Graphical and Automated Reasoning for Quantum Algorithms and Protocols

QISW — Mar. 2012

Bob Coecke
Oxford University, Computer Science, Quantum Group
The ‘Hilbert space’ quantum formalism
The ‘Hilbert space’ quantum formalism

[von Neumann 1932] Formalized quantum mechanics in “Mathematische Grundlagen der Quantenmechanik”
The ‘Hilbert space’ quantum formalism

[von Neumann 1932] Formalized quantum mechanics in “Mathematische Grundlagen der Quantenmechanik”

[von Neumann to Birkhoff 1935] “I would like to make a confession which may seem immoral: I do not believe absolutely in Hilbert space no more.” (sic)
The ‘Hilbert space’ quantum formalism

[von Neumann 1932] Formalized quantum mechanics in “Mathematische Grundlagen der Quantenmechanik”

[von Neumann to Birkhoff 1935] “I would like to make a confession which may seem immoral: I do not believe absolutely in Hilbert space no more.” (sic)

The ‘Hilbert space’ quantum formalism

[von Neumann 1932] Formalized quantum mechanics in “Mathematische Grundlagen der Quantenmechanik”

[von Neumann to Birkhoff 1935] “I would like to make a confession which may seem immoral: I do not believe absolutely in Hilbert space no more.” (sic)


[1936 – 2000] many followed them, ...
The ‘Hilbert space’ quantum formalism

[von Neumann 1932] Formalized quantum mechanics in “Mathematische Grundlagen der Quantenmechanik”

[von Neumann to Birkhoff 1935] “I would like to make a confession which may seem immoral: I do not believe absolutely in Hilbert space no more.” (sic)


[1936 – 2000] many followed them, ... and FAILED.
The ‘Hilbert space’ quantum formalism

Hilber space stuff: continuum, field structure of complex numbers, vector space over it, inner-product, etc.
The ‘Hilbert space’ quantum formalism

Hilber space stuff: continuum, field structure of complex numbers, vector space over it, inner-product, etc.

WHY?
The ‘Hilbert space’ quantum formalism

**Hilber space stuff:** continuum, field structure of complex numbers, vector space over it, inner-product, etc.

**WHY?**

**von Neumann:** only used it since it was available.
The ‘Hilbert space’ quantum formalism

**Hilber space stuff:** continuum, field structure of complex numbers, vector space over it, inner-product, etc.

**WHY?**

**von Neumann:** only used it since it was available.

**Model theory:** one can do almost anything with it.
The ‘Hilbert space’ quantum formalism

**Hilber space stuff:** continuum, field structure of complex numbers, vector space over it, inner-product, etc.

**WHY?**

**von Neumann:** only used it since it was available.

**Model theory:** one can do almost anything with it.

**Schrödinger (1935):** the stuff which is the true soul of quantum theory is ‘how quantum systems compose’.
\[ \text{tensor product structure} = \text{the other stuff} \]
tensor product structure = ?

Conceptually: *not* about properties of the individual, *but* about relationships among the individuals.
Conceptually: **not** about **properties** of the individual, **but** about **relationships** among the individuals.

Mathematically: **axiomatize** an ‘abstract tensor product’ **without reference to underlying spaces**.
Conceptually: *not* about properties of the individual, *but* about relationships among the individuals.

Mathematically: *axiomatize* an ‘abstract tensor product’ *without reference to underlying spaces*.

1. Game plan: Which assumptions (i.e. which structure) on $\otimes$ is needed to deduce *physical phenomena*?
The tensor product structure = ?

Conceptually: not about properties of the individual, but about relationships among the individuals.

Mathematically: axiomatize an ‘abstract tensor product’ without reference to underlying spaces.

1. Game plan: Which assumptions (i.e. which structure) on \( \otimes \) is needed to deduce physical phenomena?

   \[ \Rightarrow \text{Framework for Generalized Process Theories} \]

   \[ \Rightarrow \text{Operational bones for Quantum Foundations} \]
Conceptually: **not** about **properties** of the individual, **but** about **relationships** among the individuals.

Mathematically: **axiomatize** an ‘abstract tensor product’ **without reference to underlying spaces**

1. **Game plan:** Which assumptions (i.e. which structure) on $\otimes$ is needed to deduce **physical phenomena**?

2. **Additional question:** Does such an interaction structure appear elsewhere in “**our classical reality**”? 

Here, the tensor product structure $\otimes$ is being equated with the other stuff, hence the question mark (?)
Outcome 1a: “Sheer ratio of results to assumptions” confirms that we are probing something very essential.

Outcome 1a: “Sheer ratio of results to assumptions” confirms that we are probing something very essential.

Outcome 1b: Exposing this structure has already helped to solve open problems elsewhere.
Outcome 1a: “Sheer ratio of results to assumptions” confirms that we are probing something very essential.

Outcome 1b: Exposing this structure has already helped to solve open problems elsewhere.

Outcome 1c: Simple intuitive (but rigorous) diagrammatic language

Outcome 1a: “Sheer ratio of results to assumptions” confirms that we are probing something very essential.

Outcome 1b: Exposing this structure has already helped to solve open problems elsewhere.

Outcome 1c: Simple intuitive (but rigorous) diagrammatic language, meanwhile adopted by others:

“... we join the quantum picturalism revolution [1]”


  ⇒ Ross Duncan’s talk

  ⇒ DEMO


  ⇒ Aleks Kissinger’s talk
Outcome 2a:

Behaviors of matter:

Outcome 2a: Behaviors of matter:

Meaning in language:

Outcome 2a:

Behaviors of matter:

Meaning in language:

Knowledge updating:

Outcome 2b: The structure is a true (quantum) logic:

Lucas Dixon, Ross Duncan, Ben Frot, Aleks Kissinger, Alex Merry
A MINIMAL LANGUAGE FOR QUANTUM PROCESSES


— kinds of systems —

one system \hspace{2cm} n sub-systems \hspace{2cm} no system

1 \hspace{2cm} \cdots \hspace{2cm} 0
merely a new notation?

\[(g \circ f) \otimes (k \circ h) = (g \otimes k) \circ (f \otimes h)\]
merely a new notation?

\[(g \circ f) \otimes (k \circ h)\]
merely a new notation?

\[(g \otimes k) \circ (f \otimes h)\]
merely a new notation?

\[(g \circ f) \otimes (k \circ h) = (g \otimes k) \circ (f \otimes h)\]
merely a new notation?

$$(g \circ f) \otimes (k \circ h) = (g \otimes k) \circ (f \otimes h)$$

peel potato and then fry it, while, clean carrot and then boil it

= peel potato while clean carrot, and then, fry potato while boil carrot
adjoint

\[ f : A \rightarrow B \]
adjoint

\[ f^\dagger : B \rightarrow A \]
asserting (pure) entanglement

\[
\frac{\text{quantum}}{\text{classical}} = \begin{array}{c}
\text{\textbullet} \\
\text{\textbullet} \\
\end{array} = \begin{array}{c}
\text{\textbullet} \\
\text{\textbullet} \\
\end{array} = \begin{array}{c}
\text{\textbullet} \\
\text{\textbullet} \\
\end{array}
\]
asserting (pure) entanglement

\[
\frac{\text{quantum}}{\text{classical}} = \begin{array}{c}
\text{\(\Rightarrow\)}
\end{array} \begin{array}{c}
\text{introduce ‘parallel wire’ between systems:}
\end{array}
\]

subject to: only topology matters!
quantum-like

E.g.
sliding
In QM: cups = Bell-states, caps = Bell-effects, $\pi$-rotations = transpose
classical data flow
classical data flow?

⇒ quantum teleportation
Applying "decorated" normalization $f = f$

$\Rightarrow$ Entanglement swapping

$\Rightarrow$ Entanglement swapping
dagger compact categories
Thm. [Kelly-Laplaza ’80; Selinger ’05] An equational statement between expressions in dagger compact categorical language holds if and only if it is derivable in the graphical notation via homotopy.
Thm. [Kelly-Laplaza ’80; Selinger ’05] An equational statement between expressions in dagger compact categorical language holds if and only if it is derivable in the graphical notation via homotopy.

Thm. [Selinger ’08] An equational statement between expressions in dagger compact categorical language holds if and only if it is derivable in the category of finite dimensional Hilbert spaces, linear maps, tensor product, and adjoints.
In words: *Any equation involving:*

- *states, operations, effects*
- *unitarity, adjoints (e.g. self-adjoint), projections*
- *Bell-states/effects, transpose, conjugation*
- *inner-product, trace, Hilbert-Schmidt norm*
- *positivity, completely positive maps, ...*

*holds in quantum theory if and only if it can be derived in the graphical language via homotopy.*
A SLIGHTLY DIFFERENT LANGUAGE FOR NATURAL LANGUAGE MEANING

Consider meanings of **words**, e.g. as vectors (cf. Google):
What is the meaning the sentence made up of these?

--- the from-words-to-a-sentence process ---
I.e. how do we/machines produce meanings of sentences?
I.e. how do we/machines produce meanings of sentences?

Information flow within a verb:
Information flow within a verb:

Again we have:

\[ \text{verb} \]

\[ \text{subject} \]

\[ \text{object} \]

\[ \text{subject} \]
— going non-symmetric —

\[ \begin{align*}
A & \quad A^l \\
A & \quad A^r
\end{align*} \]

\[ \begin{align*}
A & \quad A \\
A & \quad A
\end{align*} \]

\[ \begin{align*}
A^l & \quad A \\
A^l & \quad A^r
\end{align*} \]

\[ \begin{align*}
A & \quad A \\
A & \quad A
\end{align*} \]

\[ \begin{align*}
A^l & \quad A^l \\
A^l & \quad A^r
\end{align*} \]

\[ \begin{align*}
A & \quad A \\
A & \quad A
\end{align*} \]
Alice $\otimes$ does $\otimes$ not $\otimes$ like $\otimes$ Bob

meaning vectors of words

grammar
Alice does not like Bob
Alice does not like Bob

meaning vectors of words

grammar
Alice $\not\rightarrow$ does $\not\rightarrow$ not $\not\rightarrow$ like $\not\rightarrow$ Bob

= $Terry \not\rightarrow$ not $\rightarrow$ like $\rightarrow$ Bob
E.g. what is “saw” in: “Alice saw Bob with a saw”.

<table>
<thead>
<tr>
<th>Model</th>
<th>High</th>
<th>Low</th>
<th>$\rho$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baseline</td>
<td>0.47</td>
<td>0.44</td>
<td>0.16</td>
</tr>
<tr>
<td>Add</td>
<td>0.90</td>
<td>0.90</td>
<td>0.05</td>
</tr>
<tr>
<td>Multiply</td>
<td>0.67</td>
<td>0.59</td>
<td>0.17</td>
</tr>
<tr>
<td>Categorical (1)</td>
<td>0.73</td>
<td>0.72</td>
<td>0.21</td>
</tr>
<tr>
<td>Categorical (2)</td>
<td>0.34</td>
<td>0.26</td>
<td>0.28</td>
</tr>
<tr>
<td>UpperBound</td>
<td>4.80</td>
<td>2.49</td>
<td>0.62</td>
</tr>
</tbody>
</table>

Mehrnoosh Sadrzadeh  Edward Grefenstette
AN EXTENDED LANGUAGE:
CLASSICALITY & OBSERVABLES
such that, for $k > 0$:
observables

‘spiders’ = \[ \left\{ \begin{array}{c}
 m \\
 n
 \end{array} \right\} \]

such that, for \( k > 0 \):
‘spiders’ = \begin{cases} \text{observables} \\ \text{such that, for } k > 0: \end{cases}

\begin{array}{c}
m + m' - k \\
n + n' - k
\end{array} =

\begin{array}{c}
m \\
n
\end{array}
— observables —

**Theorem 1.** (‘folklore’ - Kock’s TQFT ’03; Lack ’04) In any dagger symmetric monoidal category such families of spiders and dagger special commutative Frobenius algebras are in canonical bijective correspondence.

**Theorem 2.** (Coecke-Pavlovic-Vicary) In $\mathcal{F}_d\mathcal{H}ilb$ dagger (special) commutative Frobenius algebra are exactly ortho(normal) bases, nl. those of copyable elts.

---


Observables

'spiders' = \{ \}

such that, for $k > 0$:

\[
\begin{align*}
(m + m' - k) & \quad = \\
(n + n' - k)
\end{align*}
\]
complementary observables
Complementary observables

arXiv:0906.4725
A UNIVERSAL LANGUAGE
THM (Phased Z/X-calc.). Any $f : \mathbb{C}^n \rightarrow \mathbb{C}^m$ decomposes in complementary “phased” 3-spiders:

These phases arise as an **Abelian group structure** that comes with the spiders for purely abstract reasons, where inverses are the abstract conjugates.

These phases ‘add’ when spiders fuse, which can be described as families of ‘group-decorated’ spiders.

---

applications to QC models

Translation to circuits, required resources and determinism in measurement based quantum computations:

Example 18. The ubiquitous CNOT operation can be computed by the pattern $P = X_3^4 Z_2^4 Z_1^1 M_0^3 M_0^2 E_{13} E_{23} E_{34} N_3 N_4$. This yields the diagram, $D_P = H H H \pi_3 \{3\} \pi_2 \{2\} \pi_3 \{2\} \pi_2 \{2\} \pi_3 \{2\} \pi_2 \{2\}$. Where each qubit is represented by a vertical "path" from top to bottom, with qubit 1 the leftmost, and qubit 4 is the rightmost.

By virtue of the soundness of $R$ and Proposition 10, if $D_P$ can be rewritten to a circuit-like diagram without any conditional operations, then the rewrite sequence constitutes a proof that the pattern computes the same operation as the derived circuit.

Example 19. Returning to the CNOT pattern of Example 18, there is a rewrite sequence, the key steps of which are shown below, which reduces the $D_P$ to the unconditional circuit-like pattern for CNOT introduced in Example 7. This proves two things: firstly that $P$ indeed computes the CNOT unitary, and that the pattern $P$ is deterministic.


Similar stuff for TMBQC (Clare Horsman NJP’11):
Toy qubits vs. true quantum theory in one language:

\[
\frac{\text{Spekkens' qubit QM}}{\text{stabilizer qubit QM}} = \frac{Z_2 \times Z_2}{Z_4} = \text{local} \quad \text{non-local}
\]

Toy qubits vs. true quantum theory in one language:

\[
\frac{\text{Spekkens’ qubit QM}}{\text{stabilizer qubit QM}} = \frac{\mathbb{Z}_2 \times \mathbb{Z}_2}{\mathbb{Z}_4} = \frac{\text{local}}{\text{non-local}}
\]


Generalized Mermin arg. \(\Leftrightarrow\) strong complementarity

— multipartite entanglement structure —

Tripartite SLOCC-classes as comm. Frobenius algs:

\[
GHZ = |000\rangle + |111\rangle
\]

\[
W = |001\rangle + |010\rangle + |100\rangle
\]

= ‘special’ CFAs

= ‘anti-special’ CFAs

\[
\frac{\bigcirc}{\bigcirc} = |\rangle
\]

\[
\frac{\bigcirc}{\bigcirc} = \frac{\bigcirc}{\bigcirc}
\]

\[
\times + \Rightarrow \text{distributivity}
\]

GHZ-spiders

Data:

\[
\begin{cases}
  m \\
  n
\end{cases}
\quad | \quad n, m \in \mathbb{N}
\]

Rules:

\[
\begin{aligned}
  m + m' - k \\
  n + n' - k
\end{aligned}
\]

= 

\[
\begin{aligned}
  m + m' - k \\
  n + n' - k
\end{aligned}
\]
W-spiders

Data:
\[
\begin{cases}
m & \text{,} \\
, & \text{,} \\
, & \text{,} \\
n \mid n, m \in \mathbb{N}
\end{cases}
\]

Rules:
\[
\begin{align*}
m + m' - 1 & \quad = \quad m + m' - 1 \\
n + n' - 1 & \quad = \quad n + n' - 1
\end{align*}
\]
--- W-spiders ---

Data:
\[
\begin{cases}
  m \quad \text{,} \\
  n \quad \text{,} \\
  n, m \in \mathbb{N}
\end{cases}
\]

Rules:
\[
\begin{align*}
  m + m' - 2 \\
  n + n' - 2
\end{align*}
\]

= 
\[
\begin{align*}
  m + m' - 2 \\
  n + n' - 2
\end{align*}
\]
--- automation ---

Stages:

- Automated reasoning — quantomatic
- Automated theory generation — quantocosy
- Automated theorem extraction — ???

theory[mine]™
Personalized mathematical theorems

... you could be next!

NEW!
You can now purchase TheoryMine T-shirts, mouse-pads and mugs!
automated quantum reasoning

Duncan, Soloviev, Kissinger, Merry, Dixon