Mixed quantum states in higher categories

Linde Wester
Department of Computer Science, University of Oxford
(with Chris Heunen and Jamie Vicary)

June 6, 2014

Table of contents

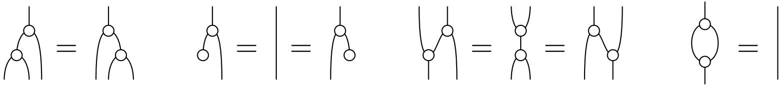
Existing models for classical and quantum data
- Special dagger Frobenius algebras
- 2-categorical quantum mechanics

The construction $2(-)$
- The theory of bimodules
- The $2(-)$ construction
- $2(\mathrm{CP}^*(-))$

Applications
- A unified description of teleportation and classical encryption
- A unified security proof

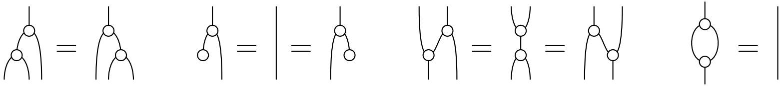
$\mathrm{CP}^*(-)$

1. Special dagger Frobenius algebras in a monoidal category **C**:

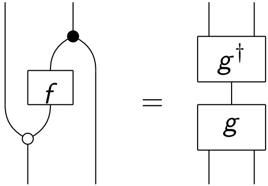


CP*(−)

1. Special dagger Frobenius algebras in a monoidal category **C**:



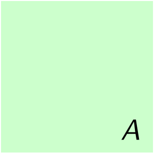
2. Completely positive maps between Frobenius algebras:
   morphisms f in **C**, for which $\exists g$ such that



2-categories and their graphical language

2-categories and their graphical language

0-cells Regions Classical information



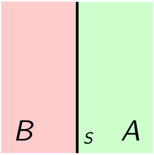
2-categories and their graphical language

0-cells	Regions	Classical information
1-cells	Lines	Quantum systems

$$B \xrightarrow[s]{} A$$

2-categories and their graphical language

0-cells	Regions	Classical information
1-cells	Lines	Quantum systems



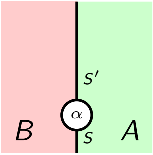
2-categories and their graphical language

0-cells	Regions	Classical information
1-cells	Lines	Quantum systems
2-cells	Vertices	Quantum dynamics

$$\begin{tikzcd} B \arrow[r, "s"'] \arrow[r, bend left=60, "s'"] \arrow[r, phantom, bend left=30, "\alpha\Uparrow"] & A \end{tikzcd}$$

2-categories and their graphical language

0-cells	Regions	Classical information
1-cells	Lines	Quantum systems
2-cells	Vertices	Quantum dynamics



2-categories and their graphical language

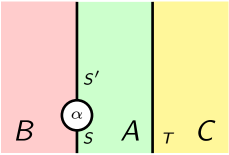
0-cells	Regions	Classical information
1-cells	Lines	Quantum systems
2-cells	Vertices	Quantum dynamics

Horizontal composition

$$\begin{tikzcd} B \arrow[r, bend left, "S'"] \arrow[r, "S"'] \arrow[r, phantom, "\alpha\Downarrow"] & A \arrow[r, "T"'] & C \end{tikzcd}$$

2-categories and their graphical language

0-cells	Regions	Classical information
1-cells	Lines	Quantum systems
2-cells	Vertices	Quantum dynamics
Horizontal composition		



2-categories and their graphical language

0-cells	Regions	Classical information
1-cells	Lines	Quantum systems
2-cells	Vertices	Quantum dynamics

Horizontal composition

Vertical composition

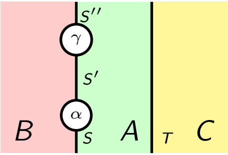
$$\begin{tikzcd}
B \arrow[r, "s"'] \arrow[r, bend left=60, "s'"{name=M}] \arrow[r, bend left=90, "s''"{name=U}] \arrow[r, phantom, bend left=30, "\Uparrow \alpha"] \arrow[r, phantom, bend left=75, "\Uparrow \gamma"] & A \arrow[r, "T"'] & C
\end{tikzcd}$$

2-categories and their graphical language

0-cells	Regions	Classical information
1-cells	Lines	Quantum systems
2-cells	Vertices	Quantum dynamics

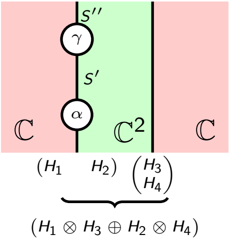
Horizontal composition

Vertical composition



2-categories and their graphical language

0-cells	Regions	Classical information
1-cells	Lines	Quantum systems
2-cells	Vertices	Quantum dynamics
Horizontal composition		
Vertical composition		



The standard example is **2Hilb**:

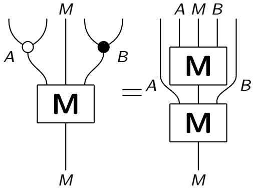
- *0-cells* given by natural numbers
- *1-cells* given by matrices of finite-dimensional Hilbert spaces
- *2-cells* given by matrices of linear maps

Quantum systems interacting with their environment

Quantum systems interacting with their environment

Let $(A, \text{mult}, \text{unit})$ and $(B, \text{mult}, \text{unit})$ be classical structures in $\mathbf{C}$.

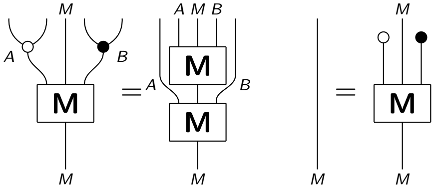
A *dagger C-D-bimodule* is a morphism $\mathbf{M}$ satisfying:



Quantum systems interacting with their environment

Let (A, ,) and (B, ,) be classical structures in **C**.

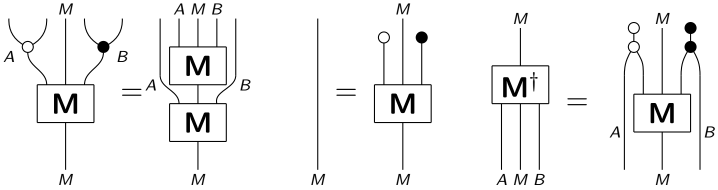
A *dagger C-D-bimodule* is a morphism **M** satisfying:



Quantum systems interacting with their environment

Let $(A, \text{(white comultiplication)}, \text{(white counit)})$ and $(B, \text{(black comultiplication)}, \text{(black counit)})$ be classical structures in $\mathbf{C}$.

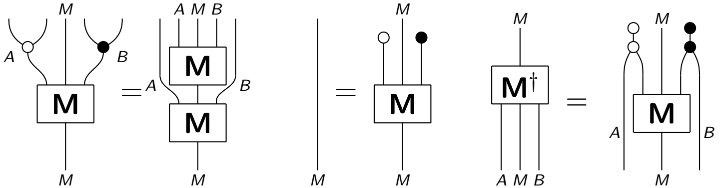
A *dagger C-D-bimodule* is a morphism $\mathbf{M}$ satisfying:



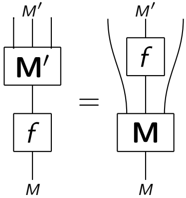
Quantum systems interacting with their environment

Let (A, , ) and (B, , ) be classical structures in $\mathbf{C}$.

A *dagger C-D-bimodule* is a morphism $\mathbf{M}$ satisfying:

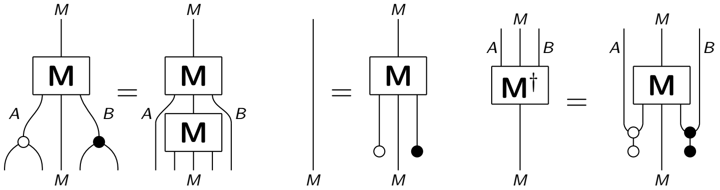


A bimodule homomorphism is a morphism $f \in \mathbf{C}$, such that

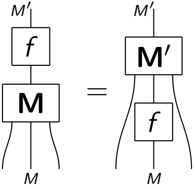


Quantum systems interacting with their environment

Let $(A, \;,\;)$ and $(B, \;,\;)$ be classical structures in $\mathbf{C}$.
A *dagger C-D-bimodule* is a morphism $\mathbf{M}$ satisfying:



A bimodule homomorphism is a morphism $f \in \mathbf{C}$, such that



The $2(-)$ construction

How can we construct the 2-category $2(\mathbf{C})$ from $\mathbf{C}$?

The $2(-)$ construction

How can we construct the 2-category $2(\mathbf{C})$ from $\mathbf{C}$?

- 0-cells: classical structures in $\mathbf{C}$

The $2(-)$ construction

How can we construct the 2-category $2(\mathbf{C})$ from $\mathbf{C}$?

- 0-cells: classical structures in $\mathbf{C}$
- 1-cells: bimodules of classical structures in $\mathbf{C}$

The $2(-)$ construction

How can we construct the 2-category $2(\mathbf{C})$ from $\mathbf{C}$?

- 0-cells: classical structures in $\mathbf{C}$
- 1-cells: bimodules of classical structures in $\mathbf{C}$
- 2-cells: module homomorphisms in $\mathbf{C}$

The $2(-)$ construction

How can we construct the 2-category $2(\mathbf{C})$ from $\mathbf{C}$?

- 0-cells: classical structures in $\mathbf{C}$
- 1-cells: bimodules of classical structures in $\mathbf{C}$
- 2-cells: module homomorphisms in $\mathbf{C}$

In representation theory: The orbifold completion of a monoidal category

The $2(-)$ construction

How can we construct the 2-category $2(\mathbf{C})$ from $\mathbf{C}$?

- 0-cells: classical structures in $\mathbf{C}$
- 1-cells: bimodules of classical structures in $\mathbf{C}$
- 2-cells: module homomorphisms in $\mathbf{C}$

In representation theory: The orbifold completion of a monoidal category

Some properties of $2(-)$ are:

The $2(-)$ construction

How can we construct the 2-category $2(\mathbf{C})$ from $\mathbf{C}$?

- 0-cells: classical structures in $\mathbf{C}$
- 1-cells: bimodules of classical structures in $\mathbf{C}$
- 2-cells: module homomorphisms in $\mathbf{C}$

In representation theory: The orbifold completion of a monoidal category

Some properties of $2(-)$ are:

- $2(\mathbf{C})$ is a 2-category.

The $2(-)$ construction

How can we construct the 2-category $2(\mathbf{C})$ from $\mathbf{C}$?

- 0-cells: classical structures in $\mathbf{C}$
- 1-cells: bimodules of classical structures in $\mathbf{C}$
- 2-cells: module homomorphisms in $\mathbf{C}$

In representation theory: The orbifold completion of a monoidal category

Some properties of $2(-)$ are:

- $2(\mathbf{C})$ is a 2-category.
- $2(-)$ preserves the dagger.

The $2(-)$ construction

How can we construct the 2-category $2(\mathbf{C})$ from $\mathbf{C}$?

- 0-cells: classical structures in $\mathbf{C}$
- 1-cells: bimodules of classical structures in $\mathbf{C}$
- 2-cells: module homomorphisms in $\mathbf{C}$

In representation theory: The orbifold completion of a monoidal category

Some properties of $2(-)$ are:

- $2(\mathbf{C})$ is a 2-category.
- $2(-)$ preserves the dagger.
- If $\mathbf{C}$ is compact, so is $2(\mathbf{C})$: 1-cells have ambidextrous duals.

The $2(-)$ construction

How can we construct the 2-category $2(\mathbf{C})$ from $\mathbf{C}$?

- 0-cells: classical structures in $\mathbf{C}$
- 1-cells: bimodules of classical structures in $\mathbf{C}$
- 2-cells: module homomorphisms in $\mathbf{C}$

In representation theory: The orbifold completion of a monoidal category

Some properties of $2(-)$ are:

- $2(\mathbf{C})$ is a 2-category.
- $2(-)$ preserves the dagger.
- If $\mathbf{C}$ is compact, so is $2(\mathbf{C})$: 1-cells have ambidextrous duals.
- If $\mathbf{C}$ has dagger biproducts, so do all hom-categories of $2(\mathbf{C})$.

The $2(-)$ construction

How can we construct the 2-category $2(\mathbf{C})$ from $\mathbf{C}$?

- 0-cells: classical structures in $\mathbf{C}$
- 1-cells: bimodules of classical structures in $\mathbf{C}$
- 2-cells: module homomorphisms in $\mathbf{C}$

In representation theory: The orbifold completion of a monoidal category

Some properties of $2(-)$ are:

- $2(\mathbf{C})$ is a 2-category.
- $2(-)$ preserves the dagger.
- If $\mathbf{C}$ is compact, so is $2(\mathbf{C})$: 1-cells have ambidextrous duals.
- If $\mathbf{C}$ has dagger biproducts, so do all hom-categories of $2(\mathbf{C})$.
- The subcategory of scalars of $2(\mathbf{C})$ corresponds to $\mathbf{C}$.

The $2(-)$ construction

How can we construct the 2-category $2(\mathbf{C})$ from $\mathbf{C}$?

- 0-cells: classical structures in $\mathbf{C}$
- 1-cells: bimodules of classical structures in $\mathbf{C}$
- 2-cells: module homomorphisms in $\mathbf{C}$

In representation theory: The orbifold completion of a monoidal category

Some properties of $2(-)$ are:

- $2(\mathbf{C})$ is a 2-category.
- $2(-)$ preserves the dagger.
- If $\mathbf{C}$ is compact, so is $2(\mathbf{C})$: 1-cells have ambidextrous duals.
- If $\mathbf{C}$ has dagger biproducts, so do all hom-categories of $2(\mathbf{C})$.
- The subcategory of scalars of $2(\mathbf{C})$ corresponds to $\mathbf{C}$.
- $2(\mathbf{FHilb})$ is isomorphic to the category $\mathbf{2Hilb}$.

The $2(-)$ construction

How can we construct the 2-category $2(\mathbf{C})$ from $\mathbf{C}$?

- 0-cells: classical structures in $\mathbf{C}$
- 1-cells: bimodules of classical structures in $\mathbf{C}$
- 2-cells: module homomorphisms in $\mathbf{C}$

In representation theory: The orbifold completion of a monoidal category

Some properties of $2(-)$ are:

- $2(\mathbf{C})$ is a 2-category.
- $2(-)$ preserves the dagger.
- If $\mathbf{C}$ is compact, so is $2(\mathbf{C})$: 1-cells have ambidextrous duals.
- If $\mathbf{C}$ has dagger biproducts, so do all hom-categories of $2(\mathbf{C})$.
- The subcategory of scalars of $2(\mathbf{C})$ corresponds to $\mathbf{C}$.
- $2(\mathbf{FHilb})$ is isomorphic to the category $\mathbf{2Hilb}$.

For proofs see LW (2013), Masters's thesis, 'Categorical Models for Quantum Computing'.

Horizontal composition in $2(-)$

Horizontal composition in $2(-)$

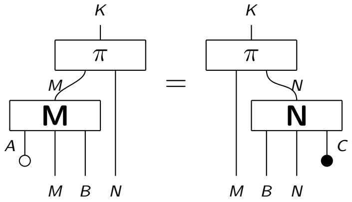
Horizontal composition is defined by the following coequaliser in **C**:

$$
\begin{tikzcd}
M \otimes B \otimes N \arrow[r, shift left, "\mathbf{M}_B \otimes id_N"] \arrow[r, shift right, "id_M \otimes {}_B\mathbf{N}"'] & M \otimes N \arrow[r, "\pi"] \arrow[dr, "f"'] & M \otimes_B N \arrow[d, dashed, "\tilde{f}"] \\
& & K
\end{tikzcd}
$$

Horizontal composition in $2(-)$

Horizontal composition is defined by the following coequaliser in $\mathbf{C}$:

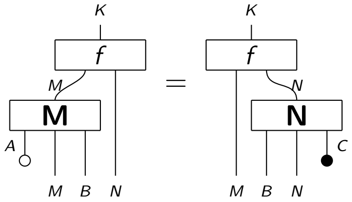
$$M \otimes B \otimes N \underset{id_M \otimes\ _B\mathbf{N}}{\overset{\mathbf{M}_B \otimes id_N}{\rightrightarrows}} M \otimes N \xrightarrow{\pi} M \otimes_B N$$



Horizontal composition in $2(-)$

Horizontal composition is defined by the following coequaliser in $\mathbf{C}$:

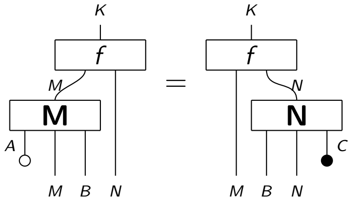
$$\begin{tikzcd}
M \otimes B \otimes N \arrow[r, shift left, "\mathbf{M}_B \otimes id_N"] \arrow[r, shift right, "id_M \otimes {}_B\mathbf{N}"'] & M \otimes N \arrow[r, "\pi"] \arrow[dr, "f"'] & M \otimes_B N \\
& & K
\end{tikzcd}$$



Horizontal composition in $2(-)$

Horizontal composition is defined by the following coequaliser in $\mathbf{C}$:

$$\begin{tikzcd} M \otimes B \otimes N \arrow[r, shift left, "\mathbf{M}_B \otimes id_N"] \arrow[r, shift right, "id_M \otimes {}_B\mathbf{N}"'] & M \otimes N \arrow[r, "\pi"] \arrow[dr, "f"'] & M \otimes_B N \arrow[d, dashed, "\tilde{f}"] \\ & & K \end{tikzcd}$$

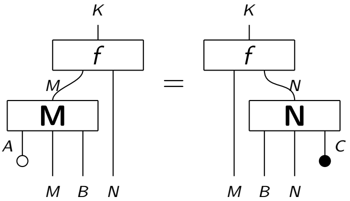


Can we find this module explicitly?

Horizontal composition in $2(-)$

Horizontal composition is defined by the following coequaliser in $\mathbf{C}$:

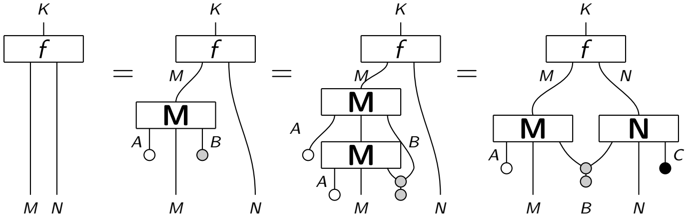
$$\begin{tikzcd}
M \otimes B \otimes N \arrow[r, shift left, "\mathbf{M}_B \otimes id_N"] \arrow[r, shift right, "id_M \otimes {}_B\mathbf{N}"'] & M \otimes N \arrow[r, "\pi"] \arrow[dr, "f"'] & M \otimes_B N \arrow[d, dashed, "\tilde{f}"] \\
 & & K
\end{tikzcd}$$



Can we find this module explicitly? Yes!

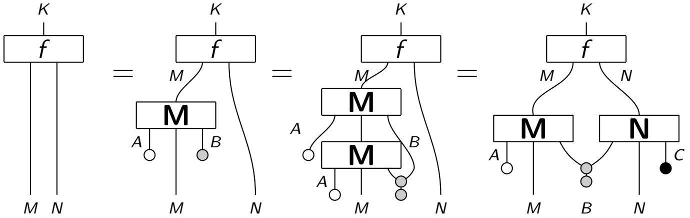
Horizontal composition in terms of dagger splittings

Any such f factorizes through **M**∘**N**:



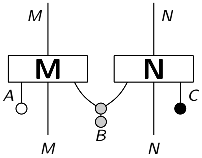
Horizontal composition in terms of dagger splittings

Any such f factorizes through **M**∘**N**:



Theorem

Finding the dagger coequaliser is equivalent to finding a dagger splitting of the following morphism:



$2(\mathrm{CP}^*(-))$

We would like to understand the 2-category '?'

$$\begin{tikzcd}
\textbf{FHilb} \arrow[r, "\mathrm{CP}^*(-)"] \arrow[d, "2(-)"'] & \mathrm{CP}^*(\textbf{FHilb}) \arrow[d, "2(-)"] \\
2(\textbf{FHilb}) \arrow[r, dashed, "\mathrm{CP}^*(-)"'] & ?
\end{tikzcd}$$

$2(\mathrm{CP}^*(-))$

We would like to understand the 2-category '?'

$$\begin{tikzcd}
\mathbf{FHilb} \arrow[r, "\mathrm{CP}^*(-)"] \arrow[d, "2(-)"'] & \mathrm{CP}^*(\mathbf{FHilb}) \arrow[d, "2(-)"] \\
2(\mathbf{FHilb}) \arrow[r, dashed, "\mathrm{CP}^*(-)"'] & ?
\end{tikzcd}$$

This is not obvious!

$2(\mathrm{CP}^*(-))$

We would like to understand the 2-category '?'

$$\begin{tikzcd}
\mathbf{FHilb} \arrow[r, "\mathrm{CP}^*(-)"] \arrow[d, "2(-)"'] & \mathrm{CP}^*(\mathbf{FHilb}) \arrow[d, "2(-)"] \\
2(\mathbf{FHilb}) \arrow[r, dashed, "\mathrm{CP}^*(-)"'] & ?
\end{tikzcd}$$

This is not obvious!

- This required a classification of classical structures in $\mathrm{CP}^*(\mathbf{FHilb})$.

$2(\mathrm{CP}^*(-))$

We would like to understand the 2-category '?'

$$\begin{tikzcd}
\textbf{FHilb} \arrow[r, "\mathrm{CP}^*(-)"] \arrow[d, "2(-)"'] & \mathrm{CP}^*(\textbf{FHilb}) \arrow[d, "2(-)"] \\
2(\textbf{FHilb}) \arrow[r, dashed, "\mathrm{CP}^*(-)"'] & ?
\end{tikzcd}$$

This is not obvious!

- This required a classification of classical structures in $\mathrm{CP}^*(\textbf{FHilb})$.
- There is a correspondence between special dagger Frobenius algebras on classical structures in **FHilb** and finite groupoids.

$2(\mathrm{CP}^*(-))$

We would like to understand the 2-category '?'

$$\begin{tikzcd}
\mathbf{FHilb} \arrow[r, "\mathrm{CP}^*(-)"] \arrow[d, "2(-)"'] & \mathrm{CP}^*(\mathbf{FHilb}) \arrow[d, "2(-)"] \\
2(\mathbf{FHilb}) \arrow[r, dashed, "\mathrm{CP}^*(-)"'] & ?
\end{tikzcd}$$

This is not obvious!

- This required a classification of classical structures in $\mathrm{CP}^*(\mathbf{FHilb})$.
- There is a correspondence between special dagger Frobenius algebras on classical structures in **FHilb** and finite groupoids.
- $\mathrm{CP}^*(\mathbf{FHilb})$ does not have all coequalisers.

Modelling POVM's

The following subcategory of $2(\mathrm{CP}^*(\textbf{FHilb}))$ is a sufficient model for modelling communication protocols:

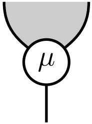
- 0-cells: natural numbers
- 1-cells: matrices of dagger Frobenius algebras
- 2-cells: matrices of completely positive maps

Modelling POVM's

The following subcategory of $2(\mathrm{CP}^*(\textbf{FHilb}))$ is a sufficient model for modelling communication protocols:

- 0-cells: natural numbers
- 1-cells: matrices of dagger Frobenius algebras
- 2-cells: matrices of completely positive maps

Measurements are defined as counit-preserving 2-cells of type:

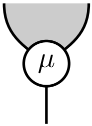


Modelling POVM's

The following subcategory of $2(\mathrm{CP}^*(\textbf{FHilb}))$ is a sufficient model for modelling communication protocols:

- 0-cells: natural numbers
- 1-cells: matrices of dagger Frobenius algebras
- 2-cells: matrices of completely positive maps

Measurements are defined as counit-preserving 2-cells of type:



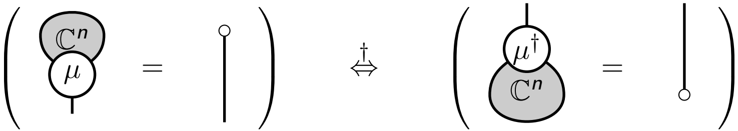
Theorem

Measurements on algebras $\mathbb{C}^n$ are exactly stochastic maps.
Measurements on algebras $B(H)$ are exactly POVMs.

Modelling POVM's

Proof.

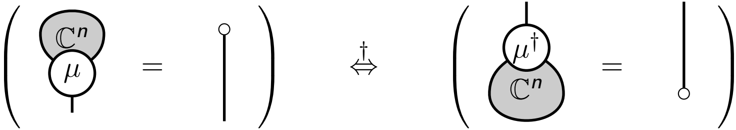
The counit preserving condition gives us



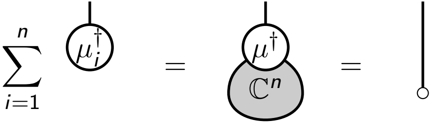
Modelling POVM's

Proof.

The counit preserving condition gives us



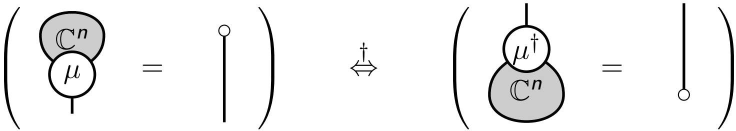
So we have the following equalities of positive elements:



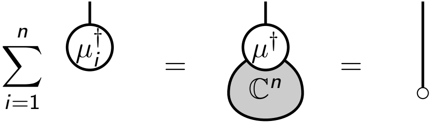
Modelling POVM's

Proof.

The counit preserving condition gives us



So we have the following equalities of positive elements:

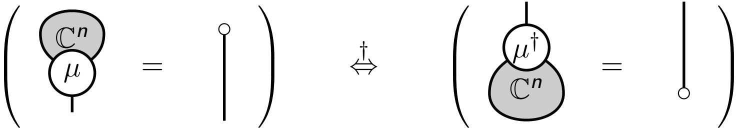


- On $\mathbb{C}^n$ this corresponds to a stochastic map

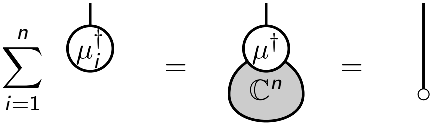
Modelling POVM's

Proof.

The counit preserving condition gives us



So we have the following equalities of positive elements:

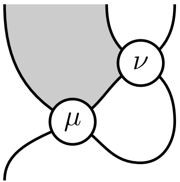


- On $\mathbb{C}^n$ this corresponds to a stochastic map
- On $B(\mathbb{C}^n)$ this corresponds to a POVM

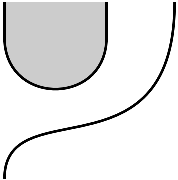
□

Classical encryption and quantum teleportation

Quantum teleportation and classical encryption are solutions to the following equation with μ a measurement and ν unitary 2-cell:

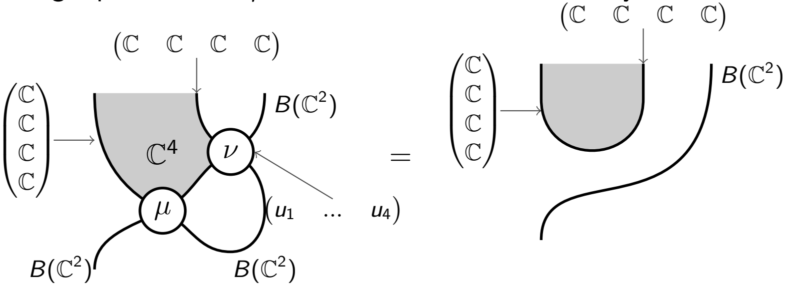


$$=$$



Classical encryption and quantum teleportation

Quantum teleportation and classical encryption are solutions to the following equation with μ a measurement and ν unitary 2-cell:

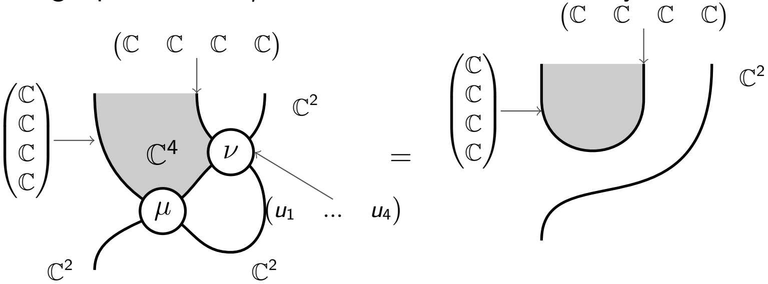


This equation corresponds to:

- quantum teleportation, if the input is a matrix algebra

Classical encryption and quantum teleportation

Quantum teleportation and classical encryption are solutions to the following equation with μ a measurement and ν unitary 2-cell:

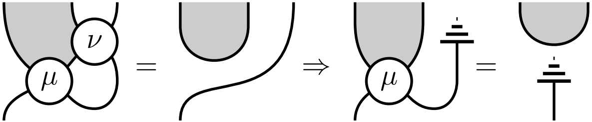


This equation corresponds to:

- quantum teleportation, if the input is a matrix algebra
- classical encryption, if the input is a classical structure

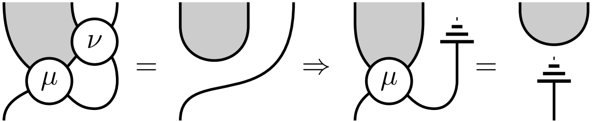
A unified security proof

When the output is destroyed, all information is lost:



A unified security proof

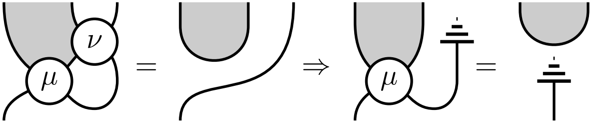
When the output is destroyed, all information is lost:



- We apply the trace map on both sides of the equation

A unified security proof

When the output is destroyed, all information is lost:



- We apply the trace map on both sides of the equation
- On the left-hand-side: ν is a family invertible completely positive maps, which are trace preserving.

So this give a unified security proof

Overview

The results:

Overview

The results:

- A categorical generalisation of **2Hilb**, based on modules:

Overview

The results:

- A categorical generalisation of **2Hilb**, based on modules: The construction $2(-)$, which preserves daggers, compactness, biproducts, such that the scalars of $2(\mathbf{C})$ correspond to $\mathbf{C}$.

Overview

The results:

- A categorical generalisation of **2Hilb**, based on modules: The construction $2(-)$, which preserves daggers, compactness, biproducts, such that the scalars of $2(\mathbf{C})$ correspond to $\mathbf{C}$.
- Horizontal composition in $2(\mathbf{C})$ is given by dagger splittings.

Overview

The results:

- A categorical generalisation of **2Hilb**, based on modules: The construction $2(-)$, which preserves daggers, compactness, biproducts, such that the scalars of $2(\mathbf{C})$ correspond to $\mathbf{C}$.
- Horizontal composition in $2(\mathbf{C})$ is given by dagger splittings.
- First steps in understanding $2(\mathrm{CP}^*(\mathbf{FHilb}))$.

Overview

The results:

- A categorical generalisation of **2Hilb**, based on modules: The construction $2(-)$, which preserves daggers, compactness, biproducts, such that the scalars of $2(\mathbf{C})$ correspond to $\mathbf{C}$.
- Horizontal composition in $2(\mathbf{C})$ is given by dagger splittings.
- First steps in understanding $2(\mathrm{CP}^*(\mathbf{FHilb}))$.
- $2(\mathbf{FHilb})$ contains a subcategory of classical structures, matrices of special dagger Frobenius algebras, and matrices of completely positive morphisms.

Overview

The results:

- A categorical generalisation of **2Hilb**, based on modules: The construction $2(-)$, which preserves daggers, compactness, biproducts, such that the scalars of $2(\mathbf{C})$ correspond to $\mathbf{C}$.
- Horizontal composition in $2(\mathbf{C})$ is given by dagger splittings.
- First steps in understanding $2(\mathrm{CP}^*(\mathbf{FHilb}))$.
- $2(\mathbf{FHilb})$ contains a subcategory of classical structures, matrices of special dagger Frobenius algebras, and matrices of completely positive morphisms.
- Unified description of teleportation and classical encryption.

Overview

The results:

- A categorical generalisation of **2Hilb**, based on modules: The construction $2(-)$, which preserves daggers, compactness, biproducts, such that the scalars of $2(\mathbf{C})$ correspond to $\mathbf{C}$.
- Horizontal composition in $2(\mathbf{C})$ is given by dagger splittings.
- First steps in understanding $2(\mathrm{CP}^*(\mathbf{FHilb}))$.
- $2(\mathbf{FHilb})$ contains a subcategory of classical structures, matrices of special dagger Frobenius algebras, and matrices of completely positive morphisms.
- Unified description of teleportation and classical encryption.
- Security proof of teleportation and classical encryption.

Overview

The results:

- A categorical generalisation of **2Hilb**, based on modules: The construction $2(-)$, which preserves daggers, compactness, biproducts, such that the scalars of $2(\mathbf{C})$ correspond to $\mathbf{C}$.
- Horizontal composition in $2(\mathbf{C})$ is given by dagger splittings.
- First steps in understanding $2(\mathrm{CP}^*(\mathbf{FHilb}))$.
- $2(\mathbf{FHilb})$ contains a subcategory of classical structures, matrices of special dagger Frobenius algebras, and matrices of completely positive morphisms.
- Unified description of teleportation and classical encryption.
- Security proof of teleportation and classical encryption.

Thank you!