Computational Adequacy and Choice: How Deep is the Rabbit Hole?

Sergey Goncharov

FAU Erlangen-Nürnberg

November 2, 2021, Oberseminar Theoretische Informatik

Setting the Stage: Adequacy in the Abstract

Classically:

- Operational semantics defines a reduction relation $\rightarrow$ on terms
- Denotational semantics defines domains DX and maps $[\![-]\!]$ from programs producing values of type X, to DX
- Soundness: If $t \longrightarrow^{\star} v$ for a value v then $[\![t]\!] = [\![v]\!]$
- (Computational) Adequacy: if $[\![t]\!] = [\![v]\!]$ then there is a reduction $t \longrightarrow^{\star} v$

Call this scenario "Coarse-Grained Adequacy". There are many variations

Fine-Grained Adequacy

- Let the reduction relation $\to$ be labelled, and let $t \to_{a_1 \ldots a_n} v$ iff $t \to_{a_1} t' \to_{a_2} \ldots \to_{a_n} v$
- Let DX be the final coalgebra $\nu\gamma. (X + A \times \gamma)$
- Fine-Grained Adequacy: if $[\![t]\!] = (w, v)$ then there is a reduction $t \to^{w} v$

Questions:

- Generic categorical[1] machinery for coarse-grained adequacy
- Generic categorical machinery for fine-grained adequacy
- Generic connection between them

[1] "Generic categorical" = at least includes **Top**

Example: Natural Number Object

- Language of programs:

$$p, q ::= \underline{a} \mid p; q \mid \text{if } c \text{ then } p \text{ else } q$$

where $\underline{a}$ ranges over atomic programs, and c over conditions

- Operational semantics (w.r.t. $\underline{a} \colon S \to S$, $c \colon S \to 2$):

$$\frac{}{\langle \sigma, \underline{a} \rangle \downarrow \underline{a}(\sigma)} \qquad \frac{\langle \sigma, p \rangle \to \langle \sigma', p' \rangle}{\langle \sigma, p; q \rangle \to \langle \sigma', p'; q \rangle} \qquad \frac{\langle \sigma, p \rangle \downarrow \sigma'}{\langle \sigma, p; q \rangle \to \langle \sigma', q \rangle}$$

$$\frac{c(\sigma) = \text{true}}{\langle \sigma, \text{if } c \text{ then } p \text{ else } q \rangle \to \langle \sigma, p \rangle} \qquad \frac{c(\sigma) = \text{false}}{\langle \sigma, \text{if } c \text{ then } p \text{ else } q \rangle \to \langle \sigma, q \rangle}$$

- Fine-grained soundness and adequacy: $\langle \sigma, p \rangle \to^n \langle \sigma', p' \rangle \downarrow \sigma''$ iff $[\![p]\!](\sigma) = (n, \sigma'')$ where the semantics $[\![p]\!] \colon S \to S \times \mathbb{N}$

Coarsenning Semantics

- Observe that we are indeed too fine-grained, i.e. if p terminates in n steps, $(\text{if true then } p \text{ else } q)$ terminates in $n+1$ steps, hence no operational equivalence:

$$p \sim \text{if true then } p \text{ else } q$$

- We can either prove coarse-grained adequacy, or (better!) quotient the denotational domain $S \times \mathbb{N}$ by weak bisimilarity:

$$\frac{}{\rhd p \approx p} \qquad \frac{}{p \approx \rhd p} \qquad \frac{p \approx q}{\rhd p \approx \rhd q}$$

- This is generic, for

$$S \times \mathbb{N} \underset{\text{id}}{\overset{\rhd}{\rightrightarrows}} S \times \mathbb{N} \xrightarrow{\text{fst}} S$$

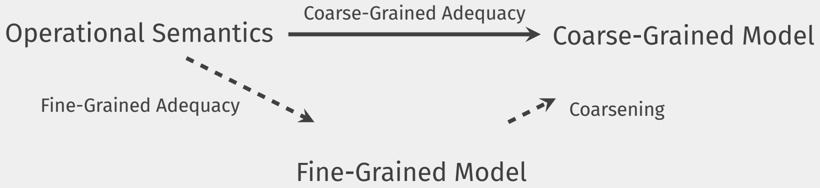
is a co-equalizer. In fact, this can be taken as a definition of the natural number object (suggested by Freyd (with $S = 1$))

- Define fine-grained semantics (e.g. using GSOS)
- This produces a monad D, so that DX collects denotations of programs with terminal values in X
- Introduce a notion of weak bisimilarity $\approx$ on D
- Obtain $\tilde{D}$ as a quotient of D

Is it possible that $\tilde{D}$ is a monad?

Spoiler: probably not, unless we rely on some weak form of the axiom of choice

Why it is a problem? Because some fundamental models of computation (prominently MLTT and HoTT) do not assume any form of choice, even very weak ones



Generally, either

- Coarse-grained adequacy fails
- Target denotational model not compositional (not a monad)
- There is some choice

Towards Semantics of Non-termination

Rutten's While-Language

Theoretical Informatics and Applications
Theoret. Informatics Appl. **33** (1999) 393–400

A NOTE ON COINDUCTION AND WEAK BISIMILARITY FOR WHILE PROGRAMS

J.J.M.M. Rutten[1]

Abstract. An illustration of coinduction in terms of a notion of weak bisimilarity is presented. First, an operational semantics $\mathcal{O}$ for while programs is defined in terms of a final automaton. It identifies any two programs that are weakly bisimilar, and induces in a canonical manner ... ed by coinduction.

...Q55.

1. Automata

Let O be a (possibly infinite) set of output symbols. An *automaton* with outputs in O is a pair $S = (S, \alpha)$ consisting of a set S of *states* and a *transition function* $\alpha : S \to O + S$. The transition function α specifies for a state s in S either an output o in O or a next state s' in S. The intuition is that in the first case, the computation is terminating, with observable output o; in the second case, the computation takes one step and will continue from the new state s'. We shall sometimes write $s \downarrow o$ if $\alpha(s) = o \in O$, and $s \longrightarrow_S s'$ if $\alpha(s) = s' \in S$. If S is clear from the context, we shall simply write $s \longrightarrow s'$.

This type of automaton is sometimes referred to as *Elgot machine*, because of the prominent role similar such structures play in the work of Elgot (*cf.* [3]).

Adding While-Loops

- $p, q ::= \underline{a} \mid p; q \mid \text{if } c \text{ then } p \text{ else } q \mid \text{while } c \text{ do } p$
- In the operational semantics add:

$$\frac{c(\sigma) = \text{true}}{\langle \sigma, \text{while } c \text{ do } p \rangle \to \langle \sigma, p; \text{while } c \text{ do } p \rangle}$$

$$\frac{c(\sigma) = \text{false}}{\langle \sigma, \text{while } c \text{ do } p \rangle \downarrow \sigma}$$

- A fine-grained semantics can be defined using (now) standard machinery over $DX = \nu\gamma.\, X + \gamma$
- Weak bisimilarity can be defined as before
- Rutten relies on $DX \cong X \times \mathbb{N} + 1$, which entails $\tilde{D}X \cong X + 1$

Rest of the talk: analysis of situations when it need not be so

Work on partiality monads

- Chapman, Uustalu, Veltri: Quotienting the delay monad by weak bisimilarity (coinduction + quotienting)
- Altenkirch, Danielsson, Kraus: Partiality, revisited - the partiality monad as a quotient inductive-inductive type (induction)
- Escardó, Knapp: Partial Elements and Recursion via Dominances in Univalent Type Theory (comparison + disciplined maps)

Work on iteration

- Adámek, Milius, Velebil: Elgot algebras
- Adámek, Milius, Velebil: Elgot theories: a new perspective of the equational properties of iteration

Iteration-Based Notion of Partiality

Our Assumptions

We work in a category **C** that

- has finite products
- has finite coproducts
- is extensive (coproducts are stable under pullbacks, coproduct injections are disjoint, pullbacks of coproduct injections exist)
- natural number object $\mathbb{N}$ exists and stable
- exponentials $X^{\mathbb{N}}$ exist

Examples: Classical and non-classical set theories, toposes, pretoposes, importantly also topological spaces **Top**

Initial Algebras as Free Objects

Consider pairs $(A, s\colon A \to A)$ where

- $A \in |\mathbf{C}|$
- s is the successor function
- These algebras form a category, and for every $X \in |\mathbf{C}|$ there a free object over X, which is precisely the initial algebra

$$\mu\gamma.\, X + \gamma \cong X \times \mathbb{N}$$

- Interpretation: $X \times \mathbb{N}$ contains only terminating computations, and remembers number of steps, needed for termination;

$$\triangleright : X \times \mathbb{N} \xrightarrow{[\mathrm{id} \times \mathrm{suc}]} X \times \mathbb{N}$$

  is the delay operator

- Let us augment our algebras $(A, s\colon A \to A)$ with means for iterating computations
- Consider morphisms of the form $h\colon S \to A + S$ with
  - values in A
  - states in S

  An iteration operator (needed to interpret while-loops!) sends h to $h^\sharp\colon S \to A$ and must satisfy laws
  - **Fixpoint:** $f^\sharp = [\mathrm{id}, s\, f^\sharp]\ f$
  - **Uniformity:** $(\mathrm{id} + h)\ f = g\ \ h \ \Rightarrow\ f^\sharp = g^\sharp\ \ h$
    for $f\colon Y \to A + Y$, $g\colon Z \to A + Z$, $h\colon Y \to Z$
- Call triples $(A, s\colon A \to A, (\text{–})^\sharp)$ guarded uniform-iteration algebras

Conjecture: The free object over X is a final coalgebra $\nu\gamma.\, X + \gamma$

(Guarded) Elgot Algebras

- The conjecture becomes true after adding one more axiom, called **Compositionality**
- Guarded uniform-iteration algebras satisfying **Compositionality** are called Elgot algebras[2] and can be defined more generaly, so that

$$\frac{f\colon X \to A + HX}{f^\sharp\colon X \to A}$$

  for arbitrary endofunctor $H\colon \mathbf{C} \to \mathbf{C}$, and an H-algebra $s\colon HA \to A$
- **Compositionality** is no longer admissible if $H \neq \mathrm{Id}$. e.g. $H = \mathrm{Id}^2$

[2] Adámek, Milius, and Velebil, "Elgot Algebras".

Unguarded Infinite Behaviours

Summarized:

	Finite Behaviour	Infinite Behaviour
Guarded (Fine-Grained)	$\mathrm{Id} \times \mathbb{N}$	$\nu\gamma.\,(\text{–} + \gamma)$
Unguarded (Coarse-Grained)	Id	?

? = Free (Unguarded) Uniform-Iteration (or Elgot?) Algebras!

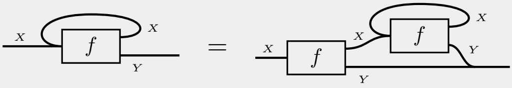
Define KX to be a free structure over X, satisfying

- **Fixpoint:** $f^\sharp = [\mathrm{id}, f^\sharp]\ f$
- **Uniformity:** $(\mathrm{id} + h)\ f = g\ \ h \ \Rightarrow\ f^\sharp = g^\sharp\ \ h$
  for $f\colon Y \to KX + Y$, $g\colon Z \to KX + Z$, $h\colon Y \to Z$

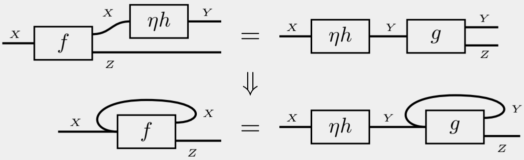
By generalities, K extends to a (strong) monad $\mathbf{K}$ whose iteration operator

$$\frac{f\colon X \to KY + X}{f^\sharp\colon X \to KY}$$

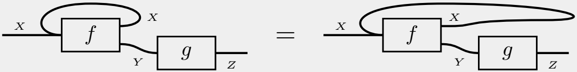
Fixpoint ($f: X \to T(Y + X)$)**:**



Uniformity ($f: X \to T(Z + X)$, $g: Y \to T(Z + Y)$, $h: X \to Y$)**:**



Naturality ($f : X \to T(Y + X)$, $g : Y \to TZ$):



Codiagonal ($f : X \to T(Y + (X + X))$):

Naturality and **Codiagonal** are basically coherence laws

Free Uniform-Iteration v.s. Initial Elgot

- Elgot monads are semantic structures for implementing side-effecting while-loops
- Elgot monads properly generalize monads with $(-)^\dagger$ calculated as least fixpoints, e.g. coalgebraic resumptions

$$\nu\gamma.\, T(X + \Sigma\gamma)$$

  form an Elgot monad of generalized processes over a given Elgot monad $\mathbf{T}$
- But (!) “initial Elgot monad” is an impredicative notion but Elgot algebra is not

Limited Principle of Omniscience

- Delay monad $D = \nu\gamma.\,(\text{–} + \gamma)$ is co-generated by

$$\frac{x : X}{\mathsf{now}\ x : DX} \qquad\qquad \frac{\sigma : DX}{\triangleright\,\sigma : DX}$$

- DX consists of precisely those infinite streams over $X \cup \{\bot\}$, which contain an element of X not more than once
- We call **C** an LPO[3] category if the embedding of $\mathbb{N}$ to $\bar{\mathbb{N}} = D1$ is a coproduct injection

Proposition: **C** is LPO iff $DX \cong X \times \mathbb{N} + 1$

[3] LPO=Limited Principle of Omniscience

LPO and non-LPO Categories

- LPO categories: classical set theories, presheaf toposes, (classical) dcpos, nominal sets, (classical) metric spaces
- Non-LPO categories: some Grothendieck toposes, most realizability toposes, intuitionistic and constructive set theories, **Top**

Why LPO = some choice?

It entails Escardó's very week countable choice: any epic

$$A + B \times (A + A') \xrightarrow{[\mathrm{inl},\mathrm{snd}]} A + A' \cong \mathbb{N}$$

has a section, which is an instance of (weak) countable choice

In any LPO category

- **K** is the maybe monad $(- + 1)$
- **K** is the initial Elgot monad
- **K** is enriched over pointed ω-complete partial orders
- *KX* is free pointed ω-complete partial orders on *X*

Beyond LPO

Monads and Categories for Partiality

- A monad is an equational lifting monad[4] if it is strong, commutative and satisfies the law

$$\begin{array}{ccc} TX & \xrightarrow{T\Delta} & T(X \times X) \\ {\scriptstyle \Delta}\downarrow & & \downarrow{\scriptstyle T(\eta \times \mathrm{id})} \\ TX \times TX & \xrightarrow{\tau} & T(KX \times X) \end{array}$$

- In terms of “do-notation“:

$$x \leftarrow p; y \leftarrow q; \eta\langle x, y\rangle = y \leftarrow q; x \leftarrow p; \eta\langle x, y\rangle$$
$$x \leftarrow p; \eta\langle x, \eta x\rangle = x \leftarrow p; \eta\langle x, p\rangle$$

- Then the Kleisli category is a restriction category[5], with

$$\frac{f : X \to TY}{\mathrm{dom}\, f : X \to TX}$$

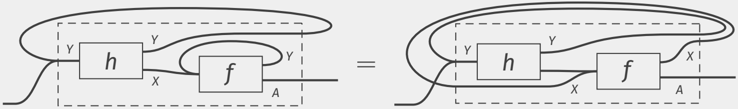
satisfying axioms of domains of definiteness

[4] Bucalo, Führmann, and Simpson, “An equational notion of lifting monad”.
[5] Cockett and Lack, “Restriction categories I: categories of partial maps”.

Theorem: If every KX exists and stable then

1. **K** is an equational lifting monad
2. Kleisli Category of **K** is a restriction category
   $\Rightarrow$ Kleisli Category of **K** is order enriched
3. Kleisli composition and strength moreover respect the order and the bottom element $\perp$ (divergence)
4. $f^\sharp$ is an internal order-limit of finite approximations ($\approx$ Kleene fixpoint theorem)

Compositionality



holds for **K** (non-trivially from Kleene's fixpoint property)

Hence, initial Uniform-iteration algebra = initial unguarded Elgot algebra

Quotienting Delay Monad

- Following previous work[6], consider weak bisimilarity over DX:

$$\frac{\sigma \approx \text{now } x}{\triangleright\, \sigma \approx \text{now } x} \qquad \frac{\text{now } x \approx \sigma}{\text{now } x \approx \triangleright\, \sigma} \qquad \frac{\triangleright\, \sigma \approx \triangleright\, \sigma'}{\sigma \approx \sigma'}$$

- We generically model it with the coequalizer:

$$D(X \times \mathbb{N}) \underset{D\mathsf{fst}}{\overset{\iota^\star}{\rightrightarrows}} DX \xrightarrow{\rho_X} \tilde{D}X \qquad (*)$$

$\Rightarrow \rho_X \triangleright = \rho_X$, but this seems to be weaker than $(*)$

Theorem: The following are equivalent:

1. $(*)$ is preserved by D
2. $\tilde{D}$ extends to a strong monad and ρ to a strong monad morphism
3. $\tilde{D}X \cong KX$ and ρ_X is iteration preserving

[6] Chapman, Uustalu, Veltri: Quotienting the delay monad by weak bisimilarity

Countable Choice

- A stronger property than preservation by D is preservation by $(-)^{\mathbb{N}}$ – this is a version of the axiom of countable choice
- If additionally $\mathbf{C}$ is an exact category (e.g. a pretopos) then $\tilde{D}$ is an Elgot monad

Open Questions: Is it initial? Is it order-enriched?

Further Work

- Implementation in Agda (for which notion of category?)
- Concrete natural examples of discrepancy of **K** and $\tilde{\mathbf{D}}$
- Concrete natural examples of **K** not being (initial) Elgot monad
- Relation between the initial Elgot monad and "free pointed ω-cpo monads"
- Other recursion call trees (e.g. $\nu\gamma.\,\text{–} + \gamma \times \gamma$) and other semantics (e.g. hybrid[7])

[7] Diezel, Goncharov: Towards Constructive Hybrid Semantics