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

Chris Heunen

Aleks Kissinger

arXiv.org:1604.05948
“Information, physics, quantum: the search for links”

*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”

“A derivation of quantum theory from physical requirements”

“Informational derivation of quantum theory”
Yes if retain only the algebraic structure of interaction between classical and quantum systems.

“Characterizing quantum theory in terms of information-theoretic constraints”
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 \hspace{1em} quantum theory

no broadcasting \iff noncommutativity
no bit commitment \iff nonlocality
no signalling \iff kinematic independence
Are there physical means for broadcasting unknown quantum states, pure or mixed, onto two separate quantum systems?

$$\text{Tr}_1(B(\rho)) = \rho = \text{Tr}_2(B(\rho))$$
Are there physical means for **committing** to a bit value, with the ability to reveal the choice later, securely?

\[
\text{reveal}\left(\text{commit}(x, s)\right) = x \\
\text{cheat}\left(\text{commit}(x, s)\right) = \text{cheat}\left(\text{commit}(y, s)\right)
\]
Are there physical means for signalling classical information faster than light?

\[ P(bx|A0) = P(bx|A1) \]
“Notation which is useful in private must be given a public value and that it should be provided with a firm theoretical foundation”

- Morphisms $f : A \rightarrow B$ depicted as boxes
- Composition: stack boxes vertically
- Tensor product: stack boxes horizontally
- Dagger: turn box upside-down
**Sound**: isotopic diagrams represent equal morphisms

\[
\begin{align*}
(k \otimes \text{id}) \circ (g \otimes h^\dagger) \circ f &= (k \otimes \text{id}) \circ (g \otimes h^\dagger) \circ f
\end{align*}
\]

**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 $\otimes$ for multiplication $A \otimes A \to A$

Frobenius law:
Any connected diagram built from the components of a special ($\mathfrak{S} = \mid$) Frobenius structure equals the following normal form:

In particular:
So any Frobenius structure is \textit{self-dual}
Let $G$ be the set of objects of a **small groupoid**.

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

Any dagger Frobenius structure in $\textbf{Rel}$ is of this form.
Let $G$ be the set of objects of a small groupoid.

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

Any dagger Frobenius structure in $\mathbf{Rel}$ is of this form.

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

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

Any dagger Frobenius structure in $\mathbf{(F)Hilb}$ is of this form.
Mixed state of dagger Frobenius structure is $I \xrightarrow{m} A$ with
A morphism $f : (A, \otimes) \rightarrow (B, \otimes)$ is completely positive when $f \otimes \text{id}$ preserves mixed states.

- **Evolution** along unitary $A \rightarrow A$
- **Preparation** of mixed state $I \rightarrow A$
- **Measurement** is $A \rightarrow (\mathbb{C}^n, \otimes)$
A morphism $f: (A, \mathcal{A}) \to (B, \mathcal{B})$ is completely positive when $f \otimes \text{id}$ preserves mixed states.

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

If and only if CP condition:

$$\sqrt{f} = \sqrt{f}X\sqrt{f}$$
- $\text{CP}[\mathcal{C}] = \text{Frobenius structures in } \mathcal{C} \text{ and morphisms in } \mathcal{C} \text{ satisfying CP condition}$

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

- $\text{CP}[\text{Rel}] = \text{small groupoids and inverse-respecting relations}$
Broadcasting map for \((A, \land)\) in \(\text{CP}[C]\) is morphism \(B: A \to A \otimes A\) with

\[
\begin{array}{c}
\begin{array}{c}
\circ \\
\end{array}
\end{array}
\quad = 
\quad \begin{array}{c}
\begin{array}{c}
\circ \\
\end{array}
\end{array}
\quad = 
\quad \begin{array}{c}
\begin{array}{c}
\circ \\
\end{array}
\end{array}
\quad B
\]
\]
- If $(A, \otimes)$ in $\text{CP}[C]$ is commutative, then it is broadcastable.

- If $C^*$-algebra in $\text{CP}[\text{FHilb}]$ is broadcastable, it is commutative.

- If groupoid in $\text{CP}[\text{Rel}]$ is broadcastable, it is totally disconnected (the only morphisms are endomorphisms).

- In general: no broadcasting $\Rightarrow$ noncommutativity.

- Classicality: biproduct of $I$ $\Rightarrow$ commutative $\Leftrightarrow$ broadcastable.
- states $H, T : I \to A \otimes B$ of $\text{CP}[C]$
- monomorphism unveil: $A \otimes B \to A \otimes B$ in $\text{CP}[C]$
- classical $(A \otimes B, \bowtie)$ in $C$ with copyable states $\overline{H} \neq \overline{T}$

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

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

**Concealing** when $\widehat{\overline{H}} = \overline{T}$
Alice cannot cheat: if

\[
\begin{align*}
\text{unveil} & \quad = \\
\text{cheat}_H & \quad = \\
\text{cheat} & \\
A & \quad B \\
& \\
& \\
A & \quad B \\
H & \\
\text{unveil} & \quad = \\
\text{cheat}_T & \quad = \\
\text{cheat} & \\
A & \quad B \\
& \
\end{align*}
\]

then not binding:

\[
\begin{align*}
\text{unveil} & \quad = \\
\text{cheat}_H & \quad = \\
H & \\
A & \quad B \\
\text{unveil} & \quad = \\
\text{cheat}_T & \quad = \\
T & \\
A & \quad B \\
\end{align*}
\]
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 $\text{CP}[\mathcal{C}]$ admits entanglement if there is state $I \rightarrow A \otimes B$ not of the form $(f \otimes g) \circ \psi$ for $\psi : I \rightarrow A' \otimes B'$ with $A', B'$ classical. The category $\mathcal{C}$ is nonlocal when every object admits entanglement.

- $\text{CP}[\text{FHilb}]$ is nonlocal
- $\text{CP}[\text{Rel}]$ is nonlocal
- In general: no bit commitment $\nRightarrow$ nonlocality
Let \((C, \otimes)\) be a dagger Frobenius structure in \(C\). A **subsystem** is another dagger Frobenius structure \((A, \otimes)\) with a unital \(*\)-homomorphism \(i: A \rightarrow C\) satisfying \(i^\dagger \circ i = \text{id}_A\). If \(\otimes\) is broadcastable, it is a **classical context**.

- If \(C = A \otimes B\), both \(A\) and \(B\) are subsystems
- If \(C = \text{FHilb}\), subsystems are \(\text{C}^*\)-subalgebras
- If \(C = \text{Rel}\), subsystems are **wide subgroupoids**
Let \((A, \mathcal{A})\) be a dagger Frobenius structure in \(\mathbf{C}\).

A **measurement** on \((A, \mathcal{A})\) is a morphism \(A \rightarrow A\) of the form

\[
E \xrightarrow{E^\dagger} E \xrightarrow{A}
\]

with \(E^\dagger \circ E = \text{id}_X\).

- 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 \((A, \bullet)\) and \((B, \bullet)\) of \((C, \bullet)\) are \textit{kinematically independent} when

\[
C_i A_i B A B = C_i A_i B A B
\]

- If \(C = \text{FHilb}\): commuting \(C^\ast\)-subalgebras
- If \(C = \text{Rel}\): commuting totally disconnected wide subgroupoids
  \((a \circ b = b \circ a\) for endomorphisms \(a \in A, b \in B\) on same object)
Two subsystems \((A, \bigcirc)\) and \((B, \bigcirc)\) of \((C, \bigcirc)\) are no signalling when

\[ i_A \quad E \quad i_B \quad i_A \quad E = i_B \]

\[ i_B \quad F \quad i_A \quad i_B \quad F = i_A \]

for all measurements \(E\) on \(A\) and \(F\) on \(B\).

- If \(C = A \otimes B\), then always no signalling
- If \(C = FHilb\), usual notion of no signalling
no signalling  $\iff$  kinematic independence
no broadcasting $\Rightarrow$ noncommutativity

no bit commitment $\not\Rightarrow\not\Leftarrow$ nonlocality

no signalling $\Leftrightarrow$ kinematic independence
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 ...?