# On Block Structures in Quantum Computation

Bart Jacobs

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

MFPS 2013





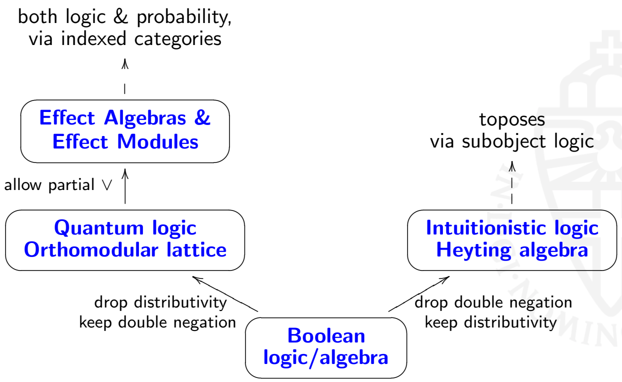
## Outline







## Quantum logic: new generalisation & challenges








## Effect algebras, definition

Effect algebras generalise the unit interval $[0,1]$ with (partial!) addition.

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

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

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

For $x \in [0,1]$ the orthosuplement is $x^\perp = 1 - x$.





## 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 $\ovee$ 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 $U \ovee V$ is defined if $U \cap V = \emptyset$, and is then equal to $U \cup V$.





## 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 $f(x \ovee x') = f(x) \ovee f(x')$.

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

A state of an effect algebra $X$ is a homomorphism $X \to [0,1]$.

A state of a measurable space is the same as a (finitely additive) measure.

## 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**

An effect module $M$ is an 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. This yields a category **EMod**.





## Effect modules, main examples

1. Effects $\mathcal{E}(H)$ on a Hilbert space: operators $A: H \to H$ satisfying $0 \leq A \leq I$, with scalar multiplication $(r, A) \mapsto rA$.
2. Fuzzy predicates $[0,1]^X$ on a set $X$, with scalar multiplication
$$r \cdot p \stackrel{\text{def}}{=} \lambda x \in X.\, r \cdot p(x).$$
3. Measurable predicates $\mathrm{Hom}(X, [0,1])$, for a measurable space $X$, with the same scalar multiplication.
4. 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.





## Effect modules, as indexed category

All the previous examples lead to functors / indexed categories of the form $\mathbf{B} \to \mathbf{EMod}^{\mathrm{op}}$, used for predicate logic

1. fuzzy predicates $[0,1]^{(-)}: \mathcal{K}\ell(\mathcal{D}) \to \mathbf{EMod}^{\mathrm{op}}$, on the Kleisli category of the distribution monad $\mathcal{D}$
2. measurable predicates $\mathcal{K}\ell(\mathcal{G}) \to \mathbf{EMod}^{\mathrm{op}}$ for the Giry monad $\mathcal{G}$ (see my LICS'13 paper)
3. Hilbert space effects $\mathbf{Hilb}_{\mathrm{isom}} \to \mathbf{EMod}^{\mathrm{op}}$ using only isometries (dagger monos) as morphisms
4. $C^*$-algebra effects, $[0,1]_{(-)}: \mathbf{Cstar}_{\mathrm{PU}} \to \mathbf{EMod}^{\mathrm{op}}$ using positive unital maps as morphisms.





## The predicate logic of effects

- These four indexed categories $\mathbf{B} \to \mathbf{EMod}^{\mathrm{op}}$ capture the essence of (probabilistic & quantum) predicate logic
- There is more (dynamical) logical structure, but it is not needed here
- We will need certain characteristic maps later





## Blocks in imperative programming

- Typical block structure:

```
{int v = 0; ...; return}
```

- temporary extension of the state space: opened by initialisation of variables, and closed by a return statement.





## Corresponding idea in quantum programming

- Quantum programs are standardly modelled as completely positive maps (acting on density matrices, or $C^*$-algebras)
- According to Stinespring's theorem, each such completely postive $S: \mathcal{DM}(H) \to \mathcal{DM}(H)$ is of the form:
$$S(\rho) = \mathrm{tr}_K\Big(U(\rho \otimes \xi)U^{\dagger}\Big)$$
- where:
  - $U$ is a unitary operator on a state space $H \otimes K$ enlarging $H$ with an "ancilla" space $K$
  - $\xi$ is an "initial" pure state $|v\rangle\langle v|$ for some vector $|v\rangle \in K$
  - $\mathrm{tr}_K$ is the partial trace operation, acting as "return"

## First steps towards general approach

**DEFINITION**

A block structure on a category **A** consists of:

- endofunctors $\mathcal{B}_n \colon \mathbf{A} \to \mathbf{A}$, for $n > 0$, with natural isos:

$$\mathcal{B}_1(X) \cong X \qquad \mathcal{B}_m(\mathcal{B}_n(X)) \cong \mathcal{B}_{m\times n}(X),$$

- two collections of natural transformations $in_n \colon \mathrm{Id} \Rightarrow \mathcal{B}_n$ and $out_n \colon \mathcal{B}_n \Rightarrow \mathrm{Id}$ with $out_n \circ in_n = \mathrm{id}$, as in:

$$\begin{array}{ccc} X & \xrightarrow{in_n} & \mathcal{B}_n(X) \\ & \searrow^{=} & \downarrow{\scriptstyle out_n} \\ & & X \end{array}$$





## A basic result

If a category **A** has coproducts $+$, then for each $n > 0$, the $n$-fold copower functor $n \cdot (-) \colon \mathbf{A} \to \mathbf{A}$ yields the copower comonad, where

$$n \cdot X = \underbrace{X + \cdots + X}_{n \text{ times}}$$

Its $\varepsilon \colon n \cdot X \to X$ and $\delta \colon n \cdot X \to n \cdot (n \cdot X)$ are:

$$\varepsilon = \nabla = [\mathrm{id}, \ldots, \mathrm{id}] \qquad \delta = \kappa_1 + \cdots + \kappa_n = [\kappa_i \circ \kappa_i]_{i \leq n}.$$

Dually, products $\times$, yields the power monad $(-)^n$.





## Example: blocks in $\mathcal{K}\ell(\mathcal{D})$

- Take $\mathcal{B}_n(X) = n \cdot X$, with counit $out = \varepsilon = \nabla \colon \mathcal{B}_n(X) \to X$
- An obvious "in" map uses uniform distribution

$$X \xrightarrow{in_n} n \cdot X \quad \text{where} \quad x \longmapsto \tfrac{1}{n}\kappa_1 x + \cdots + \tfrac{1}{n}\kappa_n x.$$

- The equation $out \circ in = \mathrm{id}$ involves Kleisli composition
- Also power $(-)^n$ forms a block structure on $\mathcal{K}\ell(\mathcal{D})$, see paper





## Example: blocks in $\mathcal{K}\ell(\mathcal{P}) = \mathbf{Rel}$

- Recall that the category $\mathcal{K}\ell(\mathcal{P}) = \mathbf{Rel}$
  - is used as model for non-deterministic computation
  - has $+$ has biproduct (both product and coproduct)
- Now copower comonad $n \cdot (-)$ and power monad $(-)^n$ coincide
- We get a block structure with (co)diagonals:

$$\begin{array}{ccc} X & \xrightarrow{in = \Delta} & n \cdot X \\ & \searrow^{=} & \downarrow{\scriptstyle out = \nabla} \\ & & X \end{array}$$





## Example: blocks in **Hilb**

- Also the category **Hilb** has biproducts: the direct sum $\oplus$ is both a product and coproduct
- Now we need to use a scaling factor for (co)diagonals, as in:

$$\begin{array}{ccc} X & \xrightarrow{in = \frac{1}{\sqrt{n}}\Delta} & n \cdot X \\ & \searrow^{=} & \downarrow{\scriptstyle out = \frac{1}{\sqrt{n}}\nabla} \\ & & X \end{array}$$

We have $out \circ in = \mathrm{id}$, with $out = in^{\dagger}$, making $in$ a dagger mono.





## Charcteristic maps

- Assume a predicate logic (model) $Pred \colon \mathbf{A} \to \mathbf{EMod}^{\mathrm{op}}$, with:
  - for a map $f$ in **A** there is substitution $Pred(f) = f^{-1}$
  - there is a block structure $\mathcal{B}_n \colon \mathbf{A} \to \mathbf{A}$
- An $n$-test on $X \in \mathbf{A}$ is an $n$-tuple $p = (p_1, \ldots, p_n)$ of predicates $p_i \in Pred(X)$ with $p_1 \ovee \cdots \ovee p_n = 1$.

**DEFINITION, of logical block structure**

1. for each $X \in \mathbf{A}$ and $n > 0$ there is a "universal" $n$-test given by $\Omega_i \in \mathcal{B}_n(X)$, stable under substitution
2. for each $n$-test $p = (p_1, \ldots, p_n)$ on $X$, there is a characteristic map $char_p \colon X \to \mathcal{B}_n(X)$ in **A** with $char_p^{-1}(\Omega_i) = p_i$.

The $char_p$ maps open a block, following the test $p$

## Non-deterministic computation: $\mathcal{K}\ell(\mathcal{P}) = \mathbf{Rel}$

- Formal point: we have a logic $Pred\colon \mathcal{K}\ell(\mathcal{P}) \to \mathbf{EA}^{\mathrm{op}}$, forming effect modules over $\{0,1\}$ instead of $[0,1]$.
- On objects, we have classical predicates $Pred(X) = \mathcal{P}(X)$. A test in it consists of *disjoint* subsets $U_i \in \mathcal{P}(X)$ with $U_1 \cup \cdots \cup U_n = X$.
- We have $\Omega_i = \{\kappa_i x \mid x \in X\} \subseteq n \cdot X = \mathcal{B}_n(X)$
- For test $U_i \in \mathcal{P}(X)$ can define by disjointness:

$$X \xrightarrow{char_U} \mathcal{B}_n(X) \quad \text{by} \quad x \longmapsto \{\kappa_i x\}, \quad \text{if } x \in U_i.$$





## $\mathcal{K}\ell(\mathcal{P}) = \mathbf{Rel}$ example, continued

- We have $char_U\colon X \to \mathcal{B}_n(X)$, where $\mathcal{B}_n = n \cdot (-)$ is the copower comonad on $\mathcal{K}\ell(\mathcal{P})$

  An obvious question is: when is $char_U$ an Eilenberg-Moore coalgebra?
- There is a clear answer, via a bijective correspondence:

$$\frac{\text{Boolean } n\text{-tests } U = (U_1, \ldots, U_n) \text{ in } \mathcal{P}(X)}{\text{Eilenberg-Moore coalgebras } X \longrightarrow \mathcal{B}_n(X) \text{ in } \mathcal{K}\ell(\mathcal{P})}$$

- Given a coalgebra $c\colon X \to n \cdot X$, we get an $n$-test with predicates $U_i = \{x \mid \kappa_i x \in c(x)\}$.





## Probabilistic computation example: $\mathcal{K}\ell(\mathcal{D})$

- Logic of fuzzy predicates $[0,1]^{(-)}\colon \mathcal{K}\ell(\mathcal{D}) \to \mathbf{EMod}^{\mathrm{op}}$
- an $n$-test $p_i \in [0,1]^X$ satisfies $p_1(x) + \cdots + p_n(x) = 1$.
- Generic predicate $\Omega_i \in [0,1]^{n \cdot X}$, with $\Omega_i(\kappa_j x) = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$
- For $n$-test $p$ on $X$, there is in $\mathcal{K}\ell(\mathcal{D})$ via the convex sum:

$$char_p(x) = p_1(x)\kappa_1 x + \cdots + p_n(x)\kappa_n x,$$

  It opens a block of options, in a probabilistic manner.





## $\mathcal{K}\ell(\mathcal{D})$ example, continued

- Again we have the coalgebra question. It works here only for a subset of $n$-tests, the projections, with $p_i^2 = p_i$.
- Then: $p_i(x) \in \{0,1\} \subseteq [0,1]$, so projections correspond to subsets.
- Thus we have correspondences:

$$\frac{\dfrac{\text{Boolean } n\text{-tests } U = (U_1, \ldots, U_n) \text{ in } \mathcal{P}(X)}{n\text{-tests of projections } p = (p_1, \ldots, p_n) \text{ in } [0,1]^X \text{ with } p_i^2 = p_i}}{\text{Eilenberg-Moore coalgebras } X \longrightarrow \mathcal{B}_n(X) \text{ in } \mathcal{K}\ell(\mathcal{D})}$$





## Continuous probabilistic computation

$\mathcal{K}\ell(\mathcal{G}) \to \mathbf{EMod}^{\mathrm{op}}$ behaves exactly as $\mathcal{K}\ell(\mathcal{D}) \to \mathbf{EMod}^{\mathrm{op}}$.

See paper for details





## Example: computation in Hilbert spaces

- Effect logic: $\mathcal{E}f\colon \mathbf{Hilb}_{\mathrm{isom}} \to \mathbf{EMod}^{\mathrm{op}}$
- $\mathcal{B}_n(H) = n \cdot H = H \oplus \cdots \oplus H$ endofunctor on $\mathbf{Hilb}_{\mathrm{isom}}$
  - with $in = \frac{1}{\sqrt{n}}\Delta$, as it is a dagger mono
  - but not with $out = \frac{1}{\sqrt{n}}\nabla$, as it is a dagger epi

  Hence this **does not** give a block structure on $\mathbf{Hilb}_{\mathrm{isom}}$.
- But we do have characteristic maps: for an $n$-test $E_i \in \mathcal{E}f(H)$ have a dagger mono:

$$H \rightarrowtail^{char_E = \langle\sqrt{E_1}, \ldots, \sqrt{E_n}\rangle} H \oplus \cdots \oplus H = \mathcal{B}_n(H)$$

## Hilbert spaces, continued

- Call an $n$-test $E_i \in \mathcal{Ef}(H)$ a von Neumann test if:
  - $E_i E_i = E_i$, so that $E_i$ is a projection
  - $E_i E_j = 0$, if $i \neq j$
- Coecke & Pavlović (2008) prove a bijective correspondence:

$$\frac{\text{von Neumann } n\text{-tests } E = (E_1, \ldots, E_n) \text{ in } \mathcal{Ef}(H)}{\text{“self-adjoint” Eilenberg-Moore coalgebras } H \to \mathcal{B}_n(H)}$$

(Self-adjointness of $c\colon H \to n \cdot H$ means that each $c_i = \pi_i \circ c$ is self-adjoint: $c_i^\dagger = c_i$)





## $C^*$-algebras

- We work with two categories of (unital) $C^*$-algebras:
  - $\mathbf{Cstar}_{\mathrm{PU}}$: maps are positive and unital
  - $\mathbf{Cstar}_{\mathrm{cPU}} \hookrightarrow \mathbf{Cstar}_{\mathrm{PU}}$: maps are completely positive
- These categories are most naturally used in opposite form:

$$\left(\mathbf{Cstar}_{\mathrm{PU}}\right)^{\mathrm{op}} \qquad \left(\mathbf{Cstar}_{\mathrm{cPU}}\right)^{\mathrm{op}}$$

just like $\mathbf{Locales} = \mathbf{Frames}^{\mathrm{op}}$ is most natural.

- There is an effect logic $[0,1]_{(-)}\colon (\mathbf{Cstar}_{\mathrm{PU}})^{\mathrm{op}} \to \mathbf{EMod}^{\mathrm{op}}$, and similarly for the ‘CPU’ case.
- There are two logical block structures, via powers and via matrices





## Power block structure

- There is product $\oplus$ of $C^*$-algebras
  - forming a coproduct in $(\mathbf{Cstar}_{\mathrm{PU}})^{\mathrm{op}}$
  - yielding a comonad on $(\mathbf{Cstar}_{\mathrm{PU}})^{\mathrm{op}}$
- In this *opposite* category $(\mathbf{Cstar}_{\mathrm{PU}})^{\mathrm{op}}$ we get

$$\begin{array}{ccc} A & \xrightarrow{in_n} & A^n \\ & \searrow^{=} & \downarrow{\scriptstyle out_n} \\ & & A, \end{array} \qquad \text{via} \qquad \left\{ \begin{array}{rcl} in_n(a_1, \ldots, a_n) & = & \dfrac{a_1 + \cdots + a_n}{n} \\ out_n(a) & = \Delta(a) = & (a, \ldots, a) \end{array} \right.$$

- For an $n$-test of effects $e_i \in [0,1]_A$ we get in $(\mathbf{Cstar}_{\mathrm{PU}})^{\mathrm{op}}$

$$A \xrightarrow{char_e} A^n \quad \text{where} \quad char_e(a_1, \ldots, a_n) = \sum_i \sqrt{e_i} a_i \sqrt{e_i}$$





## Matrix block structure

- Taking $n \times n$ matrices forms a functor:

$$\mathbf{Cstar}_{\mathrm{cPU}} \xrightarrow{\mathrm{Mat}_n} \mathbf{Cstar}_{\mathrm{cPU}}$$

- It forms a block structure in $(\mathbf{Cstar}_{\mathrm{cPU}})^{\mathrm{op}}$

$$\begin{array}{ccc} A & \xrightarrow{in_n} & \mathrm{Mat}_n(A) \\ & \searrow^{=} & \downarrow{\scriptstyle out_n} \\ & & A \end{array}$$

via:

$$in_n(M) = \frac{\mathrm{tr}(M)}{n} = \frac{1}{n} \sum_{i \leq n} M_{ii} \qquad out_n(a) = aI_n = \begin{pmatrix} a & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & a \end{pmatrix}$$





## Matrix *logical* block structure

- the universal $n$-test consists of matrices $\Omega_i = |\, i \,\rangle\langle\, i \,| \in \mathrm{Mat}_n(A)$
- for an $n$-test $e_i \in [0,1]_A$ a characteristic map $char_e\colon A \to \mathrm{Mat}_n(A)$ in $(\mathbf{Cstar}_{\mathrm{cPU}})^{\mathrm{op}}$ is given by:

$$char_e(M) = (\sqrt{e_1} \ldots \sqrt{e_n}) M \begin{pmatrix} \sqrt{e_1} \\ \vdots \\ \sqrt{e_n} \end{pmatrix}$$





## Final remarks

- Investigation of block structures, as an abstract programming language construct
  - with “open” and “close” maps
  - opening also via characteristic / measurement maps
  - logic of effect modules is needed
- This structure is present in non-deterministic, probabilistic and quantum computation
- On $C^*$-algebras: both copower and matrix block structures
  - Copower is comonad (has copy), matrix is **not** a comonad
  - precise relationship & usage requires further investigation.