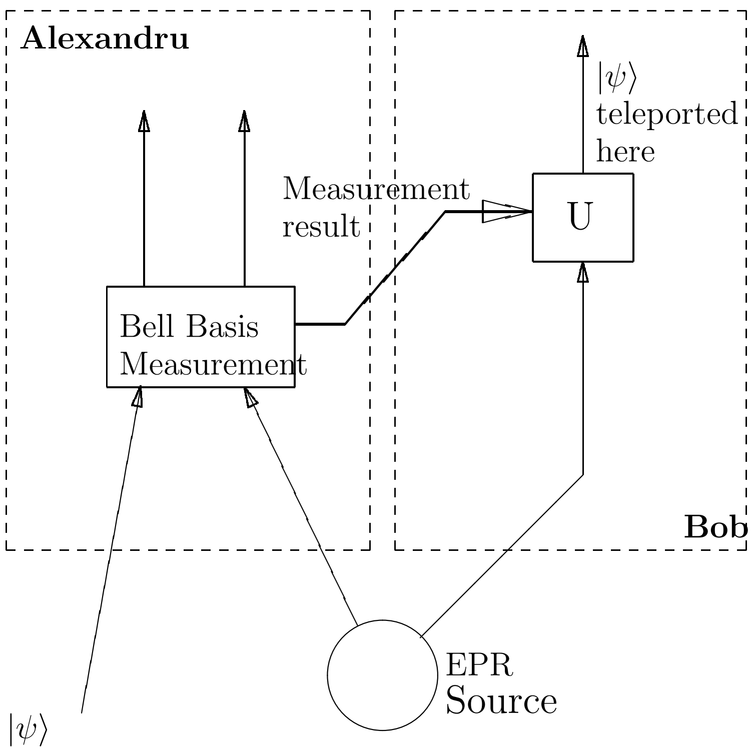
They correspond to the *Bell States*:

$$|\beta_1\rangle = |00\rangle + |11\rangle \quad |\beta_2\rangle = |00\rangle - |11\rangle$$
$$|\beta_3\rangle = |01\rangle + |10\rangle \quad |\beta_4\rangle = |01\rangle - |10\rangle$$

Teleportation

THM Impossible to duplicate an unknown quantum state.

But can *teleport* it:



More Teleportation

Let $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ then

$$(\alpha|0\rangle + \beta|1\rangle)(|00\rangle + |11\rangle)$$

$$\begin{aligned}
&= \alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle \\
&= \tfrac{1}{2}((|00\rangle + |11\rangle)(\alpha|0\rangle + \beta|1\rangle) + (|00\rangle - |11\rangle)(\alpha|0\rangle - \beta|1\rangle) \\
&\quad + (|01\rangle + |10\rangle)(\alpha|1\rangle + \beta|0\rangle) + (|01\rangle - |10\rangle)(\alpha|1\rangle - \beta|0\rangle)) \\
&= \tfrac{1}{2}(|\beta_1\rangle\,|\beta_1\psi\rangle + |\beta_2\rangle\,|\beta_2\psi\rangle + |\beta_3\rangle\,|\beta_3\psi\rangle + |\beta_4\rangle\,|\beta_4\psi\rangle)
\end{aligned}$$

The Postulates of Quantum Mechanics

1. - *State space* = finite dimensional Hilbert space;
   - *States* are 1-dim subspaces, represented by unit vectors.
2. Compound systems are formed by taking the *tensor product* of their component spaces.
3. Basic state transformations are *unitary maps*.
4. Applying a *measurement* yields:
   - a probabilistic choice of *projection* onto a basis vector;
   - knowledge about *which* projection was performed.

General Scheme

$$
\begin{tikzcd}
\text{Categorical Structure} \arrow[rr, leftrightarrow] \arrow[dr, leftrightarrow] & & \text{Logic} \arrow[dl, leftrightarrow] \\
& \text{Rewriting System} &
\end{tikzcd}
$$

Plan of Attack

$$\begin{tikzcd}
\begin{array}{c}\text{Strong Compact}\\ \text{Closed Category}\\ \text{with Biproducts}\end{array} \arrow[rr, leftrightarrow] \arrow[dr, leftrightarrow] & & \begin{array}{c}\text{Strong Compact}\\ \text{Closed Logic}\\ \text{with Biproducts}\end{array} \arrow[dl, leftrightarrow] \\
& \text{Proof-Nets} &
\end{tikzcd}$$

Compact Closed Categories

A *compact closed* category is a symmetric monoidal category where every object A has a chosen adjoint A^* and *unit* and *counit* maps

$$\eta_A : I \to A^* \otimes A$$

$$\epsilon_A : A \otimes A^* \to I$$

such that

$$\begin{tikzcd}
A \arrow[r, "\cong"] \arrow[d, "\mathrm{id}_A"'] & A \otimes I \arrow[r, "\mathrm{id}_A \otimes \eta_A"] & A \otimes (A^* \otimes A) \arrow[d, "\alpha"] \\
A & I \otimes A \arrow[l, "\cong"] & (A \otimes A^*) \otimes A \arrow[l, "\epsilon_A \otimes \mathrm{id}_A"]
\end{tikzcd}$$

Examples: vector spaces; sets and relations.

A Concrete Example: Qubits

Let Q be a 2-dim Hilbert space, with basis, $|0\rangle, |1\rangle$.

Then

$$\eta_Q : 1 \mapsto |00\rangle + |11\rangle$$

and

$$\epsilon_Q : |\psi\rangle \mapsto \langle 00 \mid \psi\rangle + \langle 11 \mid \psi\rangle.$$

We have:

- Creation of entangled states
- Projection onto an entangled state
- Use of such a pair as a quantum channel (i.e. teleportation)

Names and Conames

In any compact closed category we have

$$[A, B] \cong [I, A^* \otimes B] \cong [A \otimes B^*, I]$$

via the *name* $\ulcorner f \urcorner$ and *coname* $\llcorner f \lrcorner$ of $f : A \to B$.

$$\begin{tikzcd}
I \arrow[r, "\eta_A"] \arrow[dr, "\ulcorner f \urcorner"'] & A^* \otimes A \arrow[d, "\mathrm{id}_{A^*} \otimes f"] \\
& A^* \otimes B
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}
A \otimes B^* \arrow[d, "f \otimes \mathrm{id}_{B^*}"'] \arrow[dr, "\llcorner f \lrcorner"] & \\
B \otimes B^* \arrow[r, "\epsilon_B"'] & I
\end{tikzcd}$$

Example: Bell States

Let $\beta_i : Q \to Q$ be the the following linear maps

$$\beta_1 : \begin{array}{l} |0\rangle \mapsto |0\rangle \\ |1\rangle \mapsto |1\rangle \end{array} \qquad \beta_2 : \begin{array}{l} |0\rangle \mapsto |0\rangle \\ |1\rangle \mapsto -|1\rangle \end{array}$$

$$\beta_3 : \begin{array}{l} |0\rangle \mapsto |1\rangle \\ |1\rangle \mapsto |0\rangle \end{array} \qquad \beta_4 : \begin{array}{l} |0\rangle \mapsto |1\rangle \\ |1\rangle \mapsto -|0\rangle \end{array}$$

The *names* of these maps are the Bell states:

$$\ulcorner\beta_1\urcorner : 1 \mapsto |00\rangle + |11\rangle \quad \ulcorner\beta_2\urcorner : 1 \mapsto |00\rangle - |11\rangle$$

$$\ulcorner\beta_3\urcorner : 1 \mapsto |01\rangle + |10\rangle \quad \ulcorner\beta_4\urcorner : 1 \mapsto |01\rangle - |10\rangle$$

Scalars

In any call the endomorphisms $I \to I$ *scalars*; define scalar multiplication $s \bullet f$ by

$$A \xrightarrow{\cong} I \otimes A \xrightarrow{s \otimes f} I \otimes B \xrightarrow{\cong} B$$

In a compact closed category we have $I \cong [I, I]$.

PROP: in any symmetric monoidal category the scalars form a commutative monoid.

Strong Compact Closure

Suppose that $\mathcal{C}$ is equipped with a contravariant, involutive functor $(\cdot)^\dagger$ which is the identity on objects. Call $f^\dagger$ the *adjoint* of f.

Say that that $\mathcal{C}$ is *strongly compact closed* if

$$\epsilon_A = \sigma_{A^*,A} \circ \eta_A^\dagger.$$

Now suppose $\psi, \phi : I \to A$, we can define *abstract inner product*

$$\langle \psi \mid \phi \rangle := \psi^\dagger \circ \phi$$

Unitarity

Call an isomorphism U *unitary* if $U^\dagger = U^{-1}$. We have

$$\langle U \circ \psi \mid U \circ \phi \rangle = \langle U^\dagger \circ U \circ \psi \mid \phi \rangle = \langle \psi \mid \phi \rangle$$

Zero Objects

A *zero object* is an object which is both initial and terminal

The unique maps to and from $\mathbf{0}$ give maps $\mathbf{0}_B^A$ between every pair of objects in the category

$$A \longrightarrow \mathbf{0} \longrightarrow B$$

Biproducts

A *biproduct* $- \oplus - : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$ is both a product and a coproduct.

In the n-ary case we have injections and projections

$$A_i \xrightarrow{q_i} \bigoplus_{k=1}^{n} A_k \xrightarrow{p_j} A_j$$

such that

$$p_j \circ q_i = \begin{cases} \mathrm{id}_{A_i} \text{ if } i = j \\ \mathbf{0}_{A_j}^{A_i} \text{ otherwise} \end{cases}$$

We can define addition of arrows by:

$$
\begin{tikzcd}
A \arrow[r, "f+g"] \arrow[d, "\Delta"'] & B \\
A \oplus A \arrow[r, "f \oplus g"'] & B \oplus B \arrow[u, "\nabla"']
\end{tikzcd}
$$

Categorical Quantum Mechanics (Simplified Version)

Let $\mathcal{C}$ be a strongly compact closed category with biproducts.

1. • State spaces are objects A of $\mathcal{C}$;
   • Sates are arrows $\psi : I \to A$.
2. Compound systems are formed by taking tensor products $A \otimes B$.
3. Basic state transforms are unitary maps.
4. The action of a measurement is given by a choice of projections

$$\langle M_i \rangle_i : A \to \bigoplus_i I$$

The Free Strongly Compact Closed Category with Biproducts on a Category

$$\mathbf{Cat} \underset{U}{\overset{F}{\rightleftarrows}} \mathbf{SCCCB} \qquad F \dashv U$$

- The basic types and data transforms are given by the underlying category $\mathcal{A}$
- These provide the *atoms* and *axioms* of the logic
- Freely add the structure to get $F\mathcal{A}$.

Example: let $\mathcal{Q}$ be the category with one object Q and arrows the Bell maps $\beta_i : Q \to Q$; then $F\mathcal{A}$ can represent many teleportation like protocols. Call this the *qubit category*.

Factorisation of the Free Functor

Given the free involution, the free compact closure and the free biproduct,

$$\mathbf{Cat} \underset{}{\overset{F_\dagger}{\rightleftarrows}} \mathbf{InvCat} \qquad \mathbf{Cat} \underset{}{\overset{F_{KL}}{\rightleftarrows}} \mathbf{Com}$$

$$\mathbf{Cat} \underset{}{\overset{F_\oplus}{\rightleftarrows}} \mathbf{BipCat}$$

we can factor the functor F as

$$F = F_\oplus \circ F_{KL} \circ F_\dagger$$

Loops

The *loops* L of a category $\mathcal{A}$ are equivalence classes of endomorphisms, where each composite

$$A \xrightarrow{f_1} A_1 \xrightarrow{f_2} \cdots \xrightarrow{f_i} A_i \xrightarrow{f_{i+1}} A$$

is equivalent to all its cyclic permutations. We'll assume that every loops has a canonical representative.

Let $\langle L \rangle$ be the free commutative monoid generated by L.

The Arrows of $F_{KL}\mathcal{A}$

THM (Kelly-Laplaza) : Each arrow $A \to B$ of $F_{KL}\mathcal{A}$ is determined by the following data:

- an involution θ on the signed set $A^* \otimes B$;
- a functor $v : \theta \to \mathcal{A}$;
- an element μ of $\langle L \rangle$.

Note that that $F\mathcal{A}(I, I) = \langle L \rangle$.

Choosing the Scalars

By constructing a suitable adjunction, we can force the scalars (i.e. the loops $\langle L \rangle$) be isomorphic to any given monoid.

The Structure of $F_\oplus \mathcal{A}$

Each arrow $f : \bigoplus_i A_i \to \bigoplus_j B_j$ is a matrix

$$\begin{pmatrix} f_{11} & \cdots & f_{1n} \\ \vdots & & \vdots \\ f_{m1} & \cdots & f_{mn} \end{pmatrix}$$

where each $f_{ij} : A_i \to B_j$ is a summation of arrows of $\mathcal{A}(A_i, B_j)$.

Formulae and Axioms

The formulae are given by the grammar:

$$F ::= A \mid A^* \mid F \otimes F \mid F \oplus F$$

where A are the objects of the generating category $\mathcal{A}$.

We make the following identifications:

$$X^{**} = X$$

$$(X \otimes Y)^* = X^* \otimes Y^*$$

$$(X \oplus Y)^* = X^* \oplus Y^*$$

If $\mathcal{A}$ is discrete then we have usual propositional logic – all axioms are identities.

If $\mathcal{A}$ has non-identity arrows in $\mathcal{A}$ then to each arrow $f : A \to B$ we have additional axioms and cut rules.

Two sided sequents:

$$\Gamma \vdash \Delta \,;[L]$$

Identity Group

$$\frac{}{A \vdash A \ ; []}\ \textsf{(axiom)} \qquad \frac{\Gamma, A \vdash A, \Delta \ ; [L]}{\Gamma \vdash \Delta \ ; [L]}\ \textsf{(trace)}$$

Structure Group

$$\frac{\Gamma \vdash \Delta \ ; [L]}{\tau(\Gamma) \vdash \sigma(\Delta) \ ; [L]}\ \textsf{(exchange)}$$

Multiplicative Group

$$\frac{\Gamma \vdash \Delta \ ; [L] \qquad \Gamma' \vdash \Delta' \ ; [L']}{\Gamma, \Gamma' \vdash \Delta, \Delta' \ ; [L, L']}\ \textsf{(mix)}$$

$$\frac{\Gamma, A, B \vdash \Delta \ ; [L]}{\Gamma, A \otimes B \vdash \Delta \ ; [L]}\ \textsf{(times-L)} \qquad \frac{\Gamma \vdash A, B, \Delta \ ; [L]}{\Gamma \vdash A \otimes B, \Delta \ ; [L]}\ \textsf{(times-R)}$$

$\mathcal{A}$-Generalised Identity Group

$$\frac{f}{A \vdash B \;;[]}\ (f\text{-axiom}) \qquad \text{where } f : A \to B \text{ is an arrow of } \mathcal{A}$$

$$\frac{\Gamma, A \vdash B, \Delta \;; [L]}{\Gamma \vdash \Delta \;; [L]}\ (g\text{-trace}) \quad \text{where } g : B \to A \text{ is an arrow of } \mathcal{A}.$$

$$\frac{}{\vdash \;; [h]}\ (h\text{-unit}) \qquad \text{where } h : A \to A \text{ is a loop of } \mathcal{A}.$$

Additive Group

$$\frac{\Gamma, A_i \vdash \Delta \,; [L]}{\Gamma, A_1 \oplus A_2 \vdash \Delta \,; [L]} \ \textsf{(plus-L)} \qquad\qquad \frac{\Gamma \vdash \Delta, A_i \,; [L]}{\Gamma \vdash \Delta, A_1 \oplus A_2 \,; [L]} \ \textsf{(plus-R)}$$

for $i = 1, 2$

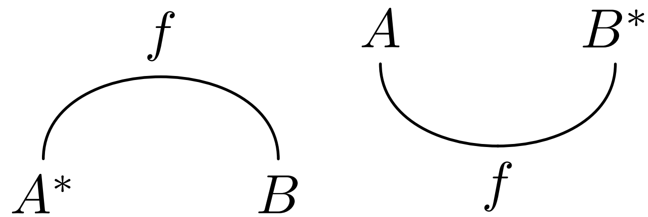
$$\frac{0^A_B}{A \vdash B \,; []} \ \textsf{(zero)} \qquad\qquad \frac{\Gamma, A \vdash B, \Delta \,; [L]}{\Gamma \vdash \Delta \,; [L]} \ \textsf{(0-cut)}$$

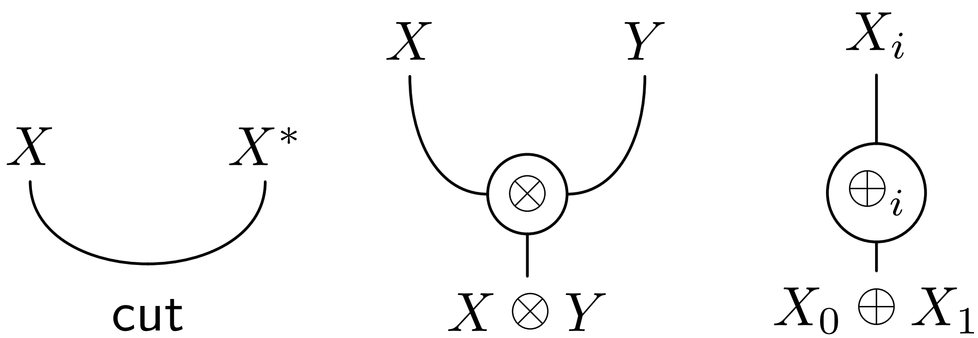
$$\frac{\Gamma \vdash \Delta \,; [L] \qquad \Gamma \vdash \Delta \,; [L']}{\Gamma \vdash \Delta \,; [L, L']} \ \textsf{(sum)}$$

Proof-Nets

A *slice* is an oriented graph, with edges labeled by formulae. The graph is constructed from the following nodes:

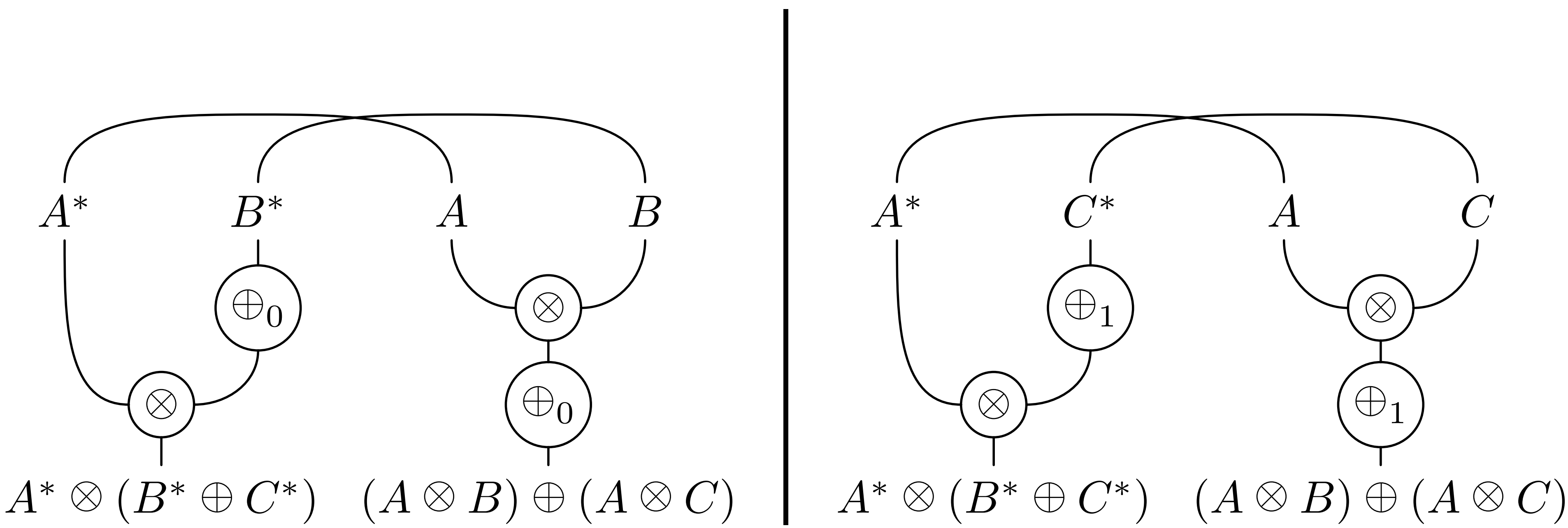
$\forall f \in \mathcal{A}[A, B]$





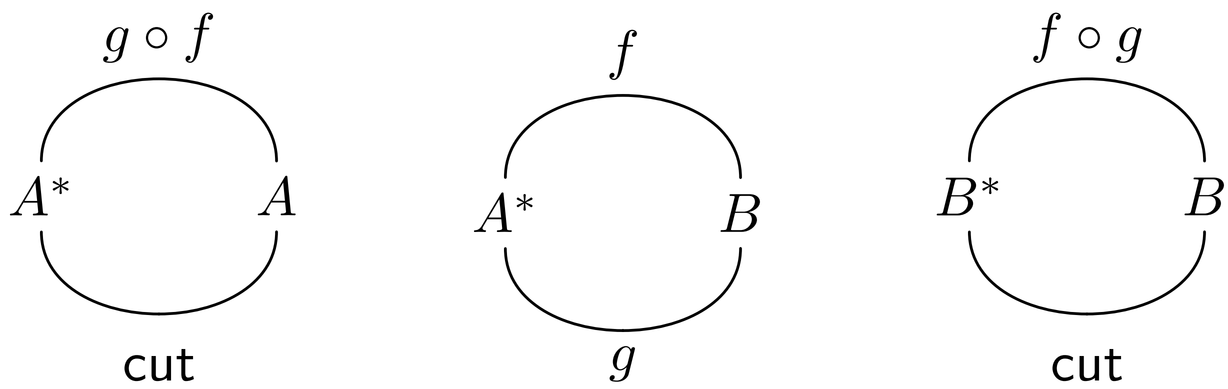
A *proof-net* is a multi-set of slices all with the same conclusions.

Example: Distributivity



Normal Forms

Suppose we have axioms $A \underset{g}{\overset{f}{\rightleftarrows}} B$. Then we can write proof-nets

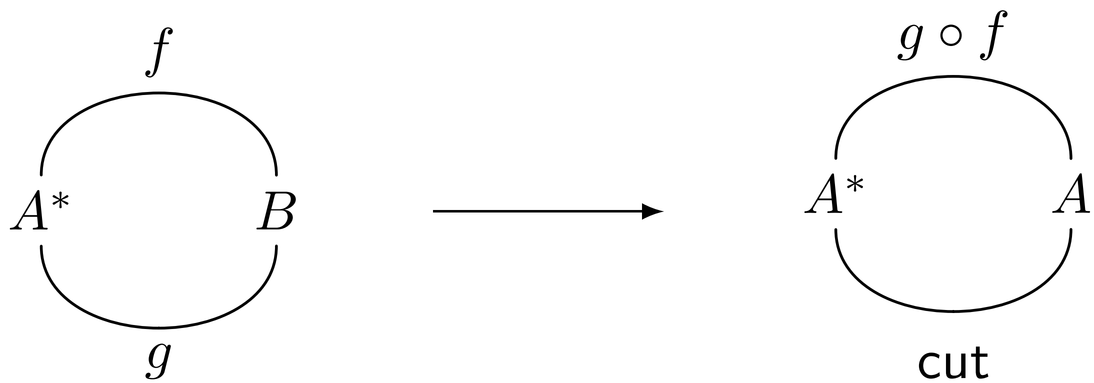


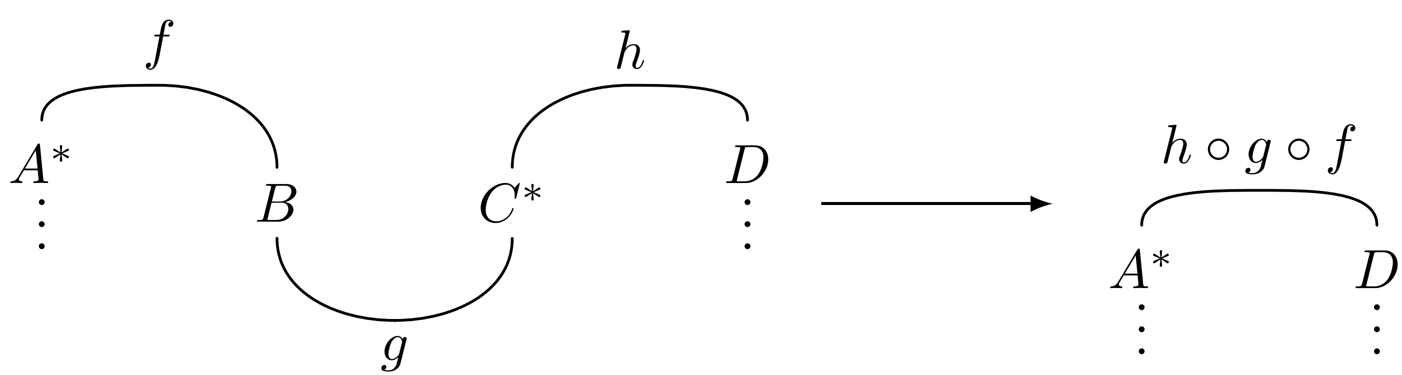
No natural way to eliminate these cuts. But note that $f \circ g$ and $g \circ f$ belong to the same equivalence class of loops. Call the outer two to be *normal loops* and identify them.

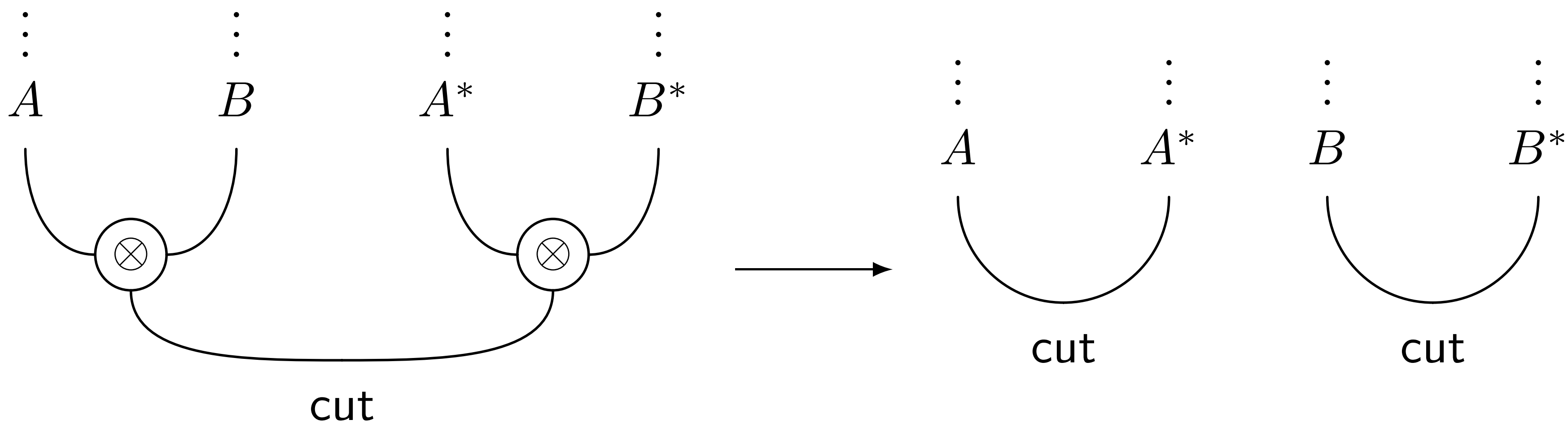
In a *normal* slice every connected component is cut-free or a normal loop. A normal proof-net has only normal slices.

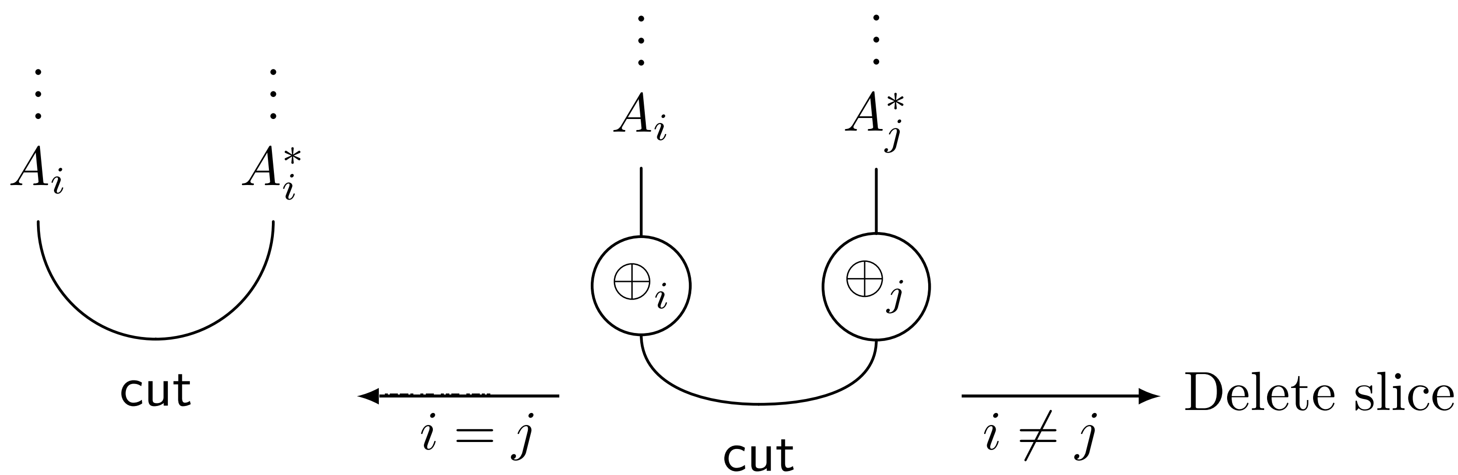
Cut-Elimination

Theorem Every proof-net can be transformed to a normal one.





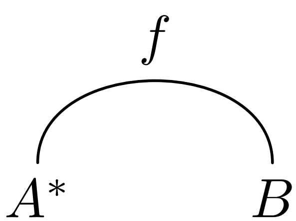

A
B
A*
B*
cut
A
A*
B
B*
cut
cut



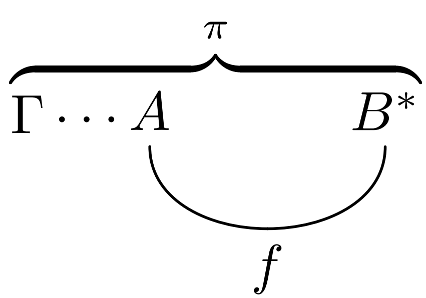
Theorem: The cut elimination procedure is strongly normalising.

Semantics

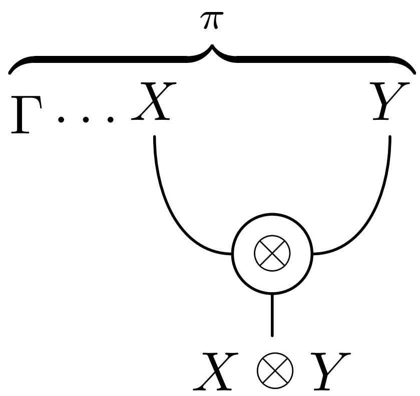
A proof-net π with conclusions Γ denotes an arrow $[\![\pi]\!] : I \to \bigotimes \Gamma$ in $F\mathcal{A}$.



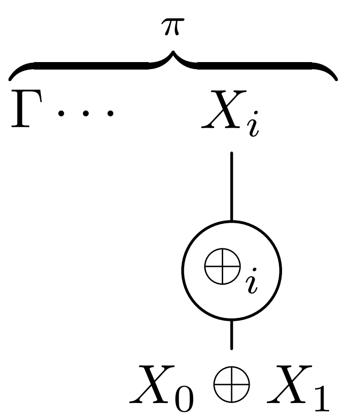
$$I \xrightarrow{\ulcorner f \urcorner} A^* \otimes B$$



$$I \xrightarrow{[\![\pi]\!]} \Gamma \otimes A \otimes B \xrightarrow{\mathrm{id}_\Gamma \otimes \llcorner f \lrcorner} \Gamma \otimes I \cong \Gamma$$



$$I \xrightarrow{[\![\pi]\!]} \Gamma \otimes X \otimes Y$$



$$I \xrightarrow{[\![\pi]\!]} \Gamma \otimes X_i \xrightarrow{\mathrm{id}_\Gamma \otimes q_i} \Gamma \otimes (X_0 \oplus X_1)$$

$$\overbrace{\Gamma \cdots X \qquad\qquad X^*}^{\pi}$$

cut

$$I \xrightarrow{[\![\pi]\!]} \Gamma \otimes A \otimes B \xrightarrow{\mathrm{id}_\Gamma \otimes \epsilon_X} \Gamma \otimes I \cong \Gamma$$

$$\overbrace{\Gamma_1 \cdots \Gamma_i}^{\pi_1} \qquad \overbrace{\Gamma_{i+1} \cdots \Gamma_n}^{\pi_2} \qquad I \cong I \otimes I \xrightarrow{[\![\pi_1]\!] \otimes [\![\pi_2]\!]} \Gamma_1 \otimes \cdots \otimes \Gamma_n$$

If proof-net π consists of the slices $\pi_1, \ldots, \pi_n$ then

$$[\![\pi]\!] = \sum_i [\![\pi_i]\!]$$

Soundness and Faithfulness

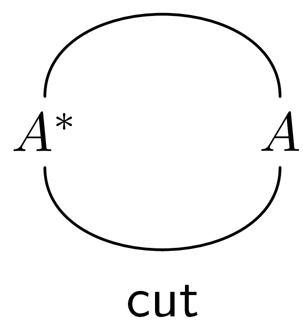
Theorem: Two proof-nets have the same denotation if and only if the have the same normal form.

Full Completeness

Theorem: For every arrow $f : A \to B$ in $F\mathcal{A}$ there is a proof-net π such that $[\![\pi]\!] = \ulcorner f \urcorner$.

Loops

The normal loop



has denotation $I \xrightarrow{\eta_A} A^* \otimes A \xrightarrow{\epsilon_{A^*}} I$

All closed loops denote scalars $I \to I$; hence normal slice denotes a state preparation and a scalar weight.

Any proof-net denotes formal linear combination of preparations; injection maps give a weighted *choice*.

Since we can choose the scalars, abstract "probabilities" can be calculated.

Example: Quantum Telephone Exchange

[Bose, Knight, Vedral]

- Alice and Bob wish to share an entangled pair.
- Initially they both share a pair with the telephone exchange (say that both of these are in the state $|00\rangle + |11\rangle$)
- The operator "connects" the two parties by applying a Bell state measurement.
- Alice and Bob now share an entangled pair.

We will model this in the logic generated by the qubit category $\mathcal{Q}$.

Quantum Telephone Exchange as a slice

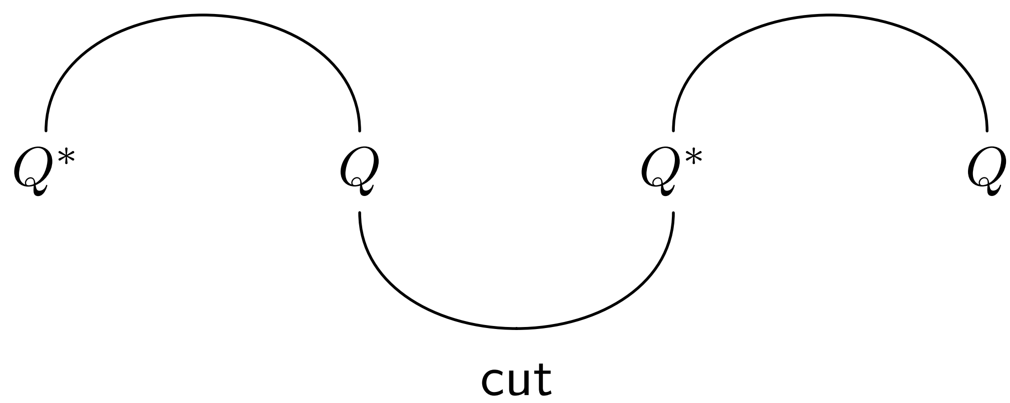
Syntax:

Semantics:

$$I \xrightarrow{\eta_Q \otimes \eta_Q} Q^* \otimes Q \otimes Q^* \otimes Q$$

Quantum Telephone Exchange as a slice

Syntax:

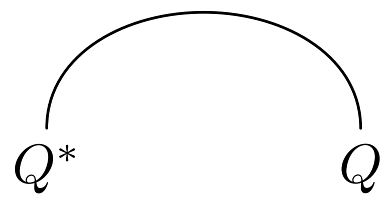


Semantics:

$$I \xrightarrow{\eta_Q \otimes \eta_Q} Q^* \otimes Q \otimes Q^* \otimes Q \xrightarrow{\mathrm{id} \otimes \epsilon_Q \otimes \mathrm{id}} Q^* \otimes Q$$

Quantum Telephone Exchange as a CCB

Syntax:

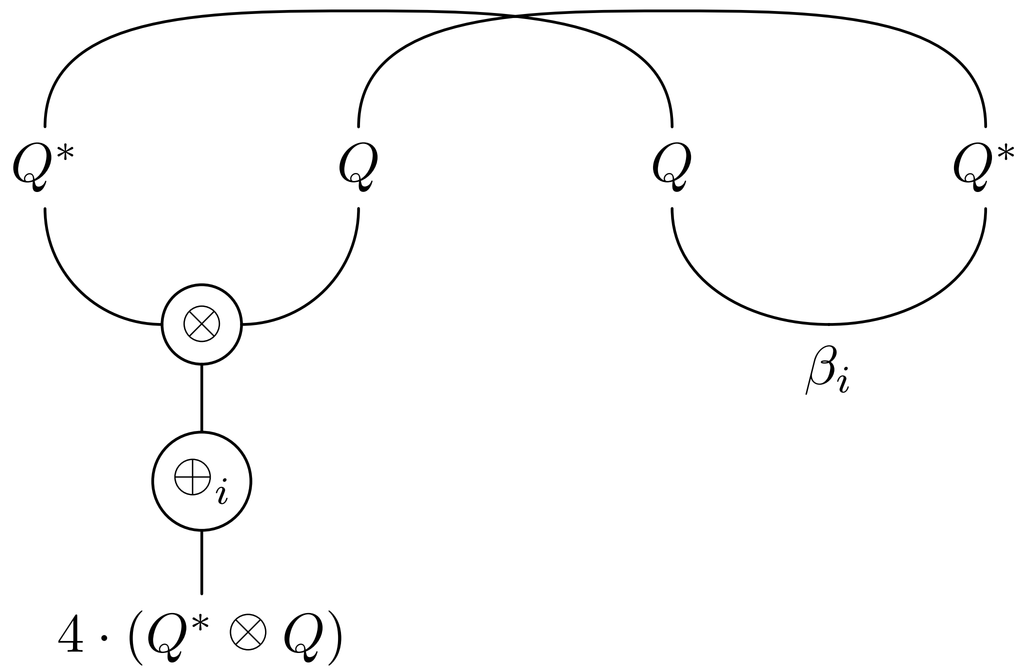


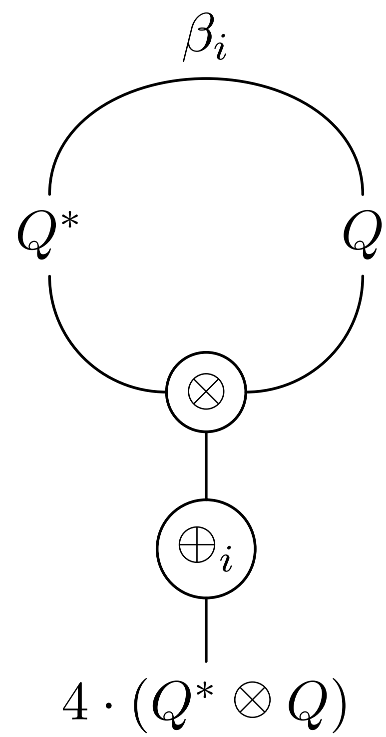
Semantics:

$$I \xrightarrow{\eta_Q} Q^* \otimes Q$$

Take 2: Quantum Telephone Exchange as a proof-net

Since we have 4 outcomes, we have distinct slices for $i = 1, 2, 3, 4$.




β_i
Q^*
Q
$\otimes$
$\oplus_i$
$4 \cdot (Q^* \otimes Q)$

Work in Progress

- Multipartite Entanglement — the free construction on a symmetric monoidal category.
- Local classical state — additive boxes
- Implementation work

Further Work

- A categorical presentation of the 1-Way model
- More precise models; spectra and orthogonality
- How much physics can we get from a free construction?