PRESENTING CONVEX SETS OF PROBABILITY DISTRIBUTIONS BY CONVEX SEMILATTICES AND UNIQUE BASES

Filippo Bonchi [1] Ana Sokolova [2] Valeria Vignudelli [3]

[1]University of Pisa, Italy

[2]University of Salzburg, Austria

[3]CNRS/ENS Lyon, France

The monad of convex sets of probability distributions
is presented by
the equational theory of convex semilattices

modelling of
nondeterministic+probabilistic programs

↓

The monad of convex sets of probability distributions
is presented by
the equational theory of convex semilattices

↑

equational reasoning on
nondeterministic+probabilistic programs

modelling of
nondeterministic+probabilistic programs

↓

The monad of convex sets of probability distributions
is presented by
the equational theory of convex semilattices

↑

equational reasoning on
nondeterministic+probabilistic programs

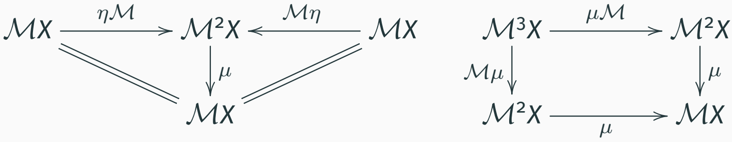
[Bonchi, Sokolova, V. LICS 2019] + verification of trace equivalence

Monads and Equational Theories for Nondeterminism and Probability

MONADS AND EQUATIONAL THEORIES

Monad $(\mathcal{M}, \eta, \mu)$
in Sets

- functor $\mathcal{M} : X \mapsto \mathcal{M}(X)$
- unit $\eta_X : X \to \mathcal{M}(X)$
- multiplication $\mu_X : \mathcal{M}\mathcal{M}(X) \to \mathcal{M}(X)$



Monad $(\mathcal{M}, \eta, \mu)$
in Sets

Equational Theory (Σ, E)

- Σ a signature
- E a set of equations

- equations $t = s$
- deductive system: equational logic
$$\{ t = s, s = u \} \vdash t = u$$
- models: algebras (A, Σ^A) satisfying the equations

Monad $(\mathcal{M}, \eta, \mu)$
in Sets

$\Longleftrightarrow$

Equational Theory (Σ, E)

- Σ a signature
- E a set of equations

(Σ, E) is a presentation of $(\mathcal{M}, \eta, \mu)$

The category **EM**$(\mathcal{M})$ of Eilenberg-Moore algebras for $(\mathcal{M}, \eta, \mu)$ is isomorphic to the category **A**(Σ, E) of algebras (models) of (Σ, E)

Category **EM**$(\mathcal{M})$

- objects: $(A, \alpha : \mathcal{M}(A) \to A)$ with α commuting with η, μ
- arrows: algebra morphisms

Category **A**(Σ, E)

- objects: models (A, Σ^A) of (Σ, E)
- arrows: homomorphisms of (Σ, E)-algebras

Monad $(\mathcal{M}, \eta, \mu)$
in Sets

$\Longleftrightarrow$

Equational Theory (Σ, E)

- Σ a signature
- E a set of equations

(Σ, E) **is a presentation of** $(\mathcal{M}, \eta, \mu)$

The category **EM**$(\mathcal{M})$ of Eilenberg-Moore algebras for $(\mathcal{M}, \eta, \mu)$ is isomorphic to the category **A**(Σ, E) of algebras (models) of (Σ, E)

Corollary:

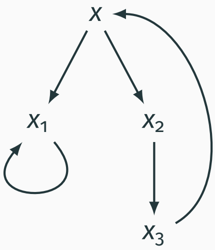
$$\mathcal{M}(X) \cong \mathit{Terms}(X, \Sigma)/_E$$

Monad $(\mathcal{M}, \eta, \mu)$
in Sets

$\Longleftrightarrow$

Equational Theory (Σ, E)

- Σ a signature
- E a set of equations



$c : X \to \mathcal{P}(X)$

$c(x) = \{x_1, x_2\}$
$c(x_1) = \{x_1\}$
...

Monad $(\mathcal{M}, \eta, \mu)$
in Sets

$\Longleftrightarrow$

Equational Theory (Σ, E)

- Σ a signature
- E a set of equations

Powerset (non-empty) monad $(\mathcal{P}, \eta, \mu)$

- $\mathcal{P} : X \mapsto \{S \mid S \text{ is a non-empty, finite subset of } X\}$
- $\eta : x \mapsto \{x\}$
- $\mu : \{S_1, \ldots, S_n\} \mapsto \bigcup_i S_i$

$\Longleftrightarrow$

Equational theory of semilattices

- Σ = binary operation $\oplus$
- axioms of E =

$$(x \oplus y) \oplus z \overset{(A)}{=} x \oplus (y \oplus z)$$
$$x \oplus y \overset{(C)}{=} y \oplus x$$
$$x \oplus x \overset{(I)}{=} x$$

EXAMPLE: NONDETERMINISM

Monad $(\mathcal{M}, \eta, \mu)$ in Sets

$\Longleftrightarrow$

Equational Theory (Σ, E)

- Σ a signature
- E a set of equations

Powerset (non-empty) monad $(\mathcal{P}, \eta, \mu)$

- $\mathcal{P} : X \mapsto \{S \mid S \text{ is a non-empty, finite subset of } X\}$
- $\eta : x \mapsto \{x\}$
- $\mu : \{S_1, \dots, S_n\} \mapsto \bigcup_i S_i$

$\Longleftrightarrow$

Equational theory of semilattices

- Σ = binary operation $\oplus$
- axioms of E =

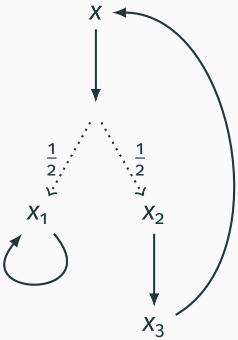
$$
\begin{aligned}
(x \oplus y) \oplus z &\overset{(A)}{=} x \oplus (y \oplus z) \\
x \oplus y &\overset{(C)}{=} y \oplus x \\
x \oplus x &\overset{(I)}{=} x
\end{aligned}
$$

Corollary:

$$\mathcal{P}(X) \cong Terms(X, \Sigma)/_E$$

Monad $(\mathcal{M}, \eta, \mu)$ in Sets $\iff$ Equational Theory (Σ, E)

- Σ a signature
- E a set of equations



$$c : X \to \mathcal{D}(X)$$

$$c(x) = \tfrac{1}{2}\, x_1 + \tfrac{1}{2}\, x_2$$
$$c(x_1) = 1\, x_1$$
...

Monad $(\mathcal{M}, \eta, \mu)$
in Sets

$\iff$

Equational Theory (Σ, E)

- Σ a signature
- E a set of equations

Distribution monad $(\mathcal{D}, \eta, \mu)$

- $\mathcal{D} : X \mapsto \{\Delta \mid \Delta$ is a finitely supported probability distribution on $X\}$
- $\eta : x \mapsto 1x$
- $\mu : \sum_i p_i \Delta_i \mapsto \sum_i p_i \cdot \Delta_i$

$\iff$

Equational theory of convex algebras

- Σ = binary operations $+_p$ for all $p \in (0, 1)$
- axioms of E =

$$(x +_q y) +_p z \stackrel{(A_p)}{=} x +_{pq} (y +_{\frac{p(1-q)}{1-pq}} z)$$

$$x +_p y \stackrel{(C_p)}{=} y +_{1-p} x$$

$$x +_p x \stackrel{(I_p)}{=} x$$

Monad $(\mathcal{M}, \eta, \mu)$
in Sets

$\Longleftrightarrow$

Equational Theory (Σ, E)

- Σ a signature
- E a set of equations

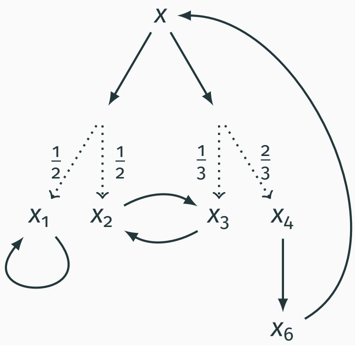
nondeterminism

+

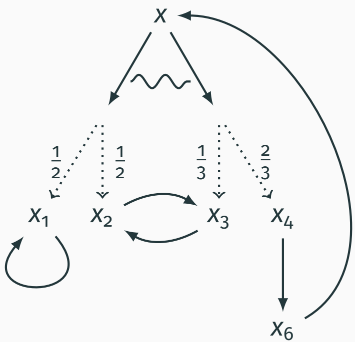
probability

=

?



- a transition reaches a set of probability distributions $\{\, \frac{1}{2}x_1 + \frac{1}{2}x_2,\ \frac{1}{3}x_3 + \frac{2}{3}x_4 \,\}$
- Problem: $\mathcal{P} \circ \mathcal{D}$ is not a monad [Varacca, Winskel 2006]

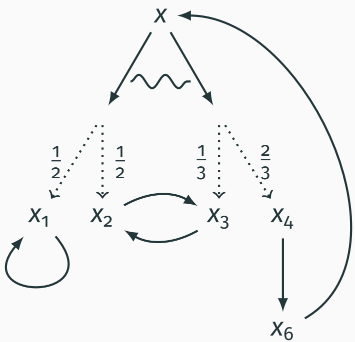


- a transition reaches a set of probability distributions $\{\frac{1}{2}x_1 + \frac{1}{2}x_2,\ \frac{1}{3}x_3 + \frac{2}{3}x_4\}$
- Problem: $\mathcal{P} \circ \mathcal{D}$ is not a monad [Varacca, Winskel 2006]

Solution: use
convex sets of probability distributions

For S a set of probability distributions

- $conv(S) = \{\sum_i p_i \cdot d_i \mid d_1, \ldots, d_n \in S \text{ and } \sum_i p_i = 1\}$
- S is convex if $S = conv(S)$



- a transition reaches a set of probability distributions $\{ \frac{1}{2}x_1 + \frac{1}{2}x_2,\ \frac{1}{3}x_3 + \frac{2}{3}x_4 \}$
- Problem: $\mathcal{P} \circ \mathcal{D}$ is not a monad [Varacca, Winskel 2006]

Solution: use
convex sets of probability distributions

For S a set of probability distributions

- $conv(S) = \{\sum_i p_i \cdot d_i \mid d_1, \dots, d_n \in S \text{ and } \sum_i p_i = 1\}$
- S is convex if $S = conv(S)$

+ accounts for probabilistic schedulers

The monad $(\mathcal{C}, \eta, \mu)$ in Sets:

- $\mathcal{C} : X \mapsto \{S \mid S$ is a non-empty, convex, finitely generated set of finitely supported probability distributions over $X\}$

- $\eta_X : X \to \mathcal{C}(X)$

$$\eta_X : x \mapsto \{\ 1x\ \}$$

- $\mu_X : \mathcal{C}\mathcal{C}(X) \to \mathcal{C}(X)$

$$\mu_X : \bigcup_i \{\Delta_i\} \mapsto \bigcup_i \mathtt{WMS}(\Delta_i)$$

with $\mathtt{WMS} : \mathcal{D}\mathcal{C}(X) \to \mathcal{C}(X)$ the *weighted Minkowski sum*

$$\mathtt{WMS}(\sum_{i=1}^{n} p_i S_i) = \{\sum_{i=1}^{n} p_i \cdot \Delta_i \mid \text{for each } 1 \le i \le n, \Delta_i \in S_i\}$$

[Jacobs 2008 ...]

Monad $(\mathcal{M}, \eta, \mu)$
in Sets

$\Leftrightarrow$

Equational Theory (Σ, E)

- Σ a signature
- E a set of equations

Convex sets (non-empty)
of distributions
monad $(\mathcal{C}, \eta, \mu)$

$\Leftrightarrow$

Equational theory of convex semilattices

- $\Sigma = \oplus$ and $+_p$ for all $p \in (0, 1)$
- axioms E :
  - axioms of semilattices
  - axioms of convex algebras
  - distributivity axiom (D)
    $(x \oplus y) +_p z \stackrel{(D)}{=} (x +_p z) \oplus (y +_p z)$

[Bonchi, Sokolova, V. 2019]

The Proof

The monad of convex sets of probability distributions
is presented by
the equational theory of convex semilattices

1. Unique base theorem:
   Every convex set of probability distributions has a unique base
2. Prove that there is a monad isomorphism
   (via unique base theorem)

For S a (finitely-generated) convex set of probability distributions, a base is a set $\{d_1, ..., d_n\}$ of distributions such that:

- $S = conv(\{d_1, ..., d_n\})$
- for all $i \in 1 \ldots n$, $d_i \notin conv(\{d_j \mid j \neq i, 1 \leq j \leq n\})$

Every convex set of probability distributions has a unique base

Two proofs:

- combinatorial, direct proof
- from functional analysis, via Krein-Milman Theorem

The monad of convex sets of probability distributions
is presented by
the equational theory of convex semilattices

1. Unique base theorem:
   Every convex set of probability distributions has a unique base
2. Prove that there is a monad isomorphism
   (via unique base theorem)

The monad of convex sets of probability distributions
is presented by
the equational theory of convex semilattices

	Category $\mathbf{EM}(\mathcal{C})$	$\simeq$	Category $\mathbf{A}(\Sigma, E)$
Equivalent:	Monad $\mathcal{C}$	$\simeq$	Monad $T_{\Sigma_{/E}}$

The monad of convex sets of probability distributions
is presented by
the equational theory of convex semilattices

	Category $\mathbf{EM}(\mathcal{C})$	$\simeq$	Category $\mathbf{A}(\Sigma, E)$
Equivalent:	Monad $\mathcal{C}$	$\simeq$	Monad $T_{\Sigma_{/E}}$

= define a natural tranformation $\iota \colon T_{\Sigma_{/E}} \Rightarrow \mathcal{C}$ such that:

- ι is a monad map
- ι is an isomorphism, i.e., it has an inverse $\kappa \colon \mathcal{C} \Rightarrow T_{\Sigma_{/E}}$

The monad of convex sets of probability distributions
is presented by
the equational theory of convex semilattices

Category $\mathbf{EM}(\mathcal{C})$ $\simeq$ Category $\mathbf{A}(\Sigma, E)$

Equivalent: Monad $\mathcal{C}$ $\simeq$ Monad $T_{\Sigma_{/E}}$

= define a natural tranformation $\iota\colon T_{\Sigma_{/E}} \Rightarrow \mathcal{C}$ such that:

- ι is a monad map
- ι is an isomorphism, i.e., it has an inverse $\kappa\colon \mathcal{C} \Rightarrow T_{\Sigma_{/E}}$

$$\kappa : S \mapsto \{d_1, \ldots, d_n\} \mapsto [t_1 \oplus \ldots \oplus t_n]_{/E}$$

↑ unique base theorem

The monad of convex sets of probability distributions
is presented by
the equational theory of convex semilattices

- A new proof, uses the unique base theorem to obtain a normal form
- Proven useful in extending the presentation result to metric spaces and to include termination
  [Mio, V. 2020][Mio, Sarkis, V. 2021]

The monad of convex sets of probability distributions
is presented by
the equational theory of convex semilattices

- A new proof, uses the unique base theorem to obtain a normal form
- Proven useful in extending the presentation result to metric spaces and to include termination
[Mio, V. 2020][Mio, Sarkis, V. 2021]

Thank you!