Coalgebra and Quantum Computing

Bart Jacobs

Institute for Computing and Information Sciences – Digital Security
Radboud University Nijmegen

MFPS 2013

Outline

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 unkown)

Prerequisites for quantum computation

- Do you need to be a quantum physicist to understand quantum computation?
- **NO!**

  > *One can be a masterful practioner 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 parallellism")
- 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

The three strangest phenomena

- **Superposition**: linear combinations of basic states
- **Entanglement** of states: explained via tensors $\otimes$
- **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 parallellism
  - 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")

(Co)algebras, pictorially

Algebras with "carrier" X are maps into X, of the form:

$$\boxed{X \quad \cdots \quad X} \xrightarrow[\text{construct}]{} X$$

Coalgebras with "state space" X are maps out of X, of the form:

$$X \xrightarrow[\text{modify/observe}]{} \boxed{X \quad \cdots \quad X}$$

The boxes are functors, usually **Sets** $\to$ **Sets**.

Automata-theoretic coalgebra examples

- A deterministic automaton with input actions A is a coalgebra:
$$X \xrightarrow{\langle \text{step}, \text{final?} \rangle} X^A \times 2$$
where $2 = \{0, 1\}$.
- A non-deterministic automaton, or transition system, with input actions A is a coalgebra:
$$X \xrightarrow{\text{succs}} \mathcal{P}(X)^A$$
- Other 'monads' than powerset $\mathcal{P}$ may be used: eg. partial automata via lift, or probabilistic automata via distribution.

Distribution monad $\mathcal{D}$

For a set X, define

$$\mathcal{D}(X) \;=\; \{\varphi\colon X \to [0,1] \mid \text{support}(\varphi) \text{ is finite, and } \textstyle\sum_x \varphi(x) = 1\}$$

Such $\varphi \in \mathcal{D}(X)$ is a formal convex combination:

$$r_1 x_1 + \cdots + r_n x_n \quad \text{where} \quad \begin{cases} \text{support}(\varphi) = \{x_1, \ldots, x_n\} \\ r_i = \varphi(x_i) > 0 \\ r_1 + \cdots + r_n = 1 \end{cases}$$

Coalgebras $X \to \mathcal{D}(X)$ are Markov chains, giving probabilistic transitions:
$$x \xrightarrow{r_i} x_i \quad \text{with} \quad \textstyle\sum_i r_i = 1.$$

Literature

1. **Coecke & Pavlović**: 2008
   - 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 **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

Standard Semantics **Quantum**

Dcpos Hilbert spaces

C^*-algebras

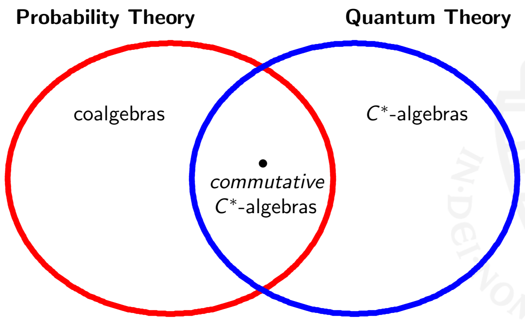
Relations

Sets

Partial functions

Boolean algebras Effect modules

Probability & quantum theory



Relevant questions

1. Is there a way to relate *commutative* C^*-algebras and coalgebraic / monadic computation?
2. What is coalgebraic / monadic about C^*-algebras in general (the proper quantum case)?

The second question has no clear answer yet, but there is more to say about the first one.

A C^*-algebra crash course

A (unital) C^*-algebra is:

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

Commutative C^*-algebra examples

1. The complex numbers $\mathbb{C}$, with usual multiplication, conjugation $\overline{-}$, and norm.
   - Also, each $\mathbb{C}^n$ with pointwise structure
   - $\ell^\infty(X)$, the set of bounded maps $X \to \mathbb{C}$, for a set X
2. 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.

Non-commutative C^*-algebra examples

1. The algebra $\mathrm{Mat}_n(\mathbb{C})$ of $n \times n$ matrices over $\mathbb{C}$, with multiplication, complex conjugation $(-)^\dagger$, and operator norm

   In fact, each finite-dimensional C^*-algebra is a product of such matrix algebras:
   $$\mathrm{Mat}_{n_1}(\mathbb{C}) \oplus \cdots \oplus \mathrm{Mat}_{n_k}(\mathbb{C})$$
2. The algebra $\mathcal{L}(H)$ of bounded operators $H \to H$, for a Hilbert space H.

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

Maps between C^*-algebras

A linear map $f \colon A \to B$ 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 $\mathbf{Cstar}_{\mathrm{MIU}}$ and $\mathbf{Cstar}_{\mathrm{PU}} \hookleftarrow \mathbf{Cstar}_{\mathrm{MIU}}$
(plus commutative/finite-dimensional variations)

MIU and PU maps

- MIU-maps are usally called $*$-homomorphisms; they are the "standard" maps in C^*-algebra theory
- Gelfand duality says: $\mathbf{CH} \simeq \left(\mathbf{CCstar}_{\mathrm{MIU}}\right)^{\mathrm{op}}$
- However, MIU-maps are very restrictive, and PU-maps are "undervalued"
- (There are also completely positive maps, but they are skipped here)

MIU-maps example

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

$$\begin{array}{c} \text{MIU-maps} \quad \mathbb{C}^n \longrightarrow \mathbb{C}^m \\ \hline\hline \text{functions} \quad m \longrightarrow n \end{array}$$

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

$$\mathbf{FinSets} \simeq \left(\mathbf{FdCCstar}_{\mathrm{MIU}}\right)^{\mathrm{op}}$$

MIU-maps example, continued

Proof of the correspondence.

- Each $f\colon m \to n$ obviously gives $(-) \circ f\colon \mathbb{C}^n \to \mathbb{C}^m$. It preserves the (pointwise) structure.
- Assume $\varphi\colon \mathbb{C}^n \to \mathbb{C}^m$ is a MIU map. Write the standard base vectors as $|i\rangle = (0, \ldots, 0, 1, 0, \ldots, 0) \in \mathbb{C}^n$.
  Since $|i\rangle \cdot |i\rangle = |i\rangle$, we get $\varphi(|i\rangle) \cdot \varphi(|i\rangle) = \varphi(|i\rangle)$, so that $\varphi(|i\rangle) = (r_{i1}, \ldots, r_{im}) \in \mathbb{C}^m$ consists of $r_{ij} \in \{0, 1\}$.
  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 $\sum_i r_{ij} = 1$, for each $j \leq m$.
  But then: for each $j \leq m$ there is precisely one $i \leq n$ with a $r_{ij} = 1$. This yields a function $m \to n$. □

PU-maps example

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

$$\frac{\text{PU-maps } \mathbb{C}^n \longrightarrow \mathbb{C}^m}{\text{functions } m \longrightarrow \mathcal{D}(n)}$$

where $\mathcal{D}$ is the distribution monad.

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

$$\mathcal{K}\ell_{\mathbb{N}}(\mathcal{D}) \simeq \left(\mathbf{FdCCstar}_{\mathrm{PU}}\right)^{\mathrm{op}}$$

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

Thus, $\mathbf{FdCCstar}_{\mathrm{PU}}$ is the Lawvere theory of the distribution monad

PU-maps example, continued

Proof of the correspondence.

- Each $f\colon m \to \mathcal{D}(n)$ gives a map $\mathbb{C}^n \to \mathbb{C}^m$ by:
$$v \longmapsto \lambda j \leq m.\ \sum_{i \leq n} f(j)(i) \cdot v(i)$$
- Assume $\varphi\colon \mathbb{C}^n \to \mathbb{C}^m$ is a PU map. The base vector $|i\rangle \in \mathbb{C}^n$ is positive, and so $\varphi(|i\rangle) = (r_{i1}, \ldots, r_{im}) \in \mathbb{C}^m$ consists of positive (real) numbers r_{ij}
  As before, $\sum_i \varphi(|i\rangle) = \varphi(1) = 1 \in \mathbb{C}^m$, so for each $j \leq m$ we have $\sum_i r_{ij} = 1$.
  Thus we get the required map $m \to \mathcal{D}(n)$. □

Beyond the finite-dimensional case

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

- There is a Radon monad $\mathcal{R}\colon \mathbf{CH} \to \mathbf{CH}$ on the category **CH** of compact Hausdorff spaces
- This monad $\mathcal{R}$ is given by states of the C^*-algebra $C(X)$:
$$\mathcal{R}(X) = \mathrm{Hom}_{\mathrm{PU}}(C(X), \mathbb{C})$$
- We then get::
$$\mathcal{K}\ell(\mathcal{R}) \simeq \left(\mathbf{CCstar}_{\mathrm{PU}}\right)^{\mathrm{op}}$$

Final remarks

- "Coalgebra and Quantum" is relatively unexplored area
  - there is clearly overlapping terminology
- In the mathematical description of the quantum world C^*-algebras play an important role
  - *commutative* C^*-algebras capture (classical) probability
- These commutative 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)