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(CP*(−))

Applications
   A unified description of teleportation and classical encryption
   A unified security proof
1. Special dagger Frobenius algebras in a monoidal category $\mathbf{C}$:
1. Special dagger Frobenius algebras in a monoidal category $\mathbb{C}$:

2. Completely positive maps between Frobenius algebras: morphisms $f$ in $\mathbb{C}$, for which $\exists g$ such that
2-categories and their graphical language
2-categories and their graphical language

$0$-cells     Regions     Classical information

The standard example is $2\text{Hilb}$:

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

$A$
2-categories and their graphical language

<table>
<thead>
<tr>
<th>0-cells</th>
<th>Regions</th>
<th>Classical information</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-cells</td>
<td>Lines</td>
<td>Quantum systems</td>
</tr>
</tbody>
</table>

\[ B \xrightarrow{s} A \]
### 2-categories and their graphical language

<table>
<thead>
<tr>
<th>0-cells</th>
<th>Regions</th>
<th>Classical information</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-cells</td>
<td>Lines</td>
<td>Quantum systems</td>
</tr>
</tbody>
</table>

The standard example is $\text{2Hilb}$:

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

```
B
s
A
```
2-categories and their graphical language

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

The standard example is $2\text{Hilb}$:

- **0-cells**: given by natural numbers
- **1-cells**: given by matrices of finite-dimensional Hilbert spaces
- **2-cells**: given by matrices of linear maps
2-categories and their graphical language

\begin{itemize}
  \item \textit{0-cells}: Regions, Classical information
  \item \textit{1-cells}: Lines, Quantum systems
  \item \textit{2-cells}: Vertices, Quantum dynamics
\end{itemize}

The standard example is $2\text{Hilb}$:

\begin{itemize}
  \item \textit{0-cells}: given by natural numbers
  \item \textit{1-cells}: given by matrices of finite-dimensional Hilbert spaces
  \item \textit{2-cells}: given by matrices of linear maps
\end{itemize}
2-categories and their graphical language

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

Horizontal composition

\[ \begin{array}{ccc}
  B & \xleftarrow{\alpha} & A \\
  \downarrow{S} & & \downarrow{\alpha} \\
  & S' & \\
\end{array} \rightarrow & A & \rightarrow \ C
\]

The standard example is $\mathbf{2Hilb}$:

0-cells given by natural numbers
1-cells given by matrices of finite-dimensional Hilbert spaces
2-cells given by matrices of linear maps
2-categories and their graphical language

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

Horizontal composition

The standard example is $\mathbf{2Hilb}$:
- **0-cells** given by natural numbers
- **1-cells** given by matrices of finite-dimensional Hilbert spaces
- **2-cells** given by matrices of linear maps
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 $\mathbf{2Hilb}$:

- **0-cells**: given by natural numbers
- **1-cells**: given by matrices of finite-dimensional Hilbert spaces
- **2-cells**: given by matrices of linear maps
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 $\mathbf{2Hilb}$:

- **0-cells**: Given by natural numbers
- **1-cells**: Given by matrices of finite-dimensional Hilbert spaces
- **2-cells**: Given by matrices of linear maps
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 $\mathbf{2Hilb}$:

- **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 \((A, \bigodot, \bigotimes)\) and \((B, \bigodot, \bigotimes)\) be classical structures in \(\mathbf{C}\).

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

\[
M \circ M \circ A \circ M \circ B = M \circ A \circ B \circ M \\
M \circ M \circ A \circ M = M \circ A \circ B \circ M
\]
Quantum systems interacting with their environment

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

A dagger \(C-D\)-bimodule is a morphism \(M\) satisfying:

\[
M = M A M B B M M = M A M B B M M = M A M B B M M = M A bimodule homomorphism is a morphism \(f \in \mathbf{C}\), such that
\]

\[
M' M M = f M' M M = f M' M M
\]
Quantum systems interacting with their environment

Let \((A, \triangleleft, \triangleright)\) and \((B, \triangledown, \blacklozenge)\) be classical structures in \(\mathbf{C}\).

A \textit{dagger} \(C-D\)-\textit{bimodule} is a morphism \(M\) satisfying:

\[
M = M A M B B M A M = M M A M A M B B M M = M A bimodule \text{ homomorphism is a morphism } f \in \mathbf{C}, \text{ such that } M' = f M M M = f M'
\]
Quantum systems interacting with their environment

Let \((A, \bigodot, \circ)\) and \((B, \bigotimes, \bullet)\) be classical structures in \(\mathcal{C}\).

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

\[
M \cdot M = A \cdot B = M \cdot M \cdot A \cdot B = \text{M}^\dagger
\]

A bimodule homomorphism is a morphism \(f \in \mathcal{C}\), such that:

\[
M' \cdot f = f \cdot M
\]
Quantum systems interacting with their environment

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

\[
M \circ M = M \circ M = M = M^\dagger \circ A \circ B = A \circ B
\]

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

\[
M' \circ f = M' \circ f
\]
The 2(−) construction

How can we construct the 2-category 2(\mathcal{C}) from \mathcal{C}?
The $2(\cdot)$ construction

How can we construct the 2-category $2(C)$ from $C$?

- 0-cells: classical structures in $C$

Some properties of $2(\cdot)$ are:

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

For proofs see LW (2013), Masters's thesis, 'Categorical Models for Quantum Computing'.
The 2(–) construction

How can we construct the 2-category $2(C)$ from $C$?

- 0-cells: classical structures in $C$
- 1-cells: bimodules of classical structures in $C$

Some properties of $2(–)$ are:

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

For proofs see LW (2013), Masters's thesis, 'Categorical Models for Quantum Computing'.
The $2(\_\_\_)$ construction

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

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

In representation theory: The orbifold completion of a monoidal category

Some properties of $2(\_\_\_)$ are:

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

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

The 2(−) construction

How can we construct the 2-category 2(C) from C?

- 0-cells: classical structures in C
- 1-cells: bimodules of classical structures in C
- 2-cells: module homomorphisms in C

In representation theory: The orbifold completion of a monoidal category
The $2(-)$ construction

How can we construct the 2-category $2(C)$ from $C$?

- 0-cells: classical structures in $C$
- 1-cells: bimodules of classical structures in $C$
- 2-cells: module homomorphisms in $C$

*In representation theory: The orbifold completion of a monoidal category*

Some properties of $2(-)$ are:

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

The $2(\cdot)$ construction

How can we construct the 2-category $2(C)$ from $C$?

- 0-cells: classical structures in $C$
- 1-cells: bimodules of classical structures in $C$
- 2-cells: module homomorphisms in $C$

In representation theory: The orbifold completion of a monoidal category

Some properties of $2(\cdot)$ are:

- $2(C)$ 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 $2(C)$ from $C$?

- 0-cells: classical structures in $C$
- 1-cells: bimodules of classical structures in $C$
- 2-cells: module homomorphisms in $C$

*In representation theory: The orbifold completion of a monoidal category*

Some properties of $2(-)$ are:

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


The 2(−) construction

How can we construct the 2-category 2(C) from C?

▶ 0-cells: classical structures in C
▶ 1-cells: bimodules of classical structures in C
▶ 2-cells: module homomorphisms in C

In representation theory: The orbifold completion of a monoidal category

Some properties of 2(−) are:

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

The $2(\cdot)$ construction

How can we construct the 2-category $2(C)$ from $C$?

- 0-cells: classical structures in $C$
- 1-cells: bimodules of classical structures in $C$
- 2-cells: module homomorphisms in $C$

In representation theory: The orbifold completion of a monoidal category

Some properties of $2(\cdot)$ are:

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

Horizontal composition in $2(-)$
Horizontal composition in $2(-)$

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

$$
\begin{array}{c}
M \otimes B \otimes N \\
\downarrow M_B \otimes \text{id}_N \\
\downarrow \text{id}_M \otimes BN
\end{array}
\rightarrow
\begin{array}{c}
M \otimes N \\
\downarrow \pi
\end{array}
\rightarrow
\begin{array}{c}
M \otimes_B N \\
\downarrow f
\end{array}
\rightarrow
\begin{array}{c}
K \\
\downarrow \tilde{f}
\end{array}
$$

Can we find this module explicitly? Yes!
Horizontal composition in 2(−)

Horizontal composition is defined by the following coequaliser in C:

\[
M \otimes B \otimes N \xrightarrow{M_B \otimes id_N} M \otimes N \xrightarrow{\pi} M \otimes_B N
\]

\[
\text{Can we find this module explicitly? Yes!}
\]
Horizontal composition in 2(−)

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

$$M \otimes B \otimes N \xrightarrow{M_B \otimes id_N} M \otimes N \xrightarrow{\pi} M \otimes_B N$$

Can we find this module explicitly?

Yes!
Horizontal composition in $\mathbb{2}(-)$

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

$$
\begin{align*}
M \otimes B \otimes N & \xrightarrow{M_B \otimes id_N} M \otimes N \\
& \xrightarrow{id_M \otimes B N} M \otimes B N
\end{align*}
$$

Can we find this module explicitly?

\[ f \]

\[ \tilde{f} \]

\[ K \]
Horizontal composition in $2(\rightarrow)$

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

$$M \otimes B \otimes N \xrightarrow{\begin{array}{c} M_B \otimes id_N \\ id_M \otimes B \otimes N \end{array}} M \otimes N \xrightarrow{\pi} M \otimes_B N$$

Can we find this module explicitly? Yes!
Horizontal composition in terms of dagger splittings

Any such $f$ factorizes through $\mathbf{M} \circ \mathbf{N}$:

$$f : \mathbf{K} \to \mathbf{M} \circ \mathbf{N} \circ \mathbf{K}$$

Thus, finding the dagger coequaliser is equivalent to finding a dagger splitting of the following morphism:
Horizontal composition in terms of dagger splittings

Any such \( f \) factorizes through \( \textbf{M} \circ \textbf{N} \):

\[
\begin{align*}
\text{Theorem} \\
\text{Finding the dagger coequaliser is equivalent to finding a dagger splitting of the following morphism:}
\end{align*}
\]
We would like to understand the 2-category $\mathcal{2}(\mathbb{C}P^*(-))$.

This is not obvious!

▶ This required a classification of classical structures in $\mathbb{C}P^*(\mathcal{F}

There is a correspondence between special dagger Frobenius algebras on classical structures in $\mathcal{F}$ and finite groupoids.

$\mathcal{2}(\mathbb{C}P^*(\mathcal{F})$ does not have all coequalisers.
We would like to understand the 2-category $\mathcal{C}$?

This is not obvious!
We would like to understand the 2-category $\mathcal{F}\text{Hilb}$. This is not obvious!

This required a classification of classical structures in $\text{CP}^*(\mathcal{F}\text{Hilb})$. There is a correspondence between special dagger Frobenius algebras on classical structures in $\mathcal{F}\text{Hilb}$ and finite groupoids. $\text{CP}^*(\mathcal{F}\text{Hilb})$ does not have all coequalisers.
We would like to understand the 2-category $\mathcal{2}(\text{CP}^*(-))$.

This is not obvious!

- This required a classification of classical structures in $\text{CP}^*(\text{FHilb})$.
- There is a correspondence between special dagger Frobenius algebras on classical structures in $\text{FHilb}$ and finite groupoids.
We would like to understand the 2-category $\mathbb{2}(\text{CP}^*(-))$

\[
\begin{array}{c}
\text{FHilb} \xrightarrow{\text{CP}^*(-)} \text{CP}^*(\text{FHilb}) \\
\downarrow 2(-) \quad \downarrow 2(-) \\
\text{2(FHilb)} \quad \rightarrow \quad \rightarrow \text{?} \\
\downarrow \quad \downarrow \\
\text{CP}^*(-) \quad \text{CP}^*(-)
\end{array}
\]

This is not obvious!

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

The following subcategory of $2(\text{CP}^*(\text{FHilb}))$ 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: $\mu$

Theorem

Measurements on algebras $C_n$ are exactly stochastic maps.

Measurements on algebras $B(H)$ are exactly POVMs.
Modelling POVM’s

The following subcategory of $2(\text{CP}^*(\text{FHilb}))$ 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:

\[
\mu
\]
Modelling POVM’s

The following subcategory of \(2(\text{CP}^*(\text{FHilb}))\) 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:

\[
\begin{array}{c}
\mu \\
\end{array}
\]

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

\[
\begin{pmatrix}
\mathcal{C}^n \\
\mu
\end{pmatrix}
= \quad
\begin{pmatrix}
\bullet
\end{pmatrix}
\quad \iff \quad
\begin{pmatrix}
\mu^{\dagger}
\end{pmatrix}
= \quad
\begin{pmatrix}
\mathcal{C}^n
\end{pmatrix}
\]

So we have the following equalities of positive elements:

\[
\sum_{i=1}^{n} \mu_{i}^{\dagger} = \mu^{\dagger} \quad \text{on} \quad \mathcal{C}^n
\]

On \( \mathcal{B}(\mathcal{C}^n) \) this corresponds to a POVM.
Modelling POVM’s

Proof.

The counit preserving condition gives us

\[
\begin{pmatrix}
\mathbb{C}^n \\
\mu
\end{pmatrix}
\begin{pmatrix}
\mathbb{C}^n \\
\mu^\dagger
\end{pmatrix}
= 
\begin{pmatrix}
\mathbb{C}^n \\
\mu^\dagger
\end{pmatrix}
\begin{pmatrix}
\mathbb{C}^n \\
\mu
\end{pmatrix}
\]

\[
\iff
\]

So we have the following equalities of positive elements:

\[
\sum_{i=1}^{n} \mu_i \mu_i^\dagger = \mu \mu^\dagger = 1
\]
Modelling POVM’s

Proof.

The counit preserving condition gives us

\[
\begin{pmatrix}
\mu \\
C^n
\end{pmatrix} \Rightarrow \begin{pmatrix}
\mu^\dagger \\
C^n
\end{pmatrix}
\]

So we have the following equalities of positive elements:

\[
\sum_{i=1}^{n} \mu_i^\dagger = \mu^\dagger = \mu^\dagger_{C^n}
\]

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

Proof.

The counit preserving condition gives us

\[ \left( \begin{array}{c} \mathbb{C}^n \\ \mu \end{array} \right) \begin{array}{c} = \\ \Leftrightarrow \end{array} \left( \begin{array}{c} \mu^\dagger \\ \mathbb{C}^n \end{array} \right) \]

So we have the following equalities of positive elements:

\[ \sum_{i=1}^{n} \mu_i^\dagger = \mu^\dagger \]

- On \( \mathbb{C}^n \) this corresponds to a stochastic map
- On \( B(\mathbb{C}^n) \) this corresponds to a POVM
Quantum teleportation and classical encryption are solutions to the following equation with $\mu$ a measurement and $\nu$ unitary 2-cell:
Quantum teleportation and classical encryption are solutions to the following equation with $\mu$ a measurement and $\nu$ unitary 2-cell:

$$\begin{pmatrix} C & C & C & C \\ C & C & C & C \\ C & C & C & C \\ C & C & C & C \end{pmatrix} \xrightarrow{\mu} B(\mathbb{C}^2) \xrightarrow{\nu} \begin{pmatrix} C \\ C \\ C \\ C \end{pmatrix} \quad = \quad \begin{pmatrix} C \\ C \\ C \\ C \end{pmatrix} \xrightarrow{\nu} B(\mathbb{C}^2) \xrightarrow{\mu} \begin{pmatrix} C & C & C & C \end{pmatrix}$$

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 $\mu$ a measurement and $\nu$ unitary 2-cell:

$$\begin{pmatrix} C & C & C & C \\ C & C & C & C \\ C & C & C & C \\ C & C & C & C \end{pmatrix} \times \begin{pmatrix} u_1 \\ \vdots \\ u_4 \end{pmatrix} = \begin{pmatrix} C \\ C \\ C \\ C \end{pmatrix}$$

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:

\[
\mu \nu = \mu = \mu
\]

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

On the left-hand-side, \( \nu \) is a family invertible completely positive maps, which are trace preserving. So this gives a unified security proof.
A unified security proof

When the output is destroyed, all information is lost:

\[ \mu \nu = \Rightarrow \mu = \]

- We apply the trace map on both sides of the equation
A unified security proof

When the output is destroyed, all information is lost:

\[ \mu \nu = \mu = \cdot \]

- We apply the trace map on both sides of the equation.
- On the left-hand-side: \( \nu \) 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 $2\text{Hilb}$, based on modules:

- Horizontal composition in $2(C)$ is given by dagger splittings.

- First steps in understanding $2(\text{CP}^*(\text{FHilb}))$.

- $2(\text{FHilb})$ 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!
Overview

The results:

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

- Horizontal composition in $2(C)$ is given by dagger splittings.

- First steps in understanding $2(\text{CP}^*(\text{FHilb}))$.

- $2(\text{FHilb})$ 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!
Overview

The results:

- A categorical generalisation of $2\text{Hilb}$, based on modules:
  The construction $2(\dashv)$, 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 $2(\mathbf{CP}^\star(\mathbf{FHilb}))$.

- $2(\mathbf{FHilb})$ 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!
Overview

The results:

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

The results:

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

- Horizontal composition in $2(C)$ is given by dagger splittings.

- First steps in understanding $2(CP^*(FHilb))$.

- $2(FHilb)$ contains a subcategory of classical structures, matrices of special dagger Frobenius algebras, and matrices of completely positive morphisms.

Thank you!
Overview

The results:

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