Reasoning on programs using Step-indexed Realizability

Guilhem Jaber

PPS, IRIF, Universite Paris Diderot

Realizability in Uruguay 2016
July 19th 2016

How to reason formally on programs ?

- Program logics (Hoare, Separation, . . .)
- Type systems (Dependent, Refinement, . . .)
- Denotational models (Domains, Games, . . .)
- Syntactic models (Realizability, Logical Relations, . . .)

Outline of the Talk

What we will do:

- Semantics proof of soundness for a simple call-by-value language with fixed points;
- Realizability model for a language with refinment types.

To show that:

- Semantic proofs of type soundness give a lot more information than syntactic one (Wright and Felleisen's "progress and preservations");
- Step-indexing is a great technique to make these proofs feasible;
- We can abstract over step-indexes using Godel-Lob Logic;
- Gidel-Lob logic can be embedded into Dependent Type theory.

Contents

A CBV λ-calculus with fixed points

$$
\begin{array}{lcl}
v & \stackrel{def}{=} & x \mid \texttt{fix}\ f(x).M \mid n \mid \textbf{true} \mid \textbf{false} \qquad (n \in \mathbb{N}, x \in \mathrm{Var}) \\
M, N & \stackrel{def}{=} & v \mid MN \mid \texttt{if}\ M\ \texttt{then}\ N_1\ \texttt{else}\ N_2 \mid \ldots \\
K & \stackrel{def}{=} & \bullet \mid vK \mid KM \mid \texttt{if}\ K\ \texttt{then}\ M\ \texttt{else}\ M' \mid \ldots \\
\tau, \sigma & \stackrel{def}{=} & \mathrm{Nat} \mid \mathrm{Bool} \mid \tau \to \sigma
\end{array}
$$

$$
\begin{array}{lcl}
(\texttt{fix}\ f(x).M)\ v & \mapsto & M\{v/x\}\{\texttt{fix}\ f(x).M/f\} \\
\texttt{if}\ \textbf{true}\ \texttt{then}\ N_1\ \texttt{else}\ N_2 & \mapsto & N_1 \\
\texttt{if}\ \textbf{false}\ \texttt{then}\ N_1\ \texttt{else}\ N_2 & \mapsto & N_2
\end{array}
$$

$$
\frac{M \mapsto M'}{K[M] \mapsto K[M']}
$$

$$
\frac{\Gamma, x : \tau, f : \tau \to \sigma \vdash M : \sigma}{\Gamma \vdash \texttt{fix}\ f(x).M : \tau \to \sigma}
$$

Realizability model

Types interpreted as set of terms.

$$\begin{aligned}
\mathcal{V}[\![\mathrm{Nat}]\!] &\overset{def}{=} \mathbb{N} \\
\mathcal{V}[\![\mathrm{Bool}]\!] &\overset{def}{=} \{\mathbf{true}, \mathbf{false}\} \\
\mathcal{V}[\![\tau \to \sigma]\!] &\overset{def}{=} \{\mathtt{fix}\ f(x).M \mid \forall v \in \mathcal{V}[\![\tau]\!].(\mathtt{fix}\ f(x).M)v \in \mathcal{E}[\![\sigma]\!]\} \\
\mathcal{E}[\![\tau]\!] &\overset{def}{=} \{M \mid \forall v.(M \mapsto^* v) \Rightarrow v \in \mathcal{V}[\![\tau]\!]\} \\
\mathcal{G}[\![\Gamma]\!] &\overset{def}{=} \{\gamma \mid \forall (x, \tau) \in \Gamma, \gamma(x) \in \mathcal{V}[\![\tau]\!]\}
\end{aligned}$$

$M \in \mathcal{E}[\![\tau]\!]$ means that M realizes τ.

Theorem (Soundness)

If $\Gamma \vdash M : \tau$ then for all $\gamma \in \mathcal{G}[\![\Gamma]\!]$, $M\{\gamma\} \in \mathcal{E}[\![\tau]\!]$.

Proof of Soundness

By induction on the derivation tree of $\Gamma \vdash M : \tau$. Interesting case: typing rule for fixed points.

$$\frac{\Gamma, x : \tau, f : \tau \to \sigma \vdash M : \sigma}{\Gamma \vdash \texttt{fix}\ f(x).M : \tau \to \sigma}$$

Proof of Soundness

By induction on the derivation tree of $\Gamma \vdash M : \tau$. Interesting case: typing rule for fixed points.

$$\frac{\Gamma, x : \tau, f : \tau \to \sigma \vdash M : \sigma}{\Gamma \vdash \texttt{fix}\ f(x).M : \tau \to \sigma}$$

- Let $\gamma \in \mathcal{G}[\![\Gamma]\!]$, we must prove that $(\texttt{fix}\ f(x).M)\{\gamma\} \in \mathcal{E}[\![\tau \to \sigma]\!]$ (?)

Proof of Soundness

By induction on the derivation tree of $\Gamma \vdash M : \tau$. Interesting case: typing rule for fixed points.

$$\frac{\Gamma, x : \tau, f : \tau \to \sigma \vdash M : \sigma}{\Gamma \vdash \texttt{fix}\ f(x).M : \tau \to \sigma}$$

- Let $\gamma \in \mathcal{G}[\![\Gamma]\!]$, we must prove that $(\texttt{fix}\ f(x).M)\{\gamma\} \in \mathcal{E}[\![\tau \to \sigma]\!]$ (?)
- i.e. $\texttt{fix}\ f(x).M\{\gamma\} \in \mathcal{V}[\![\tau \to \sigma]\!]$ (?)

Proof of Soundness

By induction on the derivation tree of $\Gamma \vdash M : \tau$. Interesting case: typing rule for fixed points.

$$\frac{\Gamma, x : \tau, f : \tau \to \sigma \vdash M : \sigma}{\Gamma \vdash \texttt{fix}\ f(x).M : \tau \to \sigma}$$

- Let $\gamma \in \mathcal{G}[\![\Gamma]\!]$, we must prove that $(\texttt{fix}\ f(x).M)\{\gamma\} \in \mathcal{E}[\![\tau \to \sigma]\!]$ (?)
- i.e. $\texttt{fix}\ f(x).M\{\gamma\} \in \mathcal{V}[\![\tau \to \sigma]\!]$ (?)
- i.e. for all $v \in \mathcal{V}[\![\tau]\!], (\texttt{fix}\ f(x).M\{\gamma\})v \in \mathcal{E}[\![\sigma]\!]$ (?)

Proof of Soundness

By induction on the derivation tree of $\Gamma \vdash M : \tau$. Interesting case: typing rule for fixed points.

$$\frac{\Gamma, x : \tau, f : \tau \to \sigma \vdash M : \sigma}{\Gamma \vdash \texttt{fix}\ f(x).M : \tau \to \sigma}$$

- Let $\gamma \in \mathcal{G}[\![\Gamma]\!]$, we must prove that $(\texttt{fix}\ f(x).M)\{\gamma\} \in \mathcal{E}[\![\tau \to \sigma]\!]$ (?)
- i.e. $\texttt{fix}\ f(x).M\{\gamma\} \in \mathcal{V}[\![\tau \to \sigma]\!]$ (?)
- i.e. for all $v \in \mathcal{V}[\![\tau]\!], (\texttt{fix}\ f(x).M\{\gamma\})v \in \mathcal{E}[\![\sigma]\!]$ (?)
- i.e. $M\{\gamma\}\{v/x\}\{(\texttt{fix}\ f(x).M\{\gamma\})/f\} \in \mathcal{E}[\![\sigma]\!]$ (?)

Proof of Soundness

By induction on the derivation tree of $\Gamma \vdash M : \tau$. Interesting case: typing rule for fixed points.

$$\frac{\Gamma, x : \tau, f : \tau \to \sigma \vdash M : \sigma}{\Gamma \vdash \texttt{fix}\ f(x).M : \tau \to \sigma}$$

- Let $\gamma \in \mathcal{G}[\![\Gamma]\!]$, we must prove that $(\texttt{fix}\ f(x).M)\{\gamma\} \in \mathcal{E}[\![\tau \to \sigma]\!]$ (?)
- i.e. $\texttt{fix}\ f(x).M\{\gamma\} \in \mathcal{V}[\![\tau \to \sigma]\!]$ (?)
- i.e. for all $v \in \mathcal{V}[\![\tau]\!], (\texttt{fix}\ f(x).M\{\gamma\})v \in \mathcal{E}[\![\sigma]\!]$ (?)
- i.e. $M\{\gamma\}\{v/x\}\{(\texttt{fix}\ f(x).M\{\gamma\})/f\} \in \mathcal{E}[\![\sigma]\!]$ (?)
- IH: for all $\gamma' \in \mathcal{G}[\![\Gamma, x : \tau, f : \tau \to \sigma]\!], M\{\gamma'\} \in \mathcal{E}[\![\tau \to \sigma]\!]$

Proof of Soundness

By induction on the derivation tree of $\Gamma \vdash M : \tau$. Interesting case: typing rule for fixed points.

$$\frac{\Gamma, x : \tau, f : \tau \to \sigma \vdash M : \sigma}{\Gamma \vdash \texttt{fix}\ f(x).M : \tau \to \sigma}$$

- Let $\gamma \in \mathcal{G}[\![\Gamma]\!]$, we must prove that $(\texttt{fix}\ f(x).M)\{\gamma\} \in \mathcal{E}[\![\tau \to \sigma]\!]$ (?)
- i.e. $\texttt{fix}\ f(x).M\{\gamma\} \in \mathcal{V}[\![\tau \to \sigma]\!]$ (?)
- i.e. for all $v \in \mathcal{V}[\![\tau]\!], (\texttt{fix}\ f(x).M\{\gamma\})v \in \mathcal{E}[\![\sigma]\!]$ (?)
- i.e. $M\{\gamma\}\{v/x\}\{(\texttt{fix}\ f(x).M\{\gamma\})/f\} \in \mathcal{E}[\![\sigma]\!]$ (?)
- IH: for all $\gamma' \in \mathcal{G}[\![\Gamma, x : \tau, f : \tau \to \sigma]\!], M\{\gamma'\} \in \mathcal{E}[\![\tau \to \sigma]\!]$
- Does $\gamma \cdot [x \mapsto v] \cdot [f \mapsto \texttt{fix}\ f(x).M\{\gamma\}] \in \mathcal{G}[\![\Gamma, x : \tau, f : \tau \to \sigma]\!]$?

Proof of Soundness

By induction on the derivation tree of $\Gamma \vdash M : \tau$. Interesting case: typing rule for fixed points.

$$\frac{\Gamma, x : \tau, f : \tau \to \sigma \vdash M : \sigma}{\Gamma \vdash \texttt{fix}\ f(x).M : \tau \to \sigma}$$

- Let $\gamma \in \mathcal{G}[\![\Gamma]\!]$, we must prove that $(\texttt{fix}\ f(x).M)\{\gamma\} \in \mathcal{E}[\![\tau \to \sigma]\!]$ (?)
- i.e. $\texttt{fix}\ f(x).M\{\gamma\} \in \mathcal{V}[\![\tau \to \sigma]\!]$ (?)
- i.e. for all $v \in \mathcal{V}[\![\tau]\!], (\texttt{fix}\ f(x).M\{\gamma\})v \in \mathcal{E}[\![\sigma]\!]$ (?)
- i.e. $M\{\gamma\}\{v/x\}\{(\texttt{fix}\ f(x).M\{\gamma\})/f\} \in \mathcal{E}[\![\sigma]\!]$ (?)
- IH: for all $\gamma' \in \mathcal{G}[\![\Gamma, x : \tau, f : \tau \to \sigma]\!], M\{\gamma'\} \in \mathcal{E}[\![\tau \to \sigma]\!]$
- Does $\gamma \cdot [x \mapsto v] \cdot [f \mapsto \texttt{fix}\ f(x).M\{\gamma\}] \in \mathcal{G}[\![\Gamma, x : \tau, f : \tau \to \sigma]\!]$?
- Only if $\texttt{fix}\ f(x).M\{\gamma\} \in \mathcal{V}[\![\tau \to \sigma]\!]$ ... That's problematic !

Step-Indexing to the rescue !

Idea: Stratify the model using natural numbers as indices ! (Appel & McAllester, Ahmed, ...)

$$
\begin{array}{lcl}
\mathcal{V}_k\,[\![\mathrm{Nat}]\!] & \stackrel{def}{=} & \mathbb{N} \\
\mathcal{V}_k\,[\![\mathrm{Bool}]\!] & \stackrel{def}{=} & \{\textbf{true}, \textbf{false}\} \\
\mathcal{V}_k\,[\![\tau \to \sigma]\!] & \stackrel{def}{=} & \{\mathtt{fix}\ f(x).M \mid \forall j \leq k. \forall v. \\
 & & \quad v \in \mathcal{V}_j\,[\![\tau]\!] \Rightarrow (\mathtt{fix}\ f(x).M)v) \in \mathcal{E}_j\,[\![\sigma]\!]\} \\
\mathcal{E}_k\,[\![\tau]\!] & \stackrel{def}{=} & \{M \mid \forall j < k. \forall v. (M \mapsto^j v) \Rightarrow v \in \mathcal{V}_{k-j}\,[\![\tau]\!]\} \\
\mathcal{G}_k\,[\![\Gamma]\!] & \stackrel{def}{=} & \{\rho \mid \forall (x, \tau) \in \Gamma, \rho(x) \in \mathcal{V}_k\,[\![\tau]\!]\}
\end{array}
$$

If M reduces in more than k steps to a value (or diverges), then $M \in \mathcal{E}[\![\tau]\!]k$!!

Theorem (Monotonicity)

If $M \in \mathcal{E}_k\,[\![\tau]\!]$ then for all $j \leq k$, $M \in \mathcal{E}_j\,[\![\tau]\!]$.

Soundness of the Step-indexed model

Theorem (Soundness)

If $\Gamma \vdash M : \tau$ *then for all* $\gamma \in \mathcal{G}_k \llbracket \Gamma \rrbracket$, $M\{\gamma\} \in \mathcal{E}_k \llbracket \tau \rrbracket$.

By induction on the derivation tree of $\Gamma \vdash M : \tau$ and *on the step-index* k.

Compatibility lemma for the fixed point

- Let $\gamma \in \mathcal{G}_k [\![\Gamma]\!]$, we must prove that $(\texttt{fix}\ f(x).M)\{\gamma\} \in \mathcal{E}_k [\![\tau \to \sigma]\!]$ (?)

Compatibility lemma for the fixed point

- Let $\gamma \in \mathcal{G}_k \llbracket \Gamma \rrbracket$, we must prove that $(\texttt{fix}\ f(x).M)\{\gamma\} \in \mathcal{E}_k \llbracket \tau \to \sigma \rrbracket$ (?)
- i.e. does $\texttt{fix}\ f(x).(M\{\gamma\}) \in \mathcal{V}_k \llbracket \tau \to \sigma \rrbracket$ (?)

Compatibility lemma for the fixed point

- Let $\gamma \in \mathcal{G}_k [\![\Gamma]\!]$, we must prove that $(\texttt{fix}\ f(x).M)\{\gamma\} \in \mathcal{E}_k [\![\tau \to \sigma]\!]$ (?)
- i.e. does $\texttt{fix}\ f(x).(M\{\gamma\}) \in \mathcal{V}_k [\![\tau \to \sigma]\!]$ (?)
- i.e. for all $j \leq k$ and $v \in \mathcal{V}_j [\![\tau]\!]$, does $(\texttt{fix}\ f(x).M\{\gamma\})v \in \mathcal{E}_j [\![\sigma]\!]$ (?)

Compatibility lemma for the fixed point

- Let $\gamma \in \mathcal{G}_k \llbracket \Gamma \rrbracket$, we must prove that $(\texttt{fix}\ f(x).M)\{\gamma\} \in \mathcal{E}_k \llbracket \tau \to \sigma \rrbracket$ (?)
- i.e. does $\texttt{fix}\ f(x).(M\{\gamma\}) \in \mathcal{V}_k \llbracket \tau \to \sigma \rrbracket$ (?)
- i.e. for all $j \leq k$ and $v \in \mathcal{V}_j \llbracket \tau \rrbracket$, does $(\texttt{fix}\ f(x).M\{\gamma\})v \in \mathcal{E}_j \llbracket \sigma \rrbracket$ (?)
- i.e.does $M\{\gamma\}\{v/x\}\{(\texttt{fix}\ f(x).M\{\gamma\})/f\} \in \mathcal{E}_{j-1} \llbracket \sigma \rrbracket$ (?)

Compatibility lemma for the fixed point

- Let $\gamma \in \mathcal{G}_k \llbracket \Gamma \rrbracket$, we must prove that $(\texttt{fix } f(x).M)\{\gamma\} \in \mathcal{E}_k \llbracket \tau \to \sigma \rrbracket$ (?)
- i.e. does $\texttt{fix } f(x).(M\{\gamma\}) \in \mathcal{V}_k \llbracket \tau \to \sigma \rrbracket$ (?)
- i.e. for all $j \leq k$ and $v \in \mathcal{V}_j \llbracket \tau \rrbracket$, does $(\texttt{fix } f(x).M\{\gamma\})v \in \mathcal{E}_j \llbracket \sigma \rrbracket$ (?)
- i.e.does $M\{\gamma\}\{v/x\}\{(\texttt{fix } f(x).M\{\gamma\})/f\} \in \mathcal{E}_{j-1} \llbracket \sigma \rrbracket$ (?)
- IH_1: for all $\gamma' \in \mathcal{G}_i \llbracket \Gamma, x : \tau, f : \tau \to \sigma \rrbracket$, $M\{\gamma'\} \in \mathcal{E}_i \llbracket \sigma \rrbracket$
  IH_2: for all $i < k, \texttt{fix } f(x).M)\{\gamma\} \in \mathcal{E}_i \llbracket \tau \to \sigma \rrbracket$

Compatibility lemma for the fixed point

- Let $\gamma \in \mathcal{G}_k \llbracket \Gamma \rrbracket$, we must prove that $(\texttt{fix}\ f(x).M)\{\gamma\} \in \mathcal{E}_k \llbracket \tau \to \sigma \rrbracket$ (?)
- i.e. does $\texttt{fix}\ f(x).(M\{\gamma\}) \in \mathcal{V}_k \llbracket \tau \to \sigma \rrbracket$ (?)
- i.e. for all $j \leq k$ and $v \in \mathcal{V}_j \llbracket \tau \rrbracket$, does $(\texttt{fix}\ f(x).M\{\gamma\})v \in \mathcal{E}_j \llbracket \sigma \rrbracket$ (?)
- i.e.does $M\{\gamma\}\{v/x\}\{(\texttt{fix}\ f(x).M\{\gamma\})/f\} \in \mathcal{E}_{j-1} \llbracket \sigma \rrbracket$ (?)
- IH_1: for all $\gamma' \in \mathcal{G}_i \llbracket \Gamma, x : \tau, f : \tau \to \sigma \rrbracket$, $M\{\gamma'\} \in \mathcal{E}_i \llbracket \sigma \rrbracket$
  IH_2: for all $i < k, \texttt{fix}\ f(x).M)\{\gamma\} \in \mathcal{E}_i \llbracket \tau \to \sigma \rrbracket$
- Does $(\gamma \cdot [x \mapsto v] \cdot [f \mapsto \texttt{fix}\ f(x).M\{\gamma\}]) \in \mathcal{G}_{j-1} \llbracket \Gamma, x : \tau, f : \tau \to \sigma \rrbracket$?

Compatibility lemma for the fixed point

- Let $\gamma \in \mathcal{G}_k [\![\Gamma]\!]$, we must prove that $(\texttt{fix}\ f(x).M)\{\gamma\} \in \mathcal{E}_k [\![\tau \to \sigma]\!]$ (?)
- i.e. does $\texttt{fix}\ f(x).(M\{\gamma\}) \in \mathcal{V}_k [\![\tau \to \sigma]\!]$ (?)
- i.e. for all $j \leq k$ and $v \in \mathcal{V}_j [\![\tau]\!]$, does $(\texttt{fix}\ f(x).M\{\gamma\})v \in \mathcal{E}_j [\![\sigma]\!]$ (?)
- i.e.does $M\{\gamma\}\{v/x\}\{(\texttt{fix}\ f(x).M\{\gamma\})/f\} \in \mathcal{E}_{j-1} [\![\sigma]\!]$ (?)
- IH_1: for all $\gamma' \in \mathcal{G}_i [\![\Gamma, x:\tau, f:\tau \to \sigma]\!]$, $M\{\gamma'\} \in \mathcal{E}_i [\![\sigma]\!]$
  IH_2: for all $i < k, \texttt{fix}\ f(x).M)\{\gamma\} \in \mathcal{E}_i [\![\tau \to \sigma]\!]$
- Does $(\gamma \cdot [x \mapsto v] \cdot [f \mapsto \texttt{fix}\ f(x).M\{\gamma\}]) \in \mathcal{G}_{j-1} [\![\Gamma, x:\tau, f:\tau \to \sigma]\!]$?
- Only if $\texttt{fix}\ f(x).M\{\gamma\} \in \mathcal{V}_{j-1} [\![\tau \to \sigma]\!]$ ... IH_2 to the rescue !

Contents

Refinement types

Arithmetic formulas as types.

$$
\begin{aligned}
\mathcal{V}_k [\![\mathrm{Nat}\{P\}]\!] &\stackrel{\textit{def}}{=} \{m \in \mathbb{N} \mid m \in P\} \\
\mathcal{V}_k [\![\mathrm{Bool}]\!] &\stackrel{\textit{def}}{=} \{\mathbf{true}, \mathbf{false}\} \\
\mathcal{V}_k [\![\tau \wedge \sigma]\!] &\stackrel{\textit{def}}{=} \mathcal{V}_k [\![\tau]\!] \cap \mathcal{V}_k [\![\sigma]\!] \\
\mathcal{V}_k [\![\forall a.\tau]\!] &\stackrel{\textit{def}}{=} \bigcap_{n \in \mathbb{N}} \mathcal{V}_k [\![\tau\{n/a\}]\!] \\
\mathcal{V}_k [\![\tau \to \sigma]\!] &\stackrel{\textit{def}}{=} \{(\lambda x.M, k) \mid \forall j \leq k.\forall v \in \mathcal{V}_j [\![\tau]\!] . \\
&\qquad\qquad (\lambda x.M)v \in \mathcal{E}[\![\sigma]\!]j\} \\
\mathcal{E}_k [\![\tau]\!] &\stackrel{\textit{def}}{=} \{M \mid \forall j < k.\forall v.(M \mapsto^j v) \Rightarrow v \in \mathcal{V}_{k-j} [\![\tau]\!]\}
\end{aligned}
$$

McCarthy's 91 function

$$\texttt{fix MC(x).if x} \leq \texttt{100 then MC(MC(x} + \texttt{11)) else x} - \texttt{10}$$

McCarthy's 91 function

$$\texttt{fix MC(x).if x} \leq \texttt{100 then MC(MC(x} + \texttt{11)) else x} - \texttt{10}$$

is in

$$\mathcal{V}_k \left[\!\left[\forall n. \left(\mathrm{Nat}\{n \leq 100\} \to \mathrm{Nat}\{91\} \right) \wedge \left(\mathrm{Nat}\{n > 100\} \to \mathrm{Nat}\{n - 10\} \right) \right]\!\right]$$

for all $k \in \mathbb{N}$

McCarthy's 91 function

$$\texttt{fix MC(x).if x} \leq \texttt{100 then MC(MC(x + 11)) else x} - \texttt{10}$$

is in

$$\mathcal{V}_k \left[\!\!\left[\forall n. \Big(\mathrm{Nat}\{n \leq 100\} \rightarrow \mathrm{Nat}\{91\} \Big) \wedge \Big(\mathrm{Nat}\{n > 100\} \rightarrow \mathrm{Nat}\{n - 10\} \Big) \right]\!\!\right]$$

for all $k \in \mathbb{N}$

By induction over the step-indexed k:

- If $k = 0$, straightforward...
- if $k > 0$, let $n \in \mathbb{N}$,
  - If $n > 100$, then we must prove that $n - 10 \in \mathcal{E}_k [\![\mathrm{Nat}\{n - 10\}]\!]$: straightforward.

McCarthy's 91 function

$$\texttt{fix MC(x).if x <= 100 then MC(MC(x + 11)) else x - 10}$$

is in

$$\mathcal{V}_k \left[\!\left[\forall n. \left(\mathrm{Nat}\{n \leq 100\} \rightarrow \mathrm{Nat}\{91\} \right) \wedge \left(\mathrm{Nat}\{n > 100\} \rightarrow \mathrm{Nat}\{n - 10\} \right) \right]\!\right]$$

for all $k \in \mathbb{N}$

If $n \leq 100$, then we must prove that $MC(MC(n+11)) \in \mathcal{E}_{k-1} [\![\mathrm{Nat}\{91\}]\!]$:

McCarthy's 91 function

$$\texttt{fix MC(x).if x} <= \texttt{100 then MC(MC(x} + \texttt{11)) else x} - \texttt{10}$$

is in

$$\mathcal{V}_k \left[\!\!\left[\forall n. \left(\mathrm{Nat}\{n \leq 100\} \to \mathrm{Nat}\{91\}\right) \wedge \left(\mathrm{Nat}\{n > 100\} \to \mathrm{Nat}\{n - 10\}\right)\right]\!\!\right]$$

for all $k \in \mathbb{N}$

If $n \leq 100$, then we must prove that $MC(MC(n+11)) \in \mathcal{E}_{k-1} [\![\mathrm{Nat}\{91\}]\!]$:

- if $n \leq 89$, we know (IH) that $MC(n+11) \in \mathcal{E}_{k-1} [\![\mathrm{Nat}\{91\}]\!]$ and $MC(91) \in \mathcal{E}_{k-1} [\![\mathrm{Nat}\{91\}]\!]$

McCarthy's 91 function

$$\texttt{fix MC(x).if x <= 100 then MC(MC(x + 11)) else x - 10}$$

is in

$$\mathcal{V}_k \left[\!\!\left[\forall n. \left(\mathrm{Nat}\{n \leq 100\} \to \mathrm{Nat}\{91\}\right) \wedge \left(\mathrm{Nat}\{n > 100\} \to \mathrm{Nat}\{n - 10\}\right)\right]\!\!\right]$$

for all $k \in \mathbb{N}$

If $n \leq 100$, then we must prove that $MC(MC(n+11)) \in \mathcal{E}_{k-1}[\![\mathrm{Nat}\{91\}]\!]$:

- if $n \leq 89$, we know (IH) that $MC(n+11) \in \mathcal{E}_{k-1}[\![\mathrm{Nat}\{91\}]\!]$ and $MC(91) \in \mathcal{E}_{k-1}[\![\mathrm{Nat}\{91\}]\!]$
- if $89 < n < 100$, we know (IH) that $MC(n+11) \in \mathcal{E}_{k-1}[\![\mathrm{Nat}\{n+1\}]\!]$ and $MC(n+1) \in \mathcal{E}_{k-1}[\![\mathrm{Nat}\{91\}]\!]$

McCarthy's 91 function

$$\texttt{fix MC(x).if x <= 100 then MC(MC(x + 11)) else x − 10}$$

is in

$$\mathcal{V}_k \left[\!\!\left[\forall n. \left(\mathrm{Nat}\{n \le 100\} \to \mathrm{Nat}\{91\} \right) \wedge \left(\mathrm{Nat}\{n > 100\} \to \mathrm{Nat}\{n - 10\} \right) \right]\!\!\right]$$

for all $k \in \mathbb{N}$

If $n \le 100$, then we must prove that $MC(MC(n+11)) \in \mathcal{E}_{k-1} [\![\mathrm{Nat}\{91\}]\!]$:

- if $n \le 89$, we know (IH) that $MC(n+11) \in \mathcal{E}_{k-1} [\![\mathrm{Nat}\{91\}]\!]$ and $MC(91) \in \mathcal{E}_{k-1} [\![\mathrm{Nat}\{91\}]\!]$
- if $89 < n < 100$, we know (IH) that $MC(n+11) \in \mathcal{E}_{k-1} [\![\mathrm{Nat}\{n+1\}]\!]$ and $MC(n+1) \in \mathcal{E}_{k-1} [\![\mathrm{Nat}\{91\}]\!]$
- if $n = 100$, we know (IH) that $MC(111) \in \mathcal{E}_{k-1} [\![\mathrm{Nat}\{101\}]\!]$ and $MC(101) \in \mathcal{E}_{k-1} [\![\mathrm{Nat}\{91\}]\!]$.

Contents

Kripke Semantics for the Metalogic

The metal-logic: Second-order *modal* logic with recursive predicates.

$$
\begin{array}{lcl}
k \models P \Rightarrow Q & \stackrel{def}{=} & \forall j \leq k.(j \models P) \Rightarrow (j \models Q) \\
k \models P \wedge Q & \stackrel{def}{=} & (k \models P) \wedge (k \models Q) \\
k \models \forall x.P & \stackrel{def}{=} & \forall x.(k \models P) \\
0 \models \triangleright P & \stackrel{def}{=} & \textbf{True} \\
k \models \triangleright P & \stackrel{def}{=} & k - 1 \models P \\
k \models \mu X.P & \stackrel{def}{=} & k \models P\{\mu X.P/X\} \\
\ldots & & \ldots
\end{array}
$$

- Monotonicity: for all j, k, P, if $j \leq k$ then $(k \models P) \Rightarrow (j \models P)$
- Lob Rule: For all $k, P : k \models (\triangleright P \Rightarrow P) \Rightarrow P$

(Nakano, LICS'00; Appel, McAllester, Mellies & Vouillon, POPL'04)

Realizability model

$$
\begin{aligned}
\mathcal{V}[\![\alpha]\!]_\rho &\overset{def}{=} P \quad \text{where } \rho(\alpha) = (P, \_)\} \\
\mathcal{V}[\![\mathrm{Unit}]\!]_\rho &\overset{def}{=} \{()\} \\
\mathcal{V}[\![\tau \to \sigma]\!]_\rho &\overset{def}{=} \{\lambda x.M \mid \forall v. v \in \mathcal{V}[\![\tau]\!]_\rho \Rightarrow (\lambda x.M)v \in \mathcal{E}[\![\sigma]\!]_\rho\} \\
\mathcal{V}[\![\forall\alpha.\tau]\!]_\rho &\overset{def}{=} \{\Lambda\alpha.M \mid \forall\sigma\forall P \in \mathrm{Pred}_\sigma(\Lambda\alpha.M)\sigma \in \mathcal{E}[\![\sigma]\!]_{\rho\cdot[\alpha\mapsto(P,\sigma)]}\} \\
\mathcal{V}[\![\exists\alpha.\tau]\!]_\rho &\overset{def}{=} \{(\mathrm{pack}\langle\sigma, v\rangle \mid \exists P \in \mathrm{Pred}_\sigma . v \in \mathcal{V}[\![\tau]\!]_{\rho\cdot[\alpha\mapsto(P,\sigma)]}\} \\
\mathcal{V}[\![\tau_1 \times \tau_2]\!]_\rho &\overset{def}{=} \{\langle u_1, u_2\rangle \mid \forall i \in \{1,2\}, u_i \in \mathcal{V}[\![\tau_i]\!]_\rho\} \\
\mathcal{V}[\![\tau_1 + \tau_2]\!]_\rho &\overset{def}{=} \{\mathrm{inj}_i(u) \mid i \in \{1,2\} \wedge u \in \mathcal{V}[\![\tau_i]\!]_\rho\} \\
\mathcal{V}[\![\mu\alpha.\tau]\!]_\rho &\overset{def}{=} \mu P.\{\mathrm{fold} v \mid \triangleright v \in \mathcal{V}[\![\tau]\!]_{\rho\cdot[\alpha\mapsto[(P,\rho(\mu\alpha.\tau))]}\} \\
\mathcal{E}[\![\tau]\!]_\rho &\overset{def}{=} \mu P.\{M \mid \forall h : w. \forall M'.(M, h) \mapsto (M', h) \\
&\qquad \Rightarrow \triangleright(M' \in \mathcal{E}[\![\tau]\!]_\rho)\}
\end{aligned}
$$

Soundness of the model

Theorem (Fundamental Theorem)

If $\Delta; \Sigma, \Gamma \vdash M : \tau$ *then for all* $k \in \mathbb{N}$,
$k \models \forall \rho \in \mathcal{D}[\![\Delta]\!], \gamma \in \mathcal{G}[\![\Gamma]\!]_\rho, M\{\gamma\}\{\rho\} \in \mathcal{E}[\![\tau]\!]_\rho$.

By induction on the derivation tree of $\Gamma \vdash M : \tau$, the proof being done inside the metalogic.

Compatibility lemma for the fixed point

- Let $\gamma \in \mathcal{G}[\![\Gamma]\!]$, we must prove that $(\texttt{fix}\ f(x).M)\{\gamma\} \in \mathcal{E}[\![\tau \to \sigma]\!]$ (?)

Compatibility lemma for the fixed point

- Let $\gamma \in \mathcal{G}[\![\Gamma]\!]$, we must prove that $(\texttt{fix}\ f(x).M)\{\gamma\} \in \mathcal{E}[\![\tau \to \sigma]\!]$ (?)
- i.e. does $\texttt{fix}\ f(x).M\{\gamma\} \in \mathcal{V}[\![\tau \to \sigma]\!]$ (?)

Compatibility lemma for the fixed point

- Let $\gamma \in \mathcal{G}[\![\Gamma]\!]$, we must prove that $(\texttt{fix}\ f(x).M)\{\gamma\} \in \mathcal{E}[\![\tau \to \sigma]\!]$ (?)
- i.e. does $\texttt{fix}\ f(x).M\{\gamma\} \in \mathcal{V}[\![\tau \to \sigma]\!]$ (?)
- i.e. for all $v \in \mathcal{V}[\![\tau]\!]$, does $(\texttt{fix}\ f(x).M\{\gamma\})v \in \mathcal{E}[\![\sigma]\!]$ (?)

Compatibility lemma for the fixed point

- Let $\gamma \in \mathcal{G}[\![\Gamma]\!]$, we must prove that $(\texttt{fix}\ f(x).M)\{\gamma\} \in \mathcal{E}[\![\tau \to \sigma]\!]$ (?)
- i.e. does $\texttt{fix}\ f(x).M\{\gamma\} \in \mathcal{V}[\![\tau \to \sigma]\!]$ (?)
- i.e. for all $v \in \mathcal{V}[\![\tau]\!]$, does $(\texttt{fix}\ f(x).M\{\gamma\})v \in \mathcal{E}[\![\sigma]\!]$ (?)
- i.e. does $\triangleright\big(M\{\gamma\}\{v/x\}\{\texttt{fix}\ f(x).M\{\gamma\}/f\} \in \mathcal{E}[\![\sigma]\!]\big)$ (?)

Compatibility lemma for the fixed point

- Let $\gamma \in \mathcal{G}[\![\Gamma]\!]$, we must prove that $(\texttt{fix}\ f(x).M)\{\gamma\} \in \mathcal{E}[\![\tau \to \sigma]\!]$ (?)
- i.e. does $\texttt{fix}\ f(x).M\{\gamma\} \in \mathcal{V}[\![\tau \to \sigma]\!]$ (?)
- i.e. for all $v \in \mathcal{V}[\![\tau]\!]$, does $(\texttt{fix}\ f(x).M\{\gamma\})v \in \mathcal{E}[\![\sigma]\!]$ (?)
- i.e. does $\triangleright\big(M\{\gamma\}\{v/x\}\{\texttt{fix}\ f(x).M\{\gamma\}/f\} \in \mathcal{E}[\![\sigma]\!]\big)$ (?)
- *IH*: for all $\gamma' \in \mathcal{G}[\![\Gamma, x : \tau, f : \tau \to \sigma]\!], M\{\gamma'\} \in \mathcal{E}[\![\sigma]\!]$
  Monotonicity: for all γ',
  $\triangleright\Big(\gamma' \in \mathcal{G}[\![\Gamma, x : \tau, f : \tau \to \sigma]\!]\Big) \Rightarrow \triangleright\Big(M\{\gamma'\} \in \mathcal{E}[\![\sigma]\!]\Big)$

Compatibility lemma for the fixed point

- Let $\gamma \in \mathcal{G}[\![\Gamma]\!]$, we must prove that $(\texttt{fix}\ f(x).M)\{\gamma\} \in \mathcal{E}[\![\tau \to \sigma]\!]$ (?)
- i.e. does $\texttt{fix}\ f(x).M\{\gamma\} \in \mathcal{V}[\![\tau \to \sigma]\!]$ (?)
- i.e. for all $v \in \mathcal{V}[\![\tau]\!]$, does $(\texttt{fix}\ f(x).M\{\gamma\})v \in \mathcal{E}[\![\sigma]\!]$ (?)
- i.e. does $\triangleright(M\{\gamma\}\{v/x\}\{\texttt{fix}\ f(x).M\{\gamma\}/f\} \in \mathcal{E}[\![\sigma]\!])$ (?)
- *IH*: for all $\gamma' \in \mathcal{G}[\![\Gamma, x : \tau, f : \tau \to \sigma]\!], M\{\gamma'\} \in \mathcal{E}[\![\sigma]\!]$
  Monotonicity: for all γ',
  $\triangleright\Big(\gamma' \in \mathcal{G}[\![\Gamma, x : \tau, f : \tau \to \sigma]\!]\Big) \Rightarrow \triangleright\Big(M\{\gamma'\} \in \mathcal{E}[\![\sigma]\!]\Big)$
- Does $\triangleright\Big(\gamma \cdot [x \mapsto v] \cdot [f \mapsto \texttt{fix}\ f(x).M\{\gamma\}] \in \mathcal{G}[\![\Gamma, x : \tau, f : \tau \to \sigma]\!]\Big)$?

Compatibility lemma for the fixed point

- Let $\gamma \in \mathcal{G}[\![\Gamma]\!]$, we must prove that $(\texttt{fix}\ f(x).M)\{\gamma\} \in \mathcal{E}[\![\tau \to \sigma]\!]$ (?)
- i.e. does $\texttt{fix}\ f(x).M\{\gamma\} \in \mathcal{V}[\![\tau \to \sigma]\!]$ (?)
- i.e. for all $v \in \mathcal{V}[\![\tau]\!]$, does $(\texttt{fix}\ f(x).M\{\gamma\})v \in \mathcal{E}[\![\sigma]\!]$ (?)
- i.e. does $\triangleright(M\{\gamma\}\{v/x\}\{\texttt{fix}\ f(x).M\{\gamma\}/f\} \in \mathcal{E}[\![\sigma]\!])$ (?)
- *IH*: for all $\gamma' \in \mathcal{G}[\![\Gamma, x : \tau, f : \tau \to \sigma]\!], M\{\gamma'\} \in \mathcal{E}[\![\sigma]\!]$
  Monotonicity: for all γ',
  $\triangleright\Big(\gamma' \in \mathcal{G}[\![\Gamma, x : \tau, f : \tau \to \sigma]\!]\Big) \Rightarrow \triangleright\Big(M\{\gamma'\} \in \mathcal{E}[\![\sigma]\!]\Big)$
- Does $\triangleright\Big(\gamma \cdot [x \mapsto v] \cdot [f \mapsto \texttt{fix}\ f(x).M\{\gamma\}] \in \mathcal{G}[\![\Gamma, x : \tau, f : \tau \to \sigma]\!]\Big)$?
- Only if $\triangleright(\texttt{fix}\ f(x).M\{\gamma\} \in \mathcal{V}[\![\tau \to \sigma]\!])$ ... Lob rule to the rescue !
  Writing P for $\texttt{fix}\ f(x).M\{\gamma\} \in \mathcal{V}[\![\tau \to \sigma]\!]$, we have $(\triangleright P \Rightarrow P) \Rightarrow P$.

Contents

Generalizing the metalogic

Goal: A Framework to

- Solve recursive domain equations as in the category of bisected ultrametric spaces,
- Hide step-indexing using Godel-Lob logic.

A semantic model: "Topos of trees" $\mathcal{S}$ = Presheaves over $\mathbb{N}$ (Birkedal et al., LICS'10):

- $F : \mathbb{N} \to \mathrm{Set}$
- for all $k \geq j$, restrictions maps $\theta_{k \to j} : F(k) \to F(j)$ s.t.
  - $\theta_{k \to k} = id_{F(k)}$
  - $\theta_{k \to j} \circ \theta_{j \to i} = \theta_{k \to i}$.

$\mathcal{S}$ is a topos $\Rightarrow$ we can model dependent type theory in it.

Calculus of Construction as the Metalogic

Dependent Products and Sums, Hierarchy of universe:
$\Pi x : T.U, \Sigma x : T.U, \mathrm{Prop}, (\mathrm{Type}_i)_{i \in \mathbb{N}}), \ldots$

Basic ingredients to define guarded recursive types:

- for all type universe $\mathcal{U} \in \{\mathrm{Prop}, \mathrm{Type}_i\}$, a term $\triangleright : \mathcal{U} \to \mathcal{U}$,
- for all types T, a term $fix_T : (\triangleright T \to T) \to T$,
  - ⇝ when T is a proposition: Lob rule,
- for all types T, a term $next_T : T \to \triangleright T$,
- for all type universe $\mathcal{U} \in \{\mathrm{Prop}, \mathrm{Type}_i\}$, a term $switch : \triangleright \mathcal{U} \to \mathcal{U}$,
  - ⇝ s.t. $switch(next_{\mathcal{U}}(T)) = \triangleright T$.

$$\boxed{fix(f) = f(next(fix(f)))}$$

Going Further

- Step-indexing is an instance of Forcing !
  - $\rightsquigarrow$ Composition of Forcing and Realizability.
- In practice: Logical Relations rather than Realizability
  - $\rightsquigarrow$ Binary v.s. Unary predicates.
  - $\rightsquigarrow$ Biorthogonal definitions (similar to Krivine realizability).
  - $\rightsquigarrow$ Great tool to prove contextual equivalence and "free theorems".
- Connection with recursive domain equations
  - $\rightsquigarrow$ 1-bounded bisected ultrametric spaces (Birkedal et al., POPL'11)
- Guarded Recursive Types
  - $\rightsquigarrow$ Useful to encode *productive* coinductive types.