Realizability semantics for the $\lambda\mu$-calculus

Karim Nour

Université Savoie Mont Blanc - LAMA - LIMD

Joint work with Péter Battyányi

GT Scalp - Orléans - 27 au 29 novembre 2023

Outline

Curry-Howard isomorphism

- The Curry-Howard isomorphism can also be extended to the case of classical logic (Felleisen, Griffin, . . .).
- Various systems have been introduced to account for this correspondence :
  - λC-calculus of Krivine,
  - $\lambda\mu$-calculus of Parigot,
  - λ_Δ-calculus of Rehof and Sorensen,
  - λ^{Sym}-calculus of Barbanera-Berardi,
  - $\overline{\lambda}\mu\tilde{\mu}$-calculus of Curien-Herbelin.
- Each system has advantages and disadvantages.

The $\lambda\mu$-calculus

- Parigot introduced the $\lambda\mu$-calculus in 1992 to capture the algorithmic content of classical logic proofs.
- His $\lambda\mu$-calculus has very good properties :
  simple syntax, confluence, subject reduction, strong normalization, . . .
- The $\lambda\mu$-calculus has some small shortcomings :
  strict syntax, abstract machine (de Groote),
  separation property or Böhm's theorem (Py & Saurin),
  representation of data types (Parigot & Nour).
- Hence we adopt de Groote's syntax.

Outline

1. Introduction
2. The $\lambda\mu$-calculus
   - Definitions
   - Properties
3. Realizability semantics
   - Introduction
   - Definitions
   - Results
4. Future work

Types and terms

Definition (Types)

Let $\mathbb{V} = \{X, Y, Z, \ldots\}$. The set of types is given by :

$$\mathbb{T} ::= \perp \mid \mathbb{V} \mid \mathbb{T} \to \mathbb{T}$$

Definition (Terms)

Let $\mathcal{V} = \{x, y, z, \ldots\}$ and $\mathcal{A} = \{\alpha, \beta, \gamma, \ldots\}$.
The definition of the $\lambda\mu$-terms is given by :

$$\mathcal{T} ::= \mathcal{V} \mid \lambda\mathcal{V}.\mathcal{T} \mid (\mathcal{T})\,\mathcal{T} \mid [\mathcal{A}]\mathcal{T} \mid \mu\mathcal{A}.\,\mathcal{T}$$

Typing relation

Definition

A context is a set of typing assumptions

$$\Gamma = x_1 : A_1, \ldots, x_n : A_n \qquad \Delta = \alpha_1 : B_1, \ldots, \alpha_m : B_m$$

where $x_1, \ldots, x_n$ *are* λ*-variables,* $\alpha_1, \ldots, \alpha_m$ *are* μ*-variables and* $A_1, \ldots, A_n, B_1, \ldots, B_m$ *are types.*

Definition

The typing relation

$$\Gamma \vdash M : T \,,\, \Delta$$

indicates that M *is a* $\lambda\mu$*-term of type* T *in context* Γ, Δ*.*

Typing rules

$$\frac{}{\Gamma , x : A \vdash x : A , \triangle} \; ax$$

$$\frac{\Gamma , x : A \vdash M : B , \triangle}{\Gamma \vdash \lambda x.M : A \to B , \triangle} \; \to_i$$

$$\frac{\Gamma \vdash M : A \to B , \triangle \qquad \Gamma \vdash N : A , \triangle}{\Gamma \vdash (M)N : B , \triangle} \; \to_e$$

Typing rules

$$\frac{\Gamma \vdash M : A\,,\ \alpha : A\,,\ \triangle}{\Gamma \vdash [\alpha]M : \bot\,,\ \alpha : A\,,\ \triangle}\ \bot_i$$

$$\frac{\Gamma \vdash M : \bot\,,\ \alpha : B\,,\ \triangle}{\Gamma \vdash \mu\alpha.M : B\,,\ \triangle}\ \bot_e$$

Reduction rules

Definition

$$(\lambda x.M)N \quad \triangleright_\beta \quad M[x := N]$$

$$(\mu\alpha.M)N \quad \triangleright_\mu \quad \mu\alpha.M\Big[[\alpha]U := [\alpha](U)N\Big]$$

$$[\alpha]\mu\beta.M \quad \triangleright_\rho \quad M[\beta := \alpha]$$

$$\mu\alpha.[\alpha]M \quad \triangleright_\theta \quad M \qquad if\ \alpha \not\in FV(M)$$

$$\mu\alpha.\mu\beta.M \quad \triangleright_\varepsilon \quad \mu\alpha.M_\beta$$

Typed reduction rules

Definition

$$(\lambda x^A.M^B)N^A \quad \triangleright_\beta \quad M^B[x := N]$$

$$(\mu\alpha^{A\to B}.M^\perp)N^A \quad \triangleright_\mu \quad \mu\alpha^B.M^\perp\left[[\alpha^{A\to B}]U := [\alpha^B](U)N\right]$$

$$[\alpha^A]\mu\beta^A.M^\perp \quad \triangleright_\rho \quad M^\perp[\beta := \alpha]$$

$$\mu\alpha^A.[\alpha^A]M^A \quad \triangleright_\theta \quad M^A \quad \textit{if } \alpha \notin FV(M)$$

$$\mu\alpha^A.\mu\beta^\perp.M^\perp \quad \triangleright_\varepsilon \quad \mu\alpha^A.M^\perp_\beta$$

Normalization

Definition

- *We write $M \triangleright M'$ if M reduces to M' in one step of reduction. We write $M \triangleright^* M'$ if $M \triangleright M_1 \triangleright M_2 \triangleright \cdots \triangleright M_k = M'$.*
- *If a $\lambda\mu$-term contains no redexes, then it is said to be normal (or in normal form).*
- *A $\lambda\mu$-term M is weakly normalizable if there exists a $\lambda\mu$-term N in normal form such that $M \triangleright^* N$.*
- *A $\lambda\mu$-term M is strongly normalizable, if there exists no infinite reduction path starting from M. That is, any possible sequence of reductions eventually leads to a normal form.*

Outline

Good properties

Theorem (Py 1998)

The reduction $\triangleright^*$ is conflente.

Theorem

If $\Gamma \vdash M : T, \triangle$ and $M \triangleright^* N$, then $\Gamma \vdash N : T, \triangle$.

Theorem (Parigot 1997)

If $\Gamma \vdash M : T, \triangle$, then M is strongly normalizable.

Proof :

- de Groote (1998) : Reducibility candidates.
- David & Nour (2003) : Arithmetical proof.

Church's numerals

Definition

$$\forall n \in \mathbb{N}, \quad \underline{n} \;=\; \lambda x.\lambda f.\overbrace{(f)\ldots(f)}^{n \text{ times}}\, x.$$

$$\mathcal{N} = X \to ((X \to X) \to X)$$

Theorem

1. *For all $n \in \mathbb{N}$, $\vdash \underline{n} : \mathcal{N}$.*
2. *If M is a λ-term and $\vdash M : \mathcal{N}$, then $\exists\, n \in \mathbb{N}$ such that $M \triangleright_\beta^* \underline{n}$.*
3. *If F is a λ-term and $\vdash F : \mathcal{N} \to \mathcal{N}$, then F defines a function on natural numbers.*

Problem and solutions

Remark

Let

$$M = \lambda x.\lambda f.\mu\alpha.[\alpha](f)\mu\beta.[\alpha]x.$$

Then M is normal and has type $\mathcal{N}$.

We need some tools to find the true value of this kind of terms (called classical natural numbers).

1. Algorithms : Parigot (1993) & Nour (1997)
2. Storage operators : Parigot (1993) & Nour (2000)
3. The reduction rule μ' : Parigot (1993)

Reduction μ'

$$(N)\mu\alpha.M \ \triangleright_{\mu'} \ \mu\alpha.M\Big[[\alpha]U := [\alpha](N)U\Big]$$

$$(N^{A\to B})\mu\alpha^{A}.M^{\perp} \ \triangleright_{\mu'} \ \mu\alpha^{B}.M^{\perp}\Big[[\alpha^{A}]U := [\alpha^{B}](N)U\Big]$$

Properties

Remark

The $\lambda\mu\mu'$-calculus is not confluent.

$(\mu\alpha.x)\mu\beta.y \triangleright_{\mu} \mu\alpha.x$ and $(\mu\alpha.x)\mu\beta.y \triangleright_{\mu'} \mu\beta.y$.

Theorem (BN 2022)

Let x, f be two different λ-variables.

If $\vdash M : \mathcal{N}$ and $((M)x)f \triangleright^{*} M' \in NF$, then $\exists\, n \in \mathbb{N}$, $M' = (f)^{n}x$.

What can we say about the normalization properties of :

- the untyped $\mu\mu'\rho\theta\varepsilon$-reduction ?
- the typed $\beta\mu\mu'\rho\theta\varepsilon$-reduction ?

The $\mu\mu'\rho\theta\varepsilon$-reduction is not SN but ...

Let $U = \mu\alpha.[\alpha][\alpha]x$, $V = \mu\beta.U$ and $M = (V)U$. We have :

$$M \ \triangleright_{\mu'} \ M_1 \ \triangleright_{\mu} \ M_2 \ \triangleright_{\rho} \ M_3 \ \triangleright_{\theta} \ M$$

Theorem (BN 2022)

The untyped $\mu\mu'\rho\theta\varepsilon$-reduction is WN.

Theorem (BN 2022)

The typed $\beta\mu\mu'\rho\theta\varepsilon$-reduction is WN.

$$M_0 \triangleright^*_{\mu\mu'\rho\varepsilon} M_1 \triangleright^*_{\beta} \triangleright^*_{\mu\mu'\rho\varepsilon} M_2 \triangleright^*_{\beta} \triangleright^*_{\mu\mu'\rho\varepsilon} \cdots \triangleright^*_{\beta} \triangleright^*_{\mu\mu'\rho\varepsilon} M_n \triangleright^*_{\theta} M_{n+1}$$

Outline

Idea

1. Associate a subset of terms with each type :

$$A \curvearrowleft |A| \subseteq \mathcal{T}$$

Have : $|A| \subseteq SN$ and $\vdash M : A \implies M \in |A|$.

2. Tait for simply typed λ-calculus (1967).
3. Girard for second order typed system $\mathcal{F}$ (1972).
4. Krivine's work (not just normalization results).
5. Difficulties for systems based on classical logic.

Parigot's method

1. Realize in another way the equality $\neg\neg A = A$.
2. Write $|A|$ as $|A|^{\perp} \rightsquigarrow \mathbf{T}$.
3. Problems :
   1. Some of the reductions are left out.
   2. Without the reduction μ'.
4. Difficulties to define a general semantics (for a completeness result).

Our goal

1. Define a fairly general semantics.
2. Consider all rules at the same time (no commutation lemmas).
3. Get several normalization results.
4. A method that applies to more reduction rules.

Ideas

1. Replacing the set SN with another $\mathbf{T}$ and search for the properties that must be satisfied.
2. The terms in $\mathbf{T}$ must be typable.
3. Interpreting the types in the set $\mathbf{T}$.
4. The interpretations must contain all the λ-variables.
5. The orthogonals must contain the empty sequence.
6. Modifying how the type constructor arrow is interpreted.
7. **We obtain a surprising result.**

Outline

Saturated set

Let $\mathbf{T} \subseteq \mathcal{T}_p$. We say that $\mathbf{T}$ is saturated if

(C1) : $\forall M \in \mathbf{T}, \forall x \in \mathcal{V}_\lambda, \lambda x.M \in \mathbf{T}$.

(C2) : $\forall M \in \mathbf{T}, \forall \alpha \in \mathcal{V}_\mu$, if $\mu\alpha.M \in \mathcal{T}_p$, then $\mu\alpha.M \in \mathbf{T}$.

(C3) : $\forall M \in \mathbf{T}, \forall \alpha \in \mathcal{V}_\mu$, if $[\alpha]M \in \mathcal{T}_p$, then $[\alpha]M \in \mathbf{T}$.

(C4) : $\forall n \geq 0, \forall N_1, \ldots, N_n \in \mathbf{T}, \forall x \in \mathcal{V}_\lambda$, if $(x)N_1 \ldots N_n \in \mathcal{T}_p$, then $(x)N_1 \ldots N_n \in \mathbf{T}$.

(C5) : $\forall M, N \in \mathcal{T}_p, \forall \bar{P} \in \mathcal{T}_p^{<\omega}$, if $N \in \mathbf{T}$, $(\lambda x.M)N\bar{P} \in \mathcal{T}_p$ and $(M[x := N])\bar{P} \in \mathbf{T}$, then $(\lambda x.M)N\bar{P} \in \mathbf{T}$.

(C6) : $\forall M \in \mathcal{T}_p, N \in \mathcal{T}_p^{<\omega}$, if $\bar{N} \in \mathbf{T}^{<\omega}$, $(\mu\alpha.M)\bar{N} \in \mathcal{T}_p$ and $\mu\alpha.M[[\alpha]U := [\alpha](U)\bar{N}] \in \mathbf{T}$, then $(\mu\alpha.M)\bar{N} \in \mathbf{T}$.

Operator $\rightsquigarrow$

Definition

Let $\mathcal{K}, \mathcal{L} \subseteq \mathbf{T}$, and $\mathcal{X} \subseteq \mathbf{T}^{<\omega}$.

1. $\mathcal{K} \rightsquigarrow \mathcal{L} = \{M \in \mathbf{T} : \forall N \in \mathcal{K},\ (M)N \in \mathcal{T}_p, \Rightarrow (M)N \in \mathcal{L}\}$.
2. $\mathcal{X} \rightsquigarrow \mathbf{T} = \{M \in \mathbf{T} \ / \ \forall \bar{N} \in \mathcal{X}, \forall \bar{P} \sqsubseteq \bar{N},\ (M)\bar{P} \in \mathcal{T}_p, \Rightarrow (M)\bar{P} \in \mathbf{T}\}$.

$\mathbf{T}$-saturated set

Let $\mathcal{S} \subseteq \mathbf{T}$. We call $\mathcal{S}$ $\mathbf{T}$-saturated if

(D1) : $\forall M, N \in \mathcal{T}_p, \forall \bar{P} \in \mathcal{T}_p^{<\omega}$, if $N \in \mathbf{T}$, $(\lambda x.M)N\bar{P} \in \mathcal{T}_p$ and $(M[x := N])\bar{P} \in \mathcal{S}$, then $(\lambda x.M)N\bar{P} \in \mathcal{S}$.

(D2) : $\forall n \geq 0, \forall N_1, \ldots, N_n \in \mathbf{T}, \forall x \in \mathcal{V}_\lambda$, if $(x)N_1 \ldots N_n \in \mathcal{T}_p$, then $(x)N_1 \ldots N_n \in \mathcal{S}$.

(D3) : $\exists \mathcal{X}_\mathcal{S} \subseteq \mathbf{T}^{<\omega}, \mathcal{S} = \mathcal{X}_\mathcal{S} \rightsquigarrow \mathbf{T}$.

Model

Definition

1. An $\mathbf{T}$-model $\mathcal{M}$ is defined by giving a sequence of $\mathbf{T}$-saturated sets $(\mathcal{S}_i)_{i\in I}$.
2. If $\mathcal{M} = (\mathcal{S}_i)_{i\in I}$ is a $\mathbf{T}$-model, we denote by $|\mathcal{M}|$ the smallest set containing the sets $\mathcal{S}_i$ and $\mathbf{T}$ and closed under the constructor $\leadsto$.

Lemma (BN 2023)

Let $\mathcal{M}$ be a $\mathbf{T}$-model. If $\mathcal{S} \in |\mathcal{M}|$, then $\mathcal{S}$ is a $\mathbf{T}$-saturated set.

Orthogonality

Definition

Let $\mathcal{M}$ be a $\mathbf{T}$-model, and $\mathcal{S} \in |\mathcal{M}|$. We write

$$\mathcal{S}^{\perp} = \left(\bigcup\{\mathcal{X} \subseteq \mathbf{T}^{<\omega} \ / \ \mathcal{S} = \mathcal{X} \leadsto \mathbf{T}\}\right) \cup \{\emptyset\}.$$

Lemma (BN 2023)

Let $\mathcal{M}$ be a $\mathbf{T}$-model, and $\mathcal{S} \in |\mathcal{M}|$. We have $\mathcal{S} = \mathcal{S}^{\perp} \leadsto \mathbf{T}$.

$\mathcal{M}$-interpretation

Definition

Let $\mathcal{M}$ be a $\mathbf{T}$-model. An $\mathcal{M}$-interpretation $\mathcal{I}$ is a function $X \mapsto \mathcal{I}(X)$ from the set of atomic types $\mathcal{V}_T$ to $|\mathcal{M}|$ which we extend for any formula as follows :

1. $\mathcal{I}(\perp) = \mathbf{T}$.
2. $\mathcal{I}(A \to B) = \mathcal{I}(A) \leadsto \mathcal{I}(B)$.

Outline

Correctness theorem

Theorem (BN 2023)

Let $\mathcal{M}$ *be a* $\mathbf{T}$*-model,* $\mathcal{I}$ *an* $\mathcal{M}$*-interpretation,*

$\Gamma = \{x_i : A_i\}_{1 \leq i \leq n}$, $\triangle = \{\alpha_j : B_j\}_{1 \leq j \leq m}$,

$M_i \in \mathcal{I}(A_i)$ *for all* $1 \leq i \leq n$,

$\bar{P}_j \sqsubseteq \bar{N}_j \in (\mathcal{I}(B_j))^{\perp}$ *for all* $1 \leq j \leq m$ *and*

$\sigma = [(x_i := M_i)_{1 \leq i \leq n}; (\alpha_j :=_r \bar{P}_j)_{1 \leq j \leq m}]$.

If $\Gamma \vdash M : A ; \Delta$ *and* $M\sigma \in \mathcal{T}_p$ *, then* $M\sigma \in \mathcal{I}(A)$.

Corollary (BN 2023)

$\mathcal{T}_p$ *is the unique saturated set.*

SN of $\beta\mu\rho\varepsilon\theta$-reduction

Theorem (BN 2023)

If $\Gamma \vdash M : A, \triangle$, *then* $M \in \mathcal{SN}_{\beta\mu\rho\varepsilon\theta}$.

Proof : Let $\mathbf{T} = \mathcal{SN}_{\beta\mu\rho\varepsilon\theta} \cap \mathcal{T}_p$.
We verify that $\mathbf{T}$ is saturated.
We only check **(C2)**.

WN of $\beta\mu\mu'\rho\varepsilon\theta$-reduction

Theorem (BN 2023)

If $\Gamma \vdash M : A, \triangle$*, then* $M \in \mathcal{WN}_{\beta\mu\mu'\rho\varepsilon\theta}$.

Proof : Let $\mathbf{T}' = \mathcal{WN}_{\beta\mu\mu'\rho\varepsilon\theta} \cap \mathcal{T}_p$.
We verify that $\mathbf{T}'$ is saturated.
We only check **(C4)**.

Future work

1. Study the system with other rules :

$$[\alpha][\beta]M \;\; \triangleright_{\delta} \;\; [\beta]M_{\alpha} \qquad (\beta \neq \alpha)$$

and

$$[\alpha][\alpha]M \;\; \triangleright_{\delta} \;\; M_{\alpha}$$

2. The second-order $\lambda\mu$-calculus has problems with the μ'-reduction. What can we do ?