A Classical Realizability Model for PML

Semantical Value Restriction & Pointed subtyping

Parametricity, Logical Relations & Realizability
(CSL 2016, Marseille, France)

Rodolphe Lepigre (rodolphe.lepigre@univ-smb.fr)

PML (Programs and Proofs)

PML (Programs and Proofs)

```
type rec N = [ Z | S of N ]
val rec add : N ⇒ N ⇒ N = fun n m →
  match n with
  | Z    → m
  | S[k] → S[add k m]
```

PML (Programs and Proofs)

```
type rec N = [ Z | S of N ]
val rec add : N ⇒ N ⇒ N = fun n m →
  match n with
  | Z    → m
  | S[k] → S[add k m]

val addZN : ∀m (add Z m ≡ m) = {}
```

PML (Programs and Proofs)

```
type rec N = [ Z | S of N ]
val rec add : N ⇒ N ⇒ N = fun n m →
  match n with
  | Z    → m
  | S[k] → S[add k m]

val addZN : ∀m (add Z m ≡ m) = {}

val rec addNZ : (n:N) ⇒ (add n Z ≡ n) = fun n →
  match n with
  | Z    → {}
  | S[k] → addNZ k; {}
```

Call-by-value Krivine Machine

$$
\begin{aligned}
v, w &::= x \mid \lambda x.t \mid \{(l_i = v_i)_{i \in I}\} \mid C[v] \\
t, u &::= a \mid v \mid t\ u \mid \mu\alpha.t \mid [\pi]t \mid v.l \mid [v \mid (C_i[x_i] \to t_i)_{i \in I}] \\
\pi, \rho &::= \alpha \mid \varepsilon \mid v \cdot \pi \mid [t]\pi
\end{aligned}
$$

Call-by-value Krivine Machine

$$
\begin{aligned}
v, w &::= x \mid \lambda x.t \mid \{(l_i = v_i)_{i\in I}\} \mid C[v] \\
t, u &::= a \mid v \mid t\ u \mid \mu\alpha.t \mid [\pi]t \mid v.l \mid [v \mid (C_i[x_i] \to t_i)_{i\in I}] \\
\pi, \rho &::= \alpha \mid \varepsilon \mid v \cdot \pi \mid [t]\pi
\end{aligned}
$$

$$
\begin{aligned}
t\ u * \pi &\succ u * [t]\pi \\
v * [t]\pi &\succ t * v \cdot \pi \\
\lambda x.t * v \cdot \pi &\succ t[x := v] * \pi \\
\mu\alpha.t * \pi &\succ t[\alpha := \pi] * \pi \\
[\pi]t * \xi &\succ t * \pi \\
\{(l_i = v_i)_{i\in I}\}.l_k * \pi &\succ v_k * \pi \\
[C_k[v] \mid (C_i[x_i] \to t_i)_{i\in I}] * \pi &\succ t_k[x_k := v] * \pi
\end{aligned}
$$

Call-by-value realizability interpretation

Call-by-value realizability interpretation

$$\llbracket A \rrbracket \in \{\Phi \subseteq \Lambda_{\text{val}} \mid v \in \Phi \wedge v \equiv w \Rightarrow w \in \Phi\}$$

$$\llbracket A \rrbracket^{\perp} = \{\pi \in \Pi \mid \forall v \in \llbracket A \rrbracket, v * \pi \in \perp\!\!\!\perp\}$$

$$\llbracket A \rrbracket^{\perp\perp} = \{t \in \Lambda \mid \forall \pi \in \llbracket A \rrbracket^{\perp}, t * \pi \in \perp\!\!\!\perp\}$$

Call-by-value realizability interpretation

$$\llbracket A \rrbracket \in \{\Phi \subseteq \Lambda_{\text{val}} \mid v \in \Phi \wedge v \equiv w \Rightarrow w \in \Phi\}$$

$$\llbracket A \rrbracket^{\perp\!\!\!\perp} = \{\pi \in \Pi \mid \forall v \in \llbracket A \rrbracket, v * \pi \in \perp\!\!\!\perp\}$$

$$\llbracket A \rrbracket^{\perp\!\!\!\perp\perp\!\!\!\perp} = \{t \in \Lambda \mid \forall \pi \in \llbracket A \rrbracket^{\perp\!\!\!\perp}, t * \pi \in \perp\!\!\!\perp\}$$

Adequacy for terms: if $\Gamma \vdash t : A$ is valid and $\rho \Vdash \Gamma$ then $t\rho \in \llbracket A\rho \rrbracket^{\perp\!\!\!\perp\perp\!\!\!\perp}$.

Call-by-value realizability interpretation

$$\begin{aligned}
[\![A]\!] &\in \{\Phi \subseteq \Lambda_{\mathrm{val}} \mid v \in \Phi \wedge v \equiv w \Rightarrow w \in \Phi\} \\
[\![A]\!]^{\perp} &= \{\pi \in \Pi \mid \forall v \in [\![A]\!], v * \pi \in \perp\!\!\!\perp\} \\
[\![A]\!]^{\perp\perp} &= \{t \in \Lambda \mid \forall \pi \in [\![A]\!]^{\perp}, t * \pi \in \perp\!\!\!\perp\}
\end{aligned}$$

Adequacy for terms: if $\Gamma \vdash t : A$ is valid and $\rho \Vdash \Gamma$ then $t\rho \in [\![A\rho]\!]^{\perp\perp}$.

Adequacy for values: if $\Gamma \vdash_{\mathrm{val}} v : A$ is valid and $\rho \Vdash \Gamma$ then $v\rho \in [\![A\rho]\!]$.

$$\begin{aligned}
[\![A]\!] &\in \{\Phi \subseteq \Lambda_{\mathrm{val}} \mid v \in \Phi \wedge v \equiv w \Rightarrow w \in \Phi\} \\
[\![A]\!]^{\perp\!\!\!\perp} &= \{\pi \in \Pi \mid \forall\, v \in [\![A]\!], v * \pi \in \perp\!\!\!\perp\} \\
[\![A]\!]^{\perp\!\!\!\perp\perp\!\!\!\perp} &= \{t \in \Lambda \mid \forall\, \pi \in [\![A]\!]^{\perp\!\!\!\perp}, t * \pi \in \perp\!\!\!\perp\}
\end{aligned}$$

Adequacy for terms: if $\Gamma \vdash t : A$ is valid and $\rho \Vdash \Gamma$ then $t\rho \in [\![A\rho]\!]^{\perp\!\!\!\perp\perp\!\!\!\perp}$.

Adequacy for values: if $\Gamma \vdash_{\mathrm{val}} v : A$ is valid and $\rho \Vdash \Gamma$ then $v\rho \in [\![A\rho]\!]$.

Since $[\![A]\!] \subseteq [\![A]\!]^{\perp\!\!\!\perp\perp\!\!\!\perp}$ we have the rule $\dfrac{\Gamma \vdash_{\mathrm{val}} v : A}{\Gamma \vdash v : A}\uparrow$.

Fairly usual typing rules

$$\frac{\Gamma, x : A \vdash t : B}{\Gamma \vdash_{\text{val}} \lambda x.t : A \Rightarrow B}\Rightarrow_i \qquad \frac{\Gamma \vdash t : A \Rightarrow B \quad \Gamma \vdash u : A}{\Gamma \vdash t\ u : B}\Rightarrow_e$$

$$\frac{(\Gamma \vdash_{\text{val}} v_i : A_i)_{i \in I}}{\Gamma \vdash_{\text{val}} \{(l_i = v_i)_{i \in I}\} : \{(l_i : A_i)_{i \in I}\}}\times_i \qquad \frac{\Gamma \vdash_{\text{val}} v : \{(l_i : A_i)_{i \in I}\} \quad k \in I}{\Gamma \vdash v.l_k : A_k}\times_e$$

$$\frac{\Gamma \vdash_{\text{val}} v : A \quad X \notin \mathrm{FV}(\Gamma)}{\Gamma \vdash_{\text{val}} v : \forall X.A}\forall_i \qquad \frac{\Gamma \vdash t : \forall X.A}{\Gamma \vdash t : A[X := B]}\forall_e$$

Equivalence types

Equivalence types

$$(\equiv) = \{(t, u) \mid \forall \pi, \forall \rho, t\rho * \pi \Downarrow \Leftrightarrow u\rho * \pi \Downarrow\}$$

$t * \pi \Downarrow$ is defined as $\exists\, v, t * \pi \succ^* v * \varepsilon$.

Equivalence types

$$(\equiv) = \{(t, u) \mid \forall \pi, \forall \rho, t\rho * \pi \Downarrow \Leftrightarrow u\rho * \pi \Downarrow\}$$

$t * \pi \Downarrow$ is defined as $\exists\, v, t * \pi \succ^* v * \varepsilon$.

$$[\![A \upharpoonright u_1 \equiv u_2]\!] = \{v \in [\![A]\!] \mid u_1 \equiv u_2\}$$

$u_1 \equiv u_2$ is defined as $\{\} \upharpoonright u_1 \equiv u_2$.

Equivalence types

$$(\equiv) = \{(t, u) \mid \forall \pi, \forall \rho, t\rho * \pi \Downarrow \Leftrightarrow u\rho * \pi \Downarrow\}$$

$t * \pi \Downarrow$ is defined as $\exists\, v, t * \pi \succ^* v * \varepsilon$.

$$[\![A \upharpoonright u_1 \equiv u_2]\!] = \{v \in [\![A]\!] \mid u_1 \equiv u_2\}$$

$u_1 \equiv u_2$ is defined as $\{\} \upharpoonright u_1 \equiv u_2$.

$$\frac{\Gamma \vdash t : A \qquad \mathcal{E}(\Gamma) \vdash u_1 \equiv u_2}{\Gamma \vdash t : A \upharpoonright u_1 \equiv u_2}\upharpoonright_i \qquad \frac{\Gamma, x : A, u_1 \equiv u_2 \vdash t : C}{\Gamma, x : A \upharpoonright u_1 \equiv u_2 \vdash t : C}\upharpoonright_e$$

Singleton and typed quantification

Singleton and typed quantification

$$[\![t \in A]\!] = \{ v \in [\![A]\!] \mid t \equiv v \}$$

$(a : A) \Rightarrow B$ is defined as $\forall a.(a \in A \Rightarrow B)$.

Singleton and typed quantification

$$[\![t \in A]\!] = \{v \in [\![A]\!] \mid t \equiv v\}$$

$(a : A) \Rightarrow B$ is defined as $\forall a.(a \in A \Rightarrow B)$.

$$\frac{\Gamma \vdash_{\text{val}} v : A}{\Gamma \vdash_{\text{val}} v : v \in A}\in_{\text{i}} \qquad \frac{\Gamma, x : A, x \equiv t \vdash u : C}{\Gamma, x : t \in A \vdash u : C}\in_{\text{e}}$$

Singleton and typed quantification

$$[\![t \in A]\!] = \{v \in [\![A]\!] \mid t \equiv v\}$$

$(a : A) \Rightarrow B$ is defined as $\forall a.(a \in A \Rightarrow B)$.

$$\frac{\Gamma \vdash_{\text{val}} v : A}{\Gamma \vdash_{\text{val}} v : v \in A}\in_{\text{i}} \qquad \frac{\Gamma, x : A, x \equiv t \vdash u : C}{\Gamma, x : t \in A \vdash u : C}\in_{\text{e}}$$

$$\frac{\Gamma, x : A \vdash t : B[a := x]}{\Gamma \vdash_{\text{val}} \lambda x.t : (a : A) \Rightarrow B} \qquad \frac{\Gamma \vdash t : (a : A) \Rightarrow B \quad \Gamma \vdash_{\text{val}} v : A}{\Gamma \vdash t\ v : B[a := v]}$$

Semantical Value Restriction

A Classical Realizability Model for a Semantical Value Restriction (ESOP 2016).

$$\frac{\Gamma \vdash_{\mathrm{val}} v : A}{\Gamma \vdash_{\mathrm{val}} v : v \in A}\in_{\mathrm{i}} \qquad \frac{\Gamma \vdash t : A \quad \mathcal{E}(\Gamma) \vdash \exists v\ v \equiv t}{\Gamma \vdash t : t \in A}\in_{\mathrm{i}}$$

A Classical Realizability Model for a Semantical Value Restriction (ESOP 2016).

$$\frac{\Gamma \vdash_{\mathrm{val}} v : A}{\Gamma \vdash_{\mathrm{val}} v : v{\in}A}\in_{\mathrm{i}} \qquad \frac{\Gamma \vdash t : A \quad \mathcal{E}(\Gamma) \vdash \exists\, v\ v \equiv t}{\Gamma \vdash t : t{\in}A}\in_{\mathrm{i}}$$

We want $\dfrac{\Gamma \vdash v : A}{\Gamma \vdash_{\mathrm{val}} v : A}\downarrow$ so we need $[\![A]\!]^{\perp\!\perp} \cap \Lambda_{\mathrm{val}} = [\![A]\!]$.

A Classical Realizability Model for a Semantical Value Restriction (ESOP 2016).

$$\frac{\Gamma \vdash_{\text{val}} v : A}{\Gamma \vdash_{\text{val}} v : v{\in}A}{\in_{\text{i}}} \qquad \frac{\Gamma \vdash t : A \quad \mathcal{E}(\Gamma) \vdash \exists\, v\ v \equiv t}{\Gamma \vdash t : t{\in}A}{\in_{\text{i}}}$$

We want $\dfrac{\Gamma \vdash v : A}{\Gamma \vdash_{\text{val}} v : A}{\downarrow}$ so we need $[\![A]\!]^{\perp\!\perp} \cap \Lambda_{\text{val}} = [\![A]\!]$.

Add a new term constructor $\delta_{v,w}$ with the rule

$$\delta_{v,w} * \pi \succ v * \pi \qquad \text{when } v \not\equiv w.$$

Toward a practical system

Practical Subtyping for System F with Sized (Co-)Induction (Unpublished 2015/2016).

Practical Subtyping for System F with Sized (Co-)Induction (Unpublished 2015/2016).

Prototype implementation: *http://lama.univ-savoie.fr/subml/*.

Practical Subtyping for System F with Sized (Co-)Induction (Unpublished 2015/2016).

Prototype implementation: *http://lama.univ-savoie.fr/subml/*.

Idea: use subtyping to handle connectives with no algorithmic contents.

Practical Subtyping for System F with Sized (Co-)Induction (Unpublished 2015/2016).

Prototype implementation: *http://lama.univ-savoie.fr/subml/*.

Idea: use subtyping to handle connectives with no algorithmic contents.

Subtyping (plus some ideas) makes things simpler.

Pointed subtyping and choice operators

Ternary judgment $t : A \subseteq B$ (pointed subtyping) instead of $A \subseteq B$.

Interpreted as $t : A$ implies $t : B$.

Pointed subtyping and choice operators

Ternary judgment $t : A \subseteq B$ (pointed subtyping) instead of $A \subseteq B$.

Interpreted as $t : A$ implies $t : B$.

Necessary to handle $t \in A$ using subtyping.

Pointed subtyping and choice operators

Ternary judgment $t : A \subseteq B$ (pointed subtyping) instead of $A \subseteq B$.

Interpreted as $t : A$ implies $t : B$.

Necessary to handle $t \in A$ using subtyping.

We use symbolic witnesses to "break binders" (no free variables).

Pointed subtyping and choice operators

Ternary judgment $t : A \subseteq B$ (pointed subtyping) instead of $A \subseteq B$.

Interpreted as $t : A$ implies $t : B$.

Necessary to handle $t \in A$ using subtyping.

We use symbolic witnesses to "break binders" (no free variables).

For example $\forall X.A$ corresponds to $A[X := \varepsilon_X(t \notin A)]$.

Pointed subtyping and choice operators

Ternary judgment $t : A \subseteq B$ (pointed subtyping) instead of $A \subseteq B$.

Interpreted as $t : A$ implies $t : B$.

Necessary to handle $t \in A$ using subtyping.

We use symbolic witnesses to "break binders" (no free variables).

For example $\forall X.A$ corresponds to $A[X := \varepsilon_X(t \notin A)]$.

Our context only contains equivalences over (closed) terms.

Typing rules

Typing rules

$$\frac{\Xi \vdash t : A \Rightarrow B \quad \Xi \vdash u : A}{\Xi \vdash t\ u : B}\Rightarrow_e$$

Typing rules

$$\frac{\Xi \vdash t : A \Rightarrow B \quad \Xi \vdash u : A}{\Xi \vdash t\ u : B}\Rightarrow_e$$

$$\frac{\Xi \vdash \varepsilon_{x \in A}(t \notin B) \in A \subseteq C}{\Xi \vdash \varepsilon_{x \in A}(t \notin B) : C}\subseteq$$

Typing rules

$$\frac{\Xi \vdash t : A \Rightarrow B \quad \Xi \vdash u : A}{\Xi \vdash t\ u : B}\Rightarrow_e$$

$$\frac{\Xi \vdash \varepsilon_{x \in A}(t \notin B) \in A \subseteq C}{\Xi \vdash \varepsilon_{x \in A}(t \notin B) : C}\subseteq$$

$$\frac{\Xi \vdash \lambda x.t \in A \Rightarrow B \subseteq C \quad \Xi \vdash t[x := \varepsilon_{x \in A}(t \notin B)] : B}{\Xi \vdash \lambda x.t : C}\Rightarrow_i$$

Typing rules

$$\frac{\Xi \vdash t : A \Rightarrow B \quad \Xi \vdash u : A}{\Xi \vdash t\ u : B}\Rightarrow_e$$

$$\frac{\Xi \vdash \varepsilon_{x \in A}(t \notin B) \in A \subseteq C}{\Xi \vdash \varepsilon_{x \in A}(t \notin B) : C}\subseteq$$

$$\frac{\Xi \vdash \lambda x.t \in A \Rightarrow B \subseteq C \quad \Xi \vdash t[x := \varepsilon_{x \in A}(t \notin B)] : B}{\Xi \vdash \lambda x.t : C}\Rightarrow_i$$

$$\frac{\Xi \vdash v : [(C_i : A_i)_{i \in I}] \quad \left(\Xi, v \equiv C_i[\varepsilon_{x_i \in A_i}(t_i \notin C)] \vdash t_i[x_i := \varepsilon_{x_i \in A_i}(t_i \notin C)] : C\right)_{i \in I}}{\Xi \vdash [v \mid (C_i[x_i] \to t_i)_{i \in I}] : C}+_e$$

Subtyping rules

Subtyping rules

$$\frac{\Xi \vdash t : A[X := C] \subseteq B}{\Xi \vdash t : \forall X.A \subseteq B}\,\forall_L$$

Subtyping rules

$$\frac{\Xi \vdash t : A[X := C] \subseteq B}{\Xi \vdash t : \forall X.A \subseteq B}\,\forall_l$$

$$\frac{\Xi \vdash t : A \subseteq B[X := \varepsilon_X(t \notin B)] \quad \Xi \vdash \exists\, v, v \equiv t}{\Xi \vdash t : A \subseteq \forall X.B}\,\forall_r$$

Subtyping rules

$$\frac{\Xi \vdash t : A[X := C] \subseteq B}{\Xi \vdash t : \forall X.A \subseteq B}\,\forall_l$$

$$\frac{\Xi \vdash t : A \subseteq B[X := \varepsilon_X(t \notin B)] \qquad \Xi \vdash \exists\, v, v \equiv t}{\Xi \vdash t : A \subseteq \forall X.B}\,\forall_r$$

$$\frac{\Xi, u_1 \equiv u_2 \vdash t : A \subseteq B}{\Xi \vdash t : A \restriction u_1 \equiv u_2 \subseteq B}\,\restriction_l$$

Subtyping rules

$$\frac{\Xi \vdash t : A[X := C] \subseteq B}{\Xi \vdash t : \forall X.A \subseteq B}\,\forall_l$$

$$\frac{\Xi \vdash t : A \subseteq B[X := \varepsilon_X(t \notin B)] \qquad \Xi \vdash \exists\, v, v \equiv t}{\Xi \vdash t : A \subseteq \forall X.B}\,\forall_r$$

$$\frac{\Xi, u_1 \equiv u_2 \vdash t : A \subseteq B}{\Xi \vdash t : A \restriction u_1 \equiv u_2 \subseteq B}\,\restriction_l$$

$$\frac{\Xi \vdash t : A \subseteq B \qquad \Xi \vdash u_1 \equiv u_2}{\Xi \vdash t : A \subseteq B \restriction u_1 \equiv u_2}\,\restriction_r$$

Adequacy (typing judgments): if $\Xi \vdash t : A$ is valid then $[\![t]\!] \in [\![A]\!]^{\perp\!\!\perp}$.

Adequacy (typing judgments): if $\Xi \vdash t : A$ is valid then $[\![t]\!] \in [\![A]\!]^{\perp\perp}$.

Adequacy (subtyping judgments): if $\Xi \vdash t : A \subseteq B$ is valid then $[\![t]\!] \in [\![A]\!]^{\perp\perp}$ implies $[\![t]\!] \in [\![B]\!]^{\perp\perp}$.

Adequacy (typing judgments): if $\Xi \vdash t : A$ is valid then $[\![t]\!] \in [\![A]\!]^{\perp\perp}$.

Adequacy (subtyping judgments): if $\Xi \vdash t : A \subseteq B$ is valid then $[\![t]\!] \in [\![A]\!]^{\perp\perp}$ implies $[\![t]\!] \in [\![B]\!]^{\perp\perp}$.

Remark: when $t = v$ it is the same as $[\![v]\!] \in [\![A]\!]$ implies $[\![v]\!] \in [\![B]\!]$.

Semantical interpretation of judgments

Adequacy (typing judgments): if $\Xi \vdash t : A$ is valid then $[\![t]\!] \in [\![A]\!]^{\perp\perp}$.

Adequacy (subtyping judgments): if $\Xi \vdash t : A \subseteq B$ is valid then $[\![t]\!] \in [\![A]\!]^{\perp\perp}$ implies $[\![t]\!] \in [\![B]\!]^{\perp\perp}$.

Remark: when $t = v$ it is the same as $[\![v]\!] \in [\![A]\!]$ implies $[\![v]\!] \in [\![B]\!]$.

But only in a model with the property $[\![A]\!]^{\perp\perp} \cap \Lambda_{\text{val}} = [\![A]\!]$.

Adequacy of the arrow introduction rule

$$\frac{\Xi \vdash \lambda x.t : A \Rightarrow B \subseteq C \qquad \Xi \vdash t[x := \varepsilon_{x \in A}(t \notin B)] : B}{\Xi \vdash \lambda x.t : C} \Rightarrow_i$$

Adequacy of the arrow introduction rule

$$\frac{\Xi \vdash \lambda x.t : A \Rightarrow B \subseteq C \qquad \Xi \vdash t[x := \varepsilon_{x \in A}(t \notin B)] : B}{\Xi \vdash \lambda x.t : C} \Rightarrow_i$$

We need to show $[\![\lambda x.t]\!] \in [\![C]\!]^{\perp\!\perp}$.

Adequacy of the arrow introduction rule

$$\frac{\Xi \vdash \lambda x.t : A \Rightarrow B \subseteq C \qquad \Xi \vdash t[x := \varepsilon_{x \in A}(t \notin B)] : B}{\Xi \vdash \lambda x.t : C} \Rightarrow_i$$

We need to show $[\![\lambda x.t]\!] \in [\![C]\!]^{\perp\perp}$.

Using the left IH it is enough to show $[\![\lambda x.t]\!] \in [\![A \Rightarrow B]\!]^{\perp\perp}$.

Adequacy of the arrow introduction rule

$$\frac{\Xi \vdash \lambda x.t : A \Rightarrow B \subseteq C \qquad \Xi \vdash t[x := \varepsilon_{x \in A}(t \notin B)] : B}{\Xi \vdash \lambda x.t : C} \Rightarrow_i$$

We need to show $[\![\lambda x.t]\!] \in [\![C]\!]^{\perp\perp}$.

Using the left IH it is enough to show $[\![\lambda x.t]\!] \in [\![A \Rightarrow B]\!]^{\perp\perp}$.

Equivalently, we can show $[\![\lambda x.t]\!] \in [\![A \Rightarrow B]\!]$.

Adequacy of the arrow introduction rule

$$\frac{\Xi \vdash \lambda x.t : A \Rightarrow B \subseteq C \qquad \Xi \vdash t[x := \varepsilon_{x \in A}(t \notin B)] : B}{\Xi \vdash \lambda x.t : C} \Rightarrow_i$$

We need to show $[\![\lambda x.t]\!] \in [\![C]\!]^{\perp\perp}$.

Using the left IH it is enough to show $[\![\lambda x.t]\!] \in [\![A \Rightarrow B]\!]^{\perp\perp}$.

Equivalently, we can show $[\![\lambda x.t]\!] \in [\![A \Rightarrow B]\!]$.

By definition $[\![\varepsilon_{x \in A}(t \notin B)]\!] = v$ such that $[\![t[x := v]]\!] \notin [\![B]\!]^{\perp\perp}$.

Adequacy of the arrow introduction rule

$$\frac{\Xi \vdash \lambda x.t : A \Rightarrow B \subseteq C \qquad \Xi \vdash t[x := \varepsilon_{x \in A}(t \notin B)] : B}{\Xi \vdash \lambda x.t : C} \Rightarrow_i$$

We need to show $[\![\lambda x.t]\!] \in [\![C]\!]^{\perp\perp}$.

Using the left IH it is enough to show $[\![\lambda x.t]\!] \in [\![A \Rightarrow B]\!]^{\perp\perp}$.

Equivalently, we can show $[\![\lambda x.t]\!] \in [\![A \Rightarrow B]\!]$.

By definition $[\![\varepsilon_{x \in A}(t \notin B)]\!] = v$ such that $[\![t[x := v]]\!] \notin [\![B]\!]^{\perp\perp}$.

There is no such term as $[\![t[x := v]]\!] \in [\![B]\!]^{\perp\perp}$ by the right IH.

Adequacy of the arrow introduction rule

$$\frac{\Xi \vdash \lambda x.t : A \Rightarrow B \subseteq C \qquad \Xi \vdash t[x := \varepsilon_{x \in A}(t \notin B)] : B}{\Xi \vdash \lambda x.t : C} \Rightarrow_i$$

We need to show $[\![\lambda x.t]\!] \in [\![C]\!]^{\perp\perp}$.

Using the left IH it is enough to show $[\![\lambda x.t]\!] \in [\![A \Rightarrow B]\!]^{\perp\perp}$.

Equivalently, we can show $[\![\lambda x.t]\!] \in [\![A \Rightarrow B]\!]$.

By definition $[\![\varepsilon_{x \in A}(t \notin B)]\!] = v$ such that $[\![t[x := v]]\!] \notin [\![B]\!]^{\perp\perp}$.

There is no such term as $[\![t[x := v]]\!] \in [\![B]\!]^{\perp\perp}$ by the right IH.

This means that for all $v \in [\![A]\!]$ we have $t[x := v] \in [\![B]\!]^{\perp\perp}$.

Adequacy of the right membership rule

$$\frac{\Xi \vdash t : A \subseteq B \quad \Xi \vdash t \equiv u \quad \Xi \vdash \exists v, v \equiv t}{\Xi \vdash t : A \subseteq u \in B} \in_r$$

Adequacy of the right membership rule

$$\frac{\Xi \vdash t : A \subseteq B \quad \Xi \vdash t \equiv u \quad \Xi \vdash \exists v, v \equiv t}{\Xi \vdash t : A \subseteq u \in B} \in_r$$

We need to show $[\![t]\!] \in [\![A]\!]^{\perp\perp} \Rightarrow [\![t]\!] \in [\![u \in B]\!]^{\perp\perp}$.

Adequacy of the right membership rule

$$\frac{\Xi \vdash t : A \subseteq B \quad \Xi \vdash t \equiv u \quad \Xi \vdash \exists v, v \equiv t}{\Xi \vdash t : A \subseteq u \in B} \in_r$$

We need to show $[\![t]\!] \in [\![A]\!]^{\perp\perp} \Rightarrow [\![t]\!] \in [\![u \in B]\!]^{\perp\perp}$.

It is enough to show $[\![t]\!] \in [\![B]\!]^{\perp\perp} \Rightarrow [\![t]\!] \in [\![u \in B]\!]^{\perp\perp}$ (first IH).

Adequacy of the right membership rule

$$\frac{\Xi \vdash t : A \subseteq B \quad \Xi \vdash t \equiv u \quad \Xi \vdash \exists v, v \equiv t}{\Xi \vdash t : A \subseteq u \in B} \in_r$$

We need to show $[\![t]\!] \in [\![A]\!]^{\perp\perp} \Rightarrow [\![t]\!] \in [\![u \in B]\!]^{\perp\perp}$.

It is enough to show $[\![t]\!] \in [\![B]\!]^{\perp\perp} \Rightarrow [\![t]\!] \in [\![u \in B]\!]^{\perp\perp}$ (first IH).

It is equivalent to show $[\![v]\!] \in [\![B]\!]^{\perp\perp} \Rightarrow [\![v]\!] \in [\![u \in B]\!]^{\perp\perp}$ for some v (right IH).

Adequacy of the right membership rule

$$\frac{\Xi \vdash t : A \subseteq B \quad \Xi \vdash t \equiv u \quad \Xi \vdash \exists v, v \equiv t}{\Xi \vdash t : A \subseteq u \in B} \in_r$$

We need to show $[\![t]\!] \in [\![A]\!]^{\perp\perp} \Rightarrow [\![t]\!] \in [\![u \in B]\!]^{\perp\perp}$.

It is enough to show $[\![t]\!] \in [\![B]\!]^{\perp\perp} \Rightarrow [\![t]\!] \in [\![u \in B]\!]^{\perp\perp}$ (first IH).

It is equivalent to show $[\![v]\!] \in [\![B]\!]^{\perp\perp} \Rightarrow [\![v]\!] \in [\![u \in B]\!]^{\perp\perp}$ for some v (right IH).

It is equivalent to show $[\![v]\!] \in [\![B]\!] \Rightarrow [\![v]\!] \in [\![u \in B]\!]$ (property of the model).

Adequacy of the right membership rule

$$\frac{\Xi \vdash t : A \subseteq B \quad \Xi \vdash t \equiv u \quad \Xi \vdash \exists v, v \equiv t}{\Xi \vdash t : A \subseteq u \in B} \in_r$$

We need to show $[\![t]\!] \in [\![A]\!]^{\perp\perp} \Rightarrow [\![t]\!] \in [\![u \in B]\!]^{\perp\perp}$.

It is enough to show $[\![t]\!] \in [\![B]\!]^{\perp\perp} \Rightarrow [\![t]\!] \in [\![u \in B]\!]^{\perp\perp}$ (first IH).

It is equivalent to show $[\![v]\!] \in [\![B]\!]^{\perp\perp} \Rightarrow [\![v]\!] \in [\![u \in B]\!]^{\perp\perp}$ for some v (right IH).

It is equivalent to show $[\![v]\!] \in [\![B]\!] \Rightarrow [\![v]\!] \in [\![u \in B]\!]$ (property of the model).

We can conclude as $v \equiv u$ (middle and right IH).

Missing parts and future work

Missing parts and future work

Inductive and coinductive types (missing)

Recursion, termination checking (missing)

Higher-order types (missing)

Missing parts and future work

Inductive and coinductive types (missing)

Recursion, termination checking (missing)

Higher-order types (missing)

Implementation of the system (in progress)

PhD thesis (in progress)

Missing parts and future work

Inductive and coinductive types (missing)
Recursion, termination checking (missing)
Higher-order types (missing)

Implementation of the system (in progress)
PhD thesis (in progress)

An efficient compiler (future work)

Missing parts and future work

Inductive and coinductive types (missing)

Recursion, termination checking (missing)

Higher-order types (missing)

Implementation of the system (in progress)

PhD thesis (in progress)

An efficient compiler (future work)

Devise a plan to take over the world with PML (future work)

Fin.