Program Semantics, according to Heisenberg and to Schrödinger

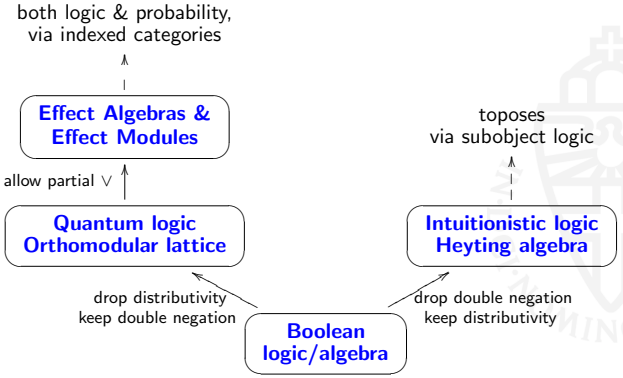
Bart Jacobs

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

IFIP WG1.3 2013

Outline

From Boolean to intuitionistic & quantum logic



A bird's eye view on non-deterministic computation I

- Semantics of non-determinsitic program is given by:
  - relations $R \subseteq X \times Y$, or, more categorically:
  - functions $X \to \mathcal{P}(Y)$, ie. maps in the Kleisli category $\mathcal{K}\ell(\mathcal{P})$
- Full & faithful functor "from Kleisli to Eilenberg-Moore"
  - here: $\mathcal{K}\ell(\mathcal{P}) \to \mathcal{EM}(\mathcal{P}) = \mathbf{CL}_\vee$
  - where $\mathbf{CL}_\vee$ is complete lattices with join-preserving maps
- According to Dijkstra, each program $s\colon X \to \mathcal{P}(Y)$ gives weakest precondition operation $\mathrm{wp}(s)\colon \mathcal{P}(Y) \to \mathcal{P}(X)$
  - Explicitly, $\mathrm{wp}(s)(Q) = \{x \mid s(x) \subseteq Q\}$
  - $\mathrm{wp}(s)$ preserves meets, so is map in $\mathbf{CL}_\wedge$

A bird's eye view on non-deterministic computation II

There are bijective correspondences:

$$\begin{array}{ll} X \xrightarrow{s} \mathcal{P}(Y) & \\ \hline \mathcal{P}(X) \longrightarrow \mathcal{P}(Y) & \bigvee\text{-preserving} \\ \hline \mathcal{P}(Y) \xrightarrow[\mathrm{wp}(s)]{} \mathcal{P}(X) & \bigwedge\text{-preserving} \end{array}$$

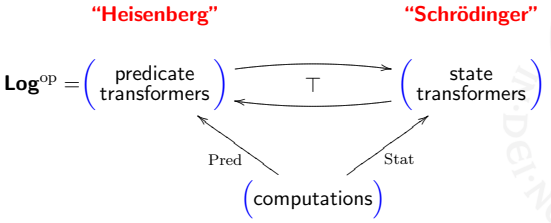
More categorically, there is a commuting diagram:

$$\begin{array}{ccc} (\mathbf{CL}_\wedge)^{\mathrm{op}} & \xrightarrow[\mathrm{Pred}]{\cong} & \mathbf{CL}_\vee = \mathcal{EM}(\mathcal{P}) \\ & \underset{\mathcal{K}\ell(\mathcal{P})}{\overset{\mathrm{Stat}}{\nwarrow}} & \end{array}$$

- The "predicate" and "state" functors $\mathrm{Pred}, \mathrm{Stat}$ are f&f
- $\mathrm{Pred}(s) = \mathrm{wp}(s) =$ "substitution", for Kleisli maps $X \xrightarrow{s} \mathcal{P}(Y)$

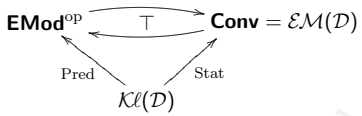
State-effect triangles

The general picture that emerges is:

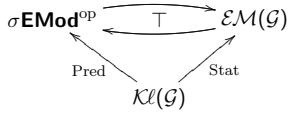


Probabilistic computation: discrete and continuous

For the distribution monad $\mathcal{D}$: **Sets** $\to$ **Sets**:

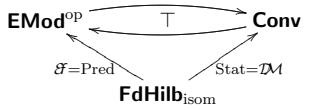


And for the Giry monad $\mathcal{G}$: **Meas** $\to$ **Meas** (see LICS'13):

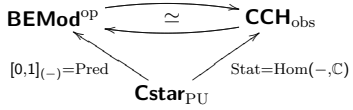


In the quantum case

Using Hilbert spaces:



And using C^*-algebras (see later):



where **BEMod** contains complete "Banach" effect modules, and $\mathbf{CCH}_{\mathrm{obs}}$ contains convex compact Hausdorff spaces.

Effect algebras, definition

Effect algebras generalise the unit interval $[0,1]$ with its (partial!) addition $+$ and "negation" $x \mapsto 1 - x$.

A Partial Commutative Monoid (PCM) consists of a set M with zero $0 \in M$ and partial operation $\circledcirc\colon M \times M \to M$, which is suitably commutative and associative.

One writes $x \perp y$ if $x \circledcirc y$ is defined.

An effect algebra is a PCM in which each element x has a unique 'orthosuplement' $x^\perp$ with $x \circledcirc x^\perp = 1\ (= 0^\perp)$
Additionally, $x \perp 1 \Rightarrow x = 0$ must hold.

Effect algebras, main examples

1. Projections / closed subspaces on a Hilbert space form an effect algebra; $P^\perp$ is orthocomplement:
$$\langle x \,|\, y \rangle = 0 \qquad \text{for all } x \in P, y \in P^\perp$$
2. Orthomodular lattices are effect algebras, with $\circledcirc$ as join $x \vee y$ only for elements with $x \perp y$, i.e. $x \leq y^\perp$
3. Each Boolean algebra is an effect algebra: it is a distributive orthomodular lattice, in which $x \perp y$ iff $x \wedge y = 0$.
   In particular, the Boolean algebra of measurable subsets of a measure space forms an effect algebra, where $U \circledcirc V$ is defined if $U \cap V = \emptyset$, and is then equal to $U \cup V$.

Effect algebras with countable sums

- Each effect algebra is a partial order, via $x \leq y$ iff $y = x \circledcirc z$, for some z.
- One speaks of a σ-effect algebra if countable joins (wrt. $\leq$) exist.
- Examples are $[0,1]$, but also measurable subsets $\Sigma_X \subseteq \mathcal{P}(X)$, wrt. a measurable space (X, Σ_X).

Homomorphisms of effect algebras

DEFINITION

A homomorphism of effect algebras $f\colon X \to Y$ satisfies:

- $f(1) = 1$
- if $x \perp x'$ then both $f(x) \perp f(x')$ and $f(x \circledcirc x') = f(x) \circledcirc f(x')$.

This yields a category **EA** of effect algebras.

The subcategory $\sigma\mathbf{EA} \hookrightarrow \mathbf{EA}$ contains σ-algebras with maps also preserving countable joins.

Examples:

- There is a functor $\mathbf{Meas}^{\mathrm{op}} \to \sigma\mathbf{EA}$, via $(A, \Sigma_X) \mapsto \Sigma_X$
- A probability measure is a map $\Sigma_X \to [0,1]$ in $\sigma\mathbf{EA}$.

Effect modules

Effect modules are effect algebras with a scalar multiplication, with scalars not from $\mathbb{R}$ or $\mathbb{C}$, but from $[0,1]$.

DEFINITION

A (σ-)effect module M is a (σ-)effect algebra with an action $[0,1] \times M \to M$ that is a "bihomomorphism"

A map of effect modules is a map of effect algebras that commutes with scalar multiplication.

We get a category **EMod**, with subcategory σ**EMod** $\hookrightarrow$ **EMod**.

Effect modules, main examples

Probabilistic examples

- Fuzzy predicates $[0,1]^X$ on a set X, with scalar multiplication
$$r \cdot p \stackrel{\text{def}}{=} \lambda x \in X.\, r \cdot p(x).$$
- Measurable predicates $\mathrm{Hom}(X, [0,1])$, for a measurable space X, with the same scalar multiplication.

Quantum examples

- Effects $\mathcal{E}(H)$ on a Hilbert space: operators $A\colon H \to H$ satisfying $0 \leq A \leq I$, with scalar multiplication $(r, A) \mapsto rA$.
- Effects in a C^*-algebra A: positive elements below the unit:
$$[0,1]_A = \{a \in A \mid 0 \leq a \leq 1\}.$$

This one covers the previous three illustrations.

The discrete probability distribution monad

The (discrete probability) distribution monad on a set X:

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

Elements of $\mathcal{D}(X)$ are formal convex combinations $\sum_i r_i x_i$ where

- $\mathrm{supp}(\varphi) = \{x_1, \ldots, x_n\} \subseteq X$
- $r_i = \varphi(x_i) \in [0,1]$, so that $\sum_i r_i = 1$.

Algebras of the distribution monad $\mathcal{D}$

- Eilenberg-Moore $\mathcal{D}(X) \xrightarrow{\alpha} X$ make X into a convex set: each *formal* convex combination $\sum_i r_i x_i$ has an interpretation as *actual* sum $\sum_i r_i x_i = \alpha(\sum_i r_i x_i) \in X$.
- Note, no $\mathbb{R}$-module structure is assumed on X; just this.
- There are equivalent descriptions as sums $x +_r y$, to be thought of as $rx + (1-r)y$
  - see Stone (1948) & Swirszcz (1974), and more recently Keimel & Doberkat
- Easy examples of convex set: $[0,1]$, or $[0,1]^A$.
- Write **Conv** $= \mathcal{EM}(\mathcal{D})$ for the category of convex sets
  - maps are affine functions, preserving convex sums

Basic adjunction, between effects and states [Ifip TCS'10]

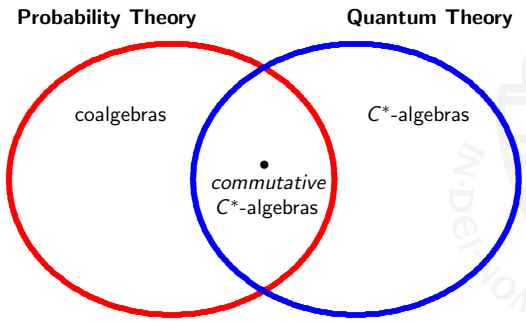
Theorem By "homming into $[0,1]$" one gets an adjunction:

$$\mathbf{EMod}^{\mathrm{op}} \underset{\mathbf{Conv}(-,[0,1])}{\overset{\mathbf{EMod}(-,[0,1])}{\rightleftarrows}} \mathbf{Conv} \quad (\top)$$

This adjunction restricts to an equivalence between:

- Banach effect modules, which have a complete norm
- convex compact Hausdorff spaces

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 $\mathbf{Cstar}_{\mathrm{PU}} \hookrightarrow \mathbf{Cstar}_{\mathrm{MIU}}$ (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:

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

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 $f : m \to n$ obviously gives $(-) \circ f : \mathbb{C}^n \to \mathbb{C}^m$. It preserves the (pointwise) structure.
- Assume $\varphi : \mathbb{C}^n \to \mathbb{C}^m$ 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 $f : m \to \mathcal{D}(n)$ 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 $\varphi : \mathbb{C}^n \to \mathbb{C}^m$ 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 $\mathcal{R} : \mathbf{CH} \to \mathbf{CH}$ on the category $\mathbf{CH}$ 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

- States-and-effect triangles capture basic structure in program semantics
  - duality between state- and predicate-transformations
- In the mathematical description of the quantum world C^*-algebras (and also W^*-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)