Semantics of Functional Programming

Computational Adequacy

Chen, Liang-Ting
lxc@iis.sinica.edu.tw

Formosan Summer School on Logic, Language, and Computation 2014

Overview
So far we have given two kinds of semantics for **PCF**. For a well-typed closed terms M of type σ,

- one gives how the well-typed closed term M is evaluated to a value V via the reduction relation $\mathsf{M} \Downarrow \mathsf{V}$;
- the other defines what the denotation $[\![\mathsf{M}]\!]$ of M is in a domain D_σ.

In this lecture, we will compare these two approaches and discuss some issues arising from them:

Correctness $\mathsf{M} \Downarrow \mathsf{V}$ implies $[\![\mathsf{M}]\!] = [\![\mathsf{V}]\!]$.

Completeness $[\![\mathsf{M}]\!] = n$ implies $\mathsf{M} \Downarrow \underline{n}$

Computational adequacy Both of correctness and completeness hold.

1 Correctness

`nat` values always converges
The bottom element $\perp$ models the divergence of computation. A value of `nat` is meant to be some natural number, so it shouldn't diverge.

Lemma 1. *For every value* V *of type* `nat`*, the denotation* $[\![\mathsf{V}]\!]$ *is an element of* $\mathbb{N}$*. In particular,* $[\![\mathsf{V}]\!] \neq \perp$*.*

Proof. By structural induction on values:

$$\frac{}{\mathtt{zero}\ \mathbf{val}}$$

$$\frac{\mathsf{M}\ \mathbf{val}}{\mathtt{suc}\ \mathsf{M}\ \mathbf{val}}$$

$$\frac{\mathsf{M}\ \mathbf{term}}{\lambda x.\, \mathsf{M}\ \mathbf{val}}$$

□

Theorem 2. *For every two well-typed closed terms* M *and* V*,* $\mathsf{M} \Downarrow \mathsf{V}$ *implies* $[\![\mathsf{M}]\!] = [\![\mathsf{V}]\!]$*.*

Proof sketch. Prove $[\![\mathsf{M}]\!] = [\![\mathsf{V}]\!] \in [\![\tau]\!]$ by structural induction on the derivation of $\mathsf{M} \Downarrow \mathsf{V}$. □

We show the case ($\Downarrow$-suc) first and the cases ($\Downarrow$-zero) and ($\Downarrow$-lam) are similar and straightforward.

- For ($\Downarrow$-suc), we show that $[\![\mathtt{suc}\ \mathsf{M}]\!] = [\![\mathtt{suc}\ \mathsf{V}]\!]$ if $[\![\mathsf{M}]\!] = [\![\mathsf{V}]\!]$. By definition, we simply calculate its denotation directly:

$$[\![\mathtt{suc}\ \mathsf{M}]\!] = S([\![\mathsf{M}]\!]) = S([\![\mathsf{V}]\!]) = [\![\mathtt{suc}\ \mathsf{V}]\!]$$

  where the middle equality follows from the induction hypothesis.

Try to do the cases ($\Downarrow$-zero), ($\Downarrow$-lam), and ($\Downarrow$-$\mathtt{ifz}_0$).
The case ($\Downarrow$-app) is interesting, because there is the binding structure.

- For ($\Downarrow$-app), we show that $[\![\mathsf{M}\ \mathsf{N}]\!] = [\![V]\!]$ if $[\![\mathsf{M}]\!] = [\![\lambda x.\, \mathsf{E}]\!]$ and $[\![\mathsf{E}[\mathsf{N}/x]]\!] = [\![V]\!]$. We calculate the denotation as follows

$$\begin{aligned}[\![\mathsf{M}\ \mathsf{N}]\!] &= ev([\![\mathsf{M}]\!], [\![\mathsf{N}]\!]) \\ &= ev([\![\lambda x.\, \mathsf{E}]\!], [\![\mathsf{N}]\!]) \\ &= ev([\![x : \sigma \vdash \mathsf{E} : \tau]\!], [\![\mathsf{N}]\!]) \\ &= [\![x : \sigma \vdash \mathsf{E} : \tau]\!]([\![\mathsf{N}]\!]) = [\![\mathsf{E}[\mathsf{N}/x]]\!] = [\![\mathsf{V}]\!]\end{aligned}$$

  where $[\![x : \sigma \vdash \mathsf{E} : \tau]\!]([\![\mathsf{N}]\!]) = [\![\mathsf{E}[\mathsf{N}/x]]\!]$ follows from Substitution Lemma.

- Complete the cases ($\Downarrow$-$\mathtt{ifz}_1$) and ($\Downarrow$-fix). *Hint.* Consider Substitution Lemma and the properties of the fixpoint operator μ.

- For ($\Downarrow$-$\mathtt{ifz}_0$), assuming $[\![\mathsf{M}]\!] = [\![\mathtt{zero}]\!] = 0$ and $[\![\mathsf{M}_0]\!] = [\![V]\!]$ we show that $[\![\mathtt{ifz}(\mathsf{M}; \mathsf{M}_0; x.\, \mathsf{M}_1)]\!] = [\![\mathsf{V}]\!]$. We calculate the denotation as follows

$$\begin{aligned}&[\![\mathtt{ifz}(\mathsf{M}; \mathsf{M}_0; x.\, \mathsf{M}_1)]\!] \\ =&\, \mathit{ifz}([\![\mathsf{M}]\!], [\![\mathsf{M}_0]\!], [\![\mathsf{M}_1]\!]) \\ =&\, \mathit{ifz}(0, [\![V]\!], [\![\mathsf{M}_1]\!]) \\ =&\, [\![V]\!]\end{aligned}$$

where the last equation follows from the definition of *ifz*.

- For ($\Downarrow$-$\texttt{ifz}_1$), we show that $[\![\texttt{ifz}(\mathsf{M}; \mathsf{M}_0; x.\, \mathsf{M}_1)]\!] = [\![\mathsf{V}]\!]$ if $[\![\mathsf{M}]\!] = [\![\texttt{suc}\ \mathsf{N}]\!] = S([\![\mathsf{N}]\!])$ and $[\![\mathsf{M}_1[\mathsf{N}/x]]\!] = [\![\mathsf{V}]\!]$.

  We know that N is a value by $\mathsf{M} \Downarrow \texttt{suc}\ \mathsf{N}$[1], so $[\![\mathsf{N}]\!] = n$ for some natural number n. It follows that

  $$\begin{aligned} & [\![\texttt{ifz}(\mathsf{M}; \mathsf{M}_0; x.\, \mathsf{M}_1)]\!] \\ = {} & \mathit{ifz}([\![\mathsf{M}]\!], [\![\mathsf{M}_0]\!], [\![x : \texttt{nat} \vdash \mathsf{M}_1 : \tau]\!]) \\ = {} & \mathit{ifz}([\![\mathsf{N}]\!] + 1, [\![\mathsf{M}_0]\!], [\![x : \texttt{nat} \vdash \mathsf{M}_1 : \tau]\!]) \\ = {} & [\![x : \texttt{nat} \vdash \mathsf{M}_1]\!]([\![\mathsf{N}]\!]) \\ = {} & [\![\mathsf{M}_1[\mathsf{N}/x]]\!] = [\![\mathsf{V}]\!] \end{aligned}$$

  where the last but one equality follows from Substitution Lemma.

- For ($\Downarrow$-fix), we show that $[\![\mathtt{Y}x.\, \mathsf{M}]\!] = [\![\mathsf{V}]\!]$ if $[\![\mathsf{M}[\mathtt{Y}x.\, \mathsf{M}/x]]\!] = [\![\mathsf{V}]\!]$. Let $f :\equiv [\![x : \sigma \vdash \mathsf{M} : \sigma]\!]$. We calculate the denotation as follows

  $$\begin{aligned} [\![\mathtt{Y}x.\, \mathsf{M}]\!] &= \mu f = f(\mu f) \\ &= [\![x : \sigma \vdash \mathsf{M} : \sigma]\!]([\![\mathtt{Y}x.\, \mathsf{M}]\!]) \\ &= [\![\mathsf{M}[\mathtt{Y}x.\, \mathsf{M}/x]]\!] = [\![V]\!] \end{aligned}$$

  where the last but one equality follows from Substitution Lemma.

2 Equational reasoning

Logical Equivalence

Definition 3 (Applicative approximation)**.** For each type σ, we define a relation $\precsim_\sigma$ between well-typed closed terms $\vdash \mathsf{M} : \sigma$.

1. For $\texttt{nat}$, define
   $$\mathsf{M} \precsim_{\texttt{nat}} \mathsf{N}$$
   if for all $n \in \mathbb{N}$, $\mathsf{M} \Downarrow \underline{n}$ implies $\mathsf{N} \Downarrow \underline{n}$
2. For $\sigma \to \tau$, define
   $$\mathsf{M} \precsim_{\sigma \to \tau} \mathsf{N}$$
   if $\mathsf{M}\ P \precsim_\tau \mathsf{N}\ P$, for every well-typed closed term P.

Two well-typed closed terms M and N of the same type σ are **logically equivalent** denoted $\mathsf{M} \simeq_\sigma \mathsf{N}$ if $\mathsf{M} \precsim_\sigma \mathsf{N}$ and $\mathsf{M} \succsim_\sigma \mathsf{N}$.

The relation $\precsim_\sigma$ is a preorder, so $\simeq_\sigma$ is indeed an equivalence.[2]

[1] Why? See Lecture I

[2] Why? Prove it. Note that an equivalence relation is defined to be a reflexive, symmetric, and transitive relation.

Proposition 4. *The logical equivalence $\simeq_\sigma$ is an equivalence relation.*

A well-typed closed term M can be replaced by another well-typed closed term N without changing its result if $\mathsf{M} \simeq_\sigma \mathsf{N}$.

Example 5. The following two well-typed closed terms are logically equivalent:

$$\lambda x.\, x : \texttt{nat} \to \texttt{nat} \quad \text{and} \quad \lambda x.\, \texttt{pred}\,(\texttt{suc}\ x) : \texttt{nat} \to \texttt{nat}$$

Reduction respects logical equivalence

Recall that from $\mathsf{M} \rightsquigarrow^* \mathsf{M}'$ and $\mathsf{M}' \Downarrow \mathsf{V}$ it follows that $\mathsf{M} \Downarrow \mathsf{V}$ in the agreement between $\rightsquigarrow$ and $\Downarrow$.

Proposition 6. *Let M and M' be well-typed closed terms of type σ. If $\mathsf{M} \rightsquigarrow^* \mathsf{M}'$, then $\mathsf{M} \succsim_\sigma \mathsf{M}'$.*

The other direction follows from the determinacy and values cannot be reduced further:

Proposition 7. *For every $\mathsf{M} \Downarrow \mathsf{V}$ and $\mathsf{M} \rightsquigarrow^* \mathsf{M}'$, we have $\mathsf{M}' \Downarrow \mathsf{V}$.*

Therefore, if $\mathsf{M} \rightsquigarrow^* \mathsf{M}'$, then $\mathsf{M} \simeq_\sigma \mathsf{M}'$. However, logical equivalence goes beyond reduction. Consider the following two well-typed closed terms of type $\texttt{nat} \to \texttt{nat} \to \texttt{nat}$:

$$\lambda x.\, \lambda y.\, x + y$$

and

$$\lambda x.\, \lambda y.\, y + x$$

Surely the addition of natural numbers are commutative, but *why?*

By definition they are already values, so they cannot be reduced to each other.

Remark 2.1. We can show directly that these two well-typed closed terms are logically equivalent in dependent type theory. Yet, we will present an external approach using denotational semantics in the absense of the identity type.

3 Computational adequacy

In the following, we will show that for every $\vdash \mathsf{M} : \texttt{nat}$ if $[\![\mathsf{M}]\!] = n$ then M reduces to the numeral $\underline{n}$.

- Define a relation R_σ for each type σ between the domain $[\![\sigma]\!] = D_\sigma$ and the collection of well-typed closed terms of type σ:
  $$R_\sigma \subseteq D_\sigma \times \mathsf{Prg}_\sigma$$
  for every type σ where $\mathsf{Prg}_\sigma = \{\, \mathsf{M} \mid\ \vdash \mathsf{M} : \sigma \,\}$.

- Then show that $[\![\mathsf{M}]\!]\ R_\sigma\ \mathsf{M}$ for every well-typed closed term M of type σ, and by construction $[\![\mathsf{M}]\!]\ R_{\mathtt{nat}}\ \mathsf{M}$ is equivalent to that $[\![M]\!] = n$ implies $\mathsf{M} \Downarrow \underline{n}$.

With this property, we can conclude that denotational equivalence entails logical equivalence.[3]

Logical relation between semantics and syntax

Definition 8 (Logical relation)**.** For every type σ, define a relation $R_\sigma \subseteq D_\sigma \times \mathsf{Prg}_\sigma$ inductively as follows:

- $d\ R_{\mathtt{nat}}\ \mathsf{M}$ if M reduces to $\underline{n}$ whenever d is a natural number:

$$d\ R_{\mathtt{nat}}\ \mathsf{M} \quad \text{if} \quad \forall n \in \mathbb{N}.\, d = n \implies \mathsf{M} \Downarrow \underline{n}$$

- for every function type, $f\ R_{\sigma\to\tau}\ \mathsf{M}$ if the outcome is always related whenever the input is related:

$$f\ R_{\sigma\to\tau}\ \mathsf{M} \quad \text{if}$$
$$\forall d, \mathsf{N}.\, d\ R_\sigma\ \mathsf{N} \implies f(d)\ R_\tau\ \mathsf{M}\ \mathsf{N}$$

For example, $0\ R_{\mathtt{nat}}\ \mathtt{zero}$, and $n+1\ R_{\mathtt{nat}}\ \mathtt{suc}\ \mathsf{M}$ wherever $n\ R_{\mathtt{nat}}\ \mathsf{M}$ for $n \in \mathbb{N}$.

Properties of R_σ

Lemma 9. *For every type σ, the following statements are true:*

1. *If $d' \sqsubseteq d$ and $d\ R_\sigma\ \mathsf{M}$, then $d'\ R_\sigma\ \mathsf{M}$;*
2. *For every $\mathsf{M} \in \mathsf{Prg}_\sigma$, the set*
$$R_\sigma \mathsf{M} \coloneqq \{\, d \in D_\sigma \mid d\ R_\sigma\ \mathsf{M} \,\}$$
contains $\perp$ and is closed under directed sups;[4]
3. *If $d\ R_\sigma\ \mathsf{M}$ and $M \precsim_\sigma \mathsf{M}'$, then $d\ R_\sigma\ \mathsf{M}'$.*

Proof. By induction on σ. □

Lemma 10 (General recursion)**.** *If we have $f\ R_{\sigma\to\sigma}\ (\lambda x.\, \mathsf{M})$, then $\mu(f)\ R_\sigma\ (\mathtt{Y}x.\, \mathsf{M})$.*

Proof sketch. By definition $\mu(f)$ is the directed supremum of the following directed sequence

$$\perp \sqsubseteq f(\perp) \sqsubseteq f^2(\perp) \sqsubseteq \cdots \sqsubseteq f^i(\perp) \sqsubseteq \cdots,$$

so it suffices to show that

$$f^i(\perp)\ R_\sigma\ (\mathtt{Y}x.\, \mathsf{M})$$

for every $i \in \mathbb{N}$, because $R_\sigma(\mathtt{Y}x.\mathsf{M})$ is closed under directed sups. We prove it by induction on i and properties of R_σ. □

The complete proof is listed below.

For $i = 0$: By definition $f^0(\perp) = \perp$, so $\perp\ R_\sigma\ (\mathtt{Y}x.\, \mathsf{M})$ follows.

For $i = n+1$: By the assumption $f\ R_{\sigma\to\sigma}\ (\lambda x.\mathsf{M})$, it follows that

$$f^{n+1}(\perp)\ R_\sigma\ (\lambda x.\, \mathsf{M})\ (\mathtt{Y}x.\, \mathsf{M})$$

by the induction hypothesis $f^n(\perp)\ R_\sigma\ (\mathtt{Y}x.\, \mathsf{M})$. The RHS reduces to $\mathsf{M}[\mathtt{Y}x.\mathsf{M}/x]$ and $\mathtt{Y}x.\mathsf{M} \rightsquigarrow \mathsf{M}[\mathtt{Y}x.\mathsf{M}/x]$, so the RHS is logically equivalent to $\mathtt{Y}x.\mathsf{M}$. Hence, it follows that

$$f^{n+1}(\perp)\ R_\sigma\ (\mathtt{Y}x.\, \mathsf{M}).$$

Therefore, it follows that $\bigsqcup_{i\in\mathbb{N}} f^i(\perp)\ R_\sigma\ (\mathtt{Y}x.\, \mathsf{M})$.

Substitution Lemm and completeness

Lemma 11 (Substitution)**.** *Let $\Gamma = x_1 : \sigma_1, \ldots, x_n : \sigma_n$ be a context and $d_i\ R_{\sigma_i}\ \mathsf{N}_i$ for all $i = 1, \ldots, n$. For every well-typed term M we have*

$$[\![\, \Gamma \vdash \mathsf{M} : \tau \,]\!](\vec{d})\ R_\tau\ \mathsf{M}[\vec{N}/\vec{x}]$$

where $\vec{d}$ stands for $(d_1, \ldots, d_n)$ and $\vec{\mathsf{N}}$ stands for $(\mathsf{N}_1, \ldots, \mathsf{N}_n)$.

Theorem 12 (Completeness)**.** *For every $\vdash \mathsf{M} : \mathtt{nat}$, we have $\mathsf{M} \Downarrow \underline{n}$ if $[\![\mathsf{M}]\!] = n$.*

Proof. A special case of the previous lemma:

$$[\![\, \vdash \mathsf{M} : \tau \,]\!](*)\ R_\sigma\ \mathsf{M}$$

where the LHS is $[\![\mathsf{M}]\!]$. □

Proof of Substitution Lemma

To prove the lemma, do induction on the typing rules for **PCF**. For convenience, we write

$$\vec{d}\ R\ \vec{\mathsf{N}} \quad \text{for} \quad d_i\ R_{\sigma_i}\ \mathsf{N}_i \quad \text{indexed by } i = 1, \ldots, n$$

where $\vec{d}$ stands for $(d_1, \ldots, d_n)$ and $\vec{\mathsf{N}}$ stands for $(\mathsf{N}_1, \ldots, \mathsf{N}_n)$.

(z), (s) These two cases follow from $0\ R_{\mathtt{nat}}\ \mathtt{zero}$ and $n+1\ R_{\mathtt{nat}}\ \mathtt{suc}\ \mathsf{M}$ whenever $n\ R_{\mathtt{nat}}\ \mathsf{M}$.

(var) To show that

$$[\![\ldots, x_i : \sigma_i, \cdots \vdash x_i : \sigma_i]\!]\ R_{\sigma_i}\ x_i[\vec{\mathsf{N}}/\vec{x}]$$

we check both sides separately. By definition, we have

$$[\![\ldots, x_i : \sigma_i, \cdots \vdash x_i : \sigma_i]\!](\vec{d}) = d_i \quad \text{and} \quad [\vec{\mathsf{N}}/\vec{x}] = \mathsf{N}_i.$$

Therefore, from the assumption it follows that $d_i\ R_\sigma\ \mathsf{N}_i$ for every i.

[3] But, the converse may fail.

[4] Let S be an arbitrary directed subset of D_σ, if $d\ R_\sigma\ \mathsf{M}$ for every $d \in S$, then $\bigsqcup S\ R_\sigma\ \mathsf{M}$.

(abs) We need to show that

$$[\![\Gamma \vdash \lambda x.\,\mathsf{M} : \tau]\!](\vec{d})\ R_{\sigma\to\tau}\ (\lambda x.\,\mathsf{M})[\vec{\mathsf{N}}/\vec{x}] \quad (1)$$

under the induction hypothesis

$$[\![\Gamma, x : \sigma \vdash \mathsf{M} : \tau]\!](\vec{d}, d)\ R_\tau\ \mathsf{M}[\,\vec{\mathsf{N}}, \mathsf{N}\ /\ \vec{x}, x\,].$$

- For the LHS, we have by definition

$$\begin{aligned}&[\![\Gamma \vdash \lambda x.\mathsf{M} : \tau]\!](\vec{d})(d)\\ &= [\![\Gamma, x : \sigma \vdash \mathsf{M} : \tau]\!](\vec{d}, d).\end{aligned}$$

- For the RHS, we have

$$\begin{aligned}&(\lambda x.\,\mathsf{M})[\vec{\mathsf{N}}/\vec{x}]\ \mathsf{N}\\ &\rightsquigarrow (\lambda x.\,\mathsf{M})[\vec{\mathsf{N}}/\vec{x}][\mathsf{N}/x]\\ &= (\lambda x.\,\mathsf{M})[\,\vec{\mathsf{N}}, \mathsf{N}\ /\ \vec{x}, x\,]\end{aligned}$$

  and it follows that these two terms are logically equivalent. Thus, (1) follows by the definition of $R_{\sigma\to\tau}$.

(Y) We show that $[\![\Gamma \vdash \mathtt{Y}x.\,\mathsf{M} : \sigma]\!](\vec{d})\ R_\sigma\ (\mathtt{Y}x.\,\mathsf{M})[\vec{\mathsf{N}}/\vec{x}]$ under the assumption that

$$[\![\Gamma, x : \sigma \vdash \mathsf{M} : \sigma]\!](\vec{d}, d)\ R_\sigma\ \mathsf{M}[\,\vec{\mathsf{N}}, \mathsf{N}/\vec{x}, x\,] \quad (2)$$

Recall the lemma for general recursion. It suffices to show $\Lambda[\![\Gamma, x : \sigma \vdash \mathsf{M} : \sigma]\!](\vec{d})\ R_{\sigma\to\sigma}\ \lambda x.\,\mathsf{M}[\vec{\mathsf{N}}/\vec{x}]$ or, equivalently

$$[\![\Gamma, x : \sigma \vdash \mathsf{M} : \sigma]\!](\vec{d}, d)\ R_\sigma\ (\lambda x.\,\mathsf{M}[\vec{\mathsf{N}}/\vec{x}])\ \mathsf{N} \quad (3)$$

for every $d\ R_\sigma\ \mathsf{N}$. The RHS can be reduced to

$$\mathsf{M}[\vec{\mathsf{N}}/\vec{x}][\mathsf{N}/x] = \mathsf{M}[\,\vec{\mathsf{N}}, \mathsf{N}\ /\ \vec{x}, x\,],$$

so (2) implies (3) by logical equivalence.

(app), (ifz) Exercises.

3.1 Applications of adequacy

Applicative approximation coincides with logical relation

Lemma 13. *For every* $\vdash \mathsf{M} : \sigma$ *and* $\vdash \mathsf{N} : \sigma$,

$$\mathsf{M} \precsim_\sigma \mathsf{N} \quad \textit{if and only if} \quad [\![\mathsf{M}]\!]\ R_\sigma\ \mathsf{N}.$$

Proof. $\mathsf{M} \precsim_\sigma \mathsf{N}$**.** By adequacy, we have $[\![\mathsf{M}]\!]\ R_\sigma\ \mathsf{M}$, so $[\![\mathsf{M}]\!]\ R_\sigma\ \mathsf{N}$.

$[\![M]\!]\ R_\sigma\ \mathsf{N}$**.** Prove it by induction on σ.

$\mathtt{nat}$**:** If $[\![\mathsf{M}]\!]\ R_{\mathtt{nat}}\ \mathsf{N}$, then $\mathsf{N} \Downarrow \underline{n}$ whenever $[\![\mathsf{M}]\!] = n$.

$\sigma \to \tau$**:** For $\sigma \to \tau$, by adequacy, we have $[\![P]\!]\ R_\sigma\ P$ for every P, so by assumption and $[\![\mathsf{M}\ P]\!] = [\![\mathsf{M}]\!]([\![P]\!])\ R_\tau\ \mathsf{N}\ P$. By induction hypothesis, $\mathsf{M}\ P \precsim_\tau \mathsf{N}\ P$ for every P, so $\mathsf{M} \precsim_{\sigma\to\tau} \mathsf{N}$ by definition.

□

Corollary 14. *Given two* $\vdash \mathsf{M} : \sigma$ *and* $\vdash \mathsf{N} : \sigma$, *if* $[\![\mathsf{M}]\!] = [\![\mathsf{N}]\!]$, *then* M *and* N *are logically equivalent.*

Proof.
1. By adequacy $[\![\mathsf{M}]\!]\ R\ \mathsf{M}$ and by assumption $[\![\mathsf{N}]\!] = [\![\mathsf{M}]\!]\ R\ \mathsf{M}$, it follows that $\mathsf{N} \precsim \mathsf{M}$.
2. Similarly, $[\![\mathsf{M}]\!]\ R\ \mathsf{N}$, so $\mathsf{M} \precsim \mathsf{N}$.

Hence, M and N are logically equivalent. □

From this property, techniques and results in denotational semantics can be used to argue logical equivalence and reductions.

Compactness

Recall that the semantics of general recursion is the least upper bound of its finite unfoldings

$$[\![\,\mathtt{Y}x.\,\mathsf{M}\,]\!] = \bigsqcup_{i\in\mathbb{N}} [\![\,\mathtt{Y}^i x.\,\mathsf{M}\,]\!]$$

where $\mathtt{Y}^i x.\,\mathsf{M}$ is defined inductively by

1. $\mathtt{Y}^0 x.\,\mathsf{M} \coloneqq \mathtt{Y}x.\,x$ and
2. $\mathtt{Y}^{n+1} x.\,\mathsf{M} \coloneqq \mathsf{M}[\mathtt{Y}^n x.\,\mathsf{M}/x]$

and $[\![\mathtt{Y}^i x.\,\mathsf{M}]\!] = [\![\lambda x.\,\mathsf{M}]\!]^i(\bot)$.

Theorem 15. *Suppose that* $x \neq y$,

$$y : \sigma \vdash E : \mathtt{nat} \quad \textit{and} \quad \vdash \mathtt{Y}x.\,\mathsf{M} : \sigma.$$

If $E[\mathtt{Y}x.\,\mathsf{M}/y] \Downarrow \underline{n}$ *then* $E[\mathtt{Y}^m x.\,\mathsf{M}/y] \Downarrow \underline{n}$ *for some* m.

Proof. By the Substitution Lemma, we have

$$[\![E[\mathtt{Y}x.\,\mathsf{M}/y]]\!] = [\![y : \sigma \vdash E : \mathtt{nat}]\!]([\![\mathtt{Y}x.\,\mathsf{M}]\!]).$$

Let $g \coloneqq [\![y : \sigma \vdash E : \mathtt{nat}]\!]$ and $f \coloneqq [\![x : \sigma \vdash \mathsf{M} : \sigma]\!]$.

$$\begin{aligned}[\![y : \sigma \vdash E : \mathtt{nat}]\!]([\![\mathtt{Y}x.\,\mathsf{M}]\!]) &= g(\mu f)\\ &= g(\bigsqcup_{i\in\mathbb{N}} f^i(\bot))\\ &= \bigsqcup_{i\in\mathbb{N}} (g \circ f^i)(\bot) = n\end{aligned}$$

Therefore there exists some $m \in \mathbb{N}$ such that $(g \circ f^m)(\bot) = n$. By adequacy, it follows that $E[\mathtt{Y}^m x.\,\mathsf{M}/y] \Downarrow \underline{n}$. □

Finite unfoldings approximate general recursion

Lemma 16. *Suppose that* $x : \sigma \vdash \mathsf{M} : \sigma$*. Then for every* $i \in \mathbb{N}$*, we have*

$$\mathtt{Y}^i x.\, \mathsf{M} \precsim_\sigma \mathtt{Y} x.\, \mathsf{M}.$$

The proof is left as an exercise.

Theorem 17 (Fixed Point Induction)**.** *Suppose that* $x : \sigma \vdash \mathsf{M} : \sigma$*,* $x : \sigma \vdash \mathsf{N} : \sigma$ *and*

$$\mathtt{Y}^i x.\, \mathsf{M} \simeq_\sigma \mathtt{Y}^i x.\, \mathsf{N}$$

for every $i \in \mathbb{N}$*. Then, we also have*

$$\mathtt{Y} x.\, \mathsf{M} \simeq_\sigma \mathtt{Y} x.\, \mathsf{N}$$

Proof. We show that $\mathtt{Y} x.\, \mathsf{M} \precsim_\sigma \mathtt{Y} x.\, \mathsf{N}$, or equivalently $[\![\mathtt{Y} x.\, \mathsf{M}]\!]\ R_\sigma\ \mathtt{Y} x.\, \mathsf{N}$, and the other direction follows similarly.

Let $f \coloneqq [\![x : \sigma \vdash \mathsf{M} : \sigma]\!]$ and $g \coloneqq [\![x : \sigma \vdash \mathsf{N} : \sigma]\!]$. Since the set

$$R_\sigma(\mathtt{Y} x.\, \mathsf{N}) = \{\, d \in D_\sigma \mid d\ R_\sigma\ \mathtt{Y} x.\, \mathsf{N} \,\}$$

is closed under directed supremum, it suffices to show that

$$[\![\mathtt{Y}^i x.\, \mathsf{M}]\!]\ R_\sigma\ \mathtt{Y} x.\, \mathsf{N}$$

for every i.

By assumption, we have $[\![\mathtt{Y}^i x.\, \mathsf{M}]\!]\ R_\sigma\ \mathtt{Y}^i x.\, \mathsf{N}$, so it suffices to show that $\mathtt{Y}^i x.\, \mathsf{N} \precsim_\sigma \mathtt{Y} x.\, \mathsf{N}$. By the previous lemma the statement follows. ☐