

A Classical Realisability Model for PML_2 with Semantical Value Restriction



Inria Saclay 22/02/2017

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

PROGRAMS AND PROOFS

PROGRAMS AND PROOFS

```
type rec N = [ Z | S of N ]  
val rec add : N  $\Rightarrow$  N  $\Rightarrow$  N =  
  fun n m  $\rightarrow$   
    match n with  
      | Z       $\rightarrow$  m  
      | S[k]   $\rightarrow$  S[add k m]
```

PROGRAMS AND PROOFS

```
type rec N = [ Z | S of N ]  
val rec add : N  $\Rightarrow$  N  $\Rightarrow$  N =  
  fun n m  $\rightarrow$   
    match n with  
      | Z       $\rightarrow$  m  
      | S[k]   $\rightarrow$  S[add k m]  
  
val addZN :  $\forall n$  (add Z n  $\equiv$  n) = {}
```

PROGRAMS AND PROOFS

```
type rec N = [ Z | S of N ]
```

```
val rec add : N  $\Rightarrow$  N  $\Rightarrow$  N =
```

```
  fun n m  $\rightarrow$ 
```

```
    match n with
```

```
      | Z       $\rightarrow$  m
```

```
      | S[k]  $\rightarrow$  S[add k m]
```

```
val addZN :  $\forall n$  (add Z n  $\equiv$  n) = {}
```

```
// val addNZ :  $\forall n$  (add n Z  $\equiv$  n) = ...
```

```
// Cannot be proved.
```

PROOFS AND TYPED QUANTIFICATION

PROOFS AND TYPED QUANTIFICATION

```
val rec addNZ : (n:N)  $\Rightarrow$  (add n Z  $\equiv$  n) =  
  fun n  $\rightarrow$   
    match n with  
    | Z       $\rightarrow$  {}  
    | S[k]  $\rightarrow$  addNZ k; {}
```

PROOFS AND TYPED QUANTIFICATION

```
val rec addNZ : (n:N)  $\Rightarrow$  (add n Z  $\equiv$  n) =
```

```
  fun n  $\rightarrow$ 
```

```
    match n with
```

```
      | Z       $\rightarrow$  {}
```

```
      | S[k]  $\rightarrow$  addNZ k; {}
```

```
val rec addNSM : (n:N)  $\Rightarrow$  (m:N)  $\Rightarrow$  (add n S[m]  $\equiv$  S[add n m]) =
```

```
  fun n m  $\rightarrow$ 
```

```
    match n with
```

```
      | Z       $\rightarrow$  {}
```

```
      | S[k]  $\rightarrow$  addNSM k m; {}
```

MIXING PROOFS AND PROGRAMS

MIXING PROOFS AND PROGRAMS

```
val rec addComm : (n:N)  $\Rightarrow$  (m:N)  $\Rightarrow$  (add n m  $\equiv$  add m n) =  
  fun n m  $\rightarrow$   
    match n with  
    | Z       $\rightarrow$  addNZ m; {}  
    | S[k]    $\rightarrow$  addComm k m; addNSM m; {}
```

MIXING PROOFS AND PROGRAMS

```
val rec addComm : (n:N)  $\Rightarrow$  (m:N)  $\Rightarrow$  (add n m  $\equiv$  add m n) =  
  fun n m  $\rightarrow$   
    match n with  
      | Z       $\rightarrow$  addNZ m; {}  
      | S[k]  $\rightarrow$  addComm k m; addNSM m; {}  
  
val add : (n:N)  $\Rightarrow$  (m:N)  $\Rightarrow$  N | (add n m  $\equiv$  add m n) =  
  fun n m  $\rightarrow$   
    addComm n m; add n m
```

MIXING PROOFS AND PROGRAMS

```
val rec addComm : (n:N)  $\Rightarrow$  (m:N)  $\Rightarrow$  (add n m  $\equiv$  add m n) =  
  fun n m  $\rightarrow$   
    match n with  
    | Z       $\rightarrow$  addNZ m; {}  
    | S[k]    $\rightarrow$  addComm k m; addNSM m; {}
```

```
val add : (n:N)  $\Rightarrow$  (m:N)  $\Rightarrow$  N | (add n m  $\equiv$  add m n) =  
  fun n m  $\rightarrow$   
    addComm n m; add n m
```

```
val add' : N  $\Rightarrow$  N  $\Rightarrow$  N = add
```

CALL-BY-VALUE KRIVINE MACHINE

$$v, w ::= x \mid \lambda x. t \mid \{(l_i = v_i)_{i \in I}\} \mid C_k[v] \mid \square$$

$$t, u ::= a \mid v \mid t u \mid \mu \alpha. t \mid [\pi]t \mid v.l_k \mid [v] (C_i[x_i] \rightarrow t_i)_{i \in I} \mid F_{v,t} \mid R_{v,t} \mid \delta_{v,w}$$

$$\pi, \rho ::= \alpha \mid \varepsilon \mid v.\pi \mid [t]\pi$$

$$p, q ::= t * \pi$$

EVALUATION IN THE MACHINE (1/2)

$$t \ u * \pi > u * [t] \pi$$

$$v * [t] \pi > t * v . \pi$$

$$\lambda x . t * v . \pi > t[x := v] * \pi$$

$$\mu \alpha . t * \pi > t[\alpha := \pi] * \pi$$

$$[\pi] t * \xi > t * \pi$$

$$\{(l_i = v_i)_{i \in I}\} . l_k * \pi > v_k * \pi \quad (k \in I)$$

$$[C_k[v] \mid (C_i[x_i] \rightarrow t_i)_{i \in I}] * \pi > t_k[x_k := v] * \pi \quad (k \in I)$$

EVALUATION IN THE MACHINE (2/2)

$$\Box * v . \pi > \Box * \pi$$

$$\Box . l_i * \pi > \Box * \pi$$

$$[\Box \mid (C_i[x_i] \rightarrow t_i)_{i \in I}] * \pi > \Box * \pi$$

$$F_{\lambda x . u, t} * \pi > t * \pi$$

$$R_{\{(l_i = v_i)_{i \in I}\}, t} * \pi > t * \pi$$

EXAMPLES

$$\begin{aligned}
 \text{not } C_1[\{\}] * \varepsilon &= (\lambda x. [x \mid C_1[y] \rightarrow C_0[\{\}] \mid C_0[y] \rightarrow C_1[\{\}]]) C_1[\{\}] * \varepsilon \\
 &> C_1[\{\}] * [\lambda x. [x \mid C_1[y] \rightarrow C_0[\{\}] \mid C_0[y] \rightarrow C_1[\{\}]] \varepsilon \\
 &> \lambda x. [x \mid C_1[y] \rightarrow C_0[\{\}] \mid C_0[y] \rightarrow C_1[\{\}]] * C_1[\{\}] . \varepsilon \\
 &> [C_1[\{\}] \mid C_1[y] \rightarrow C_0[\{\}] \mid C_0[y] \rightarrow C_1[\{\}]] * \varepsilon \\
 &> C_0[\{\}] * \varepsilon
 \end{aligned}$$

$$\begin{aligned}
 \Omega * \varepsilon &= (\lambda x. x \ x) (\lambda x. x \ x) * \varepsilon \\
 &> \lambda x. x \ x * [\lambda x. x \ x] \varepsilon \\
 &> \lambda x. x \ x * \lambda x. x \ x . \varepsilon \\
 &> (\lambda x. x \ x) (\lambda x. x \ x) * \varepsilon \\
 &> \dots
 \end{aligned}$$

OBSERVATIONAL EQUIVALENCE OVER **P**ROGRAMS

OBSERVATIONAL EQUIVALENCE OVER PROGRAMS

It is easy to quantify over evaluation contexts (i.e. stacks).

OBSERVATIONAL EQUIVALENCE OVER PROGRAMS

It is easy to quantify over evaluation contexts (i.e. stacks).

We define $p \Downarrow$ as $\exists v, p \succ^* v * \epsilon$.

OBSERVATIONAL EQUIVALENCE OVER PROGRAMS

It is easy to quantify over evaluation contexts (i.e. stacks).

We define $p \Downarrow$ as $\exists v, p \succ^* v * \varepsilon$.

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

OBSERVATIONAL EQUIVALENCE OVER PROGRAMS

It is easy to quantify over evaluation contexts (i.e. stacks).

We define $p \Downarrow$ as $\exists v, p \succ^* v * \varepsilon$.

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

We quantify over substitutions to handle free variables.

EXAMPLE OF DERIVABLE EQUIVALENCES

EXAMPLE OF DERIVABLE EQUIVALENCES

For all x, v, t we have $(\lambda x.t) v \equiv t[x := v]$.

EXAMPLE OF DERIVABLE EQUIVALENCES

For all x, v, t we have $(\lambda x.t) v \equiv t[x := v]$.

$$\begin{aligned} ((\lambda x.t) v)\rho * \pi &= (\lambda x.t\rho) v\rho * \pi \\ &> v\rho * [\lambda x.t\rho]\pi \\ &> \lambda x.t\rho * v\rho . \pi \\ &> t\rho[x := v\rho] * \pi \\ &= (t[x := v])\rho * \pi \end{aligned}$$

MORE EQUIVALENCES: CANONICAL VALUES

$$x \equiv v \Leftrightarrow v = x$$

$$\square \equiv v \Leftrightarrow v = \square$$

$$C_k[v_k] \equiv v \Leftrightarrow v = C_k[w_k] \text{ and } v_k \equiv w_k$$

$$\{(l_i = v_i)_{i \in I}\} \equiv v \Leftrightarrow v = \{(l_i = w_i)_{i \in I}\} \text{ and } \forall i \in I, v_i \equiv w_i$$

$$\lambda x. t \equiv v \Leftrightarrow v = \lambda y. u \text{ and } t \equiv u[y := x]$$

VALUE INTERPRETATION OF TYPES

A type A is interpreted as a set of values $\llbracket A \rrbracket$.

We require $\llbracket A \rrbracket$ to be closed under $(\equiv)$.

We require $\square \in \llbracket A \rrbracket$.

We have $\llbracket A \rrbracket \in \{\{\square\} \subseteq \Phi \subseteq \Lambda_v \mid v \in \Phi \wedge w \equiv v \Rightarrow w \in \Phi\}$.

(Λ_v is the set of all the values.)

VALUE INTERPRETATION OF PURE TYPES

$$\llbracket \{(l_i : A_i)_{i \in I}\} \rrbracket = \{ \{(l_i = v_i)_{i \in I}\} \mid \forall i \in I, v_i \in \llbracket A_i \rrbracket \} \cup \{\square\}$$

$$\llbracket [(C_i : A_i)_{i \in I}] \rrbracket = \cup_{i \in I} \{C_i[v] \mid v \in \llbracket A_i \rrbracket\} \cup \{\square\}$$

$$\llbracket \forall X. A \rrbracket = \cap_{\Phi} \llbracket A[X := \Phi] \rrbracket$$

$$\llbracket \exists X. A \rrbracket = \cup_{\Phi} \llbracket A[X := \Phi] \rrbracket$$

$$\llbracket \forall a. A \rrbracket = \cap_{t \in \Lambda} \llbracket A[a := t] \rrbracket$$

$$\llbracket \exists a. A \rrbracket = \cup_{t \in \Lambda} \llbracket A[a := t] \rrbracket$$

FUNCTION TYPE AND TERMS

FUNCTION TYPE AND TERMS

$$\llbracket A \Rightarrow B \rrbracket = \{\lambda x. w \mid \forall v \in \llbracket A \rrbracket, w[x := v] \in \llbracket B \rrbracket\} \cup \{\square\}$$

FUNCTION TYPE AND TERMS

$$\llbracket A \Rightarrow B \rrbracket = \{\lambda x. w \mid \forall v \in \llbracket A \rrbracket, w[x := v] \in \llbracket B \rrbracket\} \cup \{\square\}$$

What about programs that actually compute something?

FUNCTION TYPE AND TERMS

$$\llbracket A \Rightarrow B \rrbracket = \{\lambda x. w \mid \forall v \in \llbracket A \rrbracket, w[x := v] \in \llbracket B \rrbracket\} \cup \{\square\}$$

What about programs that actually compute something?

We define a completion operation $\llbracket A \rrbracket \mapsto \llbracket A \rrbracket^{\perp\perp}$.

FUNCTION TYPE AND TERMS

$$\llbracket A \Rightarrow B \rrbracket = \{\lambda x. w \mid \forall v \in \llbracket A \rrbracket, w[x := v] \in \llbracket B \rrbracket\} \cup \{\square\}$$

What about programs that actually compute something?

We define a completion operation $\llbracket A \rrbracket \mapsto \llbracket A \rrbracket^{\perp\perp}$.

The set $\llbracket A \rrbracket^{\perp\perp}$ contains terms “behaving” as values of $\llbracket A \rrbracket$.

FUNCTION TYPE AND TERMS

$$\llbracket A \Rightarrow B \rrbracket = \{\lambda x. w \mid \forall v \in \llbracket A \rrbracket, w[x := v] \in \llbracket B \rrbracket\} \cup \{\square\}$$

What about programs that actually compute something?

We define a completion operation $\llbracket A \rrbracket \mapsto \llbracket A \rrbracket^{\perp\perp}$.

The set $\llbracket A \rrbracket^{\perp\perp}$ contains terms “behaving” as values of $\llbracket A \rrbracket$.

We can then take $\llbracket A \Rightarrow B \rrbracket = \{\lambda x. t \mid \forall v \in \llbracket A \rrbracket, t[x := v] \in \llbracket B \rrbracket^{\perp\perp}\} \cup \{\square\}$

POLE AND ORTHOGONALITY

POLE AND ORTHOGONALITY

The definition of $\llbracket A \rrbracket^{\mathbb{A}}$ is parametrised by a set $\mathbb{A} \subseteq \Lambda \times \Pi$.

POLE AND ORTHOGONALITY

The definition of $\llbracket A \rrbracket^{\perp\perp}$ is parametrised by a set $\perp \subseteq \Lambda \times \Pi$.

Intuitively, $\perp$ is a set of processes that “behave well”.

POLE AND ORTHOGONALITY

The definition of $\llbracket A \rrbracket^{\perp\perp}$ is parametrised by a set $\perp \subseteq \Lambda \times \Pi$.

Intuitively, $\perp$ is a set of processes that “behave well”.

The set $\perp = \{p \in \Lambda \times \Pi \mid \exists v \in \Lambda_i, p \succ^* v * \varepsilon\}$ is a good choice.

POLE AND ORTHOGONALITY

The definition of $\llbracket A \rrbracket^{\perp\perp}$ is parametrised by a set $\perp \subseteq \Lambda \times \Pi$.

Intuitively, $\perp$ is a set of processes that “behave well”.

The set $\perp = \{p \in \Lambda \times \Pi \mid \exists v \in \Lambda_l, p \succ^* v * \varepsilon\}$ is a good choice.

$$\llbracket A \rrbracket \in \{\{\Box\} \subseteq \Phi \subseteq \Lambda_l \mid v \in \Phi \wedge v \equiv w \Rightarrow w \in \Phi\}$$

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

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

TYPING JUDGMENTS AND ADEQUACY

TYPING JUDGMENTS AND ADEQUACY

There are two forms of judgments: $\Xi \vdash_{\text{val}} v : A$ and $\Xi \vdash t : A$.

TYPING JUDGMENTS AND ADEQUACY

There are two forms of judgments: $\Xi \vdash_{\text{val}} v : A$ and $\Xi \vdash t : A$.

The context Ξ contains only equivalences of the form $u_1 \equiv u_2$.

TYPING JUDGMENTS AND ADEQUACY

There are two forms of judgments: $\Xi \vdash_{\text{val}} v : A$ and $\Xi \vdash t : A$.

The context Ξ contains only equivalences of the form $u_1 \equiv u_2$.

Everything is closed (choice operator / witness presentation).

TYPING JUDGMENTS AND ADEQUACY

There are two forms of judgments: $\Xi \vdash_{\text{val}} v : A$ and $\Xi \vdash t : A$.

The context Ξ contains only equivalences of the form $u_1 \equiv u_2$.

Everything is closed (choice operator / witness presentation).

Adequacy for terms: if $\Xi \vdash t : A$ is derivable and Ξ is valid then $\llbracket t \rrbracket \in \llbracket A \rrbracket^{\perp\perp}$.

TYPING JUDGMENTS AND ADEQUACY

There are two forms of judgments: $\Xi \vdash_{\text{val}} v : A$ and $\Xi \vdash t : A$.

The context Ξ contains only equivalences of the form $u_1 \equiv u_2$.

Everything is closed (choice operator / witness presentation).

Adequacy for terms: if $\Xi \vdash t : A$ is derivable and Ξ is valid then $\llbracket t \rrbracket \in \llbracket A \rrbracket^{\perp\perp}$.

Adequacy for values: if $\Xi \vdash_{\text{val}} v : A$ is derivable and Ξ is valid then $\llbracket v \rrbracket \in \llbracket A \rrbracket$.

TYPING JUDGMENTS AND ADEQUACY

There are two forms of judgments: $\Xi \vdash_{\text{val}} v : A$ and $\Xi \vdash t : A$.

The context Ξ contains only equivalences of the form $u_1 \equiv u_2$.

Everything is closed (choice operator / witness presentation).

Adequacy for terms: if $\Xi \vdash t : A$ is derivable and Ξ is valid then $\llbracket t \rrbracket \in \llbracket A \rrbracket^{\perp\perp}$.

Adequacy for values: if $\Xi \vdash_{\text{val}} v : A$ is derivable and Ξ is valid then $\llbracket v \rrbracket \in \llbracket A \rrbracket$.

Since $\llbracket A \rrbracket \subseteq \llbracket A \rrbracket^{\perp\perp}$ we have the rule
$$\frac{\Xi \vdash_{\text{val}} v : A}{\Xi \vdash v : A} \uparrow.$$

RATHER USUAL TYPING RULES

RATHER USUAL TYPING RULES

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

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

$$\frac{}{\Xi \vdash_{\text{val}} \varepsilon_{x \in A}(t \notin B) : A} \text{Ax}$$

RATHER USUAL TYPING RULES

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

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

$$\frac{}{\Xi \vdash_{\text{val}} \varepsilon_{x \in A}(t \notin B) : A} \text{Ax}$$

$$\frac{(\Xi \vdash_{\text{val}} v_i : A_i)_{i \in I}}{\Xi \vdash_{\text{val}} \{(l_i = v_i)_{i \in I}\} : \{(l_i : A_i)_{i \in I}\}} \times_i$$

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

RATHER USUAL TYPING RULES

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

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

$$\frac{}{\Xi \vdash_{\text{val}} \varepsilon_{x \in A}(t \notin B) : A} \text{Ax}$$

$$\frac{(\Xi \vdash_{\text{val}} v_i : A_i)_{i \in I}}{\Xi \vdash_{\text{val}} \{(l_i = v_i)_{i \in I}\} : \{(l_i : A_i)_{i \in I}\}} \times_i$$

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

$$\frac{\Xi \vdash_{\text{val}} v : A[X := \varepsilon_X(v \notin A)]}{\Xi \vdash_{\text{val}} v : \forall X. A} \forall_i$$

$$\frac{\Xi \vdash t : \forall X. A}{\Xi \vdash t : A[X := B]} \forall_e$$

EQUIVALENCE TYPES

EQUIVALENCE TYPES

$$\llbracket A \upharpoonright u_1 \equiv u_2 \rrbracket = \{v \in \llbracket A \rrbracket \mid u_1 \equiv u_2\} \cup \{\Box\}$$

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

EQUIVALENCE TYPES

$$\llbracket A \upharpoonright u_1 \equiv u_2 \rrbracket = \{v \in \llbracket A \rrbracket \mid u_1 \equiv u_2\} \cup \{\Box\}$$

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

$$\frac{\Xi \vdash t : A \quad \Xi \vdash u_1 \equiv u_2}{\Xi \vdash t : A \upharpoonright u_1 \equiv u_2} \upharpoonright_i$$

$$\frac{\Xi, u_1 \equiv u_2 \vdash_{\text{val}} \varepsilon_{x \in A} (t \notin B) : C}{\Xi \vdash_{\text{val}} \varepsilon_{x \in A \upharpoonright u_1 \equiv u_2} (t \notin B) : C} \upharpoonright_e$$

SINGLETON AND TYPED QUANTIFICATION

SINGLETON AND TYPED QUANTIFICATION

$$\llbracket t \in A \rrbracket = \{v \in \llbracket A \rrbracket \mid t \equiv v\} \cup \{\square\}$$

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

SINGLETON AND TYPED QUANTIFICATION

$$\llbracket t \in A \rrbracket = \{v \in \llbracket A \rrbracket \mid t \equiv v\} \cup \{\square\}$$

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

$$\frac{\Xi \vdash_{\text{val}} v : A}{\Xi \vdash_{\text{val}} v : v \in A} \epsilon_i$$

$$\frac{\Xi, \varepsilon_{x \in A}(t \notin B) \equiv u \vdash \varepsilon_{x \in A}(t \notin B) : C}{\Xi \vdash \varepsilon_{x \in (u \in A)}(t \notin B) : C} \epsilon_e$$

SINGLETON AND TYPED QUANTIFICATION

$$\llbracket t \in A \rrbracket = \{v \in \llbracket A \rrbracket \mid t \equiv v\} \cup \{\square\}$$

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

$$\frac{\Xi \vdash_{\text{val}} v : A}{\Xi \vdash_{\text{val}} v : v \in A} \epsilon_i$$

$$\frac{\Xi, \varepsilon_{x \in A}(t \notin B) \equiv u \vdash \varepsilon_{x \in A}(t \notin B) : C}{\Xi \vdash \varepsilon_{x \in (u \in A)}(t \notin B) : C} \epsilon_e$$

$$\frac{\Xi \vdash t[x := \varepsilon_{x \in A}(t \notin B[a := x])] : B[a := \varepsilon_{x \in A}(t \notin B[a := x])]}{\Xi \vdash_{\text{val}} \lambda x. t : (a : A) \Rightarrow B}$$

$$\frac{\Xi \vdash t : (a : A) \Rightarrow B \quad \Xi \vdash_{\text{val}} v : A}{\Xi \vdash t \ v : B[a := v]}$$

EQUIVALENCE LEARNING AND CONGRUENCE

EQUIVALENCE LEARNING AND CONGRUENCE

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

EQUIVALENCE LEARNING AND CONGRUENCE

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

$$\frac{\Xi \vdash t : v \in A \Rightarrow B \quad \Xi \vdash_{\text{val}} v : A}{\Xi \vdash t \ v : B} \Rightarrow_{e, \varepsilon}$$

EQUIVALENCE LEARNING AND CONGRUENCE

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

$$\frac{\Xi \vdash t : v \in A \Rightarrow B \quad \Xi \vdash_{\text{val}} v : A}{\Xi \vdash t \ v : B} \Rightarrow_{e, \varepsilon}$$

$$\frac{\Xi \vdash t[a := u_1] : A[a := u_1] \quad \Xi \vdash u_1 \equiv u_2}{\Xi \vdash t[a := u_2] : A[a := u_2]} \equiv$$

SEMANTICAL VALUE RESTRICTION

SEMANTICAL VALUE RESTRICTION

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

$$\frac{\Xi \vdash_{\text{val}} v : A}{\Xi \vdash_{\text{val}} v : v \in A} \epsilon_i$$

$$\frac{\Xi \vdash t : A \quad \Xi \vdash v \equiv t}{\Xi \vdash t : t \in A} \epsilon_i$$

SEMANTICAL VALUE RESTRICTION

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

$$\frac{\Xi \vdash_{\text{val}} v : A}{\Xi \vdash_{\text{val}} v : v \in A} \epsilon_i$$

$$\frac{\Xi \vdash t : A \quad \Xi \vdash v \equiv t}{\Xi \vdash t : t \in A} \epsilon_i$$

Having the rule $\frac{\Xi \vdash v : A}{\Xi \vdash_{\text{val}} v : A} \downarrow$ is enough.

SEMANTICAL VALUE RESTRICTION

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

$$\frac{\Xi \vdash_{\text{val}} v : A}{\Xi \vdash_{\text{val}} v : v \in A} \epsilon_i$$

$$\frac{\Xi \vdash t : A \quad \Xi \vdash v \equiv t}{\Xi \vdash t : t \in A} \epsilon_i$$

Having the rule $\frac{\Xi \vdash v : A}{\Xi \vdash_{\text{val}} v : A} \downarrow$ is enough.

Relaxed rules can be derived using ($\downarrow$), ($\uparrow$) and ($\equiv$).

THE NEW INSTRUCTION TRICK

THE NEW INSTRUCTION TRICK

The property $\llbracket A \rrbracket^{\perp\perp} \cap \Lambda_i \subseteq \llbracket A \rrbracket$ is not true in every realizability model.

THE NEW INSTRUCTION TRICK

The property $\llbracket A \rrbracket^{\perp\perp} \cap \Lambda_i \subseteq \llbracket A \rrbracket$ is not true in every realizability model.

To obtain it we extend the system with a new term constructor $\delta_{v,w}$
with the rule $\delta_{v,w} * \pi > v * \pi$ when $v \not\equiv w$.

THE NEW INSTRUCTION TRICK

The property $\llbracket A \rrbracket^{\perp\perp} \cap \Lambda_i \subseteq \llbracket A \rrbracket$ is not true in every realizability model.

To obtain it we extend the system with a new term constructor $\delta_{v,w}$
with the rule $\delta_{v,w} * \pi > v * \pi$ when $v \neq w$.

Idea of the proof:

- suppose $v \notin \llbracket A \rrbracket$ and show $v \notin \llbracket A \rrbracket^{\perp\perp}$,
- we need to find π such that $v * \pi \notin \perp$ and $\forall w \in \llbracket A \rrbracket, w * \pi \in \perp$,
- we can take $\pi = [\lambda x. \delta_{x,v}] \varepsilon$,
- $v * [\lambda x. \delta_{x,v}] \varepsilon > \lambda x. \delta_{x,v} * v . \varepsilon > \delta_{v,v} * \varepsilon$,
- $w * [\lambda x. \delta_{x,v}] \varepsilon > \lambda x. \delta_{x,v} * w . \varepsilon > \delta_{w,v} * \varepsilon > w * \varepsilon$.

STRATIFIED REDUCTION AND EQUIVALENCE

STRATIFIED REDUCTION AND EQUIVALENCE

The definitions of $(>)$ and $(\equiv)$ are **circular**.

STRATIFIED REDUCTION AND EQUIVALENCE

The definitions of $(>)$ and $(\equiv)$ are **circular**.

We need to rely on a stratified construction of the two relations.

$$(\rightarrow_i) = (>) \cup \{(\delta_{v,w} * \pi, v * \pi) \mid \exists j < i, v \not\equiv_j w\}$$

$$(\cong_i) = \{(t, u) \mid \forall j \leq i, \forall \pi \in \Pi, \forall \rho, t\rho * \pi \Downarrow_j \Leftrightarrow u\rho * \pi \Downarrow_j\}$$

STRATIFIED REDUCTION AND EQUIVALENCE

The definitions of $(>)$ and $(\equiv)$ are **circular**.

We need to rely on a stratified construction of the two relations.

$$(\rightarrow_i) = (>) \cup \{(\delta_{v,w} * \pi, v * \pi) \mid \exists j < i, v \not\equiv_j w\}$$

$$(\cong_i) = \{(t, u) \mid \forall j \leq i, \forall \pi \in \Pi, \forall \rho, t\rho * \pi \Downarrow_j \Leftrightarrow u\rho * \pi \Downarrow_j\}$$

We then take $(\rightarrow) = \bigcup_{i \in \mathbb{N}} (\rightarrow_i)$ and $(\cong) = \bigcap_{i \in \mathbb{N}} (\cong_i)$.

COMPATIBLE EQUIVALENCE

$$(\cong) = \{(t, u) \mid \forall i \in \mathbb{N}, \forall \pi \in \Pi, \forall \rho, t\rho * \pi \Downarrow_i \Leftrightarrow u\rho * \pi \Downarrow_i\}$$

$$(\rightarrow) = (>) \cup \{(\delta_{v,w} * \pi, v * \pi) \mid v \not\cong w\}$$

COMPATIBLE EQUIVALENCE

$$(\cong) = \{(t, u) \mid \forall i \in \mathbb{N}, \forall \pi \in \Pi, \forall \rho, t\rho * \pi \Downarrow_i \Leftrightarrow u\rho * \pi \Downarrow_i\}$$

$$(\rightarrow) = (>) \cup \{(\delta_{v,w} * \pi, v * \pi) \mid v \not\cong w\}$$

The relation $(\cong)$ is “compatible” with $(\equiv)$.

COMPATIBLE EQUIVALENCE

$$\begin{aligned}(\cong) &= \{(t, u) \mid \forall i \in \mathbb{N}, \forall \pi \in \Pi, \forall \rho, t\rho * \pi \Downarrow_i \Leftrightarrow u\rho * \pi \Downarrow_i\} \\(\rightarrow) &= (>) \cup \{(\delta_{v,w} * \pi, v * \pi) \mid v \not\cong w\}\end{aligned}$$

The relation $(\cong)$ is “compatible” with $(\equiv)$.

In particular we have $(\cong) \subseteq (\equiv)$.

COMPATIBLE EQUIVALENCE

$$\begin{aligned}(\cong) &= \{(t, u) \mid \forall i \in \mathbb{N}, \forall \pi \in \Pi, \forall \rho, t\rho * \pi \Downarrow_i \Leftrightarrow u\rho * \pi \Downarrow_i\} \\(\rightarrow) &= (>) \cup \{(\delta_{v,w} * \pi, v * \pi) \mid v \not\cong w\}\end{aligned}$$

The relation $(\cong)$ is “compatible” with $(\equiv)$.

In particular we have $(\cong) \subseteq (\equiv)$.

If for all π there is p such that $t * \pi >^* p$ and $u * \pi >^* p$ then $t \cong u$.

WORK IN PROGRESS AND FUTURE WORK

WORK IN PROGRESS AND FUTURE WORK

Implementation of the system (in progress).
Inductive and coinductive types (in progress).
Recursion, termination checking (in progress).

WORK IN PROGRESS AND FUTURE WORK

Implementation of the system (in progress).
Inductive and coinductive types (in progress).
Recursion, termination checking (in progress).

Compile PML programs (future work).
Mixing terminating / non-terminating programs (future work).

WORK IN PROGRESS AND FUTURE WORK

Implementation of the system (in progress).
Inductive and coinductive types (in progress).
Recursion, termination checking (in progress).

PhD thesis (coming soon).

Compile PML programs (future work).
Mixing terminating / non-terminating programs (future work).

Fin.