The Expectation Monad

Bart Jacobs & Jorik Mandemaker

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

13/10/2011

Information Security as a Resource, Oxford

Introduction & overview
The expectation monad, effect algebras/modules & other monads
Algebras of the expectation monad & duality
Relevance for quantum foundations & probabilistic programming
Conclusions
Radboud University Nijmegen

Outline

Introduction & overview
The expectation monad, effect algebras/modules & other monads
Algebras of the expectation monad & duality
Relevance for quantum foundations & probabilistic programming
Conclusions
Radboud University Nijmegen

Formal methods for security

- Designing cryptographic systems is notoriously difficult
- In the CS formal methods community there are various symbolic verification approaches
  - They abstract from crucial cryptographic properties
  - eg. hash functions are injective
  - and thus ignore probabilistic aspects
- Example systems:
  - Model checking: NRL and FDR; AVISPA and ProVerif
  - Theorem proving: Paulson's "inductive method"

Introduction & overview
The expectation monad, effect algebras/modules & other monads
Algebras of the expectation monad & duality
Relevance for quantum foundations & probabilistic programming
Conclusions
Radboud University Nijmegen

Security proofs

- Goldwasser and Micali (1984) introduced provable security
  - based on techniques from complexity theory
  - security is proved by reduction
  - any attack against the security of the system leads to an efficient way to solve some computationally hard problem.
- Such security proofs are notoriously sloppy and unreliable
- Gilles Barthe *et al* developed the CertiCrypt approach:
  - verification of such cryptographic proofs
  - reductions become program transformations,
  - involving probabilistic polynomial time programs, as games
- Two references:
  - G. Barthe, B. Grégoire and S. Zanella Béguelin, *Formal certification of code-based cryptographic proofs*, POPL 2009
  - S. Zanella Béguelin, *Formal Certification of Game-Based Cryptographic Proofs*, PhD 2010.

Introduction & overview
The expectation monad, effect algebras/modules & other monads
Algebras of the expectation monad & duality
Relevance for quantum foundations & probabilistic programming
Conclusions
Radboud University Nijmegen

How the reductions are formalised

- Basic transformations $(G, A) \longrightarrow^h (G', A')$, where:
  - G is a probabilistic program
  - A is a problem that is solved by G with probability $Pr[G : A]$
  - h is a function satisfying $Pr[G : A] \leq h(Pr[G' : A'])$
- These steps are formalised in the theorem prover Coq
  - including a "deep" semantics of a probabilistic programming language
  - this yields to "exact" instead of "asymptotically neglible" security properties wrt. a parameter
- The language semantics if formalised via the expectation monad, following:
  - P. Audebaud and C. Paulin-Mohring, *Proofs of randomized algorithms in Coq*, Science of Comp. Progr. (2009)

Introduction & overview
The expectation monad, effect algebras/modules & other monads
Algebras of the expectation monad & duality
Relevance for quantum foundations & probabilistic programming
Conclusions
Radboud University Nijmegen

The expectation monad within CertiCrypt

For a set X take the subset $\mathcal{E}(X)$ of functions $h\colon [0,1]^X \to [0,1]$ satisfying:

1. monotonicity: $p \leq q \Longrightarrow h(p) \leq h(q)$
2. supplement-preservation: $h(p^\perp) = h(p)^\perp$, where $p^\perp = \lambda x.\, 1 - p(x)$ and $r^\perp = 1 - r$
3. sum-preservation: $h(p + q) = h(p) + h(q)$, if $p(x) + q(x) \leq 1$ for each $x \in X$
4. scalar-preservation: $h(r \cdot p) = r \cdot h(p)$, for $r \in [0,1]$
5. preservation of countable sups of monotone predicates: $h(\bigvee_n p_n) = \bigvee_n h(p_n)$.

This has a strong effect algebra/monoid flavour!

Overview of results

1. A re-formulation of the expectation monad $\mathcal{E}$ is given via a composable pair of adjunctions
2. Relation to well-known monads:

$$\begin{tikzcd}[column sep=small] (\text{distribution } \mathcal{D}) \arrow[dr] & & \\ & ({\color{red}\text{expectation } \mathcal{E}}) \arrow[r, tail] & (\text{continuation } \mathcal{C}) \\ (\text{ultrafilter } \mathcal{UF}) \arrow[ur] & & \end{tikzcd}$$

3. Algebras of $\mathcal{E}$ are convex compact Hausdorff spaces
4. They are dually equivalent tot Banach effect modules
5. A re-formulation of Gleason's theorem:

$$[0,1] \otimes \Pr(\mathcal{H}) \cong \mathcal{Ef}(\mathcal{H})$$

Extension of classical results

Recall the classical results:

$$\mathrm{Alg}(\mathcal{UF}) \overset{\text{[Manes]}}{\simeq} (\text{compact Hausdorff sp.}) \overset{\text{[Gelfand]}}{\simeq} (\text{comm. } C^*\text{-algebras})^{\mathrm{op}}$$

Here we will give probabilistic versions:

$$\mathrm{Alg}_{\mathrm{obs}}(\mathcal{E}) \simeq (\text{convex compact Hausdorff sp.})_{\mathrm{obs}} \simeq (\text{Banach effect modules})^{\mathrm{op}}$$

(where 'obs' refers to a suitable observability condition)

The role of the dualizing object $2 = \{0,1\}$ in the classical case is played by the unit interval $[0,1]$ in the probabilistic versions.

A categorical description

$$\begin{tikzcd} \mathbf{Sets} \arrow[r, bend left, "\mathcal{D}"] \arrow[r, phantom, "\perp"] & \mathrm{Alg}(\mathcal{D}) \arrow[l, bend left, "U"] \arrow[r, bend left, "\mathbf{Conv}(-,[0,1])"] \arrow[r, phantom, "\perp"] & \mathbf{EMod}^{\mathrm{op}} \arrow[l, bend left, "\mathbf{EMod}(-,[0,1])"] \end{tikzcd}$$

$$\mathrm{Alg}(\mathcal{D}) = \mathbf{Conv}$$

- The expectation monad $\mathcal{E}\colon \mathbf{Sets} \to \mathbf{Sets}$ is obtained by the composite adjunction $\mathbf{Sets} \leftrightarrows \mathbf{EMod}^{\mathrm{op}}$
- Thus: $\mathcal{E}(X) \cong \mathbf{EMod}\Big(\mathbf{Conv}(\mathcal{D}(X),[0,1]),\ [0,1]\Big)$
  $\overset{\text{def}}{=} \mathbf{EMod}([0,1]^X, [0,1])$
- Notice the similarity with the ultrafilter monad:

$$\begin{aligned} \mathcal{UF}(X) &\cong \{\mathcal{F} \subseteq \mathcal{P}(X) \mid \mathcal{F} \text{ is an ultrafilter}\} \\ &\cong \mathbf{BA}(\mathcal{P}(X), \{0,1\}) \\ &\cong \mathbf{BA}(\{0,1\}^X, \{0,1\}) \end{aligned}$$

Intuition

- We think of elements of $h \in \mathcal{E}(X) = \mathbf{EMod}([0,1]^X, [0,1])$ as measures
- application $h(p)$ to a "fuzzy predicate" $p \in [0,1]^X$ is then integration $\int p\, dh$.
- This will be made more precise later.

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 $\mathbf{Conv} = \mathrm{Alg}(\mathcal{D})$ for the category of convex sets
  - maps are affine functions, preserving convex sums

Towards effect algebras: PCMs

Definition A partial commutative monoid (PCM) is a triple $(M, 0, \ovee)$ where $0 \in M$ and $\ovee$ is partial map $M \times M \to M$. Writing $x \perp y$ for "$x \ovee y$ is defined",

1. commutativity: $x \perp y \Longrightarrow y \perp x$ and $x \ovee y = y \ovee x$
2. zero: $0 \perp x$ and $0 \ovee x = x$
3. associativity: $x \perp y$ and $(x \ovee y) \perp z \Longrightarrow y \perp z$ and $x \perp (y \ovee z)$ and $(x \ovee y) \ovee z = x \ovee (y \ovee z)$.

Main example

Unit interval $[0,1]$, with $r \perp s \Longleftrightarrow r + s \leq 1$
In that case $r \ovee s = r + s$.

Effect algebras

Definition
An effect algebra is a PCM in which:

1. each element x has a unique *orthosupplement* $x^\perp$ with $x \ovee x^\perp = 1$, where $1 = 0^\perp$
2. $x \perp 1 \Longrightarrow x = 0$.

Examples: both from probability & logic

- Unit interval $[0,1]$, with $r^\perp = 1 - r$
- functions $A \to [0,1]$, possibly "simple"
- orthomodular lattices & Boolean algebras
- projections $\mathrm{Pr}(\mathcal{H})$ on Hilbert space $\mathcal{H}$.

Categories **EA** and **EMod** of effect algebras / modules

- A map in **EA** $f: E \to D$ satisfies $f(x \ovee y) = f(x) \ovee f(y)$, if defined, and $f(1) = 1$. Then $f(x^\perp) = f(x)^\perp$ and $f(0) = 0$.
- The category **EA** is symmetric monoidal, with initial object $2 = \{0,1\}$ as unit for $\otimes$
- Next step: monoids in **EA**, given by $\cdot : M \otimes M \to M$
  - $[0,1]$ with multiplication is an example
- Next step: effect module is $[0,1]$-action $[0,1] \otimes E \to E$
  - **EMod** is the category of such effect modules
  - Examples: $[0,1]$, and (simple) functions $A \to [0,1]$
  - Also: $\mathcal{E}f(\mathcal{H}) = \{A : \mathcal{H} \to \mathcal{H} \mid 0 \leq A \leq \mathrm{id}\}$.

Proposition
EMod $\simeq$ **poVectu**, the category of ordered vector spaces over $\mathbb{R}$ with a strong unit (for each x there is an $n \in \mathbb{N}$ with $nu \geq x$)

Expectation monad unravelled

The homset $\mathcal{E}(X) = \mathbf{EMod}([0,1]^X, [0,1])$ contains those functions $h: [0,1]^X \to [0,1]$ that satisfy:

1. $h(p \ovee q) = h(p) + h(q)$,
   for $p, q \in [0,1]^X$ with $p(x) + q(x) \leq 1$, for all $x \in X$.
2. $h(\lambda x.\, 1) = 1$
3. $h(r \cdot p) = r \cdot h(p)$, for $r \in [0,1]$ and $p \in [0,1]^X$.

Lemma
The inclusions $\mathcal{E}(X) = \mathbf{EMod}([0,1]^X, [0,1]) \hookrightarrow [0,1]^{([0,1]^X)}$ form a map of monads, from the expectation to the continuation monad.

Equivalent formulations of the expectation monad

- As homset of order vector spaces with unit:

$$\begin{aligned} \mathcal{E}(X) &\stackrel{\text{def}}{=} \mathbf{EMod}([0,1]^X, [0,1]) \\ &\cong \mathbf{poVectu}(\mathbb{R}^X, \mathbb{R}) \end{aligned}$$

  Proof: via equivalence **EMod** $\simeq$ **poVectu**.

- As finitely additive measures:

$$\mathcal{E}(X) \cong \mathbf{EA}(\mathcal{P}(X), [0,1])$$

  Proof: via denseness of simple functions in $[0,1]^X$, see also Gudder (1998).

$\boxed{\text{Expectation monad is a "robust" mathematical notion}}$

Ultrafilter monad; essentials

$$\begin{aligned} \mathcal{UF}(X) &\cong \{\mathcal{F} \subseteq \mathcal{P}(X) \mid \mathcal{F} \text{ is an ultrafilter}\} \\ &\cong \mathbf{BA}(\mathcal{P}(X), \{0,1\}) \;\cong\; \mathbf{EA}(\mathcal{P}(X), \{0,1\}) \end{aligned}$$

Thus there is an injective map of monads $\mathcal{UF} \Rightarrow \mathcal{E}$, via:

$$\begin{tikzcd} \mathcal{UF}(X) \arrow[r, "\tau_X"] \arrow[d, phantom, "\wr\|"] & \mathcal{E}(X) \arrow[d, phantom, "\wr\|"] \\ \mathbf{EA}(\mathcal{P}(X), \{0,1\}) \arrow[r, tail] & \mathbf{EA}(\mathcal{P}(X), [0,1]) \end{tikzcd}$$

Explicitly, as map:

$$\begin{aligned} \mathcal{UF}(X) &\longrightarrow \mathbf{EMod}([0,1]^X, [0,1]) = \mathcal{E}(X) \\ \mathcal{F} &\longmapsto \lambda p \in [0,1]^X.\, \mathrm{ch}(\mathcal{UF}(p)(\mathcal{F})) \end{aligned}$$

where $\mathrm{ch}: \mathcal{UF}([0,1]) \to [0,1]$ is the $\mathcal{UF}$-algebra on $[0,1]$, using that $[0,1]$ is compact Hausdorff

Topology

- The map of monads $\mathcal{UF} \Rightarrow \mathcal{E}$ induces a functor

$$\mathrm{Alg}(\mathcal{E}) \longrightarrow \mathrm{Alg}(\mathcal{UF}) = \mathbf{CH}$$

- The carrier of each $\mathcal{E}$-algebra is a compact Hausdorff space
- Explicitly, given $\alpha\colon \mathcal{E}(X) \to X$,

$$U \subseteq X \text{ is closed} \quad \text{iff} \quad \forall \mathcal{F} \in \mathcal{UF}(X).\, U \in \mathcal{F} \Longrightarrow \alpha(\tau(\mathcal{F})) \in U.$$

Compact Hausdorff topology on $\mathcal{E}(X)$

Subbasic opens are of the form:

$$\Box_s(p) = \{h \in \mathcal{E}(X) \mid h(p) > s\}.$$

where $s \in [0,1] \cap \mathbb{Q}$ and $p \in [0,1]^X$.

Distribution and expectation monad

- Recall:
  $\mathcal{D}(X) = \{\varphi\colon X \to [0,1] \,|\, \mathrm{supp}(\varphi) \text{ is finite, and } \sum_x \varphi(x) = 1\}$.
- There is a map of monads $\sigma\colon \mathcal{D} \Rightarrow \mathcal{E}$ given by:

$$\begin{aligned} \sigma(\varphi) &= \lambda p \in [0,1]^X.\, \textstyle\sum_x \varphi(x) \cdot p(x) \\ &= \lambda p \in [0,1]^X.\, \mathrm{cv}\big(\mathcal{D}(p)(\varphi)\big), \end{aligned}$$

  where $\mathrm{cv}\colon \mathcal{D}([0,1]) \to [0,1]$ is the convex structure.
- Hence there is a functor $\mathrm{Alg}(\mathcal{E}) \to \mathrm{Alg}(\mathcal{D}) = \mathbf{Conv}$.
- **Conclusion**: each $\mathcal{E}$-algebra (carrier) forms a convex compact Hausdorff space:

$$\mathrm{Alg}(\mathcal{E}) \longrightarrow \mathbf{CCH}$$

Fact: this functor is full & faithful.

Faits divers

- For a *finite* set X,

$$\mathcal{P}(X) \xrightarrow{\;\cong\;} \mathcal{UF}(X)$$

  Because: a map of Boolean algebras $h\colon \mathcal{P}(X) \to \{0,1\}$ is determined by the finitely many values $h(\{x\}) \in \{0,1\}$. They form a subset of X.

- Similarly, for a *finite* set X,

$$\mathcal{D}(X) \xrightarrow{\;\cong\;} \mathcal{E}(X)$$

  Because: a map of effect modules $h\colon [0,1]^X \to [0,1]$ is determined by $h(\mathbf{1}_{\{x\}})$.

Denseness

Proposition
The inclusions $\sigma\colon \mathcal{D}(X) \rightarrowtail \mathcal{E}(X)$ are dense: $\overline{\mathcal{D}(X)} = \mathcal{E}(X)$.

The **proof** proceeds via approximation by simple functions. We sketch that each non-empty open $U \subseteq \mathcal{E}(X)$ contains some $\sigma(\varphi) \in U$.

- write open $U \subseteq \mathcal{E}(X)$ as (finite intersection of) $\Box_s(p) = \{h \in \mathcal{E}(X) \mid h(p) > s\}$
- pick $h \in \Box_s(p)$, and find simple function $q \leq p$ with $h(q) > s$.
- $q\colon X \to [0,1]$ takes finitely many values $r_1, \ldots, r_n \in [0,1]$; write $S_i = \{x \mid q(x) = r_i\}$. Then $q = \bigovee_i r_i \mathbf{1}_{S_i}$
- Take $\varphi = \sum_i h(\mathbf{1}_{X_i}) x_i$, with chosen element $x_i \in S_i$.

Corollary
The induced map $\mathcal{UF}(\mathcal{D}(X)) \longrightarrow \mathcal{E}(X)$ is surjective.

Situation, so far

$$\begin{tikzcd}
\big(\text{distribution } \mathcal{D}\big) \arrow[dr, rightarrowtail, "\text{dense}"] & & \\
& \big(\text{expectation } \mathcal{E}\big) \arrow[r, rightarrowtail] & \big(\text{continuation } \mathcal{C}\big) \\
\big(\text{ultrafilter } \mathcal{UF}\big) \arrow[ur] & &
\end{tikzcd}$$

Example $\mathcal{E}$-algebras

- The unit interval $[0,1]$ carries an $\mathcal{E}$-algebra structure:

$$\begin{aligned} \mathcal{E}([0,1]) = \mathbf{EMod}\big([0,1]^{[0,1]}, [0,1]\big) &\longrightarrow [0,1] \\ h &\longmapsto h(\mathrm{id}_{[0,1]}) \end{aligned}$$

- For a set A, the function space $[0,1]^A$ also carries an algebra:

$$\begin{aligned} \mathcal{E}([0,1]^A) = \mathbf{EMod}\big([0,1]^{([0,1]^A)}, [0,1]\big) &\longrightarrow [0,1]^A \\ h &\longmapsto \lambda a \in A.\, h\big(\lambda f \in [0,1]^A.\, f(a)\big) \end{aligned}$$

(Algebras are closed under products)

Notation for homsets

For two convex compact Hausdorff spaces $X, Y \in \mathbf{CCH}$ one writes:

$$\mathcal{A}(X, Y) = \{f : X \to Y \mid f \text{ is affine \& continuous}\}$$

This notation will also be used when X, Y carry $\mathcal{E}$-algebras

Then $\mathcal{A}(X, Y)$ is the algebra homset, since the functor $\mathrm{Alg}(\mathcal{E}) \to \mathbf{CCH}$ is full & faithfull.

Observability

Call $X \in \mathbf{CCH}$ observable if the maps in $\mathcal{A}(X, [0,1])$ are jointly monic

- Thus $x = x'$ holds if $q(x) = q(x')$ for each $q \in \mathcal{A}(X, [0,1])$

Similarly, an algebra $\mathcal{E}(X) \to X$ will be called observable if X is observable as above.

This yields (full) subcategories:

$$\mathbf{CCH}_{\mathrm{obs}} \hookrightarrow \mathbf{CCH} \qquad \text{and} \qquad \mathrm{Alg}_{\mathrm{obs}}(\mathcal{E}) \hookrightarrow \mathrm{Alg}(\mathcal{E})$$

in which $[0,1]$ is *cogenerator*

Algebras send measures to barycenters

Lemma
Each algebra $\alpha : \mathcal{E}(X) \to X$ sends a measure to a barycenter $\alpha(h) \in X$. This is a point $x = \alpha(h)$ satisfying:

$$h(q) = q(x), \qquad \text{for all } q \in \mathcal{A}(X, [0,1])$$

Proof: Each $q \in \mathcal{A}(X, [0,1])$ is an algebra map in:

$$\begin{tikzcd}
\mathcal{E}(X) \arrow[r, "\mathcal{E}(q)"] \arrow[d, "\alpha"'] & \mathcal{E}([0,1]) \arrow[d, "k \mapsto k(\mathrm{id})"] \\
X \arrow[r, "q"'] & {[0,1]}
\end{tikzcd}$$

Thus: $q(\alpha(h)) = \mathcal{E}(q)(h)(\mathrm{id}) = h(q)$.

Algebras from barycenters

- Recall $\mathcal{D}(X) \rightarrowtail \mathcal{E}(X)$ is dense, and so $\mathcal{UF}(\mathcal{D}(X)) \twoheadrightarrow \mathcal{E}(X)$
- If X is convex compact Hausdorff, using (AC) we get:

$$\alpha \overset{\text{def}}{=} \Big(\mathcal{E}(X) \overset{\text{section}}{\rightarrowtail} \mathcal{UF}(\mathcal{D}(X)) \xrightarrow{\mathcal{UF}(\mathrm{cv})} \mathcal{UF}(X) \xrightarrow{\mathrm{ch}} X \Big)$$

- Then: $\alpha(h) \in X$ is a barycenter for $h \in \mathcal{E}(X)$
- If X is observable, α is an Eilenberg-Moore algebra
  - with observability, barycenters are necessarily unique
  - $q(x) = h(q) = q(x')$, for each q, thus $x = x'$

A probabilistic version of Manes' theorem

Theorem
$\mathrm{Alg}_{\mathrm{obs}}(\mathcal{E}) \cong \mathbf{CCH}_{\mathrm{obs}}$, ie. observable algebras of the expectation monads and observable convex compact Hausdorff spaces coincide

- the algebra structure yields the (unique) barycenter for a measure
- a crucial notion in Choquet theory

(Without 'observability' requirement the situation is unclear)

Afterthought on observability

- Let X be an observable convex compact Hausdorff space, and abbreviate $A = \mathcal{A}(X, [0,1])$.
- By definition we have an injection: $X \overset{x \mapsto \lambda q.\, q(x)}{\rightarrowtail} [0,1]^A$
- This map is both affine and continuous
  - using the product topology on $[0,1]^A$
- One more step gives an embbedding:

$$X \rightarrowtail [0,1]^A \rightarrowtail \mathbb{R}^A$$

  - where: $\mathbb{R}^A$ is a locally convex topological vector space
  - the inherited (product) topology on X coincides with the original one
  - this is the common way to study convex compact Hausdorff spaces: as subspaces of locally convex topological vector spaces

The (dual) adjunction: homming into $[0,1]$

Proposition
There is an adjunction:

$$\begin{tikzcd} \mathbf{EMod}^{\mathrm{op}} \arrow[r, bend left, "\mathbf{EMod}(-{,}[0{,}1])"] \arrow[r, phantom, "\top"] & \mathrm{Alg}(\mathcal{E}) \arrow[l, bend left, "\mathrm{Alg}(\mathcal{E})(-{,}[0{,}1])"] \end{tikzcd}$$

- The algebra on the states of an effect module M is:

$$\begin{array}{rcl} \mathcal{E}\Big(\mathbf{EMod}(M,[0,1])\Big) & \xrightarrow{\alpha_M} & \mathbf{EMod}(M,[0,1]) \\ h & \longmapsto & \lambda y \in M.\, h\big(\lambda k.\, k(y)\big) \end{array}$$

  (The induced topology is weak star)
- Next we restrict both sides to get an equivalence / duality.

On the algebra side

Lemma
For an algebra $\mathcal{E}(X) \to X$, the unit of the adjunction:

$$X \xrightarrow{\eta = \lambda x.\, \lambda q.\, q(x)} \mathbf{EMod}\Big(\mathcal{A}(X,[0,1]),\ [0,1]\Big)$$

is an isomorphism iff X is observable.

Hence there is a coreflection $\mathbf{EMod}^{\mathrm{op}} \leftrightarrows \mathrm{Alg}_{\mathrm{obs}}(\mathcal{E})$.

On the effect module side

- For an effect module M there is a counit (in $\mathbf{EMod}^{\mathrm{op}}$):

$$M \xrightarrow{\varepsilon = \lambda y.\, \lambda p.\, p(y)} \mathcal{A}\Big(\mathbf{EMod}(M,[0,1]),\ [0,1]\Big)$$

- It is an isomorphism iff M is a Banach effect module
  - this means that it is Archimedean (yielding a norm)
  - and complete in this norm
- The proof proceeds via the corresponding ordered vector spaces with unit
  - called "order unit spaces", if Archimedean
  - for these spaces V there is a "classical" dense embedding $V \rightarrowtail \mathcal{A}\big(Hom(V,\mathbb{R}),\mathbb{R}\big)$; it is an iso if V is complete.

A probabilistic version of Gelfand duality

Theorem
$\mathrm{Alg}_{\mathrm{obs}}(\mathcal{E}) \simeq \mathbf{BEMod}^{\mathrm{op}}$, ie. observable algebras of the expectation monad are dually equivalent to Banach effect modules.

Summarising we have:

$$\boxed{\mathbf{CCH}_{\mathrm{obs}} \cong \mathrm{Alg}_{\mathrm{obs}}(\mathcal{E}) \simeq \mathbf{BEMod}^{\mathrm{op}}}$$

Density matrices & effects

Recall density matrices and effects for a Hilbert space $\mathcal{H}$:

$$\begin{aligned} \mathcal{DM}(\mathcal{H}) &= \{A\colon \mathcal{H} \to \mathcal{H} \mid 0 \leq A \text{ and } \mathrm{tr}(A) = 1\} \\ \mathcal{E}f(\mathcal{H}) &= \{A\colon \mathcal{H} \to \mathcal{H} \mid 0 \leq A \text{ and } A \leq \mathrm{id}\} \end{aligned}$$

Common reading:

$\mathcal{DM}(\mathcal{H})$	(mixed) states
$\mathcal{E}f(\mathcal{H})$	predicates

eg. in the quantum weakest precondition calculus of D'Hondt & Panangaden (2006).

Duality for states and predicates

These states and predicates fit into the duality diagram:

$$\begin{tikzcd} \mathcal{DM}(\mathcal{H}) \in \mathbf{CCH}_{\mathrm{obs}} \arrow[r, bend left, "Hom(-{,}[0{,}1])"] \arrow[r, phantom, "\simeq"] & \mathbf{BEMod}^{\mathrm{op}} \ni \mathcal{E}f(\mathcal{H}) \arrow[l, bend left, "Hom(-{,}[0{,}1])"] \end{tikzcd}$$

Moreover, these states & predicates are related via isomorphisms:

$$Hom(\mathcal{E}f(\mathcal{H}),[0,1]) \cong \mathcal{DM}(\mathcal{H}) \quad \text{and} \quad Hom(\mathcal{DM}(\mathcal{H}),[0,1]) \cong \mathcal{E}f(\mathcal{H})$$

These isos form the (implicit) basis of the quantum weakest precondition calculus.

How does Gleason fit in?

Recall, Gleason's theorem says: if $\dim(\mathcal{H}) \geq 3$, then states are measures on projections:

$$\mathcal{DM}(\mathcal{H}) \cong \mathbf{EA}(\mathrm{Pr}(\mathcal{H}), [0,1])$$

The proof is really complicated.

There is a relatively easy proof of "Gleason light":

$$\mathcal{DM}(\mathcal{H}) \cong \mathbf{EMod}(\mathcal{Ef}(\mathcal{H}), [0,1])$$

See Busch (Phys. Rev. Let. 2003)

A reformulation of Gleason's theorem

Theorem
Gleason's theorem is equivalent to $[0,1] \otimes \mathrm{Pr}(\mathcal{H}) \cong \mathcal{Ef}(\mathcal{H})$.

- That is, effects are the free effect module on projections
- quantum probabilities are freely obtained from quantum logic

In one direction the proof is easy:

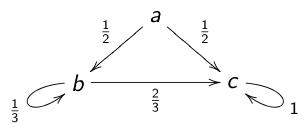
$$\begin{aligned}
\mathbf{EA}(\mathrm{Pr}(\mathcal{H}), [0,1]) &\cong \mathbf{EMod}([0,1] \otimes \mathrm{Pr}(\mathcal{H}), [0,1]) && \text{by freeness} \\
&\cong \mathbf{EMod}(\mathcal{Ef}(\mathcal{H}), [0,1]) && \text{by assumption} \\
&\cong \mathcal{DM}(\mathcal{H}) && \text{by Gleason light.}
\end{aligned}$$

Other direction, assuming Gleason

Top horizontal arrow is surjection, and also injection, in:

$$\begin{tikzcd}
{[0,1] \otimes \mathrm{Pr}(\mathcal{H})} \arrow[r, "\text{spectral}", "\text{decomposition}"'] \arrow[d, tail, "\text{dense}"'] & \mathcal{Ef}(\mathcal{H}) \arrow[d, "\text{completeness}"', "\cong"] \\
\mathcal{A}\Big(\mathbf{EMod}([0,1] \otimes \mathrm{Pr}(\mathcal{H}), [0,1]),\ [0,1]\Big) & \mathcal{A}\Big(\mathbf{EMod}(\mathcal{Ef}(\mathcal{H}), [0,1]),\ [0,1]\Big) \arrow[d, "\text{Gleason light}"', "\cong"] \\
\mathcal{A}\Big(\mathbf{EA}(\mathrm{Pr}(\mathcal{H}), [0,1]),\ [0,1]\Big) \arrow[u, "\text{freeness}", "\cong"'] \arrow[r, "\cong", "\text{Gleason}"'] & \mathcal{A}\Big(\mathcal{DM}(\mathcal{H}), [0,1]),\ [0,1]\Big)
\end{tikzcd}$$

Example probabilistic system



$$\begin{aligned}
S &\xrightarrow{\text{coalgebra}} \mathcal{D}(S) \\
a &\longmapsto \tfrac{1}{2}b + \tfrac{1}{2}c \\
b &\longmapsto \tfrac{1}{3}b + \tfrac{2}{3}c \\
c &\longmapsto 1c
\end{aligned}$$

The same system, as $\mathcal{E}$-coalgebra, via $\mathcal{D} \Rightarrow \mathcal{E}$,

$$\begin{aligned}
S &\longrightarrow \mathcal{E}(S) \\
a &\longmapsto \lambda q \in [0,1]^S.\ \tfrac{1}{2}q(b) + \tfrac{1}{2}q(c) \\
b &\longmapsto \lambda q \in [0,1]^S.\ \tfrac{1}{3}q(b) + \tfrac{2}{3}q(c) \\
c &\longmapsto \lambda q \in [0,1]^S.\ q(c)
\end{aligned}$$

Probabilistic continuation style semantics

Structure of such programs/coalgebras $S \to \mathcal{E}(S)$

- Composition monoid (; , skip), since $\mathcal{E}$ is a monad
- Loops (while/for/recursion), via joins $\bigvee$ of chains
- Finite convex sums of programs $\sum_i r_i P_i$, for $P_i \colon S \to \mathcal{E}(S)$ and $r_i \in [0,1]$ with $\sum_i r_i = 1$
- Finite probabilistic assignment $n := \varphi$, say with variable n: int and distribution $\varphi \in \mathcal{D}(\mathrm{int})$
  - use $\mathrm{upd}_n \colon S \times \mathrm{int} \to S$, giving $\mathcal{E}(\mathrm{upd}_n(s, -)) \colon \mathcal{E}(\mathrm{int}) \to \mathcal{E}(S)$
  - use $\sigma \colon \mathcal{D}(\mathrm{int}) \rightarrowtail \mathcal{E}(\mathrm{int})$, in:

$$[\![n := \varphi]\!](s) = \mathcal{E}(\mathrm{upd}_n(s, -))(\sigma(\varphi))$$

- Finite non-deterministic assignment $n := V$, for finite $V \subseteq \mathrm{int}$
  - similarly, use $\mathcal{P}(V) \cong \mathcal{UF}(V) \rightarrowtail \mathcal{E}(\mathrm{int})$

Final remarks

- Expectation monad is unexpectedly interesting
  - in probabilistic programming semantics
  - in relation to other monads
  - in convex analysis (barycenters, Choquet theory)
  - for quantum logic & probability, via duality & Gleason
- Category theory is very useful for structuring results and seeing connections
  - notably for probabilistic version of Manes & Gelfand
  - many of the ingredients are already known
  - some fruit was hanging low, but not all of it

Credit

Klaus Keimel deserves credit for coming closest

- K. Keimel, *Abstract ordered compact convex sets and algebras of the (sub)probabilistic power domain monad over ordered compact spaces*, (Alg. & Log., 2009)
  - Contains algebras via barycenters, but no duality
  - focus on measures as monads on (convex compact) spaces, like Giry monad on measure spaces
- K. Keimel, A. Rosenbusch and T. Streicher, *Relating direct and predicate transformer partial correctness semantics for an imperative probabilistic-nondeterministic language* (TCS, 2011)
  - Contains *ad hoc* monad similar to 'expectation'
  - focus on program semantics

That's it

Thanks for your attention!
Questions / remarks?