On Categorical Characterizations of No-signaling Theories

Mariami Gachechiladze

St Cross College

University Of Oxford

Supervised By Dr. Chris Heunen

This dissertation is submitted as a partial fulfillment of the degree of Master of Science in Computer Science.

September 2014

ABSTRACT

In this dissertation we demonstrate a general categorical formulation of the information - theoretic constraints given by Clifton, Bub, and Halvorson in [4]. Focus is on the correspondence between the kinematic independence of observables and the no-signaling principle. Our goal will be to build a graphical construction to reason about no superluminal information transfer between two party systems in the presence of there physical independence.

We will view algebras of observables as abstract C^*-algebras, which are actually normalisable dagger Frobenius algebras. After this, our main working environment will be category of finite dimensional Hilbert Space – **FHilb** and the "toy" category of sets and relations – **Rel**. As our secondary result we will show that the Heisenberg Principle fails in **Rel**. Our primary contribution will the graphical proof that kinematic independence does not always entail no-signaling in **Rel**. We will see that the converse correspondence is actually valid in the smallest non-abelian group structures.

ACKNOWLEDGEMENTS

At the first place I would like to thank my supervisor – Dr. Chris Heunen. Since the Hilary term when I attended a module – Categorical Quantum Mechanics taught by Chris, he has been very helpful, encouraging and always eager to answer questions. Without his guidelines and directions towards useful readings it would be impossible to fulfill my project. I am very grateful for the time and discussions that he devoted.

Also huge thanks to the Quantum Group for a very interesting year with lots of events, lectures, and meeting. Thanks to my friends from MSc in CS, MFoCS and St. Cross College for the very interesting discussions and support they showed everyday. They indeed made everything easier and nicer.

Thanks to all people who participated in organizing Oxford Computer Science program. It has been truly an outstanding journey in computer science.

Special thanks to my good friend Scott McGrew and professor Alexander Ganchev, I would not have made it this far without your support.

And finally, thanks to the best Mum and Dad, a brother, and a twin sister for giving me everything I ever needed.

(1) Contents

1. Introduction

In his 1932 work, "Mathematische Grundlagen der Quantenmechanik" (Mathematical foundations of quantum mechanics), von Neumann, a great Hungarian and American mathematician and physicist, rigorously established the mathematical working framework for quantum mechanics. Namely, he provided Dirac-von Neumann axioms, which can characterize quantum theory in terms of operations in Hilbert spaces. Since then, many scientists working in the field consider von Neumann formalism to be the language of quantum mechanics. However, much research has been conducted to explore quantum mechanics and its physical features in more general mathematics (e.g. categorical quantum mechanics).

In 1935, Schrödinger correctly noted that to detect the non-classical features of the theory, it is not enough to look at physical systems separately but most importantly, to see how they interact with other systems. This is precisely when category theory comes on board. Category theory tells us that a lot can be learned about specimens of species by observing how they interact with other specimens of the same or other species. This approach is very powerful and handy as there is no crucial need to have any information about specimens' internal structure; but it is possible to gain knowledge about individual elements by investigating the pattern of their behavior towards each other.

For more then a decade the category-theoretic view has been applied to quantum mechanics and it has been an vastly expanding area of studies. Categorical quantum mechanics is exactly employed to shift the focus from what quantum systems are to what they do. This new way of looking at quantum theory applies to the description of a physical theory specified by its algebra of observables, and in particular the class of theories whose observables form a C^*-algebra. A C^*-algebra was introduced by von Neumann right after Hilbert space formulation. So, this is a very natural way to carry on our work as categorists.

This new description of quantum theory will live in a dagger compact category. After we build up all the necessary structure and background, it can be observed that normalisable dagger Frobenius algebras, which live in our dagger compact category, are in 1-to-1 correspondence with the finite dimensional C^*-algebras. Having stated this much, we can already introduce the concrete problem that we will be exploring in this dissertation using our new construction. So, we our objective is to revisit the three fundamental information-theoretic constraints presented Clifton-Bub-Halvorson(CBH) in [4]. Clifton *at al.* in [4]

claim that these three constraints are sufficient to entail that the observables and state space of the theory is quantum mechanical.

Briefly, CBH information-theoretic constraints to describe quantum theory are following, [4]:

(1) the impossibility of superluminal information transfer between two physical systems by performing measurements on one of them;
(2) the impossibility of broadcasting the information contained in an unknown physical state;
(3) the impossibility of unconditionally secure bit commitment.

Our aim is to look at these constraints in more general categories, namely in a dagger compact category. For this, we will first model them in a category of finite dimensional Hilbert Space (**FHilb**) and later on, in a category of sets and relations **(Rel)**.

As the constraint (3) has been fully investigated before in[5] and (2) was studied in [8], we are left with (1), which we will explore by looking at the following correspondence, proved to be true by CBH : kinematic independence of observables $\Leftrightarrow$ no superluminal information transfer between them.

With help of the graphical language developed by the quantum group at the University of Oxford, we have managed to come up with the diagrammatic formulation of this correspondence as an effective tool to discuss it in a general category theory.

2. Background
Category Theory Essentials

In this section we introduce essentials from category theory that we need to work with throughout the thesis (1942–45, Samuel Eilenberg and Saunders Mac Lane).

2.1. Category and Monoidal Structure. Compactness. Dagger Structure.

Definition: 2.1.1. (Category) Category consists of:

- a collection of objects $A, B, C...$ denoted as $Ob(\mathcal{C})$;
- for every two objects A and B in $\mathcal{C}$ a set of morphisms denoted as a hom-set $\mathcal{C}(A, B)$ or $Hom_{\mathcal{C}}(A, B)$; So, every morphism has a domain and a codomain and diagrammatically it looks as follows:
$$f : A \longrightarrow B$$
- for every morphism $f \in \mathcal{C}(A, B)$ and $g \in \mathcal{C}(B, C)$, we have $g \circ f \in \mathcal{C}(A, C)$;
$$f : A \longrightarrow B; \quad g : B \longrightarrow C; \text{ So, } g \circ f : A \longrightarrow C$$
and moreover for $h \in \mathcal{C}(C, D)$, we have an **associativity law**:
$$h \circ (g \circ f) = (h \circ g) \circ f.$$
- for every object $A \in \mathcal{C}$, there in an identity morphism $id_A \in \mathcal{C}(A, A)$;
$$id_A : A \longrightarrow A$$
and it satisfies an **identity law** for every object:
$$f \circ id_A = f, \text{ and } \quad id_B \circ f = f.$$

Our running examples in this project is a category of finite dimensional Hilbert Spaces – **FHilb** and a category of sets and relations – **Rel**, which is a toy category to describe quantum mechanics.

Firstly, we need to add the monoidal structure to the category $\mathcal{C}$.

Definition: 2.1.2: (Monoidal Category and Coherence) Monoidal Category is the category $\mathcal{C}$ equipped with the following data:

- a functor, tensor product : $\otimes : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$;
- a tensor unit $I \in \mathcal{C}$;

- a natural isomorphism whose components $(A \otimes B) \otimes C \overset{\alpha_{A,B,C}}{\longrightarrow} A \otimes (B \otimes C)$ are called **associators**;
- a natural isomorphisms whose components $I \otimes A \overset{\lambda_A}{\longrightarrow} I$ $(A \otimes I \overset{\rho_A}{\longrightarrow} I)$ are called **left (right) unit**;

A category has monoidal structure if it satisfies the coherence principle. For the full definition of a monoidal category and the coherence principle see [8] .

Definition 2.1.3: (Compactness) A compact category is a symmetric monoidal category in which every object A comes with a dual object A^* and morphisms $\eta_A : I \to A \otimes A^*$ and $\varepsilon_A : A^* \otimes A \to I$ satisfying the so called "snake equations", which we will explain diagrammatically in the subsection 2.2.

The final structure we need to add to a compact category is a dagger functor, which in **FHilb** is an abstract notion for the conjugate-transpose.

Definition 2.1.4: (A dagger structure) A dagger on a category $\mathcal{C}$ is a contravariant functor $\dagger : \mathcal{C}^{op} \to \mathcal{C}$, which acts as an identity for objects – $A^\dagger = A$ and is an involution for morphisms – $(f^\dagger)^\dagger = f$ **.**

Now, we can look at the concrete categories , such as **FHilb** and **Rel** . Furthermore, let us investigate the meaning of the structure, we have built above, in each case.

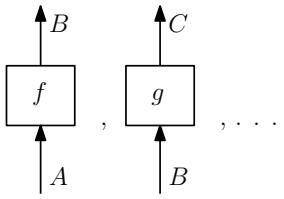
Examples 2.1.4: (Category of Finite Dimensional Hilbert Spaces – **FHilb**) Objects of **FHilb**, $Ob(\mathcal{C})$, are finite dimensional Hilbert spaces; morphisms: $f : H \longrightarrow K$, where $H, K \in Ob(\mathcal{C})$, are linear maps; composition of linear maps defines categorical composition of morphisms and identity maps are identity linear maps; a monoidal structure is an usual tensor product in Hilbert Space with an unit vector $\mathbb{C}$, and finally, a dagger is a conjugate transpose.

Example 2.1.5: (Nonstandard models of a dagger compact category : **Rel**) Objects are sets, morphisms $A \to B$ are relations $R \subseteq A \times B$. The composition of $R : A \to B$ and $S : B \to C$ is given by

$$S \circ R = \{(a, c) \in A \times C \mid \exists b \in B : \ (a, b) \in R, \ (b, c) \in S\},$$

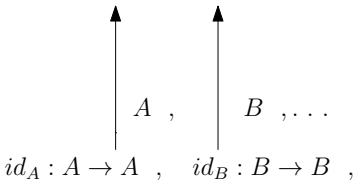
and $\{(a, a) \mid a \in A\}$ serves as an identity on A. Compactness comes in via Cartesian product. In the end, **Rel** becomes a dagger compact category by adding a dagger structure: if $(a, b) \in R$ then $(b, a) \in R^\dagger$.

2.2. **Graphical Calculus.** In this section we make a very quick overview of the graphical language, which gives the graphical notation for all the components of a monoidal category. In particular, any morphism $f : A \longrightarrow B$ can be thought as a process, which has an input of the type A and an output of the type B and diagrammatically it is denoted in the following way:



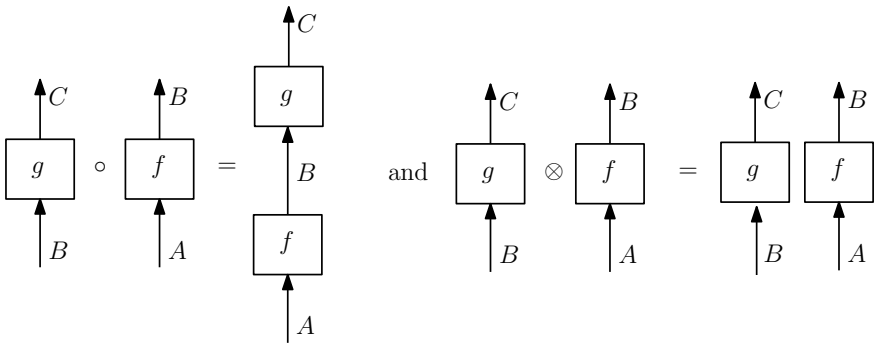
(2.1)

A process, which does nothing to its input type, is an identity map, and it is labeled by the type of an input object:



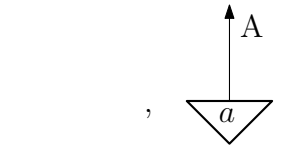
(2.2)

As processes are really morphisms in a monoidal category, we can denote a sequential and a parallel composition of processes diagrammatically in the following way:



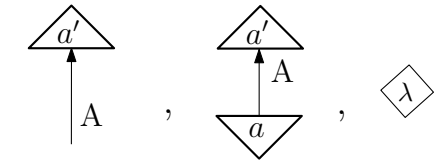
(2.3)

We draw n tensor unit in a monoidal category as an empty image. A state in a monoidal category is represented as a map from a tensor unit to an output type $a : I \longrightarrow A$:



$\alpha : I \to I$, $a : I \to A$ (2.4)

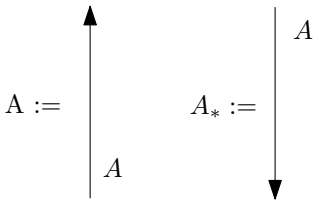
Note that, differently from other formalisms describing quantum mechanics, in which a state of the system has the central role, in the categorical formulation, a state is regarded as a regular morphism. Same for an effect, which can be thought as a measurement: a morphism which takes in a type A and maps it to the tensor unit (thus to an empty picture). So, $a' : A \to I$ and diagrammatically it looks following:



$a' : A \to I$, $a : I \to I$ (2.5)

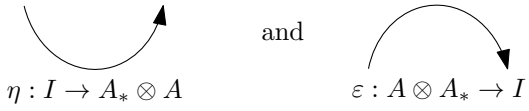
The second image shows a diagram for the inner product, which is precisely a composition of $a' \circ a : I \to I$. As you might expect, the inner product is really a number representing a probability of measuring the certain outcome. Numbers are also represented in the same way as displayed in (2.5).

A dual of an object A, A_* graphically is denoted as a wire labelled by A, but directed downwards:



(2.6)

$\eta_A : I \to A_* \otimes A$ is a cup and $\varepsilon_A : A \otimes A_* \to I$ is a cap:



(2.7)

and these two morphisms satisfy "snake equations" raised in the definition 2.1.3:

(2.8)

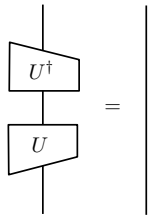
Having a dual for each object allows us to "bend the wires". So, we can already state the general principle of working with the diagrams:

"Only topology matters!"

Trivial graphical manipulations encapsulate non-trivial algebraic axioms. This means that with help of the graphical language, we do not have to keep all those axioms in mind. We are allowed to bend wires, makes them longer, shorter or act with them with any manipulation but we are not allowed to change the connectivity of an entire system. Basically, we must not alter the topology of a system. We will soon observe that this is a significant simplification of the formalism.

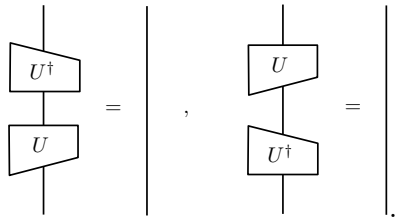
Definition 2.2.1. A map U is

- An isometry if:



(2.9)

- Unitary if:



(2.10)

The final structure that we are introducing before moving to Frobenius algebras is an environmental structure, which is also called a disregarding map and diagrammatically looks as follows:

(2.11)

2.3. **Classical Structures. Frobenius Algebras.** In this section we will overview classical structures, Frobenius laws and its connection with physical observables. We will very briefly look at $C^* - algebras$ algebraically and will investigate 1-to-1 correspondence between normalisable dagger Frobenius Algebras in **FHilb** and finite-dimensional $C^* - algebras$, which we will generalize to the lemma that normalisable dagger Frobenius algebras in an arbitrary dagger compact category are abstract $C^* - algebras$.

2.3.1 Banach algebras and $C^* - algebras$. An algebra A, as we will view it in this dissertation, is a linear associative algebra over the complex field $\mathbb{C}$. If an algebra A has a norm, it is said to be a *normed algebra*. A normed algebra A is a normed linear space and the norm satisfies:

(a) $\|ab\| \leq \|a\| \cdot \|b\|$;

(b) if A has an identity e, then $\|e\| = 1$;

In addition if A, with its norm, is complete (same as A is a Banach space), it is called a *Banach* algebra.

Now we can define an *involution map* on algebra A. $^* : A \to A$ which $a \longmapsto a^*$, where $a, a^* \in A$ and

(c) $a^{**} = a$;

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

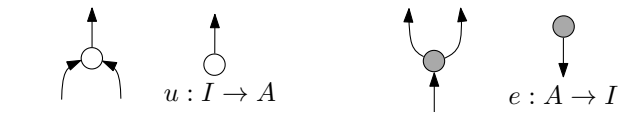
(e) $(ab)^{**} = b^* a^*$;

Definition 2.3.1.1. ($C^* - algebra$) A Banach algebra A equipped with an involution map is a $C^* - algebra$ A, if it satisfies:

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

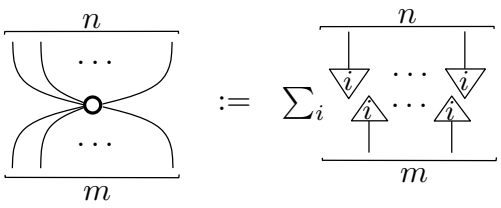
This is called a $C^* - condition$.

2.3.2 Classical Structures. Classical structures correspond to the copyable states in a (co)commutative and (co)associative manner. In [3] commutative Frobenius algebras were used to model classical data. Graphical language links a copying operation to a comonoid structure and a matching one to a monoid structure, precisely as displayed below:



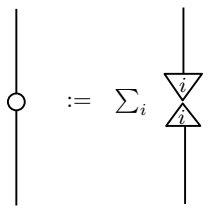
(2.12)

Definition 2.3.2.1. (Spiders) Spiders are linear maps with the following form



(2.13)

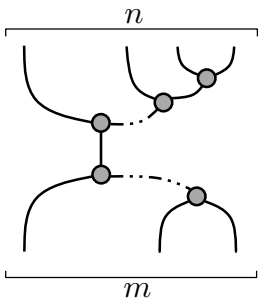
An identity wire is also a spider:



(2.14)

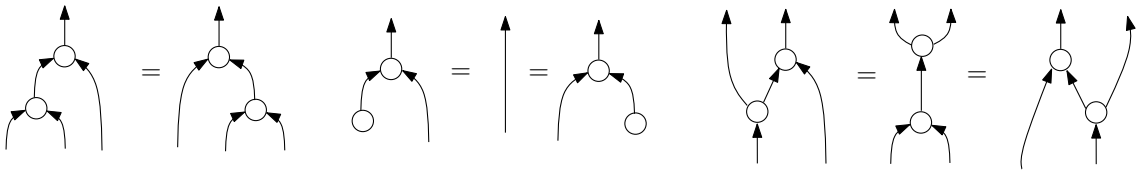
Spiders fuse if they are connected with at least one leg! [1]

Theorem 2.3.2.2. (Spider theorem [8]) Let (A, d, e) be a classical structure. Any connected morphism $A^{\otimes m} \to A^{\otimes n}$ built out of $d,\ e,\ id,\ \sigma,\ \otimes$, and $\dagger$ equals to the following normal form



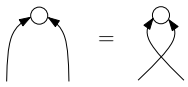
(2.15)

Definition 2.3.2.3. (Frobenius Laws via diagrams) 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:



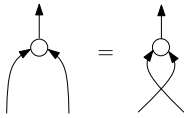
(2.16)

We say that a dagger Frobenius algebra $(A,$  $)$ is symmetric when:



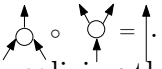
(2.17)

and it is commutative when:

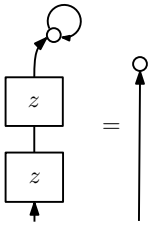


(2.18)

Commutativity implies symmetry but not other way around. Being a commutative algebra is strictly stronger then being symmetric. A dagger Frobenius algebra $\mathbb{M}_n$ is **FHilb**

is symmetric by trace property: $Tr(ab) = Tr(ba)$. On the other hand, in **FHilb** commutative dagger Frobenius algebras are in 1-to-1 correspondence with orthogonal basis. An orthonormality on its own implies the specialty of algebras –  . Frobenius algebras in categorical quantum mechanics started appearing after realizing their connection with an abstract characteristics of orthonormal basis. However, it appeared that specialty of an algebra does not always get linked to its commutativity, there are some non-commutative algebras living in **FHilb** that are special. Thus, in [2], for more general condition, term normalisability, was introduced:

Definition 2.3.2.4 A dagger Frobenius algebra $(A,$  $)$ is normalisable when it comes with the central, positive definite map $z : A \to A$, such that:

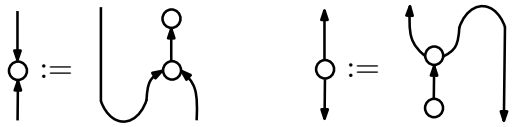


(2.19)

The map z is called a normalizer. From the definition of normalisability of algebras and with simple graphical manipulations it falls out that normalisable dagger Frobenius algebras are symmetric. And finally we get the definition:

Definition 2.3.2.5. Normalisable dagger Frobenius algebras in arbitrary categories are abstract C^*-algebras [13];

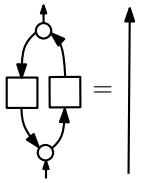
Note that, having Frobenius algebra structure means that every object has a dual. So, we have an isomorphism: $A^* \cong A$.



(2.20)

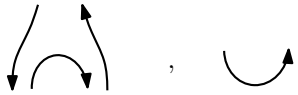
Composing these equations will gives us identities as they are inverses of each other (recall: Snake equations).

Besides, any normalisable dagger Frobenius algebra satisfies [2]:



(2.21)

Proposition 2.3.2.6. In a positive-dimensional dagger compact category, every object of the form $H^* \otimes H$ carries a canonical normalisable dagger Frobenius algebra with the following multiplication and unit



(2.22)

This abstract C^*-algebra is called an abstract matrix algebra, an algebra of all bounded operators and is denoted by $\mathfrak{B}(\mathcal{H})$.

3. **Completely Positive Maps**

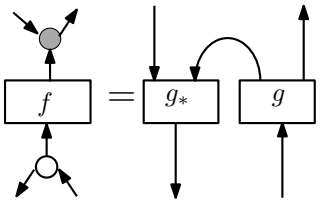
Having built up all the structure in an arbitrary category, now it is time to raise our structure to a fully abstract procedure, called the CP^*–construction that turns any dagger compact category (like **FHilb**) into a category of abstract C*-algebras with abstract completely positive maps. We will work in this new construction to show that the Heisenberg Principle presented in [10] fails in some arbitrary dagger compact categories, namely in the non-standard model, category of sets are relations – **Rel**.

3.1. **Complete Positivity.**

First we need to recall the definition of positivity and completely positive maps between C^*-algebras.

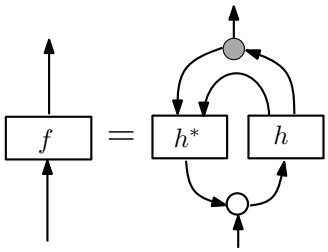
Definition 3.1.1 (Positive element and morphism. Complete positivity) An element a of a C^* -algebra A is positive if it has a form: $a = b^*b$. A linear function f between two C^*-algebras , $f : A \to B$ is positive when it maps positive elements to positive elements. It is completely positive when $f \otimes 1 : A \otimes \mathbb{M}_n \to B \otimes \mathbb{M}_n$ is positive for every $n \in N$.

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:



(3.1)

This equality is called the $CP^* - condition$ and it is equivalent to:



(3.2)

for some object X and morphism $h : A \to X \otimes B$.

It is easy to verify that if $\mathcal{C}$ is a dagger compact category, so is the category of abstract C^*-algebras in $\mathcal{C}$ and maps satisfying the CP^*-condition.

So, given any dagger compact category $\mathbf{V}$, we can define data for a new category $CP^*[\mathbf{V}]$. Its objects are normalizable dagger Frobenius algebras in $\mathbf{V}$ and morphisms $(A,$  $) \to (B,$  $)$ are morphisms $f : A \to B$ in $\mathbf{V}$ satisfying the $CP^* - condition$.

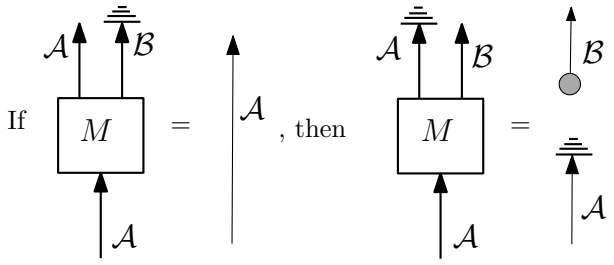
Theorem 3.1.2. If V is a dagger compact category, $CP^*[V]$ is again a well-defined dagger compact category.

Proof. See [2]. □

3.2. **The Heisenberg Principle in FHilb.** The Heisenberg principle states that obtaining information about a quantum system via performing measurement operation, changes its initial state [6]. A more precise formulation is following:

If we get information from a system whose algebra $\mathcal{A}$ is a factor (i.e. its center contains only multiples of identities – $\mathcal{A} \bigcap \mathcal{A}\prime = \mathbb{C}1$), and if we throw away (disregard) this information, then some initial states have inevitably changed.

We can consider an operation $M^* : \mathcal{A}^* \to \mathcal{A}^* \otimes \mathcal{B}^*$ to be a physical measurement of a system, which extracts some information from the system, probably changing the initial state of the system. Here, $\mathcal{A}$ is an unital $^*-$algebra and represents a physical system. $\mathcal{B}$ carries a classical structure, representing outcome of the measurement. We denote $\mathcal{A}^*$ to be a dual of $\mathcal{A}$. $\mathcal{A}^*$ consists of states of the system and $\mathcal{B}^*$ contains probabilities of measurement outcome. Diagrammatically the Heisenberg Principle looks following:



(3.3)

Let us discuss this diagrammatic notation algebraically:

If for any initial state $\rho \in \mathcal{A}^*$, assuming that $\mathcal{A}$ is a factor, $(id \otimes tr) \circ M^*(\rho) = \rho$, ($\mathcal{A}$ being a factor precisely means that $\mathcal{A}'$ is trivial and as center of $\mathcal{A}$, $Z(\mathcal{A})$ is contained in $\mathcal{A}'$), then no information can be obtained on ρ :

$$(tr \otimes id) \circ M^*(\rho) = \vartheta, \text{ where } \vartheta \text{ is independent from } \rho.$$

Theorem 3.2.1. (Multiplication Theorem) If $T : \mathcal{A} \to \mathcal{B}$ is an operator and $T(A^*A) = T(A)^*T(A)$ for some $A \in \mathcal{A}$, then $T(A^*A') = T(A)^*T(A')$ and $T(A'^*A) = T(A')^*T(A)$ for all $A' \in \mathcal{A}$.

Proof. Let's pick any $A' \in \mathcal{A}$ and $\lambda \in \mathbb{R}$.

$$T((A^* + \lambda A'^*)(A + \lambda A')) = T(A)^*T(A') + \lambda T(A^*A' + A'^*A) + \lambda^2 T(A'^*A'),$$

By Cauchy-Schwartz for all $\lambda \in \mathbb{R}$:

$$T((A^* + \lambda A'^*)(A + \lambda A')) \geq T(A)^*T(A') + \lambda(T(A)^*T(A') + T(A')^*T(A)) + \lambda^2 T(A')^*T(A')).$$

So,

$$T(A^*A' + A'^*A) \geq T(A)^*T(A') + T(A')^*T(A)$$

If we replace A by iA and A' by $-iA'$:

$$T(iA^*(-iA') + (-i)A'^*iA) \geq T(iA)^*T(-iA') + T(-iA')^*T(iA)$$

An opposite inequality holds:

$$T(A^*(A') + A'^*A) \leq T(A)^*T(A') + T(A')^*T(A)$$

So, we have an equality. Final step is to replace A' by iA' and we get precisely what we had to prove:

$$T(A^*A') = T(A)^*T(A') \text{ and } T(A'^*A) = T(A')^*T(A)$$

□

Theorem 3.2.2. (Heisenberg Principle [10]) Let M be an operation $\mathcal{A} \otimes \mathcal{B} \to \mathcal{A}$ such that

$$M(A \otimes 1) = A$$

then

$$M(1 \otimes B) \in \mathcal{A} \bigcap \mathcal{A}'.$$

In particular, if $\mathcal{A}$ is a factor, then $B \mapsto M(1 \otimes B) = \vartheta(B) \cdot 1_A$ for some state ϑ on B.

Proof. Take $A \in \mathcal{A}$, $B \in \mathcal{B}$. Using the Theorem 3.2.1[10],

$$M(1 \otimes B) \cdot A = M(1 \otimes B)M(A \otimes 1) = M(A \otimes B)$$

And also,

$$A \cdot M(1 \otimes B) = M(A \otimes 1)M(1 \otimes B) = M(A \otimes B)$$

So, $M(1 \otimes B) \in Z(\mathcal{A})$. And if $\mathcal{A}$ is a factor, equivalently center of an algebra $\mathcal{A}$ is trivial, then a map $B \mapsto M(1 \otimes B)$ is a map which sends B to $\mathbb{C} \cdot 1_A$.

□

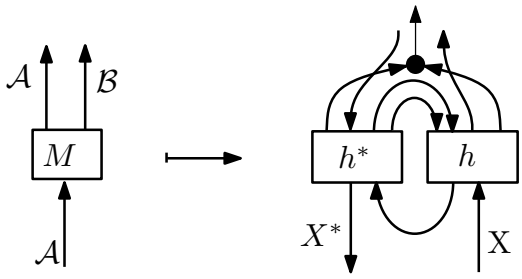
Let us see what happens when we generalize the Heisenberg Principle from **FHilb** to an arbitrary dagger compact category. We will use the CP^*-construction developed in the previous section and work in **Rel** to prove that (3.3) fails in this non-standard category.

3.3. The Heisenberg Principle in non-standard model, Rel. We discussed the structure of **Rel** in example 2.1.5. Now, we will raise this structure to our new category – CP^*[**Rel**]. We can see that these new non-standard models of $C^* - algebras$ have quite a different structure from $C^* - algebras$ in **FHilb**. It appears that normalisable dagger Frobenius algebras in Rel are (in one-to- one correspondence with) groupoids [2].

Theorem 3.3.1. The 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:



(3.4)

As we are working in the dagger compact category in **Rel**, we can forget about the directions of the arrows.

Our goal is to demonstrate some counterexample for the Heisenberg implication:

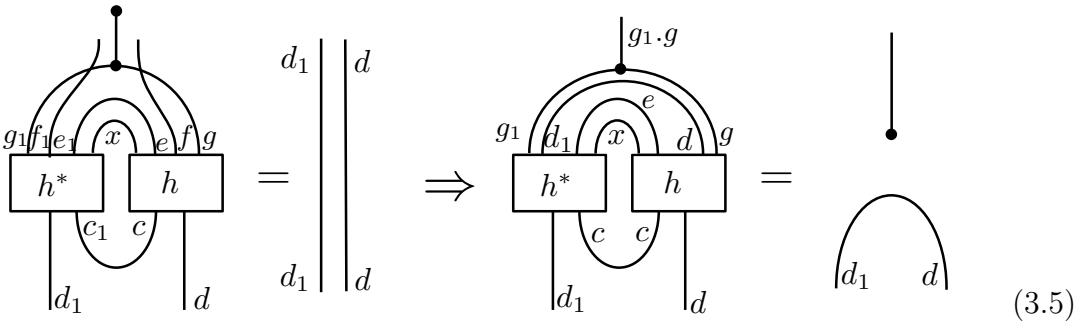
For this we can define a set $\mathcal{A}$ to be a two element set $\mathbb{Z}_2 := \{a, 1\}$ and B is also $\mathbb{Z}_2 := \{2, B\}$, where

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

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.
$h := \{((a,a),(x,1,a,2)),\ ((a,1),(x,1,1,b))\}$

Now, the Heisenberg Principle looks following:

If 

(3.5)

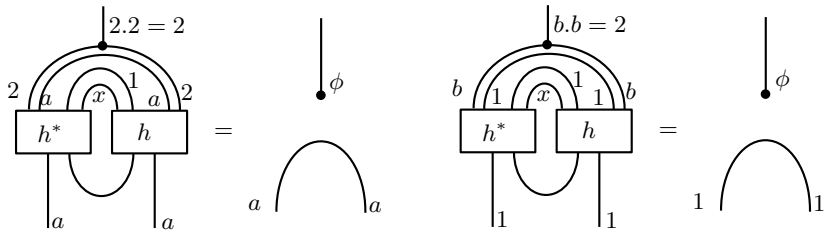
where $h := \{((c,d),(x,e,f,g)) \mid c,d,e,f \in \mathcal{A},\ g \in \mathcal{B}\}$ and $h^* := \{((d_1,c_1),(g_1,f_1,e_1,x)) \mid c_1,d_1,e_1.f_1 \in \mathcal{A},\ g_1 \in \mathcal{B}\}$. Besides, the conditional clause holds only if $h^* \otimes h := \{((d_1,d),(f_1,f)) \mid d_1 = f_1,\ d = f \text{ and } c_1 = c,\ e_1 = e\}$

For the concrete case of $h^* \otimes h$, if we consider all the possible permutation of h and h^*:

#	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	$((a,1),(x,1,1,b))$	$((1,a),(x,1,1,b))$	$((1,1),(1,1))$

Having fixed the relations, we can already discuss the right-hand side of the implication in the Heisenberg principle:

If $d_1 \neq d$, the left-hand side of the equality of the right-hand side of the implication becomes an empty picture and so does the righthand side. So, in this case implication is valid.
So, the table above is filtered down to only two members #1 and #4:



(3.6)

Now, $h^* \otimes h := \{((d,d),2 \mid \forall d \in \mathcal{A}\ \}$ but $\phi : \{\star\} \longrightarrow \{b,2\} \in \mathcal{B}$.
So, the equality does not hold.

□

To conclude this section, by demonstrating a counterexample, we have shown that the Heisenberg Principle (claiming that extracting information by performing a measurement operation on a system, changes an initial system) is not valid while working in a general $C^* - algebraic$ framework and thus in an arbitrary dagger compact category.

4. Information-Theoretic Constraints

In this section we discuss the information-theoretic constraints presented in [4]. Our novel work is to look at the correspondence between the kinematic independence and the impossibility of superluminal information transfer between two distinct physical systems by performing a measurement on one of them [4]. We think that this is a logical continuation having demonstrated a failure of the Heisenberg Principle in the general categorical framework on a single party measurement system. The plan of attack is following: at first we state the three no-go's presented in [4] and we review some of the related parts of the current research that is already done, concerning CBH characterization in a general category. Then we focus on the kinematic independence and explain why the property of two distinct physical observables being mutual diagonalizable is not a good enough criteria to guarantee the kinematic independence in an arbitrary dagger compact category. And finally, as a novel work, we introduce diagrammatic representation of the correspondence mentioned above. We show validity of our construction by duplicating the proof done in [4] in **FHilb** in digrammatic language. And finally, the diagrammatic results in an arbitrary category (e.g. **Rel**) follows.

4.1. Information-Theoretic Characterization by CHB.

The main question that Clifton-Bub-Halvorson [4] tried to answer is whether quantum physics can be reduced to the information-theoretic principles. In 2003 they presented CBH theorem, which states that:

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

(i) No superluminal information transmission between two distinct systems by acting with a measurement operator on one of them.

(ii) No broadcasting of the information contained in an unknown state.

(iii) No unconditionally secure bit commitment.

A strategy in [4] was to show that these principles are equivalent to three essential characteristics of quantum theory:

(1) If $\mathcal{A}$ and $\mathcal{B}$ are distinct physical systems, then the observables of $\mathcal{A}$ commute with those of $\mathcal{B}$.

(2) The observables of an individual system do not all commute with each other.

(3) There are physically realizable nonlocal entangled states.

4.2. **No Unconditionally Secure Bit Commitment.** Bit commitment is a cryptographic protocol in which two parties participate. These parties are Alice and Bob, as you might expect. Alice supplies her encoded message to Bob. Bob receives it but cannot decode it unless Alice provides extra data. Now Bob can read the message but he needs to make sure that protocol does not allow Alice to cheat by encoding the bit in a way that leaves the decryption invariant to her choice of either 0 or 1.

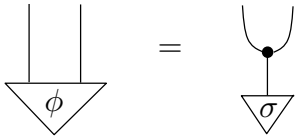
If we have a composite system $\mathcal{A} + \mathcal{B}$, consisting of two subsystems $\mathcal{A}$ and $\mathcal{B}$, 'no broadcasting' and kinematic independence conditions entail that C^*-algebras $\mathcal{A}$ and $\mathcal{B}$, whose self-adjoint elements represent the observables of A and B, are non-abelian but mutually commuting. This means that at least theoretically there exist non-local entangled states. BB84 and later on Mayers, and Lo and Chau demonstrated that Alice can always cheat in presence of an Einstein-Podolsky-Rosen pair.

In [4] CBH demonstrate that impossibility of unconditionally secure bit commitment entails that if each of the subsystems of a composite system has non-uniquely decomposable states (non-abelian algebras $\mathcal{A}$ and $\mathcal{B}$) then there exists a pair of classically correlated states $\{\rho_0, \rho_1\}$ in $\mathcal{A} \vee \mathcal{B}$ such that their marginals are identical, then these two systems must be able to hold an entangled state. The converse implication stays open in this paper. It is not investigated if having entangled subsystems mean that unconditionally secure bit commitment is impossible. However, the authors propose a possible path to success by looking at arbitrary non-abelian C^*-algebras.

The correspondence was investigated in a general dagger compact categories in [5]. [5] used the graphical language to demonstrate that having an entangled state is certainly equivalent to impossibility of unconditionally secure bit commitment in **FHilb**, however he used some properties of **FHilb** which are not particularly valid for general categories. Then he examined a "toy" category of **Rel** and he demonstrated that unconditionally secure bit commitment is indeed possible within this framework. So, when generalizing to arbitrary categories, a claim about impossibility of the protocol is invalid.

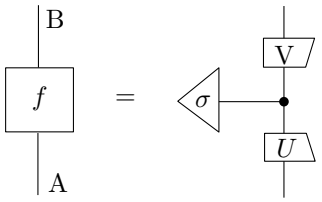
His plan of attack was following: He demonstrated impossibility in **FHilb** (Mayers, Lo and Chau) by using uniqueness of spectral decompositions. Once the proof was valid in Hilbert spaces, he lifted some parts of it to a general dagger compact category.

Definition 4.2.1. Suppose A admits a classical structure $\bullet$. We say a state $\phi : I \to A \otimes A$ is a diagonal if there is σ such that



(4.1)

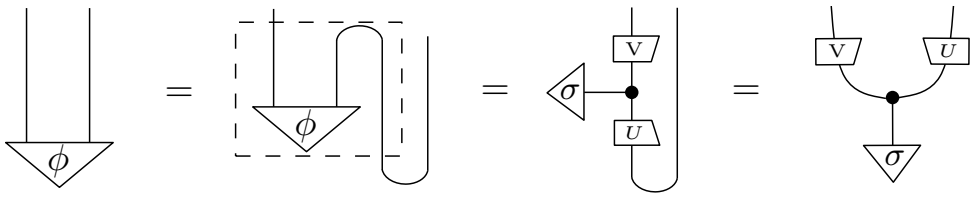
Definition 4.2.2. A dagger compact category $\mathcal{C}$ has a singular value decomposition if every morphism $f : A \to B$ in this category can be written in the following form:



(4.2)

Using last two definitions and state-process duality the corollary follows:

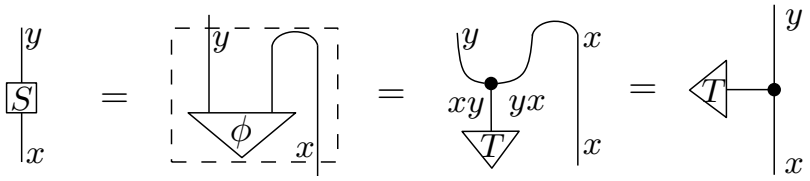
Corollary 4.2.3. (Schmidt decomposition) For any state $\phi : I \to A \otimes A$, singular value decomposition is equivalent to Schmidt decomposition:



(4.3)

This construction is used in the diagrammatic proof of impossibility of commitment protocol in **FHilb** discussed above.

A singular value decompositions in **Rel** looks rather different. As we saw above, classical structures are abelian groupoids, multiplication relates (x, y) with xy and comlultiplication acts like factorization, so it relates z to (x, y) when $z = xy$. So, diagonal states in **Rel** require factorization, such that if we have a state $S \in X \otimes X$ and $(x, y) \in S$, together with $T \subseteq X$ then $xy \in T$. So diagonal relation is given by a subset $T \subseteq X$ and has the form:



(4.4)

So, relation $(x, y) \in S$ holds only if $xy = yx \in T$.

Proposition 4.2.4. The number of points a diagonal relation relates is $|T| \cdot |X|$, where T is the subset inducing the relation and X is the classical structure.

Since unitary maps in **Rel** preserve cardinality, it is obvious that the cardinality of a singular value decomposition of a map should be equal to the cardinality of a diagonal relation. This is not always the case. Which means that **Rel** does not have a singular value decomposition. For a specific counterexample see [5]. This is also a case when we raise our structure to CPM(**Rel**) – a category of completely positive maps, where classical structures and unitaries are canonical.

Hence, the proof which was based on Schmidt decomposition cannot be employed in a general dagger compact category. Moreover, in [5] a counterexample is demonstrated.

Theorem 4.2.5. Bit commitment is possible in **Rel**.

So we have just stated that the impossibility of having unconditionally (in our case perfect, see [11] for more details) secure bit commitment between two parties while these parties possibly being entangled is not valid in a general dagger compact category. What can this result actually state? There are three possibilities which will make the postulate work in general category [5]:

First one would be strengthening the definition of a bit commitment scheme but this action does not seem reasonable for two reasons: a) The scheme and its axioms was initially built to correspond well with general intuition and classical definitions; b) It is valid in **FHilb**, which is powerful enough claim to argue for the correctness of construction in [5].

Second, strengthening the working axioms in category theory. However, this is also not justifiable because the framework of a dagger compact category, we have built above, is sufficient to model quantum phenomenon.

So, as we agree neither to change the protocol nor the working framework, we are left with accepting results as they are. Thus, we dispute CBH characterization of quantum

theory in general category theory.

By now we have only discussed correspondence $(iii) \Leftrightarrow (3)$ in presence of (1) and (2). Now we will use the similar outline for the novelty work, namely, to investigate correspondence $(i) \Leftrightarrow (1)$.

4.3. **Kinematic Independence $\Leftrightarrow$ No Superluminal Information Transfer.** We have a composite system $A + B$, consisting of two subsystems A and B with the corresponding C^*-algebras $\mathcal{A}$ and $\mathcal{B}$, whose self-adjoint elements denote the observables of A and B. Clifton et al. show that two physical observables are kinematically independent if and only if 'no signaling' or equivalently 'no superluminal information transfer' condition holds. We will first explain their proof and after, try to see what happens when we generalize it to an arbitrary dagger compact category.

4.3.1. *Commutativity and Diagonalisability.* By Nielsen and Chuang in [12] a commutator between two operators A and B are defined to be $[A, B] = AB - BA$. And we say that two operators A and B commute iff $[A, B] = 0$, equivalently iff $AB = BA$. In addition, there is a very important convention (as stated in [12]) that connects kinematic independence with the property of being simultaneously diagonalizable.

Theorem 4.3.1.1. (Simultaneous Diagonalization Theorem) If A and B are Hermitian operations, then they commute if and only if there exists some orthogonal bases such that A and B are both diagonal with respect to these basis. So, $[A, B] = 0$ is equivalent to saying that A and B are simultaneously diagonalizable.

The proof of this theorem in **FHilb** is quite straightforward (see [12]). But how do we think of diagonalizablity in terms of graphical calculus first in **FHilb** and then what do we get when we try to extend it in a general dagger compact category?

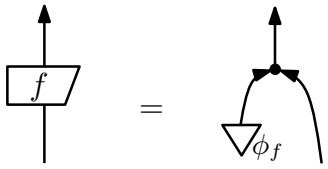
Definition 4.3.1.2. An endo-operator $N : \mathcal{H} \to \mathcal{H}$, acting on a Hilbert Space, is normal iff $[N, N^\dagger] = 0$.

Theorem 4.3.1.3. In Hilbert spaces, every normal operator N is diagonalizable.

Now we are ready to introduce diagonalization in category-theoretic way [7]. We start by introducing the concepts of compatible monoid and internally diagonalisable elements [3]. We will use this definitions to express spectral theorem.

Definition 4.3.1.4. In a monoidal category, an endomorphism $f : A \to A$ is compatible with a monoid (A, m, u) if the following holds: $m \circ (f \otimes A) = m \circ (A \otimes f) = f \circ m$

Definition 4.3.1.5. In a braided dagger compact category, $f : A \to A$ is internally diagonalisable if it can be expressed as an action of an element of commutative dagger Frobenius algebra on A:



(4.5)

,where $\phi_f : I \to A$ is a state of A.

Theorem 4.3.1.6 An endomorphism $f : A \to A$ is internally diagonalisable if and only if it is compatible with a commutative dagger Frobenius algebra and every normal endomorphism $f : A \to A$ in **FHilb** is internally diagonalisable.

So the property of being internally diagonalisable works the same as diagonalisability for **FHilb** but this is not the case when we move to **Rel**. In [7], connection between the normal and internally diagonalisable operations are investigated by choosing 2 and 3 element sets and operators on these sets are written out for both cases. In 2 element set there are total number of $2^4 = 16$ operators so corresponding 2×2 matrices, when in 3 element set this number it $2^9 = 512$. Out of these set of matrices the ones which are normal (commuting with their adjoint matrix) were filtered and then checked if they are all internally diagonalisable. It turned out that this is not always the case, not all the normal operators in **Rel** can be internally diagonalised. So, this appears to be the core difference between **FHilb** and **Rel**, while discussing the diagonalization.

Hence, although the reader might have known simultaneous diagonalisability of two operators as a criteria for their kinematic independence, we will not use it anywhere later on in our derivations for the reasons described above.

5. Kinematic Independence ⇒ No-signaling

5.1. **Kinematic Independence ⇒ No-signaling by CBH.** We will first investigate one direction of this correspondence. This constraint means that if there are two kinematically independent party systems, Alice and Bob, and they perform their local measurements, Alice's measurement cannot influence Bob's outcome and other way around as well. In other words, non-selective local measurement cannot transfer information to a physically distinct system. Let us see how the proof is handled in [4] and then investigate it in our newly developed framework.

State of the system is $u \in \mathcal{A} \vee \mathcal{B}$ (where $\mathcal{A} \vee \mathcal{B}$ in **FHilb** is the smallest $C^* - algebra$ of $\mathfrak{B}(\mathcal{H})$ containing both $\mathcal{A}$ and $\mathcal{B}$: $\cap\{\mathcal{U} \subseteq \mathfrak{B}(\mathcal{H}) \mid \mathcal{A}, \mathcal{B} \subseteq \mathcal{U}\}$. However, in **Rel** $\mathcal{A} \vee \mathcal{B}$ is the smallest groupoid containing both groupoids $\mathcal{A}$ and $\mathcal{B}$. This can be done by taking the collection of paths consisting of the arrows in $\mathcal{A}$ and $\mathcal{B}$. And indeed if the collection of arrows in $\mathcal{A}$ is: $M_A := \{f_a \text{ and } f_a^{-1}| \text{ for } \forall a \in \mathcal{A}\text{sucth that } f_a f_a^{-1} = id_a, \}$ and the collection of arrows in $\mathcal{B}$ is: $M_B := \{f_b \text{ and } f_b^{-1}| \text{ for } \forall b \in \mathcal{B}\text{sucth that } f_b f_b^{-1} = id_b, \}$, then we can denote that all morphisms in $\mathcal{A} \vee \mathcal{B}$ live in the disjoint union of $M_A \cup M_b$).

$\mathcal{A}$ and $\mathcal{B}$ are $C^* - algebras$ corresponding to Alice's and Bob's subsystems respectively. For capturing the kinematic independence of two systems, the notion of C^*-independence is developed in [4], which does not directly mean commutativity (i.e., that $[A, B] = 0$ for all $A \in \mathcal{A}$ and $B \in \mathcal{B}$), but that any state of $\mathcal{A}$ is compatible with any state of $\mathcal{B}$. So for any state $\rho_1 \in \mathcal{A}$ and $\rho_2 \in \mathcal{B}$, there is a $u \in \mathcal{A} \vee \mathcal{B}$ such that u is a product state, i.e. u restricted to $\mathcal{A}$ is ρ_1 and to $\mathcal{B}$ is ρ_2. In [6], it is demonstrated that C^*-independence of $\mathcal{A}$ and $\mathcal{B}$ holds just in case $\|A \cdot B\| = \|A\| \cdot \|B\|$ for all $A \in \mathcal{A}$ and $B \in \mathcal{B}$.

Now, Alice is ready to perform a non-selective measurement on system $u \in \mathcal{A} \vee \mathcal{B}$:

$$T(u) = \sum_{i=1}^{n} E_i^{1/2} u E_i^{1/2} \tag{5.1}$$

where $\sum_{i=1}^{n} E_i = I$ and E_i is a positive operator in $\mathcal{A}$. Performing an operator T on u gives no information to Bob if and only if operator T^* leaves Bob's system invariant.

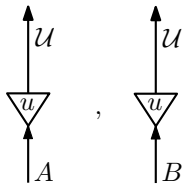
Definition 5.1.1. An operation T on the system $\mathcal{A} \vee \mathcal{B}$ carries no information to Bob just in case $(T^*\rho)\restriction_{\mathcal{B}} = (\rho)\restriction_{\mathcal{B}}$ for $\forall \rho \in \mathcal{B}$.

Since one can get all states of $\mathcal{B}$ by restricting $\mathcal{A} \vee \mathcal{B}$, $(T^*\rho)|_{\mathcal{B}} = \rho|_{\mathcal{B}}$ if and only if $\mu(T(B)) = \mu(B)$ for $\forall B \in \mathcal{B}$ and for all states $\mu \in \mathcal{B}$. So, T should leave Bob invariant : $T(B) = B$ for all $B \in \mathcal{B}$.

Following the definition of the kinematic independence and defining no-signaling as an invariance of Alice's measurement to Bob's system and outcome, [4] states that "it is clear that the kinematic independence of A and B entails that Alice's local measurement operations cannot convey any information to Bob". And indeed: $T(B) = \sum_{i=1}^{n} E_i^{1/2} B E_i^{1/2} = B$.

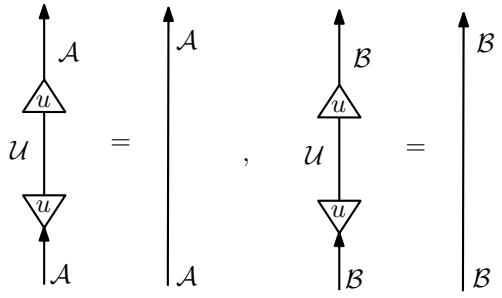
5.2. **Kinematic Independence ⇒ No-signaling in FHilb Diagrammatically.** The goal of this section is to define a no-signaling constraint in graphical calculus and demonstrate that it indeed works for kinematically independent systems in finite dimensional Hilbert spaces. This work will follow the proof in 4.3.2 step-by-step.

For a starting point, we will define an "universal algebra" $(\ \mathcal{U},$  $)$. such that $\mathcal{A}, \mathcal{B}$ are subalgebras of $\mathcal{U} \equiv \mathcal{A} \vee \mathcal{B}$. $\mathcal{A}, \mathcal{B} \subseteq \mathcal{U}$. So there is an injection map $u : \mathcal{A} \hookrightarrow \mathcal{U}$ and $u : \mathcal{B} \hookrightarrow \mathcal{U}$ which we denote diagrammatically in the following way:



(5.2)

Here a map $u : \mathcal{A} \to \mathcal{B}$ is a *-homomorphism while its dagger $u^\dagger : \mathcal{U} \to \mathcal{A}$ is a completely positive map such that:

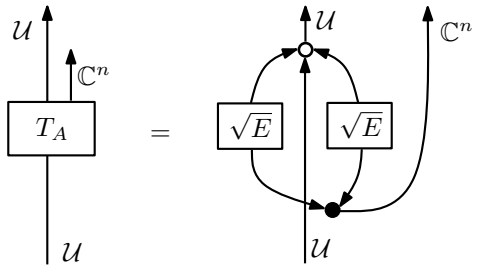


(5.3)

A measurement operator of Alice acts following way on the system $u \in \mathcal{U}$:

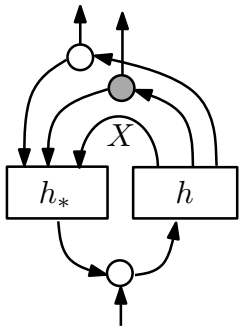
$$T_A : \ u \longrightarrow \sum_{i=1}^{n} \sqrt{E_i} u \sqrt{E_i} \ \otimes \ |i\rangle$$

where $u \in \mathcal{U}$, $\sum_{i=1}^{n} E_i = I$ and E_i is a positive operator in $\mathcal{A}$. We define a map T_A diagrammatically as well:



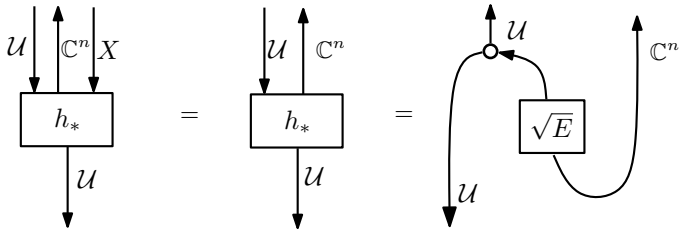
(5.5)

Our aim is to show that the measurement operator T_A that we just defined, is completely positive. For this we need to show that it satisfies the CP^*-condition, e.i. has the following form:



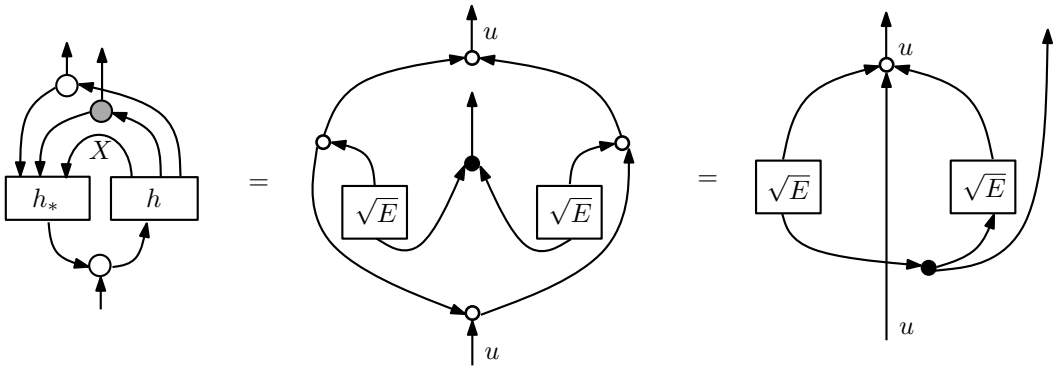
(5.6)

Let's look at h_* and respectively h individually. Take X to be a tensor unit I, so we can skip drawing X from the image.



(5.7)

The map h will be a mirror image of h_*. Substituting both h and h_* maps with the one derived above and assuming that $X = I$, we get the following result:

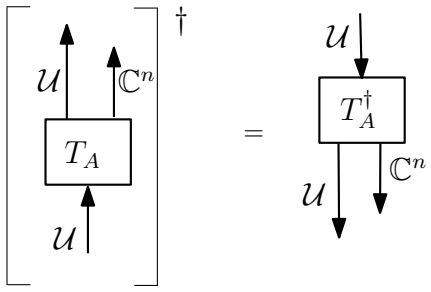


(5.8)

The second equation uses the spider theorem. So, we end up precisely where we started. Thus, the T_A map that we defined, is a completely positive map.

Having set up the completely positive map $T_A(u) = \sum_{i=1}^{n} \sqrt{E_i} u \sqrt{E_i} \otimes |i\rangle$ where $u \in \mathcal{U}$, now we have to show that this measurement operator leaves Bob's system invariant. e.i. $T_A^\dagger(1 \otimes B) = B$ for $\forall B \in \mathcal{B}$.

If $T_A : u \to u \otimes |i\rangle$, then $T_A^\dagger : u^\dagger \otimes (|i\rangle)^\dagger \to u^\dagger$:



(5.9)

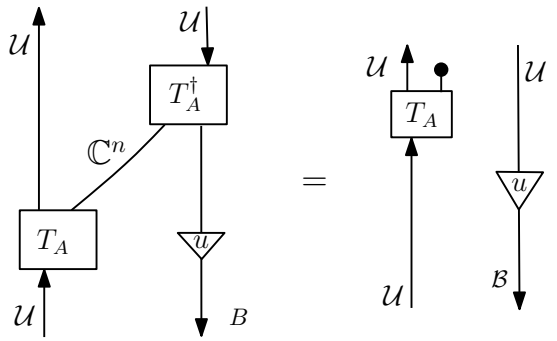
Moreover, as a dagger compact category category we are working in is symmetric, we can bend and intersect wires. So, instead of $T_A^\dagger$ will be using the following form of the map:

$$T_A^\dagger \circ \sigma : (|i\rangle)^\dagger \otimes u^\dagger \to u^\dagger$$

where σ is a swap map. So, from now on we will encapsulate the swap map in $T_A^\dagger$ and we will only be writing: $T_A^\dagger : (|i\rangle)^\dagger \otimes u^\dagger \to u^\dagger$. The purpose of this is to have a nicer and more symmetric final construction.

Theorem 5.2.1. No superluminal information transfer between Alice and Bob via Alice's measurement in the presence of the kinematic independence of physical observables

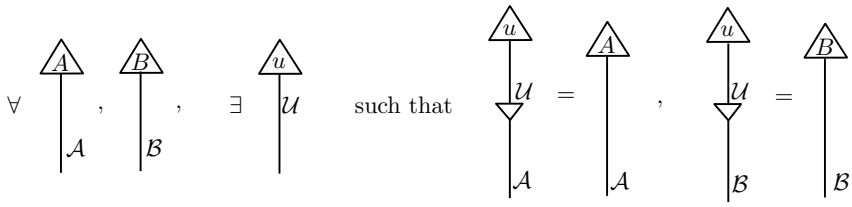
can be abstracted to the diagrammatic representation in the following way:



(5.10)

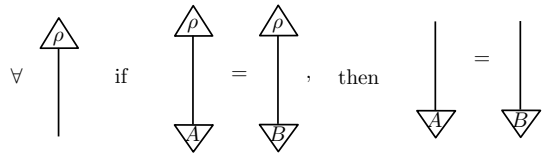
Proof. We can follow CBH proof step-by-step and construct the same proof diagrammatically. Firstly, let's define the independence using the graphical language. Note that the definition of the operator T_A by CBH is $T_A : u \to \sum_{i=1}^{n} E_i^{\frac{1}{2}} u E_i^{\frac{1}{2}}$. However, we will stick to this definition while discussing CBH proof only.

$\forall A \in \mathcal{A}$ and $\forall B \in \mathcal{B}$, $\exists u \in \mathcal{A} \vee \mathcal{B}$ such that $u|_{\mathcal{A}} = A$ and $u|_{\mathcal{B}} = B$:



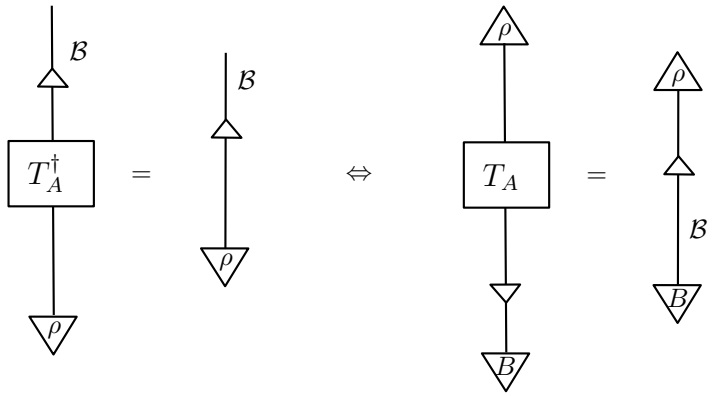
(5.11)

$\forall A \in \mathcal{A}$ and $\forall B \in \mathcal{B}$ and for all states ρ if $\rho(A) = \rho(B)$, then $A = B$:



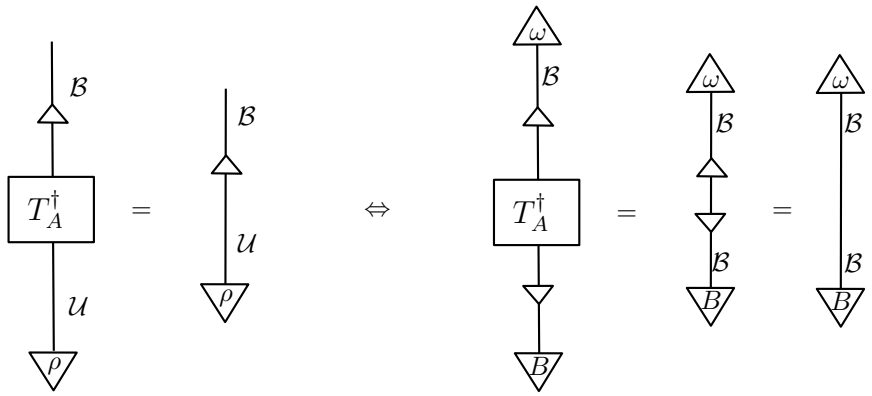
(5.12)

$(T^*\rho)|_{\mathcal{B}} = \rho|_{\mathcal{B}}$ for $\forall u \in \mathcal{U} \Leftrightarrow \rho(T(B)) = \rho(B)\ \forall B \in \mathcal{B}$. *-involution is †-structure in our case:

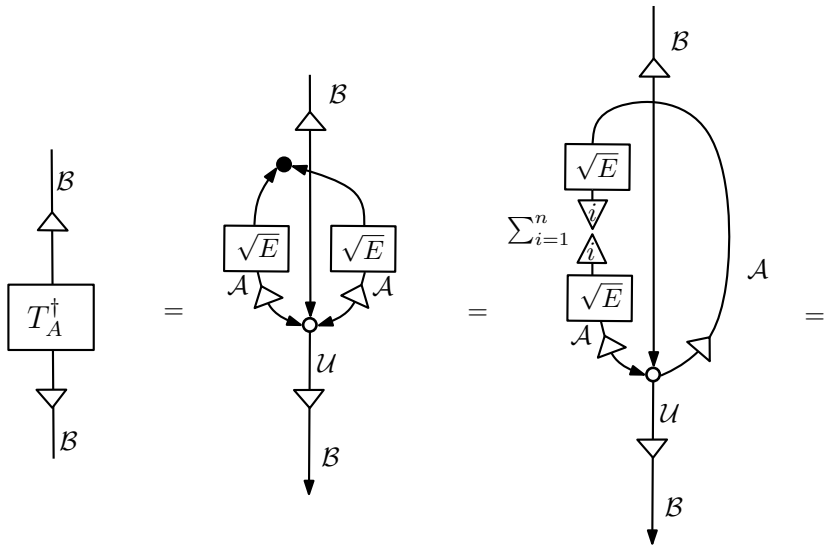


(5.13)

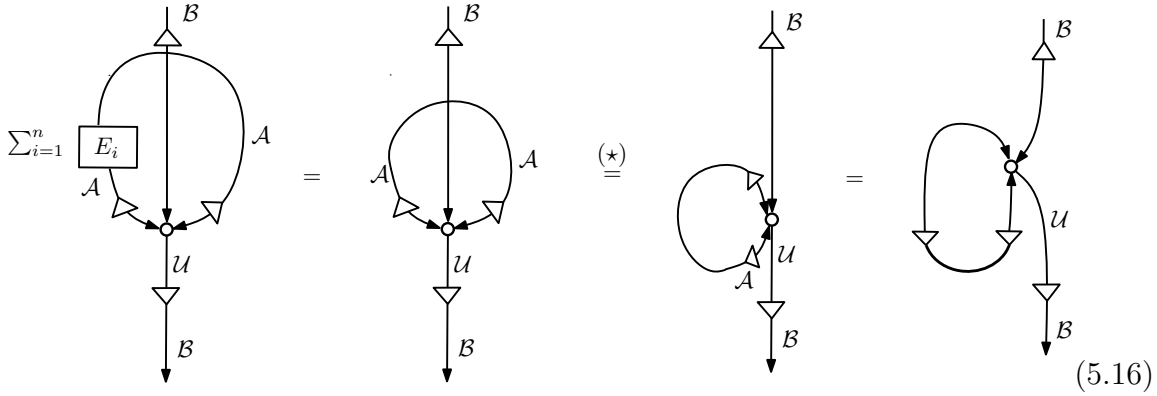
And since all states of $\mathcal{B}$ are restrictions of $\mathcal{U}$, or all states $\omega \in \mathcal{B}$:



(5.14)



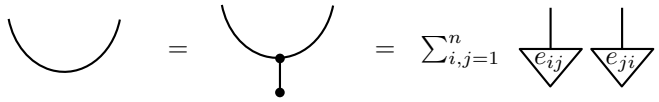
(5.15)



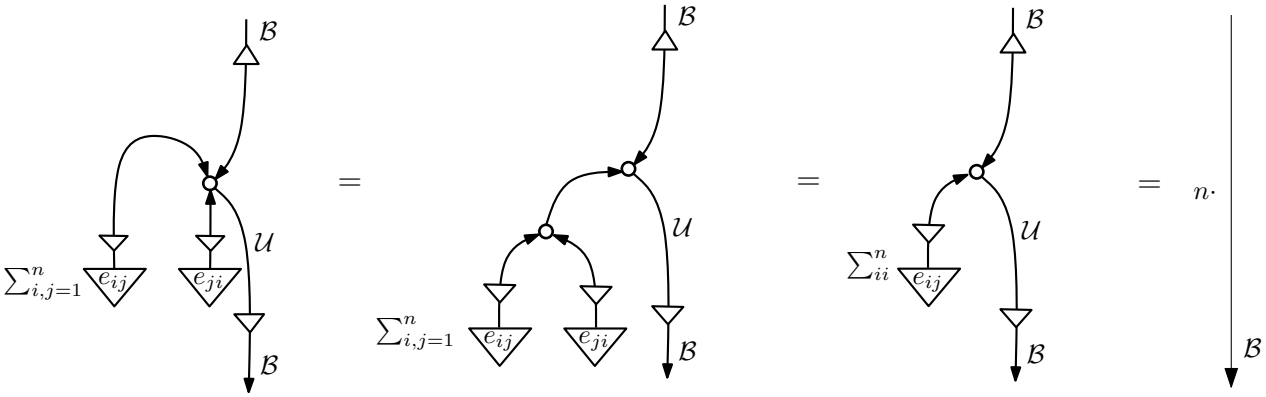
(5.16)

An equality $(\star)$ uses the independence condition – commutativity of observables of type $\mathcal{A}$ and $\mathcal{B}$. This gives us a possibility to slide the circle entirely on the left or right side as displayed in the image above.

To continue derivation, we need to use the fact that we are working in **FHilb**:

$\mathcal{A} = \mathbb{M}_n \Rightarrow$  For more detailed derivation see [2]

So, (5.17)

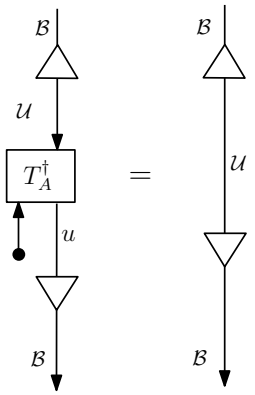


Now it is time to switch to the measurement operator which we have defined and demonstrated that it is completely positive:

$$T_A^\dagger : \langle i| \otimes u \to u$$

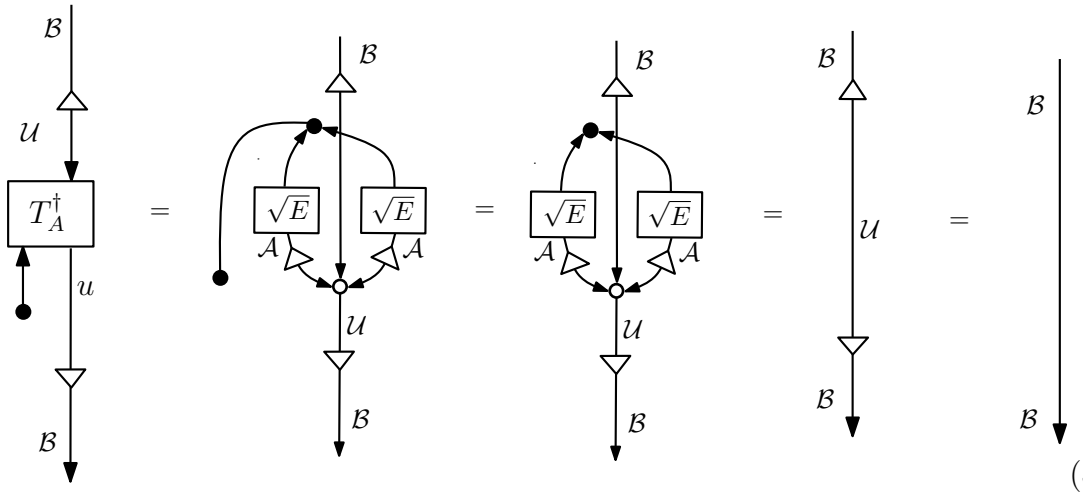
Note that we have swapped the order of input types for this operator for the reason discussed above.

So, the following diagram describes that Alice's measurement cannot influence Bob's system in **FHilb**. This representation entirely captures CBH derivation.



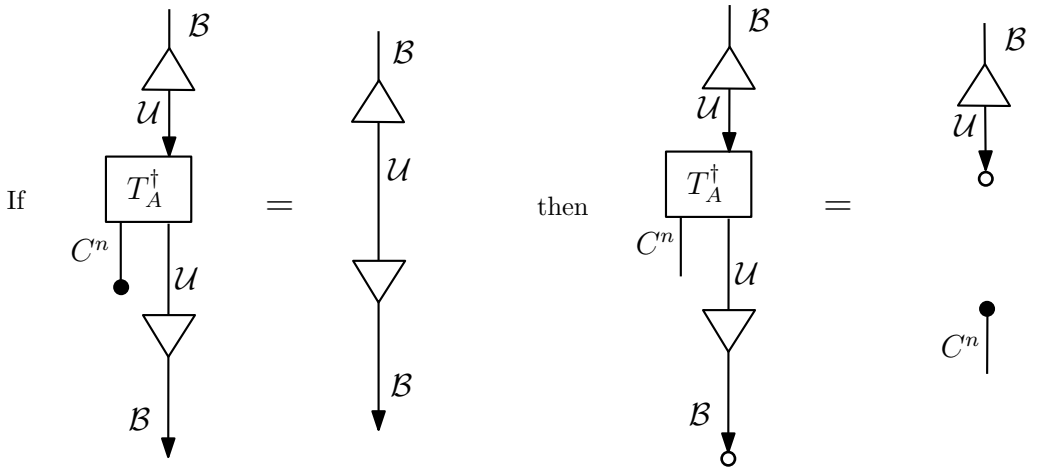
(5.18)

The derivation is very similar to the previous one, we will only demonstrate that adding Alice's classical data as an input to Bob's system, does not effect the system. We will call this equation *"Alice to Bob no-signaling condition"*.



(5.19)

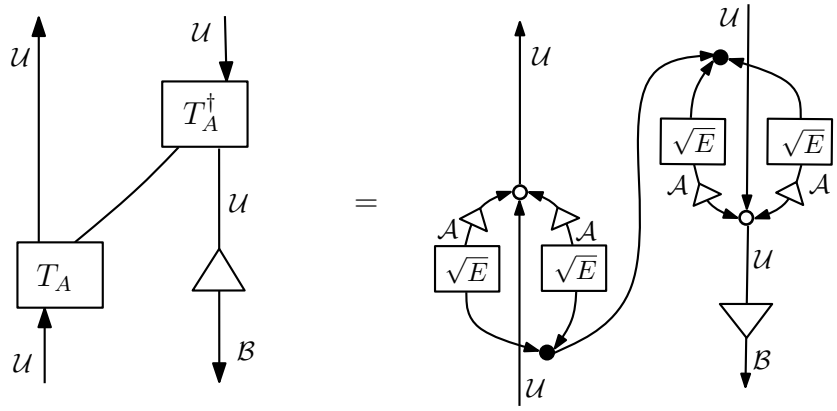
It is a natural thought that this image is very similar to the condition part of implication in the Heisenberg Principle which we discussed in Chapter 2. We know that it is indeed always valid in **FHild**. However, the question raises if we can prove validity of this construction in **Rel**? Our expectation should be that like in the case of the Heisenberg Principle, we should be able to find a counterexample in **Rel** when looking at the following construction:



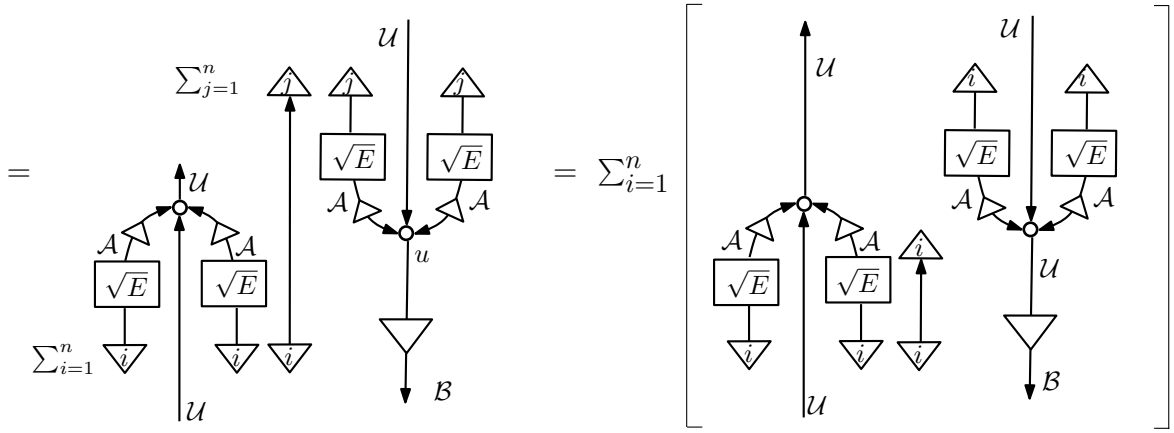
(5.20)

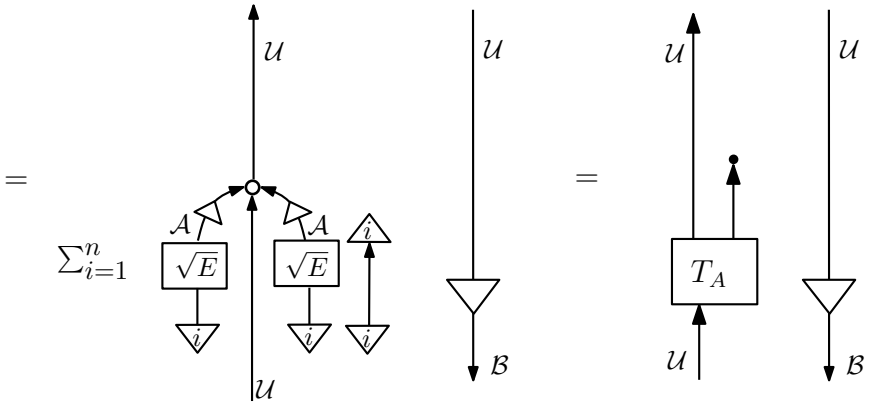
We will explore this bit later in 4.3.4. But let us first go on with the proof and see how the derivations in (5.19) fit into the bigger construction.

Let's add one more component to this scenario – Alice's measurement on system $u \in \mathcal{A} \vee \mathcal{B}$. So, Alice makes a measurement and send her outcome to Bob. We will see that this does not affect Bob's side of the measurement at all. On the other hand this gives us chance to engage the both directions of signaling within one diagram:



(5.21)

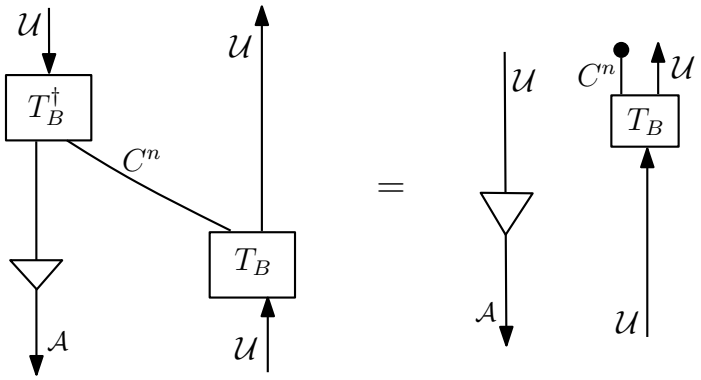




□

Now it is time to switch the roles: Bob makes a measurement on a joint system and send his outcome to Alice. Like the previous scenario, here Alice should not notice the change in her outcome regardless to Bob's measurement. $T_B(u) = \sum_{j=1}^{n} |j\rangle \otimes F_j^{1/2} u F_j^{1/2}$, where $\sum_{j=1}^{n} F_j = \mathbb{I}$ and F_j is Bob's positive operator. We have to show that $T_B^{\dagger}(A \otimes 1) = A$. Here $T_B^{\dagger}$ also encapsulates swap map $\sigma : 1 \otimes A \to A \otimes 1$.

Theorem 5.2.2. No superluminal information transfer between Alice and Bob via Bob's measurement in presence of kinematic independence of physical observables can be abstracted to the diagrammatic representation in the following way:



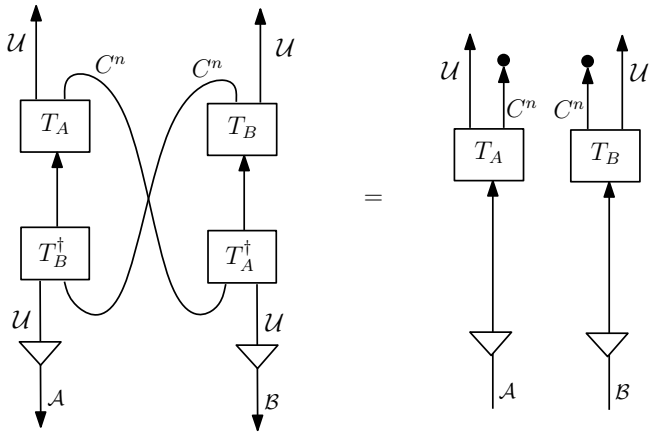
(5.22)

Proof. The set up for this proof is analogous to the proof of theorem 4.3.3.1. So, we can go ahead and directly call this bit – *"Bob to Alice no-signaling condition"*.

□

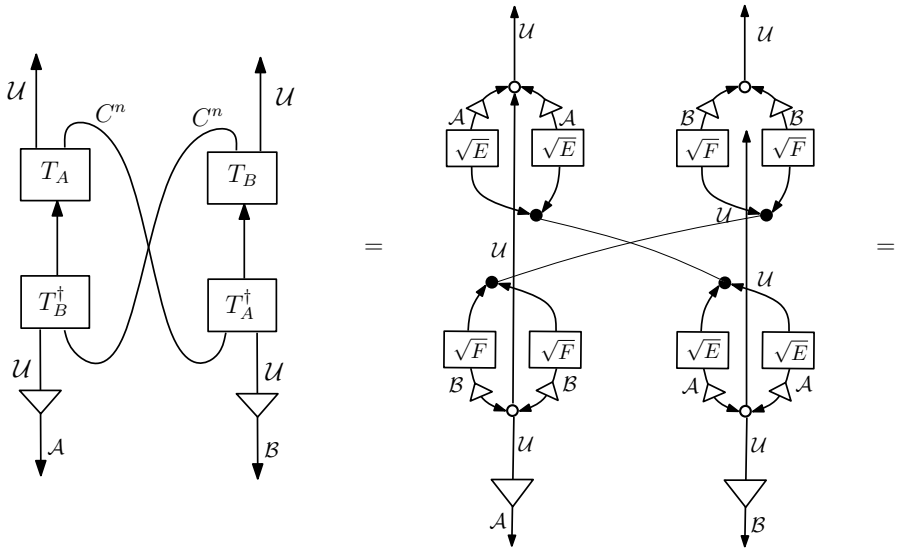
For the final step, we will combine *"Alice to Bob no-signaling condition"* and *"Bob to Alice no-signaling condition"* together. Now Alice and Bob hold independent systems and they both apply a measurement operator to their system (Alice to $\mathcal{A}$ and Bob to $\mathcal{B}$) and afterwards, they send their outcome to each other. As you might already expect Alice cannot signal to Bob and other way around as well, Bob cannot steer Alice's system via measuring his own system.

Theorem 5.2.3. No superluminal information transfer via making a measurement between two kinematically independent systems can be described using a following diagrammatic representation:

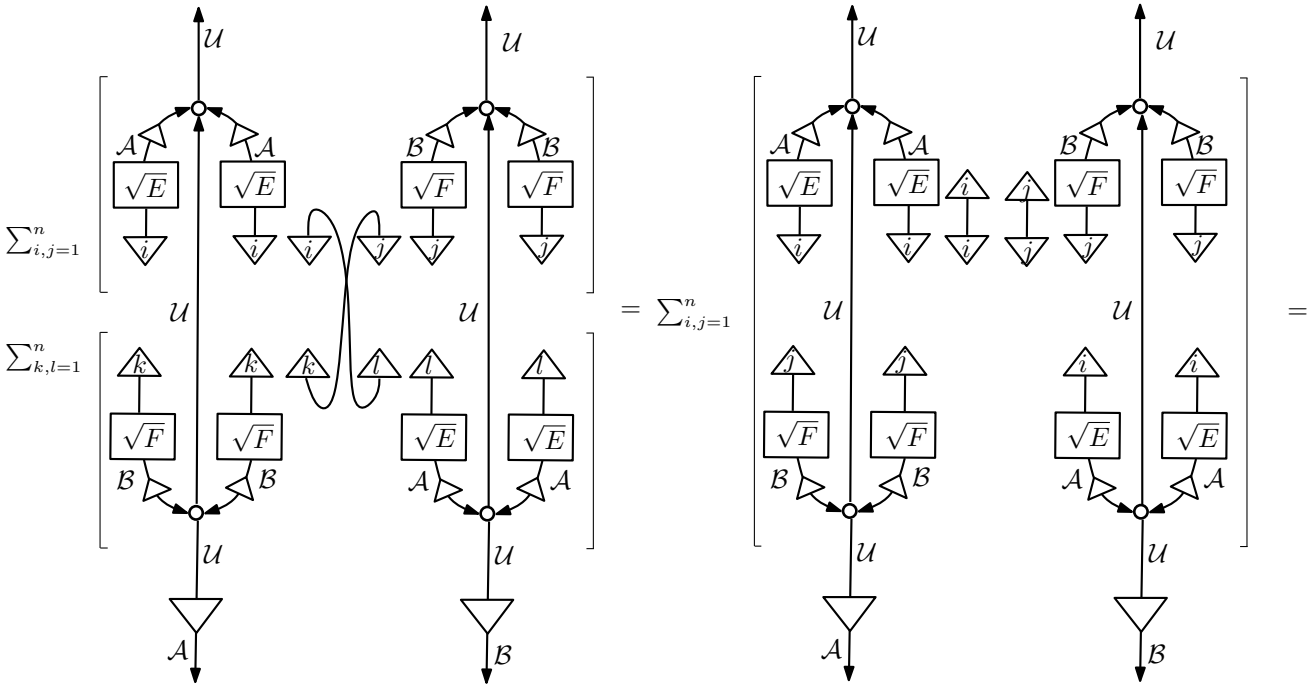


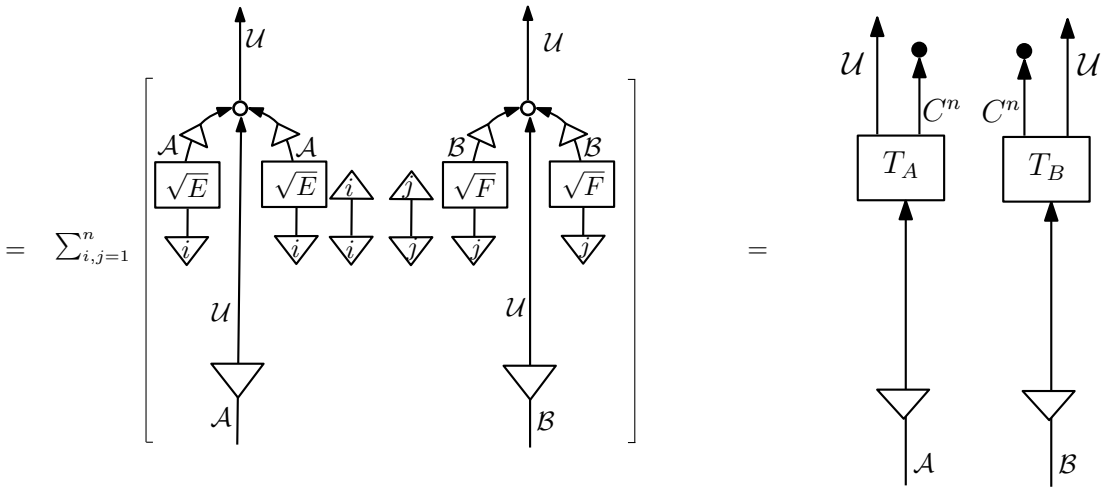
(5.23)

Proof. It is trivial to demonstrate that this equality actually holds. We have worked out all beats of this diagram one-by-one, so this definition simply combines them all together.



(5.24)



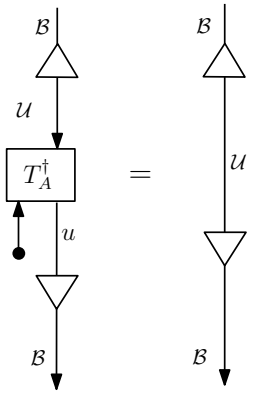


This completes the proof.

□

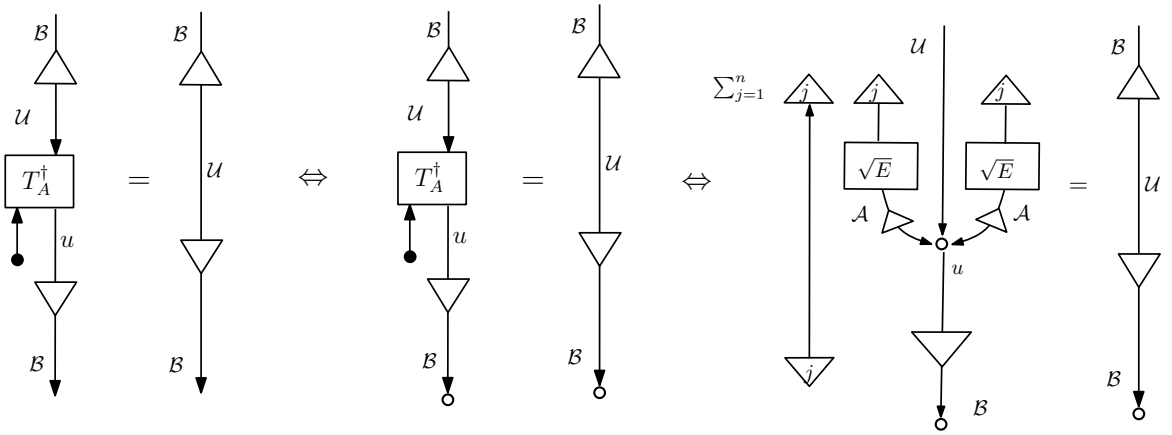
5.3. **Kinematic Independence ⇒ No-signaling in Rel Diagrammatically.** As we have abstracted CBH's independence ⇒ no-signaling implication to graphical reasoning and we have demonstrated its validity in **FHilb**. Now it is time to observe its behavior in **Rel**.

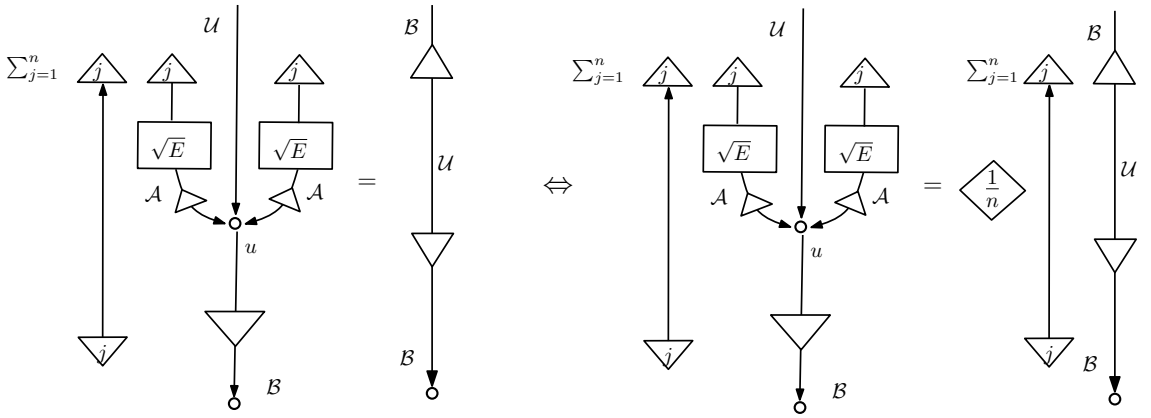
Theorem 5.3.1. The following diagrammatic equation does not always hold in **Rel** (assuming that Alice and Bob have independent observables):

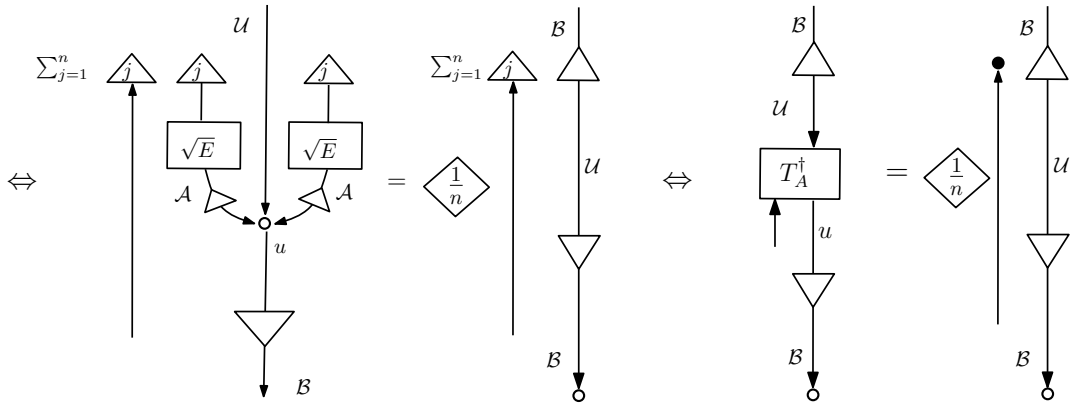


(5.25)

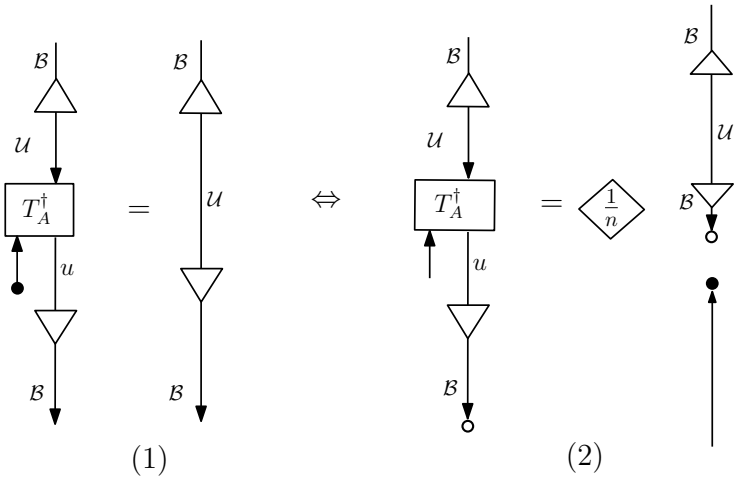
Proof. The above diagram is analogous to the left-hand side of the implication of the Heisenberg Principle. With a simple derivation we get the consequence part as well:







We get the final correspondence:



(1) (2) (5.26)

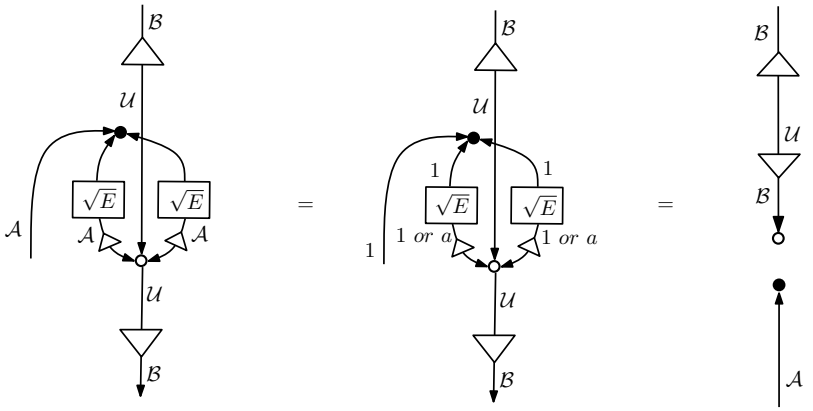
This is an exact duplicate of the Heisenberg Principle. Besides, we know it holds in **FHilb** as we saw in chapter 2 that the Heisenberg Principle works in **FHilb**. However, if we change the working category to **Rel**, we know that from (5.26), (2) does not always hold. And since we have demonstrated that (1) is equivalent to (2), (1) does not always hold as well.

□

Example 4.3.4.2: The Specific counterexample of (2) is very similar to the one demonstrated in chapter 2:

$\mathcal{A} := \{a, 1\}$ such that $a.a = 1$, $1.1 = 1$ and $a.1 = 1.a = a$
$\mathcal{B} := \{b, 2\}$

$\sqrt{E} := \{(\mathcal{A}, \mathcal{A}) \mid (a, 1), (1, 1)\}$



(3) (4) (5.27)

The only possible input in the equation (3) of (5.27) is 1. However, in (4) options are either a or 1. So, the equation does not hold in **Rel**.

Thus, CBH construction that the kinematic independence $\Rightarrow$ no superluminal information transfer via making a measurement does not hold in a general dagger compact category. Now it is time to explore the converse direction of the correspondence.

6. No-signaling ⇒ Kinematic Independence

6.1. **No-signaling ⇒ Kinematic Independence by CBH.** Now it is time to investigate the converse direction of the correspondence: If Alice cannot signal to Bob via making a measurement on her own system, is it always the case that Alice and Bob are holding independent systems? This question is addressed in [4] as follows:

State of the system is $U \in \mathcal{A} \vee \mathcal{B}$ where $\mathcal{A}$ and $\mathcal{B}$ are $C^* - algebras$ corresponding to Alice's and Bob's subsystems respectively. C^*-algebras are spanned by their effects (positive operators), the simplest POVM is defined as follows:

$$T_A(U) = E^{1/2}UE^{1/2} + (I-E)^{1/2}U(I-E)^{1/2},$$

where E is some effect in $\mathcal{A}$. Note that this is a concrete version of an equation $T_A(U) = \sum_{i=1}^{n} E_i^{1/2}UE_i^{1/2}$ for $n = 2$. We need to show that if an operator $B \in \mathcal{B}$ is self-adjoint, then $T_A(B) = B$ entails that $[E, B] = 0$.

Theorem 6.1.1. $T_A(B) = B$ for all effects $E \in \mathcal{A}$ and for all self-adjoint operators $B \in \mathcal{B}$ only if $\mathcal{A}$ and $\mathcal{B}$ are kinematically independent.

Proof.

$B = T_A(B) \;\; = E^{1/2}BE^{1/2} + (I-E)^{1/2}B(I-E)^{1/2}$

It is easy to see that: $E^{1/2}BE^{1/2} = B - (I-E)^{1/2}B(I-E)^{1/2}$

Substituting $E^{1/2}BE^{1/2} + (I-E)^{1/2}B(I-E)^{1/2}$ for B, we get :

$$\begin{aligned} E^{1/2}BE^{1/2} &= B - (I-E)^{1/2}(E^{1/2}BE^{1/2} + (I-E)^{1/2}B(I-E)^{1/2})(I-E)^{1/2} \\ &= B - (I-E)^{1/2}E^{1/2}BE^{1/2}(I-E)^{1/2} + (I-E)B(I-E) \\ &= -E^{1/2}(B - E^{1/2}BE^{1/2})E^{1/2} + BE + EB + EBE \\ &= -E^{1/2}BE^{1/2} + BE + EB \end{aligned}$$

So we get,

$[E^{1/1}, [E^{1/2}, B]] = 2E^{1/2}BE^{1/2} - BE - EB = 0.$

Let the map $d : \mathcal{U} \to \mathcal{U}$ be a bounded derivation on an unital C^*-algebra $\mathcal{A} \vee \mathcal{B}$. Then a derivation d precisely acts on B as follows:

$$d : B \to i[E^{1/2}, B].$$

So, $d^2B = 0 \;\Rightarrow\; dB$ is quasi-nilpotent i.e its spectrum is $\{0\}$ [9], which means that an operator dB has no non-zero eigenvalues. And since B is a self-adjoint operator, all its

eigenvalues are real and it can be diagonalized (According to the finite-dimensional spectral theorem, however only concerning **FHilb**, e.g. an operator represented as a Hermitian Matrix).

Thus, $dB = [E^{1/2}, B] = 0$, E and B commute for all $E \in \mathcal{A}$ and $B \in \mathcal{B}$. Since a C^*-algebra is spanned by its effects, $\mathcal{A}$ and $\mathcal{B}$ are kinematically independent.

□

6.2. **No-signaling ⇒ Kinematic Independence in Rel (try #1).** As we have the counterexample showing that independence does not always entail no-signaling, it is natural to think that investigating the converse direction in **Rel** might give us some interesting results. We start solving the problem by carefully going through the CBH proof and trying to discover the structure that might cause an existence of some counterexample. The first and most obvious candidate would be the spectral theorem used in the very last bit to prove the Theorem 6.1.1. Knowing that differently from in **FHilb**, in **Rel** not all the normal operators are internally diagonalisable, this seems to be a good point to start.

Let us take B to be a two element set. So, in II element set there are total $2^4 = 16$ operators which can be represented by matrices. It is easy to verify that only 9 matrices are normal. However, out of these 9 operators, only 5 are internally diagonalisable [7]. We are most interested in the rest 4 operators:

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

As we need $\mathcal{B}$ to be a self-adjoint operator, we are left with only 2 possibilities:

$$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

Without a loss of generality, we can pick one of these two operators. e.g. $B_1 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$ which clearly can be written as the relation $S := \{(0,1),(1,0),(1,1)\}$. We also know that our choice of an operator B must be positive.

Note that the relation R is positive if and only if R is symmetric and $b_1 R b_2 \Rightarrow b_1 R b_1$[8]. So, the relation S is not positive unless we add a pair $(0,0)$. This means now the relation S describes the matrix: $\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$.

The set of all possible matrices representing Bob's positive operator are:

$$X := \left\{ \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\}.$$

All of the four matrices are internally diagonalisable [7]. So, it it apparent we cannot discover a counterexample by employing the spectrum theorem in **Rel** in 2×2 matrices.

Now, let us take $\mathcal{B}$ to be a three element set. So, in a III element case we have $2^9 = 512$ operators. Like in the II element case, we are only interested in the positive ones. Our goal is to see if any of the matrices representing a positive operator is normal and cannot be internally diagonalisable. In a III element set, we denote all positive operators' matrices as X. The elements of a set$X$ are:

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

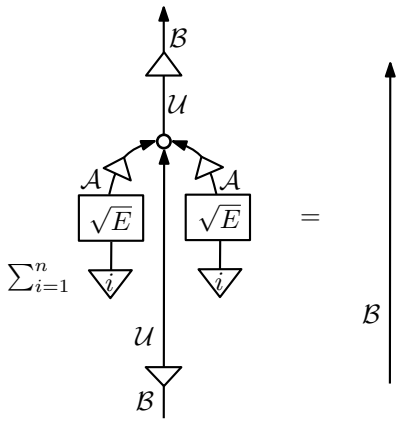
$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

[7] lists all the normal and internally diagonalisable 3×3 matrices, which includes all element of the set X. Thus we cannot find a counterexample in by looking at the spectrum theorem in 3×3 matrices in **Rel**.

Increasing the size of the set $\mathcal{B}$ increases the number of computations exponentially. For a IV element set the number possible operators is $2^{16} = 65536$. So, we think that further work to find a counterexample using this method is infeasible. Instead, we propose to use some bits of diagrammatic language that we developed.

6.3. **No-signaling $\Rightarrow$ Kinematic Independence in Rel (try #2).** As the Theorem 6.1.1. claims if $T_A(B) = B$ then $\mathcal{A}$ and $\mathcal{B}$ should be independent for all effects $E \in \mathcal{A}$

and for all self-adjoint operators $B \in \mathcal{B}$. Diagrammatically as expected, the left-hand side looks as follows:



(6.1)

Recall that , normalisable dagger Frobenius algebras in **Rel** are groupoids.

The plan of attack for discovering a counterexample is following: First choose $\mathcal{U}$ to be a non-abelian groupoid. Then fix $\mathcal{A}$ and $\mathcal{B}$ to be it's sub-groupoids such that they do not commute. Having all this, if the diagrammatic equation holds, we have found a counterexample.

The smallest non-abelian group we can take has 6 elements (Dihedral group of order 6) and is the symmetric group of degree 3, with notation S_3. Let's construct this group:

Set three objects: Red(R), Green(G), Blue(B) . Initially place them in the order RGB. Define three types of swap maps over this order: e:RGB→RGB as an identity map, $a : RGB \to GRb$ swaps the first element with second and $b : RGB \to RBG$, a map which swaps the second and third elements.

The multiplication structure works as a regular composition of two maps: $ab : RGB \to BRG$. First acts b and after a. Besides, $ba : RGB \to GBR$. So, $ab \neq ba$. We write the six permutations of the set of three objects as the following actions:

$e : RGB \to RGB$ OR ()
$a : RGB \to GRB$ OR (RG)
$b : RGB \to RBG$ OR (GB)
$ab : RGB \to BRG$ OR (RGB)
$ba : RGB \to GBR$ OR (RGB)
$aba : RGB \to BBR$ OR (RB)

It is easy to check that this structure is indeed a groupoid. i.e. each structure has an inverse.

$$ee = e \qquad (ab)(ba) = aea = aa = e$$
$$aa = e \qquad (ba)(ab) = beb = bb = e$$
$$bb = e \qquad (aba)(aba) = abeba = abba = aea = aa = e$$

The cycle graph of S_3 looks following [14]):

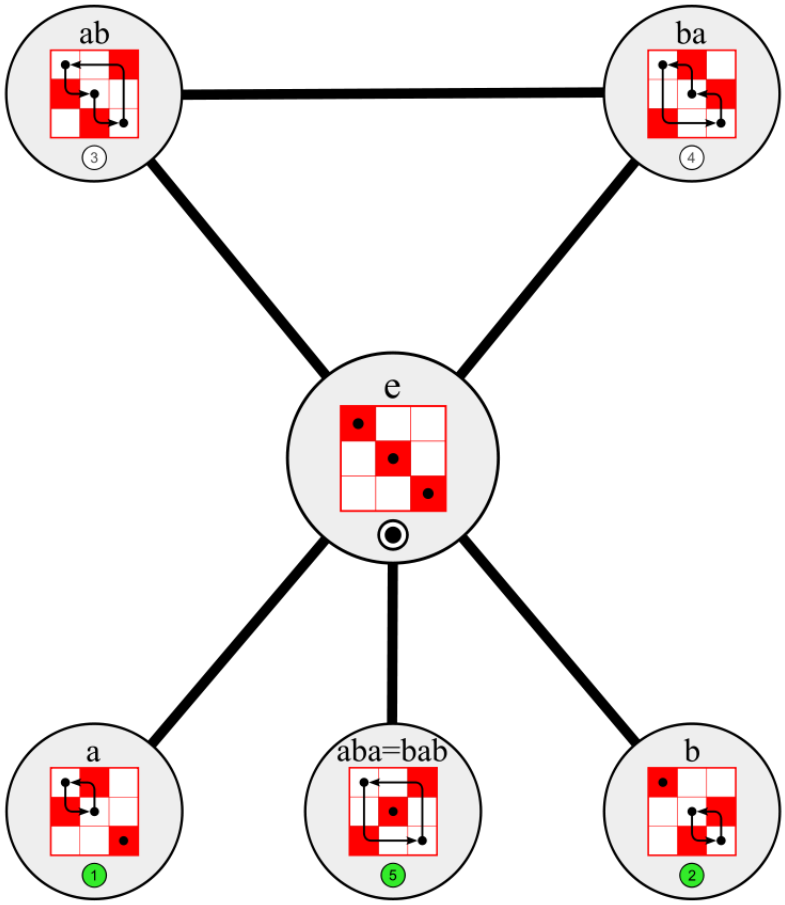


Image 6.2. Cycle graph of S_3

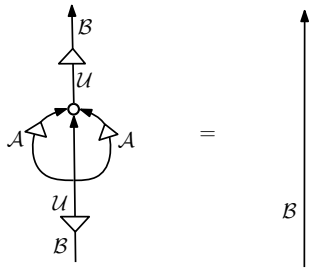
Let us denote $c := aba$, $d := ab$, $f : ba$ and summarize group operations using Cayley table [14]:

Table 6.3. Multiplication on S_3

$*$	e	a	b	c	d	f
e	e	a	b	c	d	e
a	a	e	d	f	b	c
b	b	f	e	d	c	a
c	c	d	f	e	a	b
d	d	c	a	b	f	e
f	f	b	c	a	e	d

Theorem 6.3.1. $T_A(B) = B$ holds only if $\mathcal{A}$ and $\mathcal{B}$ commute, when $\mathcal{A}, \mathcal{B} \subseteq \mathcal{U}$ and $\mathcal{U}$ is a non-abelian symmetric group S_3.

Proof. An expression $T_A(B) = B$ after simplification looks as follows :



(6.4)

The equality to hold, we need $B = ABA$ for all $B \in \mathcal{B}$ and $A \in \mathcal{A}$
Note that, the subgroups $\mathcal{A}$ and $\mathcal{B}$ contain an identity element e. So, when $B = e$,

$$e = AeA \text{ entails that } AA = e.$$

This leaves us with only 3 options for $\mathcal{A}$:= $\{a, e\}, \{b, e\}$ or $\{aba, e\}$.

We can exhaustively choose all possible elements for B and show that when $\mathcal{A}$ and $\mathcal{B}$ do not commute, $T_A(B) \neq B$.

#1	$B = a$ and $A = b$:	$ABA = aba = c \neq a$
	$B = a$ and $A = aba$:	$ABA = abaaaba = ababa = dc = cf = b \neq a$
#2	$B = b$ and $A = a$:	$ABA = bab = bd = fb = c \neq b$
	$B = b$ and $A = aba$:	$ABA = abababa = cff = cd = a \neq b$
#3	$B = aba$ and $A = a$:	$ABA = aabaa = b \neq aba$
	$B = aba$ and $A = b$:	$ABA = babab = cd = a \neq aba$
#4	$B = ab$ and $A = a$:	$ABA = aaba = ba \neq ab$
	$B = ab$ and $A = b$:	$ABA = babb = ba \neq ab$
	$B = ab$ and $A = aba$:	$ABA = ababaab = aba \neq ab$

Note that by including $ab \in \mathcal{B}$, ba automatically is in $\mathcal{B}$ as they are inverses of each other and $\mathcal{B}$ is a groupoid.

So, we cannot find any non-commutative $\mathcal{A}$, $\mathcal{B} \in \mathcal{U} \equiv S_3$ such that $T(B) = B$.

□

Our next trial was checking the quaternion group (which is a non-abelian group of order 8 and it is denoted as Q_8) and the symmetry group of a square, a dihedral group of order 8 (Dih_4).

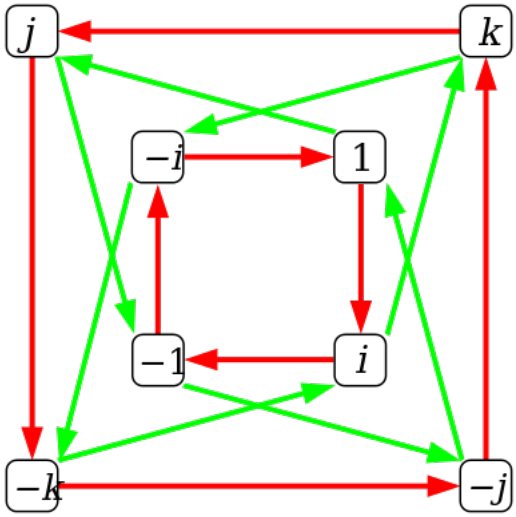
$$\mathrm{Q} = \langle -1, i, j, k \mid (-1)^2 = 1,\ i^2 = j^2 = k^2 = ijk = -1 \rangle,$$

1 is an identity element of the group and -1 commutes with other elements of the group.

Table 6.4. Multiplication on Q_8

$*$	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

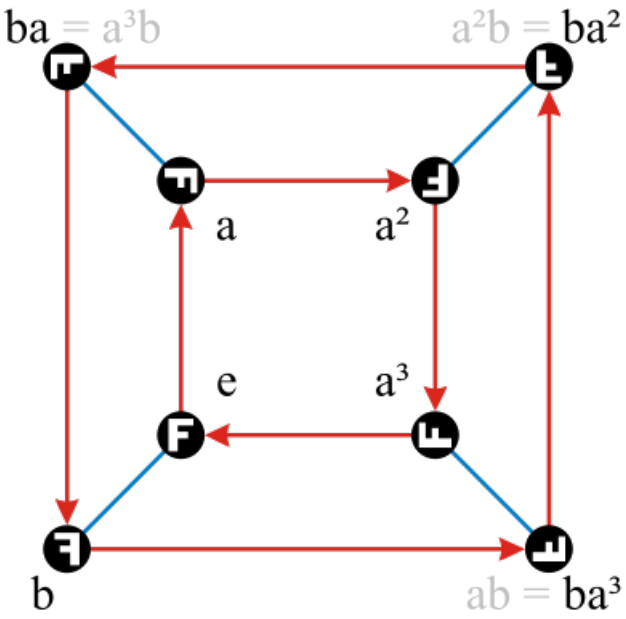
While diagrammatically the Cayley graph looks as follows [15]



6.5. Cayley graph Q_8.

The red arrows represent multiplication on the right by i, and the green arrows represent multiplication on the right by j.

Next example is Dih_4. Its Cayley graph is [15]:



6.6. Cayley graph Dih_4.

Dih_4 is called to be the group of translations of the plane, where $a,$ and b define the direction and length of the movement in the place. Such as:

$e \equiv ()$
$a \equiv$ "move $\nearrow$ for 3 miles";
$b \equiv$ "move $\searrow$ for 4 miles";
and $a \circ b \equiv$ "move $\longrightarrow$ for 5 miles" (Pythagorean theorem). (6.6) exhausts all the possible permutations of the movements in the plane, which can me defined using $e,$ $a,$ and b.

Theorem 6.3.2 $T_A(B) = B$ holds only if $\mathcal{A}$ and $\mathcal{B}$ commute, when $\mathcal{A}, \mathcal{B} \subseteq \mathcal{U}$ and $\mathcal{U}$ is either Dih_4 or the quaternion group Q_8, as defined above .

Proof. The proof of this theorem is analogous to the proof of the Therem 6.3.1. □

7. Discussion

7.1. **Summary.** We introduced the number of sufficient categorical concepts for being able to express quantum mechanics in a dagger compact category. In the background part, we also gave an overview of the graphical calculus, describing features of quantum mechanics. Our running examples of a dagger compact category were a category of finite dimensional Hilbert spaces and a category of sets and relations. Afterwards, we made a connection between the algebras of observables, expressed as finite dimensional C^*-algebras, and normalisable dagger Frobenius algebras. Consequently, we raised existing structure to fully abstract procedure, called the CP^*–construction that turns any dagger compact category (like **FHilb**) into the category of abstract C*-algebras with abstract completely positive maps. Afterwards, we used the CP^*-construction to show that the Heisenberg Principle has the counterexample in **Rel**. The proof was entirely diagrammatic.

The biggest part of our work was devoted to the abstraction of the information-theoretic constrains presented in [4] to CP^*-construction, so that we could reason about them diagrammatically. We reviewed 'No secure bit commitment' in details. [5] We saw that having the unconditionally secure bit commitment protocol is actually possible in **Rel**.

As out novel work, we chose the correspondence between no-signaling and kinematic independence of two distinct physical systems. We thought that this would be a logical continuation after finding the counterexample in the Heisenberg Principle. At first, we demonstrated that the spectral theorem in **Rel** works quite differently from the on in **FHilb**. So, we concluded that the simultaneous diagonalisability is not the precise tool to distinguish whether two observables are independent. Thus, we used the commutativity of observables as a condition of independence and we demonstrated that the 1-to-1 correspondence fails in **Rel**. Namely, we proved that while working in the category of sets and relations, the kinematic independence of two observables do not always entail the o-signaling property.

We tried to find a counterexample to show that the no-signaling property does not always entail the kinematic-independence. The proof in [4] used the spectrum theorem. Thus, knowing that in **Rel** the spectrum theorem looks quite different from the one in **FHilb** , we were hoping to detect some contradiction. However, the structure of observables Clifton et al. used in their proof was strong enough not to give us this opportunity.

In the end, we looked at the smallest non-abelian groups such as S_3, quaternion and Dih_4 and tried to take their non-commutative sub-groupoids. If such construction would allow no-signaling, it would be a counterexample. However, this was not the case in these

non-abelian groups.

7.2. **Future Work.** In this dissertation, we have demonstrated that no-signaling $\Leftrightarrow$ independence does not always hold. We have done this in one direction only. The converse implication can be investigated further in order to firmly state whether the no-signaling property can entail the kinematic independence in a general dagger compact category. Unfortunately, we do not think that there is a well-defined structure, which will be good enough to reason about it in a general category. Thus, more work can be done to first, explore more concrete group structures and then try to generalize them in more abstract sense:

(1) Check if the Theorem 6.3.1 is valid for every symmetric group S_n on elements:
If $\mathcal{U} \equiv S_n \Rightarrow$ No counterexample;
(2) We can embed any group into the symmetric one and strengthen the conclusion:
If $\mathcal{U}$ is a group $\Rightarrow$ No counterexample;
(3) Check if the non-commuting sub-groupoids cannot be just sub-groups and if they have to overlap, then:
If $\mathcal{U}$ is a groupoid $\Rightarrow$ No counterexample.

References

[1] Aleks Kissinger Bob Coecke. Quantum computer science lecture notes.

[2] Aleks Kissinger Bob Coecke, Chris Heunen. Categories of quantum and classical channels. 16 May 2013.

[3] Dusko Pavlovic Bob Coecke and Jamie Vicary. A new description of orthogonal bases. 2008.

[4] Jeffrey Bub Clifton Rob and Hans Halvorson. Characterizing quantum theory in terms of information-theoretic constraints. *Foundations of Physics*, 33.11 (2003):.

[5] Katriel Cohn-Gordon. Commitment algorithms. Master's thesis, University of Oxford, 2012.

[6] Martin Florig and Stephen J. Summers. On the statistical independence of algebras of observables. *Journal of Mathematical Physics*, 1997.

[7] Thanasis Georgiou. Quantum operators: A classical perspective. Master's thesis, Oxford University Computing Laboratory, 2009.

[8] Chris Heunen and Jamie Vicary. Introduction to categorical quantum mechanics.

[9] P. Busch J. Singh. Luders theorem for unsharp quantum measurements. *PHYSICS LETTERS*, 1998.

[10] Hans Maassen. Quantum probability quantum information theory quantum computing. Lecture notes of a course to be given in the spring semester of 2004 at the Catholic University of Nijmegen, the Netherlands.

[11] Dominic Mayers. Unconditionally secure quantum bit commitment is impossible.

[12] M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[13] Jamie Vicary. Categorical formulation of finite-dimensional quantum algebras. *Communica- tions in Mathematical Physics*, 2011.

[14] Wikipedia. Dihedral group of order 6. 2014.

[15] Wikipedia. Quaternion group. 2014.