Towards Constructive Hybrid Semantics

Sergey Goncharov

(joint work with Tim Lukas Diezel)

Oberseminar, INF8, TechFak, FAU, June 16, 2020

Meta-Introduction

How does the category theory work?

1. We formulate various assumptions, identifying classes of categories of interest (lfp, CCC, algebraic, monadic, toposes, etc)
2. We dive in and obtain various generic results in the conventional categorical language
3. We (try to) interpret and communicate the obtained knowledge to the outer word

that is where we most of the time are

From "better" to "worse":

- **Good** In terms of intrinsic universal properties: finite (co)limits, Cartesian closure
- **Worse** General well-behaivedness properties of categorical structures, e.g. regularity
- **Bad** In terms of universal properties, involving other categories to impredicatevely postulate something about the running category, e.g. partial map classifier
- **Very Bad** postulating properties of individual morphisms: excluded middle, the axiom of choice

Think of Lawvere's ETCS from this point of view to see how little the category of sets (ETCS or ZFC) has to do with categories

Defining Categories

that is what we most of the time presuppose

How is the category theory build? There are various options

1. In two stages: Introduce set theory, and axiomatize category theory inside of it
2. Introduce category theory from scratch in terms if itself (Lawvere's ETCC), while keeping the set-theoretic foundations implicit
3. Use type theory and redesign category theory as a theory inside of it, so as to comply with the type-theoretic principles (proof relevance, propositions as types, strong normalizability)

currently actively developed

Type Theory

Incidentally, "good" properties are eagerly adapted in type theory: those appear to correspond to construction of new types/terms from the existing ones.

"Bad" properties are mostly rejected, as not having computational (or constructive) meaning: subobject classifier, axioms of choice, excluded middle

Various intermediate cases (free algebras, quotients) are subject to recent intense ongoing work for proper integration into type theory, prominently to Homotopy Type Theory (HoTT)

Why Care?

- Type-theoretic formalizations can be natively transferred to proof assistants (e.g. Coq, Agda)
- Rejecting "bad" assumptions leads to a mathematically more general theory, with a larger class of models
- Type-theoretic formalizations help to identify numerous hidden uses of non-constructive principles, and thus to improve design of formalizations and implementations

Hybrid semantics is a sweet spot for exploring these ideas: if we want to have a domain of hybrid programs, they must be constructive in some sense, like the normal programs are!

Rest of Talk

Hybrid semantics, non-constructively

Categorical abstraction

Characterizing classical semantics

Some details of Agda formalization

Conclusions

Hybrid Systems, Non-Constructively

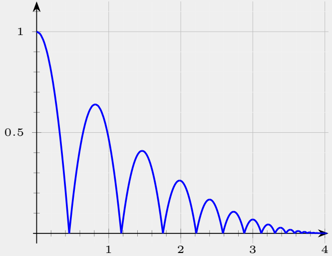
Bouncing Ball

Bouncing ball is a simple Newtonian system specified by differential equation $\ddot{h} = -g$ ($g \approx 9.8$) whose solution is

$$h(t) = h_0 + v_0 t - \frac{gt^2}{2}$$

with initial values:

- $v_0 = 0, h_0 \neq 0$ (peak height)
- $h_0 = 0, v_0 \neq 0$ (zero height)



Features:

- deterministic
- hybrid: the velocity changes discretely at the bottom $v \mapsto -cv$, but it changes continuously in the meanwhile
- progressive: every iteration consumes non-zero time
- Zeno behaviour: the state of rest is only reachable in the limit

damping factor

Bouncing ball can be formalized in an idealized language HybCore:

$$
\begin{array}{l}
x := [\![(5,0)]\!]\ \textbf{while true} \\
\{ \\
\qquad (h,v) := (x := t.\, \mathit{ball}(x,t)\ \textbf{\&}\ \mathrm{fst}\, x \geqslant 0); \\
\qquad [\![(h, -c\, v)]\!] \\
\}
\end{array}
$$

Here, $\mathit{ball}(a,b,t)$ is the solution of the initial value problem $\{\dot{h} = v, \dot{v} = -g, h(0) = a, v(0) = b\}$

The critical element of the semantics is Elgot iteration: $(f : X \to T(Y \uplus X)) \mapsto (f^\dagger : X \to TY)$ for a suitable monad T

We distinguish

- Duration semantics: $TX = \mathbb{R}_+ \times X \cup \bar{\mathbb{R}}_+$, i.e. a computation either converges in finite time and delivers a value in X, or diverges in possibly infinite time ($\bar{\mathbb{R}}_+ = \mathbb{R}_+ \cup \{\infty\}$)
- Evolution semantics: $TX = S^{[0,\mathbb{R}_+)} \times X \cup S^{[0,\bar{\mathbb{R}}_+)}$ where $S^{[0,\mathbb{R}_+)} = \Sigma_{d\colon \mathbb{R}_+} [0,d) \to S$ is the space of finite trajectories and $S^{[0,\bar{\mathbb{R}}_+)} = \Sigma_{d\colon \bar{\mathbb{R}}_+} [0,d) \to S$ is the space of possibly infinite trajectories over S

Idea for Abstraction: Vault to general monoids instead of concrete $\mathbb{R}_+$, $S^{[0,\mathbb{R}_+)}$

Fix a (not necessarily commutative) monoid $(\mathbb{M}, +, 0)$

A monoid $\mathbb{M}$-module is a set $\mathbb{E}$ equipped with a map $\triangleright : \mathbb{M} \times \mathbb{E} \to \mathbb{E}$, subject to the laws

$$0 \triangleright e = e \qquad\qquad (m + n) \triangleright e = m \triangleright (n \triangleright e)$$

Every monoid-module pair $(\mathbb{M}, \mathbb{E})$ induces the generalized writer monad: $T = \mathbb{M} \times (-) \cup \mathbb{E}$

For example, with $\mathbb{M} = \mathbb{E} = 1$ we obtain the maybe monad $(-) \cup \{\bot\}$, which is incidentally an Elgot monad

Problem: Elgotness relies on the law of excluded middle!

Categories Strike Back

We assume $\mathbb{M}$ to be ordered with 0 being the bottom and right monotone $+$

Examples: 1, $\mathbb{N}$, $\mathbb{Q}_+$, $\mathbb{R}_+$, $S^{[0,\mathbb{R}_+)}$, S^* (for last two $+$ is neither commutative, nor left monotone)

Definition (Complete $\mathbb{M}$-Modules)

An ordered $\mathbb{M}$-module is additionally equipped with a partial order $\sqsubseteq$ and $\bot$, such that

$$\frac{}{\bot \sqsubseteq x} \qquad \frac{x \sqsubseteq y}{a \triangleright x \sqsubseteq a \triangleright y} \qquad \frac{a \leqslant b}{a \triangleright \bot \sqsubseteq b \triangleright \bot}$$

An ordered $\mathbb{M}$-module is complete if for any directed $(s_i)_i$ on $\mathbb{E}$ there is a least upper bound $\bigsqcup_i s_i$ and

$$\bigsqcup_i a \triangleright s_i \sqsubseteq a \triangleright \bigsqcup_i s_i$$

Free Objects

We extend previous construction of partiality monad ($\mathbb{M} = 1$) [1]

Recall the concept of free object: Given a functor $U\colon \mathbf{C} \to \mathbf{Set}$, an object FX is free on X if there is $(\eta_X\colon X \to UFX)_X$ and for every $f\colon X \to UY$ there is unique $f^\star\colon FX \to Y$ such that

$$\begin{tikzcd}
UFX \arrow[r, dotted, "Uf^\star"] & UY \\
X \arrow[u, "\eta_X"] \arrow[ur, "f"'] &
\end{tikzcd}$$

Standard facts:

- all free objects FX exist iff F is a left adjoint to U
- if all free objects exist then $(UF, \eta, (-)^\star)$ constitutes a monad (in the form of Klesili triple)

[1] Thorsten Altenkirch, Nils Danielsson, and Nicolai Kraus. Partiality, revisited – the partiality monad as a quotient inductive-inductive type

Theorem

Let $\mathbf{Alg}_{\widetilde{L}}$ *be the category of complete* $\mathbb{M}$*-modules and* $U\colon \mathbf{Alg}_{\widetilde{L}} \to \mathbf{Set}$ *be the obvious forgetful functor*

1. *All free objects w.r.t.* U *exist, yielding a monad* $\widetilde{L}$
2. $\widetilde{L}$ *is enriched over directed complete partial orders, and moreover, Kleisli composition is strict on both sides*
3. $\widetilde{L}$ *is an Elgot monad with the iteration operator* $(f: X \to \widetilde{L}(Y \uplus X))^\dagger$ *calculated as a least fixed point of the map* $[\eta, -]^\star f\colon (X \to \widetilde{L}Y) \to (X \to \widetilde{L}Y)$

This is true both classically and constructively, thanks to quotient inductive-inductive types[2]

[2] Thorsten Altenkirch, Paolo Capriotti, Gabe Dijkstra, Nicolai Kraus, and Fredrik Nordvall Forsberg. Quotient inductive-inductive types.

$\widetilde{L}$ VIA DIRECTED COMPLETION

Let $\mathbb{M}_X = \mathbb{M} \times (X \uplus \{\bot\})$, and define $\triangleright_X$, $\sqsubseteq_X$ with rules:

$$\frac{}{a \triangleright_X (b, p) = (a + b, p)} \qquad \frac{}{(a, \mathrm{inl}\, p) \sqsubseteq_X (a, \mathrm{inl}\, p)} \qquad \frac{a \leqslant b}{(a, \mathrm{inr}\, \bot) \sqsubseteq_X (b, p)}$$

Lemma

For any set X, $(\mathbb{M}_X, \triangleright_X, (0, \mathrm{inr}\, \bot), \sqsubseteq_X)$ is an ordered $\mathbb{M}$-module.

Intuitively, we are interested in limits of directed sequences over $\mathbb{M}_X$, e.g.

- convergent: $(1, \mathrm{inr}\, \bot) \sqsubseteq_X \ldots \sqsubseteq_X (n, \mathrm{inr}\, \bot) \sqsubseteq_X (n + 1, \mathrm{inl}\, 0)$
- divergent: $(1, \mathrm{inr}\, \bot) \sqsubseteq_X \ldots \sqsubseteq_X (1, \mathrm{inr}\, \bot) \sqsubseteq_X \ldots$
- Zeno: $(1/2, \mathrm{inr}\, \bot) \sqsubseteq_X \ldots \sqsubseteq_X (n/(n + 1), \mathrm{inr}\, \bot) \sqsubseteq_X \ldots$

Directed Completion

- $(s_i)_i \lesssim_X (t_i)_i$ if $\forall i \colon \mathbb{N}.\, \exists j \colon \mathbb{N}.\, s_i \sqsubseteq_X t_j$
- $s \sim_X t$ if $s \lesssim_X t$ and $t \lesssim_X s$
- $\tilde{\mathbb{M}}_X$ is the quotient under $\sim_X$ of the set of directed sequences over $\mathbb{M}_X$ and write $[s_i]_i$ instead of $[(s_i)_i]_\sim$

Theorem (Only Classically!)

$(\tilde{\mathbb{M}}_X, \triangleright_X, \bot_X, \lessapprox_X, \overset{\approx}{\bigvee}_X)$ *is a free complete* $\mathbb{M}$*-module on* X *with*

$$[s]_\sim \lessapprox_X [t]_\sim \ \text{if}\ s \lesssim_X t \qquad a \triangleright_X [s_i]_i = [a \triangleright_X s_i]_i$$

$$\bot_X = [(0, \mathrm{inr}\,\bot)]_i \qquad \overset{\approx}{\bigvee}_{X\, i} [s_{i,j}]_j = [s_{\pi_1^{-1}(i), \pi_2^{-1}(i)}]_i$$

where $\pi(x, y) = \frac{1}{2}(x + y)(x + y + 1) + x$

Cantor pairing function

Duration and Generalized Writer

Let us write $\tilde{\mathbb{M}}_\emptyset$ as $\tilde{\mathbb{M}}$.

Theorem (Only Classically!)

- *$\tilde{L}X$ and $\tilde{\mathbb{M}}_X$ are isomorphic as complete $\mathbb{M}$-modules*
- *$\tilde{L}X \cong \mathbb{M} \times X \cup \tilde{\mathbb{M}}$ – generalized writer monad over $(\mathbb{M}, \tilde{\mathbb{M}})$*

Examples:

- for $\mathbb{M} = 1$, $\tilde{L}X = X \cup \{\bot\}$
- for $\mathbb{M} = \mathbb{N}$, $\tilde{L}X = \mathbb{N} \times X \cup \bar{\mathbb{N}}$
- **but** for $\mathbb{M} = \mathbb{R}_+$, $\tilde{L}X = \mathbb{R}_+ \times X \cup \tilde{\mathbb{R}}_+$ where $\tilde{\mathbb{R}}_+ \cong \mathbb{R}_+ \uplus (\mathbb{R}_+ \setminus \{0\}) \uplus \{\infty\} \cong \bar{\mathbb{R}}_+ \uplus (\mathbb{R}_+ \setminus \{0\})$, because of Zeno behaviour!

Conservative Completeness

Definition (Conservatively Complete Monoid Modules)

A complete $\mathbb{M}$-module is conservatively complete if for every directed $(a_i)_i$ in $\mathbb{M}$, such that $\bigvee_i a_i$ exists,

$$\bigsqcup_i a_i \triangleright \bot = \left(\bigvee_i a_i\right) \triangleright \bot$$

Analogously, we introduce free conservatively complete $\mathbb{M}$-modules $\bar{L}X$ on X, and obtain an Elgot monad $\bar{L}$

Conservative Completion

Let $\bar{\mathbb{M}}_X$ be constructed in the same way as $\tilde{\mathbb{M}}_X$, but with the additional clause added to the equivalence relation $\sim$:

$$(a_i, \mathsf{inr}\,\bot)_i \sim (a, \mathsf{inr}\,\bot)_i \qquad \text{whenever} \qquad a = \bigvee_i a_i.$$

Theorem (Only Classically)

Suppose that $\mathbb{M}$ has the following properties: given directed sequences $(a_i)_i$ and $(b_i)_i$ over $\mathbb{M}$

1. *If $\bigvee_i b_i$ exists then $\bigvee_i a + b_i = a + \bigvee_i b_i$*
2. *If $\bigvee_i a_i$ exists and for every i there exists j such that $a_i \leqslant b_j$ then either $\bigvee_i b_i$ exists or $\bigvee_i a_i \leqslant b_j$ for some j*

Then $(\bar{\mathbb{M}}_X, \triangleright_X, \bot_X, \lessapprox_X, \tilde{\tilde{\bigvee}}_X)$ is a free conservatively complete $\mathbb{M}$-module on X

Again, let $\bar{\mathbb{M}} = \bar{\mathbb{M}}_\emptyset$

Theorem

$\bar{L}X \cong \mathbb{M} \times X \cup \bar{\mathbb{M}}$

Examples:

- for $\mathbb{M}$, not exposing Zeno behaviour, $\bar{\mathbb{M}} = \tilde{\mathbb{M}}$, hence $\bar{L} \cong \tilde{L}$
- $\bar{\mathbb{R}}_+ \cong \mathbb{R}_+ \cup \{\infty\}$
- $\overline{S^{[0,\mathbb{R}_+)}} \cong S^{[0,\bar{\mathbb{R}}_+)}$
- $\overline{\mathbb{R}_+} = \mathbb{R}_+ \cup \{\infty\}$

MLTT and HoTT

In Martin-Löf Type Theory:

Formula	Type
$\top$	$\mathbf{1}$
$\bot$	$\mathbf{0}$
$A \wedge B$	$A \times B$
$A \vee B$	$A \uplus B$
$\forall x \rightarrow A(x)$	$\prod_{x : I} A(x)$
$\exists [\, x \,]\, A(x)$	$\sum_{x : I} A(x)$

Some examples:

- A is a mere proposition: $\mathsf{IsProp}\ A = \forall\ (x\ y : A) \to x \equiv y$
- A is a set: $\mathsf{IsSet}\ A = \forall\ (x\ y : A) \to \mathsf{IsProp}\ (x \equiv y)$
- A is decidable: $\mathsf{IsDec}\ A = A \vee \neg\ A$

In HoTT and in Cubical Agda (which implements HoTT), we can express properly more, e.g. propositional truncation as a quotient inductive-inductive type:

```
data ||_|| (A : Set ℓ) : Set ℓ where
  |_| : A → || A ||
  ||||-prop : IsProp || A ||
```

That is: We squash the space of proofs inhabiting *A*, to the space of mere affirmative propositions $\|A\|$

Axiom of countable choice:

```
ACω {ℓ} = ∀ (P : ℕ → Set ℓ) → (∀ n → || P n ||) → || (∀ n → P n) ||
```

We can formalize chains, intensionally and extensionally directed sequences:

$$\mathsf{Inc}\ \sigma = \forall\ (n : \mathbb{N}) \to \sigma\ n \leqslant \sigma\ (\mathsf{suc}\ n)$$
$$\mathsf{Dir}\ \sigma = \forall\ (n\ m : \mathbb{N}) \to \exists[\ k\ ]\ (\sigma\ n \leqslant \sigma\ k \land \sigma\ m \leqslant \sigma\ k)$$
$$||\mathsf{Dir}||\ \sigma = \forall\ (n\ m : \mathbb{N}) \to ||\ \exists[\ k\ ]\ (\sigma\ n \leqslant \sigma\ k \land \sigma\ m \leqslant \sigma\ k)\ ||$$

Theorem

Let (a), (b) and (c) stand for completeness of a fixed set A w.r.t. ||Dir||, Dir and Inc correspondingly. Then

- *(a) $\Rightarrow$ (b) $\Rightarrow$ (c);*
- *(b) $\Rightarrow$ (a) under countable choice;*
- *(c) $\Rightarrow$ (a) under the decidability of $\leqslant$ on A (i.e. under $\forall\ (x\ y : A) \to$ IsDec $(x \leqslant y)$).*

Further Work

Further Work

- Implement free objects in cubical Agda (currently adhoc)
- Is it possible to rebase $\widetilde{L}$ and $\bar{L}$ on extensional completeness (currently based on intensional completeness)? Which approach would be the right one if both are possible?
- Implement classical characterizations of $\widetilde{L}$ and $\bar{L}$ in cubical Agda (possible under countable choice?)
- Can the general conservative completion construction be simplified?