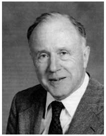
Can quantum theory be characterized in terms of information-theoretic constraints?

Chris Heunen
Aleks Kissinger

THE UNIVERSITY of EDINBURGH informatics
Radboud University

arXiv.org:1604.05948



“*Information, physics, quantum: the search for links*”
Complexity, Entropy, and the Physics of Information (Zurek), 1990.

It from bit symbolizes the idea that every item of the physical world has at bottom – a very deep bottom, in most instances – an immaterial source and explanation; that which we call reality arises in the last analysis from the posing of yes-no questions and the registering of equipment-evoked responses; in short, that all things physical are information-theoretic in origin and that this is a participatory universe.

Yes if traditional setting is generalized to operational probabilistic theories by retaining only probabilistic data as convex structure.

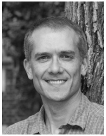
"*Quantum theory from five reasonable axioms*"
arXiv:quant-ph/0101012, 2001.


"*A derivation of quantum theory from physical requirements*"
New Journal of Physics 13(6):063001, 2011.



"*Informational derivation of quantum theory*"
Physical Review A 84(1):012311, 2011.

Yes if retain only the algebraic structure of interaction between classical and quantum systems.

"*Characterizing quantum theory in terms of information-theoretic constraints*"
Foundations of Physics 33(11):1561–1591, 2003.

"*Elegance and Enigma: the quantum interviews*"
ed: M. Schlosshauer, p. 204, 2011.

The characterization theorem we proved assumes a C-algebraic framework for physical theories, which I would now regard as not sufficiently general in the relevant sense, even though it includes a broad class of classical and quantum theories, including field theories, and hybrid theories with superselection rules.*

information theory		*quantum theory*
no broadcasting	$\Leftrightarrow$	noncommutativity
no bit commitment	$\Leftrightarrow$	nonlocality
no signalling	$\Leftrightarrow$	kinematic independence

Are there physical means for broadcasting unknown quantum states, pure or mixed, onto two separate quantum systems?

$$\mathrm{Tr}_1(B(\rho)) = \rho = \mathrm{Tr}_2(B(\rho))$$

Are there physical means for committing to a bit value, with the ability to reveal the choice later, securely?

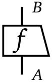
$$\mathrm{reveal}(\mathrm{commit}(x, s)) = x$$
$$\mathrm{cheat}(\mathrm{commit}(x, s)) = \mathrm{cheat}(\mathrm{commit}(y, s))$$

Are there physical means for signalling classical information faster than light?

$$\mathbb{P}(bx|A0) = \mathbb{P}(bx|A1)$$

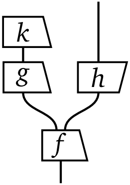
 

"Notation which is useful in private must be given a public value and that it should be provided with a firm theoretical foundation"

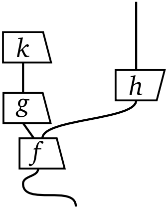
- Morphisms $f: A \to B$ depicted as boxes 

- Composition: stack boxes vertically
- Tensor product: stack boxes horizontally
- Dagger: turn box upside-down

Sound: isotopic diagrams represent equal morphisms

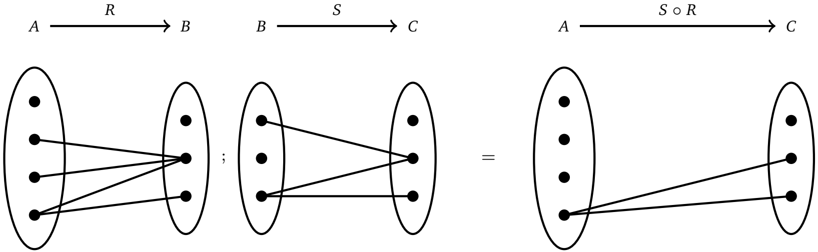


$$= \quad (k \otimes \mathrm{id}) \circ (g \otimes h^\dagger) \circ f \quad =$$

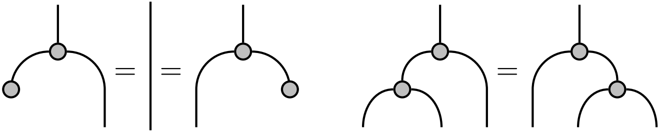


Complete: diagrams isotopic iff equal in category of Hilbert spaces

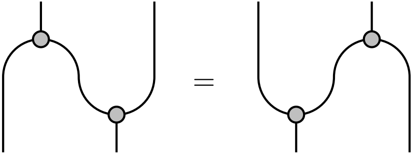
A relation $A \xrightarrow{R} B$ between sets is a subset $R \subseteq A \times B$



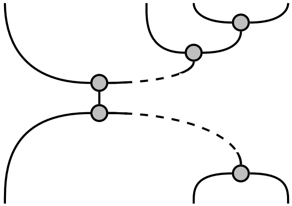
Draw  for multiplication $A \otimes A \to A$



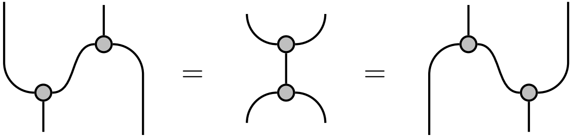
Frobenius law:

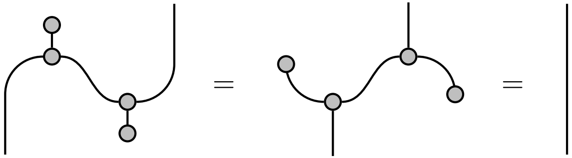


Any connected diagram built from the components of a special ( = |) Frobenius structure equals the following normal form:

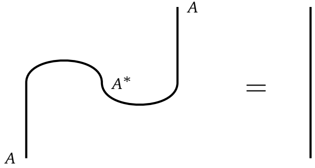


In particular:





So any Frobenius structure is self-dual



- Let G be the set of objects of a small groupoid.

$$\{*\} \mapsto \{\mathrm{id}_A \mid A \in G\} \qquad (f,g) \mapsto \begin{cases} \{f \circ g\} & \text{if } f \circ g \text{ is defined} \\ \emptyset & \text{otherwise} \end{cases}$$

Any dagger Frobenius structure in **Rel** is of this form.

- Let G be the set of objects of a small groupoid.

$$\{*\} \mapsto \{\mathrm{id}_A \mid A \in G\} \qquad (f,g) \mapsto \begin{cases} \{f \circ g\} & \text{if } f \circ g \text{ is defined} \\ \emptyset & \text{otherwise} \end{cases}$$

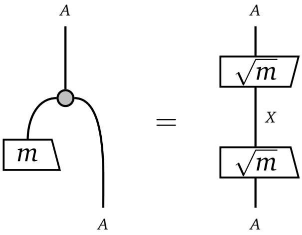
Any dagger Frobenius structure in **Rel** is of this form.

- Let G be the set of objects of a finite groupoid.

$$1 \mapsto \sum_{A \in G} \mathrm{id}_A \qquad f \otimes g \mapsto \begin{cases} f \circ g & \text{if } f \circ g \text{ is defined} \\ 0 & \text{otherwise} \end{cases}$$

Any dagger Frobenius structure in (F)**Hilb** is of this form.

Mixed state of dagger Frobenius structure is $I \xrightarrow{m} A$ with



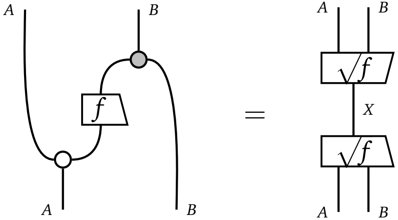
A morphism $f\colon (A, \;) \to (B, \;)$ is completely positive when $f \otimes \mathrm{id}$ preserves mixed states.

- Evolution along unitary $A \to A$
- Preparation of mixed state $I \to A$
- Measurement is $A \to (\mathbb{C}^n, \;)$

A morphism $f\colon (A, \;) \to (B, \;)$ is completely positive when $f \otimes \mathrm{id}$ preserves mixed states.

- Evolution along unitary $A \to A$
- Preparation of mixed state $I \to A$
- Measurement is $A \to (\mathbb{C}^n, \;)$

If and only if CP condition:

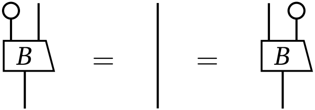


- $\mathrm{CP}[\mathbf{C}] =$ Frobenius structures in $\mathbf{C}$
  and morphisms in $\mathbf{C}$ satisfying CP condition

- $\mathrm{CP}[\mathbf{FHilb}] =$ finite-dimensional C*-algebras
  and completely positive maps

- $\mathrm{CP}[\mathbf{Rel}] =$ small groupoids
  and inverse-respecting relations

Broadcasting map for $(A, \curlywedge)$ in CP[**C**] is morphism $B\colon A \to A \otimes A$ with



- If $(A, \;)$ in CP[**C**] is commutative, then it is broadcastable

- If C*-algebra in CP[**FHilb**] is broadcastable, it is commutative

- If groupoid in CP[**Rel**] is broadcastable, it is totally disconnected
  (the only morphisms are endomorphisms)

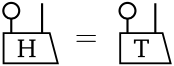
- In general: no broadcasting $\overset{\Rightarrow}{\not\Leftarrow}$ noncommutativity

- Classicality: biproduct of I $\overset{\Rightarrow}{\not\Leftarrow}$ commutative $\overset{\Rightarrow}{\not\Leftarrow}$ broadcastable

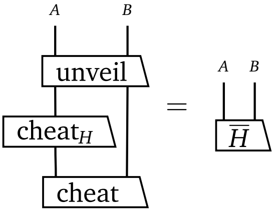
- states $H, T \colon I \to A \otimes B$ of $\mathrm{CP}[\mathbf{C}]$
- monomorphism unveil$\colon A \otimes B \to A \otimes B$ in $\mathrm{CP}[\mathbf{C}]$
- classical $(A \otimes B, \curlywedge)$ in $\mathbf{C}$ with copyable states $\overline{H} \neq \overline{T}$

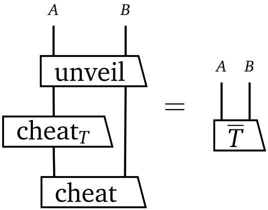
Sound when unveil $\circ\, H = \overline{H}$ and unveil $\circ\, T = \overline{T}$

Binding when $(u \otimes \mathrm{id}_B) \circ H \neq T$ for all $u \colon A \to A$ in $\mathrm{CP}[\mathbf{C}]$

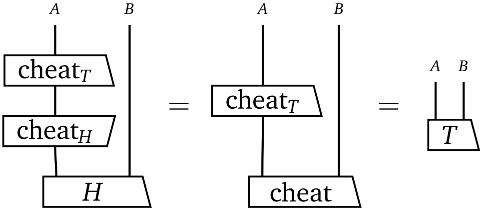
Concealing when 

Alice cannot cheat: if





then not binding:



- Secure bit commitment is impossible in CP[**FHilb**]

- Secure bit commitment is possible in CP[**Rel**]

$$A = \text{discrete groupoid on } \{0, 1, 2\}$$
$$B = \text{discrete groupoid on } \{x, y\}$$
$$H = \{(0, x), (1, y), (2, y)\} \subseteq A \times B$$
$$T = \{(1, y), (0, x), (2, x)\} \subseteq A \times B$$

$$= \mathbb{Z}_3 + \mathbb{Z}_3 \simeq H + T$$

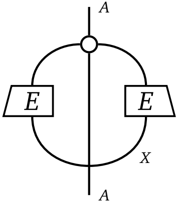
An object in CP[**C**] admits entanglement if there is state $I \to A \otimes B$ not of the form $(f \otimes g) \circ \psi$ for $\psi \colon I \to A' \otimes B'$ with A', B' classical. The category **C** is nonlocal when every object admits entanglement.

- CP[**FHilb**] is nonlocal
- CP[**Rel**] is nonlocal
- In general: no bit commitment $\overset{\not\Rightarrow}{\not\Leftarrow}$ nonlocality

Let $(C, \ )$ be a dagger Frobenius structure in $\mathbf{C}$.
A subsystem is another dagger Frobenius structure $(A, \ )$ with a unital $*$-homomorphism $i \colon A \to C$ satisfying $i^\dagger \circ i = \mathrm{id}_A$.
If is broadcastable, it is a classical context.

- If $C = A \otimes B$, both A and B are subsystems
- If $\mathbf{C} = \mathbf{FHilb}$, subsystems are C*-subalgebras
- If $\mathbf{C} = \mathbf{Rel}$, subsystems are wide subgroupoids

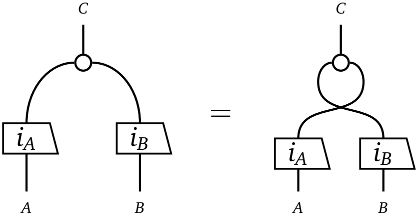
Let $(A, \;)$ be a dagger Frobenius structure in $\mathbf{C}$.
A measurement on $(A, \;)$ is a morphism $A \to A$ of the form



with $E^\dagger \circ E = \mathrm{id}_X$.

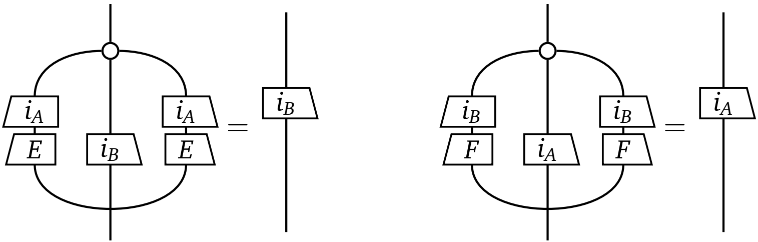
- If $\mathbf{C} = \mathbf{FHilb}$, measurements are POVMs
- If $\mathbf{C} = \mathbf{Rel}$, measurements are conjugacy classes
  (relations $\{(g, g^{-1} \circ f \circ h) \mid g, h \in E_i\}$ for disjoint families $E_i \subseteq G$)

Two subsystems $(A, \,)$ and $(B, \,)$ of $(C, \,)$ are kinematically independent when



- If $\mathbf{C} = \mathbf{FHilb}$: commuting C*-subalgebras
- If $\mathbf{C} = \mathbf{Rel}$: commuting totally disconnected wide subgroupoids
  ($a \circ b = b \circ a$ for endomorphisms $a \in A$, $b \in B$ on same object)

Two subsystems $(A, \ )$ and $(B, \ )$ of $(C, \ )$ are no signalling when



for all measurements E on A and F on B.

- If $C = A \otimes B$, then always no signalling
- If $\mathbf{C} = \mathbf{FHilb}$, usual notion of no signalling

no signalling $\iff$ kinematic independence

$$
\begin{array}{rcl}
\text{no broadcasting} & \substack{\Rightarrow \\ \not\Leftarrow} & \text{noncommutativity} \\[1ex]
\text{no bit commitment} & \substack{\not\Rightarrow \\ \not\Leftarrow} & \text{nonlocality} \\[1ex]
\text{no signalling} & \Leftrightarrow & \text{kinematic independence}
\end{array}
$$

So, can quantum theory be characterized in terms of information-theoretic constraints?

So, can quantum theory be characterized in terms of information-theoretic constraints?

Yes. No. Er, well, it depends.

So, can quantum theory be characterized in terms of information-theoretic constraints?

Yes. No. Er, well, it depends.

Yes if you think probabilities are information-theoretic.
No if you think information is purely compositional.

So, can quantum theory be characterized in terms of information-theoretic constraints?

Yes. No. Er, well, it depends.

Yes if you think probabilities are information-theoretic.[1]
No if you think information is purely compositional.

[1] Well, at least if you accept foundational axioms like tomographic locality.[2]

So, can quantum theory be characterized in terms of information-theoretic constraints?

Yes. No. Er, well, it depends.

Yes if you think probabilities are information-theoretic.[1]
No if you think information is purely compositional.

[1] Well, at least if you accept foundational axioms like tomographic locality.[2]

[2] Or if you prefer practicable protocols and think linearity is information-theoretic.

So, can quantum theory be characterized in terms of information-theoretic constraints?

Yes. No. Er, well, it depends.

Yes if you think probabilities are information-theoretic.[1]
No if you think information is purely compositional.[3]

[1] Well, at least if you accept foundational axioms like tomographic locality.[2]
[2] Or if you prefer practicable protocols and think linearity is information-theoretic.
[3] Well, at least *not in this way*.

So, can quantum theory be characterized in terms of information-theoretic constraints?

Yes. No. Er, well, it depends.

Yes if you think probabilities are information-theoretic.[1]
No if you think information is purely compositional.[3]

[1] Well, at least if you accept foundational axioms like tomographic locality.[2]
[2] Or if you prefer practicable protocols and think linearity is information-theoretic.
[3] Well, at least *not in this way*.

But maybe there is another protocol that is equivalent to nonlocality more practical than GHZ game … ?