MPRI 2.4, Functional programming and type systems
Metatheory of System F

Didier Rémy

November 03, 2017

INRIA

Plan of the course

Metatheory of System F

ADTs, Existential types, GATDs

Logical relations

Messages

Last lesson Friday, November 22

Partial exams on Friday, November 29

- Only course notes and handwritten notes are allowed.
- No electronic devices of any kind.
- Bring you own paper (preferably *double* A4 sheet)

Internships — see the course webpage

- Sharing and Unsharing in Hindley Milner
- Propagation of type annotations in Hindley-Milner based type-systems
- *Verifying Chunked Sequences, by F. Pottier (and A. Charguéraud)*
- *Plus 2 others by Yann Régis Giannas.*

(Talk to me if you are interested)

Logical relations and parametricity

Contents

What are logical relations?

So far, most proofs involving terms have proceeded by induction on the structure of *terms* (or, equivalently, *typing derivations*).

Logical relations are relations between well-typed terms defined inductively on the structure of *types*. They allow proofs between terms by induction on the structure of *types*.

Unary relations

- Unary relations are predicates on expressions
- They can be used to prove type safety and strong normalization

Binary relations

- Binary relations relates two expressions of related types.
- They can be used to prove equivalence of programs and non-interference properties.

Logical relations are a common proof method for programming languages.

Parametricity? *Inhabitants of polymorphic types*

In the presence of polymorphism (and in the absence of effects), a type can reveal a lot of information about the terms that inhabit it.

What can do a term of type $\forall\alpha.\, \alpha \to \mathit{int}$?

?

Parametricity? *Inhabitants of polymorphic types*

In the presence of polymorphism (and in the absence of effects), a type can reveal a lot of information about the terms that inhabit it.

What can do a term of type $\forall\alpha.\,\alpha \to \mathit{int}$?

- the function cannot examine its argument

so ?

Parametricity? *Inhabitants of polymorphic types*

In the presence of polymorphism (and in the absence of effects), a type can reveal a lot of information about the terms that inhabit it.

What can do a term of type $\forall\alpha.\, \alpha \to \mathit{int}$?

- the function cannot examine its argument
- it always return the same integer

for example ?

Parametricity? *Inhabitants of polymorphic types*

In the presence of polymorphism (and in the absence of effects), a type can reveal a lot of information about the terms that inhabit it.

What can do a term of type $\forall \alpha. \alpha \rightarrow$ *int* ?

- the function cannot examine its argument
- it always return the same integer
- $\lambda x. n$,
  $\lambda x. (\lambda y. y)\, n$,
  $\lambda x. (\lambda y. n)\, x$.
  etc.

What do they all have in common ?

Parametricity? *Inhabitants of polymorphic types*

In the presence of polymorphism (and in the absence of effects), a type can reveal a lot of information about the terms that inhabit it.

A term of type $\forall\alpha.\,\alpha \to \mathit{int}$?

- the function cannot examine its argument
- it always return the same integer
- $\lambda x.\,n$,
  $\lambda x.\,(\lambda y.\,y)\;n$,
  $\lambda x.\,(\lambda y.\,n)\;x$.
  etc.
- they are all $\beta\eta$-equivalent to a term of the form $\lambda x.\,n$

Parametricity? *Inhabitants of polymorphic types*

In the presence of polymorphism (and in the absence of effects), a type can reveal a lot of information about the terms that inhabit it.

A term of type $\forall\alpha.\,\alpha \to \mathit{int}$?

- behaves as $\lambda x.\,n$

Parametricity? *Inhabitants of polymorphic types*

In the presence of polymorphism (and in the absence of effects), a type can reveal a lot of information about the terms that inhabit it.

A term of type $\forall\alpha.\,\alpha \to \mathit{int}$?

- behaves as $\lambda x.\,n$

A term a of type $\forall\alpha.\,\alpha \to \alpha$?

?

Parametricity? *Inhabitants of polymorphic types*

In the presence of polymorphism (and in the absence of effects), a type can reveal a lot of information about the terms that inhabit it.

A term of type $\forall\alpha.\,\alpha \to \mathit{int}$?

- behaves as $\lambda x.\,n$

A term a of type $\forall\alpha.\,\alpha \to \alpha$?

- behaves as $\lambda x.\,x$

Parametricity? *Inhabitants of polymorphic types*

In the presence of polymorphism (and in the absence of effects), a type can reveal a lot of information about the terms that inhabit it.

A term of type $\forall\alpha.\,\alpha \to \mathit{int}$?

- behaves as $\lambda x.\,n$

A term a of type $\forall\alpha.\,\alpha \to \alpha$?

- behaves as $\lambda x.\,x$

A term type $\forall\alpha\beta.\,\alpha \to \beta \to \alpha$?

?

Parametricity? *Inhabitants of polymorphic types*

In the presence of polymorphism (and in the absence of effects), a type can reveal a lot of information about the terms that inhabit it.

A term of type $\forall\alpha.\,\alpha \to \textit{int}$?

- behaves as $\lambda x.\,n$

A term a of type $\forall\alpha.\,\alpha \to \alpha$?

- behaves as $\lambda x.\,x$

A term type $\forall\alpha\beta.\,\alpha \to \beta \to \alpha$?

- behaves as $\lambda x.\,\lambda y.\,x$

A term type $\forall\alpha.\,\alpha \to \alpha \to \alpha$?

?

Parametricity? *Inhabitants of polymorphic types*

In the presence of polymorphism (and in the absence of effects), a type can reveal a lot of information about the terms that inhabit it.

A term of type $\forall\alpha.\,\alpha \to \mathit{int}$?

- behaves as $\lambda x.\,n$

A term a of type $\forall\alpha.\,\alpha \to \alpha$?

- behaves as $\lambda x.\,x$

A term type $\forall\alpha\beta.\,\alpha \to \beta \to \alpha$?

- behaves as $\lambda x.\,\lambda y.\,x$

A term type $\forall\alpha.\,\alpha \to \alpha \to \alpha$?

- behaves either as $\lambda x.\,\lambda y.\,x$ or $\lambda x.\,\lambda y.\,y$

Pametricity *Theorems for free*

Similarly, the type of a polymorphic function may also reveal a *"free theorem"* about its behavior!

What properties may we learn from a function

$$\texttt{whoami} \;:\; \forall \alpha.\, \mathit{list}\, \alpha \to \mathit{list}\, \alpha$$

?

Pametricity *Theorems for free*

Similarly, the type of a polymorphic function may also reveal a *"free theorem"* about its behavior!

What properties may we learn from a function

$$\texttt{whoami} : \forall \alpha.\, \mathit{list}\, \alpha \to \mathit{list}\, \alpha$$

- The length of the result depends only on the length of the argument

Pametricity *Theorems for free*

Similarly, the type of a polymorphic function may also reveal a *"free theorem"* about its behavior!

What properties may we learn from a function

$$\texttt{whoami} \;:\; \forall\alpha.\, \mathit{list}\,\alpha \to \mathit{list}\,\alpha$$

- ▷ The length of the result depends only on the length of the argument
- ▷ All elements of the results are elements of the argument

Pametricity *Theorems for free*

Similarly, the type of a polymorphic function may also reveal a *"free theorem"* about its behavior!

What properties may we learn from a function

$$\texttt{whoami} \;:\; \forall \alpha.\, \mathit{list}\, \alpha \to \mathit{list}\, \alpha$$

- ▷ The length of the result depends only on the length of the argument
- ▷ All elements of the results are elements of the argument
- ▷ The choice (i, j) of pairs such that i-th element of the result is the j-th element of the argument does not depend on the element itself.

Pametricity *Theorems for free*

Similarly, the type of a polymorphic function may also reveal a *"free theorem"* about its behavior!

What properties may we learn from a function

$$\texttt{whoami} \;:\; \forall \alpha.\, \mathit{list}\, \alpha \to \mathit{list}\, \alpha$$

- ▷ The length of the result depends only on the length of the argument
- ▷ All elements of the results are elements of the argument
- ▷ The choice (i, j) of pairs such that i-th element of the result is the j-th element of the argument does not depend on the element itself.
- ▷ the function is preserved by a transformation of its argument that preserves the shape of the argument

$$\forall f, x, \quad \texttt{whoami}\;(map\; f\; x) = map\; f\; (\texttt{whoami}\; x)$$

Pametricity *Theorems for free*

Similarly, the type of a polymorphic function may also reveal a *"free theorem"* about its behavior!

What properties may we learn from a function

$$\texttt{whoami} \; : \; \forall\alpha.\, \mathit{list}\,\alpha \to \mathit{list}\,\alpha$$

What property may we learn for the list sorting function?

$$\mathit{sort} \; : \; \forall\alpha.\, (\alpha \to \alpha \to \mathit{bool}) \to \mathit{list}\,\alpha \to \mathit{list}\,\alpha$$

?

Pametricity *Theorems for free*

Similarly, the type of a polymorphic function may also reveal a *"free theorem"* about its behavior!

What properties may we learn from a function

$$\texttt{whoami} \;:\; \forall\alpha.\, \mathit{list}\,\alpha \to \mathit{list}\,\alpha$$

What property may we learn for the list sorting function?

$$\mathit{sort} \;:\; \forall\alpha.\, (\alpha \to \alpha \to \mathit{bool}) \to \mathit{list}\,\alpha \to \mathit{list}\,\alpha$$

If f is order-preserving, then sorting commutes with $map\ f$

$$(\forall x, y,\;\; \mathit{cmp}\,(f\ x)\,(f\ y) = \mathit{cmp}\ \ x\ y) \implies \\ \forall \ell,\;\; \mathit{sort}\ \ \mathit{cmp}\,(\mathit{map}\ f\ \ell) = \mathit{map}\ f\ \,(\mathit{sort}\ \mathit{cmp}\,\ell)$$

Pametricity *Theorems for free*

Similarly, the type of a polymorphic function may also reveal a *"free theorem"* about its behavior!

What properties may we learn from a function

$$\texttt{whoami} \;:\; \forall\alpha.\, \mathit{list}\,\alpha \to \mathit{list}\,\alpha$$

What property may we learn for the list sorting function?

$$\mathit{sort} \;:\; \forall\alpha.\,(\alpha \to \alpha \to \mathit{bool}) \to \mathit{list}\,\alpha \to \mathit{list}\,\alpha$$

If f is order-preserving, then sorting commutes with $map\ f$

$$(\forall x, y,\ \ \mathit{cmp}_2\ (f\ x)\ (f\ y) = \mathit{cmp}_1\ \ x\ y) \implies$$
$$\forall \ell,\ \ \mathit{sort}\ \ \mathit{cmp}_2\ (\mathit{map}\ f\ \ell) = \mathit{map}\ f\ (\mathit{sort}\ \mathit{cmp}_1\ \ell)$$

Pametricity *Theorems for free*

Similarly, the type of a polymorphic function may also reveal a *"free theorem"* about its behavior!

What properties may we learn from a function

$$\texttt{whoami} \;:\; \forall\alpha.\, \mathit{list}\,\alpha \to \mathit{list}\,\alpha$$

What property may we learn for the list sorting function?

$$\mathit{sort} \;:\; \forall\alpha.\, (\alpha \to \alpha \to \mathit{bool}) \to \mathit{list}\,\alpha \to \mathit{list}\,\alpha$$

If f is order-preserving, then sorting commutes with $map\ f$

$$(\forall x, y,\;\; \mathit{cmp}_2\ (f\ x)\ (f\ y) = \mathit{cmp}_1\ \ x\ y) \implies \\ \forall \ell,\;\; \mathit{sort}\ \ \mathit{cmp}_2\ (\mathit{map}\ f\ \ell) = \mathit{map}\ f\ (\mathit{sort}\ \mathit{cmp}_1\ \ell)$$

Application:

- If *sort* is correct on lists of integers, then it is correct on any list
- May be useful to reduce testing.

Pametricity *Theorems for free*

Similarly, the type of a polymorphic function may also reveal a *"free theorem"* about its behavior!

What properties may we learn from a function

$$\texttt{whoami} \;:\; \forall\alpha.\, \mathit{list}\,\alpha \to \mathit{list}\,\alpha$$

What property may we learn for the list sorting function?

$$\mathit{sort} \;:\; \forall\alpha.\,(\alpha \to \alpha \to \mathit{bool}) \to \mathit{list}\,\alpha \to \mathit{list}\,\alpha$$

If f is order-preserving, then sorting commutes with $map\ f$

$$(\forall x, y,\ \ \mathit{cmp}_2\ (f\ x)\ (f\ y) = \mathit{cmp}_1\ \ x\ y) \implies$$
$$\forall \ell,\ \ \mathit{sort}\ \ \mathit{cmp}_2\ (\mathit{map}\ f\ \ell) = \mathit{map}\ f\ (\mathit{sort}\ \mathit{cmp}_1\ \ell)$$

Note that there are many other inhabitants of this type, but they all satisfy this free theorem.

Can you give a few?

Pametricity *Theorems for free*

Similarly, the type of a polymorphic function may also reveal a *"free theorem"* about its behavior!

What properties may we learn from a function

$$\texttt{whoami} \;:\; \forall\alpha.\, \mathit{list}\,\alpha \to \mathit{list}\,\alpha$$

What property may we learn for the list sorting function?

$$\mathit{sort} \;:\; \forall\alpha.\, (\alpha \to \alpha \to \mathit{bool}) \to \mathit{list}\,\alpha \to \mathit{list}\,\alpha$$

If f is order-preserving, then sorting commutes with $map\ f$

$$(\forall x, y,\;\; \mathit{cmp}_2\ (f\ x)\ (f\ y) = \mathit{cmp}_1\ \ x\ y) \implies \forall \ell,\;\; \mathit{sort}\ \ \mathit{cmp}_2\ (\mathit{map}\ f\ \ell) = \mathit{map}\ f\ (\mathit{sort}\ \mathit{cmp}_1\ \ell)$$

Note that there are many other inhabitants of this type, but they all satisfy this free theorem. (e.g., a function that sorts in reverse order, or a function that removes (or adds) duplicates).

Parametricity

This phenomenon was studied by Reynolds [1983] and by Wadler [1989; 2007], among others. Wadler's paper contains the 'free theorem' about the list sorting function.

An account based on an operational semantics is offered by Pitts [2000].

Bernardy et al. [2010] generalize the idea of testing polymorphic functions to arbitrary polymorphic types and show how testing any function can be restricted to testing it on (possibly infinitely many) particular values at some particular types.

Contents

Normalization of simply-typed λ-calculus

Types usually ensure termination of programs—as long as neither types nor terms contain any form of recursion.

Normalization of simply-typed λ-calculus

Types usually ensure termination of programs—as long as neither types nor terms contain any form of recursion.

Even if one wishes to add recursion explicitly later on, it is an important property of the design that non-termination is originating from the constructions introduced especially for recursion and could not occur without them.

Normalization of simply-typed λ-calculus

Types usually ensure termination of programs—as long as neither types nor terms contain any form of recursion.

Even if one wishes to add recursion explicitly later on, it is an important property of the design that non-termination is originating from the constructions introduced especially for recursion and could not occur without them.

The simply-typed λ-calculus is also lifted at the level of types in richer type systems such as System F^ω; then, the decidability of type-equality depends on the termination of the reduction at the type level.

Normalization of simply-typed λ-calculus

Types usually ensure termination of programs—as long as neither types nor terms contain any form of recursion.

Even if one wishes to add recursion explicitly later on, it is an important property of the design that non-termination is originating from the constructions introduced especially for recursion and could not occur without them.

The simply-typed λ-calculus is also lifted at the level of types in richer type systems such as System F^ω; then, the decidability of type-equality depends on the termination of the reduction at the type level.

The proof of termination for the simply-typed λ-calculus is a simple and illustrative use of logical relations.

Notice however, that our simply-typed λ-calculus is equipped with a call-by-value semantics. Proofs of termination are usually done with a strong evaluation strategy where reduction can occur in any context.

Normalization

Proving termination of reduction in fragments of the λ-calculus is often a difficult task because reduction may create new redexes or duplicate existing ones.

Hence the size of terms may grow (much) larger during reduction. The difficulty is to find some underlying structure that decreases.

We follow the proof schema of Pierce [2002], which is a modern presentation in a call-by-value setting of an older proof by Hindley and Seldin [1986]. The proof method is due to [Tait, 1967].

Calculus

Take the call-by-value λ_{st} with primitive booleans and conditional.

Write B the type of booleans and tt and ff for *true* and *false*.

We define $\mathcal{V}[\![\tau]\!]$ and $\mathcal{E}[\![\tau]\!]$ the subsets of closed values and closed expressions of (ground) type τ by induction on types as follows:

$$
\begin{aligned}
\mathcal{V}[\![\mathsf{B}]\!] &\triangleq \{\mathsf{tt}, \mathsf{ff}\} \\
\mathcal{V}[\![\tau_1 \to \tau_2]\!] &\triangleq \{\lambda x{:}\tau_1.\, M \mid \lambda x{:}\tau_1.\, M : \tau_1 \to \tau_2 \\
&\qquad\qquad \wedge \forall V \in \mathcal{V}[\![\tau_1]\!],\ (\lambda x{:}\tau_1.\, M)\ V \in \mathcal{E}[\![\tau_2]\!]\} \\
\mathcal{E}[\![\tau]\!] &\triangleq \{M \mid M : \tau \wedge \exists V \in \mathcal{V}[\![\tau]\!], M \Downarrow V\}
\end{aligned}
$$

We write $M \Downarrow V$ for $M \longrightarrow^* V$.
The goal is to show that any closed expression of type τ is in $\mathcal{E}[\![\tau]\!]$.

Remarks

$\mathcal{V}[\![\tau]\!] \subseteq \mathcal{E}[\![\tau]\!]$—by definition.
$\mathcal{E}[\![\tau]\!]$ is closed by inverse reduction—by definition, *i.e.*
If $M : \tau$ and $M \longrightarrow N$ and $N \in \mathcal{E}[\![\tau]\!]$ then $M \in \mathcal{E}[\![\tau]\!]$.

Problem

We wish to show that every closed term of type τ is in $\mathcal{E}[\![\tau]\!]$

- Proof by induction on the typing derivation.
- Problem with abstraction: the premise is not closed.

We need to strengthen the hypothesis, *i.e.* also give a semantics to open terms.

- The semantics of open terms can be given by abstracting over the semantics of their free variables.

Generalize the definition to open terms

We define a semantic judgment for open terms $\Gamma \vDash M : \tau$ so that $\Gamma \vdash M : \tau$ implies $\Gamma \vDash M : \tau$ and $\varnothing \vDash M : \tau$ means $M \in \mathcal{E}[\![\tau]\!]$.

We interpret free term variables of type τ as *closed values* in $\mathcal{V}[\![\tau]\!]$.

We interpret environments Γ as *closing substitutions* γ, *i.e.* mappings from term variables to *closed values*:

We write $\gamma \in \mathcal{G}[\![\Gamma]\!]$ to mean $\mathrm{dom}(\gamma) = \mathrm{dom}(\Gamma)$ and $\gamma(x) \in \mathcal{V}[\![\tau]\!]$ for all $x : \tau \in \Gamma$.

$$\Gamma \vDash M : \tau \overset{\text{def}}{\iff} \forall \gamma \in \mathcal{G}[\![\Gamma]\!],\ \gamma(M) \in \mathcal{E}[\![\tau]\!]$$

Fundamental Lemma

Theorem (fundamental lemma)
If $\Gamma \vdash M : \tau$ then $\Gamma \vDash M : \tau$.

Corollary (termination of well-typed terms):
If $\varnothing \vdash M : \tau$ then $M \in \mathcal{E}[\![\tau]\!]$.

That is, closed well-typed terms of type τ evaluates to values of type τ.

Proof by induction on the typing derivation

Routine cases

Case $\Gamma \vdash \mathsf{tt} : \mathsf{B}$ *or* $\Gamma \vdash \mathsf{ff} : \mathsf{B}$: by definition, $\mathsf{tt}, \mathsf{ff} \in \mathcal{V}[\![\mathsf{B}]\!]$ and $\mathcal{V}[\![\mathsf{B}]\!] \subseteq \mathcal{E}[\![\mathsf{B}]\!]$.

Case $\Gamma \vdash x : \tau$: $\gamma \in \mathcal{G}[\![\Gamma]\!]$, thus $\gamma(x) \in \mathcal{V}[\![\tau]\!] \subseteq \mathcal{E}[\![\tau]\!]$

Case $\Gamma \vdash M_1\ M_2 : \tau$:

By inversion, $\Gamma \vdash M_1 : \tau_2 \to \tau$ and $\Gamma \vdash M_2 : \tau_2$.

Let $\gamma \in \mathcal{G}[\![\Gamma]\!]$. We have $\gamma(M_1\ M_2) = (\gamma M_1)\ (\gamma M_2)$.
By IH, we have $\Gamma \vDash M_1 : \tau_2 \to \tau$ and $\Gamma \vDash M_2 : \tau_2$.
Thus $\gamma M_1 \in \mathcal{E}[\![\tau_2 \to \tau]\!]$ $(\mathbf{1})$ and $\gamma M_2 \in \mathcal{E}[\![\tau_2]\!]$ $(\mathbf{2})$.

By (2), there exists $V \in \mathcal{V}[\![\tau_2]\!]$ such that $\gamma M_2 \Downarrow V$.
Thus $(\gamma M_1)\ (\gamma M_2) \rightsquigarrow (\gamma M_1)\ V \in \mathcal{E}[\![\tau]\!]$ by (1).

Then, $(\gamma M_1)\ (\gamma M_2) \in \mathcal{E}[\![\tau]\!]$, by closure by inverse reduction.

Case $\Gamma \vdash$ *if* M *then* M_1 *else* $M_2 : \tau$: By cases on the evaluation of γM.

Proof by induction on the typing derivation

The interesting case

Case $\Gamma \vdash \lambda x{:}\tau_1.\, M : \tau_1 \rightarrow \tau$:

Assume $\gamma \in \mathcal{G}[\![\Gamma]\!]$.
We must show that $\gamma(\lambda x{:}\tau_1.\, M) \in \mathcal{E}[\![\tau_1 \rightarrow \tau]\!]$ (1)

That is, $\lambda x{:}\tau_1.\, \gamma M \in \mathcal{V}[\![\tau_1 \rightarrow \tau]\!]$ (we may assume $x \notin \mathrm{dom}(\gamma)$ *w.l.o.g.*)

Let $V \in \mathcal{V}[\![\tau_1]\!]$, it suffices to show $(\lambda x{:}\tau_1.\, \gamma M)\ V \in \mathcal{E}[\![\tau]\!]$ (2).

We have $(\lambda x{:}\tau_1.\, \gamma M)\ V \longrightarrow (\gamma M)[x \mapsto V] = \gamma' M$
where γ' is $\gamma[x \mapsto V] \in \mathcal{G}[\![\Gamma, x : \tau_1]\!]$ (3)

Since $\Gamma, x : \tau_1 \vdash M : \tau$, we have $\Gamma, x : \tau_1 \vDash M : \tau$ by IH. Therefore by (3), we have $\gamma' M \in \mathcal{E}[\![\tau]\!]$. Since $\mathcal{E}[\![\tau]\!]$ is closed by inverse reduction, this proves (2) which finishes the proof of (1).

Variations

We have shown both *termination* and *type soundness*, simultaneously.

Termination would not hold if we had a fix point. But type soundness would still hold.

The proof may be modified by choosing:

$$\mathcal{E}[\![\tau]\!] = \{M : \tau \mid \forall N, M \Downarrow N \implies N \in \mathcal{V}[\![\tau]\!] \ \vee\ \exists N', N \longrightarrow N'\}$$

Exercise

Show type soundness with this semantics.

Contents

(Bibliography)

Mostly following Bob Harper's course notes *Practical foundations for programming languages* [Harper, 2012].

See also

- *Types, Abstraction and Parametric Polymorphism* [Reynolds, 1983]
- *Parametric Polymorphism and Operational Equivalence* [Pitts, 2000].
- *Theorems for free!* [Wadler, 1989].

We assume a call-by-name semantics for generality of the presentation, but all results also apply to a call-by-value semantics.

When are two programs equivalent

$M \Downarrow N$?

$M \Downarrow V$ and $N \Downarrow V$?

But what if M and N are functions?

Aren't $\lambda x.\,(x + x)$ and $\lambda x.\,2 * x$ equivalent?

Idea

?

When are two programs equivalent

$M \Downarrow N$?

$M \Downarrow V$ and $N \Downarrow V$?

But what if M and N are functions?

Aren't $\lambda x.(x + x)$ and $\lambda x. 2 * x$ equivalent?

Idea two functions are observationally equivalent if when applied to *equivalent arguments*, they lead to observationally *equivalent results*.

Are we general enough?

Observational equivalence

We can only *observe* the behavior of full *programs*, *i.e.* closed terms of some computation type, such as B (the only one so far).

If $M : \mathsf{B}$ and $N : \mathsf{B}$, then $M \simeq N$ iff there exists V such that $M \Downarrow V$ and $N \Downarrow V$. (Call $M \simeq N$ *behavioral equivalence*.)

To compare programs at other types, we

?

Observational equivalence

We can only *observe* the behavior of full *programs*, *i.e.* closed terms of some computation type, such as B (the only one so far).

If $M : \mathsf{B}$ and $N : \mathsf{B}$, then $M \simeq N$ iff there exists V such that $M \Downarrow V$ and $N \Downarrow V$. (Call $M \simeq N$ *behavioral equivalence*.)

To compare programs at other types, we place them in arbitrary *closing* contexts.

Definition (observational equivalence)

$$\Gamma \vdash M \cong N : \tau \;\stackrel{\triangle}{=}\; \forall \mathcal{C} : (\Gamma \rhd \tau) \leadsto (\varnothing \rhd \mathsf{B}),\, \mathcal{C}[M] \simeq \mathcal{C}[N]$$

Typing of contexts

$$\mathcal{C} : (\Gamma \rhd \tau) \leadsto (\Delta \rhd \sigma) \iff (\forall M,\; \Gamma \vdash M : \tau \implies \Delta \vdash \mathcal{C}[M] : \sigma)$$

There is an equivalent definition given by a set of typing rules. This is needed to prove some properties by induction on the typing derivations.

We write $M \cong_\tau N$ for $\varnothing \vdash M \cong N : \tau$

Observational equivalence

Observational equivalence is the coarsest consistent congruence, where:

- $\equiv$ is consistent if $\varnothing \vdash M \equiv N : \mathsf{B}$ implies $M \simeq N$.
- $\equiv$ is a congruence if it is an equivalence and is closed by context, *i.e.*

$$\Gamma \vdash M \equiv N : \tau \;\wedge\; \mathcal{C} : (\Gamma \triangleright \tau) \rightsquigarrow (\Delta \triangleright \sigma) \quad \Longrightarrow \quad \Delta \vdash \mathcal{C}[M] \equiv \mathcal{C}[N] : \sigma$$

Consistent: by definition, using the empty context.

Congruence: by compositionality of contexts.

Largest: Assume $\equiv$ is a consistent congruence. Assume $\Gamma \vdash M \equiv N : \tau$ holds and show that $\Gamma \vdash M \cong N : \tau$ holds (1).
Let $\mathcal{C} : (\Gamma \triangleright \tau) \rightsquigarrow (\varnothing \triangleright \mathsf{B})$ (2). We must show that $\mathcal{C}[M] \simeq \mathcal{C}[N]$.
This follows by consistency applied to $\Gamma \vdash \mathcal{C}[M] \equiv \mathcal{C}[N] : \mathsf{B}$ which follows by congruence from (1) and (2).

Problem with Observational Equivalence

Problems

- Observational equivalence is too difficult to test.
- Because of quantification over all contexts (too many for testing).
- But many contexts will do the same experiment.

Solution

We take advantage of types to reduce the number of experiments.

- Defining/testing the equivalence on base types.
- Propagating the definition mechanically at other types.

Logical relations provide the infrastructure for conducting such proofs.

Contents

Logical equivalence for closed terms

We inductively define $M \sim_\tau M'$ on closed terms of (ground) type τ by induction on τ:

- $M \sim_{\mathsf{B}} M'$ iff $M \simeq M'$
- $M \sim_{\tau_1 \to \tau_2} M'$ iff $\forall M_1, M_1', \;\; M_1 \sim_{\tau_1} M_1' \implies M\ M_1 \sim_{\tau_2} M'\ M_1'$

Lemma

Logical equivalence is symmetric and transitive (at any given type).

Note

Reflexivity is not obvious at all.

Logical equivalence for closed terms

Proof by induction on type τ

Case τ is B *for values*: the result is immediate.

Case τ is $\tau_1 \to \tau_2$:. By IH, symmetry and transitivity hold at types τ_1 and τ_2.

For symmetry, assume $M \sim_\tau M'$ (H), we must show $M' \sim_\tau M$. Assume $M_1 \sim_{\tau_1} M_1'$. We must show $M'\ M_1 \sim_{\tau_2} M\ M_1'$ (C). We have $M_1' \sim_{\tau_1} M_1$ by symmetry at τ_1. By (H), we have $M\ M_1' \sim_{\tau_2} M'\ M_1$ and (C) follows by symmetry at type τ_2.

For transitivity, assume $M \sim_\tau M'$ (H1) and $M' \sim_\tau M''$ (H2). To show $M \sim_\tau M''$, we assume $N \sim_{\tau_1} N''$ and show $M\ N \sim_{\tau_2} M''\ N''$ (C).
By (H1), we have $M\ N \sim_{\tau_2} M'\ N''$ (C1).
By symmetry and transitivity at type τ_1, we get $N'' \sim_{\tau_1} N''$. (Remark)
By (H2), we have $M'\ N'' \sim_{\tau_2} M''\ N''$ (C2).
(C) follows by transitivity of (C1) and (C2) at type τ_2.

Properties of logical equivalence

Closure by inverse reduction

Assume that $N : \tau$ and $M \sim_\tau M'$.
If $N \Downarrow M$ and $N' \Downarrow M'$ then $N \sim_\tau N'$.

The proof is by induction on τ.
(We show it for a single reduction step, *e.g.* on the left-hand side)

Case τ is B: By closure of behavioral equivalence $\simeq$ by inverse reduction.

Case τ is $\tau_1 \to \tau_2$: To show $N \sim_\tau M'$ we assume $M_1 \sim_{\tau_1} M_1'$ and show $N\ M_1 \sim_{\tau_2} M'\ M_1'$ (1).
From $M \sim_\tau M'$, we have $M\ M_1 \sim_{\tau_2} M'\ M_1'$. The conclusion (1) then follows by IH at type τ_2, since we have $N\ M_1 \longrightarrow M\ M_1$ as a consequence of the assumption $N \longrightarrow M$.

Consistency If $M \sim_{\mathrm{B}} M'$, then $M \simeq M'$

(Obvious, by definition.)

Logical equivalence for open terms

When $\Gamma \vdash M : \tau$ and $\Gamma \vdash M' : \tau$, we wish to define a judgment $\Gamma \vdash M \sim M' : \tau$ to mean that the open terms M and M' are equivalent at type τ.

We write $\gamma \sim_\Gamma \gamma'$ to mean that γ and γ' are two substitutions of domain $\mathrm{dom}(\Gamma)$ such that for all $x : \tau \in \mathrm{dom}(\Gamma)$, we have $\gamma(x) \sim_\tau \gamma'(x)$

Definition

$$\Gamma \vdash M \sim M' : \tau \iff \forall \gamma, \gamma',\ \gamma \sim_\Gamma \gamma' \implies \gamma(M) \sim_\tau \gamma'(M')$$

We write $M \sim_\tau N$ for $\varnothing \vdash M \sim N : \tau$

Immediate properties

Open logical equivalence is symmetric and transitive.

(Proof is immediate by the definition and the symmetry and transitivity of closed logical equivalence.)

Fundamental lemma of logical equivalence

Theorem (Reflexivity)

If $\Gamma \vdash M : \tau$, *then* $\Gamma \vdash M \sim M : \tau$.

Proof Assume $\Gamma \vdash M : \tau$ $(\mathbf{1})$ and $\gamma \sim_\Gamma \gamma'$ $(\mathbf{2})$. We must show $\gamma M \sim_\tau \gamma' M$. The proof is by induction on the typing derivation.

Case M is $\lambda x{:}\tau_1.\, N$ and τ is $\tau_1 \to \tau_2$ with $x \,\#\, \gamma, \gamma'$:
We show $\lambda x{:}\tau_1.\, \gamma N \sim_{\tau_1 \to \tau_2} \lambda x{:}\tau_1.\, \gamma' N$. Assume $M_1 \sim_{\tau_1} M_1'$ $(\mathbf{3})$.
We must show $(\lambda x{:}\tau_1.\, \gamma N)\; M_1 \sim_{\tau_2} (\lambda x{:}\tau_1.\, \gamma' N)\; M_1'$.

By inverse reduction, it suffices to show
$\gamma(N)[x \mapsto M_1] \sim_{\tau_2} \gamma'(N)[x \mapsto M_1']$, *i.e.*
$\gamma_1(N) \sim_{\tau_2} \gamma_1'(N)$ where γ_1 is $(\gamma[x \mapsto M_1])$ and γ_1' is $(\gamma'[x \mapsto M_1'])$ $(\mathbf{4})$.

We have $\gamma_1 \sim_{\Gamma, x:\tau_1} \gamma_1'$ $(\mathbf{5})$ from (2) and (3).
By inversion of typing applied to (1), we have $\Gamma, x : \tau_1 \vdash N : \tau_2$.
Thus (4) follows by induction hypothesis applied with (5).

Properties of logical equivalence

Proof (continued) Assume $\Gamma \vdash M : \tau$ and $\gamma \sim_\Gamma \gamma'$. We must show $\gamma(M) \sim_\tau \gamma'(M)$. The proof is by induction on the typing derivation.

Case M is tt *or* ff *and τ is* B: Since M is closed it suffices to show $M \sim_{\mathsf{B}} M$ which holds by reflexivity of $\sim_{\mathsf{B}}$, *i.e.* of behavioral equivalence $\simeq$.

Case M is $M_1\ M_2$: By induction hypothesis and the fact that substitution distributes over term application.

Case M is x: Immediate.

Properties of logical equivalence

Proof (continued)

Case M is if N then N_1 else N_2: By induction applied to $\Gamma \vdash N : \mathsf{B}$, we have $\Gamma \vdash N \sim N : \mathsf{B}$. Thus $\gamma N \sim_{\mathsf{B}} \gamma' N$. By consistency, we have $\gamma N \simeq \gamma' N$. *We then reason by cases on the evaluation of γN.*

If $\gamma N \Downarrow \mathsf{tt}$ then so does $\gamma' N$; then $\gamma M \Downarrow \gamma N_1$ and $\gamma' M \Downarrow \gamma' N_1$. We have $\Gamma \vdash N_1 : \tau$ by inversion of typing. By IH, we have $\gamma N_1 \sim_\tau \gamma' N_1$. By inverse reduction, we get $\gamma M \sim_\tau \gamma' M$.

Otherwise, $\gamma N \Downarrow \mathsf{ff}$, and we proceed symmetrically.

Properties of logical relations

Corollary (equivalence) Open logical relation is an equivalence relation

Corollary (Termination) If $M : \mathsf{B}$ then the evaluation of M terminates.

Proof: $M : \mathsf{B}$ implies $M \sim_{\mathsf{B}} M$ which implies $M \simeq M$, and, in turn, implies that M evaluates to either tt or ff.

Properties of logical equivalence

Logical equivalence is a congruence
If $\Gamma \vdash M \sim M' : \tau$ and $\mathcal{C} : (\Gamma \rhd \tau) \rightsquigarrow (\Delta \rhd \sigma)$, then
$\Delta \vdash \mathcal{C}[M] \sim \mathcal{C}[M'] : \sigma$.

Proof By induction on the proof of $\mathcal{C} : (\Gamma \rhd \tau) \rightsquigarrow (\Delta \rhd \sigma)$.
Similar to the proof of reflexivity. *(We need a definition of context typing derivations by a set of typing rules to be able to reason by induction on the typing derivation.)*

Corollary Logical equivalence implies observational equivalence.
If $\Gamma \vdash M \sim M' : \tau$ then $\Gamma \vdash M \cong M' : \tau$.

Proof: Logical equivalence is a consistent congruence, hence included in observational equivalence which is the coarsest such relation.

Properties of logical equivalence

Lemma
Observational equivalence of closed terms implies logical equivalence.
If $M \cong_\tau M'$ then $M' \sim_\tau M'$.

Proof by induction on τ.

Case τ is B: In the empty context, we have $M \simeq_{\mathsf{B}} M'$, hence $M \sim_{\mathsf{B}} M'$.

Case τ is $\tau_1 \to \tau_2$: By congruence of observational equivalence. To show $M \sim_\tau M'$, we assume $M_1 \sim_{\tau_1} M_1'$ $(\mathbf{1})$ and show $M\ M_1 \sim_{\tau_2} M'\ M_1$. By IH, it suffices to show $M\ M_1 \cong_{\tau_2} M'\ M_1$. This follows by congruence, from the hypothesis $M \cong_\tau M'$ and $M_1 \cong_{\tau_1} M_1'$ which follows from (1) by the previous lemma.

Properties of logical equivalence

Corollary (Value arguments)

To show $M \sim_{\tau_1 \to \tau_2} M'$, it suffices to show that $M\ V \sim_{\tau_2} M'\ V'$ for all values V and V' such that $V \sim_{\tau_1} V'$.

Proof

Assume $N \sim_{\tau_1} N'$.
There exists V and V' such that $N \Downarrow V$ and $N' \Downarrow V'$.
It suffices to show that $M\ V \sim_{\tau_2} M'\ V'$ (H) implies $M\ N \sim_{\tau_2} M'\ N'$ $(\mathbf{1})$.

We have $N \sim_{\tau_1} V$ from $N \Downarrow V$ and *closure by inverse reduction*.
Then $M\ N \sim_{\tau_2} M\ V$ follows by *congruence* of $\sim_{\tau_2}$
Similarly, we have $M'\ N' \sim_{\tau_2} M'\ V'$.

The conclusion (1) follows by transitivity of $\sim_{\tau_2}$ with (H).

Logical equivalence: application

Assume $not \triangleq \lambda x{:}\mathsf{B}.\,\mathsf{if}\ x\ \mathsf{then}\ \mathsf{ff}\ \mathsf{else}\ \mathsf{tt}$
and $M \triangleq \lambda x{:}\mathsf{B}.\,\lambda y{:}\tau.\,\lambda z{:}\tau.\,\mathsf{if}\ not\ x\ \mathsf{then}\ y\ \mathsf{else}\ z$
and $M' \triangleq \lambda x{:}\mathsf{B}.\,\lambda y{:}\tau.\,\lambda z{:}\tau.\,\mathsf{if}\ x\ \mathsf{then}\ z\ \mathsf{else}\ y$

Show that $M \cong_{\mathsf{B}\to\tau\to\tau\to\tau} M'$ (C).

?

Logical equivalence: application

Assume $not \triangleq \lambda x{:}\mathsf{B}.\,\mathsf{if}\ x\ \mathsf{then\ ff\ else\ tt}$
and $M \triangleq \lambda x{:}\mathsf{B}.\,\lambda y{:}\tau.\,\lambda z{:}\tau.\,\mathsf{if}\ not\ x\ \mathsf{then}\ y\ \mathsf{else}\ z$
and $M' \triangleq \lambda x{:}\mathsf{B}.\,\lambda y{:}\tau.\,\lambda z{:}\tau.\,\mathsf{if}\ x\ \mathsf{then}\ z\ \mathsf{else}\ y$

Show that $M \cong_{\mathsf{B}\to\tau\to\tau\to\tau} M'$ (C).

It suffices to show $M\ V_0\ V_1\ V_2 \sim_\tau M'\ V_0'\ V_1'\ V_2'$ whenever $V_0 \sim_{\mathsf{B}} V_0'$ and $V_1 \sim_\tau V_1'$ and $V_2 \sim_\tau V_2'$.

?

Logical equivalence: application

Assume $not \triangleq \lambda x{:}\mathsf{B}.\, \text{if } x \text{ then ff else tt}$
and $M \triangleq \lambda x{:}\mathsf{B}.\, \lambda y{:}\tau.\, \lambda z{:}\tau.\, \text{if } not\ x \text{ then } y \text{ else } z$
and $M' \triangleq \lambda x{:}\mathsf{B}.\, \lambda y{:}\tau.\, \lambda z{:}\tau.\, \text{if } x \text{ then } z \text{ else } y$

Show that $M \cong_{\mathsf{B}\to\tau\to\tau\to\tau} M'$ (C).

It suffices to show $M\ V_0\ V_1\ V_2 \sim_\tau M'\ V_0'\ V_1'\ V_2'$ whenever $V_0 \sim_{\mathsf{B}} V_0'$ and $V_1 \sim_\tau V_1'$ and $V_2 \sim_\tau V_2'$.

By inverse reduction, it suffices to show

$$\text{if } not\ V_0 \text{ then } V_1 \text{ else } V_2 \quad \sim_\tau \quad \text{if } V_0' \text{ then } V_2' \text{ else } V_1'$$

?

Logical equivalence: application

Assume $not \triangleq \lambda x{:}\mathsf{B}.\,\mathsf{if}\ x\ \mathsf{then\ ff\ else\ tt}$
and $M \triangleq \lambda x{:}\mathsf{B}.\,\lambda y{:}\tau.\,\lambda z{:}\tau.\,\mathsf{if}\ not\ x\ \mathsf{then}\ y\ \mathsf{else}\ z$
and $M' \triangleq \lambda x{:}\mathsf{B}.\,\lambda y{:}\tau.\,\lambda z{:}\tau.\,\mathsf{if}\ x\ \mathsf{then}\ z\ \mathsf{else}\ y$

Show that $M \cong_{\mathsf{B}\to\tau\to\tau\to\tau} M'$ (C).

It suffices to show $M\ V_0\ V_1\ V_2 \sim_\tau M'\ V_0'\ V_1'\ V_2'$ whenever $V_0 \sim_{\mathsf{B}} V_0'$ and $V_1 \sim_\tau V_1'$ and $V_2 \sim_\tau V_2'$.

By inverse reduction, it suffices to show

$$\mathsf{if}\ not\ V_0\ \mathsf{then}\ V_1\ \mathsf{else}\ V_2 \quad \sim_\tau \quad \mathsf{if}\ V_0'\ \mathsf{then}\ V_2'\ \mathsf{else}\ V_1'$$

By cases on V_0.

Case V_0 is tt: Then $not\ V_0 \Downarrow \mathsf{ff}$ and thus $M \Downarrow V_2$ while $M' \Downarrow V_2$. Then (C) follows by inverse reduction and $V_2 \sim_\tau V_2'$.

Case V_0 is ff: is symmetric.

Contents

Observational equivalence

We now extend the notion of logical equivalence to System F.

$$\tau ::= \ldots \mid \alpha \mid \forall \alpha.\, \tau \qquad\qquad M ::= \ldots \mid \Lambda \alpha. M \mid M\ \tau$$

We write typing contexts $\Delta; \Gamma$ where Δ binds variables and Γ binds program variables.

Typing of contexts becomes $\mathcal{C} : (\Delta; \Gamma \rhd \tau) \rightsquigarrow (\Delta'; \Gamma' \rhd \tau')$.

Observational equivalence

We defined $\Delta; \Gamma \vdash M \cong M' : \tau$ as

$$\forall \mathcal{C} : (\Delta; \Gamma \rhd \tau) \rightsquigarrow (\varnothing; \varnothing \rhd \mathsf{B}),\ \ \mathcal{C}[M] \simeq \mathcal{C}[M']$$

As before, write $M \cong_\tau N$ for $\varnothing; \varnothing \vdash M \cong N : \tau$ (in particular, τ is closed).

Logical equivalence

For closed terms (no free program variables)

- We need to give the semantics of polymoprhic types $\forall\alpha.\tau$
- Problem: We cannot do it in terms of the semantics of instances $\tau[\alpha \mapsto \sigma]$ since the semantics is defined by induction on types.
- Solution: we give the semantics of terms with open types—in some suitable environment that interprets type variables by logical relations.

For simple types, we defined logical relations and observed that

- they respect observational equivalence
- they are closed by inverse reduction

We require that relations used to interpret type variables satisfy those properties.

Logical equivalence

Definition A relation R between closed expressions of closed types ρ and ρ' is admissible, and we write $R : \rho \leftrightarrow \rho'$, if:

- It respects observational equivalence: If $R(M, M')$ and $N \cong_\rho M$ and $N' \cong_{\rho'} M'$, then $R(N, N')$.
- It is closed under inverse reduction: If $R(M, M')$ and $N \Downarrow M$ and $N' \Downarrow M'$, then $R(N, N')$.

Given a sequence of type variables Δ, let δ and δ' be maps from $\mathrm{dom}(\Delta)$ to closed types and let η be a map from $\mathrm{dom}(\Delta)$ that sends each type variable α to an admissible relation between values of closed types $\delta(\alpha)$ and $\delta'(\alpha)$. We write $\eta : \delta \leftrightarrow_\Delta \delta'$ for such a relation, but often leave Δ implicit.

Example of admissible relations

Take

$$\Delta \triangleq \alpha \qquad \delta \triangleq \alpha \mapsto \mathsf{B} \qquad \delta' \triangleq \alpha \mapsto \mathbb{Z}$$

Then $R : \delta \leftrightarrow_\alpha \delta'$ may be the *closure by inverse reduction* (written $\diamond$)

$$\diamond\{(\mathsf{tt}, 0)\} \cup \{(\mathsf{ff}, n) \mid n \in \mathbb{Z}^\star\}$$

where integers may be used to simulate booleans.

Allows to relate values at different types.

Logical equivalence for closed terms with open types

Assume $\eta : \delta \leftrightarrow_{\Delta} \delta'$ and $M : \delta(\tau)$ and $M' : \delta'(\tau)$.

We defined $M \sim_{\tau} M' \;\; [\eta : \delta \leftrightarrow \delta']$ by induction on τ as follows:

$$
\begin{array}{rcl}
M \sim_{\mathsf{B}} M' \;\; [\eta : \delta \leftrightarrow \delta'] & \textit{iff} & M \simeq M' \\
M \sim_{\tau_1 \to \tau_2} M' \;\; [\eta : \delta \leftrightarrow \delta'] & \textit{iff} & \textit{for all } N \sim_{\tau_1} N' \;\; [\eta : \delta \leftrightarrow \delta'], \\
 & & M\; N \sim_{\tau_2} M'\; N' \;\; [\eta : \delta \leftrightarrow \delta'] \\
M \sim_{\alpha} M' \;\; [\eta : \delta \leftrightarrow \delta'] & \textit{iff} & \eta(\alpha)(M, M') \\
M \sim_{\forall \alpha.\, \tau} M' \;\; [\eta : \delta \leftrightarrow \delta'] & \textit{iff} & \textit{for all } \rho, \rho', R : \rho \leftrightarrow \rho', \\
 & & M\; \rho \sim_{\tau} M'\; \rho' \\
 & & \quad [(\eta, \alpha \mapsto R) : (\delta, \alpha \mapsto \rho) \leftrightarrow (\delta', \alpha \mapsto \rho')]
\end{array}
$$

Logical equivalence for open terms

Definition If $\Delta; \Gamma \vdash M, M' : \tau$ we define $\Delta; \Gamma \vdash M \sim M' : \tau$ as

$$\forall \eta : \delta \leftrightarrow_{\Delta} \delta',\ \ \forall \gamma \sim_{\Gamma} \gamma' \ [\eta : \delta \leftrightarrow \delta'],\ \ \gamma(\delta(M)) \sim_{\tau} \gamma'(\delta'(M'))\ \ [\eta : \delta \leftrightarrow \delta']$$

where $\gamma \sim_{\Gamma} \gamma' \ [\eta : \delta \leftrightarrow \delta'] \triangleq \bigwedge \begin{cases} \mathrm{dom}(\gamma) = \mathrm{dom}(\gamma') = \mathrm{dom}(\Gamma) \\ \forall x : \tau \in \mathrm{dom}(\Gamma),\ \ \gamma(x) \sim_{\tau} \gamma'(x)\ [\eta : \delta \leftrightarrow \delta'] \end{cases}$

(Notations are a bit heavy, but intuitions should remain simple.)

Notice We write $M \sim_{\tau} M'$ for $\varnothing; \varnothing \vdash M \sim M' : \tau$. In particular, τ is a closed type and M and M' are closed terms of type τ. By definition, this means $M \sim_{\tau} M'\ \ [\varnothing : \varnothing \leftrightarrow \varnothing]$, which also coincide with the previous definition of logical relation for closed terms.

Properties

Closure under inverse reduction

If $M \sim_\tau M' \ [\eta : \delta \leftrightarrow \delta']$ and $N \Downarrow M$ and $N' \Downarrow M'$ (and $N : \delta(\tau)$ and $N' : \delta'(\tau)$), then $N \sim_\tau N' \ [\eta : \delta \leftrightarrow \delta']$.

Proof by induction on τ.

Similar to the monomorphic case, except for:

Case τ is $\forall \alpha. \sigma$:

To show $N \sim_\tau M' \ [\eta : \delta \leftrightarrow \delta']$,
i.e. by definition, $\forall \rho, \rho', R : \rho \leftrightarrow \rho', \ M\ \rho \sim_\tau M'\ \rho' \ [(\eta, \alpha \mapsto R)]$,
we assume $R : \rho \leftrightarrow \rho'$ and show $N\ \rho \sim_\sigma M'\ \rho' \ [\eta, \alpha \mapsto R]$.
Since $N\ \rho \longrightarrow M\ \rho$,
by induction hypothesis it suffices to show $M\ \rho \sim_\sigma M'\ \rho' \ [\eta, \alpha \mapsto R]$,
which follows from $M \sim_\tau M' \ [\eta : \delta \leftrightarrow \delta']$.

Properties

Respect for observational equivalence

If $M \sim_\tau M' \ [\eta : \delta \leftrightarrow \delta']$ and $N \cong_{\delta(\tau)} M$ and $N' \cong_{\delta'(\tau)} M'$ then $N \sim_\tau N' \ [\eta : \delta \leftrightarrow \delta']$.

Proof by induction on τ.

Assume $M \sim_\tau M' \ [\eta : \delta \leftrightarrow \delta']$ $(\mathbf{1})$ and $N \cong_{\delta(\tau)} M$ $(\mathbf{2})$. We show $N \sim_\tau M' \ [\eta : \delta \leftrightarrow \delta']$.

Case τ is $\forall \alpha.\, \sigma$:

We assume $R : \rho \leftrightarrow \rho'$ and show $N\ \rho \sim_\sigma M'\ \rho' \ [\eta, \alpha \mapsto R]$.
Since $N\ \rho \cong_{\delta(\tau)} M\ \rho$ (by (2) as $\cong$ is a congruence),
by induction hypothesis it suffices to show $M\ \rho \sim_\sigma M'\ \rho' \ [\eta, \alpha \mapsto R]$,
which follows from (1).

Properties

Corollary The relation $M \sim_\tau M' \ [\eta : \delta \leftrightarrow \delta']$ is an admissible relation between expressions of closed types $\delta(\tau)$ and $\delta'(\tau)$.

(Useful, as we may take $\sim_\tau$ for the default relation.)

Properties

Lemma (respect for observational equivalence)

If $\Delta; \Gamma \vdash M \sim M' : \tau$ and $\Delta; \Gamma \vdash M \cong N : \tau$ and $\Delta; \Gamma \vdash M' \cong N' : \tau$, then $\Delta; \Gamma \vdash N \sim N' : \tau$

Lemma (Compositionality)

$M \sim_{\tau[\alpha \mapsto \sigma]} M' \;\; [\eta : \delta \leftrightarrow \delta']$ iff

$$M \sim_{\tau} M' \;\; [(\eta, \alpha \mapsto R) : (\delta, \alpha \mapsto \delta(\sigma)) \leftrightarrow (\delta', \alpha \mapsto \delta'(\sigma))]$$

where $R : \delta(\sigma) \leftrightarrow \delta'(\sigma)$ is defined by

$$R(N, N') \iff N \sim_{\sigma} N' \;\; [\eta : \delta \leftrightarrow \delta']$$

Proof by structural induction on τ.

Parametricity

Theorem (reflexivity) If $\Delta; \Gamma \vdash M : \tau$ then $\Delta; \Gamma \vdash M \sim M : \tau$.
(Also called parametricity or the fundamental theorem.)

Proof by induction on the typing derivation.

Properties

Theorem

Logical equivalence and observational equivalence coincide.
i.e. $\Delta; \Gamma \vdash M \sim M' : \tau$ iff $\Delta; \Gamma \vdash M \cong M' : \tau$.

As a particular case, $M \sim_\tau M'$ iff $M \cong_\tau M'$.

Properties

Extensionality

$M \cong_{\tau_1 \to \tau_2} M'$ iff for all $M_1 : \tau_1$, $M\ M_1 \cong_{\tau_2} M'\ M_1$.

$M \cong_{\forall \alpha.\, \tau} M'$ iff for all closed type ρ, $M\ \rho \cong_{\tau[\alpha \mapsto \rho]} M'\ \rho$.

Proof. Forward direction is immediate as $\cong$ is a congruence.

Case Value abstraction: It suffices to show $M \sim_{\tau_1 \to \tau_2} M'$. That is, given $M_1 \sim_{\tau_1} M_1'$ $(\mathbf{1})$, we show $M\ M_1 \sim_{\tau_2} M'\ M_1'$ $(\mathbf{2})$. By assumption, we have $M\ M_1 \cong_{\tau_2} M'\ M_1$ $(\mathbf{3})$. By the fundamental lemma, we have $M' \sim_{\tau_1 \to \tau_2} M'$.
Hence, from (1), we get $M'\ M_1 \sim_{\tau_2} M'\ M_1'$,
We conclude (2) by respect for observational equivalence with (3).

Case Type abstraction: It suffices to show $M \sim_{\forall \alpha.\, \tau} M'$. That is, given $R : \rho \leftrightarrow \rho'$ we show $M\ \rho \sim_\tau M'\ \rho'\ [(\alpha \mapsto R) : (\alpha \mapsto \rho) \leftrightarrow (\alpha \mapsto \rho')]$ $(\mathbf{4})$.
By assumption, we have $M\ \rho \cong_{\tau[\alpha \mapsto \rho]} M'\ \rho$ $(\mathbf{5})$.
By the fundamental lemma, we have $M' \sim_{\forall \alpha.\, \tau} M'$.
Hence, we have $M'\ \rho \sim_\tau M'\ \rho'\ [(\alpha \mapsto R) : (\alpha \mapsto \rho) \leftrightarrow (\alpha \mapsto \rho')]$.
We conclude (4) by respect for observational equivalence with (5).

Properties

Identity extension

Let $\eta : \delta \leftrightarrow \delta$ where $\eta(\alpha)$ is observational equivalence at type $\delta(\alpha)$ for all $\alpha \in \mathrm{dom}(\delta)$. Then $M \sim_\tau M'\ [\eta : \delta \leftrightarrow \delta]$ iff $M \cong_{\delta(\tau)} M'$.

Contents

Tools

Value arguments with open types

$$M \sim_{\tau_1 \to \tau_2} M' \ [\eta] \ \text{ iff } \ \forall V, V',\ (V \sim_{\tau_1} V' \ [\eta] \implies M\, V \sim_{\tau_2} M'\, V' \ [\eta])$$

The implication follows from the definition.
The reverse is the value arguments lemma extended to open terms.
Hence, we could have used this as a definition.

Admissibility

A relation R is admissible iff it is the closure of a relation on values that is compatible with observational equivalence.
We may consider sets of $\diamond_{\tau \leftrightarrow \tau'} R$, admissible by construction, of the form

$$\{(N, N') \mid \exists (M, M') \in R,\ \ N \cong_\tau M \wedge M' \cong_{\tau'} N'\}$$

Applications *Inhabitants of $\forall\alpha.\,\alpha \to \alpha$*

Fact If $M : \forall\alpha.\,\alpha \to \alpha$, then $M \cong_{\forall\alpha.\,\alpha\to\alpha} id$ where $id \stackrel{\triangle}{=} \Lambda\alpha.\lambda x{:}\alpha.\,x$.

Proof By *extensionality*, it suffices to show that for any ρ and $N : \rho$ we have $M\ \rho\ N \cong_\rho id\ \rho\ N$. In fact, by closure by inverse reduction, it suffices to show $M\ \rho\ N \cong_\rho N$ or, equivalently, $M\ \rho\ N \sim_\rho N$ $\mathbf{(1)}$.

By parametricity, we have $M \sim_{\forall\alpha.\,\alpha\to\alpha} M$ $\mathbf{(2)}$.

Consider R equal to $\diamond_{\rho\leftrightarrow\rho}(N, N)$ and η be $\alpha \mapsto R : \rho \leftrightarrow \rho$.
R is admissible by construction.
(Reminder: $R(P, P')$ iff $P \cong_\rho N \wedge N \cong_\rho P'$.)

Since $R(N, N)$, we have $N \sim_\alpha N\ \ [\eta]$ by definition.
Hence, from (2), we have $M\ \rho\ N \sim_\alpha M\ \rho\ N\ \ [\eta]$,
i.e. $R(M\ \rho\ N, M\ \rho\ N)$, which implies (1) by definition of R.

Applications *Inhabitants of* $\forall\alpha.\,\alpha \to \alpha \to \alpha$

Fact Let σ be $\forall\alpha.\,\alpha \to \alpha \to \alpha$. If $M : \sigma$, then either
$M \cong_\sigma \mathsf{M}_1 \stackrel{\triangle}{=} \Lambda\alpha.\lambda x_1{:}\alpha.\,\lambda x_2{:}\alpha.\,x_1$ or $M \cong_\sigma \mathsf{M}_2 \stackrel{\triangle}{=} \Lambda\alpha.\lambda \mathsf{x}_1{:}\alpha.\,\lambda \mathsf{x}_2{:}\alpha.\,\mathsf{x}_2$

Proof By *extensionality*, it suffices to show that
for either $i = 1$ or $i = 2$, for any closed type ρ and $N_1, N_2 : \rho$, we have
$M\ \rho\ N_1\ N_2 \cong_\rho M_i\ \rho\ N_1\ N_2$, or, by closure by inverse reduction and replacing observational by logical equivalence that $M\ \rho\ N_1\ N_2 \cong_\sigma N_i$ **(1)**.

?

Applications *Inhabitants of* $\forall \alpha. \alpha \to \alpha \to \alpha$

Fact Let σ be $\forall \alpha. \alpha \to \alpha \to \alpha$. If $M : \sigma$, then either
$M \cong_\sigma \mathsf{M}_1 \stackrel{\triangle}{=} \Lambda\alpha.\lambda x_1{:}\alpha.\, \lambda x_2{:}\alpha.\, x_1$ or $M \cong_\sigma \mathsf{M}_2 \stackrel{\triangle}{=} \Lambda\alpha.\lambda \mathsf{x}_1{:}\alpha.\, \lambda \mathsf{x}_2{:}\alpha.\, \mathsf{x}_2$

Proof By *extensionality*, it suffices to show that
for either $i = 1$ or $i = 2$, for any closed type ρ and $N_1, N_2 : \rho$, we have
$M\ \rho\ N_1\ N_2 \cong_\rho M_i\ \rho\ N_1\ N_2$, or, by closure by inverse reduction and replacing observational by logical equivalence that $M\ \rho\ N_1\ N_2 \cong_\sigma N_i$ **(1)**. Let ρ and $N_1, N_2 : \rho$ be fixed.
Consider R equal to $\diamond_{\mathsf{B}\leftrightarrow\rho}\{(\mathsf{tt}, N_1), (\mathsf{ff}, N_2)\}$ and η be $\alpha \mapsto R : \mathsf{B} \leftrightarrow \rho$.

?

Applications *Inhabitants of* $\forall\alpha.\,\alpha \to \alpha \to \alpha$

Fact Let σ be $\forall\alpha.\,\alpha \to \alpha \to \alpha$. If $M : \sigma$, then either
$M \cong_\sigma \mathsf{M}_1 \triangleq \Lambda\alpha.\lambda x_1{:}\alpha.\,\lambda x_2{:}\alpha.\,x_1$ or $M \cong_\sigma \mathsf{M}_2 \triangleq \Lambda\alpha.\lambda \mathsf{x}_1{:}\alpha.\,\lambda \mathsf{x}_2{:}\alpha.\,\mathsf{x}_2$

Proof By *extensionality*, it suffices to show that
for either $i = 1$ or $i = 2$, for any closed type ρ and $N_1, N_2 : \rho$, we have $M\ \rho\ N_1\ N_2 \cong_\rho M_i\ \rho\ N_1\ N_2$, or, by closure by inverse reduction and replacing observational by logical equivalence that $M\ \rho\ N_1\ N_2 \cong_\sigma N_i$ (**1**). Let ρ and $N_1, N_2 : \rho$ be fixed.
Consider R equal to $\diamond_{\mathsf{B}\leftrightarrow\rho}\{(\mathsf{tt}, N_1), (\mathsf{ff}, N_2)\}$ and η be $\alpha \mapsto R : \mathsf{B} \leftrightarrow \rho$.
We have $\mathsf{tt} \sim_\alpha N_1\ [\eta]$ since $R(\mathsf{tt}, N_1)$ and, similarly, $\mathsf{ff} \sim_\alpha N_2\ [\eta]$.

We have $M \sim_\sigma M$ by parametricity.

?

Applications *Inhabitants of* $\forall\alpha.\,\alpha \to \alpha \to \alpha$

Fact Let σ be $\forall\alpha.\,\alpha \to \alpha \to \alpha$. If $M : \sigma$, then either
$M \cong_\sigma \mathsf{M}_1 \stackrel{\triangle}{=} \Lambda\alpha.\lambda x_1\!:\!\alpha.\,\lambda x_2\!:\!\alpha.\,x_1$ or $M \cong_\sigma \mathsf{M}_2 \stackrel{\triangle}{=} \Lambda\alpha.\lambda \mathsf{x}_1\!:\!\alpha.\,\lambda \mathsf{x}_2\!:\!\alpha.\,\mathsf{x}_2$

Proof By *extensionality*, it suffices to show that
for either $i = 1$ or $i = 2$, for any closed type ρ and $N_1, N_2 : \rho$, we have
$M\ \rho\ N_1\ N_2 \cong_\rho M_i\ \rho\ N_1\ N_2$, or, by closure by inverse reduction and replacing observational by logical equivalence that $M\ \rho\ N_1\ N_2 \cong_\sigma N_i$ $(\mathbf{1})$. Let ρ and $N_1, N_2 : \rho$ be fixed.
Consider R equal to $\diamond_{\mathsf{B}\leftrightarrow\rho}\{(\mathsf{tt}, N_1), (\mathsf{ff}, N_2)\}$ and η be $\alpha \mapsto R : \mathsf{B} \leftrightarrow \rho$.
We have $\mathsf{tt} \sim_\alpha N_1\ [\eta]$ since $R(\mathsf{tt}, N_1)$ and, similarly, $\mathsf{ff} \sim_\alpha N_2\ [\eta]$.

We have $M \sim_\sigma M$ by parametricity. Hence, $M\ \mathsf{B}\ \mathsf{tt}\ \mathsf{ff} \sim_\alpha M\ \rho\ N_1\ N_2\ [\eta]$, *i.e.* $R(M\ \mathsf{B}\ \mathsf{tt}\ \mathsf{ff}, M\ \rho\ N_1\ N_2)$, which means:

$$\bigvee\begin{cases} M\ \mathsf{B}\ \mathsf{tt}\ \mathsf{ff} \sim_{\mathsf{B}} \mathsf{tt} \wedge M\ \rho\ N_1\ N_2 \sim_\rho N_1 \\ M\ \mathsf{B}\ \mathsf{tt}\ \mathsf{ff} \sim_{\mathsf{B}} \mathsf{ff} \wedge M\ \rho\ N_1\ N_2 \sim_\rho N_2 \end{cases}$$

?

Applications *Inhabitants of* $\forall\alpha.\,\alpha\to\alpha\to\alpha$

Fact Let σ be $\forall\alpha.\,\alpha\to\alpha\to\alpha$. If $M:\sigma$, then either
$M \cong_\sigma \mathsf{M}_1 \stackrel{\triangle}{=} \Lambda\alpha.\lambda x_1{:}\alpha.\,\lambda x_2{:}\alpha.\,x_1$ or $M \cong_\sigma \mathsf{M}_2 \stackrel{\triangle}{=} \Lambda\alpha.\lambda \mathsf{x}_1{:}\alpha.\,\lambda \mathsf{x}_2{:}\alpha.\,\mathsf{x}_2$

Proof By *extensionality*, it suffices to show that
for either $i=1$ or $i=2$, for any closed type ρ and $N_1, N_2:\rho$, we have
$M\ \rho\ N_1\ N_2 \cong_\rho M_i\ \rho\ N_1\ N_2$, or, by closure by inverse reduction and replacing observational by logical equivalence that $M\ \rho\ N_1\ N_2 \cong_\sigma N_i$ (**1**). Let ρ and $N_1, N_2:\rho$ be fixed.
Consider R equal to $\diamond_{\mathsf{B}\leftrightarrow\rho}\{(\mathsf{tt}, N_1), (\mathsf{ff}, N_2)\}$ and η be $\alpha\mapsto R:\mathsf{B}\leftrightarrow\rho$.
We have $\mathsf{tt} \sim_\alpha N_1\ [\eta]$ since $R(\mathsf{tt}, N_1)$ and, similarly, $\mathsf{ff}\sim_\alpha N_2\ [\eta]$.

We have $M\sim_\sigma M$ by parametricity. Hence, $M\ \mathsf{B}\ \mathsf{tt}\ \mathsf{ff} \sim_\alpha M\ \rho\ N_1\ N_2\ [\eta]$, *i.e.* $R(M\ \mathsf{B}\ \mathsf{tt}\ \mathsf{ff}, M\ \rho\ N_1\ N_2)$, which means:

$$\bigvee\begin{cases} M\ \mathsf{B}\ \mathsf{tt}\ \mathsf{ff} \sim_{\mathsf{B}} \mathsf{tt} \wedge M\ \rho\ N_1\ N_2 \sim_\rho N_1 \\ M\ \mathsf{B}\ \mathsf{tt}\ \mathsf{ff} \sim_{\mathsf{B}} \mathsf{ff} \wedge M\ \rho\ N_1\ N_2 \sim_\rho N_2 \end{cases}$$

Since, M B tt ff is independent of ρ, N_1, and N_2, this actually shows (1).

Applications — *Inhabitants of* $\forall\alpha.\,\alpha \to \alpha \to \alpha$

Fact Let σ be $\forall\alpha.\,\alpha \to \alpha \to \alpha$. If $M : \sigma$, then either
$M \cong_\sigma \mathsf{M}_1 \triangleq \Lambda\alpha.\lambda x_1{:}\alpha.\,\lambda x_2{:}\alpha.\,x_1$ or $M \cong_\sigma \mathsf{M}_2 \triangleq \Lambda\alpha.\lambda \mathsf{x}_1{:}\alpha.\,\lambda \mathsf{x}_2{:}\alpha.\,\mathsf{x}_2$

Proof By *extensionality*, it suffices to show that
for either $i = 1$ or $i = 2$, for any closed type ρ and $N_1, N_2 : \rho$, we have
$M\ \rho\ N_1\ N_2 \cong_\rho M_i\ \rho\ N_1\ N_2$, or, by closure by inverse reduction and replacing observational by logical equivalence that $M\ \rho\ N_1\ N_2 \cong_\sigma N_i$ (**1**). Let ρ and $N_1, N_2 : \rho$ be fixed.
Consider R equal to $\diamond_{\mathsf{B}\leftrightarrow\rho}\{(\mathsf{tt}, N_1), (\mathsf{ff}, N_2)\}$ and η be $\alpha \mapsto R : \mathsf{B} \leftrightarrow \rho$.
We have $\mathsf{tt} \sim_\alpha N_1\ [\eta]$ since $R(\mathsf{tt}, N_1)$ and, similarly, $\mathsf{ff} \sim_\alpha N_2\ [\eta]$.

We have $M \sim_\sigma M$ by parametricity. Hence, $M\ \mathsf{B}\ \mathsf{tt}\ \mathsf{ff} \sim_\alpha M\ \rho\ N_1\ N_2\ [\eta]$, *i.e.* $R(M\ \mathsf{B}\ \mathsf{tt}\ \mathsf{ff}, M\ \rho\ N_1\ N_2)$, which means:

$$\bigvee \begin{cases} M\ \mathsf{B}\ \mathsf{tt}\ \mathsf{ff} \sim_{\mathsf{B}} \mathsf{tt} \wedge M\ \rho\ N_1\ N_2 \sim_\rho N_1 \\ M\ \mathsf{B}\ \mathsf{tt}\ \mathsf{ff} \sim_{\mathsf{B}} \mathsf{ff} \wedge M\ \rho\ N_1\ N_2 \sim_\rho N_2 \end{cases}$$

Since, $M\ \mathsf{B}\ \mathsf{tt}\ \mathsf{ff}$ is independent of ρ, N_1, and N_2, this actually shows (1).

Applications *Inhabitants of $\forall\alpha.\,\alpha \to \alpha \to \alpha$*

Fact Let σ be $\forall\alpha.\,\alpha \to \alpha \to \alpha$. If $M : \sigma$, then either
$M \cong_\sigma \mathsf{M}_1 \stackrel{\triangle}{=} \Lambda\alpha.\lambda x_1{:}\alpha.\,\lambda x_2{:}\alpha.\,x_1$ or $M \cong_\sigma \mathsf{M}_2 \stackrel{\triangle}{=} \Lambda\alpha.\lambda \mathsf{x}_1{:}\alpha.\,\lambda \mathsf{x}_2{:}\alpha.\,\mathsf{x}_2$

Proof By *extensionality*, it suffices to show that
for either $i = 1$ or $i = 2$, for any closed type ρ and $N_1, N_2 : \rho$, we have
$M\ \rho\ N_1\ N_2 \cong_\rho M_i\ \rho\ N_1\ N_2$, or, by closure by inverse reduction and replacing observational by logical equivalence that $M\ \rho\ N_1\ N_2 \cong_\sigma N_i$ $(\mathbf{1})$. Let ρ and $N_1, N_2 : \rho$ be fixed.
Consider R equal to $\diamond_{\mathbb{N}\leftrightarrow\rho}\{(\mathbf{0}, N_1), (\mathbf{1}, N_2)\}$ and η be $\alpha \mapsto R : \mathbb{N} \leftrightarrow \rho$.
We have $\mathbf{0} \sim_\alpha N_1\ [\eta]$ since $R(\mathbf{0}, N_1)$ and, similarly, $\mathbf{1} \sim_\alpha N_2\ [\eta]$.

We have $M \sim_\sigma M$ by parametricity. Hence, $M\ \mathbb{N}\ \mathbf{0}\ \mathbf{1} \sim_\alpha M\ \rho\ N_1\ N_2\ [\eta]$, *i.e.* $R(M\ \mathbb{N}\ \mathbf{0}\ \mathbf{1}, M\ \rho\ N_1\ N_2)$, which means:

$$\bigvee \begin{cases} M\ \mathbb{N}\ \mathbf{0}\ \mathbf{1} \sim_{\mathbb{N}} \mathbf{0} \wedge M\ \rho\ N_1\ N_2 \sim_\rho N_1 \\ M\ \mathbb{N}\ \mathbf{0}\ \mathbf{1} \sim_{\mathbb{N}} \mathbf{1} \wedge M\ \rho\ N_1\ N_2 \sim_\rho N_2 \end{cases}$$

Since, $M\ \mathbb{N}\ \mathbf{0}\ \mathbf{1}$ is independent of ρ, N_1, and N_2, this actually shows (1).

Applications — *Inhabitants of* $\forall\alpha.\,\alpha \to \alpha \to \alpha$

Fact Let σ be $\forall\alpha.\,\alpha \to \alpha \to \alpha$. If $M : \sigma$, then either
$M \cong_\sigma \mathsf{M}_1 \triangleq \Lambda\alpha.\lambda x_1{:}\alpha.\,\lambda x_2{:}\alpha.\,x_1$ or $M \cong_\sigma \mathsf{M}_2 \triangleq \Lambda\alpha.\lambda \mathsf{x}_1{:}\alpha.\,\lambda \mathsf{x}_2{:}\alpha.\,\mathsf{x}_2$

Proof By *extensionality*, it suffices to show that
for either $i = 1$ or $i = 2$, for any closed type ρ and $N_1, N_2 : \rho$, we have $M\ \rho\ N_1\ N_2 \cong_\rho M_i\ \rho\ N_1\ N_2$, or, by closure by inverse reduction and replacing observational by logical equivalence that $M\ \rho\ N_1\ N_2 \cong_\sigma N_i$ (**1**). Let ρ and $N_1, N_2 : \rho$ be fixed.
Consider R equal to $\diamond_{\sigma\leftrightarrow\rho}\{(\mathsf{M}_1, N_1), (\mathsf{M}_2, N_2)\}$ and η be $\alpha \mapsto R : \sigma \leftrightarrow \rho$.
We have $\mathsf{M}_1 \sim_\alpha N_1\ [\eta]$ since $R(\mathsf{M}_1, N_1)$ and, similarly, $\mathsf{M}_2 \sim_\alpha N_2\ [\eta]$.

We have $M \sim_\sigma M$ by parametricity. Hence, $M\ \sigma\ \mathsf{M}_1\ \mathsf{M}_2 \sim_\alpha M\ \rho\ N_1\ N_2\ [\eta]$, *i.e.* $R(M\ \sigma\ \mathsf{M}_1\ \mathsf{M}_2, M\ \rho\ N_1\ N_2)$, which means:

$$\bigvee \begin{cases} M\ \sigma\ \mathsf{M}_1\ \mathsf{M}_2 \sim_\sigma \mathsf{M}_1 \wedge M\ \rho\ N_1\ N_2 \sim_\rho N_1 \\ M\ \sigma\ \mathsf{M}_1\ \mathsf{M}_2 \sim_\sigma \mathsf{M}_2 \wedge M\ \rho\ N_1\ N_2 \sim_\rho N_2 \end{cases}$$

Since, $M\ \sigma\ \mathsf{M}_1\ \mathsf{M}_2$ is independent of ρ, N_1, and N_2, this actually shows (1).

Applications

Inhabitants of $\forall \alpha.\, \alpha \to \alpha \to \alpha$

Fact Let σ be $\forall \alpha.\, \alpha \to \alpha \to \alpha$. If $M : \sigma$, then either
$M \cong_\sigma \mathsf{M}_1 \triangleq \Lambda\alpha.\lambda x_1{:}\alpha.\, \lambda x_2{:}\alpha.\, x_1$ or $M \cong_\sigma \mathsf{M}_2 \triangleq \Lambda\alpha.\lambda \mathsf{x}_1{:}\alpha.\, \lambda \mathsf{x}_2{:}\alpha.\, \mathsf{x}_2$

Proof By *extensionality*, it suffices to show that
for either $i = 1$ or $i = 2$, for any closed type ρ and $N_1, N_2 : \rho$, we have
$M\ \rho\ N_1\ N_2 \cong_\rho M_i\ \rho\ N_1\ N_2$, or, by closure by inverse reduction and replacing observational by logical equivalence that $M\ \rho\ N_1\ N_2 \cong_\sigma N_i$ (1). Let ρ and $N_1, N_2 : \rho$ be fixed.
Consider R equal to $\diamond_{\mathsf{B}\leftrightarrow\rho}\{(\mathsf{tt}, N_1), (\mathsf{ff}, N_2)\}$ and η be $\alpha \mapsto R : \mathsf{B} \leftrightarrow \rho$.
We have $\mathsf{tt} \sim_\alpha N_1\ [\eta]$ since $R(\mathsf{tt}, N_1)$ and, similarly, $\mathsf{ff} \sim_\alpha N_2\ [\eta]$.

We have $M \sim_\sigma M$ by parametricity. Hence, $M\ \mathsf{B}\ \mathsf{tt}\ \mathsf{ff} \sim_\alpha M\ \rho\ N_1\ N_2\ [\eta]$, *i.e.* $R(M\ \mathsf{B}\ \mathsf{tt}\ \mathsf{ff}, M\ \rho\ N_1\ N_2)$, which means:

$$\bigvee \begin{cases} M\ \mathsf{B}\ \mathsf{tt}\ \mathsf{ff} \sim_{\mathsf{B}} \mathsf{tt} \wedge M\ \rho\ N_1\ N_2 \sim_\rho N_1 \\ M\ \mathsf{B}\ \mathsf{tt}\ \mathsf{ff} \sim_{\mathsf{B}} \mathsf{ff} \wedge M\ \rho\ N_1\ N_2 \sim_\rho N_2 \end{cases}$$

Since, M B tt ff is independent of ρ, N_1, and N_2, this actually shows (1).

Applications — *Inhabitants of* $\forall\alpha.\,\alpha \to \alpha \to \alpha$

Fact Let σ be $\forall\alpha.\,\alpha \to \alpha \to \alpha$. If $M : \sigma$, then either
$M \cong_\sigma \mathsf{M}_1 \stackrel{\triangle}{=} \Lambda\alpha.\lambda x_1{:}\alpha.\,\lambda x_2{:}\alpha.\,x_1$ or $M \cong_\sigma \mathsf{M}_2 \stackrel{\triangle}{=} \Lambda\alpha.\lambda \mathsf{x}_1{:}\alpha.\,\lambda \mathsf{x}_2{:}\alpha.\,\mathsf{x}_2$

Proof By *extensionality* *and value substitution*, it suffices to show that
for either $i = 1$ or $i = 2$, for any closed type ρ and $V_1\,, V_2\; : \rho$, we have
$M\ \rho\ V_1\ \ V_2\ \cong_\rho M_i\ \rho\ V_1\ \ V_2$, or, by closure by inverse reduction and replacing observational by logical equivalence that $M\ \rho\ V_1\ \ V_2\ \cong_\sigma V_i\ \ (\mathbf{1})$. Let ρ and $V_1\,, V_2\; : \rho$ be fixed.
Consider R equal to $\diamond_{\mathsf{B}\leftrightarrow\rho}\{(\mathsf{tt}, V_1\,), (\mathsf{ff}, V_2\,)\}$ and η be $\alpha \mapsto R : \mathsf{B} \leftrightarrow \rho$.
We have $\mathsf{tt} \sim_\alpha V_1\ \ [\eta]$ since $R(\mathsf{tt}, V_1\,)$ and, similarly, $\mathsf{ff} \sim_\alpha V_2\ \ [\eta]$.

We have $M \sim_\sigma M$ by parametricity. Hence, $M\ \mathsf{B}\ \mathsf{tt}\ \mathsf{ff} \sim_\alpha M\ \rho\ V_1\ \ V_2\ \ [\eta]$, *i.e.* $R(M\ \mathsf{B}\ \mathsf{tt}\ \mathsf{ff}, M\ \rho\ V_1\ \ V_2\,)$, which means:

$$\bigvee \begin{cases} M\ \mathsf{B}\ \mathsf{tt}\ \mathsf{ff} \sim_{\mathsf{B}} \mathsf{tt} \wedge M\ \rho\ V_1\ \ V_2\ \sim_\rho V_1 \\ M\ \mathsf{B}\ \mathsf{tt}\ \mathsf{ff} \sim_{\mathsf{B}} \mathsf{ff} \wedge M\ \rho\ V_1\ \ V_2\ \sim_\rho V_2 \end{cases}$$

Since, $M\ \mathsf{B}\ \mathsf{tt}\ \mathsf{ff}$ is independent of ρ, V_1 , and V_2 , this actually shows (1).

Applications *Inhabitants of* $\forall\alpha.\,(\alpha \to \alpha) \to \alpha \to \alpha$

?

Applications *Inhabitants of* $\forall\alpha.\,(\alpha \to \alpha) \to \alpha \to \alpha$

Fact Let σ be $\forall\alpha.\,(\alpha \to \alpha) \to \alpha \to \alpha$. If $M : \sigma$, then $M \cong_\sigma M_n$ for some integer n, where $M_n \triangleq \Lambda\alpha.\lambda f\!:\!\alpha \to \alpha.\,\lambda x\!:\!\alpha.\,f^n\,x$.

?

Applications *Inhabitants of* $\forall\alpha.\,(\alpha \to \alpha) \to \alpha \to \alpha$

Fact Let σ be $\forall\alpha.\,(\alpha \to \alpha) \to \alpha \to \alpha$. If $M : \sigma$, then $M \cong_\sigma M_n$ for some integer n, where $M_n \triangleq \Lambda\alpha.\lambda f{:}\alpha \to \alpha.\,\lambda x{:}\alpha.\,f^n\,x$.

That is, the inhabitants of $\forall\alpha.\,(\alpha \to \alpha) \to \alpha \to \alpha$ are the Church naturals.

Applications *Inhabitants of* $\forall\alpha.\,(\alpha\to\alpha)\to\alpha\to\alpha$

Fact Let σ be $\forall\alpha.\,(\alpha\to\alpha)\to\alpha\to\alpha$. If $M:\sigma$, then $M\cong_\sigma M_n$ for some integer n, where $M_n \triangleq \Lambda\alpha.\lambda f{:}\alpha\to\alpha.\,\lambda x{:}\alpha.\,f^n\,x$.

Proof

?

Applications *Inhabitants of* $\forall\alpha.\,(\alpha \to \alpha) \to \alpha \to \alpha$

Fact Let σ be $\forall\alpha.\,(\alpha \to \alpha) \to \alpha \to \alpha$. If $M : \sigma$, then $M \cong_\sigma M_n$ for some integer n, where $M_n \triangleq \Lambda\alpha.\lambda f{:}\alpha \to \alpha.\,\lambda x{:}\alpha.\,f^n\,x$.

Proof By *extensionality*, and *value arguments*, it suffices to show that there exists n such for any closed type ρ and closed values $V_1 : \rho \to \rho$ and $V_2 : \rho$, we have $M\;\rho\;V_1\;V_2 \cong_\rho M_n\;\rho\;V_1\;V_2$, or, by closure by inverse reduction and replacing observational by logical equivalence, $M\;\rho\;V_1\;V_2 \sim_\rho V_1^n\;V_2$, $(\mathbf{1})$.

?

Applications — *Inhabitants of* $\forall\alpha.\,(\alpha \to \alpha) \to \alpha \to \alpha$

Fact Let σ be $\forall\alpha.\,(\alpha \to \alpha) \to \alpha \to \alpha$. If $M : \sigma$, then $M \cong_\sigma M_n$ for some integer n, where $M_n \triangleq \Lambda\alpha.\lambda f\!:\!\alpha \to \alpha.\,\lambda x\!:\!\alpha.\,f^n\,x$.

Proof By *extensionality*, and *value arguments*, it suffices to show that there exists n such for any closed type ρ and closed values $V_1 : \rho \to \rho$ and $V_2 : \rho$, we have $M\ \rho\ V_1\ V_2 \cong_\rho M_n\ \rho\ V_1\ V_2$, or, by closure by inverse reduction and replacing observational by logical equivalence, $M\ \rho\ V_1\ V_2 \sim_\rho V_1^n\ V_2$, $(\mathbf{1})$.

Let $V_1 : \rho \to \rho$ and $V_2 : \rho$ be fixed.
Let η be $\alpha \mapsto R$ where $R : \mathbb{N} \leftrightarrow \rho$ is defined as $\diamond_{\mathbb{N}\leftrightarrow\rho}\{(k,\ V_1^k\ V_2) \mid k \in \mathbb{N}\}$.
We have $0 \sim_\alpha V_2\ \ [\eta]$ since $R(0, V_2)$ (reduce the right-hand side for $k = 0$).

We also have *succ* $\sim_{\alpha\to\alpha} V_1\ \ [\eta]$. Indeed,

?

Applications *Inhabitants of* $\forall\alpha.\,(\alpha \to \alpha) \to \alpha \to \alpha$

Fact Let σ be $\forall\alpha.\,(\alpha \to \alpha) \to \alpha \to \alpha$. If $M : \sigma$, then $M \cong_\sigma M_n$ for some integer n, where $M_n \triangleq \Lambda\alpha.\lambda f{:}\alpha \to \alpha.\,\lambda x{:}\alpha.\,f^n\,x$.

Proof By *extensionality*, and *value arguments*, it suffices to show that there exists n such for any closed type ρ and closed values $V_1 : \rho \to \rho$ and $V_2 : \rho$, we have $M\ \rho\, V_1\ V_2 \cong_\rho M_n\ \rho\, V_1\ V_2$, or, by closure by inverse reduction and replacing observational by logical equivalence, $M\ \rho\, V_1\ V_2 \sim_\rho V_1^n\ V_2$, (**1**).

Let $V_1 : \rho \to \rho$ and $V_2 : \rho$ be fixed.
Let η be $\alpha \mapsto R$ where $R : \mathbb{N} \leftrightarrow \rho$ is defined as $\diamond_{\mathbb{N}\leftrightarrow\rho}\{(k,\ V_1^k\ V_2) \mid k \in \mathbb{N}\}$.
We have $0 \sim_\alpha V_2\ \ [\eta]$ since $R(0, V_2)$ (reduce the right-hand side for $k = 0$).

We also have *succ* $\sim_{\alpha\to\alpha} V_1\ \ [\eta]$. Indeed, assume $N \sim_\alpha N'\ \ [\eta]$, *i.e.* $R(N, N')$. There exists k such that $N \cong_\mathbb{N} k$ and $N' \cong_\rho V_1^k\ V_2$. By congruence, we have *succ* $N \cong_\mathbb{N}$ *succ* $k \Downarrow k + 1$ and $V_1\ N' \cong_\rho V_1\ (V_1^k\ V_2) \Downarrow V_1^{k+1}\ V_2$. Hence $R($*succ* $N, V_1\ N')$, that is *succ* $N \sim_\alpha V_1\ N'\ \ [\eta]$.

Applications *Inhabitants of* $\forall\alpha.\,(\alpha \to \alpha) \to \alpha \to \alpha$

Fact Let σ be $\forall\alpha.\,(\alpha \to \alpha) \to \alpha \to \alpha$. If $M : \sigma$, then $M \cong_\sigma M_n$ for some integer n, where $M_n \triangleq \Lambda\alpha.\lambda f{:}\alpha \to \alpha.\,\lambda x{:}\alpha.\,f^n\,x$.

Proof By *extensionality*, and *value arguments*, it suffices to show that there exists n such for any closed type ρ and closed values $V_1 : \rho \to \rho$ and $V_2 : \rho$, we have $M\;\rho\;V_1\;V_2 \cong_\rho M_n\;\rho\;V_1\;V_2$, or, by closure by inverse reduction and replacing observational by logical equivalence, $M\;\rho\;V_1\;V_2 \sim_\rho V_1^n\;V_2$, ($\mathbf{1}$).

Let $V_1 : \rho \to \rho$ and $V_2 : \rho$ be fixed.
Let η be $\alpha \mapsto R$ where $R : \mathbb{N} \leftrightarrow \rho$ is defined as $\diamond_{\mathbb{N}\leftrightarrow\rho}\{(k,\;V_1^k\;V_2) \mid k \in \mathbb{N}\}$.
We have $0 \sim_\alpha V_2\;\;[\eta]$ since $R(0, V_2)$ (reduce the right-hand side for $k = 0$).

We also have *succ* $\sim_{\alpha\to\alpha} V_1\;\;[\eta]$. (A key to the proof.)

?

Applications *Inhabitants of* $\forall\alpha.(\alpha\to\alpha)\to\alpha\to\alpha$

Fact Let σ be $\forall\alpha.(\alpha\to\alpha)\to\alpha\to\alpha$. If $M:\sigma$, then $M \cong_\sigma M_n$ for some integer n, where $M_n \triangleq \Lambda\alpha.\lambda f{:}\alpha\to\alpha.\,\lambda x{:}\alpha.\,f^n\,x$.

Proof By *extensionality*, and *value arguments*, it suffices to show that there exists n such for any closed type ρ and closed values $V_1:\rho\to\rho$ and $V_2:\rho$, we have $M\;\rho\;V_1\;V_2 \cong_\rho M_n\;\rho\;V_1\;V_2$, or, by closure by inverse reduction and replacing observational by logical equivalence, $M\;\rho\;V_1\;V_2 \sim_\rho V_1^n\;V_2$, (**1**).

Let $V_1:\rho\to\rho$ and $V_2:\rho$ be fixed.
Let η be $\alpha\mapsto R$ where $R:\mathbb{N}\leftrightarrow\rho$ is defined as $\diamond_{\mathbb{N}\leftrightarrow\rho}\{(k,\;V_1^k\;V_2)\mid k\in\mathbb{N}\}$.
We have $0\sim_\alpha V_2\;\;[\eta]$ since $R(0,V_2)$ (reduce the right-hand side for $k=0$).

We also have *succ* $\sim_{\alpha\to\alpha} V_1\;\;[\eta]$. (A key to the proof.)

By parametricity, we have $M\sim_\sigma M$.

?

Applications — *Inhabitants of* $\forall\alpha.(\alpha \to \alpha) \to \alpha \to \alpha$

Fact Let σ be $\forall\alpha.(\alpha \to \alpha) \to \alpha \to \alpha$. If $M : \sigma$, then $M \cong_\sigma M_n$ for some integer n, where $M_n \triangleq \Lambda\alpha.\lambda f{:}\alpha \to \alpha.\,\lambda x{:}\alpha.\,f^n\,x$.

Proof By *extensionality*, and *value arguments*, it suffices to show that there exists n such for any closed type ρ and closed values $V_1 : \rho \to \rho$ and $V_2 : \rho$, we have $M\;\rho\,V_1\;V_2 \cong_\rho M_n\;\rho\,V_1\;V_2$, or, by closure by inverse reduction and replacing observational by logical equivalence, $M\;\rho\,V_1\;V_2 \sim_\rho V_1^n\;V_2$, (**1**).

Let $V_1 : \rho \to \rho$ and $V_2 : \rho$ be fixed.
Let η be $\alpha \mapsto R$ where $R : \mathbb{N} \leftrightarrow \rho$ is defined as $\diamond_{\mathbb{N}\leftrightarrow\rho}\{(k,\;V_1^k\;V_2) \mid k \in \mathbb{N}\}$.
We have $0 \sim_\alpha V_2\;\;[\eta]$ since $R(0, V_2)$ (reduce the right-hand side for $k = 0$).

We also have *succ* $\sim_{\alpha\to\alpha} V_1\;\;[\eta]$. (A key to the proof.)

By parametricity, we have $M \sim_\sigma M$. Hence, $M\;\mathbb{N}$ *succ* $0 \sim_\alpha M\;\rho\,V_1\;V_2\;\;[\eta]$, *i.e.* $R(M\;\mathbb{N}\;succ\,0, M\;\rho\,V_1\;V_2)$ which means that there exists n such that $M\;\mathbb{N}\;succ\,0 \sim_\sigma n$ and $M\;\rho\,V_1\;V_2 \sim_\rho V_1^n\;V_2$.

?

Applications *Inhabitants of* $\forall\alpha.\,(\alpha \to \alpha) \to \alpha \to \alpha$

Fact Let σ be $\forall\alpha.\,(\alpha \to \alpha) \to \alpha \to \alpha$. If $M : \sigma$, then $M \cong_\sigma M_n$ for some integer n, where $M_n \triangleq \Lambda\alpha.\lambda f{:}\alpha \to \alpha.\,\lambda x{:}\alpha.\,f^n\,x$.

Proof By *extensionality*, and *value arguments*, it suffices to show that there exists n such for any closed type ρ and closed values $V_1 : \rho \to \rho$ and $V_2 : \rho$, we have $M\ \rho\, V_1\ V_2 \cong_\rho M_n\ \rho\, V_1\ V_2$, or, by closure by inverse reduction and replacing observational by logical equivalence, $M\ \rho\, V_1\ V_2 \sim_\rho V_1^n\ V_2$, (**1**).

Let $V_1 : \rho \to \rho$ and $V_2 : \rho$ be fixed.
Let η be $\alpha \mapsto R$ where $R : \mathbb{N} \leftrightarrow \rho$ is defined as $\diamond_{\mathbb{N}\leftrightarrow\rho}\{(k,\ V_1^k\ V_2) \mid k \in \mathbb{N}\}$.
We have $0 \sim_\alpha V_2\ \ [\eta]$ since $R(0, V_2)$ (reduce the right-hand side for $k = 0$).

We also have *succ* $\sim_{\alpha\to\alpha} V_1\ \ [\eta]$. (A key to the proof.)

By parametricity, we have $M \sim_\sigma M$. Hence, $M\ \mathbb{N}$ *succ* $0 \sim_\alpha M\ \rho\, V_1\ V_2\ \ [\eta]$, *i.e.* $R(M\ \mathbb{N}\ succ\,0, M\ \rho\, V_1\ V_2)$ which means that there exists n such that $M\ \mathbb{N}\ succ\,0 \sim_\sigma n$ and $M\ \rho\, V_1\ V_2 \sim_\rho V_1^n\ V_2$.

Since, $M\ \mathbb{N}\ succ\,0$ is independent of ρ, V_1, and V_2, and all n are in different equivalence classes at the base type $\mathbb{N}$, we may conclude (1).

Applications *Inhabitants of* $\forall\alpha.\,(\alpha \to \alpha) \to \alpha \to \alpha$

?

Applications *Inhabitants of* $\forall\alpha.\,(\alpha \to \alpha) \to \alpha \to \alpha$

Fact Let *nat* be $\forall\alpha.\,(\alpha \to \alpha) \to \alpha \to \alpha$. If $M : \mathit{nat}$, then $M \cong_{\mathit{nat}} M_n$ for some integer n, where $M_n \triangleq \Lambda\alpha.\lambda f{:}\alpha \to \alpha.\,\lambda x{:}\alpha.\,f^n\,x$.

?

Applications *Inhabitants of* $\forall\alpha.\,(\alpha \to \alpha) \to \alpha \to \alpha$

Fact Let *nat* be $\forall\alpha.\,(\alpha \to \alpha) \to \alpha \to \alpha$. If $M : \textit{nat}$, then $M \cong_{\textit{nat}} M_n$ for some integer n, where $M_n \stackrel{\triangle}{=} \Lambda\alpha.\lambda f{:}\alpha \to \alpha.\, \lambda x{:}\alpha.\, f^n\, x$.

That is, the inhabitants of $\forall\alpha.\,(\alpha \to \alpha) \to \alpha \to \alpha$ are the Church naturals.

Applications *Inhabitants of* $\forall\alpha.\,(\alpha \to \alpha) \to \alpha \to \alpha$

Fact Let *nat* be $\forall\alpha.\,(\alpha \to \alpha) \to \alpha \to \alpha$. If $M : \textit{nat}$, then $M \simeq_{\textit{nat}} M_n$ for some integer n, where $M_n \triangleq \Lambda\alpha.\lambda f{:}\alpha \to \alpha.\,\lambda x{:}\alpha.\,f^n\,x$.

Proof

?

Applications *Inhabitants of* $\forall \alpha. (\alpha \to \alpha) \to \alpha \to \alpha$

Fact Let *nat* be $\forall \alpha. (\alpha \to \alpha) \to \alpha \to \alpha$. If $M : \mathit{nat}$, then $M \cong_{\mathit{nat}} M_n$ for some integer n, where $M_n \triangleq \Lambda \alpha. \lambda f : \alpha \to \alpha. \lambda x : \alpha. f^n\ x$.

Proof By *extensionality*, and *value arguments*, it suffices to show that there exists n such for any closed type ρ and closed values $V_1 : \rho \to \rho$ and $V_2 : \rho$, we have $M\ \rho\ V_1\ V_2 \cong_\rho M_n\ \rho\ V_1\ V_2$, or, by closure by inverse reduction and replacing observational by logical equivalence, $M\ \rho\ V_1\ V_2 \sim_\rho V_1^n\ V_2$, $(\mathbf{1})$.

?

Applications *Inhabitants of* $\forall\alpha.(\alpha \to \alpha) \to \alpha \to \alpha$

Fact Let *nat* be $\forall\alpha.(\alpha \to \alpha) \to \alpha \to \alpha$. If $M : \mathit{nat}$, then $M \cong_{\mathit{nat}} M_n$ for some integer n, where $M_n \triangleq \Lambda\alpha.\lambda f{:}\alpha \to \alpha.\,\lambda x{:}\alpha.\,f^n\,x$.

Proof By *extensionality*, and *value arguments*, it suffices to show that there exists n such for any closed type ρ and closed values $V_1 : \rho \to \rho$ and $V_2 : \rho$, we have $M\ \rho\ V_1\ V_2 \cong_\rho M_n\ \rho\ V_1\ V_2$, or, by closure by inverse reduction and replacing observational by logical equivalence, $M\ \rho\ V_1\ V_2 \sim_\rho V_1^n\ V_2$, $(\mathbf{1})$.

Let $V_1 : \rho \to \rho$ and $V_2 : \rho$ be fixed. Let Z and S be M_0 *nat* and M_1 *nat*.
Let η be $\alpha \mapsto R$ where $R : \mathit{nat} \leftrightarrow \rho$ defined as $\diamond^{R}_{\mathit{nat}\leftrightarrow\rho}\{(S^k\ Z,\ V_1^k\ V_2) \mid k \in \mathbb{N}\}$.
We have $Z \sim_\alpha V_2\ \ [\eta]$ since $R(Z, V_2)$ (reduce both sides for $k = 0$).

We also have $S \sim_{\alpha\to\alpha} V_1\ \ [\eta]$.

Indeed,

?

Applications — *Inhabitants of* $\forall\alpha.\,(\alpha\to\alpha)\to\alpha\to\alpha$

Fact Let *nat* be $\forall\alpha.\,(\alpha\to\alpha)\to\alpha\to\alpha$. If $M : \mathit{nat}$, then $M \cong_{\mathit{nat}} M_n$ for some integer n, where $M_n \triangleq \Lambda\alpha.\lambda f{:}\alpha\to\alpha.\,\lambda x{:}\alpha.\,f^n\,x$.

Proof By *extensionality*, and *value arguments*, it suffices to show that there exists n such for any closed type ρ and closed values $V_1 : \rho\to\rho$ and $V_2 : \rho$, we have $M\ \rho\,V_1\ V_2 \cong_\rho M_n\ \rho\,V_1\ V_2$, or, by closure by inverse reduction and replacing observational by logical equivalence, $M\ \rho\,V_1\ V_2 \sim_\rho V_1^n\ V_2$, $(\mathbf{1})$.

Let $V_1 : \rho\to\rho$ and $V_2 : \rho$ be fixed. Let Z and S be M_0 *nat* and M_1 *nat*.
Let η be $\alpha\mapsto R$ where $R : \mathit{nat}\leftrightarrow\rho$ defined as $\diamond^R_{\mathit{nat}\leftrightarrow\rho}\{(S^k\ Z,\ V_1^k\ V_2)\mid k\in\mathbb{N}\}$.
We have $Z \sim_\alpha V_2\ \ [\eta]$ since $R(Z, V_2)$ (reduce both sides for $k=0$).

We also have $S \sim_{\alpha\to\alpha} V_1\ \ [\eta]$.

Indeed, assume $N \sim_\alpha N'\ \ [\eta]$, *i.e.* $R(N, N')$.
There exists k such that $N \cong_{\mathit{nat}} S^k\ Z$ and $N' \cong_\rho V_1^k\ V_2$.
By congruence $S\,N \cong_{\mathit{nat}} S^{k+1}\ Z$ and $V_1\ N' \cong_\rho V_1^{k+1}\ V_2$.
Therefore $R(S\,N, V_1\ N')$, *i.e.* $S\,N \sim_\alpha V_1\ N'\ \ [\eta]$.

Applications *Inhabitants of* $\forall\alpha.\,(\alpha \to \alpha) \to \alpha \to \alpha$

Fact Let *nat* be $\forall\alpha.\,(\alpha \to \alpha) \to \alpha \to \alpha$. If $M : \textit{nat}$, then $M \cong_{\textit{nat}} M_n$ for some integer n, where $M_n \triangleq \Lambda\alpha.\lambda f{:}\alpha \to \alpha.\,\lambda x{:}\alpha.\,f^n\,x$.

Proof By *extensionality*, and *value arguments*, it suffices to show that there exists n such for any closed type ρ and closed values $V_1 : \rho \to \rho$ and $V_2 : \rho$, we have $M\ \rho\, V_1\ V_2 \cong_\rho M_n\ \rho\, V_1\ V_2$, or, by closure by inverse reduction and replacing observational by logical equivalence, $M\ \rho\, V_1\ V_2 \sim_\rho V_1^n\ V_2$, $(\mathbf{1})$.

Let $V_1 : \rho \to \rho$ and $V_2 : \rho$ be fixed. Let Z and S be M_0 *nat* and M_1 *nat*.
Let η be $\alpha \mapsto R$ where $R : \textit{nat} \leftrightarrow \rho$ defined as $\diamond^R_{\textit{nat}\leftrightarrow\rho}\{(S^k\ Z,\ V_1^k\ V_2) \mid k \in \mathbb{N}\}$.
We have $Z \sim_\alpha V_2\ \ [\eta]$ since $R(Z, V_2)$ (reduce both sides for $k = 0$).

We also have $S \sim_{\alpha\to\alpha} V_1\ \ [\eta]$. (A key to the proof.)

?

Applications *Inhabitants of* $\forall\alpha.\,(\alpha \to \alpha) \to \alpha \to \alpha$

Fact Let *nat* be $\forall\alpha.\,(\alpha \to \alpha) \to \alpha \to \alpha$. If $M : \mathit{nat}$, then $M \cong_{\mathit{nat}} M_n$ for some integer n, where $M_n \triangleq \Lambda\alpha.\lambda f\!:\!\alpha \to \alpha.\,\lambda x\!:\!\alpha.\,f^n\,x$.

Proof By *extensionality*, and *value arguments*, it suffices to show that there exists n such for any closed type ρ and closed values $V_1 : \rho \to \rho$ and $V_2 : \rho$, we have $M\ \rho\ V_1\ V_2 \cong_\rho M_n\ \rho\ V_1\ V_2$, or, by closure by inverse reduction and replacing observational by logical equivalence, $M\ \rho\ V_1\ V_2 \sim_\rho V_1^n\ V_2$, $(\mathbf{1})$.

Let $V_1 : \rho \to \rho$ and $V_2 : \rho$ be fixed. Let Z and S be $M_0\ \mathit{nat}$ and $M_1\ \mathit{nat}$.
Let η be $\alpha \mapsto R$ where $R : \mathit{nat} \leftrightarrow \rho$ defined as $\diamond^R_{\mathit{nat}\leftrightarrow\rho}\{(S^k\ Z,\ V_1^k\ V_2) \mid k \in \mathbb{N}\}$.
We have $Z \sim_\alpha V_2\ \ [\eta]$ since $R(Z, V_2)$ (reduce both sides for $k = 0$).

We also have $S \sim_{\alpha\to\alpha} V_1\ \ [\eta]$. (A key to the proof.)

By parametricity, we have $M \sim_{\mathit{nat}} M$.

?

Applications *Inhabitants of* $\forall\alpha.\,(\alpha \to \alpha) \to \alpha \to \alpha$

Fact Let *nat* be $\forall\alpha.\,(\alpha \to \alpha) \to \alpha \to \alpha$. If $M : \mathit{nat}$, then $M \simeq_{\mathit{nat}} M_n$ for some integer n, where $M_n \stackrel{\triangle}{=} \Lambda\alpha.\lambda f{:}\alpha \to \alpha.\,\lambda x{:}\alpha.\,f^n\,x$.

Proof By *extensionality*, and *value arguments*, it suffices to show that there exists n such for any closed type ρ and closed values $V_1 : \rho \to \rho$ and $V_2 : \rho$, we have $M\ \rho\, V_1\ V_2 \simeq_\rho M_n\ \rho\, V_1\ V_2$, or, by closure by inverse reduction and replacing observational by logical equivalence, $M\ \rho\, V_1\ V_2 \sim_\rho V_1^n\ V_2$, $(\mathbf{1})$.

Let $V_1 : \rho \to \rho$ and $V_2 : \rho$ be fixed. Let Z and S be M_0 *nat* and M_1 *nat*.
Let η be $\alpha \mapsto R$ where $R : \mathit{nat} \leftrightarrow \rho$ defined as $\diamond^R_{\mathit{nat}\leftrightarrow\rho}\{(S^k\ Z,\ V_1^k\ V_2) \mid k \in \mathbb{N}\}$.
We have $Z \sim_\alpha V_2\ \ [\eta]$ since $R(Z, V_2)$ (reduce both sides for $k = 0$).

We also have $S \sim_{\alpha\to\alpha} V_1\ \ [\eta]$. (A key to the proof.)

By parametricity, we have $M \sim_{\mathit{nat}} M$. Hence, $M\ \mathit{nat}\ S\ Z \sim_\alpha M\ \rho\, V_1\ V_2\ \ [\eta]$, *i.e.* $R(M\ \mathit{nat}\ S\ Z, M\ \rho\, V_1\ V_2)$ which means that there exists n such that $M\ \mathit{nat}\ S\ Z \sim_{\mathit{nat}} S^n\ \ Z$ and $M\ \rho\, V_1\ V_2 \sim_\rho V_1^n\ V_2$.

?

Applications *Inhabitants of* $\forall\alpha.(\alpha \to \alpha) \to \alpha \to \alpha$

Fact Let *nat* be $\forall\alpha.(\alpha \to \alpha) \to \alpha \to \alpha$. If $M : \mathit{nat}$, then $M \cong_{\mathit{nat}} M_n$ for some integer n, where $M_n \stackrel{\triangle}{=} \Lambda\alpha.\lambda f{:}\alpha \to \alpha.\,\lambda x{:}\alpha.\,f^n\,x$.

Proof By *extensionality*, and *value arguments*, it suffices to show that there exists n such for any closed type ρ and closed values $V_1 : \rho \to \rho$ and $V_2 : \rho$, we have $M\;\rho\;V_1\;V_2 \cong_\rho M_n\;\rho\;V_1\;V_2$, or, by closure by inverse reduction and replacing observational by logical equivalence, $M\;\rho\;V_1\;V_2 \sim_\rho V_1^n\;V_2$, (**1**).

Let $V_1 : \rho \to \rho$ and $V_2 : \rho$ be fixed. Let Z and S be $M_0\;\mathit{nat}$ and $M_1\;\mathit{nat}$.
Let η be $\alpha \mapsto R$ where $R : \mathit{nat} \leftrightarrow \rho$ defined as $\diamond^R_{\mathit{nat}\leftrightarrow\rho}\{(S^k\;Z,\;V_1^k\;V_2) \mid k \in \mathbb{N}\}$.
We have $Z \sim_\alpha V_2\;\;[\eta]$ since $R(Z, V_2)$ (reduce both sides for $k = 0$).

We also have $S \sim_{\alpha\to\alpha} V_1\;\;[\eta]$. (A key to the proof.)

By parametricity, we have $M \sim_{\mathit{nat}} M$. Hence, $M\;\mathit{nat}\;S\;Z \sim_\alpha M\;\rho\;V_1\;V_2\;\;[\eta]$, *i.e.* $R(M\;\mathit{nat}\;S\;Z, M\;\rho\;V_1\;V_2)$ which means that there exists n such that $M\;\mathit{nat}\;S\;Z \sim_{\mathit{nat}} S^n\;\;Z$ and $M\;\rho\;V_1\;V_2 \sim_\rho V_1^n\;V_2$.

Since, $M\;\mathit{nat}\;S\;Z$ is independent of n, we may conclude (1), provided the $S^n\;Z$ are all in different equivalence classes.

Applications $\quad sort : \forall\alpha.\,(\alpha \to \alpha \to \mathit{bool}) \to \mathit{list}\,\alpha$

Property Assume *sort* : $\forall\alpha.\,(\alpha \to \alpha \to \mathit{bool}) \to \mathit{list}\,\alpha \to \mathit{list}\,\alpha$ $(\mathbf{2})$. Then

$$(\forall x, y,\ \ \mathit{cmp}_2\ (f\ x)\ (f\ y) = \mathit{cmp}_1\ \ x\ y) \implies \forall \ell,\ \ \mathit{sort}\ \ \mathit{cmp}_2\ (\mathit{map}\ f\ \ell) = \mathit{map}\ f\ (\mathit{sort}\ \mathit{cmp}_1\ \ell)$$

Applications $\quad sort : \forall \alpha. (\alpha \to \alpha \to \mathit{bool}) \to \mathit{list}\, \alpha$

Proof We have *sort* $\sim_\sigma$ *sort* where σ is $\forall \alpha. (\alpha \to \alpha \to \mathit{bool}) \to \mathit{list}\, \alpha \to \mathit{list}\, \alpha$.

By definition, for all ρ_1, ρ_2, and all admissible relations $R : \delta_1 \leftrightarrow \delta_2$, where δ_i is $\alpha \mapsto \rho_i$ for all cp_1, cp_2,

$$\begin{aligned} &\forall \mathit{cp}_1, \mathit{cp}_2, \quad \mathit{cp}_1 \sim_{\alpha \to \alpha \to \mathsf{B}} \mathit{cp}_2\, [\eta] \implies && \textbf{(3)} \\ &\quad \forall V_1, V_2, \ (V_1 \sim_{\mathit{list}\,\alpha} V_2 \ [\eta] \implies \mathit{sort}\, \rho_1\, \mathit{cp}_1\ V_1 \sim_{\mathit{list}\,\alpha} \mathit{sort}\, \rho_2\, \mathit{cp}_2\ V_2\ [\eta]) && \textbf{(4)} \end{aligned}$$

We may restrict $R(N_1, N_2)$, *i.e.* $N_1 \sim_\alpha N_2$ to $N_2 = g\, N_1$ for some function g. Then $N_1 \sim_{\mathit{list}\,\alpha} N_2\ [\eta]$ iff $N_2 = \mathit{map}\, g\, N_1$. Thus, (4) becomes

$$\forall V_1 : \mathit{list}\, \rho, \ \ \mathit{sort}\, \rho_2\, \mathit{cp}_2\ (\mathit{map}\, g\, V_1) = \mathit{map}\, g\, (\mathit{sort}\, \rho_1\, \mathit{cp}_1\ V_1)$$

While (3) means

$$\forall V_1, V_1', V_2, V_2', \ \ V_1 \sim_\alpha V_2\ [\eta] \wedge V_1' \sim_\alpha V_2'\ [\eta] \implies \mathit{cp}_1\, V_1\, V_1' \sim_{\mathsf{B}} \mathit{cp}_2\, V_2\, V_2'\ [\eta]$$

i.e.

$$\forall V, W : \rho, \ \ \mathit{cp}_1\, V\, W \simeq_{\mathsf{B}} \mathit{cp}_2\, (g\, V)\, (g\, W)$$

Encodable features — Natural numbers

We have shown that all expressions of type *nat* behave as natural numbers. Hence, natural numbers are definable.

Still, we could also provide a type *nat* of natural numbers as primitive.

Then, if $M : nat$ and $M' : nat$, we have $M \simeq_{nat} M'$ iff there exists $V : nat$ such that $M \Downarrow V$ and $M' \Downarrow V$.

Then logical equivalence is defined as $M \sim_{nat} M' \ [\eta]$ iff $M \simeq_{nat} M'$

All properties are preserved.

Encodable features

Products

Given closed types τ_1 and τ_2, we defined

$$\begin{array}{rcl} \tau_1 \times \tau_2 & \stackrel{\triangle}{=} & \forall\alpha.\, (\tau_1 \to \tau_2 \to \alpha) \to \alpha \\ (M_1, M_2) & \stackrel{\triangle}{=} & \Lambda\alpha.\lambda x{:}\tau_1 \to \tau_2 \to \alpha.\, x\; M_1\; M_2 \\ M.i & \stackrel{\triangle}{=} & M\; (\lambda x_1{:}\tau_1.\, \lambda x_2{:}\tau_2.\, x_i) \end{array}$$

Facts

If $M : \tau_1 \times \tau_2$, then $M \cong_{\tau_1 \times \tau_2} (M_1, M_2)$ for some $M_1 : \tau_1$ and $M_2 : \tau_2$.

If $M : \tau_1 \times \tau_2$ and $M.1 \cong_{\tau_1} M_1$ and $M.2 \cong_{\tau_2} M_2$, then $M \cong_{\tau_1 \times \tau_2} (M_1, M_2)$

Primitive pairs

We may instead extend the language with *primitive* pairs.
Then, we define:

$$M \sim_{\tau_1 \times \tau_2} M' \; [\eta : \delta \leftrightarrow \delta'] \iff \forall i \in \{1, 2\},\; M.i \sim_{\tau_i} M'.i \; [\eta : \delta \leftrightarrow \delta']$$

Representation independence

A client of an existential type $\exists\alpha.\,\tau$ should not see the difference between two implementations N_1 and N_2 of $\exists\alpha.\,\tau$ with witness types σ_1 and σ_2.

A client M has type $\forall\alpha.\,\tau \to \tau'$ with $\alpha \notin \mathrm{fv}(\tau')$; it must use the argument parametrically, and the result is independent of the witness type.

Assume that σ_1 and σ_2 are two closed representation types and $R : \sigma_1 \leftrightarrow \sigma_2$ is an admissible relation between them.

Suppose that $N_1 : \tau[\alpha \mapsto \sigma_1]$ and $N_2 : \tau[\alpha \mapsto \sigma_2]$ are two equivalent implementations of the operations, *i.e.* such that $N_1 \sim_\tau N_2\ \ [\eta : \delta_1 \leftrightarrow \delta_2]$ where $\eta : \alpha \mapsto R$ and $\delta_1 : \alpha \mapsto \sigma_1$ and $\delta_2 : \alpha \mapsto \sigma_2$.

A client M satisfies $M \sim_{\forall\alpha.\,\tau\to\tau'} M\ \ [\eta : \delta \leftrightarrow \delta']$ and, in fact, $M \sim_{\forall\alpha.\,\tau\to\tau'} M$ since α does not appear free in τ'.

Thus $M\ \sigma_1\ N_1 \cong_{\tau'} M\ \sigma_2\ N_2$. That is, the behavior with the implementation N_1 with representation type σ_1 is indistinguishable from the behavior with implementation N_2 with representation type σ_2.

Contents

Existential types

Definition?

$$\textit{pack}\ N_1, \rho_1\ \textit{as}\ \exists\alpha.\tau \ \sim_{\exists\alpha.\tau}\ \textit{pack}\ N_2, \rho_2\ \textit{as}\ \exists\alpha.\tau\ \ [\eta : \delta_1 \leftrightarrow \delta_2]$$
$$\text{iff}\quad \textit{there exist}\ R : \rho_1 \leftrightarrow \rho_2,$$
$$N_1 \sim_\tau N_2\ \ [(\eta, \alpha \mapsto R) : (\delta_1, \alpha \mapsto \rho_1) \leftrightarrow (\delta_2, \alpha \mapsto \rho_2)]$$

This definition is correct but incomplete as it only relates terms of existential types in head normal forms.
We may extend it to a relation between arbitrary terms by anti-reduction closure.

Alternative definition

Instead of defining the relation on terms, we may define the relation on values and lift it to a relation on terms by anti-reduction closure.

$\mathsf{tt} \approx_{\mathsf{B}} \mathsf{tt} \;\; [\eta] \wedge \mathsf{ff} \approx_{\mathsf{B}} \mathsf{ff} \;\; [\eta]$

$\lambda x{:}\tau.\, M_1 \approx_{\tau \to \tau'} \lambda x{:}\tau.\, M_2 \;\; [\eta]$
$\quad \iff \forall V_1, V_2,\; V_1 \approx_\tau V_2 \;\; [\eta] \implies (\lambda x{:}\tau.\, M_1)\, V_1 \sim_{\tau_2} (\lambda x{:}\tau'.\, M_2)\, V_2 \;\; [\eta]$

$V_1 \approx_\alpha V_2 \;\; [\eta]$
$\quad \iff \eta(\alpha)(V_1, V_2)$

$\Lambda\alpha.V_1 \approx_{\forall\alpha.\,\tau} \Lambda\alpha.V_2 \;\; [\eta]$
$\quad \iff \forall \rho_1, \rho_2, R : \rho_1 \leftrightarrow \rho_2, (\Lambda\alpha.V_1)\, \rho_1 \sim_\tau (\Lambda\alpha.V_2)\, \rho_2 \;\; [\eta, \alpha \mapsto R]$

$\textit{pack}\; V_1, \rho_1 \;\textit{as}\; \exists\alpha.\,\tau \approx_{\exists\alpha.\,\tau} \textit{pack}\; V_2, \rho_2 \;\textit{as}\; \exists\alpha.\,\tau \;\; [\eta]$
$\quad \iff \exists R : \rho_1 \leftrightarrow \rho_2, V_1 \approx_{\eta, \rho \mapsto R} V_2 \;\; [\eta, \alpha \mapsto R]$

$M_1 \sim_\tau M_2 \;\; [\eta] \iff \exists V_1, V_2, M_1 \Downarrow V_1 \wedge M_2 \Downarrow V_2 \wedge V_1 \approx_\tau V_2 \;\; [\eta]$

where $R : \rho_1 \leftrightarrow \rho_2$ means a relation between values of type τ_1 and τ_2.
(We may require compatibility with observational equivalence on values.)

Alternative definition (variant)

$$
\begin{array}{rcl}
\mathcal{V}[\![\mathsf{B}]\!]_\eta & = & \{(\mathsf{tt},\mathsf{tt}),(\mathsf{ff},\mathsf{ff})\} \\
\mathcal{V}[\![\tau \to \tau']\!]_\eta & = & \{(\lambda x{:}\tau.\,M_1, \lambda x{:}\tau.\,M_2) \mid \forall (V_1,V_2) \in \mathcal{V}[\![\tau]\!]_\eta, \\
& & \quad ((\lambda x{:}\tau.\,M_1)\ V_1, (\lambda x{:}\tau.\,M_2)\ V_2) \in \mathcal{E}[\![\tau']\!]_\eta\} \\
\mathcal{V}[\![\alpha]\!]_\eta & = & \eta(\alpha) \\
\mathcal{V}[\![\forall\alpha.\,\tau]\!]_\eta & = & \{(\Lambda\alpha.V_1, \Lambda\alpha.V_2) \mid \forall \rho_1,\rho_2,R : \rho_1 \leftrightarrow \rho_2, \\
& & \quad ((\Lambda\alpha.V_1)\ \rho_1, (\Lambda\alpha.V_2)\ \rho_2 \in \mathcal{E}[\![\tau]\!]_{\eta,\alpha\mapsto R}\} \\
\mathcal{V}[\![\exists\alpha.\,\tau]\!]_\eta & = & \{(\mathit{pack}\ V_1,\rho_1\ \mathit{as}\ \exists\alpha.\,\tau, \mathit{pack}\ V_2,\rho_2\ \mathit{as}\ \exists\alpha.\,\tau) \\
& & \quad \mid \exists R : \rho_1 \leftrightarrow \rho_2, (V_1,V_2) \in \mathcal{V}[\![\tau]\!]_{\eta,\alpha\mapsto R}\}
\end{array}
$$

$$
\mathcal{E}[\![\tau]\!]_\eta = \{(M_1,M_2) \mid \exists (V_1,V_2) \in \mathcal{V}[\![\tau]\!]_\eta, M_1 \Downarrow V_1 \wedge M_2 \Downarrow V_2\}
$$

Existential types *Example*

Consider $V_1 \triangleq (\textit{not}, \mathsf{tt})$, and $V_2 \triangleq (\textit{succ}, 0)$ and $\sigma \triangleq (\alpha \to \alpha) \times \alpha$.
Let $R : \textit{bool} \leftrightarrow \textit{nat}$ be $\{(\mathsf{tt}, 2n), (\mathsf{ff}, 2n+1) \mid n \in \mathbb{N}\}$ and η be $\alpha \mapsto R$.

We have $(V_1, V_2) \in \mathcal{V}[\![\sigma]\!]_\eta$.

Hence, $(\textit{pack}\, V_1, \textit{bool as}\, \exists\alpha.\, \sigma,\ \textit{pack}\, V_2, \textit{nat as}\, \exists\alpha.\, \sigma) \in \mathcal{V}[\![\exists\alpha.\, \sigma]\!]$.

Proof of $\big((\textit{not}, \mathsf{tt}), (\textit{succ}, 0)\big) \in \mathcal{V}[\![(\alpha \to \alpha) \times \alpha]\!]_\eta$ **(1)**

?

Existential types *Example*

Consider $V_1 \triangleq (\textit{not}, \mathsf{tt})$, and $V_2 \triangleq (\textit{succ}, 0)$ and $\sigma \triangleq (\alpha \to \alpha) \times \alpha$.
Let $R : \textit{bool} \leftrightarrow \textit{nat}$ be $\{(\mathsf{tt}, 2n), (\mathsf{ff}, 2n+1) \mid n \in \mathbb{N}\}$ and η be $\alpha \mapsto R$.

We have $(V_1, V_2) \in \mathcal{V}[\![\sigma]\!]_\eta$.

Hence, $(\textit{pack}\, V_1, \textit{bool as}\, \exists\alpha.\, \sigma,\ \textit{pack}\, V_2, \textit{nat as}\, \exists\alpha.\, \sigma) \in \mathcal{V}[\![\exists\alpha.\, \sigma]\!]$.

Proof of $\big((\textit{not}, \mathsf{tt}), (\textit{succ}, 0)\big) \in \mathcal{V}[\![(\alpha \to \alpha) \times \alpha]\!]_\eta$ **(1)**

?

Existential types *Example*

Consider $V_1 \triangleq (\textit{not}, \mathrm{tt})$, and $V_2 \triangleq (\textit{succ}, 0)$ and $\sigma \triangleq (\alpha \to \alpha) \times \alpha$.
Let $R : \textit{bool} \leftrightarrow \textit{nat}$ be $\{(\mathrm{tt}, 2n), (\mathrm{ff}, 2n+1) \mid n \in \mathbb{N}\}$ and η be $\alpha \mapsto R$.

We have $(V_1, V_2) \in \mathcal{V}[\![\sigma]\!]_\eta$.

Hence, $(\textit{pack}\, V_1, \textit{bool as}\; \exists\alpha.\, \sigma,\ \textit{pack}\, V_2, \textit{nat as}\; \exists\alpha.\, \sigma) \in \mathcal{V}[\![\exists\alpha.\, \sigma]\!]$.

Proof of $\big((\textit{not}, \mathrm{tt}), (\textit{succ}, 0)\big) \in \mathcal{V}[\![(\alpha \to \alpha) \times \alpha]\!]_\eta$ $\mathbf{(1)}$

We have $(\mathrm{tt}, 0) \in \mathcal{V}[\![\alpha]\!]_\eta$, since $(\mathrm{tt}, 0) \in R$.
We also have $(\textit{not}, \textit{succ}) \in \mathcal{V}[\![\alpha \to \alpha]\!]_\eta$ which proves (1).

?

Existential types *Example*

Consider $V_1 \triangleq (\textit{not}, \mathrm{tt})$, and $V_2 \triangleq (\textit{succ}, 0)$ and $\sigma \triangleq (\alpha \to \alpha) \times \alpha$.
Let $R : \textit{bool} \leftrightarrow \textit{nat}$ be $\{(\mathrm{tt}, 2n), (\mathrm{ff}, 2n+1) \mid n \in \mathbb{N}\}$ and η be $\alpha \mapsto R$.

We have $(V_1, V_2) \in \mathcal{V}[\![\sigma]\!]_\eta$.

Hence, $(\textit{pack}\, V_1, \textit{bool}\ \textit{as}\ \exists\alpha.\,\sigma,\ \textit{pack}\, V_2, \textit{nat}\ \textit{as}\ \exists\alpha.\,\sigma) \in \mathcal{V}[\![\exists\alpha.\,\sigma]\!]$.

Proof of $\big((\textit{not}, \mathrm{tt}), (\textit{succ}, 0)\big) \in \mathcal{V}[\![(\alpha \to \alpha) \times \alpha]\!]_\eta$ **(1)**

We have $(\mathrm{tt}, 0) \in \mathcal{V}[\![\alpha]\!]_\eta$, since $(\mathrm{tt}, 0) \in R$.
We also have $(\textit{not}, \textit{succ}) \in \mathcal{V}[\![\alpha \to \alpha]\!]_\eta$ which proves (1).

Indeed, assume $(W_1, W_2) \in \mathcal{V}[\![\alpha]\!]_\eta$. Then (W_1, W_2) is either of the form

- $(\mathrm{tt}, 2n)$ and $(\textit{not}\, W_1, \textit{succ}\, W_2)$ reduces to $(\mathrm{ff}, 2n+1)$, or
- $(\mathrm{ff}, 2n+1)$ and $(\textit{not}\, W_1, \textit{succ}\, W_2)$ reduces to $(\mathrm{tt}, 2n+2)$.

In both cases, $(\textit{not}\, W_1, \textit{succ}\, W_2)$ reduces to a pair in R.
Hence, $(\textit{not}\, W_1, \textit{succ}\, W_2) \in \mathcal{E}[\![\alpha]\!]_\eta$.

Extensions to products and sums

$$\mathcal{V}[\![\tau \times \tau']\!]_\eta = \{(V_1, V_2) \mid V_1 \in \mathcal{V}[\![\tau]\!]_\eta \wedge V_2 \in \mathcal{V}[\![\tau']\!]_\eta\}$$

$$\begin{aligned}\mathcal{V}[\![\tau + \tau']\!]_\eta = {} & \{(\mathit{inj}_1\ V_1, \mathit{inj}_1\ V_2) \mid (V_1, V_2) \in \mathcal{V}[\![\tau]\!]_\eta\} \ \cup \\ & \{(\mathit{inj}_2\ V_2, \mathit{inj}_2\ V_2) \mid (V_1, V_2) \in \mathcal{V}[\![\tau']\!]_\eta\}\end{aligned}$$

How do we deal with recursive types?

Assume that we allow equi-recursive types.

$$\tau ::= \ldots \mid \mu\alpha.\tau$$

A naive definition would be

$$\mathcal{V}[\![\mu\alpha.\tau]\!]_\eta = \mathcal{V}[\![[\alpha \mapsto \mu\alpha.\tau]\tau]\!]_\eta$$

But this is ill-founded.

The solution is to use indexed-logical relations.

We use a sequence of decreasing relations indexed by integers (fuel), which is consumed during unfolding of recursive types.

Step-indexed logical relations (a taste)

We define a sequence $\mathcal{V}_k[\![\tau]\!]_\eta$ indexed by natural numbers $n \in \mathbb{N}$ that relates values of type τ up to n reduction steps.

$$
\begin{aligned}
\mathcal{V}_k[\![\mathsf{B}]\!]_\eta &= \{(\mathsf{tt}, \mathsf{tt}), (\mathsf{ff}, \mathsf{ff})\} \\
\mathcal{V}_k[\![\tau \to \tau']\!]_\eta &= \{(\lambda x{:}\tau.\, M_1, \lambda x{:}\tau.\, M_2) \mid \forall j < k, \forall (N_1, N_2) \in \mathcal{V}_j[\![\tau]\!]_\eta, \\
&\qquad ((\lambda x{:}\tau.\, M_1)\ N_1, (\lambda x{:}\tau.\, M_2)\ N_2) \in \mathcal{E}_j[\![\tau']\!]_\eta\} \\
\mathcal{V}_k[\![\alpha]\!]_\eta &= \eta(\alpha).k \\
\mathcal{V}_k[\![\forall \alpha.\, \tau]\!]_\eta &= \{(\Lambda\alpha_1.V_1, \Lambda\alpha_2.V_2) \mid \forall \rho_1, \rho_2, R \in \mathcal{R}^k(\rho_1, \rho_2), \\
&\qquad \forall j < k, ((\Lambda\alpha.V_1)\ \rho_1, (\Lambda\alpha.V_2)\ \rho_2) \in \mathcal{V}_j[\![\tau]\!]_{\eta, \rho \mapsto R}\} \\
\mathcal{V}_k[\![\mu\alpha.\tau]\!]_\eta &= \mathcal{V}_{k-1}[\![[\alpha \mapsto \mu\alpha.\tau]\tau]\!]_\eta
\end{aligned}
$$

$$
\begin{aligned}
\mathcal{E}_k[\![\tau]\!]_\eta &= \{(M_1, M_2) \mid \forall j < k, M_1 \Downarrow_j V_1 \\
&\qquad \Longrightarrow \exists V_2, M_2 \Downarrow V_2 \wedge (V_1, V_2) \in \mathcal{V}_{k-j}[\![\tau]\!]_\eta\}
\end{aligned}
$$

By $\Downarrow_j$ means *reduces in j-steps*

$\mathcal{R}^j(\rho_1, \rho_2)$ is a sequence of decreasing relations between closed values of closed types ρ_1 and ρ_2 of length (at least) j.

Step-indexed logical relations (a taste)

The relation is asymmetric.

If $\Delta;\Gamma \vdash M_1, M_2 : \tau$ we define $\Delta;\Gamma \vdash M_1 \lesssim M_2 : \tau$ as

$$\forall \eta \in \mathcal{R}^k_\Delta(\delta_1,\delta_2), \forall(\gamma_1,\gamma_2) \in \mathcal{G}_k[\![\Gamma]\!],\ \ (\gamma_1(\delta_1(M_1)), \gamma_2(\delta_2(M_2))) \in \mathcal{E}_k[\![\tau]\!]_\eta$$

and

$$\Delta;\Gamma \vdash M_1 \sim M_2 : \tau \ \ \triangleq\ \ \bigwedge \begin{cases} \Delta;\Gamma \vdash M_1 \lesssim M_2 : \tau \\ \Delta;\Gamma \vdash M_2 \lesssim M_1 : \tau \end{cases}$$

There are some subtleties...

Bibliography I

(Most titles have a clickable mark "▷" that links to online versions.)

▷ Jean-Philippe Bernardy, Patrik Jansson, and Koen Claessen. *Testing Polymorphic Properties, pages 125–144.* Springer Berlin Heidelberg, Berlin, Heidelberg, 2010. ISBN 978-3-642-11957-6. doi: $10.1007/978\text{-}\sigma_2 3\text{-}\sigma_2 642\text{-}\sigma_2 11957\text{-}\sigma_2 6\_8$.

Robert Harper. *Practical Foundations for Programming Languages.* Cambridge University Press, 2012.

J. Roger Hindley and Jonathan P. Seldin. *Introduction to Combinators and Lambda-Calculus.* Cambridge University Press, 1986.

Benjamin C. Pierce. *Types and Programming Languages.* MIT Press, 2002.

▷ Andrew M. Pitts. Parametric polymorphism and operational equivalence. *Mathematical Structures in Computer Science*, 10:321–359, 2000.

Bibliography II

- John C. Reynolds. Types, abstraction and parametric polymorphism. In *Information Processing 83*, pages 513–523. Elsevier Science, 1983.
- W. W. Tait. Intensional interpretations of functionals of finite type i. *The Journal of Symbolic Logic*, 32(2):pp. 198–212, 1967. ISSN 00224812.
- Philip Wadler. Theorems for free! In *Conference on Functional Programming Languages and Computer Architecture (FPCA)*, pages 347–359, September 1989.
- Philip Wadler. The Girard-Reynolds isomorphism (second edition). *Theoretical Computer Science*, 375(1–3):201–226, May 2007.