Interactive Realizers
A new Approach to Program Extraction from Non-Constructive Proofs

Ugo de'Liguoro

Dipartimento di Informatica, Università di Torino

joint work with **Stefano Berardi**

Genova, October 21th 2010

A motivating example

Let f, g and h be total recursive functions, and consider:

$$\begin{cases} \mathsf{f}(x) \leq \mathsf{f}(\mathsf{g}(x)) \\ \mathsf{f}(x) \leq \mathsf{f}(\mathsf{h}(x)) \end{cases}$$

It is classically provable that the system always has a solution in $\mathbb{N}$, namely any m such that:

$$\mathsf{f}(m) = \min \mathrm{rng}(\mathsf{f}).$$

Observe that:

- the number $\min \mathrm{rng}(\mathrm{f})$ is not computable for all total recursive f: take e.g. $\mathrm{f}_x(y) = \mathrm{r}(x, y)$ where

$$\mathrm{r}(x, y) = \text{if } \varphi_x(x) \text{ converges within } y \text{ steps then 0 else 1}$$

  then to compute $\min \mathrm{rng}(\mathrm{f}_x)$ is the same as to decide the halt.
- however we can effectively find a solution of the original problem by minimalization:

$$\min x.\mathrm{f}(x) \leq \mathrm{f}(\mathrm{g}(x)) \wedge \mathrm{f}(x) \leq \mathrm{f}(\mathrm{h}(x))$$

  thought this is a brute force algorithm

A better solution:

$m :=$ an arbitrary natural number
while $\mathrm{f}(m) > \mathrm{f}(\mathrm{g}(m)) \vee \mathrm{f}(m) > \mathrm{f}(\mathrm{h}(m))$ do
    if $\mathrm{f}(m) > \mathrm{f}(\mathrm{g}(m))$ then $m := \mathrm{g}(m)$
    else // i.e. when $\mathrm{f}(m) > \mathrm{f}(\mathrm{h}(m))$
        $m := \mathrm{h}(m)$
return m

The algorithm terminates: otherwise we would be able to construct the infinite descending chain of natural numbers

$$\mathrm{f}(m_0) > \mathrm{f}(m_1) > \cdots > \mathrm{f}(m_i) > \cdots$$

with $m_i =$ the value of m after i executions of the while body.

The theories **PRA** and **PRA** + $\mathbf{EM}_1$

- **PRA** is the quantifier free theory of primitive recursive arithmetic (see [Troelstra-Van Dalen], vol. 1)
- call $\mathcal{L}_0$ the first order predicate language with equality and without quantifiers of **PRA**
- call $\mathcal{I}_0$ the standard interpretation of $\mathcal{L}_0$ s.t. $\mathcal{I}_0 \models$ **PRA**

If $t, A \in \mathcal{L}_0$ are a term and a formula with free variables $\{x_1, \ldots, x_k\}$ then

$$[\![t]\!]^{\mathcal{I}_0} : \mathbb{N}^k \to \mathbb{N} \quad \text{and} \quad [\![A]\!]^{\mathcal{I}_0} : \mathbb{N}^k \to \mathbb{B}$$

are a primitive recursive function and predicate respectively.

With A in the language of **PRA** consider:

$$(\mathbf{EM}_1) \qquad \forall \vec{x}.\, \exists y\, A(\vec{x}, y) \vee \forall y\, \neg A(\vec{x}, y)$$

which is classically equivalent to to the skolemized version

$$\forall \vec{x}, y.\, A(\vec{x}, \varphi(\vec{x})) \vee \neg A(\vec{x}, y),$$

and to

$$\forall \vec{x}, y.\, A(\vec{x}, y) \to A(\vec{x}, \varphi(\vec{x})).$$

Let $\mathcal{L}_1$ be obtained from $\mathcal{L}_0$ by adding the symbols:

$$\chi_{\mathsf{P}} \quad \text{(a predicate)} \quad \varphi_{\mathsf{P}} \quad \text{(a function) of arity } k$$

for each predicate symbol $\mathsf{P} \in \mathcal{L}_0$ of arity $k+1$

Then **PRA** + $\mathbf{EM}_1$ is obtained from **PRA** by adding the axioms:

$$(\chi) \quad P(\vec{x}, y) \to \chi_P(\vec{x})$$
$$(\varphi) \quad \chi_P(\vec{x}) \to P(\vec{x}, \varphi_P(\vec{x}))$$

for each (definition in **PRA** of) primitive recursive predicate P.

Extracting Programs from **PRA** + $\mathbf{EM}_1$ Proofs

- A *program specification* is some formula $A(\vec{x}, y) \in \mathcal{L}_0$
- an *interactive program* is a term $t(\vec{x}) \in \mathcal{L}_1$
- a program $t(\vec{x})$ *provably satisfies the specification* $A(\vec{x}, y)$ if

$$\mathbf{PRA} + \mathbf{EM}_1 \vdash A(\vec{x}, t(\vec{x}))$$

Goal (naively): find a total recursive function $p(\vec{x})$ such that in some model $\mathcal{I} \models \mathbf{PRA} + \mathbf{EM}_1$ it is the case that

$$\forall \vec{m} \in \mathbb{N} \quad p(\vec{m}) = [\![t(\vec{m})]\!]^{\mathcal{I}}$$

Problem

There exist terms t and formulas A of $\mathcal{L}_1$ whose interpretations $[\![t]\!]^{\mathcal{I}}$ and $[\![A]\!]^{\mathcal{I}}$ aren't computable in any model $\mathcal{I}$ of **PRA** + $\mathbf{EM}_1$

Goal: find a total recursive function $p(\vec{x})$ such that:

$$\forall \vec{m} \in \mathbb{N}\ \exists \mathcal{I} \supseteq \mathcal{I}_0.\ \mathcal{I} \models \forall \vec{x}.A(\vec{x}, t(\vec{x})) \quad \& \quad p(\vec{m}) = [\![t(\vec{m})]\!]^{\mathcal{I}}$$

where observe the exchange of quantifiers w.r.t. the previous formulation, and the fact that $\mathcal{I}$ is a model of a single theorem, not of the whole theory **PRA** + $\mathbf{EM}_1$.

A constructive interpretation of **PRA** + $\mathbf{EM}_1$

Idea:

- we define a notion of (finite) approximation of a **PRA** + $\mathbf{EM}_1$ model such that the interpretation map is continuous
- we interpret non constructive proofs of **PRA** + $\mathbf{EM}_1$ as strategies sending any possible value of the parameters into some finite approximation s_0 of a **PRA** + $\mathbf{EM}_1$ model
- for any possible values of the parameters the concluding formula of the proof is true in any interpretation $\mathcal{I}$ extending the approximation s_0 associated to the parameters

Facts and States of Knowledge

- *fact*: any atomic closed formula $\mathrm{P}(\vec{m}, n) \in \mathcal{L}_0$ such that

$$[\![\mathrm{P}(\vec{m}, n)]\!]^{\mathcal{I}_0} = \text{true}$$

- *consistency*: the relation among atomic closed formulas of $\mathcal{L}_0$:

$$\mathrm{P}(\vec{m}, n) \sim \mathrm{Q}(\vec{m}', n') \Leftrightarrow [\mathrm{P} \equiv \mathrm{Q} \ \ \& \ \ \vec{m} = \vec{m}' \Rightarrow n = n']$$

  where $\equiv$ is syntactical identity

- *state*: a finite consistent set of facts

$$s = \{\mathrm{P}_1(\vec{m}_1, n_1), \ldots, \mathrm{P}_k(\vec{m}_k, n_k)\}$$

  we name $\mathbb{S}$ the set of states

For any (possibly infinite) consistent set of facts S define:

$$[\![\chi_{\mathsf{P}}]\!](\vec{m}, S) = \text{true} \Leftrightarrow \exists n \in \mathbb{N}.\ \mathsf{P}(\vec{m}, n) \in S$$

and

$$[\![\varphi_{\mathsf{P}}]\!](\vec{m}, S) = \begin{cases} n & \text{if } \mathsf{P}(\vec{m}, n) \in S \text{ for some } n \\ 0 & \text{otherwise.} \end{cases}$$

Prop. Any maximal consistent set of facts S determines an interpretation $\mathcal{I}_S \supseteq \mathcal{I}_0$ of $\mathcal{L}_1$ by putting:

$$[\![\chi_{\mathsf{P}}(\vec{m})]\!]^{\mathcal{I}_S} = [\![\chi_{\mathsf{P}}]\!](\vec{m}, S) \quad \text{and} \quad [\![\varphi_{\mathsf{P}}(\vec{m})]\!]^{\mathcal{I}_S} = [\![\varphi_{\mathsf{P}}]\!](\vec{m}, S)$$

which is a model of **PRA** + $\mathbf{EM}_1$. Viceversa any model $\mathcal{I} \supseteq \mathcal{I}_0$ determines the maximal consistent set of facts:

$$S_{\mathcal{I}} = \{\mathsf{P}(\vec{m}, n) \mid [\![\mathsf{P}(\vec{m}, n)]\!]^{\mathcal{I}} = \text{true} \wedge [\![\varphi_{\mathsf{P}}(\vec{m})]\!]^{\mathcal{I}} = n\}$$

The structure

$$(\mathbb{S}, \sqsubseteq, \uparrow, \sqcup, \bot)$$

is an effectively presented partial order with infimum and compatible finite sups, that is:

1. $\mathbb{S}$ is a decidable set
2. $s \sqsubseteq s' \Leftrightarrow s \subseteq s'$ is a computable partial order
3. $s \uparrow s' \Leftrightarrow \exists s''.\ s \sqsubseteq s'' \sqsupseteq s'$ is decidable
4. $s \sqcup s' = s \cup s'$ if $s \uparrow s'$, undefined otherwise, is computable
5. $\bot = \emptyset$

The proof of (1), (3) and (4) follows since to be a "fact" is decidable, and because of the syntactical nature of the relation $\sim$ among facts, which is decidable.

- A maximal consistent set of facts S can be viewed as the union of a (suitable) ω-chain of states:

$$s_0 \sqsubseteq s_1 \sqsubseteq \cdots \sqsubseteq s_i \sqsubseteq \cdots$$

  and this can be done in many ways
- the interpretation $[\![E]\!]^{\mathcal{I}_S}$ of any closed $E \equiv t, A$ only depends on a finite subset of S, namely on a state s_i for suitably large index i
- both $[\![\chi_P]\!](\vec{m}, s)$ and $[\![\varphi_P]\!](\vec{m}, s)$ are computable for finite s (a state)

The Approximated Interpretation of $\mathcal{L}_1$

We interpret (closed) terms into $\mathbb{N}^{\mathbb{S}}$ (i.e. objects of type $\mathbb{S} \to \mathbb{N}$), and formulas into $\mathbb{B}^{\mathbb{S}}$ (of type $\mathbb{S} \to \mathbb{B}$). In general for $\xi : \mathrm{Var} \to \mathbb{N}^{\mathbb{S}}$:

$$
\begin{aligned}
[\![x]\!]^{\mathbb{S}}_{\xi} &= \xi(x) \\
[\![n]\!]^{\mathbb{S}}_{\xi} &= \lambda s.\ n \\
[\![f(t_1,\ldots,t_n)]\!]^{\mathbb{S}}_{\xi} &= \lambda s.\ f([\![t_1]\!]^{\mathbb{S}}_{\xi}(s),\ldots,[\![t_n]\!]^{\mathbb{S}}_{\xi}(s)) \\
[\![\varphi_P(t_1,\ldots,t_n)]\!]^{\mathbb{S}}_{\xi} &= \lambda s.\ [\![\varphi_P]\!]([\![t_1]\!]^{\mathbb{S}}_{\xi}(s),\ldots,[\![t_n]\!]^{\mathbb{S}}_{\xi}(s),\ s) \\
[\![P(t_1,\ldots,t_n)]\!]^{\mathbb{S}}_{\xi} &= \lambda s.\ P([\![t_1]\!]^{\mathbb{S}}_{\xi}(s),\ldots,[\![t_n]\!]^{\mathbb{S}}_{\xi}(s)) \\
[\![\chi_P(t_1,\ldots,t_n)]\!]^{\mathbb{S}}_{\xi} &= \lambda s.\ [\![\chi_P]\!]([\![t_1]\!]^{\mathbb{S}}_{\xi}(s),\ldots,[\![t_n]\!]^{\mathbb{S}}_{\xi}(s),\ s) \\
[\![(A \wedge B)]\!]^{\mathbb{S}}_{\xi} &= \lambda s.\ [\![A]\!]^{\mathbb{S}}_{\xi}(s) \wedge [\![B]\!]^{\mathbb{S}}_{\xi}(s) \\
&\ldots
\end{aligned}
$$

A Submonad of the State Monad

The following is a Kleisli triple:

$$\begin{aligned} \mathcal{S}X &= X^{\mathbb{S}} \\ \eta_X(x) &= \lambda s.\, x \quad (\text{written } \lambda\_.\, x) \\ f^*(\alpha) &= \lambda s.\, f(\alpha(s), s) \end{aligned}$$

where $f : X \to \mathcal{S}Y$, $\alpha \in X^{\mathbb{S}}$ and $f^* : \mathcal{S}X \to \mathcal{S}Y$.

$\mathcal{S}$: **Set** $\to$ **Set** is a functor whose arrow part is:

$$\mathcal{S}f = (\eta_Y \circ f) = f \circ \_$$

The monad multiplication is $\mu_X = \mathtt{Id}^*_{\mathcal{S}X}$ that is:

$$\mu_X(\delta, s) = \delta(s, s), \quad \text{for any } \delta \in \mathcal{S}^2X = (X^{\mathbb{S}})^{\mathbb{S}} \text{ and } s \in \mathbb{S}$$

$(\mathcal{S}, \eta, \mu, t)$ is a strong monad with (unique) tensorial strength:

$$t^{\mathcal{S}}_{X,Y} : X \times \mathcal{S}Y \to \mathcal{S}(X \times Y)$$

defined as

$$t^{\mathcal{S}}_{X,Y}(x, \alpha) = \lambda s.\ (x, \alpha(s))$$

Taking as in [Moggi 91]

$$\psi_{X,Y} := (t_{X,Y} \circ c_{\mathcal{S}Y,X})^* \circ t_{\mathcal{S}Y,X} \circ c_{\mathcal{S}X,\mathcal{S}Y}$$

where $c_{X,Y} : X \times Y \to Y \times X$ is the exchange iso, we get

$$\psi_{X,Y}(\alpha, \beta) = \langle \alpha, \beta \rangle = \lambda s : \mathbb{S}.\ (\alpha(s), \beta(s)),$$

which has inverse $\gamma \mapsto (\pi_1 \circ \gamma, \pi_2 \circ \gamma)$ determining the iso $\mathcal{S}X \times \mathcal{S}Y \simeq \mathcal{S}(X \times Y)$

The Category of Global Functions

Let $\mathbf{Set}_{\mathcal{S}}$ be the Kleisli category of $\mathcal{S}$; define the isomorphic category $\mathbf{Set}^*_{\mathcal{S}}$ by $|\mathbf{Set}^*_{\mathcal{S}}| = |\mathbf{Set}_{\mathcal{S}}| = |\mathbf{Set}|$ and

$$\mathbf{Set}^*_{\mathcal{S}}(X, Y) = \{f^* \mid f \in \mathbf{Set}_{\mathcal{S}}(X, Y)\} = \{f^* \mid f : X \to \mathcal{S}Y \in \mathbf{Set}\}$$

Def. A function $g : \mathcal{S}X \to \mathcal{S}Y$ is *global* iff

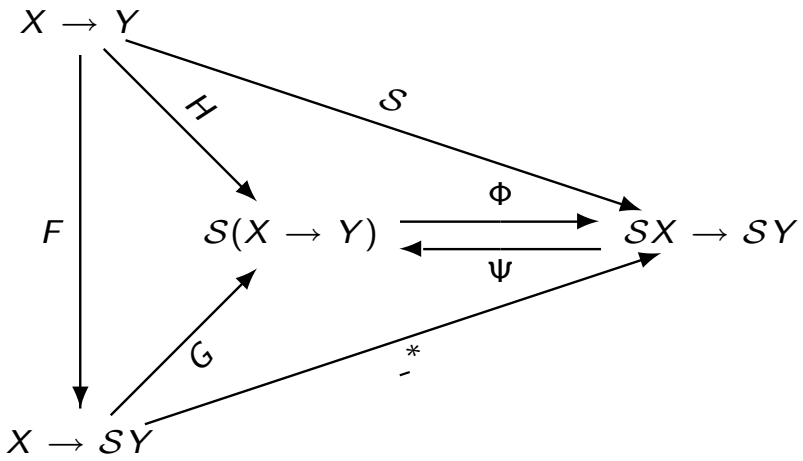
$$\forall \alpha \in \mathcal{S}X \; \forall s \in \mathbb{S}.\; g(\alpha, s) = g(\lambda\_.\, \alpha(s), s)$$

Global functions are a subset of $\mathcal{S}X \to \mathcal{S}Y$: let $s, s' \in \mathbb{S}$ be distinct, $h : \mathbb{S} \to \mathbb{S}$ s.t. $h(s) = s'$ and $\alpha \in \mathcal{S}$ s.t. $\alpha(s) \neq \alpha(s')$ then:

$$(\lambda\beta.\beta \circ h)(\alpha, s) = \alpha(s') \neq \alpha(s) = (\lambda\beta.\beta \circ h)(\lambda\_.\alpha(s), s)$$

Lemma Global functions in $\mathcal{S}X \to \mathcal{S}Y$ are exactly morphisms in $\mathbf{Set}^*_{\mathcal{S}}(X, Y)$

The following diagram commutes, and $\Psi \circ \Phi$ is a retraction:



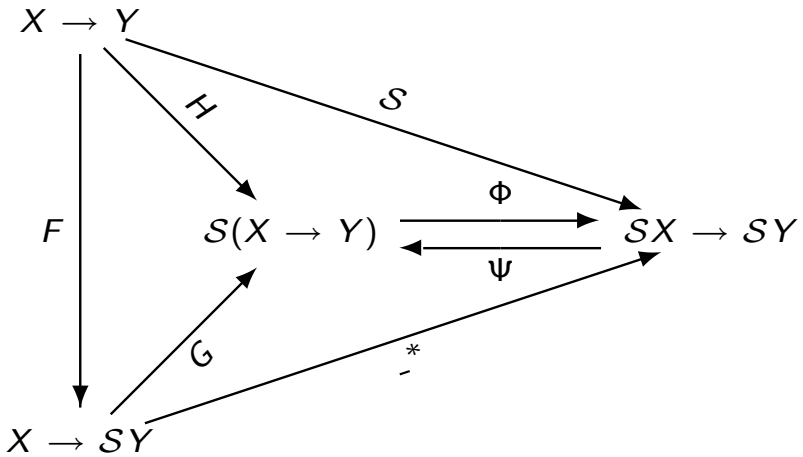
$$\Phi : \mathcal{S}(X \to Y) \to (\mathcal{S}X \to \mathcal{S}Y) \qquad \Phi(f)(\alpha, s) := f(s)(\alpha(s))$$

$$\Psi : (\mathcal{S}X \to \mathcal{S}Y) \to \mathcal{S}(X \to Y) \qquad \Psi(g)(s, x) := g(\lambda\_.x, s)$$

$$F : (X \to Y) \to (X \to \mathcal{S}Y) \quad \text{where} \quad F(f) := \lambda x \in X\ \lambda\_ \in \mathbb{S}.f(x)$$

$$G : (X \to \mathcal{S}Y) \to \mathcal{S}(X \to Y) \quad \text{where} \quad G(g) := \lambda s \in \mathbb{S}\ \lambda x \in X.g(x, s)$$

$$H : (X \to Y) \to \mathcal{S}(X \to Y) \quad \text{where} \quad H(f) := \lambda\_ \in \mathbb{S}.f$$



The image of Φ is exactly the set of global functions: if $f : X \to \mathcal{S}Y$ then for all $\alpha \in \mathcal{S}X$ and $s \in \mathbb{S}$:

$$f^*(\alpha, s) = f(\alpha(s), s) = f((\lambda\_.\alpha(s))(s), s) = f^*(\lambda\_.\alpha(s), s),$$

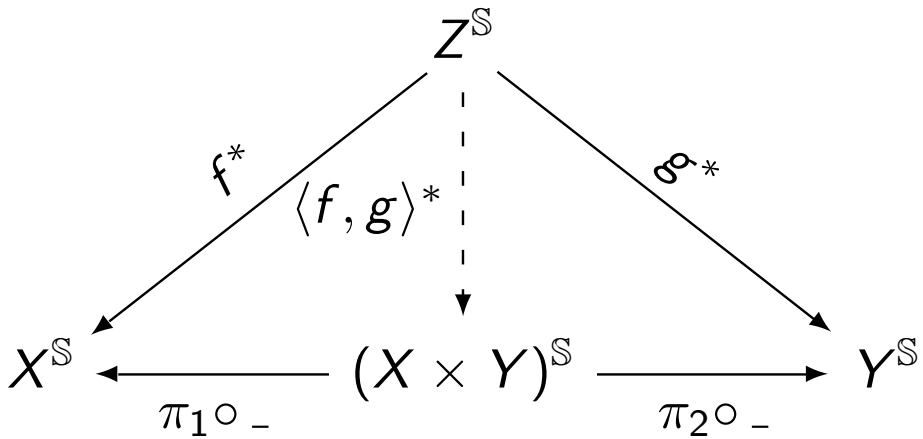
hence f^* is global. Viceversa if g is global then
$g = \Phi(h) = \lambda\alpha \in \mathcal{S}X\ s \in \mathbb{S}.\ h(s)(\alpha(s))$, for some $h : \mathbb{S} \to (X \to Y)$.
Set $f(x, s) = h(s, x)$, so that $f : X \to \mathcal{S}Y$; then:

$$g = \lambda\alpha \in \mathcal{S}X\ s \in \mathbb{S}.\ f(\alpha(s), s) = f^*.$$

$\mathbf{Set}^*_{\mathcal{S}}$ is cartesian: given $f : Z \to \mathcal{S}X$ and $g : Z \to \mathcal{S}Y$ the arrow

$$\langle f, g \rangle^* : \mathcal{S}Z \to \mathcal{S}(X \times Y)$$

is the unique one such that the following commutes:



where $\pi_i \circ \_ = \mathcal{S}\pi_i$ $(i = 1, 2)$. Then we get

$$\langle f, g \rangle^* = \langle f^*, g^* \rangle$$

up to the iso $\mathcal{S}X \times \mathcal{S}Y \simeq \mathcal{S}(X \times Y)$.

Def. $g : \mathcal{S}X_1 \times \cdots \times \mathcal{S}X_k \to \mathcal{S}Y$ is *k-global* if for all $\alpha_1, \ldots, \alpha_k, s$:

$$g(\alpha_1, \ldots, \alpha_k, s) = g(\lambda\_.\alpha_1(s), \ldots, (\lambda\_.\alpha_k(s), s)$$

Any k-global g uniquely factors through

$$\psi_{X_1,\ldots,X_k} : \mathcal{S}X_1 \times \cdots \times \mathcal{S}X_k \to \mathcal{S}(X_1 \times \cdots \times X_k)$$

by

$$\mathcal{S}X_1 \times \cdots \times \mathcal{S}X_k \xrightarrow{\psi_{X_1,\ldots,X_k}} \mathcal{S}(X_1 \times \cdots \times X_k) \xrightarrow{\hat{g}} \mathcal{S}Y$$

where $\hat{g}(\gamma) = g(\pi_1 \circ \gamma, \ldots, \pi_k \circ \gamma)$.

It follows that g is k-global if and only if $\hat{g} = g \circ \psi^{-1}$ is global.

Individuals

Def. Let $\sigma : \mathbb{N} \to \mathbb{S}$ be an ω-chain over $\mathbb{S}$, that is

$$\sigma(0) \sqsubseteq \sigma(1) \sqsubseteq \cdots \sqsubseteq \sigma(i) \sqsubseteq \cdots$$

and $\alpha \in \mathcal{S}X = X^{\mathbb{S}}$; then $\alpha \circ \sigma : \mathbb{N} \to X$ is *convergent* and it has a *limit point* $\lim(\alpha \circ \sigma) = x$ if

$$\exists i \; \forall j. \; (\alpha \circ \sigma)(i) = (\alpha \circ \sigma)(i + j) = x.$$

The mapping α is *strongly convergent* if for all ω-chain σ, $\alpha \circ \sigma$ is convergent.

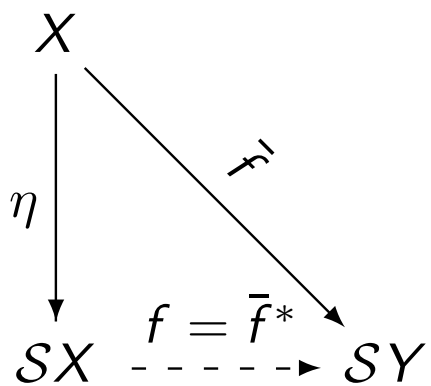
We call *individual* of X a strongly convergent $\alpha \in \mathcal{S}X$, and denote by $I(X)$ the set of individuals of X.

Density Theorem

The behaviour of a global function is completely determined by its values on constant individuals. Let $f, g : \mathcal{S}X \to \mathcal{S}Y$ be global:

1. if $f(\lambda\_.x) = g(\lambda\_.x)$ for all $x \in X$ then $f = g$
2. if $f(\lambda\_.x) \in I(Y)$ for all $x \in X$ then $f(\alpha) \in I(Y)$ for all $\alpha \in I(X)$

Part (1) follows by the fact that if f, g are global then $f = \bar{f}^*$ for some $\bar{f} : X \to \mathcal{S}Y$ (and similarly for g) and $\bar{f}^*$ is the unique arrow s.t. the following commutes:



Now recall that $\eta(x) = \lambda\_.x$

The Category of Strongly Global Functions

Def. A global $f : \mathcal{S}X \to \mathcal{S}Y$ is *strongly global* if

$$\forall x \in X.\ \ f(\lambda\_.x) \in I(Y)$$

Lemma If $f : \mathcal{S}X \to \mathcal{S}Y$ and $g : \mathcal{S}Y \to \mathcal{S}Z$ are strongly global then $g \circ f$ is strongly global. Moreover $\mathtt{Id}_{\mathcal{S}X}$ is strongly global.

Proof. $f = \bar{f}^*$ and $g = \bar{g}^*$ therefore their composition is global:

$$\bar{g}^* \circ \bar{f}^* = (\bar{g}^* \circ \bar{f})^*$$

by Kleisli composition and because global functions are exactly those of the form h^* for some h
$\beta = f(\lambda\_.x) \in I(Y)$, hence $g(\beta) \in I(Z)$ by part (2) of Density Thm, and we conclude $(g \circ f)(\lambda\_.x) \in I(Z)$

Def. A global $f : \mathcal{S}X \to \mathcal{S}Y$ is *strongly global* if

$$\forall x \in X.\ \ f(\lambda\_.x) \in I(Y)$$

By the lemma it exists a *category of strongly global functions* $\mathcal{G}$:

- $|\mathcal{G}| = |\mathbf{Set}|$ (morally the object X is $I(X)$)
- $\mathcal{G}(X, Y) = \{f \in \mathbf{Set}^*_{\mathcal{S}} \mid f \text{ is strongly global}\}$

which is a subcategory of $\mathbf{Set}^*_{\mathcal{S}}$ (hence of $\mathbf{Set}_{\mathcal{S}}$). Moreover $\mathcal{G}$ is cartesian and product and projections coincide with those in $\mathbf{Set}^*_{\mathcal{S}}$:

$$\pi_i \circ (\lambda\_.(x_1, x_2)) = \lambda\_.x_i$$

and if f, g are strongly global $\alpha = f(\lambda\_.z) \in I(X)$, $\beta = g(\lambda\_.z) \in I(X)$

$$\langle f, g\rangle(\lambda\_.z) = \langle \alpha, \beta\rangle \in I(X \times Y)$$

Approximated Interpretation Revised

For $t, A \in \mathcal{L}_1$ the interpretations $[\![t]\!]^{\mathbb{S}}$ and $[\![A]\!]^{\mathbb{S}}$ are arrows of $\mathcal{G}$:

$$I(\mathbb{N}) \times \cdots \times I(\mathbb{N}) \xrightarrow{[\![t]\!]^{\mathbb{S}}} I(\mathbb{N})$$

$$I(\mathbb{N}) \times \cdots \times I(\mathbb{N}) \xrightarrow{[\![A]\!]^{\mathbb{S}}} I(\mathbb{B})$$

e.g. if P is binary

$$[\![\varphi_{\mathsf{P}}]\!]^{\mathbb{S}} = [\![\varphi_{\mathsf{P}}]\!]^{*} \quad \text{where} \quad [\![\varphi_{\mathsf{P}}]\!] : \mathbb{N} \to \mathbb{N}^{\mathbb{S}}$$

and $[\![\varphi_{\mathsf{P}}]\!](n) \in I(\mathbb{N})$ for all n

Prop. If $t, A \in \mathcal{L}_0$ then both $[\![t]\!]^{\mathbb{S}}$ and $[\![A]\!]^{\mathbb{S}}$ are constant. In particular if **PRA** + $\mathbf{EM}_1 \vdash A$ then $[\![A]\!]^{\mathbb{S}}$ is constantly true.

Interactive Realizers

Def. An *interactive realizer* (shortly realizer) is a map $r \in \mathcal{S}(\mathbb{S}) = \mathbb{S}^{\mathbb{S}}$, such that:

1. $r \in I(\mathbb{S})$ i.e. r is strongly convergent
2. $r(s) \uparrow s$ for all $s \in \mathbb{S}$
3. $r(s) \cap s = \bot$ for all $s \in \mathbb{S}$

We call $\mathbb{R}$ the set of realizers.

A state $s \in \mathbb{S}$ is a *prefix point* of $r \in \mathbb{R}$ if $r(s) \sqsubseteq s$; we set

$$\mathit{Prefix}(r) = \{s \in \mathbb{S} \mid r(s) \sqsubseteq s\}$$

Observe that if $r \in \mathbb{R}$ then by (3):

$$r(s) \sqsubseteq s \Leftrightarrow r(s) = \bot$$

so that $\lim(r \circ \sigma) = \bot$ for any ω-chain $\sigma : \mathbb{N} \to \mathbb{S}$.

Given $s \in \mathbb{S}$ define the ω-chain $\sigma : \mathbb{N} \to \mathbb{S}$ by:

$$\begin{aligned} \sigma(0) &= s \\ \sigma(i+1) &= \sigma(i) \sqcup r(\sigma(i)) \end{aligned}$$

where $\sigma(i) \sqcup r(\sigma(i))$ exists since $r(\sigma(i)) \uparrow \sigma(i)$.

Since $r \in I(\mathbb{S})$ there exists $i_0 \in \mathbb{N}$ s.t. $r(\sigma(j)) = \perp$ for all $j \geq i_0$.

Choosing $s' = \sigma(i_0)$ we have:

$$s = \sigma(0) \sqsubseteq \sigma(i_0) = s' \in \mathit{Prefix}(r)$$

Prop. If $r \in \mathbb{R}$ then $\mathit{Prefix}(r)$ is cofinal in $\mathbb{S}$

Merging Realizers and a new Monad

A *merge* is a binary operation $\bullet : \mathbb{S} \times \mathbb{S} \to \mathbb{S}$ s.t.

1. $(\mathbb{S}, \bullet, \bot)$ is a monoid
2. if $s_1 \bullet s_2 = \bot$ then $s_1 = \bot = s_2$
3. $s_1 \bullet s_2 \subseteq s_1 \cup s_2$

Examples:

$$s_1 \bullet_0 s_2 = \begin{cases} s_1 & \text{if } s_1 \neq \bot, \\ s_2 & \text{otherwise.} \end{cases}$$

Let $\bar{s} = \{\mathrm{P}(\vec{m}, n) \mid \exists n'.\mathrm{P}(\vec{m}, n') \in s\}$:

$$s_1 \bullet_1 s_2 := s_1 \cup (s_2 \setminus \bar{s}_1)$$

For $X \subseteq \bigcup \mathbb{S}$ define $\widehat{X} := \{\mathrm{P}(\vec{m}, n) \in X \mid \forall \mathrm{P}(\vec{m}, n') \in X.n \leq n'\}$:

$$s_1 \bullet_2 s_2 := \widehat{s_1 \cup s_2}.$$

Define

$$\bullet^{\mathcal{S}} = \mathcal{S}(\bullet) \circ \psi_{\mathbb{S},\mathbb{S}} : \mathcal{S}(\mathbb{S}) \times \mathcal{S}(\mathbb{S}) \to \mathcal{S}(\mathbb{S})$$

This is a 2-global function by construction, and the following is a monoid

$$(\mathcal{S}(\mathbb{S}), \bullet^{\mathcal{S}}, \lambda\_.\, \bot)$$

Note that $(\lambda\_.s) \bullet^{\mathcal{S}} (\lambda\_.s') = \lambda\_.\, (s \bullet s')$ so $\bullet^{\mathcal{S}}$ is strongly global. We conclude that $(\mathbb{S}, \bullet^{\mathcal{S}}, \lambda\_.\, \bot)$ is a monoid in $\mathcal{G}$.

Lemma If $r, r' \in \mathbb{R}$ then

$$r \bullet^{\mathcal{S}} r' \in \mathbb{R} \quad \text{and} \quad \mathit{Prefix}(r \bullet^{\mathcal{S}} r') = \mathit{Prefix}(r) \cap \mathit{Prefix}(r')$$

(Here we use the fact that $s \bullet s' = \bot$ implies that $s = \bot = s'$)

Therefore $(\mathbb{R}, \bullet^{\mathcal{S}}, \lambda\_.\, \bot)$ is a submonoid of $(\mathcal{S}(\mathbb{S}), \bullet^{\mathcal{S}}, \lambda\_.\, \bot)$

Monads of Realizers

Let $M = (\mathbb{S}, \bullet^{\mathcal{S}}, \lambda\_.\, \bot)$ (recall that $\mathbb{S}$ is $I(\mathbb{S}) \subseteq \mathbb{S}^{\mathbb{S}}$ in $\mathcal{G}$ and we are interested into $\mathbb{R} \subseteq I(\mathbb{S})$) be the monoid determined by the merge $\bullet$, and define the functor $\mathcal{R} : \mathcal{G} \to \mathcal{G}$:

$$\mathcal{R}(X) = M \times X \qquad \mathcal{R}(g)(r, \alpha) = (r, g(\alpha))$$

where recall that $g \in \mathcal{G}(X, Y)$ is a strongly global function $g : I(X) \to I(Y)$, so $\alpha \in I(X) \subseteq X^{\mathbb{S}}$ and $g(\alpha) \in I(Y)$.

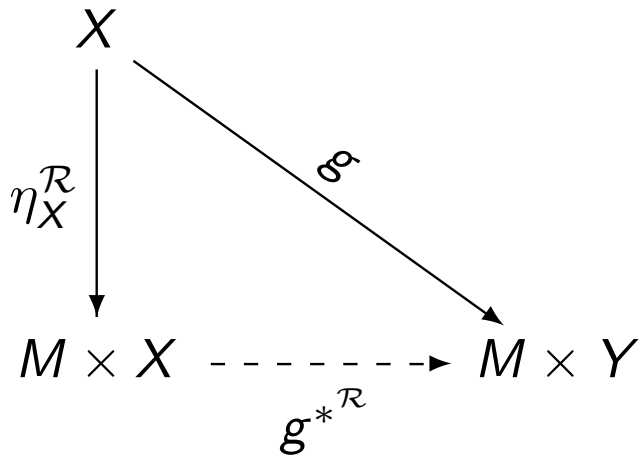
$\mathcal{R}$ is a monad over $\mathcal{G}$, that we say a *realizer monad*, with unit

$$\begin{array}{rcl} \eta^{\mathcal{R}}_X : X & \to & \mathcal{R}(X) = M \times X \\ \alpha & \mapsto & (\lambda\_.\bot\alpha) \end{array}$$

and multiplication

$$\begin{array}{rcl} \mu^{\mathcal{R}}_X : \mathcal{R}^2(X) = M \times M \times X & \to & \mathcal{R}(X) = X \times M \\ (r, r', \alpha) & \mapsto & (r \bullet^{\mathcal{S}} r', \alpha) \end{array}$$

We recover the Kleisli $(-)^{*^{\mathcal{R}}}$ extension of $\mathcal{R}$



where supposing $g(\alpha) = (r', \beta)$ we have:

$$g^{*^{\mathcal{R}}}(r, \alpha) = (\mu^{\mathcal{R}}_Y \circ \mathcal{R}(g))(r, \alpha) = \mu^{\mathcal{R}}_Y(r, g(\alpha)) = (r \bullet^{\mathcal{S}} r', \beta)$$

Interactive Forcing

Let X be any set, and $Y = \{Y_s \mid s \in \mathbb{S}\}$ with $Y_s \subseteq X$ for all s; let $r \in \mathbb{R}$ and $\alpha \in I(X)$.

Def. *r interactively forces α into Y* is defined by

$$r \Vdash \alpha : Y \quad \Leftrightarrow \quad \forall s \in \mathbb{S}\, [s \in \mathit{Prefix}(r) \Rightarrow \alpha(s) \in Y_s]$$

$\mathit{ext}(A) = \{\mathit{ext}(A)_s \mid s \in \mathbb{S}\}$ where:

$$\mathit{ext}(A)_s = \{\vec{m} \mid \mathrm{FV}(A) \subseteq \vec{x} \ \&\ |\vec{x}| = |\vec{m}| \ \&\ [\![A]\!]^{\mathcal{S}}_{\overrightarrow{[\lambda\_.m/\vec{x}]}}(s) = \mathsf{true}\}.$$

For $\vec{\alpha} = \alpha_1, \ldots, \alpha_k$ we eventually set:

$$r \Vdash \vec{\alpha} : A(\vec{x}) \quad \Leftrightarrow \quad r \Vdash \langle \alpha_1, \ldots, \alpha_k \rangle : \mathit{ext}(A)$$

The Interactive Realizability Theorem

Thm. If $\mathbf{PRA} + \mathbf{EM}_1 \vdash A(\vec{x})$ then there exists a strongly global $R : I(\mathbb{N}) \times \cdots \times I(\mathbb{N}) \to \mathbb{R}$ such that:

$$\forall \vec{\alpha} \in I(\mathbb{N}). \quad R(\vec{\alpha}) \Vdash \vec{\alpha} : A(\vec{x})$$

Moreover R, which is recursive (definable in Gödel system $\mathbf{T}$), is patterned after the proof of $A(\vec{x})$.

From the proof:

(χ)-axiom:

$$r_{\mathsf{P}}(\vec{m}, n, s) = \begin{cases} \{\mathsf{P}(\vec{m}, n)\} & \text{if } [\![\mathsf{P}(\vec{m}, n)]\!]^{\mathcal{I}_0} = \text{true and } \forall n'.\mathsf{P}(\vec{m}, n') \notin s \\ \bot & \text{else.} \end{cases}$$

Then setting $r_{\mathsf{P}}^{\mathcal{S}} = r_{\mathsf{P}}^* \circ \psi_{\mathbb{N}^{k+1}}$, for any $\vec{\alpha}, \beta \in I(\mathbb{N})$ we have:

$$r_{\mathsf{P}}^{\mathcal{S}}(\vec{\alpha}, \beta) \Vdash \vec{\alpha}, \beta : \mathsf{P}(\vec{x}, y) \to \chi_{\mathsf{P}}(\vec{x})$$

Modus Ponens:

$$\frac{r \Vdash \vec{\alpha} : A \quad r' \Vdash \vec{\alpha} : A \to B}{r \bullet^{\mathcal{S}} r' \Vdash \vec{\alpha} : B}$$