Introduction & overview

Coalgebra and quantum

Conclusions

General background

Aims of this research line

- Explore quantum computation and logic in relation to well-known computation paradigms:
  - deterministic / non-deterministic / probabilistic / …
- Seek connections especially within the general coalgebraic paradigm for state-based computation.
- Explore logic and probability

Approach

- Semantical, not algorithmic
- Using the language of category theory
  (following Abramsky, Coecke, Baez, …)

Why coalgebras?

- Coalgebras have emerged as a generic formalism for state-based computation, including e.g.
  - its own “coalgebraic modal logic”
  - bisimilarity as observational indistinguishability (with generic ‘bisimilarity-is-congruence’ proofs)
  - canonical (final) models, with sound & complete languages

- The language of quantum mechanics is very much related:
  - states and observations
  - observations disturb the state (have side-effects)
  - ongoing debates about determinism & probability
    (Einstein: God does not play dice; Bohr: internal state is unknown)

Prerequisites for quantum computation

- Do you need to be a quantum physicist to understand quantum computation?
  - NO!
  - One can be a masterful practitioner of computer science without having the foggiest notion of what a transistor is, not to mention how it works
    (David Mermin, Quantum Computer Science. An Introduction.)

- Here, as usual, we only deal with the abstract, mathematical model for quantum computation, not with its possible future realisation — which is work for physicists.

What is needed?

Main prerequisites for quantum computation

- Linear algebra (over complex numbers $\mathbb{C}$)
- Hilbert spaces and/or $C^*$-algebras (esp. finite dimensional)
- Tensors and spectral decomposition

Prerequisites for this talk

- Basic linear algebra
- Basic category theory
What is quantum computing about?

- Letting nature do matrix multiplications for us
- Computations are divided over multiple parallel worlds ("quantum parallelism")
- A new physical basis for computation
- Much focus so far on algorithms and complexity
- More recently also on semantics and quantum languages
  (Abramsky, Coeke, Panangaden, Selinger, . . .)
- Actual, physical realisation of quantum computer still embryonic
  (in the order of 10 qbits)
- Quantum key distribution more developed
  (but also under attack, see quantum hackers)

Quantum mechanics/computation is strange

- Superposition: linear combinations of basic states
- Entanglement of states: explained via tensors  (
- Measurement: side-effect: the state changes to the result of the measurement
  entangled objects are both changed when only one is measured
  Mathematical explanation via diagonalisation of operators
  (using eigenvectors & eigenvalues)

Quantum computation is powerful

- More efficient in certain tasks, via a new form of parallelism
  Notably factorisation of numbers (Shor); threatening for RSA;
- New levels of security, e.g. with key exchange via entanglement

Attractions

- New area inbetween computer science, physics and logic
  Baez & Stay: category theory forms Rosetta Stone
- Great potential for both theory and applications
  Chance to get theory in place before (programming) languages emerge
  Early in CS: programming languages came before theory
  Now we see theory precedes languages (like Quipper, recently), and implementations
- Issues are both familiar and new

What are coalgebras, intuitively?

- Mathematical models for state-based computation
- Basically only two kinds of operations:
  move to a next state, somehow (deterministically, non-deterministically, probabilistically, . . .)
  make an observation ("measurement") about the current state
- These operations can be combined ("observation has side-effect")
  Algebras with "carrier" $X$ are maps into $X$, of the form:
  \[
  \begin{array}{c}
  X \cdot \cdot \cdot X \\
  \end{array} \quad \xrightarrow{\text{construct}} X
  \]

  Coalgebras with "state space" $X$ are maps out of $X$, of the form:
  \[
  \begin{array}{c}
  X \\
  \end{array} \quad \xrightarrow{\text{modify/observe}} \quad \begin{array}{c}
  X \cdot \cdot \cdot X \\
  \end{array}
  \]

  The boxes are functors, usually Sets $\rightarrow$ Sets.
Automata-theoretic coalgebra examples

- A deterministic automaton with input actions \( A \) is a coalgebra:
  \[
  \xymatrix{
    X \ar[r]^-{(\text{step, final})} & X^A \times 2
  }
  \]
  where \( 2 = \{0, 1\} \).
- A non-deterministic automaton, or transition system, with input actions \( A \) is a coalgebra:
  \[
  X \xrightarrow{\text{success}} P(X)^A
  \]
- Other 'monads' than powerset \( P \) may be used: eg. partial automata via lift, or probabilistic automata via distribution.

Distribution monad \( D \)

For a set \( X \), define
\[
D(X) = \{ \varphi : X \to [0, 1] \mid \text{support(\( \varphi \)) is finite, and } \sum_x \varphi(x) = 1 \}
\]
Such \( \varphi \in D(X) \) is a formal convex combination:
\[
r_1x_1 + \cdots + r_nx_n \quad \text{where} \quad \{ \text{support(\( \varphi \))} = \{x_1, \ldots, x_n\} \}
\]
\[
\sum_i r_i = 1 \]
Coalgebras \( X \to D(X) \) are Markov chains, giving probabilistic transitions:
\[
x \xrightarrow{\rho} x' \quad \text{with} \quad \sum_i r_i = 1.
\]

Literature

   - Projective measurements as Eilenberg-Moore coalgebras
   - Discussed (\& extended) in own MFPS’13 contribution

2. Abramsky: LICS’10 / JPL’13
   - Characterises quantum symmetries as bisimilarity

3. Jacobs: FoSSaCS’11
   - Coalgebraic description of certain quantum computations, namely quantum walks

4. Hasuo & Hoshino: LICS’11
   - Quantum monad on \( \text{Sets} \), with quantum lambda model in its Kleisli category

5. Roumen: QPL’12
   - Quantum automata as coalgebras, with minimalisation

6. Furber & Jacobs: CALCO’13
   - Some crucial results will be discussed here.

Relevant mathematical structures

<table>
<thead>
<tr>
<th>Standard Semantics</th>
<th>Quantum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dcpos</td>
<td>Hilbert spaces</td>
</tr>
<tr>
<td>Sets</td>
<td>C*-algebras</td>
</tr>
<tr>
<td>Relations</td>
<td>Partial functions</td>
</tr>
<tr>
<td>Boolean algebras</td>
<td>Effect modules</td>
</tr>
</tbody>
</table>

Probability & quantum theory

Probability Theory

Quantum Theory

- \( C^\ast \)-algebras
- Commutative \( C^\ast \)-algebras
A (unital) $C^*$-algebra is:

- a vector space
- with a (multiplicative) monoid structure $(1, \cdot)$
- an involution $(\cdot)^*: A \to A$
- a complete norm $\| \cdot \|$, satisfying $\|x^* \cdot x\| = \|x\|^2$

The $C^*$-algebra is called:

- commutative if its multiplication is commutative
- finite-dimensional if it is finite-dimensional as vector space

The complex numbers $\mathbb{C}$, with usual multiplication, conjugation $\tau$, and norm.

- Also, each $\mathbb{C}^n$ with pointwise structure
- $L^\infty(X)$, the set of bounded maps $X \to \mathbb{C}$, for a set $X$

For a compact Hausdorff space $X$, the set $C(X)$ of continuous maps $X \to \mathbb{C}$.

According to Gelfand’s duality theorem, this is the general form of a commutative $C^*$-algebra.

The algebra $\text{Mat}_n(\mathbb{C})$ of $n \times n$ matrices over $\mathbb{C}$, with multiplication, complex conjugation $(\cdot)^*$, and operator norm.

In fact, each finite-dimensional $C^*$-algebra is a product of such matrix algebras:

$$\text{Mat}_n(\mathbb{C}) \oplus \cdots \oplus \text{Mat}_m(\mathbb{C})$$

The algebra $L(H)$ of bounded operators $H \to H$, for a Hilbert space $H$.

Each $C^*$-algebra $A$ can be described as subalgebra $A \hookrightarrow L(H)$, for some Hilbert space $H$. This is “Gelfand-Naimark”

A linear map $f: A \to B$ between $C^*$-algebras is called:

- unital (U), if $f(1) = 1$
- positive (P), if $a \geq 0 \Rightarrow f(a) \geq 0$
  (where $a \geq 0$ means $a = x^*x$, for some $x$)
- multiplicative (M), if $f(a \cdot a') = f(a) \cdot f(a')$
- involutive (I), if $f(a^*) = f(a)^*$

FACTS

- $PU \Rightarrow I$ and $MIU \Rightarrow PU$
- We use categories $\text{Cstar}_{\text{MIU}}$ and $\text{Cstar}_{\text{PU}} \hookrightarrow \text{Cstar}_{\text{MIU}}$ (plus commutative/finite-dimensional variations)

MIU- and PU-maps

- MIU-maps are usually called *-homomorphisms; they are the “standard” maps in $C^*$-algebra theory
- Gelfand duality says: $CH \cong \left(\text{Cstar}_{\text{MIU}}\right)^{op}$
- However, MIU-maps are very restrictive, and PU-maps are “undervalued”
- (There are also completely positive maps, but they are skipped here)

For $n, m \in \mathbb{N}$, there is a bijective correspondence:

$$\text{MIU-maps } \mathbb{C}^n \longrightarrow \mathbb{C}^m$$

functions $m \longrightarrow n$

Essentially, this is the finite-dimensional version of Gelfand duality:

$$\text{FinSets} \cong \left(\text{FdCstar}_{\text{MIU}}\right)^{op}$$
Proof of the correspondence.

- Each $f : m \to n$ obviously gives $(-) \circ f : \mathbb{C}^m \to \mathbb{C}^n$. It preserves the (pointwise) structure.

- Assume $\varphi : \mathbb{C}^n \to \mathbb{C}^n$ is a MIU map. Write the standard base vectors as $|i\rangle = (0, \ldots, 0, 1, 0, \ldots, 0) \in \mathbb{C}^n$.

Since $|i\rangle \cdot |j\rangle = |i\rangle$, we get $\varphi(|i\rangle) \cdot \varphi(|j\rangle) = \varphi(|i\rangle)$, so that $\varphi(|i\rangle) = (r_{i1}, \ldots, r_{in}) \in \mathbb{C}^m$ consists of $r_j \in \{0, 1\}$.  

Since $\sum_i |i\rangle = 1 \in \mathbb{C}^n$, we get $\sum_i \varphi(|i\rangle) = \varphi(1) = 1 \in \mathbb{C}^m$, so that $\sum_j r_j = 1$, for each $j \leq m$.

But then: for each $j \leq m$ there is precisely one $i \leq n$ with a $r_j = 1$. This yields a function $m \to n$. □

For $n, m \in \mathbb{N}$, there is a bijective correspondence:

\[
\begin{align*}
\text{PU-maps} & \quad \mathbb{C}^n \quad \mathbb{C}^m \\
\text{functions} & \quad m \quad D(n)
\end{align*}
\]

where $D$ is the distribution monad.

This gives "probabilistic" Gelfand duality, in the finite case:

\[
\mathcal{K}(D) \simeq (\mathcal{F}(\mathbb{C}^{\operatorname{star}}\mathbb{P}))^\text{op}
\]

where $\mathcal{K}(D) \hookrightarrow \mathcal{K}(D)$ is the full subcategory with numbers $n \in \mathbb{N}$ as objects.

Thus, $\mathcal{F}(\mathbb{C}^{\operatorname{star}}\mathbb{P})$ is the Lawvere theory of the distribution monad.

Proof of the correspondence.

- Each $f : m \to D(n)$ gives a map $\mathbb{C}^n \to \mathbb{C}^m$ by:

\[
\nu \mapsto \lambda \leq m. \sum_{j \leq m} f(j) |j\rangle \cdot \nu(j)
\]

- Assume $\varphi : \mathbb{C}^n \to \mathbb{C}^m$ is a PU map. The base vector $|i\rangle \in \mathbb{C}^n$ is positive, and so $\varphi(|i\rangle) = (r_{i1}, \ldots, r_{in}) \in \mathbb{C}^m$ consists of positive (real) numbers $r_j$.

As before, $\sum_i \varphi(|i\rangle) = \varphi(1) = 1 \in \mathbb{C}^m$, so for each $j \leq m$ we have $\sum_i r_j = 1$.

Thus we get the required map $m \to D(n)$. □

In (Furber & Jacobs, CALCO’13) it is shown that:

- There is a Radon monad $\mathcal{R} : \mathcal{C} \to \mathcal{C}$ on the category $\mathcal{C}$ of compact Hausdorff spaces

This monad $\mathcal{R}$ is given by states of the $\mathbb{C}^*$-algebra $\mathbb{C}(X)$:

\[
\mathcal{R}(X) = \text{Hom}_{\mathbb{P}}(\mathbb{C}(X), \mathbb{C})
\]

- We then get:

\[
\mathcal{K}(\mathcal{R}) \simeq (\mathbb{C}^{\star\mathbb{P}})^{\text{op}}
\]

“Coalgebra and Quantum” is relatively unexplored area

there is clearly overlapping terminology

In the mathematical description of the quantum world $\mathbb{C}^*$-algebras play an important role

- commutative $\mathbb{C}^*$-algebras capture (classical) probability

These commutative $\mathbb{C}^*$-algebras, with positive unital maps, can be described as Kleisli categories of monads

endomaps thus correspond to coalgebras (of the monad)

The general, non-commutative case does not have a crisp categorical description (yet)

- possibly, the quantum monad of Hasuo & Hoshino helps

- alternatively, Hughes’ arrows (instead of monads) could be used, following Vizzotto, Altenkirch, Sabry (2006)