Categorical axioms for functional real-number compuation 3 & 4

Alex Simpson

joint work with Martín Escardó

MAP, Leiden, 28 Nov – 2 Dec 2011

Recap / overview

Definition of (parametrized) interval object in a category with finite products.

- Implements basic principles from Euclidean geometry.
- Defines an abstract datatype for the interval.
- Proves equalities of functions.
- Works in categories of interest.

In these two lectures, elaborate mainly on fourth point.

Supermidpoint object (Escardó c. 1997)

$(A,\ \mathrm{M} : A^{N} \to A)$ satisfying:

$$m(x,x) \ = \ x$$

$$m(x,y) \ = \ m(y,x)$$

$$\mathop{\mathrm{M}}_i \mathop{\mathrm{M}}_j x_{ij} \ = \ \mathop{\mathrm{M}}_j \mathop{\mathrm{M}}_i x_{ij}$$

$$\mathop{\mathrm{M}}_i x_i \ = \ m(x_0, \mathop{\mathrm{M}}_i x_{i+1})$$

where

$$m(x,y) \ =_{\mathrm{def}} \ \mathrm{M}(x,y,y,y,y,y,\ldots)$$

Binary m defined from infinitary M.

Homomorphisms preserve M and hence m

Iterative midpoint object

A midpoint object, i.e., $(A,\ m\colon A \times A \to A)$ satisfying:

$$m(x,x) = x$$

$$m(x,y) = m(y,x)$$

$$m(m(x,y), m(z,w)) = m(m(x,z), m(y,w))$$

is iterative if $\exists\, \mathrm{M} : A^{N} \to A$ satisfying

$$\underset{i}{\mathrm{M}}\, x_i = m(x_0, \underset{i}{\mathrm{M}}\, x_{i+1})$$

$$(\,\forall i.\ x_i = m(y_i, x_{i+1})\,) \quad \Rightarrow \quad x_0 = \underset{i}{\mathrm{M}}\, y_i$$

Infinitary M defined from binary m

Homomorphisms preserve m and hence M

Relationship between notions

iterative midpoint object $\underset{\not\Leftarrow}{\Rightarrow}$ supermidpoint object

Example supermidpoint object that is not iterative:

$$(\{\bot, \top\}, \bigvee)$$

We do not know if supermidpoint objects enjoy all equational properties of iterative midpoint objects.

An equational consequence of iteration

Define $m_n \colon A^{n+1} \to A$ by

$$m_0(x_0) = x \qquad m_{n+1}(x_0, \ldots, x_n) = m(x_0, m_n(x_1, \ldots, x_n))$$

In any iterative midpoint object:

$$\mathop{\mathrm{M}}_i \mathop{\mathrm{M}}_j x_{ij} = \mathop{\mathrm{M}}_k m(x_{kk},\ m(m_k(x_{(k+1)\,0}, \ldots, x_{(k+1)\,k}), \\ m_k(x_{0\,(k+1)}, \ldots, x_{k\,(k+1)})))$$

Does this hold for every supermidpoint object?

Does adding this equation to supermidpoint objects result in a complete equational theory?

Cancellation

The cancellation law says

$$m(x, z) = m(y, z) \quad \Rightarrow \quad x = y$$

Relationship between notions:

$$\begin{array}{ccc} \text{supermidpoint} & \Leftarrow & \text{iterative midpoint} \\ \Uparrow & & \Uparrow \\ \text{cancellative supermidpoint} & \Leftrightarrow & \text{cancellative iterative midpoint} \end{array}$$

The bottom line gives the convex bodies of Martín's talks.

Approximation property

Proposition

For a supermidpoint object (A, m), the following are equivalent

- (A, m) is cancellative
- For all $(x_n)_n$, $(y_n)_,$, $(z_n)_n$, $(w_n)_n$, if

  $$m_{n+1}(x_0, \ldots, x_n, z_n) = m_{n+1}(y_0, \ldots, y_n, w_n) \qquad \forall n$$

  then

  $$\underset{i}{\mathrm{M}}\; x_i = \underset{i}{\mathrm{M}}\; y_i$$

Proof goes through in a locally cartesian closed category with natural numbers object.

Definition: Interval object (unofficial version)

An interval object $(\mathbf{I}, m, u, v)$ is a free iterative midpoint object $(\mathbf{I}, m)$ over two generators u, v.

It is cancellative if $(\mathbf{I}, m)$ is cancellative.

Any map $d\colon \mathbf{I} \to \mathbf{I}$ satisfying

$$\begin{aligned} d(m(x, m(u, v))) &= x \\ d(m(u, m(u, x))) &= u \\ d(m(v, m(v, x))) &= v \end{aligned}$$

is called a double.

Is it possible for a (cancellative) interval object to have more than one double?

Interval object in **Set**

Theorem

$([-1,1], \oplus, -1, 1)$, where $x \oplus y = \frac{1}{2}(x+y)$, is an interval object.
It is cancellative and has a unique double.

Interval object in **Set**

Theorem

$([-1,1], \oplus, -1, 1)$, where $x \oplus y = \frac{1}{2}(x+y)$, is an interval object. It is cancellative and has a unique double.

More generally

The free iterative midpoint object over a set X, is given by the set

$$\{p \colon X \to [0,1] \mid \sum_{x \in X} p(x) = 1\}$$

of probability mass functions over X.

Superconvex set (Rodé, König)

A superconvex set is a set X together with a chosen element

$$\sum_{i \in I}^{X} \lambda_i x_i \ ,$$

for every countable convex combination over X, such that the equations below are satisfied.

$$\sum_{i \in \mathbf{1}}^{X} 1x \ = \ x$$

$$\sum_{i \in \mathbf{I}}^{X} \lambda_i \big(\sum_{j \in \mathbf{J}}^{X} \mu_j x_{ij}\big) \ = \ \sum_{i \in \mathbf{I}}^{X} \big(\sum_{j \in \mathbf{J}} \lambda_i \mu_j\big) x_{ij}$$

A superaffine function is one preserving countable convex combinations.

Iterative superconvex set

A superconvex set is iterative if

$$x_n = \lambda_n y_n +^{X} (1 - \lambda_n) x_{n+1} \qquad \forall n \geq 0$$

and

$$\prod_n (1 - \lambda_n) = 0$$

together imply

$$x_0 = \sum_n^{X} \lambda_n \Big(\prod_{m<n} (1 - \lambda_m) \Big) y_n$$

Iterative midpoint = iterative superconvex

If $(X, \sum^X)$ is an iterative superconvex set, then *a fortiori*

$$m(x, y) \;=\; \frac{1}{2}x +^X \frac{1}{2}y$$

defines an iterative midpoint set.

Theorem

The above operation defines an isomorphism of categories from the category of iterative superconvex sets and superaffine maps to the category of iterative midpoint sets.

The characterisation of the free iterative midpoint object over a set X as probability mass functions on X is a consequence of this theorem, since this is easily shown to be the free superconvex set over X (König) and is iterative as a superconvex set.

In particular, if (X, m) is an iterative midpoint set, then X carries a unique superconvex structure $\sum^X$ such that

$$m(x, y) = \frac{1}{2}x +^X \frac{1}{2}y$$

Also, every homomorphism with respect to m is superaffine.

In fact, X carries a unique convex structure satisfying the above.

Iterativity is essential here. Consider the midpoint object $(\mathbb{R}, \oplus)$.

- There are $2^{2^{\aleph_0}}$ convex set structures on $\mathbb{R}$ extending $\oplus$.
- There are $2^{2^{\aleph_0}}$ homomorphisms from $(\mathbb{R}, \oplus)$ to itself that are not affine (Freyd).

Subsets of Euclidean space

Proposition

Let X be a subset of $\mathbb{R}^n$ closed under $\mathbf{x} \oplus \mathbf{y} = \frac{1}{2}(\mathbf{x} + \mathbf{y})$. Then $(X, \oplus)$ is an iterative midpoint set if and only if X is convex and bounded.

Subsets of Euclidean space

Proposition

Let X be a subset of $\mathbb{R}^n$ closed under $\mathbf{x} \oplus \mathbf{y} = \frac{1}{2}(\mathbf{x} + \mathbf{y})$. Then $(X, \oplus)$ is an iterative midpoint set if and only if X is convex and bounded.

Proposition

If X is a bounded convex subset of $\mathbb{R}^n$ then $(X, \oplus)$ is an iterative midpoint space. That is,

$$\bigoplus : (\mathbf{x}_n)_n \mapsto \sum_n 2^{-n-1} \mathbf{x}_n \ : \ X^\omega \to X$$

is continuous.

Interval object in **Top**

Theorem

$([-1,1], \oplus, -1, 1)$, with Euclidean topology, is a parametrized interval object in **Top**. (It is cancellative and has a unique double.)

Interval object in **Top**

Theorem

$([-1,1], \oplus, -1, 1)$, with Euclidean topology, is a parametrized interval object in **Top**. (It is cancellative and has a unique double.)

More generally

The parametrically free iterative midpoint space over the discrete set $\{0, \ldots, n\}$ is the n-simplex.

Interval object in **Top**

Theorem

$([-1,1], \oplus, -1, 1)$, with Euclidean topology, is a parametrized interval object in **Top**. (It is cancellative and has a unique double.)

More generally

The parametrically free iterative midpoint space over the discrete set $\{0, \ldots, n\}$ is the n-simplex.

Compactness

The n-simplex is also the parametrically free iterative midpoint object over $\{0, \ldots, n\}$ in the category of compact Hausdorff spaces.

Interval object in **Top**

Theorem

$([-1,1], \oplus, -1, 1)$, with Euclidean topology, is a parametrized interval object in **Top**. (It is cancellative and has a unique double.)

More generally

The parametrically free iterative midpoint space over the discrete set $\{0, \ldots, n\}$ is the n-simplex.

Compactness

The n-simplex is also the parametrically free iterative midpoint object over $\{0, \ldots, n\}$ in the category of compact Hausdorff spaces.

Might be interesting to consider the parametrically free iterative midpoint object over an arbitrary topological space X.

Proof of theorem

Let (A, m) be an iterative midpoint space.

Consider continuous $f\colon Z \times \{-1, 1\} \to A$.

By characterization of interval object in **Set**, there exists a unique function $g\colon Z \times [-1, 1] \to A$ satisfying

$$g(z, -1) = f(z, -1) \quad g(z, 1) = f(z, 1) \quad g(z, x \oplus y) = m(g(z, x), g(z, y))$$

So:

$$\begin{array}{ccc} Z \times \{-1, 1\}^{\omega} & \xrightarrow{f^{\omega}} & A^{\omega} \\ {\scriptstyle 1_Z \times \bigoplus} \downarrow & & \downarrow {\scriptstyle \mathrm{M}} \\ Z \times [-1, 1] & \xrightarrow{g} & A \end{array}$$

Then g is continuous since $\bigoplus$ is a stable quotient (Day & Kelly).

Topological quirks

Lemma

Suppose (A, M) is a supermidpoint space and

$$x_n \;=\; m(y_n, x_{n+1}) \qquad \forall n$$

Then x_0 is contained in every neighbourhood of $\mathrm{M}_i\, y_i$.

Proposition

Every T_1 supermidpoint space is iterative.

Proposition

Every regular (T_3) supermidpoint space is cancellative.

A constructive quirk

The characterisation of the interval object in **Set** as the free iterative midpoint object is constructive but uses AC_{00}:

$$(\forall x \colon \mathbb{N}.\, \exists y \colon \mathbb{N}.\, P(x, y)) \;\Rightarrow\; (\exists f \colon \mathbb{N} \to \mathbb{N}.\, \forall x \colon \mathbb{N}.\, P(x, f(x)))$$

AC_{00} is provable in classical logic.

However, it need not hold in sheaf categories, e.g., it fails in $\mathrm{Sh}(\mathbb{R})$.

Real numbers in a topos

In an elementary topos $\mathcal{E}$ with natural numbers object.

- Cauchy reals $\mathbf{R}_C$ = Cauchy sequences of rationals (with modulus of convergence) modulo equivalence.
- Dedekind reals $\mathbf{R}_D$ = Dedekind cuts of rationals (suitably defined).

Always $\mathbf{R}_C \subseteq \mathbf{R}_D$.

If AC_{00} holds then $\mathbf{R}_C = \mathbf{R}_D$.

In $\mathrm{Sh}(\mathbb{R})$, $\mathbf{R}_C \neq \mathbf{R}_D$ (Fourman & Hyland).

Real numbers in a topos

In an elementary topos $\mathcal{E}$ with natural numbers object.

- Cauchy reals $\mathbf{R}_C$ = Cauchy sequences of rationals (with modulus of convergence) modulo equivalence.
- Dedekind reals $\mathbf{R}_D$ = Dedekind cuts of rationals (suitably defined).

Always $\mathbf{R}_C \subseteq \mathbf{R}_D$.

If AC_{00} holds then $\mathbf{R}_C = \mathbf{R}_D$.

In $\mathrm{Sh}(\mathbb{R})$, $\mathbf{R}_C \neq \mathbf{R}_D$ (Fourman & Hyland).

$\mathbf{R}_C$ is not necessarily Cauchy complete! (Lubarsky)

Real numbers in a topos

In an elementary topos $\mathcal{E}$ with natural numbers object.

- Cauchy reals $\mathbf{R}_C$ = Cauchy sequences of rationals (with modulus of convergence) modulo equivalence.
- Dedekind reals $\mathbf{R}_D$ = Dedekind cuts of rationals (suitably defined).

Always $\mathbf{R}_C \subseteq \mathbf{R}_D$.

If AC_{00} holds then $\mathbf{R}_C = \mathbf{R}_D$.

In $\mathrm{Sh}(\mathbb{R})$, $\mathbf{R}_C \neq \mathbf{R}_D$ (Fourman & Hyland).

$\mathbf{R}_C$ is not necessarily Cauchy complete! (Lubarsky)

$\mathbf{R}_D$ is Cauchy complete.

Real numbers in a topos (continued)

In an elementary topos $\mathcal{E}$ with natural numbers object.

- Cauchy reals $\mathbf{R}_C$ = Cauchy sequences of rationals (with modulus of convergence) modulo equivalence.
- Dedekind reals $\mathbf{R}_D$ = Dedekind cuts of rationals (suitably defined).

Real numbers in a topos (continued)

In an elementary topos $\mathcal{E}$ with natural numbers object.

- Cauchy reals $\mathbf{R}_C$ = Cauchy sequences of rationals (with modulus of convergence) modulo equivalence.
- Dedekind reals $\mathbf{R}_D$ = Dedekind cuts of rationals (suitably defined).
- Euclidean reals $\mathbf{R}_E$ = Cauchy completion of $\mathbf{R}_C$ within $\mathbf{R}_D$.

Real numbers in a topos (continued)

In an elementary topos $\mathcal{E}$ with natural numbers object.

- Cauchy reals $\mathbf{R}_C$ = Cauchy sequences of rationals (with modulus of convergence) modulo equivalence.
- Dedekind reals $\mathbf{R}_D$ = Dedekind cuts of rationals (suitably defined).
- Euclidean reals $\mathbf{R}_E$ = Cauchy completion of $\mathbf{R}_C$ within $\mathbf{R}_D$.

Always $\mathbf{R}_C \subseteq \mathbf{R}_E \subseteq \mathbf{R}_D$.

In general, neither inclusion is an equality.

Redefinition: Interval object (official version)

An interval object $(\mathbf{I}, m, u, v)$ is a free cancellative iterative midpoint object $(\mathbf{I}, m)$ over two generators u, v.

Redefinition: Interval object (official version)

An interval object $(\mathbf{I}, m, u, v)$ is a free cancellative iterative midpoint object $(\mathbf{I}, m)$ over two generators u, v.

Define:

$$\begin{aligned} \mathbf{I}_D &= \{x \colon \mathbf{R}_D \mid -1 \leq x \leq 1\} \\ \mathbf{I}_E &= \mathbf{R}_E \cap \mathbf{I}_D \end{aligned}$$

Theorem

$(\mathbf{I}_E, \oplus, -1, 1)$ is an interval object in $\mathcal{E}$ with a unique double.

Redefinition: Interval object (official version)

An interval object $(\mathbf{I}, m, u, v)$ is a free cancellative iterative midpoint object $(\mathbf{I}, m)$ over two generators u, v.

Define:

$$\begin{aligned} \mathbf{I}_D &= \{x \colon \mathbf{R}_D \mid -1 \leq x \leq 1\} \\ \mathbf{I}_E &= \mathbf{R}_E \cap \mathbf{I}_D \end{aligned}$$

Theorem

$(\mathbf{I}_E, \oplus, -1, 1)$ is an interval object in $\mathcal{E}$ with a unique double.

The fact that $\mathbf{I}_E$ is closed under $\oplus$ is not obvious! This will be shown as part of the proof.

Outline proof of theorem

Work in internal logic.

Let (A, m, a, b) be a cancellative iterative midpoint object in $\mathcal{E}$, with two points a, b.

Let $\mathcal{F}$ be the family of those subsets $X \subseteq \mathbf{I}_D$ satisfying:

- $-1, 1 \in X$
- X is closed under $\oplus\colon \mathbf{I}_D \times \mathbf{I}_D \to \mathbf{I}_D$.
- X is closed under $-\colon \mathbf{I}_D \to \mathbf{I}_D$ and $d\colon \mathbf{I}_D \to \mathbf{I}_D$ (double).
- $X \subseteq \mathbf{I}_E$.
- There exists a unique homomorphism from $(X, \oplus, -1, 1)$ to (A, m, a, b).

Lemma

$(\mathcal{F}, \subseteq)$ is a directed-complete partial order with least element.

Define a monotone function $\Phi\colon \mathcal{P}(\mathbf{I}_D) \to \mathcal{P}(\mathbf{I}_D)$ by:

$$\Phi(X) = \{\bigoplus_n x_n \mid x_{(-)} : X^{\mathbf{N}}\}$$

Lemma

Φ cuts down to a (trivially monotone) function on $(\mathcal{F}, \subseteq)$.

Lemma

$(\mathcal{F}, \subseteq)$ is a directed-complete partial order with least element.

Define a monotone function $\Phi \colon \mathcal{P}(\mathbf{I}_D) \to \mathcal{P}(\mathbf{I}_D)$ by:

$$\Phi(X) = \{\bigoplus_n x_n \mid x_{(-)} \colon X^{\mathbf{N}}\}$$

Lemma

Φ cuts down to a (trivially monotone) function on $(\mathcal{F}, \subseteq)$.

The proof that $\Phi(X)$ is closed under the double function d is (excessively) technical.

Lemma

$(\mathcal{F}, \subseteq)$ is a directed-complete partial order with least element.

Define a monotone function $\Phi\colon \mathcal{P}(\mathbf{I}_D) \to \mathcal{P}(\mathbf{I}_D)$ by:

$$\Phi(X) = \{\bigoplus_n x_n \mid x_{(-)} \colon X^{\mathbf{N}}\}$$

Lemma

Φ cuts down to a (trivially monotone) function on $(\mathcal{F}, \subseteq)$.

The proof that $\Phi(X)$ is closed under the double function d is (excessively) technical.

The proof that there exists a homomorphism from $(\Phi(X), \oplus, -1, 1)$ to (A, m, a, b) makes (apparently) essential use of cancellativity of (A, m).

Theorem

Every monotone function on a directed-complete partial order with least element has a least fixed point.

Theorem (Pataraia 1996, in internal logic of a topos)
Every monotone function on a directed-complete partial order with least element has a least fixed point.

Theorem (Pataraia 1996, in internal logic of a topos)
Every monotone function on a directed-complete partial order with least element has a least fixed point.

Let $\mathbf{I}_\Phi$ be the least fixed-point of $\Phi\colon \mathcal{F} \to \mathcal{F}$.

Lemma $\mathbf{I}_\Phi = \mathbf{I}_E$.

Proof To prove that $\mathbf{I}_E \subseteq \mathbf{I}_\Phi$, show that $\mathbf{I}_\Phi$ is Cauchy complete. This is done using a combination of $\bigoplus$ and the double function d, as in Martín's talk. □

Theorem (Pataraia 1996, in internal logic of a topos)
Every monotone function on a directed-complete partial order with least element has a least fixed point.

Let $\mathbf{I}_\Phi$ be the least fixed-point of $\Phi\colon \mathcal{F} \to \mathcal{F}$.

Lemma $\mathbf{I}_\Phi = \mathbf{I}_E$.

Proof To prove that $\mathbf{I}_E \subseteq \mathbf{I}_\Phi$, show that $\mathbf{I}_\Phi$ is Cauchy complete. This is done using a combination of $\bigoplus$ and the double function d, as in Martín's talk. $\square$

Thus indeed $(\mathbf{I}_E, \oplus, -1, 1)$ is an interval object in $\mathcal{E}$ with double.

Relating interval objects between categories

Proposition

Given an adjunction $F \dashv G : \mathcal{C} \to \mathcal{D}$ between categories with finite products, the right adjoint G preserves (cancellative) iterative midpoint objects. That is G lifts to a functor $G_M : \mathcal{C}_M \to \mathcal{D}_M$.

If the left adjoint F itself has a left adjoint then $F_M \dashv G_M : \mathcal{C}_M \to \mathcal{D}_M$, and F_M preserves the interval object.

In particular

The inverse image functor of an essential geometric morphism between elementary toposes preserves interval objects.

Further directions

- Equational algebra with infinitary operations in a choice-free intuitionistic framework
- Interval object in Aczel's CZF+REA (or other generalized-predicative constructive set theories with inductively defined sets)
- Interval object in Martin-Löf type theory
- Interval object in locales / formal topology
- Characterise functions definable in system II
- Fundamental theorem of algebra
- Higher-order functionals (e.g., integration)