On Categorical Characterisations of No-signaling Theories

Mariami Gachechiladze

University of Oxford University of Siegen

MSc Thesis supervised by Dr. Chris Heunen
Department of Computer Science

March 9, 2015

Agenda

- Category theory essentials;
- Categorical quantum mechnichs; Diagrams;
- Teleportation using graphical calculus;
- No-cloning theorem using graphical calculus;
- Kinematic independence of observables $\Leftrightarrow$ No-signaling using graphical calculus.

Category Theory Essentials

Definition – Category Theory

A category $\mathcal{C}$ consists of:

- a collection $Ob(\mathcal{C})$ of objects;
- for every two objects A, B a collection $\mathcal{C}(A, B)$ of morphisms;
- for every two morphisms $f \in \mathcal{C}(A, B)$ and $g \in \mathcal{C}(B, C)$, a morphism $g \circ f \in \mathcal{C}(A, C)$;
- for every object A a morphism $id_A \in \mathcal{C}(A, A)$.

These must satisfy the following properties, for all objects A, B, C, D, and all morphisms $f \in \mathcal{C}(A, B)$, $g \in \mathcal{C}(B, C)$, $h \in \mathcal{C}(C, D)$:

- associativity: $h \circ (g \circ f) = (h \circ g) \circ f$;
- identity: $id_B \circ f = f = f \circ id_A$.

Functors; Natural Transformations - Category Theory

Don't just look at the objects; take the morphisms into account too.

A *functor* is a morphisms between two categories:
$F : \mathcal{C} \to \mathcal{D}$ assigns an object FA of $\mathcal{D}$ to every object A in $\mathcal{C}$ and $Ff : FA \to FB$ to every morphism $f : A \to B$.
Identity and composition is preserved:

$$F(g \circ f) = Fg \circ Ff, \qquad Fid_A = id_{FA}$$

Categories were only introduced to allow functors to be defined; functors were only introduced to allow natural transformations to be defined.

Additional Structure : Monoidal Categories

A monoidal category is a category $\mathcal{C}$ equipped with the following data, satisfying the property of coherence:

- a functor $\otimes : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$, called tensor product;
- and object $I \in \mathcal{C}$, called the unit object;
- a natural transformation whose components $(A \otimes B) \otimes C \underset{\alpha_{A,B,C}}{\longrightarrow} A \otimes (B \otimes C)$ are called associators;
- a natural isomorphism whose components $I \otimes A \underset{\lambda_A}{\longrightarrow} A$ are called a left unitors;
- a natural isomorphism whose components $A \otimes I \underset{\rho_A}{\longrightarrow} A$ are called right unitors;

Example - Category of Hilbert Spaces

The monoidal category of Hilbert spaces – **Hilb** is defined in the following way:

- **Objects** are Hilbert spaces;
- **Morphisms** are bounded linear maps $f, g, h \ldots$;
- **Compositions** is composition of linear maps;
- **Tensor product** $\otimes$: **Hilb** $\times$ **Hilb** $\to$ **Hilb** is a tensor product of Hilbert spaces
- **The unit object** I is the one-dimensional Hilbert space $\mathbb{C}$;
- **Associators** $\alpha_{H,J,K}$:$(H \otimes J) \otimes K \to H \otimes (J \otimes K)$ are unique linear maps satisfying $|\phi\rangle \otimes (|\chi\rangle \otimes |\psi\rangle) \mapsto (|\phi\rangle \otimes |\chi\rangle) \otimes |\psi\rangle$;
- **Left unitors** $\lambda_H : \mathbb{C} \otimes H \to H$ –unique lin. maps $1 \otimes |\phi\rangle \mapsto |\phi\rangle$;
- **Right unitors** $\rho_H : H \otimes \mathbb{C} \to H$ –unique lin. maps $|\phi\rangle \otimes 1 \mapsto |\phi\rangle$

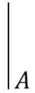
Example - Category of Sets and Relations

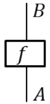
The monoidal category of Sets – **Rel** is defined in the following way:

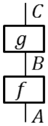
- **Objects** sets;
- **Morphisms** are $A \to B$ are relations
- **Compositions** are composition of linear maps of two relations $A \to B$ and $B \to C$;
- **Identity morphisms** $id : A \to A$ are relations $\{(a, a)|a \in A \subset A \times A\}$;
- **Tensor product** $\times$:
  is an usual cartesian product of sets.
- **The unit object** is a chosen 1-element set .

Categorical Quantum Mechanics & Diagrammatic Representation

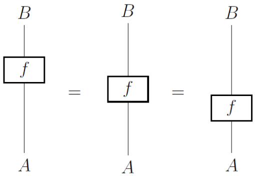
Graphical Calculus – Categorical Quantum Mechanics



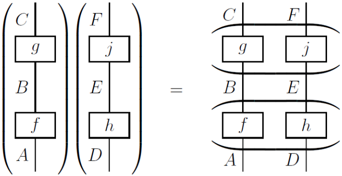




Object A: Morphism $f : A \to B$ Composition: $g \circ f : A \to B \to C$

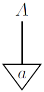


$f \circ id_A = f = id_B \circ f$

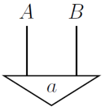


Interchange Law

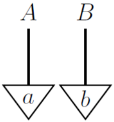
Graphical Calculus – Categorical Quantum Mechanics



State: $I \to A$



$I \to A \otimes B$



A joint state is a product state if

$$I \xrightarrow{\lambda_I^{-1}} I \otimes I \xrightarrow{a \otimes b} A \otimes B$$

An entangled state is a joint state which is not a product state. This state represents the preparation of $A \otimes B$ which cannot be decomposed as the separate preparation of A alongside with B.

Graphical Calculus – Categorical Quantum Mechanics

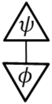
Where is an inner product?

Inner product gets encapsulated in the dagger monoidal category with the power of adjoints:

$\mathbb{C} \xrightarrow{\phi,\psi} H$

$$(\mathbb{C} \xrightarrow{\phi} H \xrightarrow{\psi^\dagger} \mathbb{C}) = \psi^\dagger(\phi(1)) = \left\langle 1 | \psi^\dagger(\phi(1)) \right\rangle = \langle \psi | \phi \rangle$$

which can be represented in the diagrammatic language in the following way:



$= \langle \psi | \phi \rangle$

Snake Equations

We draw an object L as a wire with an upward-pointing arrow, and a right dual R as a wire with a downward-pointing arrow.

The unit $I \xrightarrow{\eta} R \otimes L$ and counit $L \otimes R \xrightarrow{\varepsilon} I$ are then drawn as bent wires:

The duality equations then take the following graphical form:

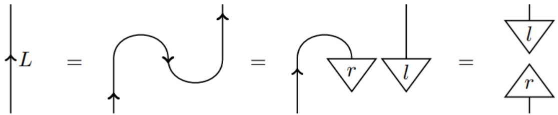
Entanglement

Our Claim: Dual objects in a monoidal category provide a categorical way to model entanglement of a pair of systems in an abstract way.

Given the dual objects $L \dashv R$, the entangled state is an unit $I \xrightarrow{\eta} R \otimes L$. And the corresponding unit is an entanglement effect $L \otimes R \xrightarrow{\varepsilon} I$.

Lemma *Let $L \dashv R$ be dual objects in a symmetric monoidal category. If the unit $I \xrightarrow{\eta} R \otimes L$ is a product state, then id_L and id_R factor through the monoidal unit object I.*

Proof. Suppose that η is the morphism $I \xrightarrow{\lambda_i^{-1}} I \otimes I \xrightarrow{r \otimes l} R \otimes L$. Then



A similar argument holds for id_R. □

Teleportation Using Graphical Calculus

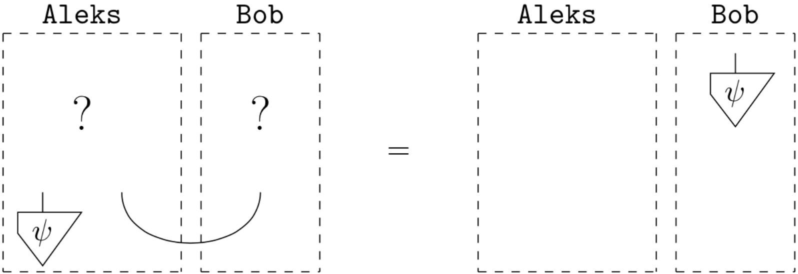
Teleportation using an "Orthodox" formalism

Alice and Bob share an entangled state: $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}[|00\rangle + |11\rangle]$.
Alice has an unknown state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ and using some local transformations and classical communication of two bits, she needs $|\psi\rangle$ to Bob.

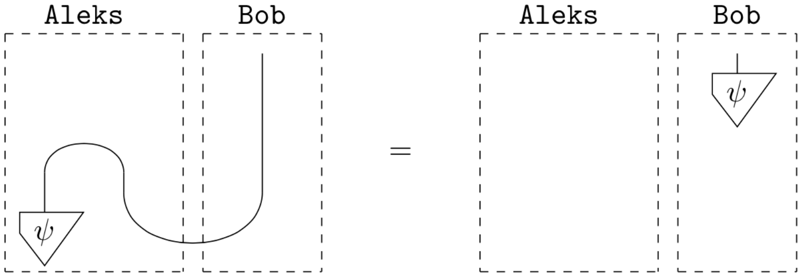
$$|\psi_0\rangle|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(\alpha(|0\rangle|00\rangle + |0\rangle|11\rangle) + \beta(|1\rangle|00\rangle + |1\rangle|11\rangle)$$

1. Alice applies the CNOT gate:
$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(\alpha(|0\rangle|00\rangle + |0\rangle|11\rangle) + \beta(|1\rangle|10\rangle + |1\rangle|01\rangle)$$
2. Alice applies Hadamard operation to the rist qubit and gets:
$$|\psi_2\rangle = \frac{1}{2}[|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle)$$
$$+|10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)]$$

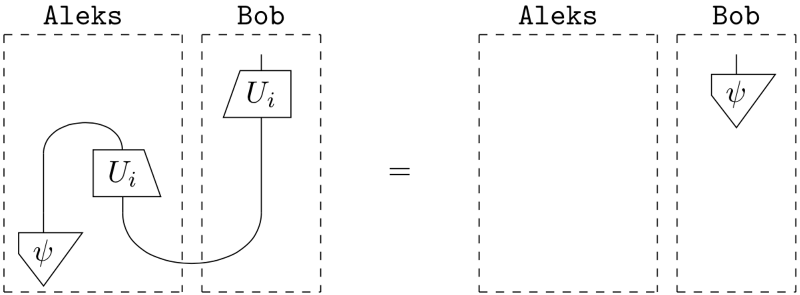
Teleportation using Graphical Calculus



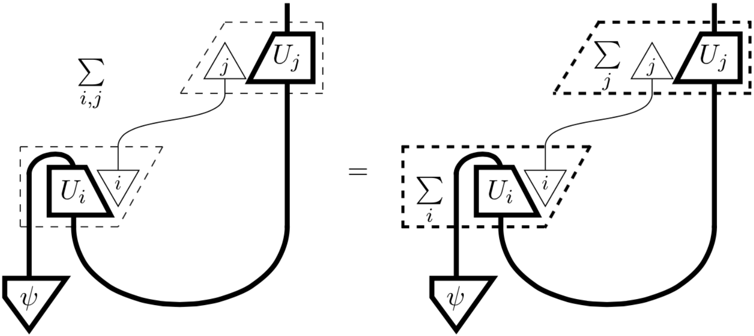
Teleportation using Graphical Calculus



Teleportation using Graphical Calculus



Teleportation using Graphical Calculus

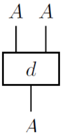


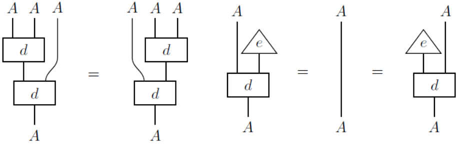
No-Cloning Theorem Using Graphical Calculus

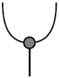
Monoid and Comonoid Structures

Comonoids

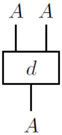
Clearly, copying should be an operation of type $A \xrightarrow{d} A \otimes A$. We draw it in the following way:



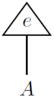


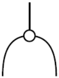


instead of

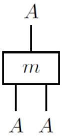


instead of

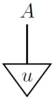




instead of

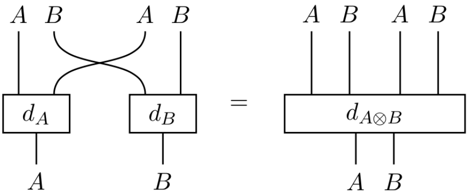


instead of



No Uniform Copying!

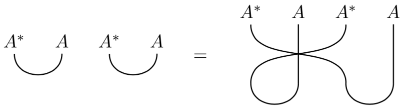
If a symmetric monoidal category has uniform copying, then the following diagram must commute:



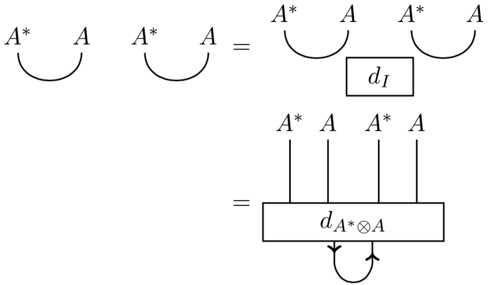
This turns out to be a drastic restriction on the category, as we will see in the Copying collapse theorem below. First we need some preparatory lemmas.

No Uniform Copying

Lemma 1. If a compact category has uniform copying, then



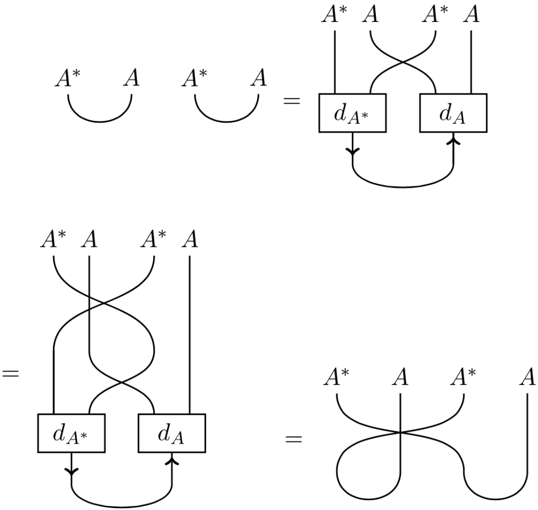
Proof.



(because $d_I = \rho_I$)

(by naturality of d)

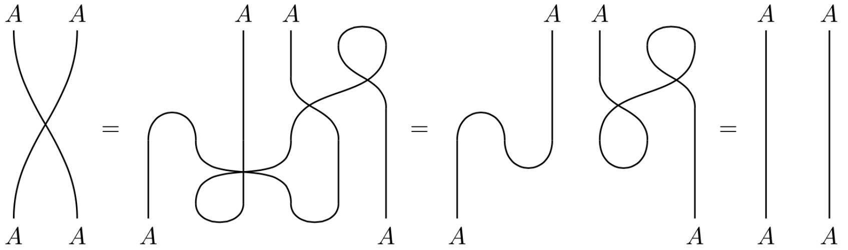
No Uniform Copying – Proof Continued



No Uniform Copying

Lemma 2. If a compact category has uniform copying, then $\sigma_{A,A} = id_{A \otimes A}$.

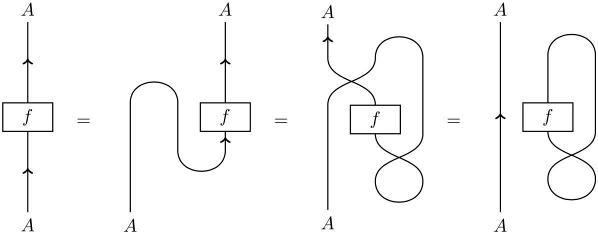
Proof.



Copy Collapses

Theorem If a compact category has uniform copying, then every f endomorphism is a scalar multiple of the identity.

Proof.



Thus, if a compact category has uniform copying, all endo-homsets are 1-dimensional, in the sense that they are in bijection with the scalars. Hence, in this sense, all objects are 1-dimensional, and the category degenerates.

Categorical Characterisations of No-signaling Theories
Supervisor: Dr. Chris Heunen

Can Quantum Theory be reduced to Information Theoretic Constraints?

The theory is quantum if and only if the following information-theoretic constraints are satisfied:

1. No superluminal information transmission between two distinct systems by acting with a measurement operator on one of them.
2. No broadcasting of the information contained in an unknown state.
3. No unconditionally secure bit commitment.

Can Quantum Theory be reduced to Information Theoretic Constraints?

The previous constraints are equivalent to ones here in **FHilb**:
(a) If $\mathcal{A}$ and $\mathcal{B}$ are distinct physical systems, then the observables of $\mathcal{A}$ commute with those of $\mathcal{B}$.
(b)The observables of an individual system do not all commute with each other.
(c) There are physically realizable nonlocal entangled states.

Banach Algebras and C*-algebras

If a linear associate algebra over the complex field $\mathbb{C}$, A has a norm and is closed, it is called a **Banach** algebra.
We can now define an involution map on an algebra A: $* : A \to A$, which $a \mapsto a^*$, where $a, a^* \in A$ and

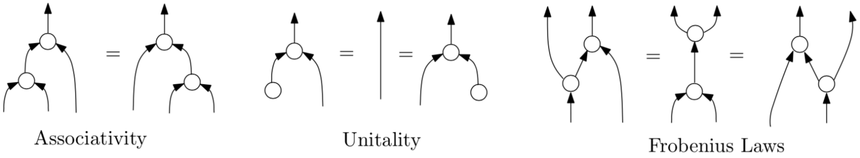
- $a^{**} = a$;
- $(\lambda a + \mu b)^* = \bar{\lambda} a^* + \bar{\mu} b^*$;
- $(ab)^* = b^* a^*$.

Definition: A Banach algebra A equipped with an involution map is a C^*- algebra A, if it satisfies:

$$||aa^*|| = ||a||^2$$

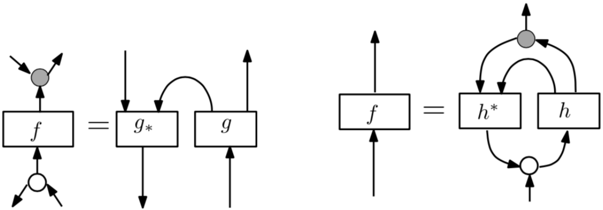
Frobenius Algebras

Definition: A dagger Frobenius algebra is an object A in a dagger monoidal category together with morphisms $m : A \otimes A \to A$ and $e : I \to A$, called a multiplication and an unit respectively, satisfying the following diagrammatic equations:



Positivity and completely positive maps between C*-algebras

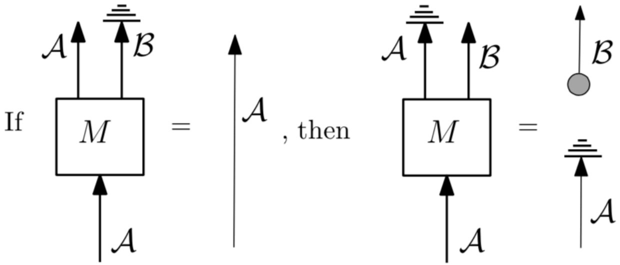
In [2] an abstract description of positive elements is generalized to maps $f : A \to B$, between two C^*-algebras $(A,$  , $)$ and $(B,$  , $)$ such that there exists an object X, called *ancilla*, and a map $g : A \to X \otimes B$ satisfying the following diagrammatic equality:



There two maps are equivalent for some object X and morphism: $A \to X \otimes B$.

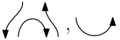
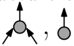
Heisenberg Principle

If we get information from a system whose algebra $\mathcal{A}$ is a factor and if we throw away (disregard) this information, then some initial states have inevitably changed.

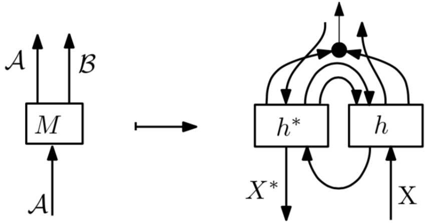


Heisenberg Principle in **Rel**

Theorem: Heisenberg principle fails in **Rel**.

Proof. As we are in $CP^* - construction$ we can consider every object of a factor $\mathcal{A}$ to have a structure of pair-of-pants-Frobenius-algebras: $\mathcal{A} \longmapsto (X_* \otimes X,$  $)$ and $\mathcal{B} \longmapsto (B,$  $)$

A map $M^* : \mathcal{A}^* \to \mathcal{A}^* \otimes \mathcal{B}^*$ can be represented as:



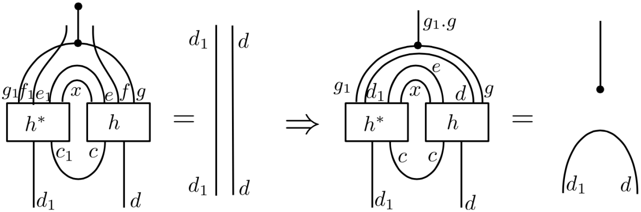
Heisenberg Principle in **Rel**

For this we can define a set $\mathcal{A}$ to be a two element set $\mathbb{Z}_2 := \{a, 1\}$ and B is also $\mathbb{Z}_2 := \{2, B\}$, where

$$b.b = 2 \qquad \text{and} \quad \text{b.2=2.b=b},$$

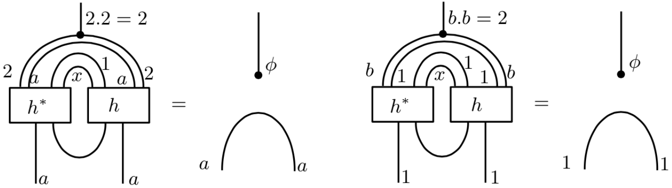
and then,
$\mathcal{A} \otimes \mathcal{A} := \{(1,1),\ (a,1),\ (1,a)\ (a,a)\}$

$h \in (\mathcal{A} \times \mathcal{A}) \times (x \times \mathcal{A} \times \mathcal{A} \times \mathcal{B})$, where x is an ancilla part.
$h := \{((a,a),(x,1,a,2)),\ ((a,1),(x,1,1,b))\}$

If 

Heisenberg Principle in **Rel**

#	h	h^*	$h^* \otimes h$
1	$((a,a),(x,1,a,2))$	$((a,a),(2,a,1,x))$	$((a,a),(a,a))$
2	$((a,a),(x,1,a,2))$	$((1,a),(x,1,1,b))$	$((1,a),(1,a))$
3	$((a,1),(x,1,1,b))$	$((a,a),(2,a,1,x))$	$((a,1),(a,1))$
4	$((a,1),(x,1,1,b))$	$((1,a),(x,1,1,b))$	$((1,1),(1,1))$



Kinematic Independence and No-signaling

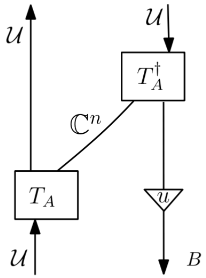
Kinematic independence $\Rightarrow$ No-signaling can be described using a following:
$\mathcal{A}$ and $\mathcal{B}$ are C^*-algebras corresponding to Alice's and Bob's subsystems. We take $u \in \mathcal{A} \vee \mathcal{B}$
Alice performs a non-selective measurement on u:

$$T(u) = \sum_{i=1}^{n} E_i^{1\backslash 2} u E_i^{1\backslash 2},$$

where $\sum_{i=1}^{n} E_i^{1\backslash 2} = I$ and E_i is a positive operator in $\mathcal{A}$.
T should leave Bob's system invariant: $T(B) = B$.

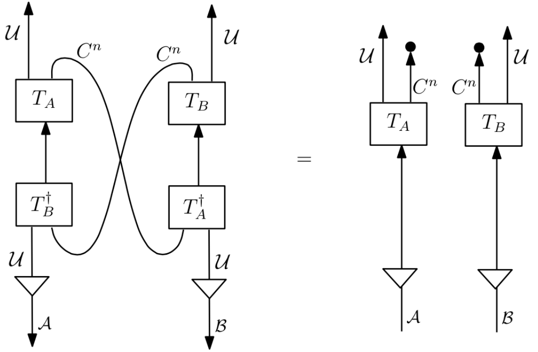
Kinematic Independence and No-signaling

Kinematic independence $\Rightarrow$ No-signaling diagrammatically:



Kinematic Independence and No-signaling

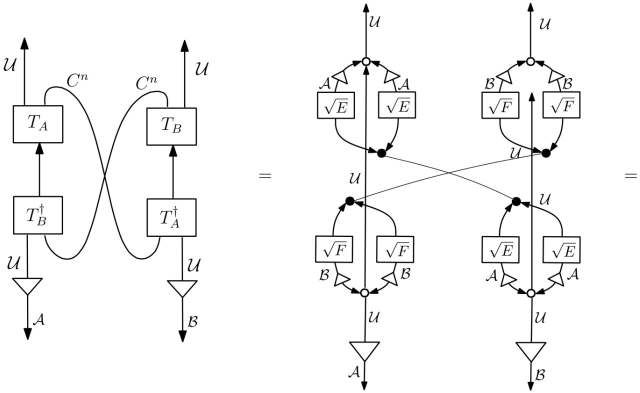
No superluminal information transfer via making a measurement between two kinematically independent systems can be described using a following diagrammatic representation:



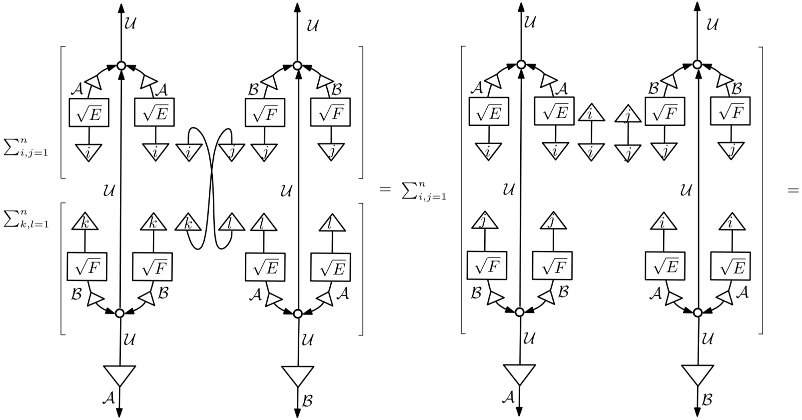
Kinematic Independence and No-signaling

Therem: This representation is indeed valid in **FHilb**:

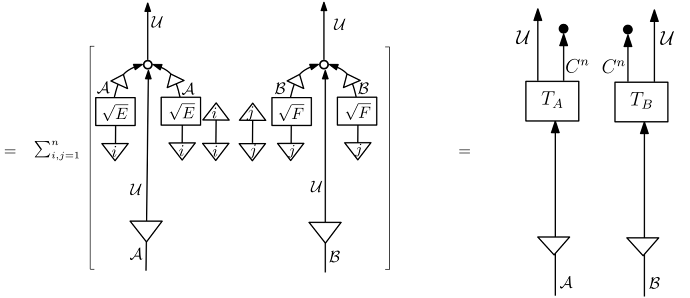
Proof:



Kinematic Independence and No-signaling



Kinematic Independence and No-signaling



This completes the proof.

□

Theorem: Kinematic independence does not always entail no-signaling in **Rel**.

Proof: Very similar to Heisenberg Principle proof, threrefore skipped.

From No-signaling to Independence

We are looking for a non-abelian group for which no-signaling still works.

Try 1: Differently from in **FHilb**, in **Rel** not all the normal operators are internally diagonalisable.

Try 2: A non-abelian symmetric group S_3

Try 3: A dihedral group of order 8 (Dih4).

But no success! :(

Further Plan of Attack

1. Check if the the result is valid for every symmetric group Sn on elements
2. We can embed any group into the symmetric one and strengthen the conclusion.
3. Check if the non-commuting sub-groupoids cannot be just sub-groups and if they have to overlap, then: If U is a groupoid $\Rightarrow$ No counterexample.

Conclusion

- Very basic introduction to category theory; **FHilb** & **Rel**;
- Use of category theory in quantum mechanics;
- No-cloning and Teleportation;
- Specific information-theoretic tasks formulated in the language of categorical quantum mechanics

Thanks for your attention!!!

Questions? Comments?