M2 LMFI – SOFIX
Quantification du second-ordre et points fixes en logique
Realizability in System F and applications to strong normalization (Preliminary version, to be completed)

Alexis Saurin

3rd february 2023

Contents

1 Introduction and motivation

In the following, one shall prove ***strong normalization of system*** F using a proof technique known as ***realizability***. This approach was initiated by Kleene and developed further by many, notably by Krivine (especially beyond the intuitionistic setting by developing a framework of realizability for classical logic, known as *classical realizability*).

One will consider Curry-style system F: we will work with pure λ-terms and show that every term that is typable is strongly normalizing. We will deduce strong normalization of Church-style system F thanks to the equivalence established in the previous chapter.

Realizability is in fact a much wider, flexible and powerful tool that allows to analyze the computational behaviour of terms from information on their types in a fine-graind way, beyond (strong) normalizability properties as one shall see on some examples.

Before coming to the realizability construction, let us begin with a remark on normalization proofs by reducibility.

To analyze normalization properties in this setting, one had to express *stability properties by argument application* (or universal instanciation in F, more generally by the effect of the destructors of the language as in T), for instance defining:

$$\mathsf{RED^{WN}}_\rho(U \to V) \quad = \quad \{t : (U \to V)^\rho \mid \forall u \in \mathsf{RED^{WN}}_\rho(U), (t)\, u \in \mathsf{RED^{WN}}_\rho(V)\}.$$

that one can see as a special case of a more general construction:

$$\mathcal{X} \to \mathcal{Y} = \{t / \forall u \in \mathcal{X}, (t)u \in \mathcal{Y}\}$$

which gives:

$$\begin{aligned} \mathsf{RED}^{\mathsf{WN}}{}_\rho(U \to V) &= \{t : (U \to V)^\rho \mid \forall u \in \mathsf{RED}^{\mathsf{WN}}{}_\rho(U), (t)\, u \in \mathsf{RED}^{\mathsf{WN}}{}_\rho(V)\} \\ &= \mathsf{RED}^{\mathsf{WN}}{}_\rho(U) \to \mathsf{RED}^{\mathsf{WN}}{}_\rho(V). \end{aligned}$$

In particular, in the simply typed case for instance, every type T is of the form: $T = U_1 \to \cdots \to (U_n \to X)$ where X is a type variable. By noting that for type variables, one set $\rho(X) = \mathsf{Norm}(X)$, one thus has, in this case:

$$\mathsf{RED}^{\mathsf{WN}}{}_\rho(T) = \{t : T^\rho \mid \forall i \leq n, \forall u_i \in \mathsf{RED}^{\mathsf{WN}}{}_\rho(U_i), (t)\, u_1 \ldots u_n \in \mathsf{Norm}(X)\}$$

One shall generalize these reducibility techniques by evidencing the central notion of applicative context: $(\square)u_1 \ldots u_n$ that on shall manipulate through the notion of stacks which give to applicative contexts a *first-class* existence.

Definition 1.1 (*(Applicative) contexts*)

Contexts and applicative contexts are defined inductively as follows:

$$\begin{aligned} C &::= \square \mid \lambda x.C \mid (t)C \mid (C)t \\ A &::= \square \mid (A)t \end{aligned}$$

2 Realizability interpretation

Let us consider Curry-Style System F: λ-terms are untyped terms and one considers a ternary typability relation, $\vdash_{\mathsf{F}} \subseteq \mathsf{Env} \times \Lambda \times \mathsf{Type}_{\mathsf{F}}$, written $\Gamma \vdash_{\mathsf{F}} t : T$.

Definition 2.1 (*Stacks*)

Let us note Π *the set of* **stacks**, *defined inductively by:*

$$\pi, \pi' ::= \emptyset \mid t \cdot \pi.$$

Π *is therefore the set of finite sequences of* λ*-terms,*

Definition 2.2 (*Processes*)

A **process** *is a pair of a* λ*-term and a stack.*
The process (t, π) *may also be written* $t \star \pi$*.*
We write $\mathsf{P} = \Lambda \times \Pi$ *for the set of processes.*

Example 2.3

One can for instance consider process $(\lambda x.(x)x, \lambda y.(y)y \cdot \emptyset)$*.*

Definition 2.4 (*Pole*)

Given a set of terms Λ_0 *containing the variables, a* Λ_0**-pole** *is a subset* $\perp\!\!\!\perp$ *of* P *satisfying following two properties of closure by anti-reduction with respect to* Λ_0*:*

1. *If* $(t\,\{u/x\}\,, \pi) \in \perp\!\!\!\perp$ *and* $u \in \Lambda_0$*, then* $(\lambda x.\, t, u \cdot \pi) \in \perp\!\!\!\perp$*.*
2. *If* $(t, u \cdot \pi) \in \perp\!\!\!\perp$ *then* $((t)\, u, \pi) \in \perp\!\!\!\perp$*.*

One shall simply speak of a pole in the following, when this is not ambiguous.

Remark 2.5

For those who know the Krivine Abstract Machine (KAM), they will note that the previous properties correspond to closure by anti-reduction of the KAM for arguments in Λ_0.

Example 2.6

The reader is invited to check that the following sets of processes are poles:

- $\emptyset, \Lambda \times \Pi$ *are poles for any choice of* Λ_0 *(satisfying the minimal conditions on* Λ_0*).*
- $\{(t, \pi) \in \mathsf{P} \mid (t)\pi \in \Lambda_{SN}\}$ *is a* Λ_{SN}*-pole. (see section on the applications of realizability to strong normalization.)*
- *Let* Λ_0 *containing the variables,* $\{(t, \pi) \mid (t)\pi \longrightarrow^\star \lambda x.x\}$ *is a* Λ_0*-pole.*

Given a pole (ie a Λ_0-pole for a certain Λ_0), one can relate sets of terms and sets of staks by a so-called ***orthogonality*** relation:

Definition 2.7 (*Orthogonality*)

Let $\perp\!\!\!\perp$ *be a pole. Let* T *be a set of terms and* F *a set of stacks. One defines* $T^\perp$ *and* $F^\perp$ *in the following way:*

$$T^\perp = \{\pi \in \Pi \mid \forall t \in T, (t, \pi) \in \perp\!\!\!\perp\} \qquad F^\perp = \{t \in \Lambda \mid \forall \pi \in F, (t, \pi) \in \perp\!\!\!\perp\}.$$

This orthogonality relation satisfies, straightforwardly, the following properties which are left to the reader as an exercise:

Proposition 2.8

- $T \subseteq U \Rightarrow U^\perp \subseteq T^\perp$;
- $T \subseteq T^{\perp\perp}$;
- $T^\perp = T^{\perp\perp\perp}$.

Reducibility was built by defining sets of λ-terms by induction on type. Here, one shall define ***sets of stacks*** by induction on type and build sets of terms by orthogonality:

Definition 2.9 (Π_0 , F_{Λ_0})

Given a Λ_0*-pole* $\perp\!\!\!\perp$, Π_0 *denotes the set of stacks built from elements of* Λ_0*.*

One shall write F_{Λ_0} *for the set of* **non-empty subsets** *of* Π_0*.*

Definition 2.10 (*Valuation*)

Given a Λ_0*-pole* $\perp\!\!\!\perp$*, a* **valuation** v *is a function from type variables to subsets of* Π_0*.*

Given a valuation v*,* X *a type variable and* $F \subseteq \Pi_0$*,* $\mathsf{v}[X := F]$ *is defined as the valuation equal to* F *on* X *and equal to* v *on any other type variable.*

Definition 2.11 (*Interpretation of a type, falsity value*)

Given a Λ_0*-pole* $\perp\!\!\!\perp$ *and a valuation* v*, one defines inductively* **the interpretation** $\|\_\|_{\mathsf{v}}$ **of F-types** *(taking values in the subsets of* Π*) as follows:*

- $\|X\|_{\mathsf{v}} = \mathsf{v}(X)$;

- $\|A \Rightarrow B\|_{\mathsf{v}} = \{t \cdot \pi \mid t \in \|A\|_{\mathsf{v}}^{\perp}, \pi \in \|B\|_{\mathsf{v}}\}$;
- $\|\forall X.A\|_{\mathsf{v}} = \cup_{\emptyset \subsetneq F \subseteq \Pi_0} \|A\|_{\mathsf{v}[X:=F]}$.

$\|T\|_{\mathsf{v}}$ will be called **the falsity value** *of T.*

Definition 2.12 (*Realizability relation, truth value*)

Given a Λ_0-pole $\perp\!\!\!\perp$ and a valuation v, a term t **realizes** *a type T, written $t \Vdash_{\mathsf{v}} T$, if $t \in \|T\|_{\mathsf{v}}^{\perp}$. Such a t is called a* **realizer** *of T.*

The set of realizers of T is written $|T|_{\mathsf{v}}$; it is equal to the orthogonal of $\|T\|_{\mathsf{v}}$ and will be called the **truth value** *of T.*

The following remark provides an intuition for the terminology of truth/falsity values.

Remark 2.13 (*Truth and falsity values*)

Realizability has two parameters: the pole and the valuation (there is actually a third parameter, the set Λ_0), even though only the pole is shown in the notation.

Whatever choice we make of Λ_0, $\emptyset$ and $\mathsf{P} = \Lambda \times \Pi$ are poles. In the case where $\perp\!\!\!\perp = \emptyset$, one has

$$F^{\perp} = \begin{cases} \Lambda & si\ F = \emptyset \\ \emptyset & si\ F \neq \emptyset \end{cases} .$$

One therefore recovers the usual bolean interpretation:

- $|A \to B|_{\rho} = \emptyset$ *if* $|A|_{\rho} = \Lambda$ *and* $|B|_{\rho} = \emptyset$ *et*
- $|A \to B|_{\rho} = \Lambda$ *otherwise.*

In the same way:

- $|\forall X.A|_{\rho} = \emptyset$ *if there exists* $F \in F_{\Lambda_0}$ *such that* $|A|_{\rho[X:=F]} = \emptyset$ *and*
- $|\forall X.A|_{\rho} = \Lambda$ *otherwise.*

This is from this interpretation that come the names **truth value and falsity values** *as one easily understands.*

One establishes a first property of the above constuctions, a classical substitutivity property which looks alike a property established for reducibility.

Lemma 2.14 (*Substitutivity of the realizability interpretation*)

For any types T, U and any type variable X, one has for every pole and every valuation v that:

$$\|T\{U/X\}\|_{\mathsf{v}} = \|T\|_{\mathsf{v}[X:=\|U\|_{\mathsf{v}}]}.$$

Proof: The lemma is proved by induction on the structure of the type, writing $\mathsf{v}' = \mathsf{v}[X := \|U\|_{\rho}]$.

- Case $T = X$ is trivial.
- Case $T = Y \neq X$ is trivial.
- Case $T = V \to W$: one has $T\{U/X\} = V\{U/X\} \to W\{U/X\}$, so that a stack π belongs to $\|T\{U/X\}\|_{\mathsf{v}}$ if, and only if, it is of the form $t \cdot \pi'$ where $t \in |V\{U/X\}|_{\mathsf{v}} = \|V\{U/X\}\|_{\mathsf{v}}^{\perp}$ and $\pi' \in \|W\{U/X\}\|_{\mathsf{v}}$, or, thanks to the induction hypothesis if, and only if, $t \in \|V\|_{\mathsf{v}'}^{\perp}$ and $\pi' \in \|W\|_{\mathsf{v}'}$, that is iff $t \cdot \pi \in \|T\|_{\mathsf{v}'}$.
- Case $T = \forall Y.V$ (with $Y \neq X$ and $Y \notin FV(U)$): one has $T\{U/X\} = \forall Y.(V\{U/X\})$ and thus $\pi \in \|T\{U/X\}\|_{\mathsf{v}}$ if, and only if, $\pi \in \|V\{U/X\}\|_{\mathsf{v}[Y:=F]}$ for some F in F_{Λ_0} and, applying the

induction hypothesis as above, if and only if $\pi \in \|V\|_{\mathsf{v}'[Y:=F]}$ for some F in F_{Λ_0}, that is if and only if $\pi \in \|T\|_{\mathsf{v}'}$.

This concludes the proof.

□

Lemma 2.15

If v is such that for any T, $\|T\|_{\mathsf{v}} \subseteq \Pi_0$ and if $F \subseteq \Pi_0$, then $\mathsf{v}' = \mathsf{v}[X := F]$ is also such that for any T, $\|T\|_{\mathsf{v}'} \subseteq \Pi_0$.

Proof: Indeed, $\|T\|_{\mathsf{v}'} \subseteq \|\forall X.T\|_{\mathsf{v}} \subseteq \Pi_0$.

□

3 Adequation lemma (Adequacy lemma)

One shall prove an adequation result of the realizability semantics to the typing.

For this, one defines two specific sorts of valuations:

Definition 3.1 (*weakly/well adapted valuations*)

A valuation v is **weakly adapted** *to a Λ_0-pole $\perp\!\!\!\perp$ if, for any type T,*

$$|T|_{\mathsf{v}} \subseteq \Lambda_0 \qquad \& \qquad \|T\|_{\mathsf{v}} \subseteq \Pi_0.$$

A valuation v is **adapted** *(or well-adapted) to a Λ_0-pole $\perp\!\!\!\perp$ if, for any type T,*

$$\mathcal{V} \subseteq |T|_{\mathsf{v}} \subseteq \Lambda_0 \qquad \& \qquad \|T\|_{\mathsf{v}} \subseteq \Pi_0.$$

Lemma 3.2

Let v be a (weakly) adapted valuation, X a type variable and $\emptyset \neq F \subseteq \Pi_0$. Then $\mathsf{v}' = \mathsf{v}[X := F]$ is (weakly) adapted as well.

Proof: Since v is adapted (resp weakly adapted), then for any type A, $\mathcal{V} \subseteq |A|_{\mathsf{v}} \subseteq \Lambda_0$ (resp. $\mathcal{V} \subseteq |A|_{\mathsf{v}} \subseteq \Lambda_0$).

First notice that $\|A\|_{\mathsf{v}'} \subseteq \|\forall X.A\|_{\mathsf{v}} \subseteq \Pi_0$ for any type A. Moreover, $|A|_{\mathsf{v}'} \subseteq \Lambda_0$ simply comes from the fact that $\|A \to \forall X.X\|_{\mathsf{v}'} = |A|_{\mathsf{v}'} \cdot \Pi_0 \subseteq \Pi_0$ so that $|A|_{\mathsf{v}'} \subseteq \Lambda_0$.

It results that v' is weakly adapted.

If moreover, v is well-adapted, $|A|_{\mathsf{v}'} \supseteq |\forall X.A|_{\mathsf{v}} \supseteq \mathcal{V}$ and v' is well-adapted as well. ■

A well-adapted valuation is therefore a weakly adapted valuation such that variables realize every type.

Remark 3.3

If one considers a realizability construction with $\Lambda_0 = \Lambda$, then every valuation is trivially weakly adapted.

Definition 3.4 (*Admissible set of terms*)

A set $\Lambda_0 \subseteq \Lambda$ is **admissible** *if there exists a Λ_0-pole $\perp\!\!\!\perp$ and a valuation v which is well-adapted for $\perp\!\!\!\perp$.*

One can now state the adequation lemma for realizability:

Lemma 3.5 (*Adequation lemma*)

Let v be a (weakly) adapted valuation for a pole $\perp\!\!\!\perp$ and let t be a term such that $x_1 : U_1, \ldots, x_n : U_n \vdash_{\mathsf{F}} t : T$ is derivable in Curry-Style F. Let $(u_i)_{1 \leq i \leq n}$ be realizers of the $(U_i)_{1 \leq i \leq n}$ (ie. $u_i \Vdash_{\mathsf{v}} U_i$ for $1 \leq i \leq n$), then $t\,\{u_i/x_i, 1 \leq i \leq n\} \Vdash_{\mathsf{v}} T$.

Proof: One proves the lemma by induction on a typing derivation d of $x_i : U_i \vdash_{\mathsf{F}} t : T$. (Note that there may exist several such typing derivations since we work with Curry-Style System F...) One shall write $\Gamma = x_1 : U_1, \ldots, x_n : U_n$ and $t' = t\{u_i/x_i, 1 \leq i \leq n\}$.

- **If d is an axiom**, the property trivialy holds since $t' = u_i$ for some i which realizes $U_i = T$ by hypothesis.
- **If d ends with $\rightarrow I$**, one has $t = \lambda x.v$, $T = U \rightarrow V$, and $x_1 : U_1, \ldots x_n : U_n, x : U \vdash_{\mathsf{F}} v : V$ Let $v' = v\{u_i/x_i, 1 \leq i \leq n\}$. We want to prove that t' realizes T for valuation v: one considers a stack $\pi \in \|T\|_{\mathsf{v}} \subseteq \Pi_0$.

  There are only two possibilities: either no such stack exists and then t' réalizes T trivially, or π has form $u \cdot \pi'$, with $u \Vdash_{\mathsf{v}} U$, $u \in \Lambda_0$ and $\pi' \in \|V\|_{\mathsf{v}}$, $\pi' \in \Lambda_0$.

  In the second case, we know by induction hypothesis that $v'\{u/x\} \Vdash_{\mathsf{v}} V$ from which $(v'\{u/x\}, \pi') \in \perp\!\!\!\perp$ and by closure by KAM-anti-reduction of $\perp\!\!\!\perp$ (more precisely by property 1.) and since $u \in |U|_{\mathsf{v}} \subseteq \Lambda_0$ by (weak) adaptation of v, one also has that $(t\{u/x\}, u \cdot \pi') \in \perp\!\!\!\perp$ which shows that $t' \Vdash_{\mathsf{v}} T$ since the stack was chosen arbitrarily.
- **If d ends with $\rightarrow E$**, then we have $t = (u)v$ with $x_1 : U_1, \ldots x_n : U_n \vdash_{\mathsf{F}} u : V \rightarrow T$ and $x_1 : U_1, \ldots x_n : U_n \vdash_{\mathsf{F}} v : V$ for some type V.

  One can apply the induction hypothesis to both derivation d_u and d_v concluding $x_1 : U_1, \ldots x_n : U_n \vdash_{\mathsf{F}} u : V \rightarrow T$ and $x_1 : U_1, \ldots x_n : U_n \vdash_{\mathsf{F}} v : V$ which ensures that $u' = u\{u_i/x_i, 1 \leq i \leq n\}$ and $v' = v\{u_i/x_i, 1 \leq i \leq n\}$ realize respectively $V \rightarrow T$ and V for valuation v.

  To show that t' realizes T, it is enough to consider an arbitrary stack π in $\|T\|_{\mathsf{v}}$ and to remark that $v' \cdot \pi \in \|V \rightarrow T\|_{\mathsf{v}} \subseteq \Pi_0$ and thus that $(u', v' \cdot \pi) \in \perp\!\!\!\perp$. As before one applies the closure properties of the pole: since $v' \in \Lambda_0$, the second closure property of the pole applies and one gets $(t', \pi) \in \perp\!\!\!\perp$, which means, since π is any stack in $\|T\|_{\mathsf{v}}$, that $t' \Vdash_{\mathsf{v}} T$.
- **If d ends with $\forall I$**, then one has $T = \forall X.U$ and $x_1 : U_1, \ldots x_n : U_n \vdash_{\mathsf{F}} t : U$ where X does not occur free in the U_i.

  To show that $t' \Vdash_{\mathsf{v}} \forall X.U$, let us consider $\pi \in \|\forall X.U\|_{\mathsf{v}}$. We know by definition of the realizability interpretation that there exists $F \subseteq \Pi_0$ non empty such that $\pi \in \|U\|_{\mathsf{v}[X:=F]}$.

  But since X is not free in the U_i the interpretation of U_i is the same in v and in $\mathsf{v}' = \mathsf{v}[X := F]$, in particular, the lemma hypothesis tells us that $u_i \Vdash_{\mathsf{v}'} U_i$ if $1 \leq i \leq n$. One can therefore apply the induction hypothesis to the subderivation of conclusion $x_1 : U_1, \ldots x_n : U_n \vdash_{\mathsf{F}} t : U$ with respect to v' (which is weakly-adapted by Lemma 3.2): $t' \Vdash_{\mathsf{v}'} U$ so that $(t', \pi) \in \perp\!\!\!\perp$ which proves that $t' \Vdash_{\mathsf{v}} \forall X.U$.
- **If d ends with $\forall E$**, then we have a subderivation d' of d, which concludes with $x_1 : U_1, \ldots x_n : U_n \vdash_{\mathsf{F}} t : \forall X.U$, with $T = U\{V/X\}$ for some V.

  Let us consider $\pi \in \|U\{V/X\}\|_{\mathsf{v}}$: we need to prove that $(t, \pi) \in \perp\!\!\!\perp$. The substitutivity lemma ensures that $\pi \in \|U\|_{\mathsf{v}[X:=\|V\|_{\mathsf{v}}]}$.

  By applying induction hypothesis to d', we have $t' \Vdash_{\mathsf{v}} \forall X.U$ so for any non empty $F \subseteq \Pi_0$, we have that $t' \Vdash_{\mathsf{v}[X:=F]} U$, and in particular when $F = \|V\|_{\mathsf{v}} \subseteq \Pi_0$.

  We then deduce that $(t', \pi) \in \perp\!\!\!\perp$.

This concludes the proof of the lemma.

□

Adequation lemma allows to deduce easily that a typed term realizes its type and that typable terms are in the intersection of all admissible sets:

Theorem 3.6

If Λ_0 is admissible and $\Gamma \vdash_{\mathsf{F}} t : T$, then $t \in \Lambda_0$.

Proof: Indeed, if Λ_0 is admissible, then there exists a pole $\perp\!\!\!\perp$ and a valuation v adapted to Λ_0. The adequation lemma can be applied to variables which are realizers of any type and $t = t\{x_i/x_i\} \in |T|_{\mathsf{v}} \subseteq \Lambda_0$.

□

To prove strong normalization of F, it is therefore sufficient to prove that the set of strongly normalizing terms is admissible, that we will do in the following.

4 Application of realizability to strong normalization of system F

As seen before, in order to prove strong normalization of System F using realizability, it is sufficient to prove that Λ_{SN} is an admissible set since Theorem 3.6 will allow to conclude that every typable term is strongly normalizable.

One shall now build a Λ_{SN}-pole $\perp\!\!\!\perp$ together with a well-adapted valuation v, that is such that for every type T,

$$\mathcal{V} \subseteq |T|_{\mathsf{v}} \subseteq \Lambda_{SN}.$$

This fact relies on two preliminary lemmas:

Lemma 4.1

For any λ-terms t, u with u strongly normalizing and π a stack, then if $t\{u/x\}\pi$ is SN, $(\lambda x.\, t)\, u\pi$ is SN.

Proof: Let t, u, π as specified in the lemma's statement.

Let us consider $t' = (\lambda x.\, t)\, u\pi$ and $t'' = (t\{u/x\})\,\pi$.

Since t'' is SN, it comes immediately that $t \in \Lambda_{SN}$ and $\pi \in \Pi_{SN}$. Assume, aiming at a contradiction that there exists an infinite reduction sequence from t'. Thanks to the above remark, this reduction cannot be infinitely in t, u or in π.

Therefore one has $t' \longrightarrow^{\star}_{\beta} (\lambda x.\, t_0)\, u_0\pi_0 \longrightarrow_{\beta} (t_0\{u_0/x\})\,\pi_0 \longrightarrow^{\star}_{\beta} \ldots$, but we know that $t'' \longrightarrow^{\star}_{\beta} (t_0\{u_0/x\})\,\pi_0 \longrightarrow^{\star}_{\beta} \ldots$ which contradicts strong normalization of t''.

□

Definition 4.2 ($\perp\!\!\!\perp_{SN}$)

Let $\perp\!\!\!\perp_{SN}$ be $\{(t,\pi) \in \mathsf{P} \mid (t)\,\pi \in \Lambda_{SN}\}$.

Proposition 4.3

$\perp\!\!\!\perp_{SN}$ is a Λ_{SN}-pole.

Proof: One shall verify both KAM-anti-reduction closure properties:

- the first is a direct consequence of the previous lemma.
- the second is trivial considering the definition of the pole since processes $((t)u, \pi)$ and $(t, u \cdot \pi)$ correspond to the same λ-term $(t)\, u\pi$.

□

Lemma 4.4

For any $F \in F_{\Lambda_{SN}}$, we have, for $\perp\!\!\!\perp_{SN}$ orthogonality:

$$\mathcal{V} \subseteq F^{\perp} \subseteq \Lambda_{SN}.$$

Proof: Let $F \in F_{\Lambda_{SN}}$.

If $x \in \mathcal{V}$ and $\pi \in F \subseteq F_{\Lambda_{SN}}$, then $(x)\,\pi \in \Lambda_{SN}$ so that $x \in F^{\perp}$ and $\mathcal{V} \subseteq F^{\perp}$.

If $t \in F^{\perp}$, as F is not empty, let $\pi \in F$. We have $(t)\,\pi \in \Lambda_{SN}$ and therefore it comes that $t \in \Lambda_{SN}$. One deduces that $F^{\perp} \subseteq \Lambda_{SN}$.

□

Proposition 4.5

Λ_{SN} is admissible.

Proof: Consider pole $\perp\!\!\!\perp_{SN}$, one defines the valuation v_{SN} such that $\mathsf{v}_{SN}(X) = \Pi_{SN}$ for any type variable X.

It is sufficient to show that for all type T, $\|T\|_{\mathsf{v}_{SN}} \in \mathsf{F}_{\mathsf{SN}}$.

More precisely, one uses a stronger induction hypothesis and proves that for any type T, $\|T\|_{\mathsf{v}_{SN}} \in \mathsf{F}_{\mathsf{SN}}$ as soon as v_{SN} takes its values in F_{SN} by induction on type T:

- Case $T = X$. Then $\|X\|_{\mathsf{v_{SN}}} = \mathsf{v_{SN}}(X) \in \mathsf{F_{SN}}$ by hypothesis on $\mathsf{v_{SN}}$.
- Case $T = U \to V$. Then, by induction hypothesis, $\|U\|_{\mathsf{v_{SN}}}, \|V\|_{\mathsf{v_{SN}}} \in \mathsf{F_{SN}}$. By the previous lemma, $|U|_{\mathsf{v_{SN}}} = \|U\|^{\perp}_{\mathsf{v_{SN}}}$ contains all variables so that $\|T\|_{\mathsf{v_{SN}}} = |U|_{\mathsf{v_{SN}}} \cdot \|V\|_{\mathsf{v_{SN}}}$ is non-empty and is a subset of Π_{SN} since $|U|_{\mathsf{v_{SN}}} \subseteq \Lambda_{\mathsf{SN}}$ (by the lemma) and $\|V\|_{\mathsf{v_{SN}}} \in \Pi_{\mathsf{SN}}$ by induction hypothesis: one has $\|T\|_{v_{SN}} \in \mathsf{F_{SN}}$.
- Case $T = \forall X.U$. Then $\|\forall X.U\|_{\mathsf{v_{SN}}} = \cup_{F \in \mathsf{F_{SN}}} \|U\|_{\mathsf{v_{SN}}[X:=F]} \subseteq \mathsf{F_{SN}}$ since every $\|U\|_{\mathsf{v_{SN}}[X:=F]} \subseteq \mathsf{F_{SN}}$ by induction hypothesis.

□

The strong normalization theorem for System F is then a simple corollary of the previous result thanks to adequation lemma for realizability:

Corollary 4.6

Every typable term in F *is strongly normalizing.*

Proof: We know by the corollary of adequation lemma that typable terms are in the intersection of all admissible sets, so that they are in Λ_{SN} which is admissible by the previous lemma.

□

Remark 4.7

One can also directly get the result from adequation lemma by instantiating realizability with Λ_{SN} *and the valuation considered in the previous proposition and by instantiating the adequation lemma on the trivial substitution* $\{x_i/x_i, 1 \leq i \leq n\}$ *since variables realize all types.*

Remark 4.8

The reducibility technique of the previous chapter can of course be extended to establish strong normalization.

5 Some more applications of realizability

Realizability is actually a flexible technique for analyzing the dynamics of λ-terms and of programs which is not restricted to normalization properties.

We give some illustrations below.

Definition 5.1 (*Some data types in System* F)

Let us consider:

- $\perp = \forall X.X$;
- $1 = \mathsf{ID} = \forall X.(X \to X)$;
- $\mathsf{Bool} = \forall X.(X \to (X \to X))$;
- $\mathsf{Nat} = \forall X.(X \to (X \to X) \to X)$;
- $T \times U = \forall X.(U \to V \to X) \to X)$;
- $T + U = \forall X.(T \to X) \to (U \to X) \to X)$;
- $\mathsf{DNE} = \forall X.((X \to \perp) \to \perp) \to X$;
- $\mathsf{List}(T) = \forall X.X \to (T \to (X \to X)) \to X$;
- $\mathsf{List} = \forall Y.\forall X.X \to (Y \to (X \to X)) \to X$;
- $\mathsf{Tree}(T) = \forall X.X \to ((T \to X) \to X) \to X$;

- $\mathsf{Tree} = \forall Y.\forall X.X \to ((Y \to X) \to X) \to X$.

The following propositions characterize the computational behavious of terms inhabiting the above types:

Proposition 5.2

There is no closed term t such that $\vdash_{\mathsf{F}} t : \bot$.

Proof: Let us apply realizability: there is to show a set of terms Λ_0, a Λ_0-pole and a weakly admissible set for this pole, allowing to use adequation lemma and its consequences.

Λ is of course an admissible set and we know that $\emptyset$ and Λ are Λ-poles (this is a general fact) and that every valuation is weakly admissible for these poles since $\Lambda_0 = \Lambda$ as noted above.

Let us consider $\perp\!\!\!\perp = \emptyset$ We have then $\|\forall X.X\|_{\mathsf{v}} = \cup_{F \in F_\Lambda} F = \Pi$.

Let us reason by contradiction and assume that there exists a term t such that $\vdash t : \forall X.X$. By the theory of realizability, we know that t realize universally $\forall X.X$ ($t \Vdash_{\mathsf{v}} \forall X.X$ for any valuation) this implies that for all $\pi \in \Pi$, we have $(t, \pi) \perp\!\!\!\perp$... which is impossible since $\perp\!\!\!\perp$ is empty: as a conclusion, such a term t cannot exist.

□

Proposition 5.3

If $\vdash_{\mathsf{F}} t : \mathsf{ID}$, then $t \longrightarrow^{\star}_{\beta} \lambda x.\, x$.

Proof: One shall again consider Λ as admissible set and consider $\perp\!\!\!\perp_x = \{(t, \pi) \mid (t)\pi \longrightarrow^{\star} x\}$. This is of course a pole since the closure properties are trivially met.

Let us consider $F^{\emptyset} = \{\emptyset\}$ (*ie.* the singleton made of the empty stack) and $\mathsf{v} = [X := F^{\emptyset}]$. We have therefore $x \Vdash_{\mathsf{v}} X$ (indeed, $(x, \emptyset) \in \perp\!\!\!\perp_x$) and if $\vdash t : \forall X.(X \to X)$ (so that in particular if it is a closed term), we have $t \Vdash_{\mathsf{v}} X \to X$ so $(t, x \cdot \emptyset) \in \perp\!\!\!\perp_x$ which ensures that $(t)x \longrightarrow^{\star} x$ by definition du pôle of the pole.

We have $(t)x \longrightarrow^{\star} (\lambda x.v)x \longrightarrow_{\beta} v \longrightarrow^{\star} x$ so that $t \longrightarrow^{\star} \lambda x.v \longrightarrow^{\star} \lambda x.x$, QED.

□

Proposition 5.4

If $\vdash_{\mathsf{F}} t : \mathsf{Bool}$, then $t \longrightarrow^{\star}_{\beta} \lambda x.\, \lambda y.\, x$ or $t \longrightarrow^{\star}_{\beta} \lambda x.\, \lambda y.\, y$.

Proof: The set $\perp\!\!\!\perp_{x,y} = \perp\!\!\!\perp_x \cup \perp\!\!\!\perp_y$ is a Λ-pole. Let us consider valuation $\mathsf{v} = [X := \{\emptyset\}]$ as before.

We clearly have $x \Vdash_{\mathsf{v}} X$ and $y \Vdash_{\mathsf{v}} X$ and by adequation lemma, if $\vdash_{\mathsf{F}} t : \mathsf{Bool}$, then $t \Vdash_{\mathsf{v}} X \to X \to X$ so that $(t)x \Vdash_{\mathsf{v}} X \to X$ and $(t)xy \Vdash_{\mathsf{v}} X$, that is $(t)xy \longrightarrow^{\star} x$ or $(t)xy \longrightarrow^{\star} y$. Since t is closed, we have: $(t)xy \longrightarrow^{\star} (\lambda x.v)xy \longrightarrow (v)y \longrightarrow^{\star} (\lambda y.w)y \longrightarrow w \longrightarrow^{\star} z \in \{x, y\}$. from which comes that $t \longrightarrow^{\star} \lambda x.v \longrightarrow^{\star} \lambda x.\lambda y.w \longrightarrow^{\star} \lambda x.\lambda y.z$ with $z \in \{x, y\}$, QED.

□

Proposition 5.5

If $\vdash_{\mathsf{F}} t : \mathsf{Nat}$, then there exists a natural n such that $t \longrightarrow^{\star}_{\beta} \lambda z.\, \lambda s.\, (s)^n z$.

Proof: Exercise.

□

Definition 5.6

If $\mathcal{X}, \mathcal{Y}$ are sets of λ-terms, we set $\mathcal{X} \to \mathcal{Y} \triangleq \{t \mid \forall u \in \mathcal{X}, (t)u \in \mathcal{Y}\}$.

Lemma 5.7

Let $\perp\!\!\!\perp$ be a Λ-pole, U, V be types of F, v be a valuation. If the pole is closed not only by anti-reduction but also by reduction, then we have $|U \to V| = |U| \to |V|$.

Proof: Exercise

□

Remark 5.8

The previous result is still true if the pole is not a Λ-pole but the valuation is adapted.

Proposition 5.9

There is no closed term t such that $\vdash_{\mathsf{F}} t : \mathsf{DNE}$.

Proof: Exercise.

□

Proof: Let us reason by contradiction, assuming t is a closed term such that $\vdash_{\mathsf{F}} t : \mathsf{DNE}$.

Consider Λ as admissible set and consider $\perp\!\!\!\perp_x = \{(t, \pi) \mid (t)\pi \longrightarrow^{\star} x\}$. Remember also that every valuation is weakly adapted wrt Λ, which is sufficient to apply adequacy lemma.

We know that t realizes universally $\forall X.(((X \to \bot) \to \bot) \to X)$, that is $t \Vdash_{\mathsf{v}} \forall X.(((X \to \bot) \to \bot) \to X)$ for any valuation v. Consider in particular $F = \{\emptyset\}$ and $G = \{x \cdot \emptyset\}$ and $\mathsf{v}_1 = [X := F]$ and $\mathsf{v}_2 = [X := G]$. We have: (i) F, G are non empty; (ii) F, G are disjoint; (iii) F, G have non empty orthogonal sets. We have $t \in |((X \to \bot) \to \bot) \to X|_{\mathsf{v}_i}$ for $i \in \{1, 2\}$.

In particular, for any $u \in |(X \to \bot) \to \bot|_{\mathsf{v}_i}$, $(t)u \in |X|_{\mathsf{v}_i} = \mathsf{v}_i(X)^{\perp}$.

For any $v \in |X \to \bot|_{\mathsf{v}_i}$ and $w \in |X|_{\mathsf{v}_i}$, $(v)w \in |\bot|_{\mathsf{v}_i} = \emptyset$. Since $|X|_{\mathsf{v}_i} \neq \emptyset$ (as $x \in |X|_{\mathsf{v}_1}$ and $\lambda x.x \in |X|_{\mathsf{v}_2}$) we have that $|X \to \bot|_{\mathsf{v}_i} = \emptyset$. It follows that $\|(X \to \bot) \to \bot\|_{\mathsf{v}_i} = \emptyset$ and $|(X \to \bot) \to \bot|_{\mathsf{v}_i} = \Lambda$.

Therefore, for any $u \in \Lambda$, $(t)u \in F^{\perp}$ and $(t)u \in G^{\perp}$ which means:

- $(t)u \longrightarrow^{\star} x$ (using $(t)u \in F^{\perp}$);
- $(t)ux \longrightarrow^{\star} x$ (using $(t)u \in G^{\perp}$).

But that would imply $(x)x =_{\beta} x$ which is not, a contradiction.

□

Proposition 5.10

Let T be a type, let $\vdash_{\mathsf{F}} t : \mathsf{List}(T)$. Assuming that $v_{::}$ and $v_{[]}$ are two variables of system F, there exists $n \geq 0$ and closed terms $a_1, \ldots, a_n$ such that $\vdash_{\mathsf{F}} a_i : T$ for $1 \leq i \leq n$ such that $t \longrightarrow_{\beta}^{\star} \lambda v_{[]}.\, \lambda v_{::}.\, ((v_{::})\, a_1((v_{::})\, a_2 \ldots ((v_{::})\, a_n v_{[]})))$.

Proof: Exercise.

□