Generic Operational Metatheory

Long internship, First year Master

Aliaume Lopez
Alex K. Simpson

August 30, 2017

University *of Ljubljana*
Faculty *of Mathematics and Physics*

école normale supérieure paris–saclay

Hosting Institution

University Of Ljubljana (FMF)

Figure 1: FMF Building

Ljubljana

Figure 2: Map of Ljubljana

	Ljubljana	Montpellier
Population	279,756	275,318
Area	163,8 km^2	56,88 km^2
Capital City	✓	✗
Bike friendly	✓✓	✓
Free Wifi	✓	✗
MFPS & Calco	✓	✗

Table 1: An unfair comparison of two cities

The computer science team

Andrej Bauer

Alex K. Simpson

PhD Students

- Neils Voorneveld
- Philipp Haselwarter
- (Brett Chenoweth)
- +7 others

And many others (Matija Pretnar …)

The computer science team

Andrej Bauer

Alex K. Simpson

PhD Students

- Neils Voorneveld
- Philipp Haselwarter
- (Brett Chenoweth)
- +7 others

And many others (Matija Pretnar ...)

Speaking of ...

Matija Pretnar & Andrej Bauer : local Calco/MFPS organisers for 2017 !

Calco 2017 & MFPS XXXIII

12–16 June 2017, Ljubljana, Slovenia

- **MFPS** Mathematical Foundations of Programming Semantics
- **Calco** Algebra and Coalgebra in Computer Science

Calco 2017 & MFPS XXXIII

12–16 June 2017, Ljubljana, Slovenia

MFPS Mathematical Foundations of Programming Semantics

Calco Algebra and Coalgebra in Computer Science

Some known faces …

12–16 June 2017, Ljubljana, Slovenia

MFPS Mathematical Foundations of Programming Semantics

Calco Algebra and Coalgebra in Computer Science

Some known faces …

12–16 June 2017, Ljubljana, Slovenia

MFPS Mathematical Foundations of Programming Semantics

Calco Algebra and Coalgebra in Computer Science

Some known faces …

12–16 June 2017, Ljubljana, Slovenia

MFPS Mathematical Foundations of Programming Semantics

Calco Algebra and Coalgebra in Computer Science

Some known faces ...

12–16 June 2017, Ljubljana, Slovenia

MFPS Mathematical Foundations of Programming Semantics

Calco Algebra and Coalgebra in Computer Science

Some known faces ...

... And many others !

Contextual Equivalence

What does this mean ?

$$\bigvee_r a \otimes (b \multimap \overline{\eth} c)!_r$$

This is just syntax !

Natural	Artificial
words	symbols
grammar	grammar
sentence	tree
meaning	?

Table 2: From natural to artificial languages

”To define it rudely but not inaptly...”

”To define it rudely but not inaptly...”

Operation Describe how to *deal with* the sentences.

”To define it rudely but not inaptly…”

Operation Describe how to *deal with* the sentences.

Denotation Describe how to *interpret* the sentences.

”To define it rudely but not inaptly…”

Operation Describe how to *deal with* the sentences.

Denotation Describe how to *interpret* the sentences.

Non termination

Operation infinite reduction, absence of derivation — meta-theory

Denotation interpreted as $\perp$ — included

”To define it rudely but not inaptly...”

Operation Describe how to *deal with* the sentences.

Denotation Describe how to *interpret* the sentences.

Non termination

Operation infinite reduction, absence of derivation — meta-theory

Denotation interpreted as $\perp$ — included

> *(Operational Semantics) equates the meaning of a syntactic entity with another syntactic entity*
>
> *Andrej Bauer*

Operational Equivalences

Operational Equivalences

- Two sentences have the same operational meaning Not so good

Operational Equivalences

- Two sentences have the same operational meaning Not so good
- We can interchange the two sentences in any bigger one and preserve meaning Contextual Equivalence

Operational Equivalences

- Two sentences have the same operational meaning Not so good
- We can interchange the two sentences in any bigger one and preserve meaning Contextual Equivalence

$$\forall C[-], C[M] \sim C[M']$$

Operational Equivalences

- Two sentences have the same operational meaning Not so good
- We can interchange the two sentences in any bigger one and preserve meaning Contextual Equivalence

$$\forall C[-], C[M] \sim C[M']$$

Two distinct things cannot have all their properties in common

Gottfried Wilhelm Leibniz (1646–1716)

Proving non-equivalence is *easy*

Find some way to discriminate behaviour

Proving equivalence is *hard*

Test *for any* context C …

> *To emphasise this point, we tease the reader with a similar informal 'proof' of contextual equivalence that turns out to be false. […] The italicised part of this 'proof' is of the same kind as in the previous case, but this time it is false.*
>
> *Andrew Pitts [7]*

Fortune favors the prepared mind

A *meaning* on simple terms is given and a contextual equivalence is derived from it. You compare it to another equivalence relation

Sound Two related sentences are contextually equivalent

Adequate Two simple sentences "obviously" equal are related

Complete Two contextually equivalent sentences are related

Alternatives

Solution	Sound	Complete	Usable	General
Coinduction	✓	✓	✗	(✓)
CIU	✓	✓	✗	✓
Domains	✓	✗	✓	✓
Games	✓	✓	✓	✗
Logical Relations	✓	✓	✓	✗
Bisimulation	✓	✗	✓	✓
Logics	✓	✓	✓	✗

Table 3: Some very rough approximations ...

Logical Relations

Logical Relations are saving the day !

A man who does not think and plan long ahead will find trouble right at his door.

Confucius

Logical Relations are saving the day !

> *A man who does not think and plan long ahead will find trouble right at his door.*
>
> *Confucius*

If all goes according to plan ...

1. Construct a (parametrised) relation $\sim$ ✓
2. Check adequacy and compatibility of $\sim$ *biorthogonality*
3. Prove reflexivity ✓
4. Prove saturation *biorthogonality*
5. Deduce $\sim = \equiv_{ctx}$ ✓
6. Profit ... ?!

Theorems for free ! [10]

Write down the definition of a polymorphic function on a piece of paper. Tell me its type, but be careful not to let me see the function's definition. I will tell you a theorem that the function satisfies.

A famous example

The only function from $\forall \alpha . \alpha \to \alpha$ is the identity function up to contextual equivalence

Two Steps from the Effects

You cannot step into the same river twice

Arbitrary signature Σ for effects ...

$$
\begin{aligned}
\tau &:= \mathsf{Nat} \mid \tau \to \tau \\
V &:= x \mid \lambda x : \tau . M \mid \mathsf{Z} \mid \mathsf{S}\, V \\
M &:= \mathsf{return}\, V \mid VV \mid \mathsf{fix}\, V \\
&\quad \mid \mathsf{case}\, V\, \mathsf{of}\, \mathsf{Z} \Rightarrow M; \mathsf{S}(x) \Rightarrow M \\
&\quad \mid \mathsf{let}\, x : \tau \Leftarrow M\, \mathsf{in}\, M \mid \sigma(V, \ldots, V) \quad \sigma \in \Sigma
\end{aligned}
$$

Figure 3: Refined Call-By-Value PCF with effects

Step by step and the thing is done

… And two steps definition

Step by step and the thing is done

… And two steps definition

1. Regular PCF semantics ✓

Step by step and the thing is done

… And two steps definition

1. Regular PCF semantics ✓
2. Semantics of effects ? ✗

Step by step and the thing is done

... And two steps definition

1. Regular PCF semantics ✓
2. Semantics of effects ? ✗

Even a fool is thought wise if he keeps silent, and discerning if he holds his tongue

Proverbs 17:28

Step by step and the thing is done

... **And two steps definition**

1. Regular PCF semantics ✓
2. Semantics of effects ? ✗

Even a fool is thought wise if he keeps silent, and discerning if he holds his tongue

Proverbs 17:28

LET'S BUILD A TREE [8] [4]

In case is wasn't obvious...

$$(\lambda x : \tau.\lambda y : \tau.(\mathsf{return}\, x) \oplus (\mathsf{return}\, y))\, \underline{0}\, \underline{1}$$

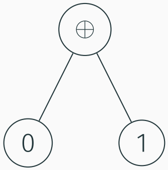
In case is wasn't obvious...

$$(\lambda y : \tau.(\mathrm{return}\,\underline{0}) \oplus (\mathrm{return}\,y))\,\underline{1}$$

In case is wasn't obvious...

$$(\text{return}\,\underline{0}) \oplus (\text{return}\,\underline{1})$$

In case is wasn't obvious...

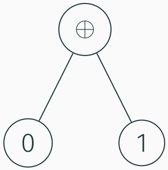


In case is wasn't obvious...

$$(\lambda x : \tau.\lambda y : \tau.(\text{return}\, x) \oplus (\text{return}\, y))\, \underline{0}\, \underline{1}$$

$$(\lambda y : \tau.(\text{return}\, \underline{0}) \oplus (\text{return}\, y))\, \underline{1}$$

$$(\text{return}\, \underline{0}) \oplus (\text{return}\, \underline{1})$$



Happy is he who can trace effects to their causes

Building the tree

$$\begin{aligned}
|S, M| &= |S', M'| && (S, M) \rightarrowtail (S', M') \\
|Id, \mathrm{return}\, V| &= V \\
|S, \sigma(M_1, \ldots, M_n)| &= \sigma(|S, M_1|, \ldots, |S, M_n|)
\end{aligned}$$

The big picture

$$\Lambda_{\mathrm{Nat}} \xrightarrow{\;|\cdot|\;} \mathrm{Tree}_{\mathrm{Nat}}$$

$$R(\Lambda_{\mathrm{Nat}}) \xleftarrow[\;|\cdot|R|\cdot|\;]{} R(\mathrm{Tree}_{\mathrm{Nat}})$$

Preorders $\sqsubseteq_b$

He enters the port with a full sail

Effects Σ a collection of symbols

Preorder $\sqsubseteq_b$ a relation on $\mathsf{Tree}_{\mathsf{Nat}}$

Preorders $\sqsubseteq_b$

He enters the port with a full sail

Effects Σ a collection of symbols

Preorder $\sqsubseteq_b$ a relation on $\mathsf{Tree}_{\mathsf{Nat}}$

He who seeks for gain, must be at some expense

- Admissible — behaves nicely with *approximation*
- Compositional — observations can be composed

Veni, Vidi, Vici ...

Theorem

Contextual preorder equals the logical relation

Veni, Vidi, Vici ...

Theorem

Contextual preorder equals the logical relation

General

- Reduction to closed terms
- Equivalence CIU
- Kleene compatible

Theorem

Contextual preorder equals the logical relation

General

- Reduction to closed terms
- Equivalence CIU
- Kleene compatible

Effects

- Stacks commute with effects
- Inequalities seen at ground type

Veni, Vidi, Vici ...

Theorem

Contextual preorder equals the logical relation

General

- Reduction to closed terms
- Equivalence CIU
- Kleene compatible

Effects

- Stacks commute with effects
- Inequalities seen at ground type

Extensions

- Polymorphism
- Recrusive types
- More effects

Practical example

Combined scheduler

Randomised Algorithms with Scheduler

- Σ coin $\oplus$, angel $\sqcup$, demon $\sqcap$
- $\sqsubseteq_b$ capture the behaviour ... and satisfies the requirements

Combined scheduler

Randomised Algorithms with Scheduler

Σ coin $\oplus$, angel $\sqcup$, demon $\sqcap$

$\sqsubseteq_b$ capture the behaviour ... and satisfies the requirements

An image is worth a thousand words

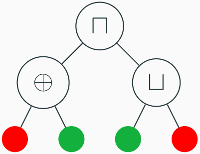


Figure 4: Beyond good and evil

Powerdomains and axiomatics …

Combining powerdomains with distributive laws is not enough (Michael Mislove [6]) …

Construction	Reference
« Previsions »	Jean-Goubault Larrecq [3]
Cones/Powercones	Regina Tix [9]
Kegelspitze	Klaus Keimel & Gordon Plotkin [5]

Table 4: Recap of the denotational side

Time to part ways ...

How I met your preorder

- From a denotation $[\![\cdot]\!]$ ✓
- From good observations [4] ✓
- From free construction (✓)
- From some operational construction ?

Compare Markov Decision Processes pointwise, where a point is an objective *set* $X \subseteq \mathrm{Nat}$:

$$t \sqsubseteq_b t' \iff \forall X \subseteq \mathrm{Nat}, \quad \inf_{\pi} \mathbb{E}^{\pi}(t \in X) \leq \inf_{\pi} \mathbb{E}^{\pi}(t' \in X)$$

Compare Markov Decision Processes pointwise, where a point is an objective *set* $X \subseteq \mathrm{Nat}$:

$$t \sqsubseteq_b t' \iff \forall X \subseteq \mathrm{Nat}, \quad \inf_{\pi} \mathbb{E}^{\pi}(t \in X) \leq \inf_{\pi} \mathbb{E}^{\pi}(t' \in X)$$

Breaks compositionality … … for very good reasons [6]

Compare Markov Decision Processes pointwise, where a point is an objective function $h : \mathrm{Nat} \to \overline{\mathbb{R}_+}$:

$$t \sqsubseteq_b t' \iff \forall h : \mathrm{Nat} \to \overline{\mathbb{R}_+}, \quad \inf_{\pi} \mathbb{E}^{\pi}(h(t)) \leq \inf_{\pi} \mathbb{E}^{\pi}(h(t'))$$

Is there some connection between him and Buffalo Bill maybe?

$$\sqsubseteq_{op} = \sqsubseteq_{[\![\cdot]\!]} = \text{free}(\sqcap) \odot \text{free}(\oplus)$$

Conclusion & Future work

Nothing's beautiful from every point of view

What has been done

- Generic operational meta-theory for *call-by-value* languages with *restricted* class of effects
- Clear connection to the *denotational* setting
- Results about behaviours of preorders
- Application to a non-trivial example

Nothing's beautiful from every point of view

What could be done

- Small extensions (recursive types, polymorphism, parametrized effects, ...) ✯
- In depth study of the generation of preorders ✯
- Link with bisimulations as done in [2] ✯ ✯
- All algebraic effects, non algebraic effects [1] ✯ ✯
- Quantitative version ✯ ✯ ✯

Questions ?

A. Bauer and M. Pretnar.
Programming with algebraic effects and handlers.
CoRR, abs/1203.1539, 2012.

U. Dal Lago, F. Gavazzo, and P. Blain Levy.
Effectful Applicative Bisimilarity: Monads, Relators, and Howe's Method (Long Version).
ArXiv e-prints, Apr. 2017.

J. Goubault-Larrecq.
Isomorphism theorems between models of mixed choice.
Mathematical Structures in Computer Science, 2016.
To appear.

P. Johann, A. Simpson, and J. Voigtländer.
A generic operational metatheory for algebraic effects.
In *2010 25th Annual IEEE Symposium on Logic in Computer Science*, pages 209–218, July 2010.

K. Keimel and G. D. Plotkin.
Mixed powerdomains for probability and nondeterminism.
Logical Methods in Computer Science, 13(1), 2017.

M. Mislove, J. Ouaknine, and J. Worrell.
Axioms for probability and nondeterminism.
Electronic Notes in Theoretical Computer Science, 96:7–28, 2004.

A. M. Pitts and I. D. B. Stark.
Higher order operational techniques in semantics.
chapter Operational Reasoning for Functions with Local State, pages 227–274. Cambridge University Press, New York, NY, USA, 1998.

G. Plotkin and J. Power.
Adequacy for algebraic effects.
In *International Conference on Foundations of Software Science and Computation Structures*, pages 1–24. Springer, 2001.

R. Tix, K. Keimel, and G. Plotkin.
Semantic domains for combining probability and non-determinism.
Electronic Notes in Theoretical Computer Science, 222:3–99, 2009.

P. Wadler.
Theorems for free!
In *Proceedings of the fourth international conference on Functional programming languages and computer architecture*, pages 347–359. ACM, 1989.