A completeness result for the simply typed $\lambda\mu$-calculus

Khelifa SABER & Karim NOUR

Laboratoire de Mathématiques (LAMA)
Université de Savoie

29 novembre 2007

The semantical proofs of SN

Theorem

Every typed term is strongly normalizable

Idea : (W. W. Tait)
$\vdash t : A$, then $t \in |A|$ where $|A| \subseteq SN$

J.-Y. Girard : [System $\mathcal{F}$]
M. Parigot : [Second order $\lambda\mu$-calculus]

Adequation Lemma

- J.-L. Krivine : A generalized adequation lemma for the system $\mathcal{F} \Longrightarrow$ Characterization of the operational behaviour of some typed terms

Adequation Lemma

- J.-L. Krivine : A generalized adequation lemma for the system $\mathcal{F} \Longrightarrow$ Characterization of the operational behaviour of some typed terms

1. A general adequation lemma for the simply typed $\lambda\mu$-calculus ?

Adequation Lemma

- J.-L. Krivine : A generalized adequation lemma for the system $\mathcal{F} \Longrightarrow$ Characterization of the operational behaviour of some typed terms

1. A general adequation lemma for the simply typed $\lambda\mu$-calculus ?

2. A converse of this lemma (the completeness result) ?

Plan

1. The simply typed $\lambda\mu$-calculus
2. The realizability semantic
3. The completeness
4. Perspectives

The typing rules

$$\Gamma \vdash t : A \,;\, \Delta$$

$$\Gamma = \{x_i : A_i\}_{1 \leq i \leq n}$$

$$\Delta = \{a_j : B_j\}_{1 \leq j \leq m}$$

The typing rules

$$\frac{}{\Gamma \vdash x_i : A_i \ ; \Delta} ax \quad \text{for } 1 \leq i \leq n.$$

$$\frac{\Gamma, x : A \vdash t : B; \Delta}{\Gamma \vdash \lambda x.t : A \to B; \Delta} \to_i \qquad \frac{\Gamma \vdash u : A \to B; \Delta \quad \Gamma \vdash v : A; \Delta}{\Gamma \vdash (u\ v) : B; \Delta} \to_e$$

$$\frac{\Gamma \vdash t : \bot; \Delta, a : A}{\Gamma \vdash \mu a.t : A; \Delta} \mu \qquad \frac{\Gamma \vdash t : A; \Delta, a : A}{\Gamma \vdash (a\ t) : \bot; \Delta, a : A} \bot$$

Syntax and reduction rules

Definition (Syntax)

$\mathcal{X}$ (*resp* $\mathcal{A}$) *the set of the* λ*-variables* (μ*-variables*)

$$\mathcal{T} := \mathcal{X} \mid \lambda\mathcal{X}.\mathcal{T} \mid (\mathcal{T}\ \mathcal{T}) \mid \mu\mathcal{A}.\mathcal{T} \mid (\mathcal{A}\ \mathcal{T})$$

Syntax and reduction rules

Definition (Syntax)

$\mathcal{X}$ (resp $\mathcal{A}$) the set of the λ-variables (μ-variables)

$$\mathcal{T} := \mathcal{X} \mid \lambda\mathcal{X}.\mathcal{T} \mid (\mathcal{T}\ \mathcal{T}) \mid \mu\mathcal{A}.\mathcal{T} \mid (\mathcal{A}\ \mathcal{T})$$

Definition (Reduction rules)

- $(\lambda x.u\ v) \triangleright_\beta u[x := v]$
- $(\mu a.u\ v) \triangleright_\mu \mu a.u[a :=^* v]$
  where $u[a :=^* v]$ is obtained from u by replacing inductively each subterm in the form $(a\ w)$ in u by $(a\ (w\ v))$.

The main properties [M. Parigot]

Theorem (Subject reduction)

If $\Gamma \vdash t : A; \Delta$ *and* $t \triangleright^* t'$ *then* $\Gamma \vdash t' : A; \Delta$

Theorem (Strong normalization)

If $\Gamma \vdash t : A; \Delta$, *then* t *is strongly normalizable*

Theorem (Confluence)

If $t \triangleright^* t_1$ *and* $t \triangleright^* t_2$, *then there exists* t_3 *such that* $t_1 \triangleright^* t_3$ *and* $t_2 \triangleright^* t_3$

The semantic

Definition

- *Let $\mathcal{S}$ be a set of terms, $\mathcal{C}$ an infinite set of classical variables. $\mathcal{S}$ is said to be $\mathcal{C}$-saturated iff :*
  - *$\mathcal{S}$ is saturated by expansion : If $t \triangleright^* t'$ and $t' \in \mathcal{S}$, then $t \in \mathcal{S}$*
  - *For each term $t \in \mathcal{S}$ and $a \in \mathcal{C}$, then $(a\ t) \in \mathcal{S}$ and $\mu a.t \in \mathcal{S}$*

The semantic

Notation (Saurin's notation*)

- *We denote $\mathcal{T} \cup \mathcal{A}$ by $\mathcal{T}'$ and $\mathcal{T}'^{<\omega}$ the set of finite sequences of $\mathcal{T}'$.*
- *Let $\pi \in \mathcal{T}'^{<\omega}$*
  - *If $\pi = u\pi'$, then $(t\ \pi) = ((t\ u)\ \pi')$*
  - *Else $\pi = a\pi'$, and then $(t\ \pi) = ((a\ t)\ \pi')$*

* A. Saurin [2005] : [*Separation in $\lambda\mu$-calcul*]

The semantic

Definition

- *Let $\mathcal{K}$ and $\mathcal{L}$ be two sets of terms :*
  $\mathcal{K} \rightsquigarrow \mathcal{L} = \{t \ / \ \text{for each } u \in \mathcal{K}, (t\ u) \in \mathcal{L}\}$

The semantic

Definition

- *Let $\mathcal{K}$ and $\mathcal{L}$ be two sets of terms :*
  $\mathcal{K} \rightsquigarrow \mathcal{L} = \{t \ / \ \text{for each } u \in \mathcal{K}, (t\ u) \in \mathcal{L}\}$

- *Let $\mathcal{S}$ be a $\mathcal{C}$-saturated and $\{\mathcal{R}_j\}_{j\in J}$ subsets of terms such that $\mathcal{R}_j = \mathcal{X}_j \rightsquigarrow \mathcal{S}$ for some $\mathcal{X}_j \subseteq \mathcal{T}'^{<\omega}$*
  A model $\mathcal{M} = \langle \mathcal{C}, \mathcal{S}, \{\mathcal{R}_j\}_{j\in J}\rangle$ is the smallest set of subsets of terms containing $\mathcal{S}$, $\mathcal{R}_j$ and closed under the constructor $\rightsquigarrow$

The interpretations

Definition

- $I(\bot) = \mathcal{S}$
- $I(A \to B) = I(A) \rightsquigarrow I(B)$

The interpretations

Definition

- $I(\bot) = \mathcal{S}$
- $I(A \to B) = I(A) \rightsquigarrow I(B)$

- $|A|_{\mathcal{M}} = \bigcap\{I(A) \,/\, I \;\; an\ \mathcal{M}\text{- }interpretation\}$
- $|A| = \bigcap\{|A|_{\mathcal{M}} \,/\, \mathcal{M}\ a\ model\}$

The correction

Lemma (Correction)

$$\vdash t : A \quad \Rightarrow \quad t \in |A|$$

The correction

Lemma (Correction)

$$\vdash t : A \quad \Rightarrow \quad t \in |A|$$

Characterization of the computational behaviour of some closed typed terms through their types :

- $\vdash \mathbb{T} : \bot \longrightarrow X$ (*exit* in the *C* programming language)
- $\vdash \mathbb{L} : (\neg X \longrightarrow X) \longrightarrow X$ (*call/cc* in the *Scheme* functional programming language)

Closed terms of type $\bot\longrightarrow X$

Theorem

If $\vdash \mathbb{T} : \bot\longrightarrow X$, *then for any finite sequence of terms* $\bar{t} = t_1 \ldots t_n$ *we have :* $(\mathbb{T}\ \bar{t})\ \triangleright^*\ \underline{\mu}.t_1$

Proof : We prove this theorem for a finite sequence of λ-variables $x\bar{y}$

- Take $\mathcal{S} = \{t \,/\, t\ \triangleright^*\ \underline{\mu}.x\}$ and $R = \{\bar{y}\} \rightsquigarrow \mathcal{S}$
- The model $\mathcal{M} = \langle \mathcal{A}, \mathcal{S}, R \rangle$, $I(X) = R$
- $\mathbb{T} \in \mathcal{S} \rightsquigarrow (\{\bar{y}\} \rightsquigarrow \mathcal{S})$, then $(\mathbb{T}\, x) \in \{\bar{y}\} \rightsquigarrow \mathcal{S}$ therefore $((\mathbb{T}\, x)\, \bar{y}) \in \mathcal{S}$

The completeness ?

1. J. R. Hindley [1983] : *Completeness for simply typed λ-calculus.*
2. J. R. Hindley [1983] : *Completeness for a system with intersection types,* (saturated sets by $\beta\eta$- equivalence).
3. R. Labib-Sami [1986] : *Completeness for the strictly positif types of the system $\mathcal{F}$.*
4. K. Nour & S. Farkh [1998] : *Completeness for the $\forall$ positif types of the system $\mathcal{F}$,* (saturated sets by weak-head β-expansion).
5. K. Nour & S. Farkh [1998] : *Completeness for the good positif types of the system $\mathcal{AF}2$,* (saturated sets by $\beta\eta$-equivalence).
6. F. Kamareddine & K. Nour [2005] : *Completeness for a system with intersection types,* (saturated sets by weak-head β-expansion).
7. T. Coquand [2005] : *Completeness for the simply typed λ-calculus,* (Kripke model).

Construction of the completeness model

Theorem

$t \in |A| \quad \Rightarrow (t \triangleright^* t') \textit{ such that } \vdash t' : A$

Proof : $t \in |A|$, then $t \in |A|_{\mathbb{M}}$, hence $t \triangleright^* t'$ such that $\vdash t' : A$

Construction of the completeness model

Notation

- *Let* $\Omega = \{x_i \,/\, i \in \mathbb{N}\} \cup \{a_j \,/\, j \in \mathbb{N}\}$ *be an enumeration of an infinite sets of* λ *and* μ *variables*
- *Let* $\Omega_1 = \{A_i \,/\, i \in \mathbb{N}\}$ *be an enumeration of all types where each type comes an infinite times*
- *Let* $\Omega_2 = \{B_j \,/\, j \in \mathbb{N}\}$ *be an enumeration of all types where the type* $\perp$ *comes an infinite times*

Construction of the completeness model

Definition

- $\mathbb{G} = \{x_i : A_i \,/\, i \in \mathbb{N}\}$ *and* $\mathbb{D} = \{a_j : B_j \,/\, j \in \mathbb{N}\}$
- $\mathbb{C} = \{a_j \,/\, (a_j : \bot) \in \mathbb{D}\}$

Construction of the completeness model

Definition

- $\mathbb{G} = \{x_i : A_i \,/\, i \in \mathbb{N}\}$ *and* $\mathbb{D} = \{a_j : B_j \,/\, j \in \mathbb{N}\}$
- $\mathbb{C} = \{a_j \,/\, (a_j : \bot) \in \mathbb{D}\}$
- *Let* t *be a term such that* $Fv(t) \subset \Omega$, *the contexts* $\mathbb{G}_t$ *and* $\mathbb{D}_t$ *are the restrictions of* $\mathbb{G}$ *and* $\mathbb{D}$ *at the declarations containing the variables* $Fv(t)$
- $\mathbb{G} \vdash^* t : A; \mathbb{D}$ *means that :* $\exists\, u$ *such that* $(t \rhd^* u)$ *and* $\mathbb{G}_u \vdash u : A; \mathbb{D}_u$

Construction of the completeness model

Definition

- $\mathbb{G} = \{x_i : A_i \,/\, i \in \mathbb{N}\}$ *and* $\mathbb{D} = \{a_j : B_j \,/\, j \in \mathbb{N}\}$
- $\mathbb{C} = \{a_j \,/\, (a_j :\bot) \in \mathbb{D}\}$
- *Let* t *be a term such that* $Fv(t) \subset \Omega$, *the contexts* $\mathbb{G}_t$ *and* $\mathbb{D}_t$ *are the restrictions of* $\mathbb{G}$ *and* $\mathbb{D}$ *at the declarations containing the variables* $Fv(t)$
- $\mathbb{G} \vdash^* t : A; \mathbb{D}$ *means that :* $\exists\, u$ *such that* $(t \rhd^* u)$ *and* $\mathbb{G}_u \vdash u : A; \mathbb{D}_u$
- $\mathbb{S} = \{t \,/\, \mathbb{G} \vdash^* t :\bot; \mathbb{D}\}$
- $\mathbb{R}_X = \{t \,/\, \mathbb{G} \vdash^* t : X; \mathbb{D}\}$

Construction of the completeness model

Lemma

- $\mathbb{S}$ *is a* $\mathbb{C}$*-saturated set*
- *The sets* $\mathbb{R}_X$ *are saturated and* $\mathbb{R}_X = \{a_j \,/\, (a_j : X) \in \mathbb{D}\} \rightsquigarrow \mathbb{S}$
- $\mathbb{M} = \langle \mathbb{C}, \mathbb{S}, (\mathbb{R}_X)_{X \in \mathcal{P}} \rangle$ *is a model*

Construction of the completeness model

Lemma

- $\mathbb{S}$ *is a* $\mathbb{C}$*-saturated set*
- *The sets* $\mathbb{R}_X$ *are saturated and* $\mathbb{R}_X = \{a_j \,/\, (a_j : X) \in \mathbb{D}\} \rightsquigarrow \mathbb{S}$
- $\mathbb{M} = \langle \mathbb{C}, \mathbb{S}, (\mathbb{R}_X)_{X \in \mathcal{P}} \rangle$ *is a model*

Definition

- $\mathbb{I}(\bot) = \mathbb{S}$
- $\mathbb{I}(X) = \mathbb{R}_X$

The completeness

Lemma

Let A be a type and t a term :

1. *If $\mathbb{G} \vdash^* t : A ; \mathbb{D}$, then $t \in \mathbb{I}(A)$*
2. *If $t \in \mathbb{I}(A)$, then $\mathbb{G} \vdash^* t : A ; \mathbb{D}$*

The completeness

Lemma

Let A be a type and t a term :

1. *If $\mathbb{G} \vdash^* t : A ; \mathbb{D}$, then $t \in \mathbb{I}(A)$*
2. *If $t \in \mathbb{I}(A)$, then $\mathbb{G} \vdash^* t : A ; \mathbb{D}$*

Proof : A simultaneous induction.

The completeness

Theorem (Completeness)

Let A be a type and t a term :
$t \in |A|$ *iff* $(t \triangleright^* t'$ *and* $\vdash t' : A)$

The completeness

Theorem (Completeness)

Let A be a type and t a term :
$t \in |A|$ *iff* $(t \triangleright^* t'$ *and* $\vdash t' : A)$

Corollary

Let A be a type and t a term

- *If $t \in |A|$, then t is normalizable and equivalent to a closed term*
- *$|A|$ is closed under equivalence*

1 The simply typed $\lambda\mu$-calculus

2 The realizability semantic

3 The completeness

4 Perspectives

Second order $\lambda\mu$-calculus

$$\frac{\Gamma \vdash t : A; \Delta}{\Gamma \vdash t : \forall X A; \Delta}\forall_i * \qquad \frac{\Gamma \vdash t : \forall X A; \Delta}{\Gamma \vdash t : A[X := F]; \Delta}\forall_e **$$

* X is not free in Γ and Δ

** For any type F

Second order $\lambda\mu$-calculus

$$\frac{\Gamma \vdash t : A; \Delta}{\Gamma \vdash t : \forall X A; \Delta} \forall_i * \qquad \frac{\Gamma \vdash t : \forall X A; \Delta}{\Gamma \vdash t : A[X := F]; \Delta} \forall_e **$$

* X is not free in Γ and Δ

** For any type F

Definition

The definition of an $\mathcal{M}$-interpretation $\mathcal{I}$ is extended as follows :
$\mathcal{I}(\forall X A) = \cap_{\mathcal{G} \in \mathcal{M}} \{\mathcal{I}^X_{\mathcal{G}}(A)\}$,

where $\mathcal{I}^X_{\mathcal{G}}$ is the $\mathcal{M}$-interpretation such that :
$\mathcal{I}^X_{\mathcal{G}}(X) = \mathcal{G}$ *and* $\mathcal{I}^X_{\mathcal{G}}(Y) = \mathcal{I}(Y)$ *for* $Y \neq X$

The $\forall^+$-types

Definition

The $\forall^+$ *(resp.* $\forall^-$ *) types are defined as follows :*

- $\forall^- = \bot \mid X \mid \forall^+ \to \forall^-$
- $\forall^+ = \bot \mid X \mid \forall^- \to \forall^+ \mid \forall X \forall^+$, *where* X *is free in the type* $\forall^+$

The $\forall^+$-types

Definition

The $\forall^+$ (resp. $\forall^-$) types are defined as follows :

- $\forall^- = \bot \mid X \mid \forall^+ \to \forall^-$
- $\forall^+ = \bot \mid X \mid \forall^- \to \forall^+ \mid \forall X \forall^+$, *where X is free in the type $\forall^+$*

Lemma

Let the term $t = \mu a.(a\, \lambda y_1.\lambda z.\mu b.(a\, \lambda y_2.\lambda x.z))$, and the types Y, $Id = X \to X$ and $Id' = \forall X(X \to X)$. Then,

1. $y : Y \vdash (t\, y) : Id'$ *and* $t \in |Y \to Id'|$
2. *But,* $\not\vdash t : Y \to Id'$
3. *Nevertheless,* $\vdash t : Y \to Id$

The $\mathcal{D}^+$-types

Completeness in the second order typed for a class of types denoted $\mathcal{D}^+$ (types which do not contain the quantifier $\forall$ in the right of the arrows) :

Definition

The $\mathcal{D}^+$, $\mathcal{D}^{++}$ and $\mathcal{D}^-$ types are defined as follows :

- $\mathcal{D}^- = \bot \mid X \mid \mathcal{D}^+ \to \mathcal{D}^-$
- $\mathcal{D}^{++} = \bot \mid X \mid \mathcal{D}^- \to \mathcal{D}^{++}$
- $\mathcal{D}^+ = \mathcal{D}^{++} \mid \forall X \mathcal{D}^+$, *where X is free in $\mathcal{D}^+$*

The typing rules

Definition

$$\frac{\Gamma \vdash u : A; \Delta \quad \Gamma \vdash v : B; \Delta}{\Gamma \vdash \langle u, v \rangle : A \wedge B; \Delta} \wedge_i$$

$$\frac{\Gamma \vdash t : A \wedge B; \Delta}{\Gamma \vdash (t \ \ \pi_1) : A; \Delta} \wedge_e^1 \qquad \frac{\Gamma \vdash t : A \wedge B; \Delta}{\Gamma \vdash (t \ \ \pi_2) : B; \Delta} \wedge_e^2$$

$$\frac{\Gamma \vdash t : A; \Delta}{\Gamma \vdash \omega_1 t : A \vee B; \Delta} \vee_i^1 \qquad \frac{\Gamma \vdash t : B; \Delta}{\Gamma \vdash \omega_2 t : A \vee B; \Delta} \vee_i^2$$

$$\frac{\Gamma \vdash t : A \vee B; \Delta \quad \Gamma, x : A \vdash u : C; \Delta \quad \Gamma, y : B \vdash v : C; \Delta}{\Gamma \vdash (t \ \ [x.u, y.v]) : C; \Delta} \vee_e$$

Interpretation

Definition

- $\mathcal{K} \curlywedge \mathcal{L} = \{t \ / \ (t\ \pi_1) \in \mathcal{K} \text{ and } (t\ \pi_2) \in \mathcal{L}\}$

Interpretation

Definition

- $\mathcal{K} \curlywedge \mathcal{L} = \{t \ / \ (t\ \pi_1) \in \mathcal{K} \text{ and } (t\ \pi_2) \in \mathcal{L}\}$
- $\mathcal{K} \curlyvee \mathcal{L} = \{t \ / \text{ for each } u, v : \text{if } (\text{for each } r \in \mathcal{K}, s \in \mathcal{L} : u[x := r] \in \mathcal{S} \text{ and } v[y := s] \in \mathcal{S}), \text{ then } (t\ [x.u, y.v]) \in \mathcal{S}\}$

Interpretation

Definition

- $\mathcal{K} \curlywedge \mathcal{L} = \{t \ / \ (t\ \pi_1) \in \mathcal{K} \text{ and } (t\ \pi_2) \in \mathcal{L}\}$
- $\mathcal{K} \curlyvee \mathcal{L} = \{t \ / \text{ for each } u, v : \text{if } (\text{for each } r \in \mathcal{K}, s \in \mathcal{L} : u[x := r] \in \mathcal{S} \text{ and } v[y := s] \in \mathcal{S}), \text{ then } (t\ [x.u, y.v]) \in \mathcal{S}\}$

Characterization of operational behaviour :
$\vdash T : A \vee \neg A$

The completeness ?

Example

Let the normal term

$t = \mu a.(a\ \langle \mu b.(a\ \langle \lambda x.x\ ,\ \mu c.(b\ \lambda y.\lambda z.z)\rangle)\ ,\ \lambda x.x\rangle)$

The completeness ?

Example

Let the normal term
$t = \mu a.(a\ \langle \mu b.(a\ \langle \lambda x.x\ ,\ \mu c.(b\ \lambda y.\lambda z.z)\rangle)\ ,\ \lambda x.x\rangle)$
We check that $t \in |A \wedge A|$, *où* $A = X \to X$

- $(t\ \pi_1) \rhd^* \mu a.(a\ \mu b.(a\ \lambda x.x)) = t_1$
- $(t\ \pi_2) \rhd^* \mu a.(a\ \lambda x.x) = t_2$
- $\vdash t_i : A$, *then* $t_i \in |A|$, *where* $t \in |A \wedge A|$

The completeness ?

Example

Let the normal term
$t = \mu a.(a\ \langle \mu b.(a\ \langle \lambda x.x\ ,\ \mu c.(b\ \lambda y.\lambda z.z)\rangle)\ ,\ \lambda x.x\rangle)$
We check that $t \in |A \wedge A|$, *où* $A = X \to X$

- $(t\ \pi_1) \rhd^* \mu a.(a\ \mu b.(a\ \lambda x.x)) = t_1$
- $(t\ \pi_2) \rhd^* \mu a.(a\ \lambda x.x) = t_2$
- $\vdash t_i : A$, *then* $t_i \in |A|$, *where* $t \in |A \wedge A|$

But t *can not have* $A \wedge A$ *as type, since* $\mu c.(b\ \lambda y.\lambda z.z)$ *can not have the type* $A \wedge A$ *with* $b : A \wedge A$

That's all !

Thanks for your attention !