A presheaf model of parametric type theory

Jean-Philippe Bernardy Thierry Coquand **Guilhem Moulin**

CHALMERS | GÖTEBORG UNIVERSITY

Types 2015, Tallinn

Parametricity: semantics of polymorphism

- Type parameters cannot be inspected.
  - Take id : $a \to a$.
    Then $\forall x : a$, id x *must be* x.

Parametricity: semantics of polymorphism

- Type parameters cannot be inspected.
  - Take id : $a \to a$.
    Then $\forall x : a$, id x *must be* x.
  - Take filter : $(a \to \mathrm{Bool}) \to \mathrm{List}\, a \to \mathrm{List}\, a$. Then
    $\forall a_1\, a_2,\ \forall (R : a_1 \to a_2 \to U),$
    $\forall f_1, f_2$ such that $(\forall x_1\, x_2, R\ x_1\ x_2 \to f_1\ x_1 \equiv f_2\ x_2),$
    $\forall xs_1, xs_2$ such that $R^*\ xs_1\ xs_2,$
    $R^*\ (\mathrm{filter}\ f_1\ xs_1)\ (\mathrm{filter}\ f_2\ xs_2)$

Parametricity: semantics of polymorphism

➠ Type parameters cannot be inspected.

- Take id : $a \to a$.
  Then $\forall x : a$, id x *must be* x.
- Take filter : $(a \to \mathrm{Bool}) \to \mathrm{List}\, a \to \mathrm{List}\, a$. Then

  $\forall a_1\, a_2,\ \forall (R : a_1 \to a_2 \to U),$
  $\forall f_1, f_2$ such that $(\forall x_1\, x_2, R\ x_1\ x_2 \to f_1\ x_1 \equiv f_2\ x_2),$
  $\forall xs_1, xs_2$ such that $R^*\ xs_1\ xs_2,$
  $R^*\ (\mathrm{filter}\ f_1\ xs_1)\ (\mathrm{filter}\ f_2\ xs_2)$

➥ These theorems on id, filter are deduced from their *type* only.

Motivation: some applications

Proofs of:

- Program transformations (*e.g.*, short-cut fusion)
- Church-encoding of datatypes *e.g.*,

$$\mathbf{N} \equiv \forall X, X \to (X \to X) \to X$$

- Well-scoped λ-terms:

$$\begin{aligned}&\textbf{data}\ \mathrm{Term}\ a : U\ \textbf{where}\\ &\quad \mathrm{var}\ \ : a \to \mathrm{Term}\ a\\ &\quad \mathrm{app} : \mathrm{Term}\ a \to \mathrm{Term}\ a \to \mathrm{Term}\ a\\ &\quad \mathrm{abs} : \mathrm{Term}\ (\mathrm{Maybe}\ a) \to \mathrm{Term}\ a\end{aligned}$$

Take id : $a \to a$.

Then $\forall x : a$, id x *must be* x.

Take $\mathrm{id} : (a : U) \to (x : a) \to a$.

Then $\forall x : a$, $\mathrm{id}\, x$ *must be* x.

Take $\mathrm{id} : (a : U) \to (x : a) \to a$.

Then $(a : U) \to (x : a) \to \mathrm{id}\, a\, x \equiv_a x$ is inhabited.

where $(\equiv)$ is the *Leibniz* equality:

$$x \equiv_a y \quad ::= \quad (P : a \to U) \to P\, x \to P\, y$$

$$\begin{array}{llll} \mathrm{refl} : & (a : U) & \to (x : a) & \to x \equiv_a x \\ \mathrm{refl} & a & x & = \lambda P : (a \to U).\ \lambda p : (P\, x).\ p \end{array}$$

Take $\mathrm{id} : (a : U) \to (x : a) \to a$.

Then $(a : U) \to (x : a) \to \mathrm{id}\, a\, x \equiv_a x$ is inhabited.

$\lambda(a : U).\ \lambda(x : a).\ ?$

Take $\mathrm{id} : (a : U) \to (x : a) \to a$.

Then $(a : U) \to (x : a) \to \mathrm{id}\, a\, x \equiv_a x$ is inhabited.

$\lambda(\mathrm{id} : (a : U) \to (x : a) \to a).\ \lambda(a : U).\ \lambda(x : a).\ ?$

Take $\mathsf{id} : (a : U) \to (x : a) \to a$.

Then $(a : U) \to (x : a) \to \mathsf{id}\, a\, x \equiv_a x$ is inhabited.

$\lambda(\mathsf{id} : (a : U) \to (x : a) \to a).\ \lambda(a : U).\ \lambda(x : a).\ ?$

$\mathsf{id}\,(a \times (\equiv_a x))\,(x, \mathsf{refl}\, a\, x) \quad : a \times (\equiv_a x)$

Take $\mathsf{id} : (a : U) \to (x : a) \to a$.

Then $(a : U) \to (x : a) \to \mathsf{id}\, a\, x \equiv_a x$ is inhabited.

$\lambda(\mathsf{id} : (a : U) \to (x : a) \to a).\ \lambda(a : U).\ \lambda(x : a).\ ?$

$$\mathsf{id}\,(a \times (\equiv_a x))\,(x, \mathsf{refl}\, a\, x) \quad : a \times (\equiv_a x)$$

$$\pi_2(\mathsf{id}\,(a \times (\equiv_a x))\,(x, \mathsf{refl}\, a\, x)) \quad : \pi_1\,(\mathsf{id}\,(a \times (\equiv_a x))\,(x, \mathsf{refl}\, a\, x)) \equiv_a x$$

Take $\mathrm{id} : (a : U) \to (x : a) \to a$.

Then $(a : U) \to (x : a) \to \mathrm{id}\, a\, x \equiv_a x$ is inhabited.

$\lambda(\mathrm{id} : (a : U) \to (x : a) \to a).\ \lambda(a : U).\ \lambda(x : a).\ ?$

$$\mathrm{id}\,(a \times (\equiv_a x))\,(x, \mathrm{refl}\, a\, x) \quad : a \times (\equiv_a x)$$

$$\pi_2(\mathrm{id}\,(a \times (\equiv_a x))\,(x, \mathrm{refl}\, a\, x)) \quad : \pi_1\,(\mathrm{id}\,(a \times (\equiv_a x))\,(x, \mathrm{refl}\, a\, x)) \equiv_a x$$

↪ We would like π_1 to commute under application!

$$a, p, A, P \coloneqq \ldots \mid (x : A) \times P \mid (a, p) \mid P \ni a \mid [\![a]\!]$$

$$\frac{\Gamma \vdash A \qquad \Gamma, x : A \vdash P}{\Gamma \vdash (x : A) \times P} \qquad \frac{\Gamma \vdash a : \lfloor A \rfloor \qquad \Gamma \vdash p : A \ni a}{\Gamma \vdash (a, p) : A}$$

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash a : \lfloor A \rfloor}{\Gamma \vdash A \ni a} \qquad \frac{\Gamma \vdash a : A}{\Gamma \vdash [\![a]\!] : A \ni \lfloor a \rfloor}$$

$$\begin{aligned} [\![(a, p)]\!] &= p \\ ((x : A) \times P[x]) \ni a &= P[a] \\ t &= (\lfloor t \rfloor, [\![t]\!]) \\ T &= (x : \lfloor T \rfloor) \times (T \ni x) \end{aligned}$$

$$\mathsf{id}\,(a \times (\equiv_a x))\,(x, \mathsf{refl}\,a\,x) \quad : a \times (\equiv_a x)$$

$$[\![\mathsf{id}\,(a \times (\equiv_a x))\,(x, \mathsf{refl}\,a\,x)]\!] \quad : (a \times (\equiv_a x)) \ni \lfloor \mathsf{id} \ldots (x, \mathsf{refl}\,a\,x) \rfloor$$
$$: (a \times (\equiv_a x)) \ni (\mathsf{id}\,a\,x)$$
$$: \mathsf{id}\,a\,x \equiv_a x$$

$$a, p, A, P \coloneqq \ldots \mid (x : A) \times_i P \mid (a,_i p) \mid P \ni_i a \mid a \cdot i$$
$$\Gamma \coloneqq () \mid \Gamma, x : A \mid \Gamma, i : \mathbb{I}$$

$$\frac{\Gamma \vdash A \qquad \Gamma, x : A \vdash P}{\Gamma, i : \mathbb{I} \vdash (x : A) \times_i P} \qquad \frac{\Gamma \vdash a : A(i\,0) \qquad \Gamma \vdash p : A \ni_i a}{\Gamma, i : \mathbb{I} \vdash (a,_i p) : A}$$

$$\frac{\Gamma, i : \mathbb{I} \vdash A \qquad \Gamma \vdash a : A(i\,0)}{\Gamma \vdash A \ni_i a} \qquad \frac{\Gamma, i : \mathbb{I} \vdash a : A}{\Gamma \vdash a \cdot i : A \ni_i a(i\,0)}$$

$$(a,_i p) \cdot i = p$$
$$((x : A) \times_i P[x]) \ni_i a = P[a]$$
$$t = (t(i\,0),_i t \cdot i)$$
$$T = (x : T(i\,0)) \times_i (T \ni_i x)$$

Computing Parametricity types

One could be tempted to add

$$U \ni_i A = A \to U$$

$$((x : A) \to B[x]) \ni_i a = (x : A) \to (x' : A \ni_i x) \to B[(x,_i x')] \ni_i (a\, x)$$

Computing Parametricity types

One could be tempted to add

$$U \ni_i A = A \to U$$

$$((x : A) \to B[x]) \ni_i a = (x : A) \to (x' : A \ni_i x) \to B[(x,_i x')] \ni_i (a\, x)$$

but this doesn't work.

Computing Parametricity types

One could be tempted to add

$$U \ni_i A = A \to U$$
$$((x : A) \to B[x]) \ni_i a = (x : A) \to (x' : A \ni_i x) \to B[(x,_i x')] \ni_i (a\, x)$$

but this doesn't work. However conversion is not needed in practice:

$$f : (Q : U \ni_i A) \to A \to U$$
$$f\, Q\, x = (A,_i Q) \ni_i x$$
$$g : (P : A \to U) \to U \ni_i A$$
$$g\, P = ((x : A) \times_i (P\, x)) \cdot i$$

Then $f\,(g\,P) = P$ and $g\,(f\,Q) = Q$

The case of Function Spaces

$$f : ((x : A) \to B[x])\ \ni_i\ a \to (x : A) \to (x' : A\ \ni_i\ x) \to B[(x,_i\, x')]\ \ni_i\ (a\, x)$$
$$f\, q\, x\, x' = ((a,_i\, q)\, (x,_i\, x')) \cdot i$$

$$g : ((x : A) \to (x' : A\ \ni_i\ x) \to B[(x,_i\, x')]\ \ni_i\ (a\, x)) \to (A \to B)\ \ni_i\ a$$
$$g\, p = ? \cdot i$$

The case of Function Spaces

$$f : ((x : A) \to B[x]) \ni_i a \to (x : A) \to (x' : A \ni_i x) \to B[(x,_i x')] \ni_i (a\, x)$$
$$f\, q\, x\, x' = ((a,_i q)\, (x,_i x')) \cdot i$$

$$g : ((x : A) \to (x' : A \ni_i x) \to B[(x,_i x')] \ni_i (a\, x)) \to (A \to B) \ni_i a$$
$$g\, p = \langle a,_i p \rangle \cdot i$$

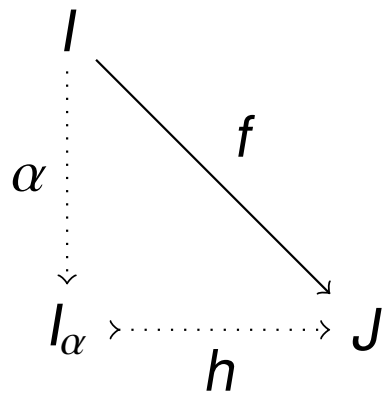
$$a, p, A, P := \ldots \mid \langle a,_i p \rangle$$

$$\frac{\Gamma \vdash a : ((x : A) \to B[x])(i\,0) \qquad \Gamma \vdash p : (x : A(i\,0)) \to (x' : A \ni_i x) \to B[(x,_i x')] \ni_i (a\, x)}{\Gamma, i : \mathbb{I} \vdash \langle a,_i p \rangle : (x : A) \to B[x]}$$

$$\langle a,_i p \rangle\, u = \langle a,_i p \rangle\, (u(i\,0),_i u \cdot i) = (a\, (u(i\,0)) \;,_i\; p\, (u(i\,0))\, (u \cdot i))$$

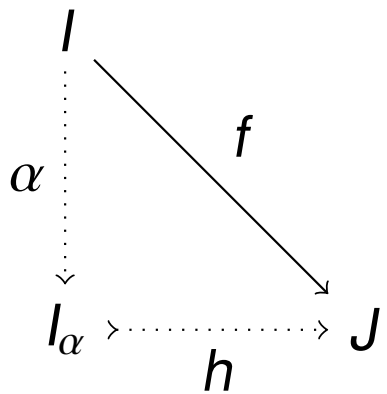
Presheaf model

- Let $\mathbb{I}$ a countable infinite set of *names* (colors), $0 \notin \mathbb{I}$.
- We consider the category **pl** of finite subsets of $\mathbb{I}$ and partial injections: $\mathrm{Hom}(I, J) = I \to J \cup \{0\}$.



Presheaf model

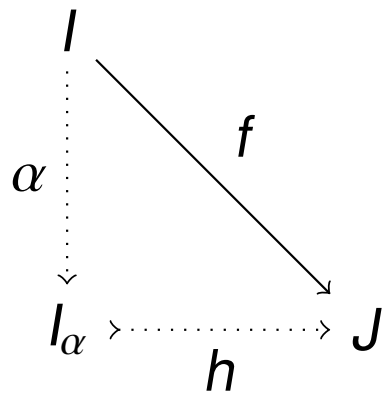
- Let $\mathbb{I}$ a countable infinite set of *names* (colors), $0 \notin \mathbb{I}$.
- We consider the category **pl** of finite subsets of $\mathbb{I}$ and partial injections: $\mathrm{Hom}(I, J) = I \to J \cup \{0\}$.



- We call I-element any $u = (u_J)_{J \subseteq I}$ (alternatively $u = (u_\alpha)$). E.g., $\{i, j\}$-elements are of the form $(u_\varnothing, u_i, u_j, u_{i,j})$.

Presheaf model

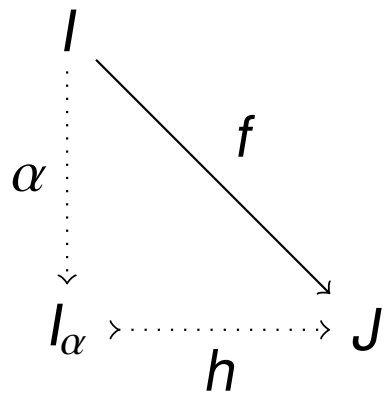
- Let $\mathbb{I}$ a countable infinite set of *names* (colors), $0 \notin \mathbb{I}$.
- We consider the category **pl** of finite subsets of $\mathbb{I}$ and partial injections: $\mathrm{Hom}(I, J) = I \to J \cup \{0\}$.



- We call I-element any $u = (u_J)_{J \subseteq I}$ (alternatively $u = (u_\alpha)$). E.g., $\{i, j\}$-elements are of the form $(u_\varnothing, u_i, u_j, u_{i,j})$.
- If u, v are two I-elements and $i \notin I$, we define the (I, i)-element $(u,_i v)$ as $(u,_i v)_J = u_J$ if $i \notin J$ and $(u,_i v)_{i,J} = v_J$.

Presheaf model

- Let $\mathbb{I}$ a countable infinite set of *names* (colors), $0 \notin \mathbb{I}$.
- We consider the category **pl** of finite subsets of $\mathbb{I}$ and partial injections: $\mathrm{Hom}(I, J) = I \to J \cup \{0\}$.



- We call I-element any $u = (u_J)_{J \subseteq I}$ (alternatively $u = (u_\alpha)$). E.g., $\{i, j\}$-elements are of the form $(u_\varnothing, u_i, u_j, u_{i,j})$.
- If u, v are two I-elements and $i \notin I$, we define the (I, i)-element $(u,_i v)$ as $(u,_i v)_J = u_J$ if $i \notin J$ and $(u,_i v)_{i,J} = v_J$.
- Any (I, i)-element can be written $u = (u_J)_{J \subseteq I} \cup (u_{i,J})_{J \subseteq I}$. We define $u(i\,0) = (u_J)_{J \subseteq I}$ and $u \cdot i = (u_{i,J})_{J \subseteq I}$.

Presheaves

A presheaf F is given by a family of sets $F(I)$ with restriction maps $F(I) \to F(J)$, $u \mapsto uf$ for $f : I \to J$ satisfying

- $u1 = u$, and
- $(uf)g = u(fg)$.

Refined presheaves

A presheaf F is given by a family of I-sets $F(I)$ with restriction maps $F(I) \to F(J)$, $u \mapsto uf$ for $f : I \to J$ satisfying

- $u1 = u$, and
- $(uf)g = u(fg)$, and
- $(u\alpha)_K = u_K$ for any $K \subseteq J$ (alternatively, $(u\alpha)_\beta = u_{\alpha\beta}$).

- A context $\Gamma \vdash$ is interpreted by a (usual) presheaf on $\mathbb{pI}^{\mathrm{opp}}$.
- A type $\Gamma \vdash A$ is interpreted by an I-set $A\rho$ for each object I and $\rho \in \Gamma(I)$, together with restriction maps $A\rho \to A(\rho f)$, $u \mapsto uf$ if $f : I \to J$ satisfying $u1 = u$ and $(uf)g = u(fg)$ for any $g : J \to K$. Furthermore the map $A\rho \to A(\rho\alpha)$, $u \mapsto u\alpha$ is the projection operation.
- A term $\Gamma \vdash a : A$ is interpreted by a I-element $a\rho \in A\rho$ for each object I and $\rho \in \Gamma(I)$, such that $(a\rho)f = a(\rho f)$ for any $f : I \to J$.

- A context $\Gamma \vdash$ is interpreted by a (usual) presheaf on $\mathrm{pI}^{\mathrm{opp}}$.
- A type $\Gamma \vdash A$ is interpreted by an I-set $A\rho$ for each object I and $\rho \in \Gamma(I)$, together with restriction maps $A\rho \to A(\rho f)$, $u \mapsto uf$ if $f : I \to J$ satisfying $u1 = u$ and $(uf)g = u(fg)$ for any $g : J \to K$. Furthermore the map $A\rho \to A(\rho\alpha)$, $u \mapsto u\alpha$ is the projection operation.
- A term $\Gamma \vdash a : A$ is interpreted by a I-element $a\rho \in A\rho$ for each object I and $\rho \in \Gamma(I)$, such that $(a\rho)f = a(\rho f)$ for any $f : I \to J$.

- If $\Gamma \vdash$ and $\Gamma \vdash A$, we interpret $\Gamma, x : A \vdash$ by $(\rho \in \Gamma(I)) \times A\rho$.
- If $\Gamma \vdash$, we interpret $\Gamma, i : \mathbb{I} \vdash$ by $\Gamma * \mathbb{I}(I)$:

$$\{[\rho, i = 0] \mid \rho \in \Gamma(I)\} \cup \{[\rho, i = j] \mid j \in I, \rho \in \Gamma(I \backslash \{j\})\}$$

Interpreting $\Gamma \vdash (x : A) \to B$ (attempt)

If $\rho \in \Gamma(I)$, $((x : A) \to B)\rho$ is interpreted by $(\lambda_f)_{f:I \to J}$ where

$$\lambda_f \in \prod_{u \in A(\rho f)} B\langle \rho f, x = u \rangle$$

such that $\mathrm{app}(\lambda_f, u)g = \mathrm{app}((\lambda_{fg}, u)g)$ for any $g : J \to K$.

Interpreting $\Gamma \vdash (x : A) \to B$

If $\rho \in \Gamma(I)$, $((x : A) \to B)\rho$ is interpreted by $((\lambda_{\alpha f})_{f : I_\alpha \rightarrowtail J})_\alpha$ where

$$\lambda_{\alpha f} \in \prod_{u \in A(\rho\alpha f)} B\langle \rho\alpha f, x = u \rangle$$

such that $\mathrm{app}(\lambda_{\alpha f}, u)g = \mathrm{app}((\lambda_{\alpha fg}, u)g)$ for any $g : J \to K$.

Interpreting $\Gamma \vdash (x : A) \to B$

If $\rho \in \Gamma(I)$, $((x : A) \to B)\rho$ is interpreted by $((\lambda_{\alpha f})_{f : I_\alpha \rightarrowtail J})_\alpha$ where

$$\lambda_{\alpha f} \in \prod_{u \in A(\rho\alpha f)} B\langle \rho\alpha f, x = u \rangle$$

such that $\mathrm{app}(\lambda_{\alpha f}, u)g = \mathrm{app}((\lambda_{\alpha fg}, u)g)$ for any $g : J \to K$.

- Similar trick for the universe.

Interpreting Parametricity constructs

$$\frac{\Gamma, i : \mathbb{I} \vdash a : A}{\Gamma \vdash a \cdot i : A \ \ni_i \ a(i\,0)} \qquad \frac{\Gamma, i : \mathbb{I} \vdash A \qquad \Gamma \vdash a : A(i\,0)}{\Gamma \vdash A \ \ni_i \ a}$$

Let $\rho \in \Gamma(I)$, $j = \mathrm{fresh}(I)$. We define

- $(a \cdot i)\rho \quad = \quad a[\rho, i = j] \cdot j$.

Interpreting Parametricity constructs

$$\frac{\Gamma, i : \mathbb{I} \vdash a : A}{\Gamma \vdash a \cdot i : A \ni_i a(i\,0)} \qquad \frac{\Gamma, i : \mathbb{I} \vdash A \qquad \Gamma \vdash a : A(i\,0)}{\Gamma \vdash A \ni_i a}$$

Let $\rho \in \Gamma(I)$, $j = \mathrm{fresh}(I)$. We define

- $(a \cdot i)\rho \quad = \quad a[\rho, i = j] \cdot j.$
- $(A \ni_i a)\rho \quad = \quad \left\{ v \mid (a\rho, {}_j\, v) \in A[\rho, i = j] \right\}$

Interpreting Parametricity constructs (cont.)

$$\frac{\Gamma \vdash a : A\,(i\,0) \qquad \Gamma \vdash p : A \ni_i a}{\Gamma, i : \mathbb{I} \vdash (a,_i p) : A} \qquad \frac{\Gamma \vdash A \qquad \Gamma, x : A \vdash P}{\Gamma, i : \mathbb{I} \vdash (x : A) \times_i P}$$

Let $[\rho, i = \varphi] \in \Gamma * \mathbb{I}(I)$. If $\varphi = 0$, we define

- $(a,_i p)[\rho, i = 0] = a\rho$
- $((x : A) \times_i P)[\rho, i = 0] = A\rho$

Interpreting Parametricity constructs (cont.)

$$\frac{\Gamma \vdash a : A\,(i\,0) \qquad \Gamma \vdash p : A \Eparr_i a}{\Gamma, i : \mathbb{I} \vdash (a,_i p) : A} \qquad \frac{\Gamma \vdash A \qquad \Gamma, x : A \vdash P}{\Gamma, i : \mathbb{I} \vdash (x : A) \times_i P}$$

Let $[\rho, i = \varphi] \in \Gamma * \mathbb{I}(I)$. If $\varphi = 0$, we define

- $(a,_i p)[\rho, i = 0] = a\rho$
- $((x : A) \times_i P)[\rho, i = 0] = A\rho$

If $\varphi = j \in I$ then $\rho \in \Gamma(I \backslash \{j\})$, and we define

- $(a,_i p)[\rho, i = j] = (a\rho,_j p\rho)$
- $((x : A) \times_i P)[\rho, i = j] = \left\{(u,_j v) \mid u \in A\rho, v \in P\langle \rho, x = u\rangle\right\}$

Summary

- Syntax with internalized parametricity (better candidate for a core TT with Int. Param. than our previous attempts).
- Each type is associated with as many parametricity predicate as there are of colors.
- “Compute” parametricity types via isomorphisms.
- Haskell evaluator.
- Denotational semantics given by a presheaf model à la Bezem-Coquand-Huber.