Mathematical specifications of programming languages

Ambroise Lafont[1]

[1]University of New South Wales
Sydney, Australia

October 23, 2020

That is the question

What is a programming language, mathematically?

- In the literature, no well-established consensus.

Differential λ-calculus [Ehrhard-Regnier 2003]

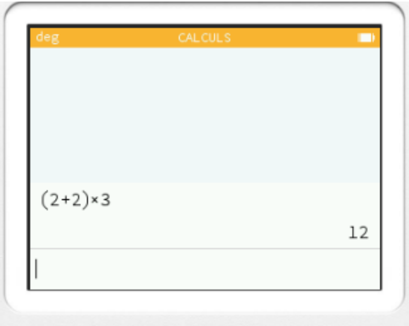
$\sim$10 pages (section 2 $\longrightarrow$ beginning of section 3) describing the programming language and proving some properties.

- In this talk:
  - a tentative notion of programming language, transition monads (FSCD 2020, with Tom and Andre Hirschowitz), and
  - a discipline for automatically generating well-behaved transition monads.
  - in the untyped case for ease of presentation (simply-typed case works as well)

What is a programming language?

2 components:

- **Syntax**: formal language for writing programs;
- **Operational semantics**: how do programs *execute*.



$$(2+2)\times 3 \xrightarrow{\text{1 execution step}} 4 \times 3 \xrightarrow{\text{1 execution step}} 12$$

What is a programming language?

A graph whose vertices are programs.

$$\begin{tikzcd}
(2+2)\times 3 \arrow[d] \\
4\times 3 \arrow[d] \\
12
\end{tikzcd}
\qquad
\begin{tikzcd}
 & 3\times 2+2\times 2 \arrow[dl] \arrow[dr] & \\
6+2\times 2 \arrow[dr] & & 3\times 2+4 \arrow[dl] \\
 & 6+4 \arrow[d] & \\
 & 10 &
\end{tikzcd}
\qquad
\begin{tikzcd}
x+(5+4) \arrow[d] \\
x+9
\end{tikzcd}$$

Variables = placeholders for expressions

- Substitution: $(x+(5+4))[x := 12] = 12+(5+4)$
- Reductions are stable under substitution

$$\frac{{\color{red}x}+(5+4) \longrightarrow {\color{red}x}+9}{{\color{red}12}+(5+4) \longrightarrow {\color{red}12}+9}.$$

$\rightsquigarrow$ Transition monads!

A difficulty

Bound variables and α-equivalence

α-**equivalence**:

$$\lambda x.x \quad \text{should be identified with} \quad \lambda y.y$$

"x is bound by λ in $\lambda x.x$"

Specifying programming languages: **initial semantics**

- Constructing syntax and reductions may be complex (cf. differential λ-calculus).
- Often easier to describe the models.

Model $\approx$ graph with interpretation of the operations and reductions

a model of arithmetic expressions: $\mathbb{Z}$ (or rather $\mathbb{Z}[x, y, \ldots]$)

- Syntactic "+" $\rightsquigarrow$ actual "+" ,
- Syntactic "×" $\rightsquigarrow$ actual "×" , ...

- Programming language = initial model.
- Initiality $\Rightarrow$ recursion principle.

Notion of signature

- Associated notion (category) of models.
- Effective iff the initial model (specified object) exists.

Related work: syntax

Two main notions of syntax:

- Substitution monoids ($\approx$ finitary monads) [Fiore-Plotkin-Turi, 1999].
- Nominal sets [Gabbay-Pitts, 1999].

wider recursion principle | more structured models

$[\mathbb{N}, \mathrm{Set}]$ — nominal sets — monads

This approach: monads

Related work: specifying syntax

Main notions of signature for monads:

- Pointed strong endofunctors [Fiore-Plotkin-Turi, 1999].
- Equational systems [Fiore-Hur, 2010].
- Modules [Hirschowitz-Maggesi, 2007].

This approach: modules

Related work: semantics

Semantic notions of programming language:

- Distributive laws [Plotkin-Turi, 1997].
- double categories [Meseguer, the Montanari school].

Do not cover higher-order languages.

- 2-categories [Power, Seely,...].
- relative monads [Ahrens, 2016].

Only covers congruent semantics.

In this talk

- Mathematical definition of programming languages as **transition monads**.
- Signatures for specifying them
- Systematic use of monads and modules for taking care of substitution.

Outline

1. Transition monads
   - Graphs
   - Substitution
   - Definition
2. Generating transition monads (Initial Semantics)
   - Three-level specification
   - Examples
3. Compilation and initiality

Outline

Ingredients

- Programming languages (PLs) as graphs
  - (**Syntax**) vertices = terms
  - (**Semantics**) arrows = reductions between terms
- Simultaneous substitution: variables $\mapsto$ terms
  - monads and modules over them

Example

λ-calculus with β-reduction:

- **Syntax:** $S, T \quad ::= x \mid S\ T \mid \lambda x.S$
- Modulo α-**equivalence**, e.g.

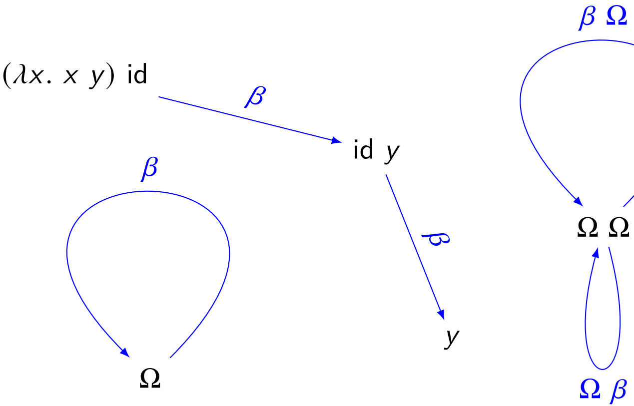
$$\lambda x.x = \lambda y.y$$

- **Reductions:** $(\lambda x.t)\ u \xrightarrow{\beta} t[x := u] \qquad + \quad$ congruences

Outline

PLs as graphs

Example: λ-calculus with β-reduction



- **(Syntax)** vertices = terms e.g. $\Omega = (\lambda x.x\,x)\,(\lambda x.x\,x)$
- **(Semantics)** arrows = reductions

Graphs

Definition

Graph $=$ a quadruple (A, V, σ, τ) where

$$A = \{\text{arrows}\} \qquad \sigma = \text{source of an arrow}$$
$$V = \{\text{vertices}\} \qquad \tau = \text{target of an arrow}$$

$$A \overset{\sigma}{\underset{\tau}{\rightrightarrows}} V$$

$$\sigma : \begin{array}{ccc} A & \to & V \\ t \xrightarrow{r} u & \mapsto & t \end{array} \qquad \tau : \begin{array}{ccc} A & \to & V \\ t \xrightarrow{r} u & \mapsto & u \end{array}$$

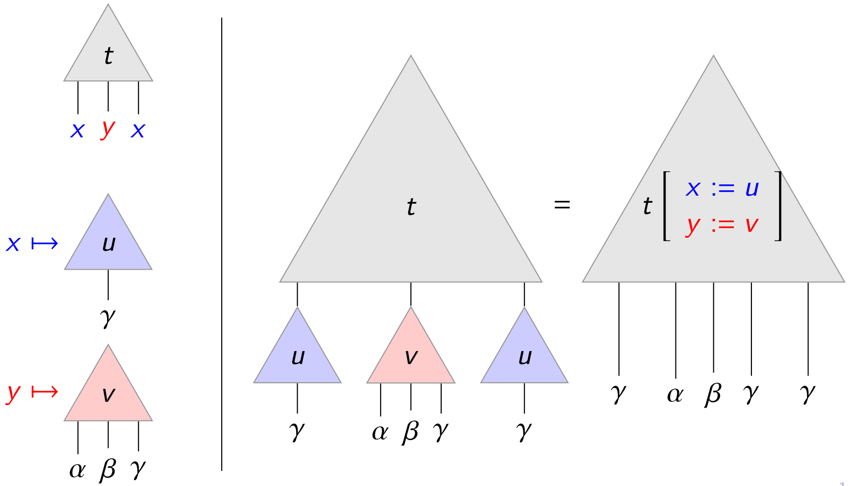
$$\sigma(r) \xrightarrow{r} \tau(r)$$

Outline

Simultaneous substitution

Syntax comes with substitution

terms (e.g. λ-terms) $=$ trees with free variables as (distinguished) leaves.

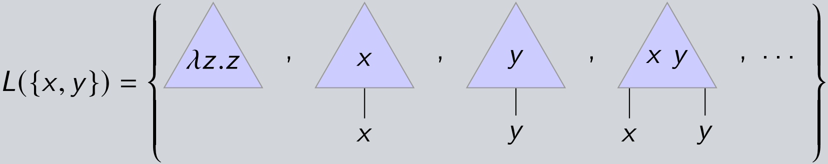


Simultaneous substitution made formal

Free variables indexing

$$X \mapsto \{\text{terms taking free variables in } X\}$$

Example: λ-calculus



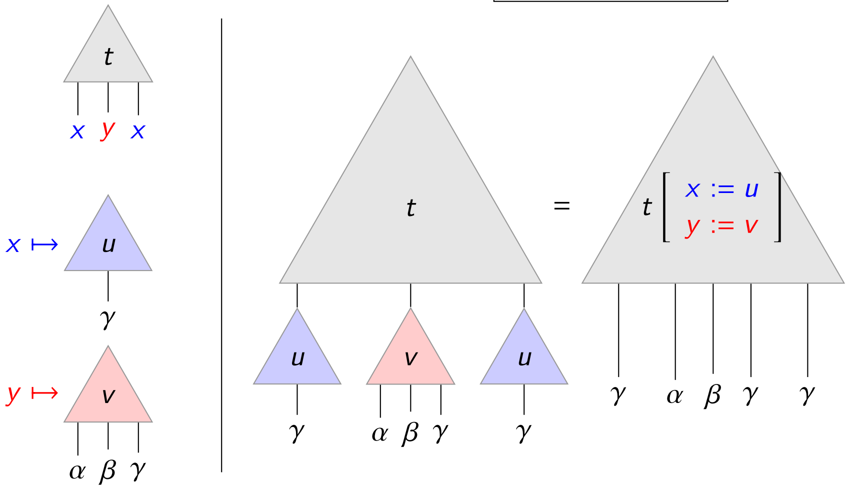
Simultaneous substitution (bind)

$$\forall f : X \to L(Y), \qquad \boxed{\begin{array}{rl} L(X) & \to L(Y) \\ t & \mapsto t[x \mapsto f(x)] \quad (\text{or } t[f]) \end{array}}$$

Simultaneous substitution

$$\forall f : X \to L(Y), \quad X = \{x, y\} \quad Y = \{\alpha, \beta, \gamma\}$$

$$\boxed{\begin{array}{rl} L(X) & \to L(Y) \\ t & \mapsto t[f] \end{array}}$$



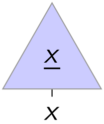
Monads model simultaneous substitution

λ-calculus as a monad $(L, \_[\_], \eta)$

1. Simultaneous substitution $(L, \_[\_])$
2. Variables are terms

$$\eta_X : \quad X \quad \rightarrow \quad L(X)$$

$$x \quad \mapsto$$



3. Substitution laws:

$$\underline{x}[f] = f(x) \qquad\qquad t[x \mapsto \underline{x}] = t$$

$+$ associativity:

$$t[f][g] = t\,[x \mapsto f(x)[g]]$$

Substitution for semantics

Syntax supports substitution. This is also true of semantics.

Our notion of PL:

- **Syntax**: a monad $(L, \_[\_], \eta)$
- **Semantics**:
  - graphs $R(X) \underset{\tau_X}{\overset{\sigma_X}{\rightrightarrows}} L(X)$ for each X

    $R(X) =$ total set of reductions between terms taking free variables in X

  - substitution of reduction: variables $\mapsto$ L-**terms**.

$$\frac{t \xrightarrow{r} u}{t[f] \xrightarrow{r[f]} u[f]}$$

- $\Rightarrow$ R is a L-module, and σ,τ are module morphisms (see next slide)

Substitution for semantics made formal

R as a **module** over L

R supports L-monadic substitution:

$$\forall f : X \to \boldsymbol{L}(Y), \quad \boxed{\begin{array}{rl} R(X) & \to R(Y) \\ r & \mapsto r[x \mapsto f(x)] \quad (\text{or } r[f]) \end{array}}$$

+ substitution laws

Other examples of L-modules: L, $L \times L$, 1, ...

σ and τ as L-**module morphisms**

$$t \xrightarrow{r} u \;\rightsquigarrow\; t' \xrightarrow{r[f]} u' \quad \text{with} \quad \begin{cases} t' = t[f] \\ u' = u[f] \end{cases} \text{ i.e., } \begin{cases} \sigma(r[f]) = \sigma(r)[f] \\ \tau(r[f]) = \tau(r)[f] \end{cases}$$

Commutation with substitution $\Leftrightarrow$ Module morphisms $\sigma, \tau : R \to L$.

Outline

Transition monads (first attempt)

Summary: graphs + substitution.

Definition

A **transition monad** $R \overset{\sigma}{\underset{\tau}{\rightrightarrows}} T$ consists of

- T = monad (= module over itself)
- R = module over T
- $\sigma, \tau : R \to T$ are T-module morphisms.

Example

λ-calculus with β-reduction.

- Untyped case: base category = Set
- Simply-typed case: base category = Set^{Types}

What about big-step cbv λ-calculus? Terms reduce to values, not terms!

Transition monads

Generalising cbv λ-calculus, and reduction monads

cbv λ-calculus (big-step)	*Values* (monad)	$$\begin{tikzcd} & \mathit{Transitions} \arrow[dl, "\mathit{source}"'] \arrow[dr, "\mathit{target}"] & \\ \mathit{Terms} & & \mathit{Values} \end{tikzcd}$$
transition monads	a monad T	T-module morphisms $M_1 \xleftarrow{\mathit{source}} \mathit{Trans} \xrightarrow{\mathit{target}} M_2$
reduction monads[1]	a monad T	$T \xleftarrow{\mathit{source}} \mathit{Trans} \xrightarrow{\mathit{target}} T$

Examples: $\bar{\lambda}\mu$-calculus, cbv λ-calculus, π-calculus, differential λ-calculus, GSOS specs

[1]POPL'20 with B.Ahrens, A. Hirschowitz, M. Maggesi.

Morphisms of transition monads

Simple case $M_i = T$

PLs	$\Leftrightarrow$	Transition monads
Compilations	$\Leftrightarrow$	Morphisms of transition monads

Morphism $(T \leftarrow Trans \rightarrow T) \longrightarrow (T' \leftarrow Trans' \rightarrow T') =$

(Syntax) A *monad morphism*[1] $T \xrightarrow{c} T'$

(Semantics) *Forward simulation*[2]: if $t_1 \xrightarrow{r} t_2$, *then* $c(t_1) \xrightarrow{[\![r]\!]} c(t_2)$

Examples (POPL'20, detailed later)

- λ-calculus + fixpoint op. $\longrightarrow$ λ-calculus
- λ-calculus + explicit substitution $t[x/u]$ $\longrightarrow$ λ-calculus

[1] mapping preserving substitution and variables

[2] backward simulations are often considered as a correctness criteria

Outline

Outline

1. Transition monads
   - Graphs
   - Substitution
   - Definition
2. Generating transition monads (Initial Semantics)
   - Three-level specification
   - Examples
3. Compilation and initiality

Constructing *transition monads*

We have a definition of programming languages as transition monads.

Can we construct them from *simple specifications*?

We provide:

- a notion of *simple specification* = **signature** for transition monads
- a theorem ensuring the existence (unique up to iso) of a transition monad matching a spec

Three-level specification

Transition monad $= (T\ ,\ M_1 \xleftarrow{source} Trans \xrightarrow{target} M_2)$

Three spec steps:

Step	Component	Nature	Specification
1	T	monad	Operations + Equations
2	M_1, M_2	T-modules	Operations + Equations
3	*Trans*, *source*, *target*	"transition structure"	Transition rules as $\dfrac{t_1 \to u_1 \ldots t_n \to u_n}{t \to u}$

$\Rightarrow$ Three notions of signatures.

Outline

1. Transition monads
   - Graphs
   - Substitution
   - Definition
2. Generating transition monads (Initial Semantics)
   - Three-level specification
   - Examples
3. Compilation and initiality

Examples

Transition monad $= (\,T\,,\ M_1 \xleftarrow{source} Trans \xrightarrow{target} M_2)$

Upcoming examples

1.	cbn λ-calculus	full signature (sketched)
2.	cbn λ-calculus	signature for T
3.	cbn λ-calculus	left congruence rule for application
4.	cbn λ-calculus	congruence rule for abstraction (involves a binding variable)
5.	cbv λ-calculus	signature for M_i
6.	differential λ-calculus	signature for M_i
7.	differential λ-calculus	signature for T

Example 1/7: small-step cbn λ-calculus

Transition monad = $(T \;,\; M_1 \xleftarrow{source} Trans \xrightarrow{target} M_2)$

Signature for cbn λ-calculus

Step	Component	Nature	Specification
1	T	monad	Operations = app, abs
2	M_1, M_2	T-modules	$M_1 = M_2 = T$
3	*Trans*, *source*, *target*	"transition structure"	β-rule + congruences

Example 2/7: Specify the monad of λ-terms

(untyped) cbn λ-calculus: $(T, T \xleftarrow{source} Trans \xrightarrow{target} T)$

- Syntax "generated" by

application	$T \times T \to T$	
λ-abstraction $\lambda x.t$	$T' \to T$	$T' =$ module of terms depending on an extra variable
(variables)	$Var \to T$	

Signature for T

2 operations (application/abstraction)

- Monads always have variables: no need to specify them
- "operation"= *module morphism*: compatible with substitution:

$$(t_1\ t_2)[y \mapsto u_y] = t_1[y \mapsto u_y]\ t_2[y \mapsto u_y]$$

References "Second-order equational logic" Fiore-Hur '10,
"Modular specification of monads" Ahrens et al. '19

Disgression on T'

- M'= **derivative** of a module M:

$$M'(X) = M(\overbrace{X \amalg \{\diamond\}}^{X \text{ extended with a fresh variable } \diamond})$$

used to model an operation binding a variable.

$$\mathrm{abs} : \quad L' \quad \to L \qquad \left\{ \begin{aligned} \mathrm{abs}_X : L(X \amalg \{\diamond\}) &\to L(X) \\ t &\mapsto \lambda \diamond . t \end{aligned} \right.$$

Example 3/7: Left congruence for application

cbn λ-calculus: $(T, T \xleftarrow{source} Trans \xrightarrow{target} T)$

Left congruence rule for application

$$\frac{t_1 \longrightarrow t_2}{app(t_1, u) \longrightarrow app(t_2, u)}$$

- Easy interpretation of transition rules:

Components of the rule	Interpreted as...
3 "metavariables": t_1, t_2, u	a "metavariable" T-module $V = T \times T \times T$
1 "premise": $t_1 \longrightarrow t_2$	$V \to M_1 \times M_2$ $(t_1, t_2, u) \mapsto (t_1, t_2)$ (T-module morphism)
"conclusion": $app(t_1, u) \longrightarrow app(t_2, u)$	$V \to M_1 \times M_2$ $(t_1, t_2, u) \mapsto (\, app(t_1, u),\ app(t_2, u)\,)$

Example 4/7: Binding variables in rules

cbn λ-calculus: $(T, T \xleftarrow{source} Trans \xrightarrow{target} T)$

Congruence rule for abstraction

$$\frac{t_1 \longrightarrow t_2}{\lambda x.t_1 \longrightarrow \lambda x.t_2}$$

- "metavariables" t_1 and t_2: terms that may depend on x.
- $T' =$ T-module of terms depending on an additional variable

Components of the rule	Interpreted as...
2 "metavariables": t_1,t_2	a "metavariable" T-module $V = T' \times T'$
1 "premise": $t_1 \to t_2$	$V \to T' \times T'$ $(t_1,t_2) \mapsto (t_1, t_2)$ (T-module morphism)
"conclusion": $\lambda x.t_1 \to \lambda x.t_2$	$V \to T \times T$ $(t_1, t_2) \mapsto (\lambda x.t_1, \lambda x.t_2)$

Example 5/7: Specify M_i for cbv

$$\text{Transition monad} = (T, \quad M_1 \xleftarrow{source} Trans \xrightarrow{target} M_2)$$
$$\text{cbv } \lambda\text{-calculus} = (Vals, Tms \xleftarrow{source} Trans \xrightarrow{target} Vals)$$

Syntax of values and terms

$$\begin{aligned} Vals:\ v, w &::= x \mid \lambda x.t \\ Tms:\ t, u &::= \underbrace{x \mid \lambda x.t}_{} \mid t\ u \\ &::= \quad v \quad \mid t\ u \end{aligned} \quad \Rightarrow \quad \begin{aligned} \text{terms} &= \text{binary trees } \textit{of} \text{ values} \\ Tms &= BinTree \circ Vals \end{aligned}$$

In fact, by definition of a transition monad,

- M_i is always of the shape $S_i \circ T$. Here,

  $T = Vals \qquad M_1 = BinTree \circ T \qquad M_2 = Id \circ T (= T)$

- Signature for M_i = Signature for S_i

Signature for *BinTree*

variables + 1 binary operation (accounts for $t\ u$ in Tms)

Example 6/7: Specify M_i for DLC

Transition monad $= (T\ ,\ M_1 \xleftarrow{source} Trans \xrightarrow{target} M_2)$

Differential λ-calculus (DLC)

Syntax monad T of terms (a variant of λ-calculus)

Semantics a $\underbrace{\text{term } t}_{M_1 = Id \circ T\ (=T)}$ reduces to a $\underbrace{\text{multiterm } t_1 + \cdots + t_n}$

multiterms = formal sum of terms

$M_2 = FormalSum \circ T$

Signature for *FormalSum*

Operations	a constant 0, a binary operation $+$, variables
Equations	commutativity, associativity, unitality

Example 7/7: the monad of DLC

differential λ-calculus: $(T, M_1 \xleftarrow{source} Trans \xrightarrow{target} M_2)$

- Syntax of DLC $=$ variant of λ-calculus

Application of DLC

$$app : (t, U) \mapsto t\ U$$

$$\begin{aligned} \text{input of } app &= \text{a term } t \text{ and a multi-term } U = u_1 + \cdots + u_n \\ &= \text{a term and a formal sum } of \text{ terms} \\ \text{input } module \text{ of } app &= T \times (FormalSum \circ T) \end{aligned}$$

Signature for T

3 operations (no equation):

application $t\ U$	$T \times (FormalSum \circ T) \to T$
differential application $Dt \cdot u$	$T \times T \to T$
λ-abstraction	(as before)

Outline

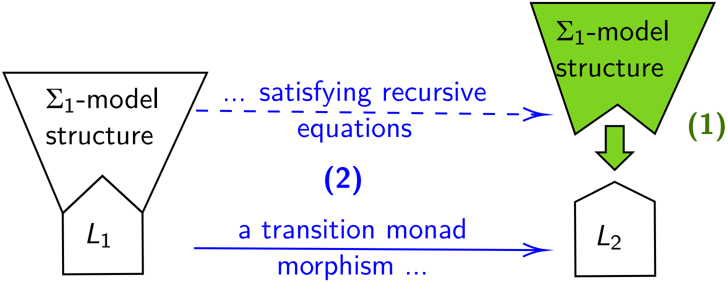
1. Transition monads
   - Graphs
   - Substitution
   - Definition
2. Generating transition monads (Initial Semantics)
   - Three-level specification
   - Examples
3. Compilation and initiality

Generating compilations by initiality

Initiality ≈ recursion principle

$$\underbrace{L_1}_{\substack{\text{specified by a signature } \Sigma_1: \\ L_1 \,=\, \textbf{initial model} \text{ of } \Sigma_1}} \longrightarrow L_2$$

Data generating a compilation: a Σ_1-model structure for L_2
$\Rightarrow$ By recursion/**initiality**, get a model morphism $L_1 \to L_2$



Examples

$$\underbrace{L_1}_{\text{specified by a signature } \Sigma_1:} \longrightarrow L_2$$

Recipe:

1. provide a Σ_1-model structure for L_2
2. as a model morphism, the induced compilation satisfies recursive equations.

Upcoming examples (POPL'20)

- λ-calculus + formal fixpoint op. $\longrightarrow$ λ-calculus
  1. construct a fixpoint operator in λ-calculus
  2. formal fixpoint operator $\mapsto$ constructed fixpoint operator
- λ-calculus + explicit substitution[1] $t[x/u]$ $\longrightarrow$ λ-calculus
  1. consider λ-calculus with its unary substitution operation
  2. explicit substitution $\mapsto$ real substitution

[1] A Theory of Explicit Substitutions with Safe and Full Composition, [Kesner 2009]

Example 1/2: compiling λ-calculus + formal fixpoint op.

$$\underbrace{L_{\text{fix}}}_{\text{specified by "}\Sigma_L + \Sigma_{\text{fix}}\text{"}} \longrightarrow \underbrace{L}_{\text{specified by } \Sigma_L} \quad (\lambda\text{-calculus})$$

Signature Σ_{fix} specifying a fixpoint operator

- an operation $T' \xrightarrow{\text{fix}} T$
- reductions $\boxed{\text{fix(t)}\rightarrow\text{t[x}\mapsto \text{fix(t)]}}$ $(t \in T'(X) = T(X \amalg \{x\}))$

Needed: a model structure on L for Σ_{fix} (already has the Σ_L-part)

- choose a fixpoint combinator: a term Y s.t. $Yu \rightarrow^*_\beta u(Yu)$
- define $\text{fix}(t) := Y(\lambda x.t)$

$$\underbrace{Y(\lambda x.t)}_{\text{fix}(t)} \rightarrow^*_\beta (\lambda x.t)(Y(\lambda x.t)) \rightarrow_\beta \underbrace{t[x \mapsto Y(\lambda x.t)]}_{t[x\mapsto\text{fix}(t)]}$$

Example 2/2: compiling λ-calculus + explicit substitution

$$\underbrace{L_{ex}}_{\text{specified by "}\Sigma_L\setminus\{\beta\}+\Sigma_{ex}\text{"}} \longrightarrow \underbrace{L}_{\text{specified by }\Sigma_L} \quad (\lambda\text{-calculus})$$

Signature Σ_{ex} for the explicit substitution

- an operation $T' \times T \xrightarrow{(t,u)\mapsto t[x/u]} T$ s.t.

$$\boxed{t[x/u][y/v] = t[y/v][x/u]} \quad \text{if } x \notin fv(v), y \notin fv(u)$$

- β-reduction $\boxed{(\lambda x.t)u \to t[x/u]}$ + congruences +

$$\boxed{\text{t[x/u][y/v]}\to\text{t[y/v][x/u[y/v]]}} \quad \text{if } x \notin fv(u),\ y \in fv(u)$$

Needed: a model structure on L for Σ_{ex}

- use the real susbtitution $T' \times T \xrightarrow{(t,u)\mapsto t[x\mapsto u]} T$
- β-reduction + congruences + reflexive reduction

$$t[x \mapsto u][y \mapsto v] \overset{=}{\to} t[y \mapsto v][x \mapsto u[y \mapsto v]]$$

Perspectives

- Generalise well-known theorems, e.g. Howe's method:
  - "A cellular Howe's theorem", LICS'20 with T. Hirschowitz and P. Borthelle, in a simpler setting.
- Morphisms of transition monads = compilations
  - explore different variants (different correctness criteria).
  - try "academic" examples, e.g, Plotkin's CPS translations of λ-calculus.
  - "effective" Coq formalization (theory already formalized using UniMath for the syntax)
- Effectful transitions?