The non-logic of quantum computation

OR:
How I learned to live without propositions-as-types

Ross Duncan
Mathematically Structured Programming Group
University of Strathclyde
2004

“The 1st occasional Bellairs workshop on semantic techniques in quantum computing”
BTP → IJTP

Causal Evolution in
Discrete Quantum Systems
What is the logic of quantum computation?
The Curry-Howard-Lambek correspondence

Cartesian closed categories \rightarrow \text{Simply typed } \lambda\text{-calculus} \rightarrow \text{Intuitionistic Logic} \rightarrow \text{Cartesian closed categories}
General Scheme

Categorical Structure  ←  Logic

Rewriting system

Ross Duncan • PrakashFest • Oxford 2014
Proofs and types

Proofs and programs are the same thing.

- Propositions are types.
- Many different proofs of the same theorem: processes producing output of that type.
- Less interested in the validity of propositions than the relationship between proofs.
Proofs and types

Pragmatics:

● The type of a program should provide some useful information about that program.

● The type system should exclude (certain) programming errors.
Proofs and types

Pragmatics:

- The type of a program should provide some useful information about that program.
- The type system should exclude (certain) programming errors.

“It type checks — it must be right”
The objective:

Categorical Structure → Logic

Logic → Rewriting system

Rewriting system → Categorical Structure
The objective:

Quantum Categorical Structure

Quantum Logic

Quantum Rewriting system
Quantum Logic

The Birkhoff-von Neumann approach and its problems
Propositions and projectors

A proposition is a question with a yes/no answer:

\[ A = \text{“Is the spin up?”} \]

but the answer will be given by a quantum measurement:

\[ \psi \models A \iff p_A |\psi\rangle = |\psi\rangle \]

hence each proposition corresponds to a pair of orthogonal subspaces.

The “lattice of propositions” is simply the collection of closed subspaces ordered under inclusion.
Distributivity Fails

In general we have \( p_A p_B \neq p_B p_A \) which implies the failure of distributivity.

Consider:

\[
\begin{align*}
\perp &= (A \land B) \lor (A^\perp \land B) \\
&\neq (A \lor A^\perp) \land B = B
\end{align*}
\]

hence such a lattice is not distributive.

(It does satisfy a weaker law called orthomodularity which I won’t discuss.)
No deduction theorem

**Theorem:** Suppose we can define a connective $\rightarrow$ such that

$$A \land X \leq B \iff X \leq A \rightarrow B$$

then the lattice is distributive.

**Corollary:** Quantum logic does not admit modus ponens.

Note that the sub-lattice defined by any set of commuting projectors is just a boolean lattice.
Quantum Mechanics

Overview of the physical theory
No-Cloning and No-Deleting

Theorem: There are no quantum operations $D$ such that

$$D : |\psi\rangle \leftrightarrow |\psi\rangle \otimes |\psi\rangle$$
$$D : |\phi\rangle \leftrightarrow |\phi\rangle \otimes |\phi\rangle$$

unless $|\psi\rangle$ and $|\phi\rangle$ are orthogonal [Wooters & Zurek 1982]

Theorem: There are no quantum operations $E$ such that

$$E : |\psi\rangle \leftrightarrow |0\rangle$$
$$E : |\phi\rangle \leftrightarrow |0\rangle$$

unless $|\psi\rangle$ and $|\phi\rangle$ are orthogonal [Pati & Braunstein 2000]
No-Cloning and No-Deleting

Linear types have been proposed* to capture this:

\[ \,!A \quad A \otimes B \]

Separate classical and quantum data in a hybrid machine


**Hensinger et al, Nature 2005
No-Cloning and No-Deleting

Linear types have been proposed* to capture this:

No-Cloning and No-Deleting

Not good enough!

---

Map-State Duality

Recall that there is an isomorphism:

\[ A \rightarrow B \cong A \otimes B \]

\[ I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \leftrightarrow \quad |00\rangle + |11\rangle =: |\text{Bell}_1\rangle \]

\[ X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \leftrightarrow \quad |01\rangle + |10\rangle =: |\text{Bell}_2\rangle \]

\[ Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \leftrightarrow \quad |00\rangle - |11\rangle =: |\text{Bell}_3\rangle \]

\[ XZ = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \leftrightarrow \quad |01\rangle - |10\rangle =: |\text{Bell}_4\rangle \]
Quantum Teleportation

\[ |\psi\rangle \rightarrow |00\rangle + |11\rangle \]
Quantum Teleportation

\[ |\psi\rangle \]

\[ \langle 00| + \langle 11| \]

\[ |00\rangle + |11\rangle \]
Channels via entanglement

Bennett at al:

“Note that qubits are a directed channel resource, sent in a particular direction from the sender to the receiver; by contrast [entangled pairs] are an undirected resource shared between the sender and receiver.”

Teleporting an unknown quantum state via dual classical and EPR channels, PRL, 1993

This suggests that the type of an entangled pair should be the linear type $Q \otimes Q$ rather than the usual $Q \rightarrow Q$. 
More Entanglement

Entanglement can be used for a lot more than just transmitting information:

MBQC is a universal model of computation which is based on the flow of information through large entangled states.
Propositions as types for QM

A logic based on processes not properties
What is the quantum version?

- We want a logic of “quantum processes”

Some hints as to what this should be:
- entangled systems can’t be described by a Cartesian product
- map-state duality suggests we should have a “function-type”
- no-cloning and no-deleting imply that the underlying setting should be linear
- ....however we still need some way to represent non-determinism
The quantum version:
The quantum version:
The quantum version:

A categorical semantics of quantum protocols

Samson Abramsky and Bob Coecke

Oxford University Computing Laboratory,
Wolfson Building, Parks Road, Oxford OX1 3QD, UK.
samson.abramsky · bob.coecke@comlab.ox.ac.uk
The quantum version:

\(\dagger\)-compact closed categories with \(\dagger\)-biproducts

\[ A \text{ categorical semantics of quantum protocols} \]

Samson Abramsky and Bob Coecke

Oxford University Computing Laboratory,
Wolfson Building, Parks Road, Oxford OX1 3QD, UK.

samson.abramsky · bob.coecke@comlab.ox.ac.uk
\[ Q \xrightarrow{\lceil 1_Q \rceil} Q \otimes (Q^* \otimes Q) \xrightarrow{\alpha} (Q \otimes Q^*) \otimes Q \]

\[ \langle \lceil 1_Q \rceil, \lceil x \rceil, \lceil z \rceil, \lceil xz \rceil \rangle \otimes 1_Q \]

\[ (I \oplus I \oplus I \oplus I) \otimes Q \]

\[ Q \oplus Q \oplus Q \oplus Q \]

\[ 1_Q \oplus x^\dagger \oplus z^\dagger \oplus (xz)^\dagger \]

\[ Q \oplus Q \oplus Q \oplus Q \]
\[ Q \xrightarrow{\iota_{1_Q}} Q \otimes (Q^* \otimes Q) \xrightarrow{\alpha} (Q \otimes Q^*) \otimes Q \xrightarrow{\text{Relocalise}} (I \oplus I \oplus I \oplus I) \otimes Q \]

\[ \langle \bot 1_Q, \bot x, \bot z, \bot xz \rangle \otimes 1_Q \]

\[ (I \oplus I \oplus I \oplus I) \otimes Q \]

\[ Q \oplus Q \oplus Q \oplus Q \]

\[ 1_Q \oplus x^\dagger \oplus z^\dagger \oplus (xz)^\dagger \]

\[ Q \oplus Q \oplus Q \oplus Q \]
\[ Q \xrightarrow{1_Q} Q \otimes (Q^* \otimes Q) \xrightarrow{\alpha} (Q \otimes Q^*) \otimes Q \]

Bell basis measurement

\[ \langle \perp 1_Q, \perp x, \perp z, \perp xz \rangle \otimes 1_Q \]

\[ (I \oplus I \oplus I \oplus I) \otimes Q \]

\[ \cong \]

\[ Q \oplus Q \oplus Q \oplus Q \]

\[ 1_Q \oplus x^\dagger \oplus z^\dagger \oplus (xz)\dagger \]

\[ Q \oplus Q \oplus Q \oplus Q \]
\[ Q \xrightarrow{\{1_Q\}} Q \otimes (Q^* \otimes Q) \xrightarrow{\alpha} (Q \otimes Q^*) \otimes Q \]

\[
\langle \perp 1_Q, \perp x, \perp z, \perp xz \rangle \otimes 1_Q
\]

\[
(I \oplus I \oplus I \oplus I) \otimes Q
\]

\[
Q \oplus Q \oplus Q \oplus Q
\]

\[
1_Q \oplus x^\dagger \oplus z^\dagger \oplus (xz)^\dagger
\]

\[
Q \oplus Q \oplus Q \oplus Q
\]
\[ Q \xrightarrow{\left[1_Q\right]} Q \otimes (Q^* \otimes Q) \xrightarrow{\alpha} (Q \otimes Q^*) \otimes Q \]

\[ \langle \downarrow 1_Q, \downarrow x, \downarrow z, \downarrow xz \rangle \otimes 1_Q \]

\[ (I \oplus I \oplus I \oplus I) \otimes Q \]

\[ \cong \]

\[ Q \oplus Q \oplus Q \oplus Q \]

\[ 1_Q \oplus x^\dagger \oplus z^\dagger \oplus (xz)^\dagger \]

\[ Q \oplus Q \oplus Q \oplus Q \]

**Unitary correction**
\[
Q \xrightarrow{1_Q} Q \otimes (Q^* \otimes Q) \xrightarrow{\alpha} (Q \otimes Q^*) \otimes Q
\]

\[
\langle \perp 1_Q, \perp x, \perp z, \perp xz \rangle \otimes 1_Q
\]

\[
(I \oplus I \oplus I \oplus I) \otimes Q
\]

\[
Q \oplus Q \oplus Q \oplus Q
\]

\[
1_Q \oplus x^\dagger \oplus z^\dagger \oplus (xz)^\dagger
\]

\[
Q \oplus Q \oplus Q \oplus Q
\]

**Specification**
An invitation:

Programming Research Group

THE LOGIC OF ENTANGLEMENT.
AN INVITATION.

(VERSION 0.9999)

Bob Coecke

PRG-RR-03-12
An invitation:

161 pages!
The quantum version:

†-compact closed categories with †-biproducts

Generalised self-dual proof-nets

Tensor-sum logic
The connectives

Classical logic

\[ \neg \neg A = A \]
\[ \neg (A \land B) = \neg A \lor \neg B \]
\[ \neg (A \lor B) = \neg A \land \neg B \]
The connectives

**Linear logic**

(MALL)

\[
A^\perp \perp = A \\
(A \otimes B)^\perp = A^\perp \multimap B^\perp \\
(A \multimap B)^\perp = A^\perp \otimes B^\perp \\
(A \& B)^\perp = A^\perp \oplus B^\perp \\
(A \oplus B)^\perp = A^\perp \& B^\perp
\]

<table>
<thead>
<tr>
<th></th>
<th>conjunction</th>
<th>disjunction</th>
</tr>
</thead>
<tbody>
<tr>
<td>multiplicative</td>
<td>(\otimes)</td>
<td>(\multimap)</td>
</tr>
<tr>
<td>additive</td>
<td>(&amp;)</td>
<td>(\oplus)</td>
</tr>
</tbody>
</table>
The connectives

Tensor-sum “logic”

\[ A^{**} = A \]
\[ (A \otimes B)^* = A^* \otimes B^* \]
\[ (A \oplus B)^* = A^* \oplus B^* \]
A professional opinion:

“One must leave it in the department of atrocities...”

A professional opinion:

“One must leave it in the department of atrocities…”


“Here one witnesses a frank divorce between the logical viewpoint and the category-theoretic viewpoint, for which $\otimes = \otimes$ is not absurd. Thus, in algebra, the tensor is often equal to the cotensor, for instance in finite dimensional vector spaces ... This remark illustrates the gap separating logic and categories, by the way quite legitimate activities, that one should not try to crush one upon another.”
Tensor-Sum Logic

Tensor-sum logic is a Gentzen system, designed to capture the structure of a certain free category on some generators $\mathcal{A}$.

- Essentially it is MALL with self-dual connectives
- Every proof has an interpretation as an arrow of $F\mathcal{A}$
- Every arrow of $F\mathcal{A}$ has a corresponding proof
- The system is cut-eliminating, and the cut-elimination procedure is sound wrt the interpretation.
Tensor-Sum Logic

Tensor-sum logic is a Gentzen system, designed to capture the structure of a certain free category on some generators $\mathcal{A}$.

- Essentially it is MALL with self-dual connectives
- Every proof has an interpretation as an arrow of $F\mathcal{A}$
- Every arrow of $F\mathcal{A}$ has a corresponding proof
- The system is cut-eliminating, and the cut-elimination procedure is sound wrt the interpretation.

It has some oddities as a logical system:

- Every entailment $A \vdash B$ is derivable with a zero proof
- Self-duality allows the formation of self-cuts
  - the empty sequent is derivable in many inequivalent ways
Proof-nets for tensor and sum

Define a system of proof-nets with non-logical axioms:
Proof-nets for tensor and sum

Define a system of proof-nets with non-logical axioms:
Proof-nets for tensor and sum

Define a system of proof-nets with non-logical axioms:

Theorem: cut-elimination is strongly normalising
Example: teleportation

The shared Bell state and the input qubit:
Example: teleportation

The Bell basis measurement
Example: teleportation

The classically controlled corrections:
Example: teleportation

The whole protocol:
Example: teleportation

The whole protocol:
Example: teleportation
Example: teleportation
Example: teleportation
Example: teleportation
Example: teleportation
Example: teleportation
Example: teleportation
Example: teleportation

\[ Z^2 = 1_Q \]

\[ Y^2 = 1_Q \]

\[ X^2 = 1_Q \]
Example: teleportation
Full completeness

**Theorem:** Let $\mathcal{P}$ be a compact symmetric polycategory. There is an equivalence of categories between $\text{Circ}(\mathcal{P})$ and $\text{PN}(\mathcal{P})$. 
The biproduct

We used the biproduct to encode the branching nature of quantum processes.

- The diagonal map shows the possibility of different choices:
  \[ Q \xrightarrow{\Delta} Q \oplus Q \]

- But what about the codiagonal?
  \[ Q \oplus Q \xrightarrow{\nabla} Q \]

- Semantically this corresponds to superposition rather than probabilistic mixing --- the wrong interpretation

- To properly address the issue of probabilities in QM we use Selinger’s CPM construction
Normal form theorem

Pure logic, determined by premise

A unique A-labelled circuit

Pure logic determined by conclusion
Types for entanglement?

Can we regain the separation between $\otimes$ and $\exists$ to talk about entanglement?

- Entangled states do not form a subspace
- Do double gluing on $\text{fdHilb}$
  - $\otimes$ gives product states
  - $\exists$ gives all states
- Hence $\otimes$ is a subtype of $\exists$
How many types anyway?

**Defn:** A state $S$ is said to be *SLOCC reachable* from state $S’$ if there is a sequence of stochastic local operations and classical communications producing $S$ from $S’$.

**Defn:** If $S$ and $S’$ are mutually SLOCC reachable then they are *SLOCC equivalent*.
How many types anyway?

**Prop:** For 2-qubit states there are 2 SLOCC classes:
How many types anyway?

**Prop:** For 3-qubit states there are 6 SLOCC classes:
How many types anyway?

**Prop:** For 4-qubit states there are *uncountably many* SLOCC classes
How many types anyway?

**Prop:** For 4-qubit states there are *uncountably many* SLOCC classes

Forget about types to describe entanglement

Just look at the terms
The ZX-calculus

Quantum processes, diagrammatically

Ross Duncan • PrakashFest • Oxford 2014
“Classical” Quantum States

When can a quantum state be treated as if classical?

- no-go theorems allow copying and deleting of orthogonal states;

In other words:

- A quantum state may be copied and deleted if it is an eigenstate of some known observable.

We’ll use this property to formalise observables in terms of copying and deleting operations.
Classical Structures

\[ \delta = \quad \epsilon = \quad \delta^\dagger = \quad \epsilon^\dagger = \]

\[ = \quad = \quad = \quad = \]

\[ = \quad = \quad = \quad = \]

\[ = \quad = \quad = \quad = \]

\[ = \quad = \quad = \quad = \]
In other words: a classical structure is a special commutative $\dagger$-Frobenius algebra.
Classical Structures

\[ \delta = \quad \epsilon = \quad \delta^\dagger = \quad \epsilon^\dagger = \]

**Theorem**: in $\text{FDHilb}$, classical structures are in bijective correspondence to bases. [Coecke, Pavlovic, Vicary]
Classical Structures

\[ \delta = \quad \epsilon = \quad \delta^\dagger = \quad \epsilon^\dagger = \]

**Theorem**: in \textbf{FDHilb}, classical structures are in bijective correspondence to bases. [Coecke, Pavlovic, Vicary]

Each (well behaved) observable defines a basis, therefore: every observable defines a classical structure!
Classical Structures

In other words: a classical structure is a special commutative $\dagger$-Frobenius algebra. Theorem: in $\text{FDHilb}$, classical structures are in bijective correspondence to bases. [Coecke, Pavlovic, Vicary]

Each (well behaved) observable defines a basis, therefore: every observable defines a classical structure!

Still not enough!
Enough equations (probably)

Final ingredient: complementarity
Enough equations (probably)

Final ingredient: complementarity

Only 86 pages!
Complementary Observables

\[ |\langle a_i | b_j \rangle| = \frac{1}{\sqrt{D}} \]
Strong Complementarity

Strongly complementary observables form a bialgebra

\[
\begin{align*}
\text{Strongly complementary observables} & \quad \text{bialgebra} \\
\text{Diagram} & \quad \text{Equation}
\end{align*}
\]
Strongly complementary observables form Hopf algebras

Theorem:

Remark: under the assumption of *enough classical points* the “strong” assumption is not needed; simple complementarity suffices
Strong Complementarity

Many useful properties now follow… too many to discuss!

I claim that such interacting algebras are a fundamental new structure for computer science.

See work of Sobocinski and various coauthors

Interacting Bialgebras are Frobenius

Filippo Bonchi\(^1\), Paweł Sobociński\(^2\) and Fabio Zanasi\(^1\)

\(^1\) ENS de Lyon, Université de Lyon, CNRS, INRIA, France
\(^2\) University of Southampton, UK
**ZX-calculus syntax**

**Defn:** A *diagram* is an undirected open graph generated by the above vertices.

**Defn:** Let $\mathbb{D}$ be the dagger compact category of diagrams s.t.

$$(\cdot)^\dagger : \alpha \mapsto -\alpha$$
Equations
Equations

(bialgebra) =

(copying)

(hopf)

(colour change)
Example: 2-Qubit Quantum Fourier Transform

\[ j_1 = |1\rangle \]
\[ j_0 = |0\rangle \]

Input qubits

controlled gate \( Z_{\pi/2} \)

\(-\pi/4\) \( \pi/4\)
Example: 2-Qubit Quantum Fourier Transform

\[ \frac{\pi}{4} \]  

\[ -\frac{\pi}{4} \]  

\[ \frac{\pi}{4} \]
Example: 2-Qubit Quantum Fourier Transform
Example: 2-Qubit Quantum Fourier Transform

\[
\begin{align*}
\frac{\pi}{4} & \\
\pi & \\
\pi & \\
-\frac{\pi}{4} & \\
\frac{\pi}{4} & 
\end{align*}
\]
Example: 2-Qubit Quantum Fourier Transform
Example: 2-Qubit Quantum Fourier Transform
Example: 2-Qubit Quantum Fourier Transform

\[ \pi/4 \quad -\pi/4 \quad \pi \quad \pi/4 \]
Example: 2-Qubit Quantum Fourier Transform

\[ \pi \]

\[ -\pi/4 \quad \pi \quad \pi/4 \]
Example: 2-Qubit Quantum Fourier Transform
Example: 2-Qubit Quantum Fourier Transform
Example: 2-Qubit Quantum Fourier Transform

\[ \begin{align*}
    j_0 &= |0\rangle + e^{i\frac{\pi}{2}} |1\rangle \\
    j_1 &= |0\rangle + e^{i\pi} |1\rangle
\end{align*} \]
Extensions (1)

The calculus as presented does not deal with non-determinism or probabilities. Two extensions:

- Conditional vertices:
  ![Diagram of conditional vertices]
  \( \alpha, S' \)

- Selinger’s CPM construction:
  ![Diagram of Selinger’s CPM construction]
Extensions (2)

The CPM approach was used to prove that strong complementarity is equivalent to non-locality:

... justifying the claim that this is a fundamental notion for QM
The conditional vertices approach was used to prove the correctness of quantum programs:
Extensions (3)

... and error-correcting codes:
Advertising

Graphical tool for doing graphical calculations:

http://dream.inf.ed.ac.uk/projects/quantomatic/
Happy Birthday Prakash!