LFCS

Laboratory for Foundations of Computer Science
Department of Computer Science - The University of Edinburgh

An Ideal Model for an Extended λ-Calculus with Refinement

by

J Levy
J Agustí
F Esteva
P García

LFCS Report Series

ECS-LFCS-91-188

LFCS
Department of Computer Science
University of Edinburgh
The King's Buildings
Edinburgh EH9 3JZ

November 1991

An Ideal Model for an Extended λ-Calculus with Refinement

J. Levy, J. Agustí, F. Esteva, P. García*
Centre d'Estudis Avançats de Blanes (CSIC)
Camí de Sta. Bàrbara s/n
E-17300 Blanes, Girona, Spain
e-mail : levy@ceab.es and agusti@ceab.es

Contents

1 Introduction

In Computer Science, Lambda Calculus (i. e. the subject of [Bar81] and [HS86]) has been mainly used as the skeleton of functional programming languages [Lan64]. It has also been used as a higher order parameterization mechanism in some specification languages [ST91]. In this paper we view λ-calculus as both the applicative structure of a programming formalism and a low-level specification formalism. Considered as a programming formalism, its operational semantics is the usual one, mainly based on β-reduction. More unusual is to consider λ-calculus as a specification formalism which admits a precise notion of refinement between λ-expressions. By specification we mean here an intensional description of a set of objects sharing some properties and the refinement relation expresses the correctness of a step in the incremental development of a program from a specification. Lambda expressions can be considered specifications so far we make them denote not elements of a domain [1] as usual, but a particular poset of them. Then an expression can

*Research supported by the CICYT project SPES number 880j382.

[1] We take the category of domains to be the one called consistently complete and ω-algebraic partial ordered set, built using Scott's techniques [Sco76]

be refined by giving another expression whose denotation is included in the denotation of the former. We model the refinement relation between expressions as the inclusion relation between sets. The limited expressive power of λ-calculus as a specification formalism is compensated for by the fact that there is a formal refinement relation [LAEG90] which is semidecidable and can be checked by a complete procedure.

Having in mind the interpretation of λ-expressions as specifications, we have taken closed ideals [2] as denotations of λ-expressions. There are different reasons that support this decision. Ideals establish a coherent link between the inclusion order of ideals and the order of its elements. When introducing the semantics of λ-expressions in subsection 1.1, we will see another reason to have ideals as semantic objects. These and other similar reasons have been given in [MPS86] to model polymorphic types as ideals. Furthermore, λ-expressions can also be seen as types denoting a set of values and the refinement relation can be compared with the subtype relation in [Car88] [Rey85] and with the containment relation between types in [Mit88]. In the same research line, there are several systems [ML79] [CABea86] [CH88] [LB88] in which types and values are so intertwined that types become program specifications and programs become constructive proofs that such specifications are satisfiable. For instance, in the Calculus of Constructions [CH88], λ-expressions have been used to represent both values and types. In that paper and in [ML79], however, value expressions and type expressions are rigorously distinguished and a type relation between values and types is formalized. Less rigorous is the distinction in Nuprl [CABea86] and in Pebble [LB88]. For instance types are taken in Pebble as values at compile time. However in all those systems the distinction between values and types is made in some sense. Here, on the contrary, the distinction is completely dropped from the very beginning and the type membership relation is replaced by a particular subtype relation called refinement. Although these considerations about and comparisons between λ-expressions as specifications and as types have guided our intuition and can be exploited in future research as a guide for program development, they will not be further developed in this paper. The construction of the semantic domain of ideals in which this discussion acquires a precise meaning is the priority endeavour here.

Given that we want λ-expressions to denote ideals and that the set of ideals is closed under union, intersection and cartesian product (see lemma 2.7) it seems natural to extend pure λ-calculus with these set operators. Besides these operators we have extended pure λ-calculus with the recursion operator. The syntax of the extended λ-calculus is then the following one, where e ranges over expressions and x over variables:

$$e ::= x \mid top \mid error \mid \lambda x.e \mid e(e) \mid e \cup e \mid e \cap e \mid e \times e \mid fst(e) \mid scd(e) \mid \mu x.e \qquad (1)$$

We want to give semantics to these expressions in the domain of ideals $\mathcal{I}(U)$, the domain of elements U being the solution of the equation:

$$U \cong K + U \times U + [\mathcal{I}(U) \to U] \qquad (2)$$

where K is any initially given domain and $[\mathcal{I}(U) \to U]$ stands for the set of continuous functions from $\mathcal{I}(U)$ to U.

In subsection 1.1 we motivate the particular form of this equation. The main goal of the paper is to prove that the domain of ideals $\mathcal{I}(U)$ is a semantic model of the extended λ-calculus. A simple refinement relationship can be defined in this domain of ideals as follows. An expression

[2] Closed ideals are a particular class of posets left closed and closed under least upper bounds of increasing sequences, henceforth ideals for short [MPS86].

e_1 refines another expression e_2, written $e_1 \leq e_2$, if the ideal denoted by the first, $[\![e_1]\!]$, is included in the ideal denoted by the second, $[\![e_2]\!]$, that is:

$$e_1 \leq e_2 \text{ if and only if } [\![e_1]\!] \subseteq [\![e_2]\!]$$

where $[\![\_]\!]$ is used here informally to mean the semantic function whose precise definition is given in section 4. The formalization of the refinement relation $\leq$ in a calculus of refinements is the subject of another paper [LAEG90]. Based on this calculus we are defining a specification-programming language which allows formal program development following the stepwise refinement paradigm.

The rest of the introduction motivates some technical decisions taken in order to interpret extended λ-expressions as specifications. In section 2 we show that ideals of a domain form also a domain. This result enables us to build a solution of the previously mentioned isomorphism equation (2). In section 3 a natural connection between functions on ideals and ideals of functions on values is defined. The properties of that connection are used in section 4 to prove that the domain of ideals is a model of the extended λ-calculus. A satisfaction relation is defined between the model and the refinement formulae. This opens up the way to the definition of a sound entailment relation on the set of refinement formulae.

1.1 Semantics of λ-expressions as specifications

λ-expressions usually denote elements of a domain solution of an equation similar to the following one:

$$V \cong K + V \times V + [V \to V] \tag{3}$$

However, as we have mentioned before, we want the expressions (1) of our extended λ-calculus denote ideals of some domain of elements. An easy way would be to take the domain V defined by (3) as the domain of elements on which the set of ideals $\mathcal{I}(V)$ is defined. Unfortunately this does not work. In this subsection we will show why V is not adequate and why we need the domain U defined by (2) as the domain of elements on which to build ideals. To do that we must, first of all, give an idea of the semantics of λ-expressions. The detailed semantics of λ-expressions is the subject of section 4.

In the ideals semantic domain the interpretation of the symbols $\cup$, $\cap$ and $\times$ in (1) is straightforward. They denote the set operators union, intersection and cartesian product, as intended. Less evident is the interpretation of λ-abstraction, application and recursion. The semantics of recursion can be derived from the semantics of λ-abstraction and application, as known. Therefore, only the semantics of these two constructors will be discussed in the following.

The standard interpretation of λ-abstraction is a function whose computation is performed using β-reduction. In our case, as variables denote ideals, one might expect λ-abstraction to denote functions from ideals to ideals. But functions on ideals are not ideals. This conflicts with the intended semantics. On the one hand we want to keep β-reduction as the computational mechanism for our λ-abstractions and, on the other hand, we want λ-abstractions denote ideals, not functions on ideals. We need then an appropriate connection between functions on ideals and ideals (of functions on elements). Fortunately there is a natural connection, defined by two maps $+$ and $*$ as follows:

$$\begin{aligned} + &: (\mathcal{I}(V) \to \mathcal{I}(V)) \to \mathcal{I}(V) \\ * &: \mathcal{I}(V) \to (\mathcal{I}(V) \to \mathcal{I}(V)) \end{aligned}$$

where for any $F : \mathcal{I}(V) \to \mathcal{I}(V)$, the set $+(F)$, noted F^+, is defined by

$$F^+ = \{f : V \to V \mid f(\epsilon) \in F(I) \text{ for every } I \in \mathcal{I}(V) \text{ and } \epsilon \in I\}$$

which can be proved to be an ideal, and where for any $I \in \mathcal{I}(V)$, $*(I)$ noted I^*, is defined by

$$I^*(J) = \{f(\epsilon) \mid \epsilon \in J \text{ and } f \in I\}$$

Using $+$ and $*$ we can define the semantics of λ-abstractions and applications in $\mathcal{I}(V)$ as follows:

$$\begin{array}{rcl} [\![\lambda x \,.\, e]\!]_\rho & = & [\lambda \epsilon \,.\, [\![e]\!]_{\rho[\epsilon/x]}]^+ \\ [\![e_1(e_2)]\!]_\rho & = & [[\![e_1]\!]_\rho]^* ([\![e_2]\!]_\rho) \end{array}$$

On the other hand, using β-reduction we have:

$$(\lambda x \,.\, e_1)(e_2) =_\beta e_1[e_2/x]$$

Then if we want to have β-reduction as computational mechanism, the following equation must hold:

$$F^{+*} = F \tag{4}$$

where $F = \lambda \epsilon \,.\, [\![e]\!]_{\rho[\epsilon/x]}$.

A necessary condition for this equality to hold (see [SST90]) is that F must be an additive function, a morphism with respect to the union operator. However not all functions defined by λ-expressions are additive. A simple example of a non-additive function is the one defined by the expression $\lambda x \,.\, x \times x$. As can be seen in the following, this function does not satisfy equality (4) for the flat domain $N_\perp$ of natural numbers:

$$(\lambda x \,.\, x \times x)(N_\perp) = N_\perp \times N_\perp \neq \{(n, n) \mid n \in N_\perp\} = (\lambda x \,.\, x \times x)^{+*}(N_\perp)$$

This example makes clear that the set of functions from V to V can not catch the behavior of functions from $\mathcal{I}(V)$ to $\mathcal{I}(V)$. As can be seen by analyzing the example above, the operator $+$ must be defined using functions not from V to V but from $\mathcal{I}(V)$ to V. Then the basic domain of elements from which ideals are built can not be the solution of (3) but must be the solution of (2). Using the domain U defined by (2) the definition of the operators $+$ and $*$ which connect $\mathcal{I}(U) \to \mathcal{I}(U)$ and $\mathcal{I}(U)$ is now:

$$\begin{array}{rcl} F^+ & = & \{f : \mathcal{I}(U) \to U \mid f(I) \in F(I) \text{ for every } I \in \mathcal{I}(U)\} \\ I^*(X) & = & \overline{\{f(X) \mid f \in [\mathcal{I}(U) \to U] \cap I\}} \end{array}$$

An important result is that with this new definition it can be proved (see theorem 3.6) the following:

$$F^{+*} = F \text{ if and only if } F \text{ is a continuous function} \tag{5}$$

Then for the equality (5) to hold we must prove that λ-expressions define continuous functions on ideals. The proof relies on the fact that ideals are closed under least upper bounds of increasing sequences. This is one of the reasons that have led us to take the domain of closed ideals as semantic domain. It is easy to see that in a wider domain, the domain of order ideals for instance, the function F defined by $F(x) = [\lambda y \,.\, x]^+$ is not continuous. To prove it, let us take an

increasing sequence of ideals on the flat domain $N_\perp$, defined by $\{\{\perp, 0..n\}\}_{n\in N}$ with least upper bound $\bigsqcup_{n\in N}\{\perp, 0..n\} = {}^3N_\perp$. If F were continuous then the following equality would hold:

$$\begin{array}{rcl} F(\bigcup_{n\in N}\{\perp, 0..n\}) & = & \{f \mid \forall I \in \mathcal{H}(U)\ f(I) \in N_\perp\} \\ & \neq & \bigcup_{n\in N}\{f \mid \forall I \in \mathcal{H}(U)\ f(I) \in \{\perp, 0..n\}\} \\ & = & \bigcup_{n\in N} F(\{\perp, 0..n\}) \end{array}$$

However this equality is not true. The maximum function, defined as $max(\{\perp, 0..n\}) = n$ over these ideals, belongs to the left hand side but not to the right hand side. The order ideal defined by the right hand side contains an increasing sequence of functions $\{f_n\}_{n\in N}$ defined by $f_n(I) = max(I)$ if $max(I) \in \{\perp, 0..n\}$ or $f_n(I) = \perp$ otherwise, whose least upper bound is the maximum function, but as it is not closed the maximum function does not need belong to it. The conclusion is that we need the ideals to be closed in order to keep β-reduction as the operational semantics of the extended λ-calculus.

2 Domain construction

The semantics of the proposed extended λ-calculus (1) depends on the solution of the isomorphism equation (2) as shown in the previous section. Solutions to isomorphism equations like (3) are usually found using cpos. However, equation (2) introduces a new construction when compared with equation (3), the space of continuous functions $[\mathcal{I}(U) \to U]$. So, the U and $\mathcal{I}(U)$ domains are closely intertwined in equation (2). This fact makes it rather difficult to face the solution of (2) using only the properties of cpos. For instance, the proof of the continuity of functions relies on having a constructive way to calculate the least upper bounds (lub) of increasing sequences. There is no such constructive way to compute lubs for the set of ideals $\mathcal{I}(U)$ of a cpo U, even knowing that $\mathcal{I}(U)$ is a complete lattice (see lemma 2.7). As has been shown in [MPS86] when ideals are involved the suitable structure to work with is the category of domains, given that, the set of ideals of a domain is also a domain (see lemma 2.19). Domains allow to define a very useful closure operator which can be used to build the minimum ideal that contains a given set. This operator is used, for instance, to define the embeddings between the sets of ideals in the solution of equation (2). Given an embedding between cpos D and E, to prove that there exists an embedding between $\mathcal{I}(D)$ and $\mathcal{I}(E)$ we have needed to suppose that D and E are domains (see lemma 2.24). The closure operator has been also used to define the semantics of the application I^* (see definition 3.1). At the end of the section we use standard techniques to solve the equation (2).

2.1 Preliminary definitions

In this section we present some preliminary definitions.

Definition 2.1 *A poset $(D, \sqsubseteq_D)$ is said to be a Complete Partial Order (cpo) if*

1. *D has a minimum noted by $\perp_D$.*
2. *Every increasing sequence $\{x_i\}_{i\geq 0}$ has a least upper bound (lub), in D, noted by $\bigsqcup_{i\geq 0} x_i$.*

[3]The least upper bound of an increasing sequence of order ideals is given by their union.

Definition 2.2 *Given two cpos $(D, \sqsubseteq_D)$ and $(E, \sqsubseteq_E)$, a map $f : D \to E$ is said to be continuous if for every increasing sequence $\{X_i\}_{i\geq 0}$ of elements of D, $\bigsqcup_{i\geq 0} f(X_i) = f(\bigsqcup_{i\geq 0} X_i)$.*[4]

Definition 2.3 *Given a cpo $(D, \sqsubseteq_D)$, a subset $I \subseteq D$ is said to be an order ideal, noted $I \in \mathcal{H}(D)$, if*

1. *$I \neq \emptyset$.*
2. *If $y \sqsubseteq_D x$ and $x \in D$ then $y \in D$.*

Definition 2.4 *An order ideal $I \subseteq D$ is said to be a closed ideal (ideal for short), noted $I \in \mathcal{I}(D)$, if*

3. *For every increasing sequence $\{x_i\}_{i\geq 0}$ such that $x_i \in I$, $\bigsqcup_{i\geq 0} x_i \in I$.*

Definition 2.5 *Given two posets $(D, \sqsubseteq_D)$ and $(E, \sqsubseteq_E)$, the following posets can be defined:*

1. *The coalesced sum $(D+E, \sqsubseteq_{D+E})$ where $D+E \equiv \{(d, \perp_E) \mid d \in D\} \cup \{(\perp_D, e) \mid e \in E\}$ and $(d, e) \sqsubseteq_{D+E} (d', e')$ if and only if $d \sqsubseteq_D d'$ and $e \sqsubseteq_E e'$.*
2. *The smash product $(D \otimes E, \sqsubseteq_{D\otimes E})$ where $D \otimes E \equiv \{(d, e) \mid d \in D - \{\perp_D\} \wedge e \in E - \{\perp_E\}\} \cup \{(\perp_D, \perp_E)\}$ and $(d, e) \sqsubseteq_{D\otimes E} (d', e')$ if and only if $d \sqsubseteq_D d'$ and $e \sqsubseteq_E e'$.*
3. *The continuous function space $([D \to E], \sqsubseteq_{[D\to E]})$ where $f \sqsubseteq_{[D\to E]} g$ if and only if for any $x \in D$ we have $f(x) \sqsubseteq_E g(x)$.* [5]
4. *The order ideal set $(\mathcal{H}(D), \sqsubseteq_{\mathcal{H}(D)})$ where $A \sqsubseteq_{\mathcal{H}(D)} B$ if and only if $A \subseteq B$.*
5. *The closed ideal set $(\mathcal{I}(D), \sqsubseteq_{\mathcal{I}(D)})$ where $A \sqsubseteq_{\mathcal{I}(D)} B$ if and only if $A \subseteq B$.*

Lemma 2.6 *Given two cpos $(D, \sqsubseteq_D)$ and $(E, \sqsubseteq_E)$ the following posets are cpos:*

1. *The coalesced sum $(D + E, \sqsubseteq_{D+E})$ with bottom element $(\perp_D, \perp_E)$ and $\bigsqcup_{i\geq 0}(a_i, b_i) = (\bigsqcup_{i\geq 0} a_i, \bigsqcup_{i\geq 0} b_i)$ for the increasing sequence $\{(a_i, b_i)\}_{i\geq 0}$.*
2. *The smash product $(D \otimes E, \sqsubseteq_{D\otimes E})$ with $\perp_{D\otimes E} = (\perp_D, \perp_E)$ and $\bigsqcup_{i\geq 0}(a_i, b_i) = (\bigsqcup_{i\geq 0} a_i, \bigsqcup_{i\geq 0} b_i)$.*
3. *The function space $([D \to E], \sqsubseteq_{[D\to E]})$ with $[\perp_{[D\to E]}](x) = \perp_E$ for any $x \in D$ and $[\bigsqcup_{i\geq 0} f_i](x) = \bigsqcup_{i\geq 0}[f_i(x)]$.*
4. *The set of order ideals $(\mathcal{H}(D), \sqsubseteq_{\mathcal{H}(D)})$ with $\perp_{\mathcal{H}(D)} = \{\perp_D\}$ and $\bigsqcup_{i\geq 0} X_i = \bigcup_{i\geq 0} X_i$.*
5. *The set of closed ideals $(\mathcal{I}(D), \sqsubseteq_{\mathcal{I}(D)})$ with $\perp_{\mathcal{I}(D)} = \{\perp_D\}$ and $\bigsqcup_{i\geq 0} X_i = \bigcap\{Y \in \mathcal{I}(D) \mid X_i \subseteq Y \text{ for all } i \geq 0\}$.*

---

[4] *Note that f continuous implies f monotonic and, therefore, $\{f(X_i)\}_{i\geq 0}$ is an increasing sequence, so $\bigsqcup_{i\geq 0} f(X_i)$ exists.*

[5] *¿From now on we will use the convention*
$f : D \to E$ means that f maps elements of D to E and
$f \in [D \to E]$ is a stronger condition that means $f : D \to E$ and f is continuous.

Lemma 2.7 *Let $(\mathcal{I}(D), \sqsubseteq_{\mathcal{I}(D)})$ be the cpo of closed ideals of D. If X,$Y \in \mathcal{I}(D)$ then $X \cup Y$, $X \cap Y$, $X \otimes Y \in \mathcal{I}(D)$. Moreover $(\mathcal{I}(D), \bigcap, \bigvee)$ is a complete lattice where $\bigcap$ is the usual intersection and $\bigvee$ is defined by $\bigvee_{i \in I} X_i \equiv \bigcap\{Y \in \mathcal{I}(D) \mid X_i \subseteq Y \text{ for all } i \in I\}$.* [6]

Corollary 2.8 *For every finite set $\{a_1, \ldots, a_n\} \subset D$, the set $I_{(a_1,\ldots,a_n)} \equiv \{x \in D \mid$ there exists $a_i \in A$ such that $x \sqsubseteq a_i\}$ is a closed ideal. We will name $I_{(a_1,\ldots,a_n)}$ the ideal generated by $\{a_1, \ldots, a_n\}$.*

Definition 2.9 *Let D be a cpo and $x \in D$. We say that x is ω-finite if for any increasing sequence $\{a_i\}_{i \geq 0}$ with $x \sqsubseteq \bigsqcup_{i \geq 0} a_i$ there exists $k \in N$ such that $x \sqsubseteq a_k$.*

Definition 2.10 *Let D be a cpo.*

We say that D is consistently complete if every upper boundered set $X \subseteq D$ has least upper bound.

We say that D is ω-algebraic if

1. *D has countably many ω-finite elements.*
2. *For any $x \in D$ the set of ω-finite elements less than x is directed and has x as least upper bound.*

And, we say that D is a domain if

1. *D is consistently complete.*
2. *and D is ω-algebraic.*

Property 2.11 *[MPS86]*

1. *Countable flat cpos are domains.*
2. *The cpo constructors $+$, $\otimes$ and $[\_ \to \_]$ send domains to domains.*

Lemma 2.12 *Let D be a ω-algebraic cpo. For every $x \in D$ there exists an increasing sequence $\{x_i\}_{i \geq 0}$ of ω-finite elements of D with $\bigsqcup_{i \geq 0} x_i = x$.*

Proof: The set of ω-finite elements less than x is countable and directed. Let $\{a_1, \ldots, a_n, \ldots\}$ be this set. Because it is directed, we can construct the increasing chain $a_1 \sqsubseteq c_{1,2} \sqsubseteq \ldots \sqsubseteq c_{1,2,\ldots,n} \sqsubseteq \ldots$ where $c_{1,2,\ldots,n}$ is an upper bound of $\{c_{1,\ldots,n-1}, a_n\}$ belonging to the set of ω-finite elements less than x, that is, belonging to $\{a_1, \ldots, a_n, \ldots\}$. Thus, it's easy to see that $\bigsqcup_{i \geq 0} c_{1,\ldots,i} = x$. □

ω-algebraic elements of a domain are a countable base that generates all the domain elements using only the least upper bound operator $\bigsqcup$.

2.2 Constructing a domain of ideals

We will prove now that the $\mathcal{I}(\_)$ constructor also maps domains to domains, in order to ensure that the set of ideals of a domain forms also a domain.

[6] *In general, the infinite union of closed ideals is not a closed ideal.*

Definition 2.13 *For any set $X \in \mathcal{P}(D)$ we define:*

$$\begin{array}{rcl} X^0 & \equiv & \{x \in X \mid x \text{ is } \omega\text{-finite}\} \\ \overline{X} & \equiv & \{\bigsqcup_{i\geq 0} a_i \mid \{a_i\}_{i\geq 0} \text{is an increasing sequence in } X\} \end{array}$$

Property 2.14 *Let D be an ω-algebraic cpo.*

1. *The map $C : \mathcal{H}(D) \to \mathcal{H}(D)$ defined by $C(X) = \overline{X}$ is a closure operator.*
2. *For all $I \in \mathcal{I}(D)$ we have $\overline{I^0} = I$.*
3. *For all $H \in \mathcal{H}(D)$ we have $\overline{H}^0 = H^0$ and $\overline{H^0} = \overline{H}$.*
4. *For all ideal increasing sequence $\{I_i\}_{i\geq 0}$ in $\mathcal{I}(D)$ we have $\bigsqcup_{i\geq 0} I_i = \overline{\bigcup_{i\geq 0} I_i^0}$.*

Proof: It can be constructed easily from lemma 2.12. □

Definition 2.15 *A set X is said to be maximal complete if for every element $x \in X$, exists a maximal*[7] *element $m \in X$ such that $x \sqsubseteq m$.*

Fact 2.16

1. *The ideal $I_{(a_1,\ldots,a_n)}$ generated by the finite set $\{a_1,\ldots,a_n\}$ is maximal complete and the set of maximals of $I_{(a_1,\ldots,a_n)}$ is the set of maximals of $\{a_1,\ldots,a_n\}$.*
2. *If the ideal J is maximal complete, then it is generated by the set M of its maximal elements $J = I_M$.*

These properties allow us to characterize the ω-finite ideals of $\mathcal{I}(D)$.

Lemma 2.17 *An ideal $I \in \mathcal{I}(D)$ is ω-finite ($I \in \mathcal{I}(D)^0$) if and only if it is maximal complete, and the set of maximal elements is finite and contains only ω-finite elements.*

Proof:

$\Leftarrow$) Let $\{a_1,\ldots,a_n\}$ be the set of maximal elements, and let $I \subseteq \bigsqcup_{i\geq 0} A_i = \overline{\bigcup_{i\geq 0} A_i^0}$. For every maximal elements a_r we can say $a_r \in \overline{\bigcup_{i\geq 0} A_i^0}$. But, because a_r is an ω-finite element there exists $k_r \in N$ such that $a_r \in A_{k_r}$. There are a finite number of maximals, thus there exists $k = \max\{k_1,\ldots,k_n\}$ such that $a_i \in A_k$ for all $i = 1,\ldots,n$. Using fact 2.16 it is easy to see that $I \subseteq A_k$.

$\Rightarrow$) Because D is a domain, I^0 must be countable. Let $I^0 = \{a_i \mid i \in N\}$ be an enumeration of I^0, and $I_{(a_0)} \sqsubseteq I_{(a_0,a_1)} \sqsubseteq \ldots \sqsubseteq I_{(a_0,\ldots,a_n)} \sqsubseteq \ldots \sqsubseteq I$ be the sequence of ideals generated by $\{a_0\}$, $\{a_0,a_1\},\ldots,\{a_0,\ldots,a_n\},\ldots$ An easy computation shows that $I = \bigsqcup_{i\geq 0} I_{(a_0,\ldots,a_i)}$ and $I \not\sqsubseteq I_{(a_0,\ldots,a_i)}$ for all $i \in N$. Therefore, I is not an ω-finite ideal.
The first point can be proved by $\bigsqcup_{i\geq 0} I_{(a_0,\ldots,a_i)} = \overline{\bigcup_{i\geq 0} I^0_{(a_0,\ldots,a_i)}} = \overline{\bigcup_{i\geq 0}\{a_0,\ldots,a_i\}} = \overline{I^0} = I$.
The second point, $I \not\sqsubseteq I_{(a_0,\ldots,a_i)}$, is justified because fact 2.16 ensures that $I_{(a_0,\ldots,a_i)}$ satisfies the lemma conditions (is maximal complete and has a finite set of ω-finite maximal elements), and I does not satisfy these conditions. □

[7] *A maximal element x of a set X is an element of X with no other element in X greater than it.*

Lemma 2.18 *If D is ω-algebraic, $\mathcal{I}(D)$ is also ω-algebraic.*

Proof:

1. There are countably many ω-finite ideals because they are characterized by a finite number of ω-finite elements from D, and there are countably many of them.

2. The set of ω-finite ideals less than any $I \in \mathcal{I}(D)$ is directed. The proof is an easy consequence of the equality $I_{(a_1,\ldots,a_n)} \cup I_{(b_1,\ldots,b_m)} = I_{(a_1,\ldots,a_n,b_1,\ldots,b_m)}$.

3. The lub of such set is I.
We have to find an increasing sequence $\{I_i\}_{i\geq 0}$ such that

$$\bigsqcup_{i\geq 0} I_i = \overline{\bigcup_{i\geq 0} I_i^0} = \overline{I^0} = I$$

The set I has countably many ω-finite elements (because the number of such elements in the domain is countable). Let $a_1, \ldots, a_n, \ldots$ be an enumeration of them. Then we can construct the increasing sequence taking I_i equal to the ideal generated by $\{a_1, \ldots, a_i\}$. □

Theorem 2.19 *If D is a domain, $\mathcal{I}(D)$ is also a domain.*

Proof: If D is a domain, lemma 2.18 ensures that it is ω-algebraic, and lemma 2.7 proves the completeness. □

2.3 Embeddings connecting domains of ideals

Here we will define a functional $\hat{\mathcal{I}}$ that maps functions on domains to functions on the corresponding domain of ideals. We prove that the functional $\hat{\mathcal{I}}$ preserves embeddings, and other properties needed in the following subsection.

Definition 2.20 *Let E and D be cpos. A continuous map $\phi : D \to E$ is an embedding if there exists a continuous map $\phi^R : E \to D$ such that*

$$\begin{aligned} \phi^R \circ \phi &= id_D \\ \phi \circ \phi^R &\sqsubseteq id_E \end{aligned}$$

Definition 2.21 *Let $f : D \to E$ and $g : D' \to E'$ be embeddings. We define $f \hat{\otimes} g$, $f \hat{+} g$, and $f^R \hat{\to} g$ as usual, and*

$$\begin{array}{rrcl} f\hat{\otimes}g: & D \otimes D' & \to & E \otimes E' \\ & (x,y) & \to & (f(x), g(y)) \end{array}$$

$$\begin{array}{rrcl} f\hat{+}g: & D + D' & \to & E + E' \\ & x & \to & \begin{cases} (f(a), \bot_{E'}) & if\ x = (a, \bot_{D'}) \\ (\bot_E, g(b)) & if\ x = (\bot_D, b) \end{cases} \end{array}$$

$$\begin{array}{rrcl} f^R\hat{\to}g: & [D \to D'] & \to & [E \to E'] \\ & h & \to & g \circ h \circ f^R \end{array}$$

$$\begin{array}{rrcl} \hat{\mathcal{H}}(f): & \mathcal{H}(D) & \to & \mathcal{H}(E) \\ & A & \to & \{y \in E \mid \exists x \in A\ y \sqsubseteq f(x)\} \end{array}$$

$$\begin{array}{rrcl} \hat{\mathcal{I}}(f): & \mathcal{I}(D) & \to & \mathcal{I}(E) \\ & A & \to & \overline{\{y \in E \mid \exists x \in A\ y \sqsubseteq f(x)\}}^{8} \end{array}$$

Fact 2.22

$$\hat{\mathcal{I}}(f)_{(A)} = \overline{\{y \in E \mid \exists x \in A\ y \sqsubseteq f(x)\}} = \overline{\{y \in E^0 \mid \exists x \in A^0\ y \sqsubseteq f(x)\}}$$

Proof: Using $\overline{I} = \overline{I^0}$, that can be deduced from properties 2.14, we have

$$\overline{\{y \in E \mid \exists x \in A\ y \sqsubseteq f(x)\}} = \overline{\{y \in E^0 \mid \exists x \in A\ y \sqsubseteq f(x)\}}$$

Now, if x is not ω-finite, there exists an increasing sequence $\{x_i\}_{i \geq 0}$ of ω-finite elements with $x = \bigsqcup_{i \geq 0} x_i$. Using the continuity of f, $y \sqsubseteq f(x) = f(\bigsqcup_{i \geq 0} x_i) = \bigsqcup_{i \geq 0} f(x_i)$, and using the ω-finiteness of y, there exists $n \in N$ such that $y \sqsubseteq f(x_n)$, with $x_n \in A^0$, because $x_n \sqsubseteq x$ and A is an ideal set. Therefore, we can say that if there exists $x \in A$ with $y \sqsubseteq f(x)$, then there exists $x' \in A^0$ with $y \sqsubseteq f(x') \sqsubseteq f(x)$, which ensures:

$$\overline{\{y \in E^0 \mid \exists x \in A\ y \sqsubseteq f(x)\}} = \overline{\{y \in E^0 \mid \exists x \in A^0\ y \sqsubseteq f(x)\}}$$

□

Lemma 2.23 *Let $f : D \to E$ and $g : E \to F$ be continuous functions over domains then $\hat{\mathcal{I}}(g) \circ \hat{\mathcal{I}}(f) = \hat{\mathcal{I}}(g \circ f)$.*

[8] *In this definition we suppose in addition that D and E are domains.*

Proof:

$$\begin{aligned}
\hat{\mathcal{I}}(g) \circ \hat{\mathcal{I}}(f)_{(A)} &= \overline{\{z \in F^0 \mid \exists y \in \hat{\mathcal{I}}(f)_{(A)}{}^0 \; z \sqsubseteq g(y)\}} \\
&= \overline{\{z \in F^0 \mid \exists y \in \{y' \in E^0 \mid \exists x \in A^0 \; y' \sqsubseteq f(x)\} \; z \sqsubseteq g(y)\}} \\
&= \overline{\{z \in F^0 \mid \exists y \in E^0 \; \exists x \in A^0 \; y \sqsubseteq f(x) \text{ and } z \sqsubseteq g(y)\}} \\
&= \ldots
\end{aligned}$$

But, because $z \sqsubseteq g(y)$ and $y \sqsubseteq f(x)$, by the monotonicity of g we can ensure that $z \sqsubseteq g(f(x))$. Then

$$\ldots \subseteq \overline{\{z \in F^0 \mid \exists x \in A^0 \; z \sqsubseteq g(f(x))\}} = \hat{\mathcal{I}}(g \circ f)_{(A)}$$

In the other direction, from $z \sqsubseteq g(f(x))$ we have to find an ω-finite y such that $z \sqsubseteq g(y)$ and $y \sqsubseteq f(x)$. We already know that x and z are ω-finite. If $f(x)$ is ω-finite we can take $y \equiv f(x)$. If this is not the case, then there exists an increasing sequence $\{t_i\}_{i \geq 0}$ of ω-finite elements such that $f(x) = \bigsqcup_{i \geq 0} t_i$. Using the continuity of g we can say $z \sqsubseteq g(f(x)) \sqsubseteq g(\bigsqcup_{i \geq 0} t_i) = \bigsqcup_{i \geq 0} g(t_i)$. And using the ω-finiteness of z, there exists $n \in N$ such that $z \sqsubseteq g(t_n)$. We can take then $y \equiv t_n$, which ensures $y \sqsubseteq f(x)$ and the ω-finite of y, therefore we can say

$$\ldots \supseteq \overline{\{z \in F^0 \mid \exists x \in A^0 \; z \sqsubseteq g(f(x))\}} = \hat{\mathcal{I}}(g \circ f)_{(A)}$$

□

Lemma 2.24 *Let f and g be embeddings. Then the following functions are embeddings:*

1. *$f \hat{\otimes} g$, with $(f \hat{\otimes} g)^R = f^R \hat{\otimes} g^R$.*
2. *$f \hat{+} g$, with $(f \hat{+} g)^R = f^R \hat{+} g^R$.*
3. *$f^R \hat{\rightarrow} g$, with $(f^R \hat{\rightarrow} g)^R = f \hat{\rightarrow} g^R$.*
4. *$\hat{\mathcal{H}}(f)$ with $(\hat{\mathcal{H}}(f))^R = \hat{\mathcal{H}}(f^R)$.*
5. *$\hat{\mathcal{I}}(f)$ with $(\hat{\mathcal{I}}(f))^R = \hat{\mathcal{I}}(f^R)$.*
6. *$g \circ f$ with $(g \circ f)^R = f^R \circ g^R$.*

Proof: We will prove the $\hat{\mathcal{I}}$ case

1. If A is an ideal then $\hat{\mathcal{I}}(f)_{(A)}$ is also an ideal.
It's easy to see that $B \equiv \{y \in E \mid \exists x \in A \; y \sqsubseteq f(x)\}$ is an hereditary set because if $y' \in B$ then there exists $x \in A$ such that $y' \sqsubseteq f(x)$, and if $y \sqsubseteq y'$ we can find an $x \in A^0$ (the same x that for y') such that $y \sqsubseteq f(x)$ (which is the condition for $y \in B$).
The property 2.14 allows to prove that $\overline{\{y \in E \mid \exists x \in A \; y \sqsubseteq f(x)\}}$ is an ideal set of $\mathcal{I}(E)$ if E is a domain, because it is the closure of an order ideal of $\mathcal{H}(E)$.

2. If f is continuous then $\hat{\mathcal{I}}(f)$ is also continuous.
We have

$$\begin{aligned}
\hat{\mathcal{I}}(f)_{(\bigsqcup_{n \geq 0} A_n)} &= \overline{\{y \in E^0 \mid \exists x \in [\bigsqcup_{n \geq 0} A_n]^0 \; y \sqsubseteq f(x)\}} = \overline{\{y \in E^0 \mid \exists x \in \bigcup_{n \geq 0} A_n^0 \; y \sqsubseteq f(x)\}} \\
&= \overline{\bigcup_{n \geq 0} \{y \in E^0 \mid \exists x \in A_n^0 \; y \sqsubseteq f(x)\}} = \overline{\bigcup_{n \geq 0} \hat{\mathcal{I}}(f)_{(A_n)}} = \bigsqcup_{n \geq 0} \hat{\mathcal{I}}(f)_{(A_n)}
\end{aligned}$$

3. If f is an embedding then $\hat{\mathcal{I}}(f)$ is also an embedding, with $\hat{\mathcal{I}}(f)^R = \hat{\mathcal{I}}(f^R)$.
The function $\hat{\mathcal{I}}(f^R)$ is continuous because f^R is continuous; let us see that it satisfies the two relations. For the first one, using lemma 2.23 we have

$$\hat{\mathcal{I}}(f^R) \circ \hat{\mathcal{I}}(f)_{(A)} = \hat{\mathcal{I}}(f^R \circ f)_{(A)} = \overline{\{y \in D \mid \exists x \in A \;\; y \sqsubseteq f^R(f(x)) = x\}} = \overline{A} = A$$

because f is an embedding. For the second one, using the same lemma,

$$\hat{\mathcal{I}}(f) \circ \hat{\mathcal{I}}(f^R)_{(A)} = \hat{\mathcal{I}}(f \circ f^R)_{(A)} = \overline{\{y \in E \mid \exists x \in A \;\; y \sqsubseteq f(f^R(x)) \sqsubseteq x\}} \subseteq A$$

□

Fact 2.25 *Let $f : D \to E$ be an embedding between the domains D and E, and $A \in \mathcal{I}(D)$. For any ideal $I \in \mathcal{I}(E)$ verifying that for any $y \in I$ with $f^R(y) \in A$, we have $\hat{\mathcal{I}}(f)_{(A)} \subseteq I$.*

Lemma 2.26 *The functional $\hat{\mathcal{I}}$ is continuous, that is, for every increasing sequence $\{f_i\}_{i\geq 0}$ and every ideal $A \in \mathcal{I}(D)$, $\hat{\mathcal{I}}(\bigsqcup_{i\geq 0} f_i)_{(A)} = \bigsqcup_{i\geq 0} \hat{\mathcal{I}}(f_i)_{(A)}$ is satisfied.*

Proof:

$$\hat{\mathcal{I}}(\bigsqcup_{i\geq 0} f_i)_{(A)} = \overline{\{y \in E^0 \mid \exists x \in A^0 \;\; y \sqsubseteq [\bigsqcup_{i\geq 0} f_i](x) = \bigsqcup_{i\geq 0} f_i(x)\}} = \ldots$$

Using that y is ω-finite, we can say that there exists $n \in N$ such that $y \sqsubseteq f_n(x)$. Then

$$\overline{\{y \in E^0 \mid \exists x \in A^0 \;\; \exists n \in N \;\; y \sqsubseteq f_n(x)\}} = \overline{\bigcup_{i\geq 0} \hat{\mathcal{I}}(f_i)_{(A)}}^{\,0} = \bigsqcup_{i\geq 0} \hat{\mathcal{I}}(f_i)_{(A)}$$

□

In the domain construction it is shown why the continuity of all functionals between cpos is important.

2.4 Solving the isomorphism equation

Formally we define this semantic domain U as the least solution of the isomorphism:

$$U \cong K + U \otimes U + [\mathcal{I}(U) \to U]$$

To construct the semantic domain U we use an initial non empty domain of values $(K, \sqsubseteq_K)$, with bottom element $(\bot_K)$. In this domain we include all the predefined constants we want to have. It would be, for instance:

We enrich this initial domain with pairs and functions in order to construct our semantic domain.

To construct the domain U we will use the usual limiting process. We will base the construction in lemma 2 (the basic lemma) of [SP82]. Given a category K (in our case the category of domains), with initial object $\bot_K$, and a functor $F : K \to K$, this lemma ensures that there exists the initial

F-algebra (A, α), where $\alpha : FA \to A$, provided that $\mu : \Delta \to A$ and $F\mu : F\Delta \to FA$ are colimiting cones where Δ is the ω-chain $< F^n(\bot_K), F^n(\bot_{F_\bot}) >$.

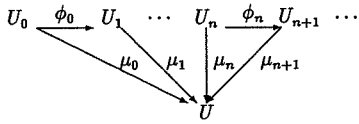
First we construct the domain chain Δ:

$$\begin{aligned} U_0 &= \{\bot\} \\ U_{n+1} &= K + U_n \otimes U_n + [\mathcal{I}(U_n) \to U_n] \end{aligned}$$

Connected by the embeddings $\phi_n : U_n \to U_{n+1}$ defined as:

$$\begin{aligned} \phi_0 &= id_{\{\bot\}} \\ \phi_{n+1} &= id_K \hat{+} (\phi_n \hat{\otimes} \phi_n) \hat{+} (\hat{\mathcal{I}}(\phi_n))^R \hat{\to} \phi_n) \end{aligned}$$

Then we define U as the colimit of the chain $< U_n, \phi_n >$ in the category of domains.



Definition 2.27 *The domain U is the set of sequences:*

$$U \equiv \{\{u_n\}_{n\geq 0} \mid u_n = \phi_n^R(u_{n+1}) \in U_n\}$$

This set has a domain structure with bottom element $\{\bot\}_{n\geq 0}$ and the pointwise order $\{u_n\}_{n\geq 0} \sqsubseteq_U \{v_n\}_{n\geq 0}$ if and only if for any $n \in N$ we have $u_n \sqsubseteq_{U_n} v_n$.

Lemma 2.28 *$\mu :< U_n, \phi_n > \to U$ is a colimiting cone.*

Proof: We complete the cone, taking:

$$\mu_n(u) = \{a_m\}_{m\geq 0} \text{ with } a_m = \begin{cases} \phi_m^R \circ \phi_{m+1}^R \circ \ldots \circ \phi_{n-1}^R(u) & \text{if } m < n \\ u & \text{if } m = n \\ \phi_{m-1} \circ \phi_{m-2} \circ \ldots \circ \phi_n(u) & \text{if } m > n \end{cases}$$

$$\mu_n^R(\{u_m\}_{m\geq 0}) = u_n$$

To prove that the cone exists we have to check

$$\begin{aligned} &\mu_n : U_n \to U \\ &\mu_n = \mu_{n+1} \circ \phi_n \end{aligned}$$

And to prove that U is its colimit we have to check that $\{\mu_n \circ \mu_n^R\}_{n\geq 0}$ is an increasing chain with least upper bound:

$$\bigsqcup_{n\geq 0} \mu_n \circ \mu_n^R = id_U$$

Let us see this equality:

$$\left(\bigsqcup_{i\geq 0} \mu_i \circ \mu_i^R\right)(\{u_n\}_{n\geq 0}) = \bigsqcup_{i\geq 0} \mu_i(u_i) = \bigsqcup_{i\geq 0} (u_0, u_1, \ldots, u_i, \phi_i(u_i), \phi_{i+1} \circ \phi_i(u_i), \ldots) = \{u_n\}_{n\geq 0}$$

because $\phi_n^R \circ \phi_{n+1}^R \circ \ldots \circ \phi_{i-1}^R(u_i) = u_n$ and $\phi_{n-1} \circ \phi_{n-2} \circ \ldots \circ \phi_i(u_i) \sqsubseteq u_n$. □

In order to construct the cone $F\mu$ we define the functor F in the category of domains,

$$\begin{aligned} F(D) &= K + D \otimes D + [\mathcal{I}(D) \to D] \\ F(f) &= id_K \hat{+} f \hat{\otimes} f \hat{+} (\hat{\mathcal{I}}(f))^R \hat{\to} f \end{aligned}$$

Lemma 2.29 *The functor F satisfies:*

1. *The functor F is well defined (maps embeddings between domains to embeddings between domains, maps the identity embedding into the identity embedding, and for every embeddings f and g, $F(f \circ g) = F(f) \circ F(g)$).*
2. *For any embedding f, $F(f^R) = F(f)^R$.*
3. *For any increasing sequence $\{f_i\}_{i\geq 0}$ of embeddings, $F(\bigsqcup_{i\geq 0} f_n) = \bigsqcup_{i\geq 0} F(f_n)$.*

Proof: These properties have been proved for the $\hat{\to}$, $\hat{\otimes}$, $\hat{+}$ and $\circ$ cases [MPS86]; then, we only need to prove the case $\hat{\mathcal{I}}(f)$.

1. The third property is a particular case of lemma 2.23.
2. It has been proved in lemma 2.24.
3. This continuity condition is ensured by lemma 2.26. □

The cone $F\mu$ is composed by the domain chain

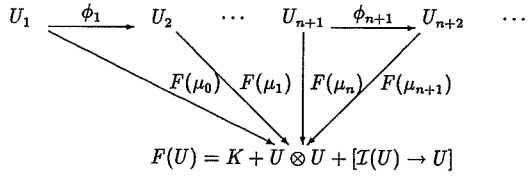
$$F(U_n) = K + U_n \otimes U_n + [\mathcal{I}(U_n) \to U_n] = U_{n+1}$$

connected by the embeddings

$$F(\phi_n) = id_K \hat{+} \phi_n \hat{\otimes} \phi_n \hat{+} (\hat{\mathcal{I}}(\phi_n))^R \hat{\to} \phi_n = \phi_{n+1}$$

That is, the same cone shifted a position to the right.
For the cone $F\mu$ we can prove the following lemma:

Lemma 2.30 *$F(\mu)$ is a cone with colimit $F(U) = K + U \otimes U + [\mathcal{I}(U) \to U]$.*



Proof: We have to prove that

$$\begin{aligned} F(\mu_n) &: F(U_n) \to F(U) \\ F(\mu_n) &= F(\mu_{n+1}) \circ F(\phi_n) \end{aligned}$$

and that $\{F(\mu_n) \circ F(\mu_n)^R\}_{n\geq 0}$ is an increasing sequence with

$$\bigsqcup_{n\geq 0} F(\mu_n) \circ F(\mu_n)^R = id_{F(U)}$$

This last fact can be proved checking the equality chain

$$\bigsqcup_{n\geq 0} F(\mu_n)\circ F(\mu_n)^R = \bigsqcup_{n\geq 0} F(\mu_n)\circ F(\mu_n^R) = \bigsqcup_{n\geq 0} F(\mu_n\circ\mu_n^R) = F\left(\bigsqcup_{n\geq 0}\mu_n\circ\mu_n^R\right) = F(id_U) = id_{F(U)}$$

that is a direct consequence of lemma 2.29 □

Lemma 2.28, lemma 2.30, and basic lemma 2 of [SP82] allow us to ensure the following theorem.

Theorem 2.31 *The domain U is the initial fixed point of $U \equiv K + U\otimes U + [\mathcal{I}(U)\to U]$, where the isomorphism is given by*

$$\theta = \bigsqcup_{n\geq 0} F(\mu_n)\circ\mu_{n+1}^R$$

and its inverse by

$$\theta^{-1} = \bigsqcup_{n\geq 0}\mu_{n+1}\circ F(\mu_n^R)$$

Using theorem 2.19 we have that $\mathcal{I}(U)$ is also a domain.

3 The set $[\mathcal{I}(U)\to\mathcal{I}(U)]$ and its connection with $\mathcal{I}(U)$

In this section the connection between continuous functions from ideals to ideals and ideals of continuous functions is studied by means of the operators $+$ and $*$. These operators

$$\begin{aligned} + &: (\mathcal{I}(U)\to\mathcal{I}(U))\to\mathcal{I}(U)\\ * &: \mathcal{I}(U)\to(\mathcal{I}(U)\to\mathcal{I}(U))\end{aligned}$$

restricted to continuous functions $[\mathcal{I}(U)\to U]$ define a Galois connection between domains because they are monotonic and $F^{+*} = F$ and $I^{*+}\supseteq I$ for any $F\in[\mathcal{I}(U)\to\mathcal{I}(U)]$ and any $I\in\mathcal{I}(U)$.

These operators will be used to give semantics to λ-abstraction and application, and their properties assure the soundness of β-reduction and a condition for the soundness of η-reduction.

Definition 3.1 *Let $F:\mathcal{I}(U)\to\mathcal{I}(U)$ be a function between ideals, and $X, I\in\mathcal{I}(U)$ be ideals, the operators $+$ and $*$ are defined by:*

$$F^+ \equiv \{f\in[\mathcal{I}(U)\to U] \mid f(X)\in F(X) \text{ for every } X\in\mathcal{I}(U)\}$$

$$I^*(X) \equiv \overline{\{f(X)\mid f\in[\mathcal{I}(U)\to U]\cap I\}}$$

It is evident that the operators $+$ and $*$ are monotonic (if $F\sqsubseteq G$ then $F^+\subseteq G^+$ and if $I\subseteq J$ then $I^*\sqsubseteq J^*$). It can also be proved that they have the intended functionality.

Property 3.2 *The $+$ and $*$ operators satisfy:*

1. *If $F:\mathcal{I}(U)\to\mathcal{I}(U)$ then $F^+\in\mathcal{I}(U)$.*
2. *If $I\in\mathcal{I}(U)$ then $I^*:\mathcal{I}(U)\to\mathcal{I}(U)$.*

Proof:

1. If $F : \mathcal{I}(U) \to \mathcal{I}(U)$ then $F^+ \in \mathcal{I}(U)$.

(i) Let us prove $F^+ \in \mathcal{H}(U)$.
Suppose that $f \in F^+$ and $g \sqsubseteq f$. For any $\epsilon \in \mathcal{I}(U)$ we have $g(\epsilon) \sqsubseteq f(\epsilon) \in F(\epsilon)$. If $F(\epsilon)$ is an order ideal we can say $g(\epsilon) \in F(\epsilon)$, which ensures that $g \in F^+$.

(ii) Let us prove $\overline{F^+} = F^+$.
Suppose that $f \in \overline{F^+}$, then there exists an increasing sequence $\{f_i\}_{i\geq 0}$ with $\bigsqcup_{i\geq 0} f_i = f$ and $f_i \in F^+$ for any $i \in N$. This second condition allows us to say for any $\epsilon \in \mathcal{I}(U)$ that $f_i(\epsilon) \in F(\epsilon)$. And using the closeness of $F(\epsilon)$ for the increasing sequence $\{f_i(\epsilon)\}_{i\geq 0}$, $[\bigsqcup_{i\geq 0} f_i](\epsilon) = \bigsqcup_{i\geq 0}[f_i(\epsilon)] \in F(\epsilon)$ therefore $f = \bigsqcup_{i\geq 0} f_i \in F^+$.

2. If $I \in \mathcal{I}(U)$ then $I^* : \mathcal{I}(U) \to \mathcal{I}(U)$.

(i) Let us define $I^{**}(X) \equiv \{f(X) \mid \forall f : \mathcal{I}(U) \to U \;\; f \in M\}$. which satisfies $I^*(X) = \overline{I^{**}(X)}$.
We will prove the functionality $I^{**} : \mathcal{H}(U) \to \mathcal{H}(U)$.
Suppose $p \in I^{**}(X)$, then, it has to exists $f \in I$ such that $p = f(X)$. We prove that for every $q \sqsubseteq p$ there exists $g \in I$ with $g(X) = q$.
Lemma 2.12 allows us to suppose the existence of an increasing sequence $\{q_i\}_{i\geq 0}$ of ω-algebraic values with $\bigsqcup_{i\geq 0} q_i = q$. With this sequence we can define

$$g(\epsilon) = \begin{cases} \max_{i\geq 0}\{q_i \mid q_i \sqsubseteq f(\epsilon)\} & \text{if } q \not\sqsubseteq f(\epsilon) \\ q & \text{if } q \sqsubseteq f(\epsilon) \end{cases}$$

where the maximum is always computable if $q \not\sqsubseteq f(\epsilon)$, and $g \sqsubseteq g$, which ensures $g \in I$.
It is evident, by the definition of g, that $g(X) = q$, because $q \sqsubseteq p = f(X)$.
Let us prove that g is continuous, by cases.
If $g(\overline{\bigcup_{i\geq 0} X_i}) = q_n$ then $q_n \sqsubseteq f(\overline{\bigcup_{i\geq 0} X_i}) = \bigsqcup_{i\geq 0} f(X_i)$, using the definition of the function cases and the continuity of f. Now, using that q_n is ω-finite, there exists $L \in N$ with $q_n \sqsubseteq f(X_L)$. Thus, using the definition of g and the definition of lub, we can say $q_n \sqsubseteq g(X_L) \sqsubseteq \bigsqcup_{l\geq 0} g(X_l)$.
If $g(\overline{\bigcup_{i\geq 0} X_i}) = q$ then $q \sqsubseteq f(\overline{\bigcup_{i\geq 0} X_i}) = \bigsqcup_{i\geq 0} f(X_i)$. For any $k \in N$ we have $q_k \sqsubseteq q \sqsubseteq \bigsqcup_{i\geq 0} f(X_i)$, and using the same lemma, there exists $L \in N$ such that $q_k \sqsubseteq f(X_L)$. This condition, by the definition of g, ensures $q_k \sqsubseteq g(X_L) \sqsubseteq \bigsqcup_{l\geq 0} g(X_l)$. Now, using $q = \bigsqcup_{k\geq 0} q_k$ and the definition of lub, $g(\overline{\bigcup_{i\geq 0} X_i}) = q = \bigsqcup_{k\geq 0} q_k \sqsubseteq \bigsqcup_{l\geq 0} g(X_l)$.
The inclusion $\bigsqcup_{i\geq 0} g(X_I) \sqsubseteq g(\overline{\bigcup_{i\geq 0} X_i})$ is proved by the evident monotonicity of g.

(ii) Let us prove $I^* : \mathcal{I}(U) \to \mathcal{I}(U)$.
If $X \in \mathcal{I}(U)$ then $X \in \mathcal{H}(U)$, and, as we have seen in the previous point, $I^{**}(X) \in \mathcal{H}(U)$. Using properties 2.14 we have $I^*(X) = \overline{I^{**}(X)} \in \mathcal{I}(U)$.

□

Lemma 3.3 *The function $I^* : \mathcal{I}(U) \to \mathcal{I}(U)$ is continuous.*

Proof:

Case $I^*(\bigsqcup_{i\geq 0} X_i) \subseteq \bigsqcup_{i\geq 0} I^*(X_i)$**:**
Let us prove first $I^{**}(\bigsqcup_{i\geq 0} X_i) \subseteq \bigsqcup_{i\geq 0} I^{**}(X_i)$.
Suppose $p \in I^{**}(\bigsqcup_{i\geq 0} X_i)$ then there exists $g \in I$ with $g(\overline{\bigcup_{i\geq 0} X_i}) = p$. By the continuity of g we have $p = \bigsqcup_{i\geq 0} g(X_i)$. For any $j \in N$ evidently $g(X_j) \in \{f(X_j) \mid f \in I\} = I^{**}(X_j) \subseteq \bigcup_{i\geq 0} I^{**}(X_i)$. And by the definition of closure, $p = \bigsqcup_{j\geq 0} g(X_j) \in \overline{\bigcup_{i\geq 0} I^{**}(X_i)}$.

Now, we can say $I^*(\bigsqcup_{i\geq 0} X_i) = \overline{I^{**}(\bigsqcup_{i\geq 0} X_i} \subseteq \overline{\bigsqcup_{i\geq 0} I^{**}(X_i)} = \bigsqcup_{i\geq 0} I^{**}(X_i) \subseteq \bigsqcup_{i\geq 0} I^*(X_i)$.
Case $\bigsqcup_{i\geq 0} I^*(X_i) \subseteq I^*(\bigsqcup_{i\geq 0} X_i)$:
Using $\bigcup_{i\geq 0} I^*(X_i) \subseteq I^*(\overline{\bigcup_{i\geq 0} X_i})$, that can be proved by the monotonicity and closeness of $\mathcal{I}^*$, we have $\overline{\bigcup_{i\geq 0} I^*(X_i)} \subseteq \overline{I^*(\overline{\bigcup_{i\geq 0} X_i})} = I^*(\overline{\bigcup_{i\geq 0} X_i})$. □

Now we will prove some interesting results about the operators + and $*$, and the relation between them.

Fact 3.4 *For any $F,G : \mathcal{I}(U) \to \mathcal{I}(U)$ we have $(F \cap G)^+ = F^+ \cap G^+$.*

Proof: Both membership conditions $\forall X \in \mathcal{I}(U)\ f(x) \in F(X) \cap G(X)$ and $\forall Y \in \mathcal{I}(U)\ f(Y) \in F(Y) \wedge \forall Z \in \mathcal{I}(U)\ f(Z) \in F(Z)$ are equivalent. □

There is no relation between $F^+ \otimes G^+$ and $(F \otimes G)^+$ because $F^+ \otimes G^+$ is a set of function pairs and $(F \otimes G)^+$ is a set of functions that return pairs. For the $\cup$ case only one direction of inclusion is satisfied.

Lemma 3.5 *For any $F : \mathcal{I}(U) \to \mathcal{I}(U)$ and any $X \in \mathcal{I}(U)$, $F^{+*}(X) \subseteq F(X)$.*
For any $I \in \mathcal{I}(U)$, $I^{*+} \supseteq I$.

Theorem 3.6 *For any $F : \mathcal{I}(U) \to \mathcal{I}(U)$:*

$$F^{+*} = F \quad \textit{if and only if} \quad F \textit{ is continuous}$$

Proof:

$\Rightarrow$ If the equality is satisfied, taking into account that F^+ is an ideal, and that $*$ constructs continuous functions from ideals (as ensures lemma 3.3), F will be a continuous function.

$\Leftarrow$ The inclusion $F^{+*} \subseteq F$ is ensured by lemma 3.5; we will prove the inclusion $F^{+*} \supseteq F$.
Let $p \in F(A)$ and $\{p_i\}_{i\geq 0}$ be an increasing sequence of ω-finite elements with $\bigsqcup_{i\geq 0} p_i = p$. We define

$$\begin{array}{rcl} f: \mathcal{I}(U) & \to & U \\ X & \to & \begin{cases} p & \text{if } p \in F(X) \\ \max_{i\geq 0}\{p_i \mid p_i \in F(X)\} & \text{if } p \notin F(X) \end{cases}^{9} \end{array}$$

It is evident that $f \in F^+$ and $f(A) = p$. We have to prove that f is continuous.
The inclusion $\bigsqcup_{i\geq 0} f(X_i) \sqsubseteq f(\bigsqcup_{i\geq 0} X_i)$ is ensured by the evident monotonicity of f. The inverse inclusion will be proved by cases.
Suppose $f(\overline{\bigcup_{i\geq 0} X_i}) = p_k$ for any $k \in N$ then we have $p_k \in \overline{\bigcup_{i\geq 0} F(X_i)}$ but because p_k is ω-finite we have $p_k \in \bigcup_{i\geq 0} F(X_i)$. Then there exists $l \in N$ such that $p_k \in F(X_l)$. Using the definition of f, $p_k \sqsubseteq f(X_l)$. And, by the lub properties:

$$f(\overline{\bigcup_{i\geq 0} X_i}) = p_k \sqsubseteq \bigsqcup_{l\geq 0} f(X_l)$$

[9] This maximum element exist because if $p_i \in F(X)$ for any $i \in N$ then $p \in F(X)$ because $F(X) \in \mathcal{I}(U)$ and it is closed under increasing sequences.

Suppose that $f(\overline{\bigcup_{i\geq 0} X_i}) = p$ then, by the definition of f and continuity of F:

$$p_k \sqsubseteq p \in F(\overline{\bigcup_{i\geq 0} X_i}) = \overline{\bigcup_{i\geq 0} F(X_i)}$$

and using that p_k is ω-finite we have for any $k \in N$ that $p_k \in \bigcup_{i\geq 0} F(X_i)$ or what its the same, there exists $L \in N$ such that $p_k \in F(X_L)$, that is, $p_k \sqsubseteq f(X_L)$. Now, using the lub properties:

$$f(\overline{\bigcup_{i\geq 0} X_i}) = p = \bigsqcup_{k\geq 0} p_k \sqsubseteq \bigsqcup_{l\geq 0} f(X_l)$$

□

This theorem will be used to prove β-reduction soundness. It says that the $*$ operator is the inverse of $+$. The $+$ operator is a morphism for the $\cap$, but not for the other operations.

Theorem 3.7 *For any $I \in \mathcal{I}(U)$*

$I^{*+} = I$ *if and only if* I *satisfies that* $[\forall \epsilon \in \mathcal{I}(U)\ \exists g \in I\ f(\epsilon) = g(\epsilon)]$ *implies* $f \in I$

This theorem makes explicit the conditions in which the η-reduction is valid.
We will prove the existence of fix point for the recursive definitions.

Theorem 3.8 *(Least fix point theorem)*
Let $F : \mathcal{I}(U) \to \mathcal{I}(U)$ be a continuous function then there exists $A \in \mathcal{I}(U)$ such that:

1. *It is a fix point, $F(A) = A$.*
2. *It is the least fix point, $\forall B \in \mathcal{I}(U)\ F(B) = B \Rightarrow A \subseteq B$.*

Proof: Let us define the sequence $\{A_n\}_{n\geq 0}$ as:

$$\begin{aligned} A_0 &= \{\bot_U\} \\ A_{n+1} &= F(A_n) \end{aligned}$$

Starting from $\{\bot_U\} \subseteq F(\{\bot_U\})$, by induction and the monotonicity of F we can prove $A_n \subseteq A_{n+1}$ for any $n \in N$. Thus, $\{A_n\}_{n\geq 0}$ is an increasing sequence, and it has to have lub. Let us define A as this lub

$$A = \bigsqcup_{n\geq 0} A_n$$

1. $A = F(A)$
Using the continuity of F and the definition of A_n, $A = \bigsqcup_{n\geq 1} A_n = \bigsqcup_{n\geq 0} F(A_n) = F(\bigsqcup_{n\geq 0} A_n) = F(A)$

2. $\forall B \in \mathcal{I}(U)\ F(B) = B \Rightarrow A \subseteq B$
We have $\{\bot_U\} \subseteq B$. If $A_n \subseteq B$, by monotonicity, $A_{n+1} = F(A_n) \subseteq F(B) = B$. And by induction $A_n \subseteq B$ for any $n \in N$. Using the definition of lub we have $A \equiv \bigsqcup_{n\geq 0} A_n \subseteq B$. □

4 A model for the extended λ-calculus with refinement

We give the semantic rules to map the language expressions over the semantic domain.

The semantic domain is:

$$\mathcal{D} = \mathcal{I}(U)$$

The semantic function is parametric in the valuation. These functions map identifiers to domain values:

$$\rho : Ident \to \mathcal{I}(U)$$

The semantic function is:

$$\xi : Expressions \to [Ident \to \mathcal{I}(U)] \to \mathcal{I}(U)$$

Defined by cases:

$$\begin{array}{lcl}
\xi[\![error]\!]_\rho & = & \{\bot_U\} \\
\xi[\![top]\!]_\rho & = & U \\
\xi[\![x]\!]_\rho & = & \rho[\![x]\!] \\
\xi[\![A \cup B]\!]_\rho & = & \xi[\![A]\!]_\rho \cup \xi[\![B]\!]_\rho \\
\xi[\![A \cap B]\!]_\rho & = & \xi[\![A]\!]_\rho \cap \xi[\![B]\!]_\rho \\
\xi[\![A \times B]\!]_\rho & = & \xi[\![A]\!]_\rho \otimes \xi[\![B]\!]_\rho \\
\xi[\![fst\ (A)]\!]_\rho & = & fst\ ([\![A]\!]_\rho) \\
\xi[\![scd\ (A)]\!]_\rho & = & scd\ ([\![A]\!]_\rho) \\
\xi[\![\lambda x.A]\!]_\rho & = & (\lambda\, \epsilon\, .\, \xi[\![A]\!]_{\rho[\epsilon/x]})^+ \\
\xi[\![A(B)]\!]_\rho & = & (\xi[\![A]\!]_\rho)^* (\xi[\![B]\!]_\rho) \\
\xi[\![\mu x.A]\!]_\rho & = & \bigsqcup_{n \geq 0} (\lambda\, \epsilon\, .\, \xi[\![A]\!]_{\rho[\epsilon/x]})^n (\{\bot_U\})
\end{array}$$

Where $\rho[\epsilon/x]$ is the valuation ρ, except that it maps x to ϵ.

Definition 4.1 *The n-ary function $F : \mathcal{I}(U)^n \to \mathcal{I}(U)$ is defined by an expression A with $x_1, \ldots, x_n$ as free variables, if it assigns $F(I_1, \ldots, I_n) = \xi[\![A]\!]_{[I_1/x_1, \ldots, I_n/x_n]}$. We will note the set of n-ary functions defined by an expression by $\mathcal{F}^n$.*

Fact 4.2 *The set $\mathcal{F}^n$ of n-ary functions defined by an expression is the smallest set such that*

1. *If $F(x_1, \ldots, x_n) = K$ for any $K \in \mathcal{I}(U)$ then $F \in \mathcal{F}^n$.*
2. *If $F(x_1, \ldots, x_n) = x_i$ then $F \in \mathcal{F}^n$.*
3. *For every $F, G \in \mathcal{F}^n$, $F \cup G, F \cap G, F \otimes G, fst(F), scd(F)$ and $F^*(G) \in \mathcal{F}^n$.*
4. *For every $F(x_1, \ldots, x_{n+1}) \in \mathcal{F}^{n+1}$,*
   $[\lambda\, x_{n+1}\, .\, F(x_1, \ldots, x_{n+1})]^+$ and $\bigsqcup_{n \geq 0} [\lambda\, x_{n+1}\, .\, F(x_1, \ldots, x_{n+1})]^n (\{\bot_U\}) \in \mathcal{F}^n$.

Lemma 4.3 *If F is defined by an expression then it is continuous.*

Proof: For the two firsts cases, and for $\cup$, $\cap$, $\otimes$, $fst(\ )$, $scd(\ )$, this result is evident. We will focus our attention in the other cases. In them, the assigned result $F(X_1,\ldots,X_n)$ is one of the following:

1. $F(X_1,\ldots,X_n) = [\lambda Y\,.\,G(X_1,\ldots,X_n,Y)]^+$
We have to check

$$[\lambda Y\,.\,G(\bigsqcup_{i\geq 0} X_i, Y)]^+ = \bigsqcup_{i\geq 0}[\lambda Y\,.\,G(X_i,Y)]^+$$

Case $\supseteq$:
This inclusion is easy to prove by the monotonicity and closeness of the constructor. The same reasoning will be used in the other cases.
By monotonicity we can prove, for any $i \in N$,

$$[\lambda Y\,.\,G(X_i,Y)]^+ \subseteq [\lambda Y\,.\,G(\bigsqcup_{j\geq 0} X_j, Y)]^+$$

And using the properties of the union and the closeness of the operator $+$,

$$\overline{\bigcup_{i\geq 0}[\lambda Y\,.\,G(X_i,Y)]^+} \subseteq [\lambda Y\,.\,G(\bigsqcup_{j\geq 0} X_j, Y)]^+$$

Case $\subseteq$:
If $f \in F(\bigsqcup_{i\geq 0} X_i) = [\lambda Y\,.\,G(\bigsqcup_{i\geq 0} X_i, Y)]^+$ then

$$\forall \epsilon \in \mathcal{I}(U)\ \ f(\epsilon) \in G(\bigsqcup_{k\geq 0} X_k, \epsilon)$$

For every $f(\epsilon)$ there exists an increasing sequence $\{q_i^{(\epsilon)}\}_{i\geq 0}$ of ω-finite elements with $\bigsqcup_{i\geq} q_i^{(\epsilon)} = f(\epsilon)$. Working with it we can say

$$\forall i \in N\ \ \forall \epsilon \in \mathcal{I}(U)\ \ \exists k \in N\ \ q_i^{(\epsilon)} \in G(X_k, \epsilon)$$

Let us see how we can construct an increasing sequence $\{f_n\}_{n\geq 0}$ of continuous functions with $f = \bigsqcup_{n\geq 0} f_n$ and for any $n \in N$ and ϵ, $f_n(\epsilon) \in G(X_n, \epsilon)$. We define this function sequence as

$$f_n(\epsilon) \equiv \begin{cases} f(\epsilon) & \text{if } f(\epsilon) \in G(X_n,\epsilon) \\ \max_{i\geq 0}\{q_i^{(\epsilon)} \mid q_i^{(\epsilon)} \in G(X_n,\epsilon)\} & \text{otherwise} \end{cases}$$

The condition $\bigsqcup_{n\geq 0} f_n = f$ is ensured by the fact that for any i and ϵ there exists a k such that $q_i^{(\epsilon)} \in G(X_k,\epsilon)$. It is enough to ensure the existence of a k such that $q_i^{(\epsilon)} \sqsubseteq f_k(\epsilon)$ for any ϵ and i. To prove that f_n are continuous functions we can follow a reasoning similar to that used in theorem 3.6, to prove the f continuity, and based on the continuity of $G(X_n,\epsilon)$ on ϵ.

2. $F(X_1,\ldots,X_n) = [G(X_1,\ldots,X_n)]^*[H(X_1,\ldots,X_n)]$.
We have to check

$$G(\bigsqcup_{i\geq 0} X_i)^*(H(\bigsqcup_{j\geq 0} X_j)) \subseteq \bigsqcup_{k\geq 0} G(X_k)^*(H(X_k))$$

because the other inclusion is ensured by the evident monotonicity.
We have, using the continuity of f and the hypothesis of induction, that

$$G(\bigsqcup_{i\geq 0} X_i)^*(H(\bigsqcup_{j\geq 0} X_j)) = \{f(H(\bigsqcup_{i\geq 0} X_i)) \mid \forall f \in G(\bigsqcup_{j\geq 0} X_i)\} = \{\bigsqcup_{i\geq 0} f(H(X_i)) \mid \forall f \in \bigsqcup_{j\geq 0} G(X_j)\}$$

Taking into account that f can be expressed as the least upper bound of an increasing sequence, we have

$$\ldots = \{\bigsqcup_{i\geq 0}\bigsqcup_{k\geq 0} f_k(H(X_i)) \mid \forall\{f_k\}_{k\geq 0} \in \bigcup_{j\geq 0} G(X_j)\}$$

The double sequence $\{f_k(H(X_i))\}_{k\geq 0, i\geq 0}$ can be transformed into a simple sequence belonging to

$$\bigcup_{i\geq 0}\{f(H(X_i)) \mid f \in \bigcup_{j\geq 0} G(X_j)\} = \bigcup_{i\geq 0}\{f(H(X_i)) \mid f \in G(X_i)\}$$

Thus, its lub $\bigsqcup_{k\geq 0, i\geq 0} f_k(H(X_i))$ belongs to

$$\overline{\bigcup_{i\geq 0}\{f(H(X_i)) \mid f \in G(X_i)\}} = \bigsqcup_{i\geq 0} G(X_i)^*(H(X_i))$$

3. $F(X_1,\ldots,X_n) = \bigsqcup_{n\geq 0}[\lambda Y\,.\,G(X_1,\ldots,X_n,Y)]^n[H(X_1,\ldots,X_n)]$.
Let us follow the equality chain:

$$\begin{aligned} F(\bigsqcup_{i\geq 0} X_i) &= \bigsqcup_{n\geq 0}[\lambda Y\,.\,G(\bigsqcup_{i\geq 0} X_i, Y)]^n H(\bigsqcup_{j\geq 0} X_j) \\ &= \bigsqcup_{n\geq 0} G(\bigsqcup_{i_1\geq 0} X_{i_1}, G(\bigsqcup_{i_2\geq 0} X_{i_2}, \cdots G(\bigsqcup_{i_n\geq 0} X_{i_n}, H(\bigsqcup_{j\geq 0} X_j))\cdots)) \end{aligned}$$

Appling the continuity property to G and H we obtain

$$\ldots = \bigsqcup_{n\geq 0}\bigsqcup_{i_1\geq 0}\bigsqcup_{i_2\geq 0}\cdots\bigsqcup_{i_n\geq 0}\bigsqcup_{j\geq 0} G(X_{i_1}, G(X_{i_2},\cdots G(X_{i_n}, H(X_j))\cdots))$$

and, taking into account that

$$G(X_{i_1}, G(X_{i_2},\cdots G(X_{i_n}, H(X_j))\cdots)) \subseteq G(X_k, G(X_k,\cdots G(X_k, H(X_k))\cdots))$$

where $k = \max\{i_1,\ldots,i_n,j\}$, we have

$$\ldots = \bigsqcup_{n\geq 0}\bigsqcup_{k\geq 0} G(X_k, G(X_k,\cdots G(X_k, H(X_k))\cdots)) = \bigsqcup_{n\geq 0}\bigsqcup_{k\geq 0}[\lambda Y\,.\,G(X_k,Y)]^n(H(X_k))$$

and changing the order between the two limits

$$\ldots = \bigsqcup_{k\geq 0}\bigsqcup_{n\geq 0}[\lambda Y\,.\,G(X_k,Y)]^n(H(X_k)) = \bigsqcup_{k\geq 0} F(X_k)$$

This change can be done because

$$\bigsqcup_{i\geq 0}\bigsqcup_{j\geq 0} A_{ij} = \overline{\bigcup_{i\geq 0}\bigcup_{j\geq 0} A^0_{ij}}^{0} = \overline{\bigcup_{i\geq 0, j\geq 0} A^0_{ij}} = \overline{\bigcup_{j\geq 0}\bigcup_{i\geq 0} A^0_{ij}}^{0} = \bigsqcup_{j\geq 0}\bigsqcup_{i\geq 0} A_{ij}$$

□

We use the definition 11.3 of [HS86] for λ-calculus models. We define application as:

$$p \circ q = p^*(q)$$

With this definition, the following theorem can be proved.

Theorem 4.4 *$< \mathcal{I}(U_K), \circ, \xi[\![\ ]\!] >$ is a model for the $\lambda\beta$-calculus for every initial domain K used to build U.*

Proof: We have to check that the following conditions are satisfied:

1. $\xi[\![x]\!]_\rho = \rho(x)$ for all variable x. This is trivial for the definition of $\xi[\![\ ]\!]$.

2. $\xi[\![P\ Q]\!]_\rho = (\xi[\![P]\!]_\rho)^*(\xi[\![Q]\!]_\rho) = \xi[\![P]\!]_\rho \circ \xi[\![Q]\!]_\rho$.

3. Using the definition of $\circ$ we have $\xi[\![\lambda\, x\,.\,P]\!]_\rho \circ d = (\xi[\![P]\!]_\rho(x))^{+*}(d)$, and using the theorem 3.6 $(\xi[\![P]\!]_\rho(x))^{+*}(d) = (\xi[\![P]\!]_\rho(x))(d) = \xi[\![P]\!]_{[d/x]\rho}$.

4. $\xi[\![M]\!]_\rho = \xi[\![M]\!]_\sigma$ if $\rho(x) = \sigma(x)$ for all $x \in FV(M)$. This is trivial for the definition of $\xi[\![\ ]\!]$.

5. $\xi[\![\lambda\, y\,.\,M[y/x]]\!]_\rho = (\lambda\, y\,.\,\xi[\![M[y/x]]\!]_\rho)^+ = (\lambda\, x\,.\,\xi[\![M]\!]_\rho)^+ = \xi[\![\lambda\, x\,.\,M]\!]_\rho$ if $y \in FV(M)$.

6. If for every $d \in \mathcal{I}(U)$ we have $\xi[\![M]\!]_{[d/x]\rho} = \xi[\![N]\!]_{[d/x]\rho}$ then $\xi[\![\lambda\, x\,.\,M]\!]_\rho = \xi[\![\lambda\, x\,.\,N]\!]_\rho$.
¿From the premise $\xi[\![M]\!]_{[d/x]\rho} = \xi[\![N]\!]_{[d/x]\rho}$ we can deduce $\lambda\, x\,.\,\xi[\![M]\!]_\rho = \lambda\, x\,.\,\xi[\![N]\!]_\rho$, and from it the desired result $(\lambda\, x\,.\,\xi[\![M]\!]_\rho)^+ = (\lambda\, x\,.\,\xi[\![N]\!]_\rho)^+$. □

Fact 4.5 *$< \mathcal{I}(U_K), \circ, \xi[\![\ ]\!] >$ is not a model for the $\lambda\beta\eta$-calculus because it doesn't satisfy the condition $\lambda\, x\,.\,M(x) = M$ if $x \notin FV(M)$. Theorem 3.7 makes explicit the conditions in which η-reduction is valid.*

Proof: We can see that

$$\xi[\![\lambda\, x\,.\,M(x)]\!]_\rho = (\lambda\, \epsilon\,.\,\xi[\![M(x)]\!]_{[\epsilon/x]\rho})^+ = (\lambda\, \epsilon\,.\,(\xi[\![M]\!]_\rho)^*(\epsilon))^+ = (\xi[\![M]\!]_\rho)^{*+} \neq \xi[\![M]\!]_\rho$$

□

Theorem 11.12 of [HS86] ensures us that our model, being a λ-model, satisfies all provable equations of $\lambda\beta$. Furthermore, our model allows to define a new type of formulae based in the refinement relation ($\leq$). This order relation generalizes the $\lambda\beta$ equality in the sense that the equality relation can be defined from the order relation as follows:

$$M =_\beta N \ \textit{if and only if}\ \ M \leq N \ \ \textit{and} \ \ N \leq M.$$

The following is a precise definition of the relation of refinement which motivates the interpretation of the extended λ-calculus as a specification language.

Definition 4.6 *An expression e_1 is a refinement of another expression e_2 (noted $e_1 \leq e_2$) if and only if for any valuation ρ it is satisfied $\xi[\![e_1]\!]_\rho \subseteq \xi[\![e_2]\!]_\rho$.*

5 Conclusions and future work

The main goal of this paper is to show that λ-calculus, extended with some set operators, can be interpreted in a domain whose elements are a particular class of sets, the closed ideals. The main reason of such interpretation is that it allows to define very naturally a refinement relationship between λ-expressions. The formal theory of refinement is the subject of another paper where its normalization properties are studied and an efficient algorithm for checking this relation is given. On top of this extended λ-calculus with refinement we plan to build a functional programming language which supports formal program development following the stepwise refinement paradigm. We also plan to study the potential of this language to specify and manipulate logics, in particular the role of refinement in proof checking.

Acknowledgements

We acknowledge M. Fourman, R. Hindley, Z. Luo, D. Pym, D. Sannella and G. Valiente for their help and comments on this paper.

References

[Bar81] H. P. Barendregt. *"The Lambda Calculus: its syntax and semantics"*, volume 103 of *Studies in Logic and the Foundations of Mathematics*. Elsevier Science Publishers B. V., 1981.

[CABea86] R. L. Constable, S. F. Allen, H. M. Bromley, and W. R. Cleaveland et al. *"Implementing Mathematics with the Nuprl Proof Development System"*. Prentice-Hall, 1986.

[Car88] L. Cardelli. "A Semantics of Multiple Inheritance". *Information and Computation*, 76:138–164, 1988.

[CH88] T. Coquand and G. Huet. "The Calculus of Constructions". *Information and Computation*, 76:95–120, 1988.

[HS86] J. R. Hindley and J. P. Seldin. *"Introduction to Combinators and λ-Calculus"*. Number 1 in London Mathematical Society Student Texts. Cambridge University Press, 1986.

[LAEG90] J. Levy, J. Agustí, F. Esteva, and P. Garcia. "COR: A Calculus of Refinements". Technical report, Centre d'Estudis Avançats de Blanes, Blanes, Spain, 1990.

[Lan64] P. Landin. "The Next 700 Programming Languages". *Comm. ACM*, 9:157–166, 1964.

[LB88] B. Lampson and R. Burstall. "Pebble, a Kernel Language for Modules and Abstract Data Types". *Information and Computation*, 76:278–346, 1988.

[Mit88] J. C. Mitchell. "Polymorphic Type Inference and Containment". *Information and Control*, 76:211–249, 1988.

[ML79] P. Martin-Löf. "Constructive Mathematics and Computer Programming". In *Proc. of the sixth International Congress for Logic, Methodology and Philosophy of Science*. North Holland, 1979.

[MPS86] D. MacQueen, G. Plotkin, and R. Sethi. "An Ideal Model for Recursive Polymorphic Types". *Information and Control*, 71:95–130, 1986.

[Rey85] J. C. Reynolds. "Three Approaches to Type Structure". Number 185 in Lecture Notes in Computer Science, pages 97–138. Springer-Verlag, 1985.

[Sco76] D. S. Scott. "Data Types as Lattices". *SIAM Journal on Computing*, 5(3):522–587, September 1976.

[SP82] M. B. Smyth and G. D. Plotkin. "Category-Theoretic Solution of Recursive Domain Equations". *SIAM Journal on Computing*, 11:761–783, 1982.

[SST90] D. Sannella, S. Sokolowski, and A. Tarlecki. "Toward formal development of programs from algebraic specifications: parameterisation revisited". (Draft), April 1990.

[ST91] D. Sannella and A. Tarlecki. "A kernel specification formalism with higher-order parameterisation". In *Proc. 7 th Workshop on Specification of Abstract Data Types*, Lecture Notes in Computer Science, Wusterhausen, GDR, 1991. Springer-Verlag.