



# Lambda-calculi for (strict) parallel functions

G rard Boudol

## ► To cite this version:

G rard Boudol. Lambda-calculi for (strict) parallel functions. [Research Report] RR-1387, INRIA. 1991, pp.56. inria-00075174

**HAL Id: inria-00075174**

**<https://inria.hal.science/inria-00075174>**

Submitted on 24 May 2006

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destin e au d p t et   la diffusion de documents scientifiques de niveau recherche, publi s ou non,  manant des  tablissements d'enseignement et de recherche fran ais ou  trangers, des laboratoires publics ou priv s.



UNITÉ DE RECHERCHE  
INRIA-SOPHIA ANTIPOLIS

Institut National  
de Recherche  
en Informatique  
et en Automatique

Domaine de Voluceau  
Rocquencourt  
B.P. 105  
78153 Le Chesnay Cedex  
France  
Tél.: (1) 39 63 55 11

# Rapports de Recherche

N° 1387

*Programme 2*

*Calcul symbolique, Programmation et Génie logiciel*

## LAMBDA-CALCULI FOR (STRICT) PARALLEL FUNCTIONS

Gérard BOUDOL

Janvier 1991



★ R R - 1 3 8 7 ★

## Lambda-Calculi for (strict) Parallel Functions

### Lambda-Calculs pour les Fonctions Parallèles (strictes)

*Gérard Boudol*

INRIA Sophia-Antipolis

06565-VALBONNE FRANCE

#### **Abstract.**

We introduce two  $\lambda$ -calculi and show that they are expressive for two canonical domains of parallel functions. The first calculus is an enrichment of the lazy, call-by-name  $\lambda$ -calculus with call-by-value abstractions and parallel composition, while in the second the usual call-by-name abstractions are disallowed. The corresponding domains are respectively Abramsky's domain  $D = (D \rightarrow D)_\perp$ , a lifted function space, and  $D = (D \rightarrow_\perp D)_\perp$ , a lifted domain of strict functions. These domains are lattices, and we show that the parallelism is adequately represented by the join operator, while call-by-value abstractions correspond to strict functions. The proofs of the results rely on a completeness theorem for the logical presentation of the semantics.

#### **Résumé.**

Nous introduisons deux  $\lambda$ -calculs, dont nous montrons qu'ils sont expressifs pour deux domaines canoniques de fonctions parallèles. Le premier de ces calculs est une extension du  $\lambda$ -calcul paresseux en appel par nom, consistant en l'ajout d'un mécanisme d'abstraction fonctionnant en appel par valeur, et d'une construction de composition parallèle. Le second calcul est semblable, mais l'appel par nom n'y est pas autorisé. Les domaines correspondant sont respectivement le domaine d'Abramsky  $D = (D \rightarrow D)_\perp$ , qui est l'élévation d'un espace de fonctions, et  $D = (D \rightarrow_\perp D)_\perp$ , qui est l'élévation d'un espace de fonctions strictes. Ces domaines sont des treillis, et nous montrons que l'opération de borne supérieure fournit une interprétation adéquate du parallélisme, tandis que l'appel par valeur détermine des fonctions strictes. La preuve des résultats repose sur un théorème de complétude concernant la présentation logique de la sémantique.



# Lambda-Calculi for (strict) Parallel Functions

*G rard Boudol*

INRIA Sophia-Antipolis

06565-VALBONNE FRANCE

## Abstract.

We introduce two  $\lambda$ -calculi and show that they are expressive for two canonical domains of parallel functions. The first calculus is an enrichment of the lazy, call-by-name  $\lambda$ -calculus with call-by-value abstractions and parallel composition, while in the second the usual call-by-name abstractions are disallowed. The corresponding domains are respectively Abramsky's domain  $D = (D \rightarrow D)_\perp$ , a lifted function space, and  $D = (D \rightarrow_\perp D)_\perp$ , a lifted domain of strict functions. These domains are lattices, and we show that the parallelism is adequately represented by the join operator, while call-by-value abstractions correspond to strict functions. The proofs of the results rely on a completeness theorem for the logical presentation of the semantics.

## Content

1. Introduction
2. The  $\lambda^*_j$  and  $\lambda^y_j$  Calculi
  - 2.1 Syntax and Evaluation
  - 2.2 Reduction. Preliminary Results
3. Semantics
  - 3.1 The Canonical Domains
  - 3.2 Logical Presentation of the Domains
  - 3.3 The Logical Systems
4. Completeness and Full Abstraction
  - 4.1 Testing
  - 4.2 Realizability and Soundness
  - 4.3 Main Results
  - 4.4 Some Consequences
5. The Logical Systems: Proofs
  - 5.1 Structural Properties: Weakening and Cut
  - 5.2 Extensionality, Paste and Reduction
  - 5.3 Characteristic Terms

---

This work has been partly supported by ESPRIT Basic Research Action 3011 CEDiSYS.

## 1. Introduction.

### The Full Abstraction Problem.

The main theme of this work is the full-abstraction problem for programming languages. This problem, first raised by Milner in [27], can be stated as follows: given a programming language, can we provide a mathematical interpretation of this language such that the resulting semantic equality on programs coincides with operational indistinguishability?

According to Scott [39], what is intended as “mathematical interpretation” is an abstract semantics involving objects that do not refer to a particular way of computing, if not by abstract means, like continuity or stability (*cf.* Berry & al. 85[7]). Such an abstract semantics would provide a simple intuition about the meaning of programs. But obviously, programs have to be run on a machine, and an abstract semantics has to agree with operational semantics in some way (see again Scott 70[39], and [7,26]). The full abstraction criterion is one way to assess the agreement between a programming language and an abstract semantics for it. Another naturally arising criterion is the *expressivity*, or *completeness*, of the language with respect to an abstract interpretation: a language is expressive (resp. fully expressive, or universal) if all the finite (resp. computable) objects of the domain of interpretation are definable in the language. As a matter of fact, these two criteria are closely related.

We can also turn the full abstraction problem the other way round: given a semantical domain of “objects”, can we find a programming language for it, that is a language in which to express these abstract objects? This is the way we shall take: we introduce two extensions of the pure, untyped  $\lambda$ -calculus, which are expressive respectively w.r.t. a notion of “parallel function”, and of strict “parallel function”. Our notion of parallel function is quite trivial: we consider domains of continuous functions where any function can be regarded as parallel. We shall not make any attempt at bringing out a notion of “truly parallel” – or conversely of “sequential” – function. For some elements in this direction, see the work of Berry and Curien [7,16].

Let us recall some well-known results about full abstraction in the case of functional languages (for a survey see Berry & al. 85[7] and Stoughton 88[44]). This question was investigated by Plotkin [35], who showed that the model of continuous functions over cpo’s is not fully abstract for the PCF language, a typed lambda-calculus extended with fixed-points, boolean and arithmetical features. However, this model becomes fully abstract when PCF is enriched with a “parallel or” facility, and the extended language is expressive with respect to the model.

We shall look more closely at the situation of the pure, untyped  $\lambda$ -calculus with respect to the full abstraction problem, concentrating on Abramsky’s ideas [3,4]; for what regards the “classical”  $\lambda$ -calculus we refer to Barendregt’s book [5]. Let us first give some general definitions: a programming language consists of a syntax for programs together with an evaluation mechanism, e.g. an abstract machine. These two ingredients are the only means to define the operational semantics of programs. The syntactic features of the language provide a notion of *test*: a test is a program context  $C[\ ]$ , and two programs are operationally equivalent when they pass exactly the same tests. To observe the success of a test  $C[M]$ , we have to make it run on the machine, using the evaluation mechanism of the language.

This evaluation mechanism will be formalized by means of a predicate  $M \Downarrow K$  meaning “ $K$  is a value of  $M$ ”. Usually this also means that  $K$  is a normal form of  $M$  with respect to some reduction strategy. We shall say that the program  $M$  *converges*, in notation  $M \Downarrow$ , if it has a value, i.e.  $\exists K \ M \Downarrow K$ . Conversely divergence is denoted  $M \Uparrow$ . The notion of convergence, or termination, is, according to Abramsky, the only operationally *observable* property, something like “getting the

prompt” on the screen (see also Meyer [26]). Then the success of a test  $C[M]$  is its termination, and operational indistinguishability is given by means of the *testing* or *observation preorder*, whose definition, due to Morris, cf. [5] exercise 16.5.5, is as follows:

$$M \sqsubseteq_{\mathcal{O}} N \Leftrightarrow_{\text{def}} \forall C. C[M] \Downarrow \Rightarrow C[N] \Downarrow$$

Clearly, this preorder does not say anything about the abstract nature of the objects involved in the language. An interpretation, assigning a meaning  $\llbracket M \rrbracket$  to  $M$  in some semantic domain (cpo), is said to be

- (i) *adequate* if it induces a precongruence, and assigns no significant value to a divergent program, that is:

$$\llbracket M \rrbracket \sqsubseteq \llbracket N \rrbracket \Rightarrow \forall C. \llbracket C[M] \rrbracket \sqsubseteq \llbracket C[N] \rrbracket \quad \text{and} \quad \llbracket M \rrbracket = \perp \Leftrightarrow M \Uparrow$$

- (ii) *fully abstract* if it is adequate and reflects the operational distinctions, that is:

$$M \sqsubseteq_{\mathcal{O}} N \Rightarrow \llbracket M \rrbracket \sqsubseteq \llbracket N \rrbracket$$

Clearly an adequate semantics does not equate operationally distinct programs, that is it satisfies:

$$\llbracket M \rrbracket \sqsubseteq \llbracket N \rrbracket \Rightarrow M \sqsubseteq_{\mathcal{O}} N$$

### The $\lambda$ -Calculus: Evaluation Rules and Domain Equations.

Let us now examine the full abstraction problem for the pure  $\lambda$ -calculus. First we should say that this calculus is more appropriate to deal with “abstract machines” than to provide a model for “programming languages”. For this last purpose one should use a typed calculus, with some constants and  $\delta$ -rules, like PCF. Therefore our discussion will concentrate on evaluation rules, and more precisely on parameter passing mechanisms and their semantic counterpart.

For the pure  $\lambda$ -calculus, the adequacy requirement can be stated as follows: recall that this calculus is based upon the assertions:

$$\begin{aligned} \beta : (\lambda x M)N &= M[N/x] \\ \nu : M = M' &\Rightarrow MN = M'N \\ \mu : N = N' &\Rightarrow MN = MN' \\ \xi : M = M' &\Rightarrow \lambda x M = \lambda x M' \end{aligned}$$

Then an adequate semantics of the  $\lambda$ -calculus should satisfy these assertions, and also the requirement concerning divergence. This last property depends on the evaluation mechanism. Let us denote by  $\vec{\beta}$ ,  $\vec{\nu}$ ,  $\vec{\mu}$  and  $\vec{\xi}$  the conditional rewriting rules obtained by orienting the preceding equations  $M = N$  from left to right. Can these rules be considered as providing an evaluation mechanism?

The answer is as follows: first, there is *no* adequate semantics if we allow all these to be evaluation rules. Let us see this quite well-known result in some detail: let  $\mathbf{K} = \lambda xy.x$  be the usual “right cancellator”, or “left choice”,  $\Delta = \lambda x(xx)$  the “duplicator” and  $\Omega = \Delta\Delta$  the typical divergent term. Since  $\mathbf{K}$  is convergent, we should have  $\llbracket \Omega \rrbracket \neq \llbracket \mathbf{K} \rrbracket$  in any adequate semantics. If for any term  $M$  we let  $F_M = \lambda x((xM)\Omega)$ , then the term  $F_M$  is divergent, therefore we should have  $\llbracket F_M \rrbracket = \llbracket F_N \rrbracket$  for all  $M$  and  $N$ , but  $F_M \mathbf{K} =_{\beta} M$ , hence  $\llbracket M \rrbracket = \llbracket N \rrbracket$ , contradicting the existence of an adequate interpretation. The problem is with  $\vec{\mu}$ , which has to be dropped.

Second, if evaluation is given by  $\tilde{\beta}$ ,  $\tilde{\nu}$  and  $\tilde{\xi}$ , we get a *call-by-name* calculus, since one never evaluates the argument  $N$  in an application  $MN$ . This is also an *eager*, or *strong* calculus since one may evaluate the body  $M$  of a function  $\lambda xM$ . In this calculus the (closed) values are the “head normal forms”<sup>(1)</sup>. Note that due to the rule  $\tilde{\nu}$  we have  $M\uparrow \Rightarrow MN\uparrow$ , therefore  $\perp(x) = \perp$  in any adequate semantics. Similarly, due to the rule  $\tilde{\xi}$  we have  $M\uparrow \Rightarrow \lambda xM\uparrow$ , therefore an adequate semantics should satisfy  $\lambda x\perp = \perp$ . The strong call-by-name  $\lambda$ -calculus has an adequate, i.e. sensible, and fully abstract semantics, namely Scott’s  $D_\infty$ -interpretation studied by Wadsworth in [45] (cf. [5] thm. 19.2.9). However, the  $D_\infty$ -interpretation is quite strange, since no finite non-trivial element of  $D_\infty$  is  $\lambda$ -definable; in other words: the “ $\beta\nu\xi$ -calculus” is not expressive (i.e. it is incomplete) with respect to  $D_\infty$ . Here the problem is with the  $\tilde{\xi}$ -rule.

We are then left with  $\tilde{\beta}$  and  $\tilde{\nu}$ , and the situation appears much better; this is Abramsky’s *lazy*  $\lambda$ -calculus [3]. This calculus is *lazy*, or *weak*, since one cannot evaluate the body  $M$  of an abstraction  $\lambda xM$ ; it is still a call-by-name calculus since  $\tilde{\mu}$  is not allowed as an evaluation rule. In the lazy  $\lambda$ -calculus, with “ $\beta\nu$ -evaluation”, there are many more convergent terms than in the “classical”  $\lambda$ -calculus: the (closed) values are “weak head normal forms”, that is abstractions  $\lambda xM$ . In other words, the convergent terms are those that can *accept an input*, possibly after some internal evaluation. The typically divergent term is still  $\Omega$ , but for instance  $\Upsilon = \lambda x\Omega$ , which is clearly “finite”, is now strictly greater than  $\Omega$  in any adequate semantics.

For what regards the lazy  $\lambda$ -calculus, we should first mention that Lévy proposed in [24] an adequate semantics for this calculus, built using syntactic means. Also Longo [25] studied some “very sensible” models of the  $\lambda$ -calculus, distinguishing the terms  $\lambda x_1 \dots x_n.\Omega$ . More roughly, one can distinguish in the lazy  $\lambda$ -calculus two kinds of objects: the undefined objects, like  $\Omega$ , and the truly functional values, like  $\lambda xM$ . In other words, any adequate semantics should satisfy  $\lambda x\perp \neq \perp$ . Accounting for this fact, Abramsky proposed to interpret the lazy  $\lambda$ -calculus in a domain  $D_\star$  which is the canonical solution of the equation:

$$D = (D \rightarrow D)_\perp$$

where  $(X \rightarrow Y)$  is the usual domain of continuous functions, extensionally ordered, and  $X_\perp$  the lifting construct. So Abramsky’s domain consists of all, possibly “non-sequential”, continuous functions over itself, plus a non-functional undefined object.

However, the  $D_\star$ -interpretation of the lazy  $\lambda$ -calculus is not fully abstract – more precisely, it is “over-generous”. One can show for instance that the terms  $A = \lambda x(x(x\Omega))$  and  $B = \lambda x(x(\lambda y(x\Omega y)))$  are operationally indistinguishable; but if we consider the step function  $\delta: D_\star \rightarrow D_\star$  given by:

$$\delta(x) = \begin{cases} \text{Id} & \text{(the identity function) if } x \neq \perp \\ \perp & \text{otherwise} \end{cases}$$

then  $\llbracket A \rrbracket(\delta) \neq \llbracket B \rrbracket(\delta)$ . Therefore the element  $\delta$  of  $D_\star$  is *not* definable in the lazy  $\lambda$ -calculus. Abramsky and Ong [4,32,33] proposed to enrich the lazy  $\lambda$ -calculus with a combinator **C** for *convergence testing*, satisfying:

$$\mathbf{C}M \xrightarrow{*} \mathbf{I} \Leftrightarrow M\Downarrow \quad \text{and} \quad \mathbf{C}M\uparrow \Leftrightarrow M\uparrow$$

where  $\mathbf{I} = \lambda xx$  is the usual identity combinator (thus  $\llbracket \mathbf{C} \rrbracket = \delta$ ). However, this seems a little ad hoc, both from a programming language point of view (or more accurately from an abstract machine

<sup>(1)</sup> warning: this does not mean that the usual notion of “ $N$  is a hnf of  $M$ ” corresponds to  $\beta\nu\xi$ -evaluation. For instance if  $M$  reduces to  $N$  then  $\lambda x(xN)$  “is a hnf of”  $\lambda x(xM)$ , but  $\lambda x(xM)$  does not  $\beta\nu\xi$ -reduce to  $\lambda x(xN)$ . What we get is the “principal” hnf.



point of view) and from a denotational point of view. Then the question is: can we find another, more “natural” formulation the weak  $\lambda$ -calculus with convergence testing? Abramsky remarked that the combinator **C** is a variant of the usual “left cancellator”, or “right choice”  $\mathbf{F} = \lambda xy.y$ , namely: **C** is the same as **F**, but strict in its first argument. Therefore we should extend the  $\lambda$ -calculus so as to be able to define such a strict function which is in fact nearly independent of its argument. Then an appealing solution to the previous question consists in considering not only the usual call-by-name abstraction  $\lambda xM$ , but also a *call-by-value abstraction*  $\lambda^v xM$ , like the one considered by Plotkin in [34]. The corresponding  $\beta$ -rule is:

$$\tilde{\beta}_v : (\lambda^v xM)K \rightarrow M[K/x] \quad \text{where } K \text{ is a value (normal form)}$$

Obviously we should also add:

$$\tilde{\mu}_v : N \rightarrow N' \Rightarrow (\lambda^v xM)N \rightarrow (\lambda^v xM)N'$$

Clearly we may now define the convergence testing combinator by  $\mathbf{C} = \lambda^v x\mathbf{I}$ , and conversely the call-by-value abstractions  $\lambda^v xM$  can be simulated using the convergence testing combinator, namely by  $\lambda^v xM = \lambda x(\mathbf{C}x)M$  (see also the “call-by-value simulation” of Ong [33]). Then introducing the call-by-value abstractions provides a satisfactory means for testing potential termination. Note that the call-by-name abstractions are still useful, in the untyped calculus, to define non-strict constructs like the “if-then-else”  $\text{cond} = \lambda xyz.xyz$ . However we shall see that, while call-by-name is not enough to set up an expressive calculus, as we saw above, the standard call-by-value parameter passing mechanism is in some sense sufficiently powerful.

Let us call  $\lambda^*$ -calculus the  $\lambda$ -calculus enriched with call-by-value abstractions, equipped with the evaluation rules  $\tilde{\beta}$ ,  $\tilde{\nu}$ ,  $\tilde{\beta}_v$  and  $\tilde{\mu}_v$ , and  $\lambda^v$ -calculus the call-by-value  $\lambda$ -calculus, where the ordinary call-by-name abstractions are discarded. It should be clear that, since  $N \uparrow \Rightarrow (\lambda^v xM)N \uparrow$ , the call-by-value abstractions must be interpreted as *strict* continuous functions, i.e. such that  $f(\perp) = \perp$ . In particular, we can adequately interpret in this way the  $\lambda^*$ -calculus in Abramsky’s domain  $D_*$ .

For what regards the  $\lambda^v$ -calculus, or *strict*  $\lambda$ -calculus, one can provide an adequate semantics for it by means of *partial functions*, as shown by Plotkin 85[37] for the typed case, and Moggi 86[29]. However, it is simpler to use *strict functions*: let  $(X \rightarrow_\perp Y)$  be the domain of *strict* continuous functions from  $X$  to  $Y$ . Obviously one still has to use the lifting construct to reflect the distinction between divergent and convergent  $\lambda^v$ -terms, the values being the truly functional terms  $\lambda^v xM$ . Then the canonical domain for the  $\lambda^v$ -calculus is the initial solution  $D_S$  of the equation:

$$D = (D \rightarrow_\perp D)_\perp$$

The strict canonical domain  $D_S$  has another definition, which is technically more convenient: note that there is an obvious isomorphism  $(X_\perp \rightarrow_\perp Y) \cong (X \rightarrow Y)$ , therefore if we denote by  $V$  the domain of *values*, that is  $(D_S \rightarrow_\perp D_S)$ , we may also define our strict domain by the following system of equations:

$$\begin{cases} D_S = V_\perp & \text{where} \\ V = (V \rightarrow D_S) \end{cases}$$

Following the terminology of Moggi 89[30], we could call  $D_S$  the domain of *computations*. Note that, since  $V = (V \rightarrow V_\perp)$ , we may also regard the values as *partial functions* over  $V$ . In other words,  $D_S$  is a partial function space (see Plotkin 85[37]), enriched with a denotation  $\perp$  for the “non-existent” objects. The lifted strict function space  $(X \rightarrow_\perp Y)_\perp$  is what Abramsky [3,4] calls the Landin-Plotkin function space. It is used by Sitaram & Felleisen in [18] to give a fully abstract semantics for a call-by-value PCF enriched with a parallel combinator.

### Parallel Functions.

The reader should not be surprised to be told that the  $D_*$ -interpretation of the  $\lambda^*$ -calculus and the  $D_S$ -interpretation of the  $\lambda^V$ -calculus are not fully abstract: these languages still lack some parallel facility. For instance, it can be seen that the function of  $D_*$  given by:

$$\pi(x)(y) = \begin{cases} \text{Id} & \text{if } x \neq \perp \text{ or } y \neq \perp \\ \perp & \text{otherwise} \end{cases}$$

is not  $\lambda^*$ -definable. This is clearly a "parallel" function since, although the value of  $\pi(x)(y)$  only depends in general on the value of  $x$  or on the value of  $y$ , to compute  $\pi(x)(y)$  we have to compute concurrently  $x$  and  $y$ . The computation of such a function is non-deterministic in that we have to evaluate both arguments and cannot say in advance which will finish first.

Abramsky [3,4] proposed to enrich the  $\lambda$ -calculus with a parallel convergence testing combinator  $\mathbf{P}$ , whose interpretation is the function  $\pi$  above (see [4] def. 7.2.7). This combinator is what Barendregt calls "parallel or", see [5] §14.4. Note that we can define  $\mathbf{C} = \lambda x \mathbf{P} x x$ . Then the resulting language is expressive with respect to  $D_*$ , and the  $D_*$ -semantics is fully abstract for it - for all these results, see Abramsky and Ong [4]. This solves the problem stated above: the lazy  $\lambda$ -calculus with parallel convergence testing provides an expressive language for parallel functions. A similar result holds for lazy PCF, see [8,15].

However, extending the language with this combinator seems again a little ad hoc: instead of adding a special combinator, distinguishing a particular element of the domain, we would like to know which control mechanism could model "parallel computations", and to which property of the domain it would correspond. One may remark that to evaluate  $\mathbf{P} M N$  amounts to concurrently evaluate  $\mathbf{C} M$  and  $\mathbf{C} N$ , therefore the parallel convergence testing combinator could be defined as a parallel composition of  $\lambda x \lambda y (\mathbf{C} x)$  and  $\lambda x \lambda y (\mathbf{C} y)$ . This is the solution we shall adopt, introducing a *parallel composition operator*  $(M \parallel N)$ . The operational meaning of this operator is as follows: the evaluation of  $(M \parallel N)$  initiates two concurrent sub-computations, one for each component, and this term will have a value as soon as one of its components has a value. As usual, we shall formalize a concurrent computation as the non-deterministic interleaving of its sub-computations. Then the evaluation of a parallel combination is given by the following rules:

$$M \rightarrow M' \Rightarrow (M \parallel N) \rightarrow (M' \parallel N) \quad \text{and} \quad (N \parallel M) \rightarrow (N \parallel M')$$

However, we have to change our mind about the notion of observation, or more precisely about the notion of result, since these rules do not reflect the idea that  $(M \parallel N)$  has a value if one of the components,  $M$  or  $N$ , has a value: a value can no longer be just a normal form, since for instance if  $M$  has an infinite computation while  $N$  converges, then  $(M \parallel N)$  has an infinite computation, hence no normal form, while it should have a value. Therefore we define a value as a term of a special shape, which can be produced at any stage throughout the computation, and not necessarily at the end. More precisely, a value is produced as soon as one concurrent component has terminated. Therefore the syntax of the values is given by the grammar:

$$K ::= \lambda x M \mid \lambda^V x M \mid (K \parallel M) \mid (M \parallel K)$$

where  $M$  stands for any term. Intuitively, a value can be regarded as a set of functional elements. Then we shall define the evaluation predicate  $M \Downarrow K$ , for any closed term  $M$ , in such a way that:

$$M \Downarrow K \Leftrightarrow K \text{ is a value \& } M \xrightarrow{*} K$$

The notion of convergence, which is the basis of the operational semantics, still means “to have a value”, but now this is not the same as “to have a terminating evaluation”. However, the convergence property can be adequately interpreted as “to have a terminating sub-computation”, and observing a term means to concurrently observe its components. It is also worth noting that, although our notion of reduction (see § 2.2) satisfies the Church-Rosser property, the calculus is non-deterministic: a given term may have several (compatible) values.

There is a rule missing concerning parallel composition: a term  $(M \parallel N)$  is, in general, made of functional units, i.e. abstractions. Then we have to say how it can be applied to an argument. This is the aim of the next rule, which says that the operand is shared between the functional units of the operator:

$$(M \parallel N)P \rightarrow (MP \parallel NP)$$

Clearly the sharing of data among concurrent programs does not introduce any conflict, since the data are distributed to all the components.

Let us see now what is the abstract meaning of concurrency: it can be noted that the canonical domains  $D_*$  and  $D_s$  are in fact *algebraic (complete) lattices*, with all joins<sup>(2)</sup>. Then it turns out that the parallel composition can be adequately interpreted as the *join* operator, or *sup*, which is typically “non-sequential” or more precisely non-stable, that is:

$$\llbracket M \parallel N \rrbracket = \llbracket M \rrbracket \sqcup \llbracket N \rrbracket$$

Then the parallel composition operator will be also called the *concurrent join*, and the calculi we propose for parallel functions are respectively the  $\lambda_j^*$ -calculus, that is the *call-by-name* and *call-by-value*  $\lambda$ -calculus *with join*, and  $\lambda_j^V$ -calculus, the *call-by-value* or *strict*  $\lambda$ -calculus *with join*.

Using the idea that a parallel function is the join of some more basic functional elements, it is easy for instance to “program” a parallel disjunction. Let us see this in more detail: first recall that  $\mathbf{K}$  and  $\mathbf{F}$  may be regarded as the *truth values*, respectively true and false. Then parallel disjunction  $\mathbf{O}$  is just the join  $(\mathbf{V}_l \parallel \mathbf{V}_r)$  of “left sequential disjunction”  $\mathbf{V}_l = \lambda xy.(x\mathbf{K})y$ , that is  $\mathbf{V}_l = \lambda xy.\text{cond}x\mathbf{K}y$ , and “right sequential disjunction”  $\mathbf{V}_r = \lambda xy.(y\mathbf{K})x$ , or  $\mathbf{V}_r = \lambda xy.\text{cond}y\mathbf{K}x$  (cf. Curien [16]). One should note that evaluating a parallel combination always yields another parallel combination, therefore, though  $(\mathbf{K} \parallel \Omega) = \mathbf{K}$  is a valid semantic equation, we cannot get simply the value  $\mathbf{K}$  in evaluating  $\mathbf{O}MN$  for instance.

Let us now return to the full abstraction problem: recall that this property relates a semantical preorder with a testing preorder, and that a test is just a program context. However, to test properly the non-closed terms of the  $\lambda_j^V$ -calculus, we have to slightly enrich the notion of test. The reason is that there is in the  $\lambda_j^V$ -calculus an asymmetry between the two ways of closing a term, namely abstraction and substitution: in  $\lambda^V xM$  the bound variable  $x$  only stands for *values*, i.e. terms having a normal form, while one can substitute any term for a free variable. This makes a difference from Plotkin’s  $\lambda_v$ -calculus [34], where a variable is always supposed to stand for “existent” objects. As a matter of fact, distinguishing between the ranges of free and bound variables is a standard matter in existence logic, see for instance Scott 79[41].

Without the power of substitution we would not be able to test any difference between  $x$  and  $\lambda^V y(xy)$ , as we should be, since  $\llbracket x \rrbracket \rho = \perp$  if  $\rho$  is an environment assigning the value  $\perp$  to  $x$ , while  $\llbracket \lambda^V y(xy) \rrbracket \rho \neq \perp$ . Therefore we should in principle include substitution as a fully explicit

---

<sup>(2)</sup> as we shall see the canonical domains are also (lower) powerdomains, with the join as the union operator.

computational mechanism, as it is done by Abadi, Cardelli, Curien & Lévy in [1] for instance. This means that we should introduce terms of the form  $M\sigma$ , that is general closures, where  $\sigma$  is a syntactic “environment”, and extend the abstract machine to deal with them. However, we shall content ourselves here with “semi-explicit” substitutions. More precisely, substitutions will be involved here only by two means: first we shall consider tests of the form  $C[M\sigma]$ , where  $M\sigma$  is not a term, but denotes the result of applying the substitution  $\sigma$  to the term  $M$  – this is supposed to be provided by an outer evaluation procedure. Second, to avoid any problem with “fresh names” and  $\alpha$ -conversion, we shall replace the ordinary abstractions  $\lambda x M$ , and also the strict ones, by *closures*, i.e. pairs  $\langle \lambda x M, \sigma \rangle$  made of a functional value and an environment. Then the calculi  $\lambda_J^*$  and  $\lambda_J^V$  for parallel functions that will be studied here have the following syntax: the grammar of the first is

$$\begin{aligned} M &::= x \mid \langle \lambda x M, \sigma \rangle \mid \langle \lambda^V x M, \sigma \rangle \mid (MM) \mid (M \parallel M) \\ \sigma &::= \varepsilon \mid [M/x]\sigma \end{aligned}$$

while we disallow the use of  $\langle \lambda x M, \sigma \rangle$  for the strict sub-calculus  $\lambda_J^V$ . The usual abstractions  $\lambda x M$  and  $\lambda^V x M$  are notations for closures where the environment part is the empty substitution  $\varepsilon$ .

Since one may define the parallel convergence combinator by  $\mathbf{P} = (\lambda x \lambda y (\mathbf{C}x) \parallel \lambda x \lambda y (\mathbf{C}y))$  where  $\mathbf{C} = \lambda^V x \mathbf{I}$ , it is not surprising, in view of Abramsky’s results, that the following holds:

**THEOREM 1.** *The  $\lambda_J^*$ -calculus is complete with respect to the canonical domain  $D_*$ . Moreover the  $D_*$ -interpretation of this calculus is fully abstract.*

We show that a similar result holds in the strict case:

**THEOREM 2.** *The  $\lambda_J^V$ -calculus is complete with respect to the canonical domain  $D_S$ . Moreover the  $D_S$ -interpretation of this calculus is fully abstract.*

Before giving an idea of the proofs, let us say a few words about domains. Scott originally proposed to work with lattices, and we saw that this seems quite convenient for dealing with “parallel” functions. However, the meaning of the  $\top$  element in Scott’s work was not entirely clear. Sometimes, as in [39],  $\top$  is an “over-determined”, inconsistent element, sometimes it is the most multivalued element, as in [40]. I think both interpretations are right: as the join of all values,  $\top$  is clearly the most multivalued element. But then  $\top$  does not provide much information: anything is true of it. This is reflected in the syntax: in the  $\lambda_J^*$ -calculus we can define an “ogre”, namely:

$$\Upsilon_* =_{\text{def}} (\lambda x \lambda y (xx))(\lambda x \lambda y (xx))$$

This combinator is the “best” one, greater than any other. But it is not a very interesting one: since  $\Upsilon_* \rightarrow \lambda y \Upsilon_*$ , the ogre can repeatedly accept any input value you propose, but then it simply ignores it and returns the prompt.

The use of lattices in semantics was criticized, for instance by Plotkin in [36], for the reason that some natural identities, concerning the “if-then-else” construct, fail if the  $\top$  element is admitted. The first expected identity, namely:

$$\text{cond}XY Y = Y$$

(where  $X$  and  $Y$  are values) refers implicitly to a notion of “type”: we cannot guarantee anything if the first argument of the if-then-else is not a “boolean”. Indeed we have  $\text{cond}\Upsilon_*XX = \Upsilon_*$ , but also  $\text{cond}(\mathbf{K} \parallel \mathbf{F})XY = (X \parallel Y)$ , hence  $\text{cond}(\mathbf{K} \parallel \mathbf{F})XX = X$ . The other expected identity, that is:

$$\text{cond}X(\text{cond}XYZ)V = \text{cond}XYV$$

assumes implicitly that  $X$  is either true or false (or undefined). Obviously this equation does not hold in a non-deterministic language, where  $X$  may be the join of the truth values.

Another criticism against lattices, based on the negative results of Plotkin [35], is presented by Bloom [9] and Meyer [26]: Meyer argued that, although the mathematical results they provide are quite nice, lattices should be rejected because any expressive language for them has to be “unreasonable” – this meaning that the evaluation mechanism has to be inherently non-deterministic (non-confluent). As we indicated above, our notion of reduction is indeed confluent, but the notion of observation is non-deterministic, since we cannot predict the relative speed of execution of the concurrent components. Unlike Bloom [9], we do not regard “single-valuedness as an essential criterion”. One may also question the choice of lattices he made: we would choose a powerdomain (see section 3.1.1) for the domain of integers, instead of the flat lattice used in [35,9].

### The Proofs of Full Abstraction.

As we indicated above, the main point of this paper is to show that the interpretations of the  $\lambda_j^*$  and  $\lambda_j^\vee$  calculi, respectively in the domains  $D_\star$  and  $D_S$ , provide adequate and fully abstract semantics for these languages. For the first one, this is more or less an adaptation of Abramsky & Ong’s results [4]. As far as I know, the second full abstraction result is new. We shall prove both these results here, since the proofs follow exactly the same lines. Now let us see how these proofs are articulated:

(1) the first step is to give a concrete presentation of the canonical domains. This is done using Scott’s information systems [43]. Then it can be observed, following the work of Coppo & al. [12,13], that another equivalent concrete presentation is by means of *filters of logical formulae*. This formalizes Scott’s idea that “elements of a domain can be identified with the sets of propositions true of them”, which was already realized in Coppo & al. [11,6]. This is also a simple instance of Abramsky’s theory of “domains in logical form” [2]. Then the domains are *logical domains*. The logic for  $D_\star$  is:

$$\phi ::= \omega \mid (\phi \rightarrow \phi) \mid (\phi \wedge \phi)$$

together with an axiomatization of the entailment relation  $\phi \leq \psi$  meaning intuitively “ $\phi$  implies  $\psi$ ”. This is the logic of Abramsky 88 [3], and also, apart from the propositional variables, of Dezani & Margaria 86 [17]. For the strict domain, the formulae belong to a subset of the previous logic, given by:

$$\begin{aligned} \psi &::= \omega \mid \zeta \mid (\psi \wedge \psi) \\ \zeta &::= (\omega \rightarrow \omega) \mid (\zeta \wedge \zeta) \mid (\zeta \rightarrow \psi) \end{aligned}$$

with a slightly different axiomatization of the entailment relation.

Since the abstract meaning  $\llbracket M \rrbracket$  of a term  $M$  is now a set of formulae, we can recast the interpretation of the calculi using the logical presentation of the domains, and we get “typing systems”, that is logical natural deduction systems allowing one to prove sequents of the form:

$$x_1 : \phi_1, \dots, x_n : \phi_n \vdash M : \phi$$

It turns out that, for closed terms:

$$\vdash M : \phi \Leftrightarrow \phi \in \llbracket M \rrbracket$$

Therefore if we define an “assertional preorder”, or syntactic logical preorder, by:

$$M \sqsubseteq_S N \Leftrightarrow_{\text{def}} \forall \phi. \vdash M : \phi \Rightarrow \vdash N : \phi$$

we have

$$\llbracket M \rrbracket \subseteq \llbracket N \rrbracket \Leftrightarrow M \sqsubseteq_S N$$

(2) the second, easy step consists in giving a “realizability interpretation” of the formulae as sets of closed terms, namely:

$$\begin{aligned} \models M : \omega &\Leftrightarrow_{\text{def}} \text{true} \\ \models M : (\phi \wedge \psi) &\Leftrightarrow_{\text{def}} \models M : \phi \ \& \ \models M : \psi \\ \models M : (\phi \rightarrow \psi) &\Leftrightarrow_{\text{def}} M \Downarrow \ \& \ \forall R. \ \models R : \phi \Rightarrow \models (MR) : \psi \end{aligned}$$

It is worth noting the similarity between this interpretation and Hindley’s “ $F$ -semantics” for type schemes [19,17]. Again associated with this interpretation we find a semantic logical preorder:

$$M \sqsubseteq_{\mathcal{L}} N \Leftrightarrow_{\text{def}} \forall \phi. \ \models M : \phi \Rightarrow \models N : \phi$$

and it is quite easy to show that this is implied by the testing preorder:

$$M \sqsubseteq_{\mathcal{O}} N \Rightarrow M \sqsubseteq_{\mathcal{L}} N$$

(3) finally the heart of the full abstraction proof is the *soundness* and *completeness* theorem, that is:

$$x_1 : \phi_1, \dots, x_n : \phi_n \models M : \phi \Leftrightarrow x_1 : \phi_1, \dots, x_n : \phi_n \vdash M : \phi$$

The key fact for completeness is that any compact element of the domain  $D_*$  (resp.  $D_S$ ) is  $\lambda_j^*$ -definable (resp.  $\lambda_j^V$ -definable) – in other words, our languages are complete with respect to their abstract interpretations, namely:

$$\forall \phi \exists \mathbf{M}_\phi. \vdash \mathbf{M}_\phi : \psi \Leftrightarrow \phi \leq \psi$$

This is the only result for which we need the concurrent join  $\parallel$ , together with the call-by-value abstractions: the logical meaning of parallelism is the conjunction, while the call-by-value abstractions provide a test for existence. The essential rôle of this definability result is not a surprise: although it was not formulated in logical terms in the pioneering work of Plotkin 77[35] and Milner 77[28], the completeness of the language was recognized as a crucial property for the full abstraction problem (see also [7], lemma 5.1.2).

Summarizing, we can picture the architecture of the whole proof as follows:

$$\begin{array}{ccc} M \sqsubseteq_{\mathcal{O}} N & \Leftarrow & \llbracket M \rrbracket \subseteq \llbracket N \rrbracket \\ \Downarrow & & \Downarrow \\ M \sqsubseteq_{\mathcal{L}} N & \Leftrightarrow & M \sqsubseteq_S N \end{array}$$

NOTE: although the results are simple adaptations of more or less standard ones, most of the proofs will be given in full details. The facts concerning the left side of the above diagram are directly adapted from [3,4]. For the lower side, we use proof techniques mainly due to Coppo [6,10,12], Hindley [19,20], Krivine [21]; the idea of the “characteristic terms”  $\mathbf{M}_\phi$  is due to Abramsky [3] (see also [14] where Coppo remarked that the proof of completeness relies upon the existence of “characteristic values” for each type). We shall only give hints for the proofs concerning the right side of the diagram; we refer the interested reader to [13], but we hope that he/she will think it is an instructive exercise to find out the arguments. We will mainly take into consideration the “constructive” presentation of the canonical interpretations: in fact these interpretations are given by means of the logical natural deduction systems.

**Acknowledgments.** Merci à Jean-Jacques Lévy: l’enseignement tiré de discussions tenues avec lui m’a été fort utile pour l’élaboration de ce travail.

## 2. The $\lambda_j^*$ and $\lambda_j^v$ Calculi.

### 2.1 Syntax and Evaluation.

To build the terms of our calculi, we assume given an infinite set  $X$  of variables. As we just said in the introduction, the  $\lambda_j^*$ -calculus is given by the grammar:

$$\begin{aligned} (\Lambda_j^*) \quad M &::= x \mid \langle \lambda x M, \sigma \rangle \mid \langle \lambda^v x M, \sigma \rangle \mid (MM) \mid (M \parallel M) \\ (\Sigma) \quad \sigma &::= \varepsilon \mid [M/x]\sigma \end{aligned}$$

where  $x$  is any variable.

We call  $\parallel$  the *concurrent join*, or *parallel composition*,  $\langle \lambda x M, \sigma \rangle$  a *call-by-name closure*,  $\langle \lambda^v x M, \sigma \rangle$  a *call-by-value closure*, and  $\varepsilon$  the empty (or identity) substitution. We shall use  $M, N, P, Q, R, \dots$  to denote terms of  $\Lambda_j^*$ . The set of call-by-value terms, or  $\lambda_j^v$ -terms, built without using the closures  $\langle \lambda x M, \sigma \rangle$ , is  $\Lambda_j^v$ . We shall often use the standard abstraction construct  $\lambda x M$  as an abbreviation for  $\langle \lambda x M, \varepsilon \rangle$ , and similarly for  $\lambda^v x M$ . As usual, we omit some parentheses, denoting  $(MN)$  by  $MN$ , and use the standard abbreviations, namely  $\lambda x_1 \dots x_n. M$  for  $\lambda x_1 \dots \lambda x_n M$  and  $M N_1 \dots N_k$  for  $(\dots (M N_1) \dots N_k)$ .

We shall use a *structural ordering* on  $\Lambda_j^* \cup \Sigma$ , denoted  $s \propto t$ , meaning that  $s$  is a syntactic component of  $t$ . The formal definition of this ordering should be obvious. In particular we have  $\sigma \propto \langle \lambda x M, \sigma \rangle$  and  $\sigma \propto \langle \lambda^v x M, \sigma \rangle$ , and  $\sigma \propto [M/x]\sigma$  and  $M \propto [M/x]\sigma$ . It should be clear that this ordering is noetherian, that is there is no strictly decreasing infinite chain for it. This allows us to use structural induction, that is induction on the structural ordering, in definitions and proofs.

The following combinators were already introduced, at least in their non-strict version:

$$\begin{aligned} \text{identity: } I &= \lambda x x \quad \text{and} \quad I_s = \lambda^v x x \\ \text{duplicator: } \Delta &= \lambda x (xx) \quad \text{and} \quad \Delta_s = \lambda^v x (xx) \\ \text{divergence: } \Omega &= \Delta \Delta \quad \text{and} \quad \Omega_s = \Delta_s \Delta_s \\ \text{least value: } \Upsilon &= \lambda x \Omega \quad \text{and} \quad \Upsilon_s = \lambda^v x \Omega_s \\ \text{truth values: } T &= \lambda x \lambda y x = K \quad \text{and} \quad F = \lambda y \lambda x x \\ &\quad T_s = \lambda^v x \lambda^v y x = K_s \quad \text{and} \quad F_s = \lambda^v y \lambda^v x x \\ \text{ogre: } \Upsilon_* &= (\lambda x \lambda y (xx))(\lambda x \lambda y (xx)). \end{aligned}$$

The substitution  $[M/x]\sigma$  can also be regarded as an *environment*, providing the value  $M$  for  $x$ , and acting as a stack: if  $\sigma$  also assigns a value for  $x$ , this value is ignored. This is formalized by defining the value  $\sigma(x)$  of the variable  $x$  in the environment  $\sigma$ , as follows:

$$\begin{aligned} \varepsilon(x) &= x \\ ([M/y]\sigma)(x) &= \begin{cases} M & \text{if } y = x \\ \sigma(x) & \text{otherwise} \end{cases} \end{aligned}$$

The set  $\text{fv}(M)$  of *free variables* of  $M$  is given by:

$$\begin{aligned} \text{fv}(x) &= \{x\} \\ \text{fv}(\langle \lambda x M, \sigma \rangle) &= \{v \mid \exists z. z \in \text{fv}(M) - \{x\} \ \& \ v \in \text{fv}(\sigma(z))\} = \text{fv}(\langle \lambda^v x M, \sigma \rangle) \\ \text{fv}(MN) &= \text{fv}(M) \cup \text{fv}(N) = \text{fv}(M \parallel N) \end{aligned}$$

As usual, a term  $M$  is said to be *closed* if  $\text{fv}(M) = \emptyset$ . The set of closed terms is denoted  $(\Lambda_j^*)^\circ$ . Similarly  $(\Lambda_j^v)^\circ$  is the set of closed  $\lambda_j^v$ -terms.

We shall regard as given, by an outer evaluation procedure, the operations of *composition* of substitutions  $(\sigma \circ \rho)$  and *application*  $M\sigma$  of a substitution  $\sigma$  to a term  $M$ . These operations are supposed to satisfy:

$$\begin{aligned} x\sigma &= \sigma(x) \\ \langle \lambda x M, \sigma \rangle \rho &= \langle \lambda x M, (\sigma \circ \rho) \rangle \\ \langle \lambda^v x M, \sigma \rangle \rho &= \langle \lambda^v x M, (\sigma \circ \rho) \rangle \\ (MN)\sigma &= (M\sigma N\sigma) \\ (M \parallel N)\sigma &= (M\sigma \parallel N\sigma) \\ (\varepsilon \circ \rho) &= \rho \\ ([M/x]\sigma) \circ \rho &= [M\rho/x](\sigma \circ \rho) \end{aligned}$$

One may note that the evaluation mechanism for  $M\sigma$  does not have to be especially sophisticated. In particular, there is no need for converting bound variables using new names. It is a very easy exercise to show the following:

**LEMMA 2.1.**

- (i)  $M\varepsilon = M$  and  $\sigma \circ \varepsilon = \sigma$
- (ii)  $(M\sigma)\rho = M(\sigma \circ \rho)$  and  $(\rho \circ \sigma_0) \circ \sigma_1 = \rho \circ (\sigma_0 \circ \sigma_1)$

We shall use the standard notion of *context*: a  $\lambda_j^*$ -context, or simply context (resp.  $\lambda_j^v$ -context, or strict context) is a term built using the  $\lambda_j^*$ -constructs (resp. the  $\lambda_j^v$ -constructs), and possibly a new constant  $\square$ , the *hole*. However, we do not need the hole to occur in the environment part of a closure context. Then the syntax of  $\lambda_j^*$ -contexts is given by the grammar:

$$C ::= \square \mid x \mid \langle \lambda x C, \sigma \rangle \mid \langle \lambda^v x C, \sigma \rangle \mid (CC) \mid (C \parallel C)$$

The  $\lambda_j^v$ -contexts are given by a similar grammar, where the call-by-name closures are discarded. Filling the hole with the context  $B$  in the context  $C$  gives the context  $C[B]$  (the definition, by structural induction, is obvious). Note that in this operation, some free variables of  $B$  may be bound by the context  $C$ , e.g.  $(\lambda x \square)[x] = \lambda x x$ . We shall say that a context  $C$  *closes* the term  $M$  if  $C[M]$  is closed.

Let us now define the *evaluation mechanism* for  $\lambda_j^*$ -terms, formalized as a relation  $M \Downarrow K$  meaning “ $K$  is a partial normal form of  $M$ ”, or a *value* of  $M$ . In principle we should define two such relations  $\Downarrow_*$  and  $\Downarrow_v$ , but in fact the latter is just the restriction of the former to the set of  $\lambda_j^v$ -terms. The *partial normal forms*, or *values*, ranged over by  $K, J, L \dots$  are closures  $\langle \lambda x M, \sigma \rangle$  or  $\langle \lambda^v x M, \sigma \rangle$ , and parallel combinations including at least one partial normal form. Then the syntax of partial normal forms is given by the grammar:

$$K ::= \langle \lambda x M, \sigma \rangle \mid \langle \lambda^v x M, \sigma \rangle \mid (K \parallel M) \mid (M \parallel K)$$

where  $M$  stands for any term.

We only define evaluation for closed terms, i.e.  $M \in (\Lambda_j^*)^\circ$ , by means of the rules given below. Our first two rules for evaluation just assert that the closures are their own normal form:

R1.1: $\langle \lambda x M, \sigma \rangle \Downarrow \langle \lambda x M, \sigma \rangle$	R1.2: $\langle \lambda^v x M, \sigma \rangle \Downarrow \langle \lambda^v x M, \sigma \rangle$
--	--

The next rules describe how to evaluate an application  $MN$ : to do so we have first to evaluate the operator  $M$  into a partial normal form, if any. Then there are three cases: if this partial normal



form for  $M$  is a call-by-name closure  $\langle \lambda x R, \rho \rangle$ , then we have to evaluate the body  $R$  of this closure in the updated environment  $[N/x]\rho$ , that is:

$$\text{R2.1 : } \frac{M \Downarrow \langle \lambda x R, \rho \rangle, R[N/x]\rho \Downarrow K}{(MN) \Downarrow K}$$

If the partial normal form for the operator  $M$  is a call-by-value closure  $\langle \lambda^v x R, \rho \rangle$ , then we have to evaluate the operand  $N$  into a partial normal form  $J$ , and then to evaluate the body  $R$  in the updated environment  $[J/x]\rho$ , that is:

$$\text{R2.2 : } \frac{M \Downarrow \langle \lambda^v x R, \rho \rangle, N \Downarrow J, R[J/x]\rho \Downarrow K}{(MN) \Downarrow K}$$

Note that these two rules implicitly call for the substitution procedure that has to return a term for  $R[N/x]\rho$  or  $R[J/x]\rho$ . One should remark that the rule R2.2 is not exactly the one of Plotkin's  $\lambda_v$ -calculus [34], since here a variable is not taken as a "value".

The last case of the evaluation of an application  $MN$  is the one where the partial normal form we get for the operand  $M$  is a parallel combination  $(M_0 \parallel M_1)$ . In this case the evaluation proceeds by distributing the operand  $N$  to the concurrent components, that is:

$$\text{R2.3 : } \frac{M \Downarrow (M_0 \parallel M_1), (M_0 N \parallel M_1 N) \Downarrow K}{(MN) \Downarrow K}$$

Let us see an example of evaluation using these rules: since  $(\lambda y(xx))[M/x]\varepsilon = \langle \lambda y(xx), [M/x]\varepsilon \rangle$  and  $\lambda x \lambda y(xx) \Downarrow \lambda x \lambda y(xx)$ , one has:

$$\Upsilon_* \Downarrow \langle \lambda y(xx), [\lambda x \lambda y(xx)]/x \varepsilon \rangle$$

Moreover

$$(xx)[X/y][\lambda x \lambda y(xx)]/x \varepsilon = \Upsilon_*$$

therefore

$$\Upsilon_* X \Downarrow \langle \lambda y(xx), [\lambda x \lambda y(xx)]/x \varepsilon \rangle$$

Our last rules for evaluation concern the concurrent join. They simply assert that to evaluate  $(M \parallel N)$ , one has to evaluate  $M$  or  $N$  and join the partial normal forms, that is:

$$\text{R3.1 : } \frac{M \Downarrow K}{(M \parallel N) \Downarrow (K \parallel N)} \quad \text{R3.2 : } \frac{N \Downarrow J}{(M \parallel N) \Downarrow (M \parallel J)}$$

$$\text{R3.3 : } \frac{M \Downarrow K, N \Downarrow J}{(M \parallel N) \Downarrow (K \parallel J)}$$

It should be clear that although we have some choice in evaluating  $(M \parallel N)$ , the rules R3's would preserve a Church-Rosser property, that is:

$$M \Downarrow K_0 \ \& \ M \Downarrow K_1 \Rightarrow \exists K. K_0 \Downarrow K \ \& \ K_1 \Downarrow K$$

However, this property fails to hold, owing to the rule R2.2: if  $M$  has two distinct partial normal forms  $K_0$  and  $K_1$ , as it is generally the case if  $M = (M_0 \parallel M_1)$ , then  $(\lambda^v x \lambda y R)M$  will converge to the partial normal forms  $\langle \lambda y R, [K_0/x]\varepsilon \rangle$  and  $\langle \lambda y R, [K_1/x]\varepsilon \rangle$ , and these two have no common partial normal form. However we shall see that the non-determinism of the evaluation mechanism does not create real conflicts: in fact evaluating the environment part of a closure would not be incorrect. This will be shown in the next section. To this end we shall use the following facts about evaluation:

**LEMMA 2.2.**

- (i) if  $K$  is a partial normal form then  $K \Downarrow K$
- (ii)  $M \Downarrow K \ \& \ K \Downarrow L \Rightarrow M \Downarrow L$
- (iii)  $(MN) \Downarrow K \Leftrightarrow \exists L. M \Downarrow L \ \& \ (LN) \Downarrow K.$

**PROOF:** the first point should be obvious. One shows the second one by induction on the inference of  $M \Downarrow K$ . Let us see the case of R3.1, that is  $M = (P \parallel Q)$  and  $K = (J \parallel Q)$  with  $P \Downarrow J$ . Then  $K \Downarrow L$  can only be proved using R3.1, R3.2 or R3.3; in this last case we have  $L = (J' \parallel Q')$  with  $J \Downarrow J'$  and  $Q \Downarrow Q'$ , therefore  $P \Downarrow J'$  by induction hypothesis, and  $M \Downarrow L$  by R3.3. The other cases are left to the reader.

For what regards the third point, the implication  $(MN) \Downarrow K \Rightarrow \exists L. M \Downarrow L \ \& \ (LN) \Downarrow K$  should be clear, since  $(MN) \Downarrow K$  can only be proved using R2.1, R2.2 or R2.3, and each of these rules implies  $M \Downarrow L$  for some  $L$  (note that, by the first point of the lemma,  $L \Downarrow L$ ). Conversely one proves  $M \Downarrow L \ \& \ (LN) \Downarrow K \Rightarrow (MN) \Downarrow K$  by induction on the proof of  $M \Downarrow L$ . The details are omitted  $\square$

We shall say that a closed term  $M$  is *convergent* (resp. *divergent*), in notation  $M \Downarrow$  (resp.  $M \Uparrow$ ), if it has a value, that is there exists  $K$  such that  $M \Downarrow K$  (resp. there is no such  $K$ ). It should be clear that  $\Omega \Uparrow$  for instance, since a proof of  $\Omega \Downarrow K$  would call for a shorter proof of the same fact, and that the following holds:

$$M \Uparrow \Rightarrow MN \Uparrow$$

Moreover in the call-by-value calculus  $\lambda^v$  we also have:

$$N \Uparrow_v \Rightarrow MN \Uparrow_v$$

## 2.2 Reduction. Preliminary Results.

In this section we establish some results regarding substitutions and a notion of reduction. Let us first define a congruence relation  $M \equiv N$ , meaning “ $M$  and  $N$  are the same, up to some garbage collection”. The “garbage collection” operates on the environment part of the closures. Typically we will have  $\langle \lambda x M, \sigma \rangle \equiv \langle \lambda x M, \rho \rangle$  if  $\sigma(z) = \rho(z)$  for all  $z \in \text{fv}(M) - \{x\}$ , and similarly for the strict closures. Then this relation, which will be called gc-equivalence, is the least one such that:

- (i)  $M \equiv M$  and  
 $M \equiv M' \Rightarrow M' \equiv M$  and  
 $M \equiv M'' \ \& \ M'' \equiv M' \Rightarrow M \equiv M'$
- (ii)  $M \equiv M' \Rightarrow \begin{cases} (MN) \equiv (M'N) \ \& \ (NM) \equiv (NM') \\ (M \parallel N) \equiv (M' \parallel N) \ \& \ (N \parallel M) \equiv (N \parallel M') \end{cases}$
- (iii)  $(\forall z \in \text{fv}(M) - \{x\}. \sigma(z) \equiv \rho(z)) \Rightarrow \begin{cases} \langle \lambda x M, \sigma \rangle \equiv \langle \lambda x M, \rho \rangle \\ \langle \lambda^v x M, \sigma \rangle \equiv \langle \lambda^v x M, \rho \rangle \end{cases}$

An obvious remark is:  $M \equiv N \Rightarrow \text{fv}(M) = \text{fv}(N)$ .

LEMMA 2.3.

- (i)  $\forall x \in \text{fv}(M). \sigma(x) \equiv \rho(x) \Rightarrow M\sigma \equiv M\rho$
- (ii)  $M \equiv N \Rightarrow M\sigma \equiv N\sigma$

PROOF: for the first point one proceeds by induction on  $M$ . The only case deserving some consideration is the case of closures. So let us assume that  $M = \langle \lambda x N, \varsigma \rangle$  for instance. Then  $M\sigma = \langle \lambda x N, \varsigma \circ \sigma \rangle$ , and for all  $z \in \text{fv}(N) - \{x\}$  we have  $(\varsigma(z))\sigma \equiv (\varsigma(z))\rho$  by induction hypothesis, and  $(\varsigma(z))\sigma = (\varsigma \circ \sigma)(z)$  by the lemma 2.1, and similarly  $(\varsigma(z))\rho = (\varsigma \circ \rho)(z)$ , therefore  $M\sigma \equiv M\rho$  by definition of the equivalence.

For the second point, one proceeds by induction on the definition of  $M \equiv N$ . If this is obtained using the last clause of the definition, we have  $M = \langle \lambda x R, \varsigma \rangle$  and  $N = \langle \lambda x R, \rho \rangle$  with  $\varsigma(z) \equiv \rho(z)$  for all  $z \in \text{fv}(R) - \{x\}$  (or  $M$  and  $N$  are strict closures). Since by the lemma 2.1 we have  $(\varsigma \circ \sigma)(z) = (\varsigma(z))\sigma$  and  $(\rho \circ \sigma)(z) = (\rho(z))\sigma$ , by induction hypothesis  $(\varsigma \circ \sigma)(z) \equiv (\rho \circ \sigma)(z)$ , therefore  $M\sigma \equiv N\sigma$  by definition of the equivalence. All the other cases are easy  $\square$

An obvious consequence is:

COROLLARY 2.4.  $M \equiv N \ \& \ \forall x \in \text{fv}(M). \sigma(x) \equiv \rho(x) \Rightarrow M\sigma \equiv N\rho$

For instance we have

$$x \notin \text{fv}(M) \Rightarrow M[R/x]\sigma \equiv M\sigma$$

Note also that if  $M$  is closed then  $M\sigma \equiv M$ , since  $M\sigma \equiv M\varepsilon = M$ .

Now we introduce a notion of *reduction*  $M \triangleright N$ , between closed terms, to be read “ $N$  is a reduction of  $M$ ”. This relation, extending the usual  $\beta$ -reduction – except that the  $\xi$ -rule is limited to reduction in the environment part of the closures –, will provide us with an alternative presentation of the operational semantics. Since we want to show a Church-Rosser property for reduction, we will allow to reduce simultaneously several redexes in a given term. Then the reduction relation is the least relation on closed terms satisfying:

- (i)  $M \triangleright M$
- (ii)  $(\forall z \in \text{fv}(M) - \{x\}. \sigma(z) \triangleright \rho(z)) \Rightarrow \begin{cases} \langle \lambda x M, \sigma \rangle \triangleright \langle \lambda x M, \rho \rangle \\ \langle \lambda^v x M, \sigma \rangle \triangleright \langle \lambda^v x M, \rho \rangle \end{cases}$
- (iii)  $M \triangleright M' \ \& \ N \triangleright N' \Rightarrow \begin{cases} (MN) \triangleright (M'N') \\ (M \parallel N) \triangleright (M' \parallel N') \end{cases}$

- (iv)  $\langle \lambda x M, \sigma \rangle N \triangleright M[N/x]\sigma$  and  
 $\langle \lambda^v x M, \sigma \rangle K \triangleright M[K/x]\sigma$  if  $K$  is a partial normal form, and  
 $(M_0 \parallel M_1)N \triangleright (M_0 N \parallel M_1 N)$

An obvious remark is:

**REMARK 2.5.** If  $K$  is a partial normal form and  $K \triangleright N$  then  $N$  is a partial normal form.

Another observation is that gc-equivalent terms may be reduced to each other:

**LEMMA 2.6.** For  $M$  closed  $M \equiv N \Rightarrow M \triangleright N \ \& \ N \triangleright M$ .

**PROOF:** by induction on the definition of  $M \equiv N$ , trivial  $\square$

To establish the Church-Rosser property, we need first to show the following:

**LEMMA 2.7.** If  $\sigma_0(x) \triangleright \sigma_1(x)$  for any  $x \in \text{fv}(M)$  then  $M\sigma_0 \triangleright M\sigma_1$ .

**PROOF:** by induction on the term  $M$ . Let us just see the case  $M = \langle \lambda x R, \rho \rangle$ . Then, for  $i = 0, 1$   $M\sigma_i = \langle \lambda x R, \rho_i \rangle$  where  $\rho_i = (\rho \circ \sigma_i)$ , that is  $\rho_i(z) = (\rho(z))\sigma_i$  (see the lemma 2.1). By induction hypothesis  $\rho_0(z) \triangleright \rho_1(z)$  for any  $z \in \text{fv}(R) - \{x\}$ , hence  $M\sigma_0 \triangleright M\sigma_1$  by definition of the reduction relation. All the other cases are left to the reader  $\square$

Now we show that the reduction relation has the Church-Rosser property:

**LEMMA (the CHURCH-ROSSER PROPERTY) 2.8.**  $M \triangleright K_0 \ \& \ M \triangleright K_1 \Rightarrow \exists K. K_0 \triangleright K \ \& \ K_1 \triangleright K$

**PROOF:** this is trivial if  $K_0 = M$  or  $K_1 = M$  or  $K_0 = K_1$ . Then we shall assume  $K_i \neq M$  and  $K_0 \neq K_1$ . We proceed by induction on  $M$ , examining the possible critical pairs. In fact we can, by symmetry, restrict our investigations to the following cases:

- if  $M = \langle \lambda x R, \sigma \rangle$  then  $K_i = \langle \lambda x R, \sigma_i \rangle$  with  $\sigma(z) \triangleright \sigma_i(z)$  for any  $z \in \text{fv}(R) - \{x\}$ . By induction hypothesis, for any  $z \in \text{fv}(R) - \{x\}$  there exists  $\rho(z)$  such that  $\sigma_i(z) \triangleright \rho(z)$ . Therefore we may let  $K = \langle \lambda x R, \rho \rangle$ . The case of  $M = \langle \lambda^v x R, \sigma \rangle$  is entirely similar.

- if  $M = (PQ)$  with  $K_0 = (P'Q')$ ,  $P \triangleright P'$  and  $Q \triangleright Q'$  then there are four cases. The first one, where  $K_1 = (P''Q'')$ ,  $P \triangleright P''$  and  $Q \triangleright Q''$  is obvious: one simply uses the induction hypothesis. If  $P = \langle \lambda x R, \sigma \rangle$  and  $K_1 = R[Q/x]\sigma$ , then  $P' = \langle \lambda x R, \rho \rangle$  with  $\sigma(z) \triangleright \rho(z)$  for any  $z \in \text{fv}(R) - \{x\}$ . Let  $K = R[Q'/x]\rho$ ; then  $K_0 \triangleright K$  by definition of the reduction relation, and  $K_1 \triangleright K$  by the previous lemma. The case of  $P = \langle \lambda^v x R, \sigma \rangle$  and  $K = R[Q/x]\sigma$ , where  $Q$  is a partial normal form, is entirely similar (from the remark 2.5  $Q'$  is also a partial normal form). Finally if  $P = (P_0 \parallel P_1)$  and  $K_1 = (P_0 Q \parallel P_1 Q)$ , then it is easy to see that  $P' = (P'_0 \parallel P'_1)$  with  $P_i \triangleright P'_i$ . We let  $K = (P'_0 Q' \parallel P'_1 Q')$ ; clearly  $K_0 \triangleright K$  since  $K_0 = (P'_0 \parallel P'_1)Q'$ . Moreover  $P_i Q \triangleright P'_i Q'$  by definition of the reduction relation, therefore  $K_1 \triangleright K$ .

- if  $M = (P \parallel Q)$  then clearly  $K_i = (P_i \parallel Q_i)$  with  $P \triangleright P_i$  and  $Q \triangleright Q_i$ , and we simply use the induction hypothesis  $\square$

Let us denote by  $N \triangleleft M$  the converse of the reduction relation. Now we introduce a relation of *conversion*  $M \bowtie N$  between closed terms. As usual this is just the reflexive and transitive closure of  $\triangleright \cup \triangleleft$ , that is:

$$M \bowtie N \Leftrightarrow_{\text{def}} M(\triangleright \cup \triangleleft)^* N$$

Clearly this convertibility relation is an equivalence, and an obvious consequence of the Church-Rosser property is:

**COROLLARY 2.9.**  $M \bowtie N \Leftrightarrow \exists R. M \triangleright^* R \ \& \ N \triangleright^* R$

To conclude this section we relate the reduction relation and the evaluation relation introduced in the previous section. More precisely, we show that if a term has a value, then it reduces to this value, and that reduction and evaluation commute:

LEMMA 2.10.

- (i)  $M \Downarrow K \Rightarrow M \triangleright^* K$
- (ii)  $M \triangleright N \ \& \ N \Downarrow K \Rightarrow \exists L. M \Downarrow L \ \& \ L \triangleright K$

PROOF: we prove the first point by induction on the inference of  $M \Downarrow K$ . Let us just see the case of R2.2:  $M = (PQ)$ ,  $P \Downarrow \langle \lambda^v x R, \sigma \rangle$ ,  $Q \Downarrow J$  and  $R[J/x]\sigma \Downarrow K$ . Then by induction hypothesis  $P \triangleright^* \langle \lambda^v x R, \sigma \rangle$  and  $Q \triangleright^* J$ , therefore  $M \triangleright^* \langle \lambda^v x R, \sigma \rangle J$ , hence  $M \triangleright^* R[J/x]\sigma$  since  $J$  is a partial normal form, and finally  $M \triangleright^* K$  by induction hypothesis on  $R[J/x]\sigma \Downarrow K$ . The other cases are left to the reader.

For the second point we proceed by induction on the proof of  $N \Downarrow K$ , and then by case on the definition of  $M \triangleright N$ . In fact we can factorize three cases for  $M \triangleright N$ : first, the result is trivial if  $M = N$ . Moreover, if  $M = \langle \lambda x P, \rho \rangle Q$  and  $N = P[Q/x]\rho$  then  $M \Downarrow K$  by R2.1, and similarly if  $M = \langle \lambda^v x P, \rho \rangle Q$  and  $N = P[Q/x]\rho$ , where  $Q$  is a partial normal form, then  $M \Downarrow K$  by R2.2 since  $Q \Downarrow Q$ . These cases will not be taken into account in the following proof.

- if  $N \Downarrow K$  is proved using R1.1, then  $N = K = \langle \lambda x R, \sigma \rangle$ . The only possibility for inferring  $M \triangleright \langle \lambda x R, \sigma \rangle$  – apart from the cases mentioned above – is  $M = \langle \lambda x R, \rho \rangle$  with  $\rho(z) \triangleright \sigma(z)$  for any  $z \in \text{fv}(R) - \{x\}$ . This case is trivial since  $M \Downarrow M$ .

- the proof is similar if  $N \Downarrow K$  is inferred using R1.2.

- if  $N \Downarrow K$  is proved using R2.2 (we shall not investigate the case of R2.1, which is entirely analogous) then  $N = (PQ)$  with  $P \Downarrow \langle \lambda^v x R, \sigma \rangle$ ,  $Q \Downarrow J$  and  $R[J/x]\sigma \Downarrow K$ . Again the only possibility for inferring  $M \triangleright N$  we have to consider is:  $M = (P'Q')$  with  $P' \triangleright P$  and  $Q' \triangleright Q$ . Then by induction hypothesis there exist  $P''$  and  $J'$  such that  $P' \Downarrow P'' \triangleright \langle \lambda^v x R, \sigma \rangle$  and  $Q' \Downarrow J' \triangleright J$ . Since  $P''$  is a partial normal form we have  $P'' = \langle \lambda^v x R, \rho \rangle$  with  $\rho(z) \triangleright \sigma(z)$  for any  $z \in \text{fv}(R) - \{x\}$ . Then by the lemma 2.7  $R[J'/x]\rho \triangleright R[J/x]\sigma$ , therefore by induction hypothesis there exists  $L$  such that  $R[J'/x]\rho \Downarrow L \triangleright K$ , and  $M \Downarrow L$  by R2.2.

- if  $N \Downarrow K$  is proved by means of R2.3 then  $N = (PQ)$  with  $P \Downarrow (P_0 \parallel P_1)$  and  $(P_0 Q \parallel P_1 Q) \Downarrow K$ . Assume that  $M = (P'Q')$  with  $P' \triangleright P$  and  $Q' \triangleright Q$ . By induction hypothesis there exist  $P''$  such that  $P' \Downarrow P'' \triangleright (P_0 \parallel P_1)$ . Since  $P''$  is a partial normal form we have  $P'' = (P'_0 \parallel P'_1)$  with  $P'_i \triangleright P_i$ , therefore  $P'_i Q \triangleright P_i Q'$ , hence  $(P'_0 Q \parallel P'_1 Q) \triangleright (P_0 Q' \parallel P_1 Q')$ . By induction hypothesis there exists  $L$  such that  $(P'_0 Q \parallel P'_1 Q) \Downarrow L$  and  $L \triangleright K$ , therefore  $M \Downarrow L$  by R2.3.

The remaining cases (R3.1, R3.2 and R3.3) are left to the reader  $\square$

COROLLARY 2.11.  $M \bowtie N \Rightarrow M \Downarrow \Leftrightarrow N \Downarrow$

PROOF: if  $M \Downarrow K$  then  $M \triangleright^* K$  by the previous lemma, therefore  $M \bowtie N \ \& \ M \Downarrow K \Rightarrow N \bowtie K$ . By the corollary 2.9 there exists  $R$  such that  $N \triangleright^* R$  and  $K \triangleright^* R$ . Since  $K$  is a partial normal form,  $R$  is also a partial normal form, hence  $R \Downarrow R$ , and an obvious consequence of the previous lemma is  $N \triangleright^* R \ \& \ R \Downarrow \Rightarrow N \Downarrow \square$

The results about conversion we shall use later can be summarized as follows:

PROPOSITION 2.12. *The conversion relation  $\bowtie$  has the following properties:*

- (i)  $M \equiv N \Rightarrow M \bowtie N$
- (ii)  $M \bowtie N \Rightarrow M \Downarrow \Leftrightarrow N \Downarrow$

- (iii)  $M \bowtie N \Rightarrow (MR) \bowtie (NR)$
- (iv)  $\langle \lambda x M, \sigma \rangle N \bowtie M[N/x]\sigma$
- (v)  $N \Downarrow \Rightarrow \langle \lambda^v x M, \sigma \rangle N \bowtie M[N/x]\sigma$

**PROOF:** the first and second points have already been established. The third and fourth point result directly from the definition of the reduction relation. The last point is true since  $N \Downarrow$  implies  $N \triangleright^* J$  for some partial normal form  $J$ , therefore we have  $\langle \lambda^v x M, \sigma \rangle N \triangleright^* \langle \lambda^v x M, \sigma \rangle J \triangleright M[J/x]\sigma$ , and  $M[N/x]\sigma \triangleright^* M[J/x]\sigma$  (lemma 2.7)  $\square$

### 3. Semantics.

#### 3.1 The Canonical Domains.

In this section we introduce the domains  $D_\star$  and  $D_\mathfrak{s}$  that we shall use to interpret the  $\lambda_\star^\dagger$  and  $\lambda_\mathfrak{s}^\dagger$  calculi. These domains are respectively the initial solutions of the equations:

$$D = (D \rightarrow D)_\perp$$

and

$$\begin{cases} D = V_\perp & \text{where} \\ V = (V \rightarrow D) \end{cases}$$

where  $X_\perp$  is the usual *lifting* of  $X$ , adjoining a new bottom element to  $X$ , and  $(X \rightarrow Y)$  is the domain of *continuous functions* from  $X$  to  $Y$ . It is worth noting that the initial solutions of these equations yield *prime algebraic lattices* (cf. [31]).

This section will be quite allusive – in particular no proof will be given. The reason is that we regard the *logical interpretation*, given below, as the actual interpretation. Here we will begin with some abstract concepts, and introduce the logical content of these concepts by gradual changes in the notations: first we recall some definitions concerning lattices, which will be dealt with using Scott's information systems [43]. This will provides us with an explicit presentation of the canonical domains  $D_\star$  and  $D_\mathfrak{s}$ , using standard means to solve recursive domain equations (see for instance Larsen & Winskel 84[22]). Finally we will get a logical characterization à la Coppo [12,13] of our domains by giving a syntax for the canonical information systems.

##### 3.1.1 Algebraic Lattices.

We first recall some standard definitions concerning lattices. A *complete lattice* is a partial order  $(L, \sqsubseteq)$  such that each subset  $X$  of  $L$  has a least upper bound  $\bigsqcup X$ . The least upper bound of two elements  $x$  and  $y$  is their *join*  $x \sqcup y$ . A complete lattice has a least and a greatest element, namely  $\perp = \bigsqcup \emptyset$  and  $\top = \bigsqcup L$ . The *lifting* construct builds a complete lattice  $L_\perp$  out of a given complete lattice  $L$ : this simply consists in adding a new bottom element. A subset  $X$  of  $L$  is *directed* if for any finite subset  $Y$  of  $X$  there exists  $x \in X$  such that  $\bigsqcup Y \sqsubseteq x$  (therefore a directed set is non-empty). Given two complete lattices  $L_0$  and  $L_1$ , a function  $f: L_0 \rightarrow L_1$  is *continuous* iff it preserves the joins of directed subsets, that is iff for any directed subset  $X$  of  $L$  we have  $f(\bigsqcup X) = \bigsqcup f(X)$ . The set  $(L_0 \rightarrow L_1)$  of continous functions, extensionally ordered, i.e.  $f \sqsubseteq g \Leftrightarrow_{\text{def}} \forall x \ f(x) \sqsubseteq_1 g(x)$ , is a complete lattice.

An element  $c$  of a complete lattice  $L$  is *compact* iff for any subset  $X$  of  $L$  such that  $c \sqsubseteq \bigsqcup X$  there exists a finite subset  $Y$  of  $X$  such that  $c \sqsubseteq \bigsqcup Y$ . We shall use  $\mathcal{K}(L)$  to denote the set of

compact elements of  $L$ . A complete lattice is *algebraic* if any element  $e$  of  $L$  is the join of the compact points it dominates:

$$e = \bigsqcup \{c \mid c \in \mathcal{K}(L) \text{ \& } c \sqsubseteq e\}$$

The representation of algebraic lattices by means of information systems will rest upon the following well-known characterization: *every algebraic lattice is isomorphic to the family of ideals of a join-semilattice with bottom element*. Let us spell out this statement: a join semilattice with bottom is a partial order such that any finite subset has a join. An ideal is a directed cone, that is a directed subset  $X$  such that  $x \in X \text{ \& } y \sqsubseteq x \Rightarrow y \in X$ . By a *family* we mean any set of sets, ordered by inclusion.

A fundamental fact about algebraic lattices is that a continuous function  $f$  from an algebraic lattice  $L_0$  to an algebraic lattice  $L_1$  is uniquely determined by the set of pairs:

$$\mathbf{graph}(f) = \{(c, d) \mid c \in \mathcal{K}(L_0), d \in \mathcal{K}(L_1) \text{ \& } d \sqsubseteq_1 f(c)\}$$

We could say that a pair  $(c, d) \in \mathbf{graph}(f)$  is an “element of information” about the function  $f$ , requiring the information  $c$  on the input to produce the information  $d$  on the output. Note that the information  $(c, d)$  is better than  $(c', d')$  if it requires less – i.e.  $c \sqsubseteq_0 c'$  – to produce more – i.e.  $d' \sqsubseteq_1 d$ . This is the basic idea of the concrete representation of continuous functions over algebraic lattices that will be used below.

As we shall see our canonical domains have a property stronger than algebraicity, namely they are prime algebraic lattices. Let us recall the definition, taken from Nielsen, Plotkin & Winskel [31]. First we say that an element  $p$  of a lattice  $L$  is *prime* iff  $p \sqsubseteq x \sqcup y$  implies  $p \sqsubseteq x$  or  $p \sqsubseteq y$ . Note that  $\perp$  is prime according to our terminology. We shall denote by  $\mathcal{P}(L)$  the set of prime elements of  $L$ , and by  $\mathcal{KP}(L)$  the set of compact prime elements – these are, apart from  $\perp$ , the “complete primes” of [31]. Then a complete lattice is *prime algebraic* if any element  $e$  of  $L$  is the join of the compact primes it dominates:

$$e = \bigsqcup \{c \mid c \in \mathcal{KP}(L) \text{ \& } c \sqsubseteq e\}$$

Note that if  $c$  is compact then it is the join of a *finite* number of compact primes, that is  $c = p_1 \sqcup \dots \sqcup p_n$  for some  $p_i \in \mathcal{KP}(L)$ .

We shall not use here the characterization of prime algebraic lattices given by Nielsen, Plotkin & Winskel, but it is worth noting that any prime algebraic lattice is a kind of powerdomain. Given any poset  $(P, \sqsubseteq)$ , we could define the *lower powerdomain*, or Hoare powerdomain  $P^b$  of this poset as the family of ideals of the pre-ordered set  $(\mathbf{Fin}(P), \sqsubseteq^b)$ , where  $\mathbf{Fin}(P)$  is the set of finite non-empty subsets of  $P$ , and  $u \sqsubseteq^b v$  is given by:

$$u \sqsubseteq^b v \Leftrightarrow_{\text{def}} \forall x \in u \exists y \in v. x \sqsubseteq y$$

For instance if the poset  $(P, \sqsubseteq)$  is discrete, that is  $\sqsubseteq$  is the equality, then its lower powerdomain is just (isomorphic to) the powerset of  $P$ , that is the set of subsets of  $P$ , ordered by inclusion. The union in  $P^b$  is given by:

$$X \sqcup Y =_{\text{def}} \{u \cup v \mid u \in X \text{ \& } v \in Y\}$$

Usually one uses this definition of powerdomain when  $P$  is the set of compact elements of some domain. Here we will use it as follows: given a prime algebraic lattice  $(L, \sqsubseteq)$  we define its *prime powerdomain*  $\mathcal{H}(L)$  as the lower powerdomain of the poset  $(\mathcal{KP}(L), \sqsubseteq)$  of compact prime elements of  $L$ . Then we have:

**LEMMA.** *Any prime algebraic lattice is isomorphic to its own prime powerdomain:  $L \cong \mathcal{H}(L)$ . Moreover the union in  $\mathcal{H}(L)$  corresponds to the join in  $L$ .*

### 3.1.2 Information Systems.

We can give a more concrete formulation of the afore mentioned characterization of algebraic lattices, using Scott's notion of information system. Since we are interested in lattices, the information systems we use do not involve the consistency predicate. Moreover, we shall disallow the empty set to enter into consideration. Then our definition is as follows:

**DEFINITION (INFORMATION SYSTEMS) 3.1.** An information system is a structure  $S = (A, \Delta, \vdash)$  where  $A$  is the set of atoms,  $\Delta \in A$  and  $\vdash$  is a relation over finite non-empty subsets of  $A$  satisfying:

$$D1: u \vdash \{\Delta\}$$

$$D2: u \vdash v \ \& \ v \vdash w \Rightarrow u \vdash w$$

$$D3: u \subseteq v \Rightarrow v \vdash u$$

$$D4: u \vdash v \ \& \ u \vdash w \Rightarrow u \vdash v \cup w$$

Let us introduce some notations:  $\mathbf{Fin}(A)$  is the set of finite non-empty subsets of  $A$ , ranged over by  $u, v, w \dots$ . Sometimes we shall denote  $u \vdash v$  by  $a_1, \dots, a_n \vdash b_1, \dots, b_k$  when  $u = \{a_1, \dots, a_n\}$  and  $v = \{b_1, \dots, b_k\}$ . For instance  $a_1, \dots, a_n \vdash \Delta$  in any information system.

A basic example is the following: let  $(K, \sqsubseteq)$  be a join semilattice with bottom  $\perp$ . Then it is easy to see that the structure  $(K, \perp, \vdash)$  where  $\vdash$  is given by

$$a_1, \dots, a_n \vdash b_1, \dots, b_k \Leftrightarrow_{\text{def}} (b_1 \sqcup \dots \sqcup b_k) \sqsubseteq (a_1 \sqcup \dots \sqcup a_n)$$

is an information structure.

According to Scott, we may interpret the atoms  $a \in A$  of an information structure as the "propositions" that can be made about the "elements" described by the information structure. The "proposition"  $\Delta$  means true, and the deduction (or entailment) relation  $u \vdash v$  formalizes the idea that if the "propositions" of  $u$  are true of some element, then the "propositions" of  $v$  are also true of the same element. In fact, an element is just the set of propositions true of it. Then the domain of  $S$  is the family  $(\mathcal{D}(S), \subseteq)$  of non-empty, deductively closed subsets of  $A$ , that is:

$$X \in \mathcal{D}(S) \Leftrightarrow_{\text{def}} \begin{cases} X \subseteq A \ \& \ \Delta \in X \\ u \subseteq X \ \& \ u \vdash v \Rightarrow v \subseteq X \end{cases} \quad \text{and}$$

Remark: for any deductively closed subset  $X$  of  $A$  we have  $X \neq \emptyset \Leftrightarrow \Delta \in X$ , since  $u \vdash \Delta$  for any  $u \in \mathbf{Fin}(A)$ . We shall also call the elements of  $\mathcal{D}(S)$  the configurations of  $S$ . For instance, given a non-empty subset  $X$  of  $A$ , the set:

$$\overline{X} =_{\text{def}} \bigcup \{v \mid \exists u \subseteq X. u \vdash v\}$$

is an element of  $\mathcal{D}(S)$ , the least one containing  $X$ . Note that this element is also:

$$\overline{X} = \bigcap \{U \mid U \in \mathcal{D}(S) \ \& \ X \subseteq U\}$$

In this last formula, the subset  $X$  of  $A$  can be empty; we shall call this set  $\overline{X}$  the closure of  $X$ . It can be noted that, for  $u, v \in \mathbf{Fin}(A)$ :

$$v \subseteq \overline{u} \Leftrightarrow u \vdash v$$

Returning to our previous basic example, we can see that for a join semilattice  $(K, \sqsubseteq)$  with bottom  $\perp$ , the elements of the domain of the information structure  $(K, \perp, \vdash)$  – as defined above – are the ideals of the poset  $(K, \sqsubseteq)$ . More generally, information structures provide us with a concrete presentation of algebraic lattices:



**PROPOSITION.** A poset  $(L, \sqsubseteq)$  is an algebraic lattice if and only if it is isomorphic to the domain of an information structure. More precisely:

- (i) for any information system the poset  $(\mathcal{D}(S), \sqsubseteq)$  is an algebraic lattice, whose compact elements are the sets  $\bar{u}$  for  $u \in \mathbf{Fin}(A)$
- (ii) any algebraic lattice  $(L, \sqsubseteq)$  is isomorphic to the family of ideals of the join semilattice with bottom of its compact elements  $(\mathcal{K}(L), \sqsubseteq)$ .

In particular, it is easy to see that for all  $X \in \mathcal{D}(S)$ :

$$X = \bigcup_{u \subseteq X} \bar{u}$$

In  $\mathcal{D}(S)$ , we can describe the join as follows:

$$X \sqcup Y = \overline{X \cup Y}$$

We mentioned that the continuous functions between complete lattices form a complete lattice. This lattice is algebraic (resp. prime algebraic) if the domain and range are algebraic (resp. prime algebraic). Then we can give an explicit description of the continuous functions, at the level of information systems: a continuous function  $f$  is represented by an *approximable mapping* between information systems, which is the set of pairs  $(u, v)$  such that  $(\bar{u}, \bar{v}) \in \mathbf{graph}(f)$ . This set has to satisfy some properties, listed in the following definition, adapted from Scott [43] (see also Coppo & al. 83[13]):

**DEFINITION (APPROXIMABLE MAPPINGS).** Let  $S_i = (A_i, \Delta_i, \vdash_i)$  for  $i = 0, 1$  be two information systems. An approximable mapping from  $S_0$  to  $S_1$  is a relation  $f$  from  $\mathbf{Fin}(A_0)$  to  $\mathbf{Fin}(A_1)$  such that:

- (i)  $\{\Delta_0\} f \{\Delta_1\}$
- (ii)  $u f v \ \& \ u f w \Rightarrow u f (v \cup w)$
- (iii)  $u' \vdash_0 u \ \& \ u f v \ \& \ v \vdash_1 v' \Rightarrow u' f v'$

An approximable mapping  $f$  from  $S_0$  to  $S_1$  represents a function  $\mathbf{fun}(f): \mathcal{D}(S_0) \rightarrow \mathcal{D}(S_1)$  given by:

$$\mathbf{fun}(f)(X) =_{\text{def}} \bigcup \{v \mid \exists u \subseteq X. u f v\}$$

This is more or less Plotkin's set-theoretical definition of application (see Barendregt [5]).

For instance it is easy to see that, given  $S = (A, \Delta, \vdash)$ , the relation  $\vdash$  is an approximable mapping over  $S$ , and that  $\mathbf{fun}(\vdash)$  is the identity function. Remark that for any approximable mapping  $f$  we have:

$$\mathbf{fun}(f)(\bar{u}) = \bigcup \{v \mid u f v\}$$

The approximable mappings concretely represent continuous functions:

**PROPOSITION.** If  $f$  is an approximable mapping from  $S_0$  to  $S_1$  then  $\mathbf{fun}(f)$  is a continuous function from  $\mathcal{D}(S_0)$  to  $\mathcal{D}(S_1)$ . Conversely, if  $g$  is a continuous function from  $\mathcal{D}(S_0)$  to  $\mathcal{D}(S_1)$  then the relation  $\mathbf{map}(g)$  given by:

$$(u, v) \in \mathbf{map}(g) \Leftrightarrow_{\text{def}} v \subseteq g(\bar{u})$$

is an approximable mapping such that  $g = \mathbf{fun}(\mathbf{map}(g))$ . This establishes an isomorphism between the poset of continuous functions, extensionally ordered, and the family of approximable mappings, ordered by inclusion.

### 3.1.3 Construction of the Canonical Domains.

Now we use the information systems to solve the domain equations  $D = (D \rightarrow D)_\perp$  and  $D = V_\perp$  where  $V = (V \rightarrow D)$ . We have to give two constructions on information systems, respectively representing the lifting construct and the exponentiation – or more accurately the family of approximable mappings.

It is very easy to define the lifting of information structures: let  $S = (A, \Delta, \vdash)$  be an information structure, and let us define  $S'$  as  $(A', \Delta', \vdash')$  where  $A' = A \cup \{\Delta'\}$  (with  $\Delta' \notin A$ ), and  $\vdash'$  is the least relation containing  $\vdash$  and satisfying D1-D4 of the definition 3.1. Then it is not difficult to see that  $\mathcal{D}(S')$  is isomorphic to  $(\mathcal{D}(S))_\perp$ , and more precisely:

$$X \in \mathcal{D}(S') \Leftrightarrow X = \{\Delta'\} \text{ or } \exists Y \in \mathcal{D}(S). X = \{\Delta'\} \cup Y$$

The second construct is the “exponentiation”: let  $S_i = (A_i, \Delta_i, \vdash_i)$  for  $i = 0, 1$  be two information systems. We define

$$(S_0 \rightarrow S_1) = (A, \Delta, \vdash)$$

as follows:

- (1)  $A$  is the set of pairs of finite non-empty subsets of  $A_0$  and  $A_1$ , that is  $A = \text{Fin}(A_0) \times \text{Fin}(A_1)$
- (2)  $\Delta = (\{\Delta_0\}, \{\Delta_1\})$
- (3)  $\vdash$  is the least relation satisfying D1-D4 of the definition 3.1, and
  - (3-1)  $(u, v), (u, w) \vdash (u, v \cup w)$
  - (3-2)  $u' \vdash_0 u \ \& \ v \vdash_1 v' \Rightarrow (u, v) \vdash (u', v')$

Note that due to the clause D1 of the definition 3.1 we have

$$(u_1, v_1), \dots, (u_n, v_n) \vdash (\{\Delta_0\}, \{\Delta_1\})$$

Then we can show that this is an appropriate representation of the domain of approximable mappings:

**LEMMA.**  $f \in \mathcal{D}(S_0 \rightarrow S_1)$  if and only if  $f$  is an approximable mapping from  $S_0$  to  $S_1$ .

A consequence of this result is that the poset  $(\mathcal{D}(S_0 \rightarrow S_1), \sqsubseteq)$  of continuous functions is isomorphic to  $(\mathcal{D}(S_0 \rightarrow S_1), \subseteq)$ . We are now ready to give the information systems describing the canonical domains; the constructions are very similar to the Plotkin-Scott-Engeler’s one, see Barendregt [5], definition 5.4.5. Intuitively the information system for  $D_\star$  is the least one that is closed for both the lifting and the exponentiation constructs:

**DEFINITION (the CANONICAL INFORMATION SYSTEM) 3.2.** *The canonical information system is  $S_\star = (A_\star, \Delta, \vdash_\star)$  where  $A_\star$  is the least set such that:*

- (i)  $\Delta \in A_\star$
- (ii)  $u, v \in \text{Fin}(A_\star) \Rightarrow (u, v) \in A_\star$

and  $\vdash_\star$  is the least relation on  $\text{Fin}(A_\star)$  satisfying the clauses D1-D4 of the definition 3.1, and also the clauses defining the exponentiation of information systems, that is:

- $D_\star 5:$   $u \in \text{Fin}(A_\star - \{\Delta\}) \Rightarrow u \vdash_\star (\{\Delta\}, \{\Delta\})$
- $D_\star 6:$   $(u, v), (u, w) \vdash_\star (u, v \cup w)$
- $D_\star 7:$   $u' \vdash_\star u \ \& \ v \vdash_\star v' \Rightarrow (u, v) \vdash_\star (u', v')$

Clearly if we let  $D_* = \mathcal{D}(S_*)$  then this domain satisfies the equation:

$$D_* = (D_* \rightarrow D_*)_{\perp}$$

For the strict canonical domain  $D_S$ , the definition is quite similar:

**DEFINITION (the STRICT CANONICAL INFORMATION SYSTEM) 3.3.** *The strict canonical information system is  $S_S = (A_S \cup \{\Delta\}, \Delta, \vdash_S)$  where  $A_S$  is the least set such that:*

(i)  $\nabla \in A_S$  with  $\nabla \neq \Delta$

(ii)  $u \in \text{Fin}(A_S) \ \& \ v \in \text{Fin}(A_S \cup \{\Delta\}) \Rightarrow (u, v) \in A_S$

and  $\vdash_S$  is the least relation on  $\text{Fin}(A_S) \cup \{\Delta\}$  satisfying the clauses D1-D4 of the definition 3.1, and also:

Ds5:  $u \in \text{Fin}(A_S) \Rightarrow u \vdash_S \{\nabla\} \ \& \ u \vdash_S (\{\nabla\}, \{\Delta\})$

Ds6:  $(u, v), (u, w) \vdash_S (u, v \cup w)$

Ds7:  $u' \vdash_S u \ \& \ v \vdash_S v' \Rightarrow (u, v) \vdash_S (u', v')$

Note that in Ds6 and Ds7 it is implicitly assumed that  $u, u' \in \text{Fin}(A_S)$  – otherwise we could not form  $(u, v \cup w)$ ,  $(u, v)$  and  $(u', v')$ . Clearly if we let  $D_S = \mathcal{D}(S_S)$  and  $V = D_S - \{\Delta\}$  then these domains satisfy the equations:

$$\begin{cases} D_S = V_{\perp} \\ V = (V \rightarrow D_S) \end{cases}$$

### 3.2 Logical Presentation of the Domains.

Information systems provide us with a concrete representation for algebraic lattices. In fact one can give an even more concrete presentation by using a *syntax* for information systems. This syntax will be a *logical* one: this formalizes Scott's intuitive explanations about information systems (cf. Coppo & al. 83[13], Dezani & Margaria 86[17], and Abramsky 87[2]).

The logical representation of algebraic lattices relies upon a statement *dual* to the one we used in introducing information systems, namely: *every algebraic lattice is isomorphic to the family of filters of a meet-semilattice with top element*. A meet semilattice with top element  $\top$  is a poset  $(K, \sqsubseteq)$  such that any finite subset  $Y$  has a meet, that is a greatest lower bound  $\prod Y$ . A filter is a subset  $X$  which is filtered (that is: for any finite subset  $Y$  of  $X$  there exists  $x \in X$  such that  $x \sqsubseteq \prod Y$ ) and satisfies  $x \in X \ \& \ x \sqsubseteq y \Rightarrow y \in X$ . Clearly a meet-semilattice  $(K, \sqsubseteq)$  with top  $\top$  determines an information structure  $(K, \vdash, \top)$  where  $\vdash$  is given by:

$$a_1, \dots, a_n \vdash b_1, \dots, b_k \Leftrightarrow (a_1 \sqcap \dots \sqcap a_n) \sqsubseteq (b_1 \sqcap \dots \sqcap b_k)$$

The domain of this information structure is the family of filters of  $(K, \sqsubseteq)$ .

The formulae of the logical language associated with a given information system  $S = (A, \Delta, \vdash)$  describe the finite non-empty subsets of  $A$ , that is elements of  $\text{Fin}(A)$ . We assume given an atomic proposition for each singleton  $\{a\}$  where  $a \in A$ . In particular we shall always use  $\omega$  to denote  $\{\Delta\}$ , so that  $\omega$  means “true”. The union of two elements  $u$  and  $v$  of  $\text{Fin}(A)$  respectively denoted by  $\phi$  and  $\psi$  will be denoted by  $\phi \wedge \psi$ , the conjunction of  $\phi$  and  $\psi$ . This is consistent with the interpretation of  $u \cup v$  as a set of propositions that can be made about some elements of the domain  $\mathcal{D}(S)$ . Then the logical language associated with  $S$  is the set of formulae given by the grammar:

$$\phi ::= p \mid \omega \mid (\phi \wedge \phi)$$

where  $p$  is any atomic proposition.

The next step is to represent the deduction relation  $\vdash$ . This is turned into an entailment relation between formulae,  $\phi \leq \psi$  (which could also be written  $\phi \Rightarrow \psi$ , that is “ $\psi$  is a consequence of  $\phi$ ”) corresponding to  $u \vdash v$ . Then for instance a deduction

$$a_1, \dots, a_n \vdash b_1, \dots, b_k$$

will be denoted by

$$p_1 \wedge \dots \wedge p_n \leq q_1 \wedge \dots \wedge q_k$$

Translating the clauses D1-D4 of the definition 3.1, we see that the entailment relation has to satisfy first the following two axioms corresponding to D1-D2:

$$\boxed{\text{E1: } \phi \leq \omega \quad \text{E2: } \frac{\phi \leq \tau, \tau \leq \psi}{\phi \leq \psi}}$$

To formulate D3 we remark that this requirement is equivalent to  $u \vdash u$  and  $u \cup v \vdash u$  (for  $u, v \in \text{Fin}(A)$ ). Since the conjunction is not a priori associative and commutative, we shall give two axioms for this last clause. Then we get:

$$\boxed{\text{E3.1: } \phi \leq \phi \quad \text{E3.2: } (\phi \wedge \psi) \leq \phi \quad \text{E3.3: } (\phi \wedge \psi) \leq \psi}$$

Then  $\leq$  is a preorder on formulae, and  $\omega$  is the greatest, or “most general” formula. Finally the axiomatization of D4 is:

$$\boxed{\text{E4: } \frac{\phi \leq \psi_0, \phi \leq \psi_1}{\phi \leq (\psi_0 \wedge \psi_1)}}$$

If we let:

$$\phi \sim \psi \Leftrightarrow_{\text{def}} \phi \leq \psi \ \& \ \psi \leq \phi$$

it is easy to see that:

$$\begin{aligned} \phi \wedge \omega &\sim \phi \\ \phi \wedge \psi &\sim \psi \wedge \phi \\ \phi \wedge (\psi \wedge \zeta) &\sim (\phi \wedge \psi) \wedge \zeta \end{aligned}$$

This allows us to use the notation  $\bigwedge_i \phi_i$  for finite conjunctions, up to  $\sim$  (with the convention that the empty conjunction is  $\omega$ ). One can also remark for instance that  $\phi \sim (\phi \wedge \phi)$ .

**REMARK 3.4.**  $\phi_0 \leq \psi_0 \ \& \ \phi_1 \leq \psi_1 \Rightarrow \phi_0 \wedge \phi_1 \leq \psi_0 \wedge \psi_1$

Finally we have to reflect in the logic the notion of element of the domain, that is deductively closed non-empty subset of  $A$ . As we saw above, the appropriate notion is that of a filter of formulae:

**DEFINITION (FILTERS).** A filter is a set  $F$  of formulae such that

- (i)  $\omega \in F$
- (ii)  $\phi \in F \ \& \ \psi \in F \Rightarrow \phi \wedge \psi \in F$
- (iii)  $\phi \in F \ \& \ \phi \leq \psi \Rightarrow \psi \in F$ .

For instance, for any formula  $\phi$  the set  $\phi\uparrow = \{\psi \mid \phi \leq \psi\}$  is a (principal) filter, generated by  $\phi$ . We let the reader convince him/herself that given an information system one can introduce some further axioms for entailment, so that the domain determined by the information system is isomorphic to the family of filters of this logic. We shall only detail the cases of  $S_*$  and  $S_s$ .

To deal with the exponentiation construct, we have to give a syntax for the finite non-empty sets of pairs  $(u, v)$  – in the strict case we also have to add a new propositional constant  $\gamma$  denoting  $\{\nabla\}$ . Taking advantage of the recursive nature of  $A_*$  and  $A_s$ , we can describe these pairs (or more precisely the singletons consisting of one of these pairs) as *implicative* formulae  $(\phi \rightarrow \psi)$ , and in the strict case  $(\zeta \rightarrow \phi)$  where  $\zeta$  and  $\phi$  respectively represent elements of  $\text{Fin}(A_s)$  and  $\text{Fin}(A_s \cup \{\Delta\})$ . An implicative formula  $\phi \rightarrow \psi$  represents an element of information about a function  $f$ , meaning that if we have the information  $\phi$  on the argument  $x$ , then we can be sure that the information  $\psi$  is true of the result  $f(x)$ . Then the logical language for  $D_*$  is as follows:

$$(\Phi_*) \quad \phi ::= \omega \mid (\phi \rightarrow \phi) \mid (\phi \wedge \phi)$$

As for  $D_s$  we have:

$$(\Phi_s) \quad \phi ::= \omega \mid \zeta \mid (\phi \wedge \phi)$$

$$(\Gamma) \quad \zeta ::= \gamma \mid (\zeta \wedge \zeta) \mid (\zeta \rightarrow \phi)$$

The proposition  $\gamma$  could be called the “existence proposition”, or the “convergence formula”, a name that will be justified later.

We shall denote by  $\leq_*$  and  $\leq_s$  the entailment relations respectively representing  $\vdash_*$  and  $\vdash_s$ . Both these relations have to satisfy the clauses E1-E4. Then  $\leq_*$  is the least relation on  $\Phi_*$  satisfying E1-E4 (where one should obviously replace  $\leq$  by  $\leq_*$ ), and the clauses corresponding to  $D_{*5}$ - $D_{*7}$ , that is:

$$E_{*5}: (\phi \rightarrow \omega) \leq_* (\omega \rightarrow \omega) \quad E_{*6}: ((\phi \rightarrow \phi_0) \wedge (\phi \rightarrow \phi_1)) \leq_* (\phi \rightarrow (\phi_0 \wedge \phi_1))$$

$$E_{*7}: \frac{\phi_0 \geq_* \phi_1, \psi_0 \leq_* \psi_1}{(\phi_0 \rightarrow \psi_0) \leq_* (\phi_1 \rightarrow \psi_1)}$$

Note that  $E_{*5}$  is not the exact image of  $D_{*5}$ , which would be:

$$(\phi_1 \rightarrow \psi_1) \wedge \dots \wedge (\phi_n \rightarrow \psi_n) \leq_* (\omega \rightarrow \omega)$$

However it should be clear that this holds, since:

$$\begin{aligned} (\phi_1 \rightarrow \psi_1) \wedge \dots \wedge (\phi_n \rightarrow \psi_n) &\leq_* (\phi_1 \rightarrow \psi_1) && \text{by E3.2} \\ &\leq_* (\phi_1 \rightarrow \omega) && \text{by E1, E}_{*7} \\ &\leq_* (\omega \rightarrow \omega) && \text{by E}_{*5} \end{aligned}$$

For what regards the strict case, we define the strict entailment relation  $\phi \leq_s \psi$  as the least one satisfying E1-E4 above (where one should obviously replace  $\leq$  by  $\leq_s$ ), and the clauses corresponding to  $D_{s5}$ - $D_{s7}$ , that is, using  $\zeta$ ,  $\zeta_0, \zeta_1$  and  $\phi_0, \phi_1$  to range over  $\Gamma$  and  $\Phi_s$  respectively:

$$Es5.1: \zeta \leq_s \gamma \quad Es5.2: \zeta \leq_s (\gamma \rightarrow \omega)$$

$$\text{Es6 : } ((\zeta \rightarrow \phi_0) \wedge (\zeta \rightarrow \phi_1)) \leq_s (\zeta \rightarrow (\phi_0 \wedge \phi_1))$$

$$\text{Es7 : } \frac{\zeta_0 \geq_s \zeta_1, \phi_0 \leq_s \phi_1}{(\zeta_0 \rightarrow \phi_0) \leq_s (\zeta_1 \rightarrow \phi_1)}$$

One can see for instance that  $\gamma \sim_s \gamma \rightarrow \omega$ . This expresses the fact that there is just one least element in the domain  $V$ , namely  $\gamma \uparrow$ , and that the “propositions”  $\{\nabla\}$  and  $(\{\nabla\}, \{\Delta\})$  should be regarded as identical. More generally we have  $\gamma \sim_s \zeta \rightarrow \omega$  for any  $\zeta \in \Gamma$ .

We could call  $(\Gamma, \leq_s)$  the *logic of partial functions*. The logic  $(\Phi_*, \leq_*)$  is exactly the one of Dezani & Margaria 86[17] (if we forget about the propositional variables, which are not needed since there is a non-trivial initial solution to the canonical domain equation) and of Abramsky 88[3]. As a matter of fact, the “logics”  $(\Phi_*, \leq_*)$  and  $(\Phi_s, \leq_s)$  would perhaps better be named, following Curry, *functionality theories*, and the formulae *functional characters*, since some “logical” properties do not hold here. For instance, although  $\omega$  means “true” and  $\phi \leq \psi$  means “ $\psi$  is a consequence of  $\phi$ ” (or  $\psi$  is more general than  $\phi$ ), one has  $\phi \rightarrow \omega \not\leq_* \omega$ , and in fact “ $\phi$  implies true” is strictly more informative than “true”; indeed one has  $\lambda x \perp \neq \perp$ . Similarly  $\omega \rightarrow \phi \not\leq_* \phi$ . Note that  $\phi \rightarrow \omega \sim \omega$  holds in the logic of Scott’s  $D_\infty$  domain, see [12].

Let us denote by  $\mathcal{F}(\Phi_*, \leq_*)$  and  $\mathcal{F}(\Phi_s, \leq_s)$  the set of filters of our logics. It should be clear that they provide us with another representation of the canonical domains (cf. Coppo & al. 84[12], Abramsky 88[2,3]):

**PROPOSITION.** *The canonical domain  $D_*$  is isomorphic to the family  $\mathcal{F}(\Phi_*, \leq_*)$ . Similarly the strict canonical domain  $D_s$  is isomorphic to the family  $\mathcal{F}(\Phi_s, \leq_s)$  of filters of the strict logic.*

**PROOF (outline):** we just treat the case of  $D_s$ . One formalizes the idea that the formulae represent the finite non-empty sets of “propositions” of the strict canonical information system by defining  $j: \Phi_s \rightarrow \text{Fin}(A_s \cup \{\Delta\})$  as follows:

$$\begin{cases} j(\omega) = \{\Delta\} \\ j(\phi \wedge \psi) = j(\phi) \cup j(\psi) \\ j(\gamma) = \{\nabla\} \\ j(\zeta \rightarrow \phi) = \{(j(\zeta), j(\phi))\} \end{cases}$$

Then one proves:

- (1) for any  $a \in A_s \cup \{\Delta\}$  there exists  $\phi \in \Phi_s$  such that  $j(\phi) = \{a\}$  (this is very easy). Then for any  $u \in \text{Fin}(A_s) \cup \{\Delta\}$  there exists  $\phi \in \Phi_s$  such that  $j(\phi) = u$ . Moreover  $\phi \in \Gamma \Leftrightarrow j(\phi) \subseteq A_s$ .
- (2) if  $\phi \leq_s \psi$  then  $j(\phi) \vdash_s j(\psi)$  (by induction on the definition of  $\phi \leq_s \psi$ ). Therefore if we let  $h(X) = \{\phi \mid j(\phi) \subseteq X\}$  for  $X \subseteq A_s \cup \{\Delta\}$  we have  $X \in D_s \Rightarrow h(X) \in \mathcal{F}(\Phi_s, \leq_s)$ .
- (3) if  $j(\phi) \vdash_s j(\psi)$  then  $\phi \leq_s \psi$ , by induction on the definition of  $j(\phi) \vdash_s j(\psi)$ . This is a little bit more elaborated: one should prove that  $j(\psi) = u \cup v$  if and only if  $\psi \sim_s \psi_0 \wedge \psi_1$  where  $j(\psi_0) = u$  and  $j(\psi_1) = v$ . Therefore if we let  $g(F) = \bigcup \{j(\phi) \mid \phi \in F\}$  for  $F \subseteq \Phi_s$  we have  $F \in \mathcal{F}(\Phi_s, \leq_s) \Rightarrow g(F) \in D_s$ .

Finally it is easy to check that the pair  $h, g$  provides us with the required isomorphism  $\square$

### 3.3 The Logical Systems.

In this section we give the interpretations of the  $\lambda_j^*$ -calculus and  $\lambda_j^s$ -calculus in their respective canonical domains, that is  $D_*$  and  $D_s$ . We shall begin with an abstract definition of the semantics,

and then derive their logical formulations, that is natural deduction systems, using as an intermediary step a concrete formulation in terms of approximable mappings. We shall not be very formal in this derivation, since we regard the natural deduction systems as providing the actual semantics of the  $\lambda_j^*$ -terms and  $\lambda_j^V$ -terms.

### 3.3.1 Abstract Interpretation of the $\lambda_j^*$ and $\lambda_j^V$ Calculi.

Let us recall that, following Scott's work (see Barendregt [5]), we can interpret the  $\lambda$ -calculus in any reflexive domain, that is a domain  $D$  whose own function space is a retract of itself. This is the case for our canonical domains, if in the strict case we take as "function space" the domain of strict continuous functions, since  $D_s$  is isomorphic to  $(D_s \rightarrow_\perp D_s)_\perp$ . In fact the specific retracts we use are given by the two obvious mappings associated with the lifting construct:

$$\text{down}_\star: D_\star \rightarrow (D_\star \rightarrow D_\star) \quad \text{and} \quad \text{up}_\star: (D_\star \rightarrow D_\star) \rightarrow D_\star$$

and

$$\text{down}_s: D_s \rightarrow V \quad \text{and} \quad \text{up}_s: V \rightarrow D_s$$

satisfying  $\text{down}(\text{up}(f)) = f$ . Then we can interpret our calculi as usual, the semantic value  $\llbracket M \rrbracket$  of the term  $M \in \Lambda_j^*$  being a mapping from environments to  $D_\star$ , and similarly for  $M \in \Lambda_j^V$ . Given a domain  $D$ , an environment is a mapping  $\rho: X \rightarrow D$  assigning values to the variables, such that  $\rho(x) = \perp$  except for finitely many variables. To give this interpretation we use the *updating* operation on environments, defined as follows: the updating of  $\rho$  by  $e \in D$  at  $x \in X$ , denoted  $[x \mapsto e]\rho$ , is given by:

$$([x \mapsto e]\rho)(y) = \begin{cases} e & \text{if } y = x \\ \rho(y) & \text{otherwise} \end{cases}$$

We shall also interpret a substitution  $\sigma \in \Sigma$  as a mapping  $\llbracket \sigma \rrbracket$  from environments to environments. Then, omitting the obvious subscripts  $\star$  and  $s$ , the semantics of our calculi is given by the following equations:

$$\begin{aligned} \llbracket x \rrbracket \rho &= \rho(x) \\ \llbracket \langle \lambda x M, \sigma \rangle \rrbracket_\star \rho &= \text{up}_\star(f) \quad \text{where } f(e) = \llbracket M \rrbracket_\star([x \mapsto e](\llbracket \sigma \rrbracket_\star \rho)) \\ \llbracket \langle \lambda^V x M, \sigma \rangle \rrbracket \rho &= \text{up}(g) \quad \text{where } g(e) = \begin{cases} \perp & \text{if } e = \perp \\ \llbracket M \rrbracket([x \mapsto e](\llbracket \sigma \rrbracket \rho)) & \text{otherwise} \end{cases} \\ \llbracket MN \rrbracket \rho &= (\text{down}(\llbracket M \rrbracket \rho))(\llbracket N \rrbracket \rho) \\ \llbracket M \parallel N \rrbracket \rho &= (\llbracket M \rrbracket \rho) \sqcup (\llbracket N \rrbracket \rho) \\ \llbracket \varepsilon \rrbracket \rho &= \rho \\ \llbracket [M/x]\sigma \rrbracket \rho &= [x \mapsto \llbracket M \rrbracket \rho](\llbracket \sigma \rrbracket \rho) \end{aligned}$$

The extensional semantic preorders  $M \sqsubseteq_\star N$  on  $\lambda_j^*$ -terms and  $M \sqsubseteq_s N$  for the  $\lambda_j^V$ -terms are given by the same definition, where  $D$  stands for  $D_\star$  or  $D_s$ :

$$M \sqsubseteq N \Leftrightarrow_{\text{def}} \forall \rho: X \rightarrow D. \llbracket M \rrbracket \rho \sqsubseteq \llbracket N \rrbracket \rho$$

Now we want to give a more explicit description of the semantics, using the concrete presentations of the canonical domains. First we can rephrase the previous equations, taking into account the fact that  $\llbracket M \rrbracket \rho$  is a subset of  $A$  (where  $A$  is  $A_\star$  or, in the strict case,  $A_s \cup \{\Delta\}$ ), and more precisely a configuration of  $S$  (where  $S$  is  $S_\star$  or  $S_s$  in the strict case). In view of the logical interpretation,

we shall in fact describe  $\llbracket M \rrbracket \rho$  as a union of elements of  $\mathbf{Fin}(A)$ . The first item, that is  $\llbracket x \rrbracket \rho = \rho(x)$ , can be pedantically formulated as follows:

S1:  $\llbracket x \rrbracket \rho$  is the least subset of  $A$  such that  $u \subseteq \rho(x) \Rightarrow u \subseteq \llbracket x \rrbracket \rho$  where, as before,  $u$  ranges over  $\mathbf{Fin}(A)$ .

The concrete formulations of the interpretation of the closures is a bit more elaborated. Let us first deal with  $\llbracket (\lambda x M, \sigma) \rrbracket_* \rho = \mathbf{up}_*(f)$  where:

$$f(e) = \llbracket M \rrbracket_*([x \mapsto e](\llbracket \sigma \rrbracket_* \rho))$$

is, by construction, a continuous function from  $D_*$  to itself, or more precisely the approximable mapping:

$$\{(u, v) \mid v \subseteq \llbracket M \rrbracket_*([x \mapsto \bar{u}](\llbracket \sigma \rrbracket_* \rho))\}$$

Since  $\mathbf{up}_*(X) = X \cup \{\Delta\}$  we can describe more concretely the interpretation of  $\langle \lambda x M, \sigma \rangle$  in  $D_*$  as follows:

S2.1:  $\llbracket \langle \lambda x M, \sigma \rangle \rrbracket_* \rho$  is the least configuration of  $S_*$  such that

$$v \subseteq \llbracket M \rrbracket_*([x \mapsto \bar{u}](\llbracket \sigma \rrbracket_* \rho)) \Rightarrow (u, v) \in \llbracket \langle \lambda x M, \sigma \rangle \rrbracket_* \rho$$

Similarly for  $\llbracket \langle \lambda^v x M, \sigma \rangle \rrbracket_* \rho = \mathbf{up}_*(g)$ , the strict function  $g$  is represented by the approximable mapping:

$$\{\Delta\} \cup \{(u, v) \mid \bar{u} \neq \{\Delta\} \ \& \ v \subseteq \llbracket M \rrbracket_*([x \mapsto \bar{u}](\llbracket \sigma \rrbracket_* \rho))\}$$

It is not difficult to see that  $\bar{u} \neq \{\Delta\} \Leftrightarrow u \vdash_* (\{\Delta\}, \{\Delta\})$ , therefore we can describe more concretely the interpretation of  $\langle \lambda^v x M, \sigma \rangle$  in  $D_*$  as follows:

S2.2:  $\llbracket \langle \lambda^v x M, \sigma \rangle \rrbracket_* \rho$  is the least configuration of  $S_*$  such that

$$u \vdash_* (\{\Delta\}, \{\Delta\}) \ \& \ v \subseteq \llbracket M \rrbracket_*([x \mapsto \bar{u}](\llbracket \sigma \rrbracket_* \rho)) \Rightarrow (u, v) \in \llbracket \langle \lambda^v x M, \sigma \rangle \rrbracket_* \rho$$

We let the reader convinces him/herself that the following is an appropriate formulation of the interpretation of  $\langle \lambda^v x M, \sigma \rangle$  in  $D_S$ :

Ss2:  $\llbracket \langle \lambda^v x M, \sigma \rangle \rrbracket_{S\rho}$  is the least configuration of  $S_S$  such that

$$u \in \mathbf{Fin}(A_S) \ \& \ v \subseteq \llbracket M \rrbracket_S([x \mapsto \bar{u}](\llbracket \sigma \rrbracket_{S\rho})) \Rightarrow (u, v) \in \llbracket \langle \lambda^v x M, \sigma \rangle \rrbracket_{S\rho}$$

To interpret an application  $MN$  we used  $\mathbf{down}(\llbracket M \rrbracket \rho)$ , or more precisely the function represented by this element of the domain, that is  $\mathbf{fun}(\mathbf{down}(\llbracket M \rrbracket \rho))$ . Then it is not difficult to check that we can rephrase the definition of  $\llbracket MN \rrbracket \rho$  as follows:

S3:  $\llbracket MN \rrbracket \rho$  is the least configuration of  $S$  such that

$$u \subseteq \llbracket N \rrbracket \rho \ \& \ (u, v) \in \llbracket M \rrbracket \rho \Rightarrow v \subseteq \llbracket MN \rrbracket \rho$$

Note that in the strict case, it is implicitly assumed that  $u \in \mathbf{Fin}(A_S)$ , since otherwise we could not form  $(u, v)$ . Finally the interpretation of  $\llbracket M \parallel N \rrbracket \rho$ , that is the join of  $\llbracket M \rrbracket \rho$  and  $\llbracket N \rrbracket \rho$ , is quite simple to formulate:

S4:  $\llbracket M \parallel N \rrbracket \rho$  is the least configuration of  $S$  such that

$$u \subseteq \llbracket M \rrbracket \rho \ \& \ v \subseteq \llbracket N \rrbracket \rho \Rightarrow u \cup v \subseteq \llbracket M \parallel N \rrbracket \rho$$



### 3.3.2 Logical Interpretation of the $\lambda_j^*$ and $\lambda_j^\vee$ Calculi.

Now we want to take a further step, making an explicit use of the fact that the elements of the canonical domains are filters of formulae. Then we shall describe  $\phi \in \llbracket M \rrbracket \rho$ , where  $\rho$  is now a mapping from  $X$  to the family of filters (either  $\mathcal{F}(\Phi_*, \leq_*)$  or  $\mathcal{F}(\Phi_s, \leq_s)$ ), by means of a “typing system”, or more accurately a *logical natural deduction system* allowing us to prove *sequents*, that is statements of the form  $H \vdash M : \phi$ . In fact we have to elaborate two logical systems, one for  $H \vdash_* M : \phi$ , with  $M \in \Lambda_j^*$  and  $\phi \in \Phi_*$ , and the other for  $H \vdash_s M : \phi$ , with  $M \in \Lambda_j^\vee$  and  $\phi \in \Phi_s$ . Since they share some rules, we begin with some generalities, not distinguishing the two kinds of sequents.

In a sequent  $H \vdash M : \phi$ ,  $H$  is a “logical environment”, called *hypothesis*, that is a mapping  $H : X \rightarrow \Phi$  (where  $\Phi$  is either  $\Phi_*$  or  $\Phi_s$ ) such that  $H(x) \sim \omega$  except for finitely many variables. Then an hypothesis  $H$  may be represented as usual as a sequence  $x_1 : \phi_1, \dots, x_n : \phi_n$  (where the variables  $x$  such that  $H(x) \not\sim \omega$  are among the  $x_i$ 's). In particular we write  $\vdash M : \phi$  for  $H \vdash M : \phi$  where  $H(x) \sim \omega$  for all  $x$ . Therefore the natural deduction systems will allow us to prove facts of the form:

$$(*) \quad x_1 : \phi_1, \dots, x_n : \phi_n \vdash M : \phi$$

to be read: “from the hypothesis that the value of the variables  $x_i$ 's satisfy the formulae  $\phi_i$ 's we may infer that the expression  $M$  satisfy  $\phi$ ”. In fact we shall also use the comma occurring in the hypothesis as a symbol for the “updating” operation on hypotheses. More precisely we define, for all hypotheses  $H$  and  $G$ , the updating of  $G$  by  $H$ , denoted  $(H, G)$ , as follows:

$$(H, G)(x) = \begin{cases} H(x) & \text{if } H(x) \not\sim \omega \\ G(x) & \text{otherwise} \end{cases}$$

Then in the notation  $x_1 : \phi_1, \dots, x_n : \phi_n$  a given variable may occur several times – its value is the leftmost one in the sequence. Note also that  $(x : \omega, H) = H$  for instance.

We shall say that an environment  $\rho$ , which assigns a filter of formulae to a variable, *satisfies* the hypothesis  $H$  if  $H(x) \in \rho(x)$  for all  $x \in X$ . To define the logical systems we give the logical formulation of the previous semantic equations S1-S4 defining the interpretations of our calculi, guided by the idea that a sequent of the form  $(*)$  above means:

$$(**) \quad \phi_1 \in \rho(x_1), \dots, \phi_n \in \rho(x_n) \Rightarrow \phi \in \llbracket M \rrbracket \rho$$

that is:  $H \vdash M : \phi$  iff  $\phi \in \llbracket M \rrbracket \rho$  for all environments  $\rho$  satisfying  $H$ . The first rules to state assert that  $\llbracket M \rrbracket \rho$  is a filter, that is:

$$\boxed{\begin{array}{ll} \text{L1 : } H \vdash M : \omega & \text{L2 : } \frac{H \vdash M : \phi, H \vdash M : \psi}{H \vdash M : (\phi \wedge \psi)} \end{array}}$$

$$\boxed{\text{L3 : } \frac{H \vdash M : \phi}{H \vdash M : \psi} \phi \leq \psi}$$

Note that the usual rules for elimination of conjunction are derived from L3 (using E3.2, E3.3):

$$\frac{H \vdash M : \phi \wedge \psi}{H \vdash M : \phi} \quad \frac{H \vdash M : \phi \wedge \psi}{H \vdash M : \psi}$$

Now we give the rules corresponding to terms formation. For the variables we have the obvious rule, corresponding to S1:

$$\boxed{\text{L4 : } x : \phi, H \vdash x : \phi}$$

To give the logical meaning of  $\langle \lambda x M, \sigma \rangle$  (in the “ $\lambda_J^*$ -logical system”) we introduce another kind of sequent, namely  $H \vdash \sigma : G$  to be read: “from the hypothesis  $H$  we may infer that the substitution  $\sigma$  satisfies the hypothesis  $G$ ”. The rules for this type of sequent will be given below.

Then the “typing” rule for the usual, call-by-name closures corresponding to the definition S2.1 of  $\llbracket \langle \lambda x M, \sigma \rangle \rrbracket_{\star} \rho$  is:

$$\boxed{\text{L5.1 : } \frac{x : \psi, G \vdash_{\star} M : \phi, H \vdash_{\star} \sigma : G}{H \vdash_{\star} \langle \lambda x M, \sigma \rangle : (\psi \rightarrow \phi)}}$$

Obviously this rule is not a part of the “ $\lambda_J^V$ -logical system”. In this system we only have to give a rule for the call-by-value closures  $\langle \lambda^V x M, \sigma \rangle$ . In fact the rule is exactly the same as the previous one, with the exception that to form  $(\psi \rightarrow \phi)$  we must have  $\psi \in \Gamma$ . We shall leave this assumption implicit, simply using  $\zeta$  as a generic name for formulae of  $\Gamma$ . Then the strict rule, corresponding to Ss2, is:

$$\boxed{\text{Ls5 : } \frac{x : \zeta, G \vdash_s M : \phi, H \vdash_s \sigma : G}{H \vdash_s \langle \lambda^V x M, \sigma \rangle : (\zeta \rightarrow \phi)}}$$

To formulate the “typing” rule for strict closures in the  $\lambda_J^*$ -logical system, we have to translate the assumption  $u \vdash_{\star} (\{\Delta\}, \{\Delta\})$  of S2.2 in logical words. Then we get:

$$\boxed{\text{L5.2 : } \frac{x : \psi, G \vdash_{\star} M : \phi, H \vdash_{\star} \sigma : G}{H \vdash_{\star} \langle \lambda^V x M, \sigma \rangle : (\psi \rightarrow \phi)} \psi \leq_{\star} (\omega \rightarrow \omega)}$$

To state the rule for application, corresponding to the semantic equation S3 for  $\llbracket MN \rrbracket_{\rho}$ , we use an assumption  $H \vdash M : (\psi \rightarrow \phi)$ , corresponding to  $(u, v) \in \llbracket M \rrbracket_{\rho}$ . Then in the strict case, we should have to say that  $\psi \in \Gamma$  (this means that, unlike Scott 79[41], we use a restricted form of “modus ponens”). As previously, this will be left implicit, and we give the same rule for both logical systems, namely:

$$\boxed{\text{L6 : } \frac{H \vdash M : (\psi \rightarrow \phi), H \vdash N : \psi}{H \vdash (MN) : \phi}}$$

The rule for the concurrent join, corresponding to S4, is obvious:

$$\boxed{\text{L7 : } \frac{H \vdash M : \phi, H \vdash N : \psi}{H \vdash (M \parallel N) : (\phi \wedge \psi)}}$$

Finally we have to give the rules for  $H \vdash \sigma : G$ , whose meaning is:

$$H \vdash [N_1/x_1] \cdots [N_k/x_k] \varepsilon : G \Leftrightarrow \forall i. H \vdash N_i : G(x_i)$$

Note however that since  $\varepsilon$  is the identity, we should also require that for any variable  $x$  not in  $\{x_1, \dots, x_k\}$  the formula  $G(x)$  is in the filter generated by  $H(x)$ , that is  $H(x) \leq G(x)$ . Let us introduce a notation:

$$H \leq G \Leftrightarrow_{\text{def}} \forall x \in X. H(x) \leq G(x)$$

Then the rules for  $H \vdash \sigma : G$  are the following:

$\text{S1: } \frac{}{H \vdash \varepsilon : G} H \leq G$	$\text{S2: } \frac{H \vdash M : \phi, H \vdash \sigma : G}{H \vdash [M/x]\sigma : (x : \phi, G)}$
--	---

Summarizing, the  $\lambda_j^*$ -logical system consists of all the rules above, except Ls5. Obviously one should have written  $\vdash_*$  instead of  $\vdash$  in the general rules L1-L4, L6-L7 and S1-S2. A similar remark applies for the  $\lambda_j^y$ -logical system, whose rules are the ones above, except L5.1 and L5.2. Moreover, in these systems the terms and formulae are respectively taken to be either in  $\Lambda_j^*$  and  $\Phi_*$  or in  $\Lambda_j^y$  and  $\Phi_*$ . In what follows, when we write  $H \vdash M : \phi$ , in most cases we intend that this sequent is provable by means of the previous rules.

Let us see some examples: since  $\lambda x M$  is a notation for  $\langle \lambda x M, \varepsilon \rangle$ , we can derive the usual rule for abstractions:

$$\frac{x : \psi, H \vdash_* M : \phi}{H \vdash_* \lambda x M : (\psi \rightarrow \phi)}$$

Then the inference rules L4, L5.1, L6 are the usual rules in Curry's typing system, while L1-L3 are typical of Coppo's typing systems [6,12]. One can also see that the following two rules are derivable from L7, using L1, L3 and  $\phi \wedge \omega \leq \phi$ :

$$\frac{H \vdash M : \phi}{H \vdash (M \parallel N) : \phi} \quad \frac{H \vdash N : \psi}{H \vdash (M \parallel N) : \psi}$$

In fact, we could have used these two rules instead of L7.

Some comments about these systems are in order: we do not regard the natural deduction systems as *typing* systems, because the notion of *type* usually refers to an idea of *constraint*. Types were introduced to avoid paradoxical situations, and more precisely to rule out self-application. They are of common use in mathematics, and in programming where they provide a discipline which ensures robust programs. In this case typability does not imply convergence, whereas in any "Curry-Howard" typing system a typable term is strongly convergent (as well as its subterms). Although the relation between the logical system and the computational notion of convergence turns out to be, as usual, a central question (see for instance Leivant [23] or Krivine [21]), it should be clear that the purpose of "typing" systems à la Coppo is not to restrict programs formation, but rather to tell something logical about meaningful programs. Then we could say, following Leivant [23], that Coppo's systems implement an idea of "types as formulae" (but not "programs as proofs"), where  $\psi \rightarrow \phi$  is an assertion about the functional character of a program, and conjunction is just a way to join such assertions.

As we said above, we regard the logical systems as providing the actual interpretation of the  $\lambda_j^*$  and  $\lambda_j^y$  calculi in the canonical (logical) domains. In particular, it should be clear that we can now reformulate the *semantical preorders* on the terms of the calculi as follows:

$M \sqsubseteq_{\mathcal{S}} N \Leftrightarrow_{\text{def}} \forall H \forall \phi. H \vdash M : \phi \Rightarrow H \vdash N : \phi$
--

Obviously this definition should have been particularized into two cases, namely  $\sqsubseteq_S^*$  and  $\sqsubseteq_S^5$  for each of the calculi. However, we shall in most occasions give just one statement, when its takes exactly the same form for the two calculi.

Since the rules of the natural deduction systems for proving  $H \vdash M : \phi$  are either independent of the term  $M$ , or composing assertions on the subterms of  $M$ , it is not surprising that these preorders are *precongruences*:

LEMMA 3.5.  $M \sqsubseteq_S N \Rightarrow \forall C. C[M] \sqsubseteq_S C[N]$

PROOF: by a tedious induction on the inference of  $H \vdash C[M] : \phi$ , and by case on the context  $C$ , omitted  $\square$

We shall also prove later that the semantical preorders are preserved by instantiation, that is:

LEMMA 3.6.  $M \sqsubseteq_S N \Rightarrow \forall \sigma. M\sigma \sqsubseteq_S N\sigma$

## 4. Completeness and Full Abstraction.

### 4.1 Testing.

In this section we introduce some preorders on terms of our calculi, which will be denoted  $\sqsubseteq$ , decorated with various subscripts. The associated equivalences will be denoted  $\simeq$ , with the corresponding subscripts. Obviously each preorder has two versions, one for the  $\lambda_j^*$ -calculus and the other for the  $\lambda_j^5$ -calculus. These preorders should be denoted  $\sqsubseteq^*$  and  $\sqsubseteq^5$ , decorated with the relevant subscript, but we shall mostly leave implicit this distinction between the two calculi.

The definition of most of our preorders relies upon an *operational criterion* according to which a (closed) convergent term is better than any other one, that is:

$$M \prec N \Leftrightarrow_{\text{def}} M \Downarrow \Rightarrow N \Downarrow$$

This is a preorder, which is not a precongruence: for instance in the  $\lambda_j^*$ -calculus we have  $\mathbf{F} \prec \mathbf{I}$  but  $\mathbf{F}\Omega \not\prec \mathbf{I}\Omega$ , and in the  $\lambda_j^5$ -calculus,  $\lambda^5 xx \prec \lambda^5 x\Omega$ , but  $(\lambda^5 xx)\lambda^5 x\Omega \not\prec (\lambda^5 x\Omega)\lambda^5 x\Omega$ .

Our first preorder is the *testing* preorder, already mentioned in the introduction. The *tests* are simply pairs  $(C, \sigma)$  made of a context  $C$  – to be more precise, a  $\lambda_j^*$ -context or a  $\lambda_j^5$ -context – and an environment  $\sigma$ , assigning  $\lambda_j^*$ -terms or  $\lambda_j^5$ -terms to the variables. The success of a test  $(C, \sigma)$  applied to  $M$  is the convergence of  $C[M\sigma]$ . This only makes sense if  $C[M\sigma]$  can be evaluated, that is if it is a closed term. Then in the definition of the testing preorder, we have to require the tested terms to be closed by the test:

DEFINITION (TESTING or OBSERVATION PREORDER).

$$M \sqsubseteq_O N \Leftrightarrow_{\text{def}} \forall \sigma \forall C \text{ closing } M\sigma \ \& \ N\sigma. C[M\sigma] \prec C[N\sigma]$$

Our main goal is to show a full abstraction result for each of our calculi, that is we want to prove that the testing preorders coincide with the semantical preorders:

$$M \sqsubseteq_S N \Leftrightarrow M \sqsubseteq_O N$$

To this end, we have to relate the testing ability with the logical character of the abstract interpretations of our calculi. Since these interpretations are functional, it is not surprising that a property of *operational extensionality* (see Bloom [9]), or a *context lemma* (see Milner 77[28] and Berry &

al. [7]) holds. That is, the testing ability may be restricted to *applicative  $\lambda_j^*$ -tests* and *applicative  $\lambda_j^V$ -test*, namely, for the first case:

$$A ::= \square \mid (\lambda x A, \sigma) \mid (\lambda^V x A, \sigma) \mid (AM)$$

where  $M$  is any closed  $\lambda_j^*$ -term and  $\sigma$  any  $\lambda_j^*$ -environment. The corresponding testing preorders, that is *applicative testing preorders*, are denoted  $\sqsubseteq_{\mathcal{A}}$ . For instance  $\mathbf{T} \not\sqsubseteq_{\mathcal{A}} \mathbf{F}$ , since these two terms are distinguished by the test  $\square\Omega\mathbf{I}$ . Similarly the terms  $\mathbf{I}$  and  $\mathbf{A} = \lambda xy.xy$  are distinguished by  $\square\Omega$ . We let the reader find similar examples for the  $\lambda_j^V$ -calculus. It should be obvious that testing is stronger than applicative testing, that is:

$$M \sqsubseteq_{\mathcal{O}} N \Rightarrow M \sqsubseteq_{\mathcal{A}} N$$

We shall see later the converse implication, showing that applicative tests are enough to provide us with the full power of testing.

In the rest of this section we give some alternative characterizations of applicative testing, as a trace preorder, and by means of a kind of “logical relation”. More precisely, we prove that applicative testing is equivalent to an extensional preorder on terms – in fact we only prove one implication here; the other one will be a consequence of the full abstraction result. We cannot define extensional equality simply as the least relation  $\simeq$  such that (for closed terms):

$$M \simeq N \Leftrightarrow \forall R. MR \simeq NR$$

since this relation is inconsistent:  $M \simeq N$  for all  $M$  and  $N$  is the least fixed-point of this recursive definition. We have to incorporate a type distinction, giving some information on the functional character of  $M$  and  $N$ . In fact this distinction is given by our operational criterion: a (closed) term is “functional” if it is convergent. The definition of the extensional preorder, due to Abramsky [3] and inspired by the well-known Park & Milner’s notion of bisimulation, is as follows:

**DEFINITION and LEMMA (APPLICATIVE SIMULATION and EXTENSIONAL PREORDER).**

A relation  $\mathcal{R}$  on closed term is an *applicative simulation* if:

$$M \mathcal{R} N \Rightarrow \begin{cases} M \prec N \\ \forall Q. (MQ) \mathcal{R} (NQ) \end{cases} \quad \text{and}$$

The relation on closed terms given by:

$$M \sqsubseteq_{\mathcal{E}} N \Leftrightarrow_{\text{def}} \exists \mathcal{R} \text{ applicative simulation } M \mathcal{R} N$$

is an *applicative simulation* and a *preorder*, called the *extensional preorder*.

**PROOF:** one shows that the composition of two applicative simulations is an applicative simulation  $\square$

The  $(\lambda_j^*$  and  $\lambda_j^V)$  extensional preorders are extended to arbitrary terms by instantiation:

$$M \sqsubseteq_{\mathcal{E}} N \Leftrightarrow_{\text{def}} \forall \sigma \text{ closing } M \ \& \ N. M\sigma \sqsubseteq_{\mathcal{E}} N\sigma$$

An important example of applicative simulation is provided by the convertibility relation of the section 2.2:

**LEMMA 4.1.** *The convertibility relation  $\bowtie$  is an applicative simulation, therefore:*

$$M \bowtie N \Rightarrow M \simeq_{\mathcal{E}} N$$

This is a direct consequence of the proposition 2.12. Let us see some other examples. The first one will show that, for  $M$  and  $N$  closed:

$$M \sqsubseteq_{\varepsilon} (M \parallel N) \quad \& \quad M \sqsubseteq_{\varepsilon} (N \parallel M)$$

**LEMMA 4.2.** *Let  $\mathcal{R}$  be the relation on closed terms given by:*

$$M \mathcal{R} N \Leftrightarrow_{\text{def}} \exists P. N \bowtie (M \parallel P) \text{ or } N \bowtie (P \parallel N)$$

*Then  $\mathcal{R}$  is an applicative simulation.*

**PROOF:** clearly  $M \prec (M \parallel P)$  (by the evaluation rule R3.1) and  $M \prec (P \parallel N)$  (by the evaluation rule R3.2), therefore  $M \mathcal{R} N \Rightarrow M \prec N$  by the corollary 2.11. If  $M \mathcal{R} N$ , with for instance  $N \bowtie (M \parallel P)$  then  $NQ \bowtie (M \parallel P)Q \bowtie (MQ \parallel PQ)$  by definition of the convertibility relation. Therefore  $M \mathcal{R} N \Rightarrow MQ \mathcal{R} NQ$  for all closed term  $Q$   $\square$

Another example of applicative simulation will show that applicative testing is stronger than the extensional preorder:

**LEMMA 4.3.** *The relation  $\mathcal{R}$  on closed terms given by:*

$$M \mathcal{R} N \Leftrightarrow_{\text{def}} \forall A \text{ (closed applicative test) } A[M] \prec A[N]$$

*is an applicative simulation, therefore:*

$$M \sqsubseteq_{\mathcal{A}} N \Rightarrow M \sqsubseteq_{\varepsilon} N$$

**PROOF:** clearly  $M \mathcal{R} N \Rightarrow M \prec N$  (take  $A = \square$  in the definition), and  $M \mathcal{R} N \Rightarrow MQ \mathcal{R} NQ$  since for any applicative test  $A$  the context  $A[\square Q]$  is an applicative test, and  $A[MQ] = (A[\square Q])[M]$ . Since  $(M\sigma)\rho = M(\sigma \circ \rho)$  (lemma 2.1) it is easy to see that

$$M \sqsubseteq_{\mathcal{A}} N \Rightarrow \forall \sigma. M\sigma \sqsubseteq_{\mathcal{A}} N\sigma$$

Therefore if  $M \sqsubseteq_{\mathcal{A}} N$  then  $M\sigma \sqsubseteq_{\mathcal{A}} N\sigma$  for all  $\sigma$  closing  $M$  and  $N$ , hence  $M\sigma \mathcal{R} N\sigma$ , and  $M \sqsubseteq_{\varepsilon} N$  by definition of the extensional preorder  $\square$

The extensional preorder coincides with a trace preorder, which we define now:

**DEFINITION (TRACE PREORDER).** *The set  $T(M)$  of traces of a closed term  $M$  is the set of (possibly empty) sequences  $R_1 \cdots R_k$  of closed terms such that  $M R_1 \cdots R_k \Downarrow$ . The trace preorder on closed terms is given by:*

$$M \sqsubseteq_{\mathcal{T}} N \Leftrightarrow_{\text{def}} T(M) \subseteq T(N)$$

Obviously we should have defined  $\lambda_j^*$ -traces of  $\lambda_j^*$ -terms, and  $\lambda_j^{\forall}$ -traces of  $\lambda_j^{\forall}$ -terms. The trace preorder is extended to arbitrary terms by instantiation:

$$M \sqsubseteq_{\mathcal{T}} N \Leftrightarrow_{\text{def}} \forall \sigma \text{ closing } M \ \& \ N. M\sigma \sqsubseteq_{\mathcal{T}} N\sigma$$

Now we show that the trace preorder and extensional preorder coincide:

**LEMMA 4.4.**  $M \sqsubseteq_{\varepsilon} N \Leftrightarrow M \sqsubseteq_{\mathcal{T}} N$

**PROOF:** clearly the relation  $\sqsubseteq_{\mathcal{T}}$ , on closed terms, is an applicative simulation, since  $M \Downarrow$  if and only if the empty sequence is a trace of  $M$ , and  $U \in T(MQ) \Leftrightarrow QU \in T(M)$ . Then  $M \sqsubseteq_{\mathcal{T}} N \Rightarrow M \sqsubseteq_{\varepsilon} N$ . Conversely, one easily proves by induction on  $k$  that if  $\mathcal{R}$  is an applicative simulation then

$$M \mathcal{R} N \Rightarrow \forall R_1, \dots, R_k. (M R_1 \cdots R_k) \mathcal{R} (N R_1 \cdots R_k)$$

Moreover  $P \mathcal{R} Q \Rightarrow P \prec Q$  by definition, hence the lemma  $\square$

Summarizing, we have established:

$$M \sqsubseteq_O N \Rightarrow M \sqsubseteq_A N \Rightarrow M \sqsubseteq_E N \Leftrightarrow M \sqsubseteq_T N$$

We shall see that, as a consequence of the full abstraction result, all these preorders are in fact the same.

#### 4.2 Realizability and Soundness.

A further step towards the full abstraction result consists in giving a “realizability” interpretation of the formulae of  $\Phi_*$  and  $\Phi_s$ . That is, each formula denotes a set of closed terms (respectively  $\lambda_j^*$ -terms or  $\lambda_j^v$ -terms) realizing the given formula. This interpretation is due, for the typed  $\lambda$ -calculus, to Tait. It was originally called “convertibility”, and later on received the names of “reducibility” or “computability” (a generalization of this semantics of formulae is credited to Reynolds and Scott in [19,6]). We denote “ $M$  realizes  $\phi$ ” by  $\models M : \phi$ . We have to define a  $\lambda_j^*$ -realizability, denoted  $\models_* M : \phi$ , and a  $\lambda_j^v$ -realizability  $\models_s M : \phi$ . The first two clauses of the two definitions are the same:

$$\begin{aligned} \models M : \omega &\Leftrightarrow_{\text{def}} \text{true} \\ \models M : (\phi \wedge \psi) &\Leftrightarrow_{\text{def}} \models M : \phi \ \& \ \models M : \psi \end{aligned}$$

Then a closed term realizes the formula  $\psi \rightarrow \phi$  (of  $\Phi_*$ ) when it is a functional term, that is it converges, and when applied to arguments realizing  $\psi$  then any result it returns realizes  $\phi$ :

$$\models_* M : (\psi \rightarrow \phi) \Leftrightarrow_{\text{def}} M \Downarrow \ \& \ \forall R \in (\Lambda_j^*)^\circ \ \models_* R : \psi \Rightarrow \models_* MR : \phi$$

This interpretation suggests that we could have denoted  $\psi \rightarrow \phi$  as a “Hennessy-Milner modal formula”  $[\psi]\phi$ . As one can see, this interpretation of the formulae of  $\Phi_*$ , adapted from the one given by Abramsky in [3], is essentially the “ $F$ -semantics” of Hindley ([19], see also Dezani & Margaria [17]). The realizability interpretation of  $\Phi_*$  entirely relies upon the convergence property  $M \Downarrow$ . In fact it entails a characterization of this property: a closed  $\lambda_j^*$ -term is convergent if and only if it realizes the formula  $\omega \rightarrow \omega$ , that is

**REMARK 4.5.**  $\forall M \in (\Lambda_j^*)^\circ \quad M \Downarrow \Leftrightarrow \models_* M : (\omega \rightarrow \omega)$

In the strict case, the convergence formula is  $\gamma$ . Then the  $\lambda_j^v$ -realizability is given by:

$$\begin{aligned} \models_s M : \gamma &\Leftrightarrow_{\text{def}} M \Downarrow \\ \models_s M : (\zeta \rightarrow \phi) &\Leftrightarrow_{\text{def}} M \Downarrow \ \& \ \forall R \in (\Lambda_j^v)^\circ \ \models_s R : \zeta \Rightarrow \models_s MR : \phi \end{aligned}$$

To simplify the presentation, we shall also denote by  $\gamma$  the convergence formula of the logic  $\Phi_*$ , that is  $\gamma = \omega \rightarrow \omega$ .

We can introduce a *logical preorder* (in fact, two preorders) on closed terms relative to this interpretation of the formulae: a term is logically less than another one whenever it realizes less formulae, that is:

$$M \sqsubseteq_L N \Leftrightarrow_{\text{def}} \forall \phi. \models M : \phi \Rightarrow \models N : \phi$$

This preorder is extended to arbitrary terms by instantiation:

$$M \sqsubseteq_L N \Leftrightarrow_{\text{def}} \forall \sigma \text{ closed } M\sigma \sqsubseteq_L N\sigma$$

Now we want to show that this preorder is weaker than the testing preorder. By virtue of the results of the previous section, it is enough to show:

**LEMMA.** *If  $\mathcal{R}$  is an applicative simulation and  $M \mathcal{R} N$  then  $\models M : \phi \Rightarrow \models N : \phi$  for any formula  $\phi$ .*

whose proof (by induction on the formula  $\phi$ ) is trivial. As a consequence, we have now:

PROPOSITION 4.6.

$$M \sqsubseteq_O N \Rightarrow M \sqsubseteq_A N \Rightarrow M \sqsubseteq_\varepsilon N \Leftrightarrow M \sqsubseteq_T N \Rightarrow M \sqsubseteq_\mathcal{L} N$$

Now to show that the testing preorder is stronger than the semantical preorder, we have to relate the realizability interpretation of the logics with the natural deduction system. Indeed the comparison of  $\models M : \phi$  and  $\vdash M : \phi$  is the central topic of this work. As usual, this comparison takes the form of a *soundness* and *completeness* result. We shall prove first the soundness of the natural deduction systems with respect to an extension of the realizability interpretation. We let  $H \models M : \phi$ , to be read as “ $M$  realizes  $\phi$  under the hypothesis  $H$ ”, if  $M\sigma$  realizes  $\phi$  for any substitution  $\sigma$  satisfying the hypothesis  $H$  regarding the free variables of  $M$ . Formally:

$$H \models M : \phi \Leftrightarrow_{\text{def}} \forall \sigma (\forall x \in \text{fv}(M). \models \sigma(x) : H(x)) \Rightarrow \models M\sigma : \phi$$

Note that in this definition it is implicitly assumed that  $\sigma(x)$  is a closed term for any  $x \in \text{fv}(M)$ .

REMARK 4.7.  $M \sqsubseteq_\mathcal{L} N \Rightarrow \forall \phi \forall H. H \models M : \phi \Rightarrow H \models N : \phi$

The soundness property of the natural deduction systems is:

$$H \vdash M : \phi \Rightarrow H \models M : \phi$$

The argument is the standard one: this implication is proved by induction on the inference of the sequent  $H \vdash M : \phi$ . To this end we first show the validity of the natural deduction rules, apart the rules concerning the closures. The validity of L1 and L2 is trivial. The validity of L3 results from the following:

LEMMA 4.8. If  $\models M : \phi$  and  $\phi \leq \psi$  then  $\models M : \psi$ .

PROOF: by induction on the definition of  $\phi \leq \psi$ , straightforward (in the case of Es5.1 and Es5.2 one proves  $\zeta \in \Gamma \ \& \ \models M : \zeta \Rightarrow M \Downarrow$ , by induction on the formula  $\zeta$ )  $\square$

By definition of the interpretation of  $(\psi \rightarrow \phi)$ , the rule L6 is valid. It is easy to see that the rule L7 is valid: if  $H \models M : \phi$  and  $H \models N : \psi$ , let  $\sigma$  be a substitution such that  $\models \sigma(x) : H(x)$  for any  $x \in \text{fv}(M \parallel N)$ . Then  $\models M\sigma : \phi$  and  $\models N\sigma : \psi$ . Since  $M\sigma \sqsubseteq_\mathcal{L} (M\sigma \parallel N\sigma)$  and  $N\sigma \sqsubseteq_\mathcal{L} (M\sigma \parallel N\sigma)$  by the lemma 4.2 and the proposition 4.6, we have  $\models (M \parallel N)\sigma : \phi$  and  $\models (M \parallel N)\sigma : \psi$ , therefore  $H \models (M \parallel N) : (\phi \wedge \psi)$ .

PROPOSITION (SOUNDNESS). If  $H \vdash M : \phi$  then  $H \models M : \phi$ .

PROOF: in fact we prove simultaneously

$$H \vdash M : \phi \Rightarrow H \models M : \phi \quad \text{and} \quad H \vdash \sigma : G \Rightarrow \forall x. H \models \sigma(x) : G(x)$$

by induction on the inference of the sequents. From the previous remarks, we only have to examine the cases of S1, S2, L5.1, Ls5 and L5.2.

- if  $H \vdash \varepsilon : G$  (by means of S1) with  $H(x) \leq G(x)$  for any variable  $x$ , and if  $\rho$  is a substitution such that  $\models \rho(x) : H(x)$  then  $\models \rho(x) : G(x)$  by the previous lemma, and  $x\rho = (\varepsilon(x))\rho = \rho(x)$ , therefore  $H \models \varepsilon(x) : G(x)$ .

- if  $H \vdash [M/x]\sigma : (x : \phi, G)$  by S2, that is  $H \vdash M : \phi$  and  $H \vdash \sigma : G$ , then one simply uses the induction hypotheses.



• if  $M = \langle \lambda x P, \sigma \rangle$ ,  $\phi = \psi \rightarrow \tau$ ,  $x : \psi$ ,  $G \vdash_* P : \tau$  and  $H \vdash_* \sigma : G$ , let  $\rho$  be a substitution such that  $\models \rho(z) : H(z)$  for any  $z \in \text{fv}(M)$ . We have to show that  $\models M\rho : \psi \rightarrow \tau$ . Clearly  $M\rho \Downarrow$  since  $M\rho$  is a closure. Let  $R$  be a closed term such that  $\models R : \psi$ . We have  $(M\rho)R \bowtie P[R/x](\sigma \circ \rho)$  therefore, by the lemma 4.1 and the proposition 4.6, it is enough to show that  $\models P[R/x](\sigma \circ \rho) : \tau$ . By induction hypothesis on the inference of  $H \vdash_* \sigma : G$  we have  $H \models \sigma(y) : G(y)$  for any variable  $y$ , therefore  $\models (\sigma \circ \rho)(y) : G(y)$  for  $y \in \text{fv}(P) - \{x\}$ . Then we use the induction hypothesis on the proof of  $x : \psi$ ,  $G \vdash_* P : \tau$ .

• the case of Ls5 is similar: here we have  $M = \langle \lambda^V x P, \sigma \rangle$  and  $\phi = \zeta \rightarrow \tau$ , with  $\zeta \in \Gamma$ . Clearly  $\zeta \leq_s \gamma$  by Es5.1, therefore if  $\models_s R : \zeta$  then  $R \Downarrow$ . By the proposition 2.12 we have in this case  $(M\rho)R \bowtie P[R/x](\sigma \circ \rho)$ . The rest of the proof is the same as for L5.1. The proof in the case of L5.2 follows exactly the same lines  $\square$

### 4.3 Main Results (Completeness and Full Abstraction).

As announced, we shall prove a completeness theorem, that is:

$$H \models M : \phi \Rightarrow H \vdash M : \phi$$

An obvious consequence of soundness and completeness (and of the proposition 4.6 and remark 4.7) is a first half of the full abstraction result, namely that the testing preorders are stronger than the semantical preorders:

$$M \sqsubseteq_o N \Rightarrow M \sqsubseteq_s N$$

Before seeing the converse, let us indicate what are the main points in proving the completeness theorem. First we will show some structural properties, namely weakening, cut and paste. Our weakening result is somewhat stronger than the usual one. It relies upon an extension of the entailment relation to hypotheses, relative to a given set of variables  $V$ . Let us define:

$$G \leq^V H \Leftrightarrow_{\text{def}} \forall x \in V. G(x) \leq H(x)$$

We shall omit the superscript when it is  $X$ . For instance  $(G, H) \leq G$  for any  $G$  and  $H$ . Then the *weakening* lemma – which would perhaps better be named “strengthening” <sup>(3)</sup> – asserts that if under the hypothesis  $H$  we can prove that  $M$  satisfies  $\phi$ , then by strengthening the hypothesis, we are able to prove the same fact. Formally, if  $\text{fv}(M) \subseteq V$  then

$$H \vdash M : \phi \ \& \ G \leq^V H \Rightarrow G \vdash M : \phi$$

Then we have the usual *cut* property, that is the validity of the rule:

$$\frac{H \vdash N : \psi \quad , \quad x : \psi, H \vdash M : \phi}{H \vdash M[N/x] : \phi}$$

We shall prove more generally:

$$H \vdash \sigma : G \ \& \ G \vdash M : \phi \Rightarrow H \vdash M\sigma : \phi$$

---

<sup>(3)</sup> the usual names of the structural properties refer to a “bottom-up” search for a proof of a given sequent. If we think of a “top-down” construction of proofs, we should find dual names for these properties, exchanging for instance cut and paste.

In Coppo's typing systems a kind of converse property, which we call *paste*, also holds, see for instance Krivine [21]. This property says that a proof of  $H \vdash M\sigma : \phi$  is always composed of proofs of intermediary assertions for the  $\sigma(x)$ 's and a proof that  $M$  satisfies  $\phi$  under the corresponding hypothesis:

$$H \vdash M\sigma : \phi \Rightarrow \exists G. H \vdash \sigma : G \ \& \ G \vdash M : \phi$$

The main property we have to prove is that the computational property of convergence can be ascertained using the natural deduction system:

**CONVERGENCE LEMMA.**

$$H \models M : \gamma \Rightarrow H \vdash M : \gamma$$

The proof of this lemma uses two auxiliary results, the first one being:

**CONVERGENCE LEMMA, CLOSED TERMS.** *If  $M$  is a closed term then  $M \Downarrow \Rightarrow \vdash M : \gamma$ .*

The crucial fact allowing us to prove the convergence lemma is the definability of the compact elements of the canonical domains, that is the principal filters generated by a formula  $\{\psi \mid \phi \leq \psi\}$ . Then the definability result can be stated as follows:

**CHARACTERIZATION LEMMA.** *For any formula  $\phi \in \Phi_*$  (resp.  $\phi \in \Phi_S$ ) there exists a closed  $\lambda_j^*$ -term (resp.  $\lambda_j^V$ -term)  $\mathbf{M}_\phi$  such that*

$$\vdash \mathbf{M}_\phi : \psi \Leftrightarrow \phi \leq \psi$$

This is the only result for which we need to have the call-by-value closures and the concurrent join in the syntax. To define the characteristic terms  $\mathbf{M}_\phi$  we associate with each formula  $\phi$  a "test for  $\phi$ ", that is, in the case of the  $\lambda_j^*$ -calculus, a closed  $\lambda_j^*$ -term  $\mathbf{T}_\phi$  such that  $\models_* M : \phi \Rightarrow \mathbf{T}_\phi M \Downarrow \mathbf{I}$ . For the  $\lambda_j^V$ -calculus these terms will be only defined for formulae of  $\Gamma$ , and they will be such that  $\models_S M : \zeta \Rightarrow \mathbf{T}_\zeta M \Downarrow \mathbf{I}_S$  where the strict identity  $\mathbf{I}_S$  is  $\lambda^V x x$ . The construction of these terms is, in the case of the  $\lambda_j^*$ -calculus, as follows:

$\mathbf{M}_\omega = \Omega$ $\mathbf{T}_\omega = \mathbf{F} = \lambda y \lambda x x$ $\mathbf{M}_{\phi \wedge \psi} = (\mathbf{M}_\phi \parallel \mathbf{M}_\psi)$ $\mathbf{T}_{\phi \wedge \psi} = \lambda x (\mathbf{T}_\phi x) (\mathbf{T}_\psi x)$ $\mathbf{M}_{\phi \rightarrow \psi} = \lambda x (\mathbf{T}_\phi x) \mathbf{M}_\psi$ $\mathbf{T}_{\phi \rightarrow \psi} = \lambda^V x (\mathbf{T}_\psi (x \mathbf{M}_\phi))$
---

As for the  $\lambda^\vee$ -calculus, we define the characteristic terms and testing terms as follows:

$$\begin{aligned}
\mathbf{M}_\omega &= \Omega_s \\
\mathbf{M}_\gamma &= \lambda^\vee x \Omega_s \\
\mathbf{T}_\gamma &= \mathbf{F}_s = \lambda^\vee y \lambda^\vee x x \\
\mathbf{M}_{\phi \wedge \psi} &= (\mathbf{M}_\phi \parallel \mathbf{M}_\psi) \\
\mathbf{T}_{\zeta \wedge \tau} &= \lambda^\vee x (\mathbf{T}_\zeta x) (\mathbf{T}_\tau x) \\
\mathbf{M}_{\zeta \rightarrow \phi} &= \lambda^\vee x (\mathbf{T}_\zeta x) \mathbf{M}_\phi \\
\mathbf{T}_{\zeta \rightarrow \phi} &= \begin{cases} \mathbf{T}_\gamma & \text{if } \phi \in \Phi_s - \Gamma \\ \lambda^\vee x \mathbf{T}_\phi(x \mathbf{M}_\zeta) & \text{otherwise} \end{cases}
\end{aligned}$$

We can now prove that the convergence lemma holds:

**PROOF of the CONVERGENCE LEMMA:** Assume that  $H \models M : \gamma$ ,  $\text{fv}(M) = \{x_1, \dots, x_n\}$  and  $H(x_i) = \phi_i$ . Let  $\chi$  be the substitution given by

$$\chi = [\mathbf{M}_{\phi_1}/x_1] \cdots [\mathbf{M}_{\phi_n}/x_n] \varepsilon$$

Then, since  $\models \chi(x) : H(x)$  for  $x \in \text{fv}(M)$  by the characterization lemma above and soundness, we have  $M\chi \Downarrow$ , hence, by the convergence lemma for closed terms:

$$\vdash M\chi : \gamma$$

Then by paste there exist  $\psi_1, \dots, \psi_n$  such that

$$x_1 : \psi_1, \dots, x_n : \psi_n \vdash M : \gamma$$

and  $\vdash \chi(x_i) : \psi_i$ . Then, by the characterization lemma,  $H(x_i) \leq \psi_i$  for  $x_i \in \text{fv}(M)$ , therefore by weakening  $H \vdash M : \gamma$   $\square$

Finally to prove the completeness theorem, we use Hindley's method [19,20], by means of a refinement of the usual deduction theorem, namely:

**EXTENSIONALITY LEMMA (THE DEDUCTION THEOREM).**

$$H \vdash M : \phi \rightarrow \psi \Leftrightarrow H \vdash M : \gamma \quad \text{and} \quad x : \phi, H \vdash Mx : \psi \quad \text{for some } x \notin \text{fv}(M)$$

Dezani and Margaria showed in [17] that such a property was needed for completeness: they added to the "typing" system a rule, called Hindley's rule, whose typical instance is:

$$\frac{H \vdash M : \phi \wedge (\omega \rightarrow \omega)}{H \vdash \lambda x (Mx) : \phi} \quad x \notin \text{fv}(M)$$

**PROOF of the COMPLETENESS THEOREM:** we show  $H \models M : \phi \Rightarrow H \vdash M : \phi$  by induction on the formula  $\phi$ . The cases where  $\phi = \omega$  and  $\phi = \phi_0 \wedge \phi_1$  are obvious (using L1 and L2). If  $\phi = \gamma$  then we use the convergence lemma.

If  $H \models M : \phi \rightarrow \psi$  then  $\models M\sigma : \phi \rightarrow \psi$  for any substitution  $\sigma$  such that  $\models \sigma(z) : H(z)$  for all  $z \in \text{fv}(M)$ . Then  $M\sigma \Downarrow$  and  $\models (M\sigma)R : \psi$  for any closed term  $R$  such that  $\models R : \phi$ . Since  $H \models M : \gamma$  we have  $H \vdash M : \gamma$  by the convergence lemma. Let  $x$  be a variable not in  $\text{fv}(M)$ . Then by the lemma 2.3, propositions 2.12 and 4.6, we have:

$$(M\sigma)R \simeq_{\mathcal{L}} (Mx)[R/x]\sigma$$

hence  $x : \phi, H \models Mx : \psi$  by definition. By induction hypothesis

$$x : \phi, H \vdash Mx : \psi$$

therefore  $H \vdash M : \phi \rightarrow \psi$  by the extensionality lemma  $\square$

To conclude this section we show how to prove the second half of the full abstraction result, that is more precisely the *adequacy theorem*:

$$M \sqsubseteq_{\mathcal{S}} N \Rightarrow M \sqsubseteq_{\mathcal{O}} N$$

We have to prove that  $M \sqsubseteq_{\mathcal{S}} N \Rightarrow C[M\sigma] \prec C[N\sigma]$  for any substitution  $\sigma$  and context  $C$ , closing  $M\sigma$  and  $N\sigma$ . We have seen (lemma 3.5) that:

$$M \sqsubseteq_{\mathcal{S}} N \Rightarrow \forall C. C[M] \sqsubseteq_{\mathcal{S}} C[N]$$

We also announced that the semantical preorders are preserved by instantiation (lemma 3.6). We can now prove this result:

**LEMMA.**  $M \sqsubseteq_{\mathcal{S}} N \Rightarrow \forall \sigma. M\sigma \sqsubseteq_{\mathcal{S}} N\sigma$

**PROOF:** if  $H \vdash M\sigma : \phi$  then by paste there exists an hypothesis  $G$  such that  $H \vdash \sigma : G$  and  $G \vdash M : \phi$ . Then  $G \vdash N : \phi$  since  $M \sqsubseteq_{\mathcal{S}} N$ , and  $H \vdash N\sigma : \phi$  by cut  $\square$

An obvious consequence of these lemmas is:

$$M \sqsubseteq_{\mathcal{S}} N \Rightarrow \forall \sigma \forall C. C[M\sigma] \sqsubseteq_{\mathcal{S}} C[N\sigma]$$

Therefore to prove the full abstraction theorem it just remains to show that a closed term is convergent if and only if it has a non-trivial semantic value, that is:

**LEMMA (COMPUTATIONAL ADEQUACY) 4.9.** *For any closed term  $M$*

$$\llbracket M \rrbracket \neq \perp \Leftrightarrow M \Downarrow$$

**PROOF:** since  $\llbracket M \rrbracket \neq \perp \Leftrightarrow \gamma \in \llbracket M \rrbracket \Leftrightarrow \vdash M : \gamma$ , the implication  $M \Downarrow \Rightarrow \llbracket M \rrbracket \neq \perp$  is just a reformulation of the convergence lemma for closed terms. The converse implication is a consequence of the soundness of the natural deduction systems with respect to the realizability interpretation, since  $\llbracket M \rrbracket \neq \perp \Leftrightarrow \vdash M : \gamma \Rightarrow \models M : \gamma \Leftrightarrow M \Downarrow \square$

One should note that the adequacy results do not involve the characterization lemma. This means that the canonical domains  $D_*$  and  $D_{\mathcal{S}}$  provide us with adequate abstract models respectively for the usual (lazy)  $\lambda$ -calculus and the weak call-by-value  $\lambda$ -calculus, see Abramsky & Ong [4] and Moggi [29].

It remains to prove the results mentioned above, that is: weakening, cut and paste, the convergence lemma for closed terms, the characterization lemma and the extensionality lemma (the deduction theorem). This will be done in the next section, but we first give some consequences of completeness and full abstraction.

#### 4.4 Some Consequences.

A first obvious consequence of full abstraction is that all the previously encountered preorders coincide. Then we can forget about the subscripts, and simply write  $M \sqsubseteq N$  and  $M \simeq N$ . Here we list, without proving them, some properties of this preorder (these are mostly given for the  $\lambda_j^*$ -calculus. The reader is invited to find the appropriate strict versions). It is a precongruence, and in particular we have:

$$\begin{aligned} (\mu^*) \quad M \sqsubseteq M' &\Rightarrow NM \sqsubseteq NM' \\ (\nu^*) \quad M \sqsubseteq M' &\Rightarrow MN \sqsubseteq M'N \\ (\xi^*) \quad M \sqsubseteq M' &\Rightarrow \lambda xM \sqsubseteq \lambda xM' \end{aligned}$$

The equations  $\mu$  and  $\xi$  are semantically valid, therefore they can be used to perform some optimizations. For instance if we define a left sequential disjunction by  $\mathbf{V}_l = \lambda xy. \text{cond}x\mathbf{K}y$ , then we also have  $\mathbf{V}_l \simeq \lambda xy. (x\mathbf{K})y$ .

We already mentioned that the conversion relation is stronger than the semantical equality, that is  $M \bowtie N \Rightarrow M \simeq N$ , since it is a symmetric applicative simulation. Then for instance we have:

$$\begin{aligned} M \equiv N &\Rightarrow M \simeq N \\ \langle \lambda xM, \sigma \rangle N &\simeq M[N/x]\sigma \\ N \Downarrow &\Rightarrow \langle \lambda^v xM, \sigma \rangle N \simeq M[N/x]\sigma \end{aligned}$$

As in Scott 80[42] and Abramsky 89[3], a weak version of the “functionality principle”  $\eta$  holds, that is:

$$\eta^- : \quad M \sqsubseteq \lambda x(Mx) \quad (x \text{ not free in } M)$$

Similarly one has  $M \sqsubseteq \lambda^v x(Mx)$ . Moreover one can check that:

$$M \Downarrow \Rightarrow M \simeq \lambda x(Mx) \quad (x \text{ not free in } M)$$

The  $\omega$ -rule of the  $\lambda$ -calculus (see Barendregt [5] definition 4.1.10) is not valid: for instance we have  $\Omega R \simeq (\lambda x\Omega)R$  for all closed terms  $R$ , but  $\Omega \not\simeq \lambda x\Omega$ . However we have, for closed terms:

$$M \sqsubseteq N \Leftrightarrow (M \prec N \ \& \ \forall R \text{ closed. } MR \sqsubseteq NR)$$

Since the following holds, for closed terms:

$$\models M : \phi \Leftrightarrow \mathbf{M}_\phi \sqsubseteq M$$

one can see that the axiomatization of entailment is *complete*, that is:

$$\begin{aligned} \phi \leq \psi &\Leftrightarrow \mathbf{M}_\phi \sqsubseteq \mathbf{M}_\psi \\ &\Leftrightarrow \forall M. \models M : \phi \Rightarrow \models M : \psi \end{aligned}$$

The full testing ability is achieved using only *finite* tests, namely  $C_\phi = (\mathbf{T}_\phi \square)$  since we have

$$\models M : \phi \Leftrightarrow C_\phi[M] \Downarrow$$

Similarly we could have restricted applicative tests to finite data, that is:

$$A_f ::= \square \mid \langle \lambda xA_f, \sigma \rangle \mid \langle \lambda^v xA_f, \sigma \rangle \mid (A_f \mathbf{M}_\phi)$$

Obviously  $(M \parallel N)$  is the least upper bound of  $M$  and  $N$ :

$$\forall P. M \subseteq P \ \& \ N \subseteq P \Leftrightarrow (M \parallel N) \subseteq P$$

therefore the usual properties of the join (namely the ones of set-theoretic union) hold:

$$\begin{aligned} (M \parallel (N \parallel P)) &\simeq ((M \parallel N) \parallel P) \\ (M \parallel N) &\simeq (N \parallel M) \\ (M \parallel M) &\simeq M \\ (M \parallel \Omega) &\simeq M \end{aligned}$$

Moreover we have:

$$\begin{aligned} (M \parallel N)P &\simeq (MP \parallel NP) \\ \lambda x(M \parallel N) &\simeq (\lambda x M \parallel \lambda x N) \\ \lambda^v x(M \parallel N) &\simeq (\lambda^v x M \parallel \lambda^v x N) \end{aligned}$$

Similarly we have  $(MN \parallel MP) \subseteq M(N \parallel P)$ , but the converse is false in general. For instance if  $t = \gamma \rightarrow (\omega \rightarrow \gamma)$  and  $f = \omega \rightarrow (\gamma \rightarrow \gamma)$ , then we have  $\mathbf{T}_{t \wedge f}(\mathbf{K} \parallel \mathbf{F}) \Downarrow$ , whereas  $\mathbf{T}_{t \wedge f} \mathbf{K} \Uparrow$  and  $\mathbf{T}_{t \wedge f} \mathbf{F} \Uparrow$ . We indicated in the introduction how to define a parallel disjunction (parallel or):

$$\mathbf{O} =_{\text{def}} \lambda xy. ((x\mathbf{T})y \parallel ((y\mathbf{T})x)) = (\mathbf{V}_l \parallel \mathbf{V}_r)$$

One can check that this combinator satisfies the required properties, namely:

$$\begin{aligned} (\mathbf{O}\Omega)\mathbf{T} &\simeq \mathbf{T} \simeq (\mathbf{O}\mathbf{T})\Omega \\ (\mathbf{O}\mathbf{F})\mathbf{F} &\simeq \mathbf{F} \end{aligned}$$

## 5. The Logical Systems: Proofs.

### 5.1 Structural Properties: Weakening and Cut.

Usually in a logical calculus there is no particular “annotation” associated with the formulae: a sequent has the form  $\Gamma \vdash \phi$  where  $\Gamma = \phi_1, \dots, \phi_n$  is a sequence of formulae. In fact this sequence is almost always a multiset, since one usually assumes the *exchange* rule:

$$\frac{\Gamma, \phi, \psi, \Delta \vdash \zeta}{\Gamma, \psi, \phi, \Delta \vdash \zeta}$$

However, in our systems we can only exchange two items  $x:\phi$  and  $y:\psi$  in the hypothesis if the variables are distinct. For instance  $x:\phi, x:\psi \vdash x:\phi$ , but the sequent  $x:\psi, x:\phi \vdash x:\phi$ , which is not provable unless  $\psi \leq \phi$ , would lead to the wrong conclusion  $\vdash \lambda x \lambda x x:\phi \rightarrow (\psi \rightarrow \phi)$ . Similarly, the *contraction* rule

$$\frac{\Gamma, \phi, \phi, \Delta \vdash \zeta}{\Gamma, \phi, \Delta \vdash \zeta}$$

does not really make sense in our systems: obviously we may contract  $x:\phi, x:\phi$  into  $x:\phi$ , but it would be absurd to try to contract  $x:\phi, y:\phi$  if  $x \neq y$ . Another rule which is frequently assumed (and, indeed, needed to “type”  $\lambda$ -terms such as  $\mathbf{K}$ ) is the *weakening* rule:

$$\frac{\Gamma \vdash \phi}{\Gamma, \Delta \vdash \phi}$$

To show that this rule holds in our logical systems, we need two preliminary results. Let us first show that we cannot infer more about a variable than assumed:

**LEMMA 5.1.**  $H \vdash x:\phi \Leftrightarrow H(x) \leq \phi$

**PROOF:** the implication  $H(x) \leq \phi \Rightarrow H \vdash x:\phi$  clearly holds, by virtue of L4 and L3. The converse is easily proved by induction on the inference of the sequent  $H \vdash x:\phi$  (which can only be inferred by means of L1, L2, L3 or L4). One uses the general laws E1, E4, E2 and E3.1 for entailment  $\square$

Then we remark that proving that a substitution  $\sigma$  satisfies an hypothesis  $G$  amounts to show that each “element”  $\sigma(x)$  of the substitution satisfies the corresponding hypothesis:

**LEMMA 5.2.**  $H \vdash \sigma:G \Leftrightarrow \forall x. H \vdash \sigma(x):G(x)$

**PROOF:** it is easy to show that  $H \vdash \sigma:G \Rightarrow \forall x. H \vdash \sigma(x):G(x)$ , by induction on the inference of  $H \vdash \sigma:G$ . In the case of  $\sigma = \varepsilon$  one uses L4 and L3. Conversely if  $H \vdash \sigma(x):G(x)$  then one proceeds by induction on  $\sigma$ . In the case of  $\sigma = \varepsilon$  one uses the previous lemma. If  $\sigma = [M/y]\rho$ , let  $\phi = G(y)$  and  $G' = (y:\omega, G)$ . Then  $H \vdash \rho(x):G'(x)$  for any variable  $x$ , therefore  $H \vdash \rho:G'$  by induction hypothesis. Since  $H \vdash M:\phi$  and  $(y:\phi, G') = G$  we have  $H \vdash \sigma:G$  by S2  $\square$

It should be clear that if a sequent  $H \vdash \sigma:G$  is used, by means of the rules for the closures, in the inference of a sequent  $F \vdash M:\phi$ , then for any variable  $x$  either  $H \vdash \sigma(x):G(x)$ , with a proof shorter than the one of  $F \vdash M:\phi$ , or  $\sigma(x) = x$  and  $H(x) \leq G(x)$ . This fact will be used to establish some of the following technical results. In particular, we can now prove our weakening lemma:

**LEMMA (WEAKENING) 5.3.** If  $H \vdash M:\phi$  and  $G \leq^V H$  with  $\text{fv}(M) \subseteq V$  then  $G \vdash M:\phi$ .

**PROOF:** by induction on the inference of the sequent  $H \vdash M:\phi$ , and by case on the last rule used in this inference:

- this is obvious for L1. For L2 and L3, we simply use the induction hypothesis.
- for L4 we have  $M = x$ , hence  $x \in V$ , and  $H = (x:\phi, H')$ . Then  $G \leq^V H$  implies  $G = (x:\psi, G')$  with  $\psi \leq \phi$ . By L4 and L3 we then have  $G \vdash x:\phi$ .
- for L5.1,  $M = \langle \lambda x R, \sigma \rangle$  and  $\phi = \psi \rightarrow \tau$  with  $x:\psi, F \vdash_\star R:\tau$  and  $H \vdash_\star \sigma:F$ . Let  $F'$  be the hypothesis given by:

$$F'(z) = \begin{cases} F(z) & \text{if } z \in \text{fv}(R) - \{x\} \\ \omega & \text{otherwise} \end{cases}$$

Let  $W = \text{fv}(R)$ . Then  $(x:\psi, F') \leq_\star^W (x:\psi, F)$  therefore by induction hypothesis:

$$x:\psi, F' \vdash_\star R:\tau$$

Let us show that  $G \vdash_\star \sigma(z):F'(z)$  for any variable  $z$ :

- this is true if  $z \notin \text{fv}(R) - \{x\}$ , by L1.
- if  $z \in \text{fv}(R) - \{x\}$  and  $H \vdash_\star \sigma(z):F(z)$  with a proof that is shorter than the one of  $H \vdash_\star M:\phi$ , then by induction hypothesis  $G \vdash_\star \sigma(z):F(z)$ , and  $F'(z) = F(z)$ .
- if  $z \in \text{fv}(R) - \{x\}$  with  $\sigma(z) = z$  and  $H(z) \leq_\star F(z)$  then  $z \in V$ , therefore  $G(z) \leq_\star H(z)$ , and  $F(z) = F'(z)$ , hence  $G \vdash_\star \sigma(z):F'(z)$  by L4 and L3.

Then  $G \vdash_\star \sigma:F'$  by the lemma 5.2, hence  $G \vdash_\star M:\phi$  by L5.1. The cases of L5 and L5.2 are entirely similar.

- for L6 we have  $M = (PQ)$  with  $H \vdash P:(\psi \rightarrow \phi)$  and  $H \vdash Q:\psi$ . Since  $\text{fv}(P) \subseteq \text{fv}(M)$  and  $\text{fv}(Q) \subseteq \text{fv}(M)$  we have by induction hypothesis  $G \vdash P:(\psi \rightarrow \phi)$  and  $G \vdash Q:\psi$ , and we use L6 to infer  $G \vdash M:\phi$ . The argument is similar for L7  $\square$

Let us see some instances of this lemma: we saw that  $(H, F) \leq H$ , therefore the usual weakening rule is valid:

$$H \vdash M:\phi \Rightarrow H, F \vdash M:\phi$$

This lemma also allows us to “restrict” the hypothesis to the free variables of the subject term  $M$ , assigning  $\omega$  to any other variable, or to introduce conjunction into the hypotheses: given two hypotheses  $F$  and  $G$  we define their conjunction  $F \wedge G$  by  $(F \wedge G)(x) = F(x) \wedge G(x)$  for all  $x$ . The following fact is an easy consequence of E3.2, E3.3 and E4:

REMARK.  $H \leq^V F \wedge G \Leftrightarrow H \leq^V F \ \& \ H \leq^V G$

Therefore we have:

COROLLARY 5.4. *If  $F \vdash M : \phi$  or  $G \vdash M : \phi$  then  $F \wedge G \vdash M : \phi$ .*

Another structural rule (in the usual logical sense, that is concerning the structure of the hypotheses) which should hold in any sequent calculus is the *cut* rule, whose usual formulation is:

$$\frac{\Gamma \vdash \psi \quad \psi, \Gamma \vdash \phi}{\Gamma \vdash \phi}$$

In our system, the cut rule will result from:

PROPOSITION 5.5. *If  $H \vdash M : \phi$  &  $G \vdash \sigma : H \Rightarrow G \vdash M\sigma : \phi$ .*

PROOF: by induction on the inference of the sequent  $H \vdash M : \phi$ , and by case on the last rule used in this inference. The only cases deserving some consideration are L5.1, Ls5 and L5.2. In the case of L5.1 we have  $M = \langle \lambda x R, \rho \rangle$  and  $\phi = \psi \rightarrow \tau$  with  $x : \psi$ ,  $F \vdash_\star R : \tau$  and  $H \vdash_\star \rho : F$ . Let us show that  $G \vdash_\star (\rho \circ \sigma)(z) : F(z)$  for any variable  $z$ : if  $H \vdash_\star \rho(z) : F(z)$  with a proof that is shorter than the one of  $H \vdash_\star M : \phi$ , then by induction hypothesis  $G \vdash_\star (\rho \circ \sigma)(z) : F(z)$  since  $(\rho \circ \sigma)(z) = (\rho(z))\sigma$  (lemma 2.1). Otherwise  $\rho(z) = z$  and  $H(z) \leq_\star F(z)$ , in which case  $(\rho \circ \sigma)(z) = \sigma(z)$ . Since  $G \vdash_\star \sigma(z) : H(z)$  (lemma 5.2) we have  $G(z) \vdash_\star \sigma(z) : F(z)$  by L3. Then  $G \vdash_\star (\rho \circ \sigma) : F$  by the lemma 5.2, and  $G \vdash_\star M\sigma : \phi$  by L5.1 since  $M\sigma = \langle \lambda x R, \rho \circ \sigma \rangle$ . The cases of Ls5 and L5.2 are entirely similar  $\square$

COROLLARY (CUT) 5.6.  $H \vdash N : \psi \ \& \ x : \psi, H \vdash M : \phi \Rightarrow H \vdash M([N/x]\varepsilon) : \phi$

PROOF: by S1 we have  $H \vdash \varepsilon : H$ , therefore  $H \vdash [N/x]\varepsilon : (x : \psi, H)$  by S2  $\square$

## 5.2 Extensionality, Paste and Reduction.

In this section we first prove a refined version of the deduction theorem. The usual statement of the deduction theorem, in logical systems without “annotations” is:

$$\Gamma \vdash \phi \rightarrow \psi \Leftrightarrow \phi, \Gamma \vdash \psi$$

Assuming that in the strict case  $\phi \rightarrow \psi$  is a well-formed formula, that is  $\phi \in \Gamma$ , it is very easy to prove that this holds in our logical systems: in the “ $\Leftarrow$ ” direction, this is just L5.1 or Ls5. For the converse, if  $H \vdash M : \phi \rightarrow \psi$  and  $x$  is a variable not in  $\text{fv}(M)$  then  $x : \phi, H \vdash M : \phi \rightarrow \psi$  by weakening, and  $x : \phi, H \vdash x : \phi$  by L4, therefore  $x : \phi, H \vdash Mx : \psi$  by L6 (modus ponens). However if we abstract once more we get the term  $\lambda x Mx$  or  $\lambda^\forall x Mx$  which is usually more informative than  $M$  (for instance if  $M = \Omega$  or  $M = \Omega_\Sigma$ ). As indicated above, we need a more refined result. Recall that  $\gamma$  denotes the formula  $\omega \rightarrow \omega$  in the  $\Phi_\star$ -logic. Then our sharpened deduction theorem is:



**EXTENSIONALITY LEMMA (THE DEDUCTION THEOREM) 5.7.**  $H \vdash M : \phi \rightarrow \psi$  if and only if  $H \vdash M : \gamma$  and  $x : \phi, H \vdash Mx : \psi$  for some  $x \notin \text{fv}(M)$  (assuming that  $\phi \in \Gamma$  in the strict case).

**PROOF:** if  $H \vdash_* M : \phi \rightarrow \psi$  then we have  $H \vdash_* M : \omega \rightarrow \omega$  by L3 since by E1, E<sub>\*</sub>7 and E<sub>\*</sub>5

$$\phi \rightarrow \psi \leq_* \phi \rightarrow \omega \leq_* \omega \rightarrow \omega$$

Similarly in the strict case  $H \vdash_s M : \gamma$  since  $\phi \rightarrow \psi \leq_s \gamma$  by Es5.1. Moreover if  $x \notin \text{fv}(M)$  we have by weakening  $x : \phi, H \vdash M : \phi \rightarrow \psi$  and  $x : \phi, H \vdash x : \phi$  by L4. Then by L6 we get  $x : \phi, H \vdash Mx : \psi$ .

Conversely, assume that  $H \vdash M : \gamma$  and  $x : \phi, H \vdash Mx : \psi$  with  $x \notin \text{fv}(M)$ , and  $\phi \in \Gamma$  in the strict case. We prove that  $H \vdash M : \phi \rightarrow \psi$  by induction on the inference of  $x : \phi, H \vdash Mx : \psi$ :

- if this sequent is proved using L1 then  $\psi = \omega$ , and  $H \vdash M : (\phi \rightarrow \omega)$  by L3 since  $H \vdash M : \gamma$  and  $\gamma \leq \phi \rightarrow \omega$  (by E1 and E<sub>\*</sub>7, or Es5.2, Es5.1 and Es7)
- by L2, we have  $\psi = \psi_0 \wedge \psi_1$ , and by induction hypothesis  $H \vdash M : \phi \rightarrow \psi_i$ . Then by L2  $H \vdash M : (\phi \rightarrow \psi_0) \wedge (\phi \rightarrow \psi_1)$ , hence by L3 and E<sub>\*</sub>6 (or Es6) we get  $H \vdash M : \phi \rightarrow (\psi_0 \wedge \psi_1)$ .
- by L3,  $x : \phi, H \vdash Mx : \psi'$  for some  $\psi'$  such that  $\psi' \leq \psi$ . Then by induction hypothesis  $H \vdash M : \phi \rightarrow \psi'$ , hence  $H \vdash M : \phi \rightarrow \psi$  by L3 since  $\phi \rightarrow \psi' \leq \phi \rightarrow \psi$  (by E<sub>\*</sub>7 or Es7).
- the only remaining case is L6. Then for some  $\phi'$  we have  $x : \phi, H \vdash M : \phi' \rightarrow \psi$  and  $x : \phi, H \vdash x : \phi'$ . By the lemma 5.1,  $\phi \leq \phi'$ , therefore by L3,  $x : \phi, H \vdash M : \phi \rightarrow \psi$  since  $\phi' \rightarrow \psi \leq \phi \rightarrow \psi$  (by E<sub>\*</sub>7 or Es7). Since  $x \notin \text{fv}(M)$  we have  $H \vdash M : \phi \rightarrow \psi$  by weakening  $\square$

An important property of Coppo's typing systems is that if a term  $M$  reduces into  $N$  and  $N$  satisfies  $\phi$  under the hypothesis  $H$ , then the same holds for  $M$  (cf. [10,21]). Since we defined reduction only for closed terms, we will show here:

$$M \triangleright N \ \& \ \vdash N : \phi \Rightarrow \vdash M : \phi$$

In other words, reduction is decreasing with respect to "typability", that is with respect to the semantical preorder. To establish this property in the case of the  $\beta$ -rules, we need to know how to "type"  $R[Q/x]\rho$ . This is expressed in the paste property, proved below. Let us first see some auxiliary properties. One can remark that the rules L1, L2 and L3 can be extended to substitutions:

**LEMMA 5.8.**

- (i) if  $G(x) = \omega$  for any  $x$  then  $H \vdash \sigma : G$  for any  $H$  and  $\sigma$
- (ii) if  $H \vdash \sigma : G_0$  and  $H \vdash \sigma : G_1$  then  $H \vdash \sigma : G_0 \wedge G_1$
- (iii) if  $H \vdash \sigma : G$  and  $G \leq F$  then  $H \vdash \sigma : F$ .

**PROOF:** trivial  $\square$

Similarly, the weakening lemma holds for the sequents concerning substitutions, that is:

**LEMMA 5.9.**  $H \vdash \sigma : G \ \& \ F \leq H \Rightarrow F \vdash \sigma : G$

Now we can prove the paste property:

**PROPOSITION (PASTE) 5.10.**  $H \vdash M\sigma : \phi \Rightarrow \exists G. H \vdash \sigma : G \ \& \ G \vdash M : \phi$

**PROOF:** we show simultaneously

$$H \vdash M\sigma : \phi \Rightarrow \exists G. H \vdash \sigma : G \ \& \ G \vdash M : \phi$$

and

$$H \vdash \rho \circ \sigma : F \Rightarrow \exists G. H \vdash \sigma : G \ \& \ G \vdash \rho : F$$

by structural induction on  $M$  and  $\rho$ , and then by induction on the proofs of the sequents. The sequent  $H \vdash M\sigma : \phi$  can only be proved using one of the “filter rules” L1, L2 or L3, or using a specific rule depending on the structure of  $M$ . In fact we can “factorize” the cases of L1, L2 and L3, regardless of the shape of  $M$ :

- if  $H \vdash M\sigma : \phi$  is proved using L1, then  $\phi = \omega$  and we can let  $G(x) = \omega$  for any  $x$ . Then  $H \vdash \sigma : G$  by the lemma 5.8, and  $G \vdash M : \phi$  by L1.
- if  $H \vdash M\sigma : \phi$  is proved using L2 then  $\phi = \phi_0 \wedge \phi_1$  with  $H \vdash M\sigma : \phi_i$ . Then by induction hypothesis (on the inference of the sequents) there exists  $G_i$  such that  $H \vdash \sigma : G_i$  and  $G_i \vdash M : \phi_i$ . Let  $G = G_0 \wedge G_1$ ; then by the lemma 5.8 above  $H \vdash \sigma : G$ , and  $G \vdash M : \phi_i$  by weakening, therefore  $G \vdash M : \phi$  by L2.
- if  $H \vdash M\sigma : \phi$  is proved using L3, there exists  $\psi$  such that  $\psi \leq \phi$  and  $H \vdash M\sigma : \psi$ . By induction hypothesis (on the proof of the sequents) there exists  $G$  such that  $H \vdash \sigma : G$  and  $G \vdash M : \psi$ , therefore  $G \vdash M : \phi$  by L3.

Now we examine the various possibilities for  $M$ :

- if  $M$  is a variable, say  $x$ , then we let  $G = x : \phi$ . We have  $H \vdash \sigma(y) : G(y)$  for any variable  $y$  since  $\sigma(x) = M\sigma$ , therefore  $H \vdash \sigma : G$  by the lemma 5.2, and  $G \vdash x : \phi$  by L4.
- if  $M = \langle \lambda x R, \rho \rangle$ , then  $M\sigma = \langle \lambda x R, \rho \circ \sigma \rangle$ , and we may assume that  $H \vdash M\sigma : \phi$  is proved using L5.1, that is:  $\phi = \psi \rightarrow \tau$  with  $x : \psi$ ,  $F \vdash R : \tau$  and  $H \vdash \rho \circ \sigma : F$ . By induction hypothesis (recall that  $\rho \propto M$ ) there exists  $G$  such that  $H \vdash \sigma : G$  and  $G \vdash \rho : F$ . Then  $G \vdash M : \phi$  by L5.1. The proof is the same for  $M = \langle \lambda^v x R, \rho \rangle$  (with  $H \vdash M : \phi$  inferred by means of L5.2 or L5.5).
- if  $M = M_0 M_1$  we have  $M\sigma = M_0 \sigma M_1 \sigma$ , and we may assume that  $H \vdash M\sigma : \phi$  is proved using L6, that is  $H \vdash M_0 \sigma : \psi \rightarrow \phi$  and  $H \vdash M_1 \sigma : \psi$ . By induction hypothesis there exist  $G_0$  and  $G_1$  such that  $H \vdash \sigma : G_i$  and  $G_0 \vdash M_0 : \psi \rightarrow \phi$  and  $G_1 \vdash M_1 : \psi$ . Let  $G = G_0 \wedge G_1$ ; then  $H \vdash \sigma : G$  by the lemma 5.8 above, and  $G \vdash M_0 : \psi \rightarrow \phi$  and  $G \vdash M_1 : \psi$  by weakening, therefore  $G \vdash M : \phi$  by L6.
- if  $M = (M_0 \parallel M_1)$  then  $M\sigma = (M_0 \sigma \parallel M_1 \sigma)$ , and we may assume that  $H \vdash M\sigma : \phi$  is proved by means of L7, that is  $\phi = \phi_0 \wedge \phi_1$  with  $H \vdash M_i \sigma : \phi_i$ . By induction hypothesis there exists  $G_i$  such that  $H \vdash \sigma : G_i$  and  $G_i \vdash M_i : \phi_i$ . Let  $G = G_0 \wedge G_1$ ; then by the lemma 5.8 above  $H \vdash \sigma : G$  and  $G \vdash M_i : \phi_i$  by weakening, therefore  $G \vdash M : \phi$  by L7.

Finally we examine the two possible cases for  $\rho$ :

- if  $\rho = \varepsilon$  then  $\rho \circ \sigma = \sigma$ . We let  $G = F$ ; then  $H \vdash \sigma : G$  and  $G \vdash \rho : F$  by S1.
- if  $\rho = [M/x]\rho'$  then  $\rho \circ \sigma = [M\sigma/x](\rho' \circ \sigma)$ , and  $H \vdash \rho \circ \sigma : F$  can only be proved using S2, that is:  $F = (x : \phi, F')$  with  $H \vdash M\sigma : \phi$  and  $H \vdash \rho' \circ \sigma : F'$ . Then by induction hypothesis (recall that  $M \propto \rho$  and  $\rho' \propto \rho$ ) there exist  $G'$  and  $G''$  such that  $H \vdash \sigma : G'$  and  $G' \vdash M : \phi$ , and  $H \vdash \sigma : G''$  and  $G'' \vdash \rho' : F'$ . Let  $G = G' \wedge G''$ . Then by the lemma 5.8 above  $H \vdash \sigma : G$ , and  $G \vdash M : \phi$  by weakening, and  $G \vdash \rho' : F'$  by the lemma 5.9. Therefore  $G \vdash \rho : F$  by S2.  $\square$

To show that reduction is semantically decreasing, we need some preliminary results. We let the reader check that the following holds:

**REMARK 5.11.**  $\forall \phi \in \Phi_s \ \exists \zeta \in \Gamma. \phi \wedge \gamma \sim_s \zeta$

Let us show that any partial normal form satisfies the convergence formula:

LEMMA 5.12. *If  $K$  is a partial normal form then  $\vdash K : \gamma$ .*

PROOF: by induction on the definition of the notion of partial normal form.

- if  $K$  is a closure  $\langle \lambda x R, \rho \rangle$ , let  $G$  be the hypothesis given by  $G(z) = \omega$  for any variable  $z$ . Then  $x : \omega, G \vdash_\star R : \omega$  by L1, and  $\vdash_\star \rho : G$  (by S1, or by a repeated use of L1 and S2 if  $\rho \neq \varepsilon$ ). Then  $\vdash_\star K : \gamma$  by L5.1.

- if  $K = \langle \lambda^\vee x R, \rho \rangle$ , let  $G$  be the hypothesis given by  $G(z) = \omega$  for any variable  $z$ . Then  $x : \gamma, G \vdash_\star R : \omega$  by L1, and  $\vdash_\star \rho : G$ . Then  $\vdash_\star K : \gamma \rightarrow \omega$  by L5.2, therefore  $\vdash_\star K : \gamma$  by E<sub>5</sub>.5 and L3. Similarly  $\vdash_\mathbf{s} K : \gamma \rightarrow \omega$  by Ls5, hence  $\vdash_\mathbf{s} K : \gamma$  by Es5.1 and L3.

- if  $K$  is  $(M \parallel N)$  where  $M$  or  $N$  is a partial normal form, then we use the induction hypothesis and the fact that  $\vdash P_i : \phi \Rightarrow \vdash (P_0 \parallel P_1) : \phi$  (see § 3.3.2)  $\square$

PROPOSITION (REDUCTION is DECREASING) 5.13.  $M \triangleright N \ \& \ \vdash N : \phi \Rightarrow \vdash M : \phi$

PROOF: by induction on the definition of  $M \triangleright N$ , and then on the inference of  $\vdash N : \phi$ . As in the proof of the paste property, it is easy to see that one can “factorize” the cases where this sequent is proved by means of L1, L2 or L3. This is left to the reader. In the rest of the proof we shall not take these cases into consideration.

- if  $M = \langle \lambda x R, \sigma \rangle$  and  $N = \langle \lambda x R, \rho \rangle$  with  $\sigma(z) \triangleright \rho(z)$  for  $z \in \text{fv}(R) - \{x\}$ , we may assume that  $\vdash N : \phi$  is proved by means of L5.1, that is  $\phi = \psi \rightarrow \tau$  with  $x : \psi, H \vdash R : \tau$  and  $\vdash \rho : H$ . Let  $G$  be the hypothesis given by:

$$G(z) = \begin{cases} H(z) & \text{if } z \in \text{fv}(R) - \{x\} \\ \omega & \text{otherwise} \end{cases}$$

Then  $x : \psi, G \vdash R : \tau$  by weakening and  $\vdash \rho : G$  by the lemma 5.8 since  $H \leq G$ . By the lemma 5.2 we have  $\vdash \rho(z) : G(z)$  for any  $z$ , therefore by induction hypothesis (since the proof of  $\sigma(z) \triangleright \rho(z)$  is shorter than the one of  $M \triangleright N$ )  $\vdash \sigma(z) : G(z)$  for  $z \in \text{fv}(R) - \{x\}$ , and  $\vdash \sigma(z) : G(z)$  for  $z \notin \text{fv}(R) - \{x\}$  by L1. Then  $\vdash \sigma : G$  by the lemma 5.2, and  $\vdash M : \phi$  by L5.1.

- the proof is the same for  $M = \langle \lambda^\vee x R, \sigma \rangle$  and  $N = \langle \lambda^\vee x R, \rho \rangle$  with  $\sigma(z) \triangleright \rho(z)$  for  $z \in \text{fv}(R) - \{x\}$ .
- if  $M = M_0 M_1$  and  $N = N_0 N_1$  with  $M_i \triangleright N_i$ , we may assume that  $\vdash N : \phi$  is proved by L6, that is  $\vdash N_0 : \psi \rightarrow \phi$  and  $\vdash N_1 : \psi$ . Then we use the induction hypothesis and L6 to show  $\vdash M : \phi$ . The argument is similar if  $M = (M_0 \parallel M_1)$  and  $N = (N_0 \parallel N_1)$  with  $M_i \triangleright N_i$ , and  $\vdash N : \phi$  is proved using L7.

- if  $M = \langle \lambda x R, \sigma \rangle P$  and  $N = R[P/x]\sigma$  then by paste there exists  $H$  such that  $\vdash [P/x]\sigma : H$  and  $H \vdash R : \phi$ . The first sequent can only be inferred using S2, that is  $H = (x : \psi, G)$  for some  $\psi$  and  $G$  such that  $\vdash P : \psi$  and  $\vdash \sigma : G$ . Then  $x : \psi, G \vdash R : \phi$ , therefore  $\vdash \langle \lambda x R, \sigma \rangle : \phi$  by L5.1, and  $\vdash M : \phi$  by L6 since  $\vdash P : \psi$ .

- if  $M = \langle \lambda^\vee x R, \sigma \rangle K$  and  $N = R[K/x]\sigma$  where  $K$  is a partial normal form, then we may assume that  $\vdash N : \phi$  is proved by means of L5.2 (in the  $\lambda^\vee_j$ -calculus) or by means of Ls5 (in the  $\lambda^\vee_j$ -calculus). In any case, by paste there exists  $H$  such that  $\vdash [K/x]\sigma : H$  and  $H \vdash R : \phi$ . Then there exist  $\psi$  and  $G$  such that  $H = (x : \psi, G)$ , and  $\vdash [K/x]\sigma : H$  is inferred, by S2, from  $\vdash K : \psi$  and  $\vdash \sigma : G$ . By the lemma 5.12 we have  $\vdash K : \gamma$ . Then in the  $\lambda^\vee_j$ -calculus we have  $x : \psi \wedge \gamma, G \vdash R : \phi$  by weakening, therefore  $\vdash \langle \lambda^\vee x R, \sigma \rangle : \psi \wedge \gamma \rightarrow \phi$  since  $\psi \wedge \gamma \leq_\star \omega \rightarrow \omega$ . Since  $\vdash K : \psi \wedge \gamma$  by L2, we get  $\vdash M : \phi$  by L6. The proof is similar in the  $\lambda^\vee_j$ -calculus since we know by the remark 5.11 that there exists  $\zeta \in \Gamma$  such that  $\zeta \sim_\mathbf{s} \psi \wedge \gamma$ , therefore  $x : \zeta, G \vdash R : \phi$  and  $\vdash K : \zeta$ .

- the only remaining case is  $M = (M_0 \parallel M_1)P$  and  $N = (M_0 P \parallel M_1 P)$ . We may assume that  $\vdash N : \phi$  is proved using L7, that is  $\phi = \phi_0 \wedge \phi_1$  with  $\vdash M_i P : \phi_i$ . These sequents can be inferred by means of L1, L2, L3 or L6. By symmetry, we can restrict our investigations to the following cases:

••  $\vdash M_0P : \phi_0$  and  $\vdash M_1P : \phi_1$  are both proved by L1, i.e.  $\phi_i = \omega$ . Then  $\phi \sim \omega$ , therefore  $\vdash M : \phi$  by L1 and L3.

••  $\vdash M_0P : \phi_0$  is proved using L2, that is  $\phi_0 = \psi_0 \wedge \psi_1$  with  $\vdash M_0P : \psi_i$ . Then  $\vdash N : \psi_i \wedge \phi_1$  (by L7) with a proof shorter than the one of  $\vdash N : \phi$ , therefore by induction hypothesis  $\vdash M : \psi_i \wedge \phi_1$ , hence  $\vdash M : \phi$  by L2 and L3 since  $(\psi_0 \wedge \phi_1) \wedge (\psi_1 \wedge \phi_1) \sim \phi$ .

•• if  $\vdash M_0P : \phi_0$  is proved by means of L3, then there exist  $\psi \leq \phi_0$  such that  $\vdash M_0P : \psi$ . Then  $\vdash N : \psi \wedge \phi_1$  (by L7) with a proof shorter than the one of  $\vdash N : \phi$ , therefore by induction hypothesis  $\vdash M : \psi \wedge \phi_1$ , hence  $\vdash M : \phi$  by L3 since  $\psi \wedge \phi_1 \leq \phi$ .

•• if  $\vdash M_0P : \phi_0$  by L6, we have  $\vdash M_0 : \psi_0 \rightarrow \phi_0$  and  $\vdash P : \psi_0$  for some  $\psi_0$ . Note that  $\vdash (M_0 \parallel M_1) : \psi_0 \rightarrow \phi_0$  (see § 3.3.2), therefore  $\vdash M : \phi_0$  by L6. Here we only have two cases to take into consideration: if  $\vdash M_1P : \phi_1$  by L1, that is  $\phi_1 = \omega$ , then  $\vdash M : \phi$  by L3 since  $\phi = \phi_0 \wedge \omega \sim \phi_0$ . Otherwise we may assume that  $\vdash M_1P : \phi_1$  is inferred using L6, that is  $\vdash M_1 : \psi_1 \rightarrow \phi_1$  and  $\vdash P : \psi_1$  for some  $\psi_1$ . As above we have  $\vdash (M_0 \parallel M_1) : \psi_1 \rightarrow \phi_1$ , therefore  $\vdash M : \phi_1$  by L6, and  $\vdash M : \phi$  by L2  $\square$

We can now prove the convergence lemma for closed terms, as an easy consequence of the previous proposition:

**COROLLARY 5.14.** *If  $M$  is a closed term then  $M \Downarrow \Rightarrow \vdash M : \gamma$ .*

**PROOF:** if  $M \Downarrow$  then by definition there exists a closed partial normal form  $K$  such that  $M \Downarrow K$ . Then by the lemma 2.10 we have  $M \triangleright^* K$ , and  $\vdash K : \gamma$  by the lemma 5.12. It should be obvious, from the previous proposition, that  $N \triangleright^* R \ \& \ \vdash R : \phi \Rightarrow \vdash N : \phi$ , therefore  $\vdash M : \gamma$   $\square$

### 5.3 Characteristic Terms.

To establish our last result, that is the characterization lemma, it will be convenient to use a restricted natural deduction system which, although incomplete, allows us to prove the “essential” properties (i.e. formulae) of the terms. This restricted logical system is quite close to the original Coppo’s system [10,11]. The sequents in this system will be denoted  $H \Vdash M : \phi$ , though the restriction actually concerns the formulae. To see what are the special formulae we use, let us define inductively the *decomposition* relation  $\phi \triangleright \psi$  between formulae of  $\Phi_*$  or  $\Phi_S$ , as follows:

- (i)  $\omega \triangleright \omega$  and  $\gamma \triangleright \gamma$
- (ii)  $\phi \triangleright \pi \Rightarrow \begin{cases} \phi \wedge \psi \triangleright \pi \\ \psi \wedge \phi \triangleright \pi \\ \psi \rightarrow \phi \triangleright \psi \rightarrow \pi \end{cases}$

**REMARK 5.15.**  $\phi \triangleright \psi \Rightarrow \phi \leq \psi$

**DEFINITION (IRREDUCIBLE FORMULAE).** *A formula  $\phi$  is irreducible if  $\phi \triangleright \pi \Rightarrow \pi = \phi$ .*

We shall denote by  $\Pi_*$  and  $\Pi_S$  the sets of irreducible formulae. Clearly these sets are given by the grammars:

$$(\Pi_*) \quad \pi ::= \omega \mid (\phi \rightarrow \pi)$$

where  $\phi$  is any formula of  $\Phi_*$ , and

$$(\Pi_S) \quad \pi ::= \omega \mid \gamma \mid (\zeta \rightarrow \pi)$$

where  $\zeta$  is any formula of  $\Gamma$ . In what follows we shall mostly use the symbol  $\Pi$ , without subscript, for the set of irreducible formulae. An obvious observation is that if  $\phi \triangleright \psi$  then  $\psi$  is an irreducible

formula. Let us see that any formula is equivalent to a conjunction of irreducible ones – recall that:

$$\phi \sim \psi \Leftrightarrow \phi \leq \psi \ \& \ \psi \leq \phi$$

**LEMMA 5.16.** *For any  $\phi$  the set  $\phi^* = \{\pi \mid \phi \triangleright \pi\}$  is non-empty and finite. Moreover  $\phi \sim \bigwedge \{\pi \mid \phi \triangleright \pi\}$ .*

**PROOF** (sketch): by induction on the definition of  $\phi \triangleright \pi$ , trivial. Note that  $(\phi \wedge \psi)^* = \phi^* \cup \psi^*$ . For the case  $\psi \rightarrow \phi$  one uses the equivalence  $(\psi \rightarrow \bigwedge_{1 \leq i \leq n} \phi_i) \sim \bigwedge_{1 \leq i \leq n} (\psi \rightarrow \phi_i)$   $\square$

A consequence of this fact is that any irreducible formula (distinct from  $\omega$  and  $\gamma$ ) can be written, up to  $\sim$ , as  $\pi_1 \wedge \dots \wedge \pi_k \rightarrow \pi$  where  $\pi$  and the  $\pi_i$ 's are irreducible.

Now we study the entailment relation  $\phi \leq \psi$  by means of irreducible formulae (cf. Barendregt & al. [6], Hindley 82[20], Abramsky 88[3]). Let  $\ll_*$  and  $\ll_s$  be the least relations on  $\Pi_*$  and  $\Pi_s$  satisfying

$$\boxed{\text{F1: } \phi \ll_* \omega \quad \text{F2: } \frac{\pi_0 \ll_* \pi, \pi \ll_* \pi_1}{\pi_0 \ll_* \pi_1} \quad \text{F3: } \pi \ll_* \pi}$$

and, for the first one:

$$\boxed{\text{F}_{*4}: (\phi \rightarrow \omega) \ll_* (\omega \rightarrow \omega) \quad \text{F}_{*5}: \frac{\phi_0 \geq_* \phi_1, \pi_0 \ll_* \pi_1}{(\phi_0 \rightarrow \pi_0) \ll_* (\phi_1 \rightarrow \pi_1)}}$$

while in the strict case:

$$\boxed{\text{Fs4.1: } (\zeta \rightarrow \pi) \ll_s \gamma \quad \text{Fs4.2: } \gamma \ll_s (\gamma \rightarrow \omega)}$$

$$\boxed{\text{Fs5: } \frac{\zeta_0 \geq_s \zeta_1, \pi_0 \ll_s \pi_1}{(\zeta_0 \rightarrow \pi_0) \ll_s (\zeta_1 \rightarrow \pi_1)}}$$

**LEMMA 5.17.**  $\phi \leq \psi \Leftrightarrow \forall \psi' (\psi \triangleright \psi' \Rightarrow \exists \phi' (\phi \triangleright \phi' \ \& \ \phi' \ll \psi'))$

**PROOF** (sketch): the “ $\Leftarrow$ ” part is clear from the previous lemma. The converse implication is easily established by induction on the definition of  $\phi \leq \psi$ . For the cases of Es5.1 and Es5.2 one remarks that if  $\zeta \in \Gamma$  and  $\zeta \triangleright \pi$  then  $\pi = \gamma$  or  $\pi = (\zeta' \rightarrow \pi')$  with  $\zeta' \in \Gamma$  and  $\pi' \in \Pi_s$   $\square$

We could have written this property as:

$$\phi \leq \psi \Leftrightarrow \forall \psi' \in \psi^* \exists \phi' \in \phi^*. \phi' \ll \psi'$$

Let us see some consequences of this characterization of the entailment relation. For instance the reader could show that the irreducible formulae represent the compact prime filters:

**LEMMA.** *A filter  $F$  is compact prime if and only if there exists an irreducible formula  $\pi \in \Pi$  such that  $F = \pi \uparrow$ .*

Then the previous lemma is just a reformulation of the fact that the canonical domains are also powerdomains, see § 4.1.1. We can also characterize the formulae generating the least element of the domain:

**DEFINITION (TRIVIAL FORMULAE).** *A formula  $\phi$  is trivial if  $\phi \sim \omega$ .*

Clearly  $\phi$  is trivial if and only if  $\omega \leq \phi$ . Then  $\phi \wedge \psi$  is trivial if and only if both  $\phi$  and  $\psi$  are trivial.

LEMMA 5.18.

$$(i) \phi \sim \omega \Leftrightarrow \phi^* = \{\omega\}$$

$$(ii) \phi \not\sim \omega \Leftrightarrow \phi \leq \gamma \text{ and, in the strict case } (\zeta \rightarrow \phi) \sim_s \gamma \Leftrightarrow \phi \sim_s \omega.$$

PROOF:

(i) if  $\phi \sim \omega$  then  $\omega \leq \phi$  and by the previous lemma there exists  $\pi \in \phi^*$  such that  $\omega \ll \pi$ . It is easy to see, by induction on the definition of  $\ll$ , that  $\omega \ll \pi \Leftrightarrow \pi = \omega$ . Therefore  $\phi^* = \{\omega\}$ .

(ii) since  $\gamma^* = \{\gamma\}$ , the formula  $\gamma$  is non-trivial, by the previous point, and clearly  $\phi \leq \psi \not\sim \omega \Rightarrow \phi \not\sim \omega$ . Conversely if  $\phi \not\sim \omega$  then by the previous lemma there exists  $\pi \in \phi^*$  such that  $\omega \not\ll \pi$ . It is obvious that this implies  $\pi = \phi \rightarrow \tau$  since  $\pi$  is irreducible, or in the strict case  $\pi = \gamma$  or  $\pi = \zeta \rightarrow \tau$ , hence  $\pi \leq \gamma$  by E1, E<sub>\*</sub>7 and E<sub>\*</sub>5, or by Es5.1. Then  $\phi \leq \gamma$  since  $\phi \leq \pi$  (remark 5.15). The last point is left to the reader  $\square$

Now we introduce the restricted logical systems, which essentially consist in disallowing L2 and L3, and in proving only irreducible assertions about the terms. The two restricted systems share the following rules:

$$T1: H \Vdash M : \omega \quad T2: \frac{}{x : \phi, H \Vdash x : \psi} \phi \triangleright \psi$$

$$T4: \frac{H \Vdash M : (\phi \rightarrow \psi), H \Vdash N : \phi_i \quad (1 \leq i \leq k)}{H \Vdash (MN) : \psi} \phi_1 \wedge \dots \wedge \phi_k \leq \phi$$

$$T5.1: \frac{H \Vdash M : \phi}{H \Vdash (M \parallel N) : \phi} \quad T5.2: \frac{H \Vdash N : \psi}{H \Vdash (M \parallel N) : \psi}$$

The rules for closures are the same as L5.1, L5.2 and Ls5:

$$T3.1: \frac{x : \psi, G \Vdash_* M : \phi, H \vdash_* \sigma : G}{H \Vdash_* \langle \lambda x M, \sigma \rangle : (\psi \rightarrow \phi)}$$

$$T3.2: \frac{x : \psi, G \Vdash_* M : \phi, H \vdash_* \sigma : G}{H \Vdash_* \langle \lambda^v x M, \sigma \rangle : (\psi \rightarrow \phi)} \psi \leq_* (\omega \rightarrow \omega)$$

$$Ts3: \frac{x : \zeta, G \Vdash_s M : \phi, H \vdash_s \sigma : G}{H \Vdash_s \langle \lambda^v x M, \sigma \rangle : (\zeta \rightarrow \phi)}$$

It is easily checked, by induction on the inference of the sequents, that:

REMARK. If  $H \Vdash M : \phi$  then  $\phi$  is an irreducible formula.

REMARK 5.19.  $x : \phi, H \Vdash x : \psi \Rightarrow \phi \leq \psi$

Now we relate the logical systems, showing first that the sequents provable in the restricted systems are also provable in the full logical systems, and that the restricted assertions that can be made about a term generate the filter of all possible properties of this term.

**PROPOSITION 5.20.**

- (i)  $H \Vdash M : \phi \Rightarrow H \vdash M : \phi$
- (ii)  $H \vdash M : \phi \Rightarrow \exists \pi_1, \dots, \pi_n \in \Pi. \pi_1 \wedge \dots \wedge \pi_n \leq \phi \ \& \ \forall i. H \Vdash M : \pi_i$

**PROOF:** one easily proves the first point by induction on the inference of the sequent  $H \Vdash M : \phi$ , using the remark 5.19 above. Let us just check the case of T4: we have  $H \Vdash P : \phi \rightarrow \psi$  and  $H \Vdash Q : \phi_i$  with  $\phi_1 \wedge \dots \wedge \phi_k \leq \phi$ . Then by induction hypothesis  $H \vdash P : \phi \rightarrow \psi$  and  $H \vdash Q : \phi_i$ , therefore  $H \vdash Q : \phi$  by L2 and L3, hence  $H \vdash (PQ) : \psi$  by L6.

Now we prove the second point by induction on the inference of the sequent  $H \vdash M : \phi$ . This is trivial for L1, L2, L3 (using the induction hypothesis) and L4 (using the lemma 5.16).

• for L5.1 we have  $\phi = \xi \rightarrow \tau$  and  $M = \langle \lambda x R, \sigma \rangle$ , with  $x : \xi, G \vdash_\star R : \tau$  and  $H \vdash_\star \sigma : G$ . Then by induction hypothesis there exist  $\tau_1, \dots, \tau_n$  such that  $\tau_1 \wedge \dots \wedge \tau_n \leq \tau$  and  $x : \xi, G \vdash_\star R : \tau_i$ . We let  $\pi_i = \xi \rightarrow \tau_i$ ; these are irreducible formulae, since the  $\tau_i$ 's are irreducible. By T3.1 we have  $H \Vdash_\star M : \pi_i$  for all  $i$ , and

$$\pi_1 \wedge \dots \wedge \pi_n \sim (\xi \rightarrow \bigwedge_{1 \leq i \leq n} \tau_i) \leq \xi \rightarrow \tau$$

The proof is the same for L5.2 and L5.5.

• for L6 we have  $M = (PQ)$  with  $H \vdash P : \psi \rightarrow \phi$  and  $H \vdash Q : \psi$ . We may assume  $\phi \neq \omega$ , since  $H \Vdash M : \omega$  can be proved by means of T1. Then if we let  $\{\phi_1, \dots, \phi_n\} = \{\phi' \mid \phi' \neq \omega \ \& \ \phi \triangleright \phi'\}$  we have  $\phi \sim \phi_1 \wedge \dots \wedge \phi_n$ . By induction hypothesis there exist  $\tau_1, \dots, \tau_k$  such that  $\tau_1 \wedge \dots \wedge \tau_k \leq \psi \rightarrow \phi$  and  $H \Vdash P : \tau_i$ . By the lemma 5.17 for any  $j$  ( $1 \leq j \leq n$ ) there exists  $i_j$  such that  $\tau_{i_j} \ll \psi \rightarrow \phi_j$ . Since this can only be proved by means of F2, F3, and F<sub>5</sub> or F<sub>5</sub>, we clearly have  $\tau_{i_j} = \psi_j \rightarrow \pi_j$  with  $\psi_j \geq \psi$  and  $\pi_j \ll \phi_j$ , therefore  $\pi_1 \wedge \dots \wedge \pi_n \leq \phi$ . By induction hypothesis on  $H \vdash Q : \psi$  there exist  $\xi_1, \dots, \xi_m$  such that  $\xi_1 \wedge \dots \wedge \xi_m \leq \psi$  and  $H \Vdash Q : \xi_h$ . Then  $\xi_1 \wedge \dots \wedge \xi_m \leq \psi_j$  for any  $j$ , therefore  $H \Vdash M : \pi_j$  for any  $j$ , by T4.

The case of L7 is trivial (using the induction hypothesis)  $\square$

Let us now introduce the characteristic terms and show that they satisfy their specification. We define for each formula  $\phi \in \Phi_\star$ , and respectively in the strict case for each  $\phi \in \Phi_s$  and  $\zeta \in \Gamma$ , a pair of closed  $\lambda_j^\star$ -terms (resp.  $\lambda_j^s$ -terms)  $\mathbf{M}_\phi$  and  $\mathbf{T}_\phi$  (resp.  $\mathbf{M}_\phi^s$  and  $\mathbf{T}_\zeta^s$ ) such that:

- (i)  $\vdash_\star \mathbf{M}_\phi : \phi$
  - (ii)  $\vdash_\star \mathbf{T}_\phi : \phi \rightarrow (\psi \rightarrow \psi)$  for any  $\psi \in \Phi_\star$
- and
- (iii)  $\vdash_s \mathbf{M}_\phi^s : \phi$
  - (iv)  $\vdash_s \mathbf{T}_\zeta^s : \zeta \rightarrow (\psi \rightarrow \psi)$  for any  $\psi \in \Gamma$ .

We define these terms inductively, checking the required properties:

$$\begin{aligned} \mathbf{M}_\omega &= \Omega \\ \mathbf{M}_\omega^s &= \Omega_s \\ \mathbf{T}_\omega &= \mathbf{F} = \lambda y \lambda x x \end{aligned}$$

Clearly  $\vdash \mathbf{M}_\omega : \omega$  by L1, and similarly for  $\mathbf{M}_\omega^s$ . To show that  $\vdash \mathbf{F} : \omega \rightarrow (\psi \rightarrow \psi)$  is an easy exercise,

$$\begin{aligned}\mathbf{M}_\gamma^s &= \lambda^v x \Omega_s \\ \mathbf{T}_\gamma^s &= \lambda^v y \lambda^v x x\end{aligned}$$

We have  $x : \gamma \vdash \Omega_s : \omega$  by L1, therefore  $\vdash \mathbf{M}_\gamma^s : \gamma \rightarrow \omega$  by Ls5 (recall that  $\lambda^v x \Omega_s$  is an abbreviation for  $\langle \lambda^v x \Omega_s, \varepsilon \rangle$ , and that  $H \vdash \varepsilon : H$  by S1). Then  $\vdash \mathbf{M}_\gamma^s : \gamma$  by L3 since  $\gamma \rightarrow \omega \leq \gamma$  by Es5.1. It is easy to see, using Ls5 twice, that  $\vdash \mathbf{T}_\gamma^s : \gamma \rightarrow (\psi \rightarrow \psi)$ .

$$\begin{aligned}\mathbf{M}_{\phi \wedge \psi} &= (\mathbf{M}_\phi \parallel \mathbf{M}_\psi) \\ \mathbf{T}_{\phi \wedge \psi} &= \lambda x (\mathbf{T}_\phi x) (\mathbf{T}_\psi x)\end{aligned}$$

By induction hypothesis we have  $\vdash \mathbf{M}_\phi : \phi$  and  $\vdash \mathbf{M}_\psi : \psi$ , therefore by L7:

$$\vdash (\mathbf{M}_\phi \parallel \mathbf{M}_\psi) : \phi \wedge \psi$$

as required. By induction hypothesis, for any  $\tau$  we have  $\vdash \mathbf{T}_\phi : \phi \rightarrow (\tau \rightarrow \tau)$ , hence by weakening

$$x : \phi \wedge \psi \vdash \mathbf{T}_\phi : \phi \rightarrow (\tau \rightarrow \tau)$$

Moreover by L4 and L3:  $x : \phi \wedge \psi \vdash x : \phi$ . Then using L6:

$$x : \phi \wedge \psi \vdash \mathbf{T}_\phi x : \tau \rightarrow \tau$$

Similarly we have  $x : \phi \wedge \psi \vdash \mathbf{T}_\psi x : \xi \rightarrow \xi$ . Let  $\tau = (\xi \rightarrow \xi)$ ; then by L6:

$$x : \phi \wedge \psi \vdash (\mathbf{T}_\phi x) (\mathbf{T}_\psi x) : \xi \rightarrow \xi$$

and finally  $\vdash \lambda x (\mathbf{T}_\phi x) (\mathbf{T}_\psi x) : (\phi \wedge \psi) \rightarrow (\xi \rightarrow \xi)$  by L5.1, that is the required property of  $\mathbf{T}_{\phi \wedge \psi}$ . The proofs are entirely similar for:

$$\begin{aligned}\mathbf{M}_{\phi \wedge \psi}^s &= (\mathbf{M}_\phi^s \parallel \mathbf{M}_\psi^s) \\ \mathbf{T}_{\zeta \wedge \tau}^s &= \lambda^v x (\mathbf{T}_\zeta^s x) (\mathbf{T}_\tau^s x)\end{aligned}$$

The last case of the definition of the characteristic terms concerns implicative formulae:

$$\begin{aligned}\mathbf{M}_{\phi \rightarrow \psi} &= \lambda x (\mathbf{T}_\phi x) \mathbf{M}_\psi \\ \mathbf{T}_{\phi \rightarrow \psi} &= \lambda^v x (\mathbf{T}_\psi (x \mathbf{M}_\phi))\end{aligned}$$

By induction hypothesis  $x : \phi \vdash \mathbf{M}_\psi : \psi$ . As we saw above

$$x : \phi \vdash \mathbf{T}_\phi x : \psi \rightarrow \psi$$

Then by L6:

$$x : \phi \vdash (\mathbf{T}_\phi x) \mathbf{M}_\psi : \psi$$

and by L5.1 we get the required property of  $\mathbf{M}_{\phi \rightarrow \psi}$ , namely:

$$\vdash \lambda x (\mathbf{T}_\phi x) \mathbf{M}_\psi : \phi \rightarrow \psi$$



By induction hypothesis  $\vdash \mathbf{M}_\phi : \phi$  therefore by L4 and L6 (and weakening):

$$x : \phi \rightarrow \psi \vdash (x\mathbf{M}_\phi) : \psi$$

Using the induction hypothesis on  $\mathbf{T}_\psi$  we have, by weakening and L6:

$$x : \phi \rightarrow \psi \vdash \mathbf{T}_\psi(x\mathbf{M}_\phi) : \xi \rightarrow \xi$$

Since  $\phi \rightarrow \psi \leq_* \omega \rightarrow \omega$  by E<sub>\*</sub>7 and E<sub>\*</sub>5, we get :

$$\vdash \lambda^v x (\mathbf{T}_\psi(x\mathbf{M}_\phi)) : (\phi \rightarrow \psi) \rightarrow (\xi \rightarrow \xi)$$

by L5.2. For what regards the strict calculus, we define:

$$\begin{aligned} \mathbf{M}_{\zeta \rightarrow \phi}^s &= \lambda^v x (\mathbf{T}_\zeta^s x) \mathbf{M}_\phi^s \\ \mathbf{T}_{\zeta \rightarrow \phi}^s &= \begin{cases} \mathbf{T}_\gamma^s & \text{if } \phi \in \Phi_s - \Gamma \\ \lambda^v x \mathbf{T}_\phi^s(x\mathbf{M}_\zeta^s) & \text{otherwise} \end{cases} \end{aligned}$$

The proof that  $\vdash \mathbf{M}_{\zeta \rightarrow \phi}^s : \zeta \rightarrow \phi$  proceeds exactly as for  $\mathbf{M}_{\phi \rightarrow \psi}$ . If  $\phi \in \Phi_s - \Gamma$  then  $\phi \sim \omega$ , therefore  $\zeta \rightarrow \phi \sim \gamma$ . We saw that  $\vdash \mathbf{T}_\gamma^s : \gamma \rightarrow (\psi \rightarrow \psi)$ , hence in this case  $\vdash \mathbf{T}_{\zeta \rightarrow \phi}^s : \gamma \rightarrow (\psi \rightarrow \psi)$  by L3. Otherwise, that is if  $\phi \in \Gamma$ , we proceed as for  $\mathbf{T}_{\phi \rightarrow \psi}$ .

PROPOSITION 5.21.

- (i)  $H \Vdash_* \mathbf{M}_\phi : \psi \Rightarrow \phi \leq_* \psi$  and  $H \Vdash_s \mathbf{M}_\phi^s : \psi \Rightarrow \phi \leq_s \psi$
- (ii)  $H \Vdash_* \mathbf{T}_\phi : \psi \rightarrow (\zeta \rightarrow \tau) \Rightarrow \phi \geq_* \psi \ \& \ \zeta \leq_* \tau$  and  
 $H \Vdash_s \mathbf{T}_\phi^s : \psi \rightarrow (\zeta \rightarrow \tau) \Rightarrow \phi \geq_s \psi \ \& \ \zeta \leq_s \tau$

PROOF: by induction on the formula  $\phi$ . Clearly we may assume that the sequents  $H \Vdash_* \mathbf{M}_\phi : \psi$  and  $H \Vdash_s \mathbf{M}_\phi^s : \psi$  are not proved by means of T1, since in this case  $\psi = \omega$ , and obviously  $\phi \leq \omega$  by E1.

- assume that  $H \Vdash_* \mathbf{M}_\omega : \psi$ , that is  $H \Vdash_* \Omega : \psi$ , with  $\psi \not\leq_* \omega$ . Then we would have by the lemma 5.18,  $\psi \leq_* \gamma$ , hence  $H \vdash_* \Omega : \gamma$  by the proposition 5.30 and L3. But then by soundness we would have  $\models_* \Omega : \gamma$ , and this is impossible since  $\Omega \uparrow$ . Therefore  $H \Vdash_* \mathbf{M}_\omega : \psi \Rightarrow \omega \leq_* \psi$ . The proof is the same for  $\mathbf{M}_\omega^s$ .

- the sequent  $H \Vdash_* \mathbf{T}_\omega : \psi \rightarrow (\zeta \rightarrow \tau)$  can only be proved by means of T3.1, that is

$$x : \psi, G \Vdash_* \lambda y y : \zeta \rightarrow \tau$$

and  $H \leq_* G$  (recall that  $H \vdash \varepsilon : G$  can only be inferred using S1). To prove this sequent one must use T3.1, thus  $y : \zeta, F \Vdash_* y : \tau$  with  $(x : \psi, F) \leq_* F$ . Then by the remark 5.19 we have  $\zeta \leq_* \tau$ , and obviously  $\omega \geq_* \psi$ . The argument is the same for  $\mathbf{T}_\gamma^s$ . Note that if  $H \Vdash_s \mathbf{T}_\gamma^s : \psi \rightarrow (\zeta \rightarrow \tau)$  we have  $\psi \in \Gamma$ , therefore  $\gamma \geq_s \psi$ .

- the sequent  $H \Vdash_s \mathbf{M}_\gamma^s : \psi$  can only be proved using Ls5 (or T1), that is  $\psi = \zeta \rightarrow \tau$  with  $x : \zeta, G \Vdash_s \Omega_s : \tau$ . We have seen that this implies  $\tau \sim_s \omega$ , hence  $\psi \sim_s \gamma$  by the lemma 5.18.

- the sequent  $H \Vdash_* (\mathbf{M}_\phi \parallel \mathbf{M}_\psi) : \tau$  is proved using T5.1 or T5.2 (or T1). In this last case for instance  $\psi \leq_* \tau$  by induction hypothesis, therefore  $\phi \wedge \psi \leq_* \tau$  by E3.3 and E2. For T5.1 one uses E3.2. The proof is the same for  $H \Vdash_s (\mathbf{M}_\phi^s \parallel \mathbf{M}_\psi^s) : \tau$ .

• the sequent  $H \Vdash_{\star} \mathbf{T}_{\phi \wedge \psi} : \delta \rightarrow (\zeta \rightarrow \tau)$  is proved by means of T3.1, thus

$$x : \delta, G \Vdash_{\star} (\mathbf{T}_{\phi} x)(\mathbf{T}_{\psi} x) : \zeta \rightarrow \tau$$

with  $H \leq_{\star} G$ . Since this one must be proved using T4, there exist  $\nu$  and  $\nu_1, \dots, \nu_m$  such that  $\nu_1 \wedge \dots \wedge \nu_m \leq_{\star} \nu$  and

$$\begin{aligned} (1-i) \quad & x : \delta, G \Vdash_{\star} \mathbf{T}_{\psi} x : \nu_i \\ (2) \quad & x : \delta, G \Vdash_{\star} \mathbf{T}_{\phi} x : \nu \rightarrow (\zeta \rightarrow \tau) \end{aligned}$$

This second sequent is proved by T4, thus:

$$\begin{aligned} (3) \quad & x : \delta, G \Vdash_{\star} x : \mu_j \quad \text{with } \mu_1 \wedge \dots \wedge \mu_n \leq_{\star} \mu \\ (4) \quad & x : \delta, G \Vdash_{\star} \mathbf{T}_{\phi} : \mu \rightarrow (\nu \rightarrow (\zeta \rightarrow \tau)) \end{aligned}$$

Then  $\delta \leq_{\star} \mu$  by the remark 5.19. Moreover  $\mu \leq_{\star} \phi$  by induction hypothesis regarding (4), hence  $\delta \leq_{\star} \phi$  (recall that we have to show  $\phi \wedge \psi \geq_{\star} \delta$  and  $\zeta \leq_{\star} \tau$ ), and  $\nu \leq_{\star} \zeta \rightarrow \tau$  (induction hypothesis), hence  $\nu_1 \wedge \dots \wedge \nu_m \leq_{\star} \zeta \rightarrow \tau$ . Then, since each  $\nu_i$  is irreducible, as well as  $\tau$ , from the lemma 5.17  $\nu_i \ll_{\star} \zeta \rightarrow \tau$  for some  $i$ . It is easily seen that this implies  $\nu_i = \xi \rightarrow \pi$  with  $\xi \geq_{\star} \zeta$  and  $\pi \ll_{\star} \tau$ . Therefore the sequent (1-i) is proved using T4, that is:

$$\begin{aligned} x : \delta, G \Vdash_{\star} x : \eta_h \quad & \text{with } \eta_1 \wedge \dots \wedge \eta_r \leq \eta \\ x : \delta, G \Vdash_{\star} \mathbf{T}_{\psi} : \eta \rightarrow (\xi \rightarrow \pi) \end{aligned}$$

By induction hypothesis  $\eta \leq_{\star} \psi$ , and by the remark 5.19,  $\delta \leq_{\star} \eta_h$ , hence

$$\delta \leq_{\star} \eta_1 \wedge \dots \wedge \eta_r \leq_{\star} \eta \leq_{\star} \psi$$

and finally  $\delta \leq_{\star} \phi \wedge \psi$ . Moreover, by induction hypothesis  $\xi \leq_{\star} \pi$ , therefore  $\zeta \leq_{\star} \xi \leq_{\star} \pi \leq_{\star} \tau$ , that is  $\zeta \leq_{\star} \tau$ . The proof is the same in the strict case, i.e. for  $H \Vdash_{\mathbf{s}} \mathbf{T}_{\phi \wedge \psi} : \delta \rightarrow (\zeta \rightarrow \tau)$ .

• if  $H \Vdash_{\star} \mathbf{M}_{\phi \rightarrow \psi} : \zeta$ , then this sequent is proved by means of T3 (or T1), that is  $\zeta = \xi \rightarrow \tau$  with

$$x : \xi, G \Vdash_{\star} (\mathbf{T}_{\phi} x) \mathbf{M}_{\psi} : \tau$$

where  $H \leq_{\star} G$ . If this sequent is proved using T1 then  $\tau = \omega$  and we have  $\phi \rightarrow \psi \leq_{\star} \zeta$  since:

$$\phi \rightarrow \psi \leq_{\star} \phi \rightarrow \omega \leq_{\star} \omega \rightarrow \omega \leq_{\star} \xi \rightarrow \omega$$

Otherwise there exist  $\nu$  and  $\nu_1, \dots, \nu_m$  such that  $\nu_1 \wedge \dots \wedge \nu_m \leq \nu$  and

$$\begin{aligned} x : \xi, G \Vdash_{\star} \mathbf{M}_{\psi} : \nu_i \\ x : \xi, G \Vdash_{\star} \mathbf{T}_{\phi} x : \nu \rightarrow \tau \end{aligned}$$

By induction hypothesis  $\psi \leq_{\star} \nu_i$  for all  $i$ , therefore  $\psi \leq_{\star} \nu$ . The second sequent is proved by T4, thus:

$$\begin{aligned} x : \xi, G \Vdash_{\star} x : \mu_j \quad & \text{with } \mu_1 \wedge \dots \wedge \mu_n \leq \mu \\ x : \xi, G \Vdash_{\star} \mathbf{T}_{\phi} : \mu \rightarrow (\nu \rightarrow \tau) \end{aligned}$$

Then  $\xi \leq_* \mu_j$  by the remark 5.19, hence  $\xi \leq_* \mu$ . Moreover  $\mu \leq_* \phi$  and  $\nu \leq_* \tau$  by induction hypothesis, hence  $\xi \leq_* \phi$  and  $\psi \leq_* \tau$ , which implies  $\phi \rightarrow \psi \leq_* \xi \rightarrow \tau = \zeta$ . The proof is entirely similar in the strict case, that is for  $H \vdash_s \mathbf{M}_{\phi \rightarrow \psi}^s : \zeta$ . Note that if  $\zeta = \xi \rightarrow \tau$  with  $\tau = \omega$  then  $\phi \rightarrow \psi \leq_s \zeta$  by Es5.2 and Es7 (and Es5.1).

• the sequent  $H \vdash_* \mathbf{T}_{\phi \rightarrow \psi} : \theta \rightarrow (\zeta \rightarrow \tau)$  can only be inferred by means of T3.2, that is:

$$x : \theta, G \vdash_* \mathbf{T}_\psi(x\mathbf{M}_\phi) : \zeta \rightarrow \tau$$

with  $H \leq_* G$  and  $\theta \leq_* \gamma$ . Then this sequent is proved using T4, and there exist  $\nu$  and  $\nu_1, \dots, \nu_k$  such that  $\nu_1 \wedge \dots \wedge \nu_k \leq_* \nu$  and:

$$\begin{aligned} (1-i) \quad & x : \theta, G \vdash_* (x\mathbf{M}_\phi) : \nu_i \\ (2) \quad & x : \theta, G \vdash_* \mathbf{T}_\psi : \nu \rightarrow (\zeta \rightarrow \tau) \end{aligned}$$

By induction hypothesis on (2) we have  $\psi \geq_* \nu$  and  $\zeta \leq_* \tau$ . It remains to show  $\phi \rightarrow \psi \geq_* \theta$ . We distinguish two cases:

•• if  $\psi \sim \omega$  then  $\phi \rightarrow \psi \sim \gamma$  (lemma 5.18), and we saw that  $\theta \leq_* \gamma$  (this was the side condition associated with the use of T3.2 in proving  $H \vdash_* \mathbf{T}_{\phi \rightarrow \psi} : \theta \rightarrow (\zeta \rightarrow \tau)$ ).

•• otherwise we have  $\nu \not\sim_* \omega$ , therefore the set  $\{\delta_1, \dots, \delta_n\} = \{\nu_1, \dots, \nu_k\} - \{\omega\}$  is non-empty, and

$$\nu_1 \wedge \dots \wedge \nu_k \sim_* \delta_1 \wedge \dots \wedge \delta_n \leq_* \nu$$

The sequent

$$x : \theta, G \vdash_* (x\mathbf{M}_\phi) : \delta_j$$

can only be inferred by means of T4, therefore we have

$$\begin{aligned} & x : \theta, G \vdash_* x : \eta_j \rightarrow \delta_j \\ & x : \theta, G \vdash_* \mathbf{M}_\phi : \eta_i^j \quad \text{with} \quad \eta_1^j \wedge \dots \wedge \eta_m^j \leq_* \eta_j \end{aligned}$$

By induction hypothesis  $\phi \leq_* \eta_i^j$ , hence  $\phi \leq_* \eta_j$ . This implies  $\eta_j \rightarrow \delta_j \leq_* \phi \rightarrow \delta_j$ , therefore

$$\begin{aligned} \bigwedge_{1 \leq j \leq n} (\eta_j \rightarrow \delta_j) & \leq_* \bigwedge_{1 \leq j \leq n} (\phi \rightarrow \delta_j) \sim_* (\phi \rightarrow \bigwedge_{1 \leq j \leq n} \delta_j) \\ & \leq_* \phi \rightarrow \nu \leq_* \phi \rightarrow \psi \end{aligned}$$

By the remark 5.19 we have  $\theta \leq_* \eta_j \rightarrow \delta_j$  for any  $j$ , therefore  $\theta \leq_* \phi \rightarrow \psi$ .

The proof is the same for the strict case, that is  $H \vdash_s \mathbf{T}_{\phi \rightarrow \psi}^s : \theta \rightarrow (\zeta \rightarrow \tau)$ . Note that if  $\psi \sim_s \omega$  then  $\psi \in \Phi_s - \Gamma$  by the lemma 5.18; in this case  $\mathbf{T}_{\phi \rightarrow \psi}^s = \mathbf{T}_\gamma^s$ , and this was already treated  $\square$

Finally we can establish the characterization lemma:

**COROLLARY (CHARACTERIZATION LEMMA) 5.22.** *For any formula  $\phi$*

$$\vdash_* \mathbf{M}_\phi : \psi \Leftrightarrow \phi \leq_* \psi \quad \text{and} \quad \vdash_s \mathbf{M}_\phi^s : \psi \Leftrightarrow \phi \leq_s \psi$$

**PROOF:** we have seen that  $\vdash_* \mathbf{M}_\phi : \phi$ , therefore if  $\phi \leq_* \psi$  we have  $\vdash_* \mathbf{M}_\phi : \psi$  by L3. Conversely if  $\vdash_* \mathbf{M}_\phi : \psi$  then by the proposition 5.30 there exist  $\psi_1, \dots, \psi_k$  such that

$$\psi_1 \wedge \dots \wedge \psi_k \leq \psi \quad \text{and} \quad \forall i. \vdash_* \mathbf{M}_\phi : \psi_i$$

Then we have  $\phi \leq_* \psi_i$  for all  $i$  by the previous proposition, hence  $\phi \leq_* \psi$ . The proof is the same in the strict case  $\square$

## REFERENCES

- [1] M. ABADI, L. CARDELLI, P.-L. CURIEN, J.-J. LÉVY, *Explicit substitutions*, POPL 90 (1990) 31-46.
- [2] S. ABRAMSKY, *Domain theory in logical form*, LICS 87 (1987) 47-53.
- [3] S. ABRAMSKY, *The lazy lambda-calculus*, in *Research Topics in Functional Programming* (D. Turner, Ed.), Addison-Wesley (1989) 65-116.
- [4] S. ABRAMSKY, C.-H.L. ONG, *Full abstraction in the lazy lambda-calculus*, Research Report, Dept. of Computing, Imperial College (1989) to appear in *Information and Computation*.
- [5] H. BARENDREGT, *The Lambda Calculus*, Studies in Logic 103, North-Holland, Revised Edition (1984).
- [6] H. BARENDREGT, M. COPPO, M. DEZANI-CIANCAGLINI, *A filter lambda model and the completeness of type assignment*, J. of Symbolic Logic 48 (1983) 931-940.
- [7] G. BERRY, P.-L. CURIEN, J.-J. LÉVY, *Full abstraction for sequential languages: the state of the art*, in *Algebraic Methods in Semantics* (M. Nivat & J. C. Reynolds, Eds), Cambridge University Press (1985) 90-132.
- [8] B. BLOOM, J.G. RIECKE, *LCF should be lifted*, Conf. on Algebraic Methodology and Software Technology, University of Iowa (1989) 133-136.
- [9] B. BLOOM, *Can LCF be topped? Flat lattice models of typed lambda-calculus*, Information and Computation 87 (1990) 264-301.
- [10] M. COPPO, M. DEZANI-CIANCAGLINI, B. VENERI, *Functional characters of solvable terms*, Zeit. Math. Logik Grund. 27 (1981) 45-58.
- [11] M. COPPO, M. DEZANI-CIANCAGLINI, B. VENERI, *Principal type schemes and lambda-calculus semantics*, In *To H.B. Curry: Essays on Combinatory Logic, Lambda Calculus and Formalism* (J.R. Hindley and J.P. Seldin, Eds.), Academic Press (1980) 535-560.
- [12] M. COPPO, M. DEZANI-CIANCAGLINI, F. HONSELL, G. LONGO, *Extended type structures and filter lambda models*, Logic Colloquium 82, North-Holland (1984) 241-262.
- [13] M. COPPO, M. DEZANI-CIANCAGLINI, G. LONGO, *Applicative information systems*, CAAP 83, Lecture Notes in Comput. Sci. 159 (1983) 35-64.
- [14] M. COPPO, *Completeness of type assignment in continuous lambda models*, Theoretical Comput. Sci. 29 (1984) 309-324.
- [15] S. COSMADAKIS, A.R. MEYER, J.G. RIECKE, *Completeness for typed lazy inequalities*, LICS 90 (1990) 312-320.
- [16] P.-L. CURIEN, *Categorical Combinators, Sequential Algorithms and Functional Programming*, Research Notes in Theoretical Computer Science, Pitman, Wiley (1986).
- [17] M. DEZANI-CIANCAGLINI, I. MARGARIA, *A characterization of F-complete type assignments*, Theoretical Comput. Sci. 45 (1986) 121-157.
- [18] DORAI SITARAM, M. FELLEISEN, *Reasoning with continuations II: full abstraction for models of control*, 1990 ACM Conf. on Lisp and Functional Programming (1990) 161-175.
- [19] R. HINDLEY, *The completeness theorem for typing  $\lambda$ -terms*, Theoretical Comput. Sci. 22

(1983) 1-17 and 127-133.

- [20] R. HINDLEY, *The simple semantics for Coppo-Dezani-Sallé types*, Intern. Symp. on Programming, Lecture Notes in Comput. Sci. 137 (1982) 212-226.
- [21] J.-L. KRIVINE, *Lambda-Calcul: Types et Modèles*, Masson, Paris (1990).
- [22] K.G. LARSEN, G. WINSKEL, *Using information systems to solve recursive domain equations effectively*, Semantics of Data Types, Lecture Notes in Comput. Sci. 173 (1984) 109-130.
- [23] D. LEIVANT, *Typing and computational properties of lambda expressions*, Theoretical Comput. Sci. 44 (1986) 51-68.
- [24] J.-J. LÉVY, *An algebraic interpretation of the  $\lambda\beta K$ -calculus; and an application of a labelled  $\lambda$ -calculus*, Theoretical Comput. Sci. 2 (1976) 97-114.
- [25] G. LONGO, *Set-theoretical models of  $\lambda$ -calculus: theories, expansions, isomorphisms*, Annals of Pure and Applied Logic 24 (1983) 153-188.
- [26] A.R. MEYER, *Semantical paradigms*, LICS 88 (1988) 236-253.
- [27] R. MILNER, *Processes: a mathematical model of computing agents*, Logic Colloquium 73, North-Holland (1973) 157-173.
- [28] R. MILNER, *Fully abstract models of typed  $\lambda$ -calculi*, Theoretical Comput. Sci. 4 (1977) 1-22.
- [29] E. MOGGI, *Categories of partial morphisms and the  $\lambda_P$ -calculus*, Lecture Notes in Comput. Sci. 240 (1986) 242-251.
- [30] E. MOGGI, *Computational  $\lambda$ -calculus and monads*, LICS 89 (1989) 14-23.
- [31] M. NIELSEN, G. PLOTKIN, G. WINSKEL, *Petri nets, event structures and domains*, Theoret. Comput. Sci. 13 (1981) 85-108.
- [32] C.-H.L. ONG, *The Lazy Lambda-Calculus: an Investigation into the Foundations of Functional Programming*, PhD Thesis, Dept. of Computing, Imperial College (1988).
- [33] C.-H.L. ONG, *Fully abstract models of the lazy lambda calculus*, 29<sup>th</sup> FOCS (1988) 368-376.
- [34] G. PLOTKIN, *Call-by-name, call-by-value and the  $\lambda$ -calculus*, Theoret. Comput. Sci. 1 (1975) 125-159.
- [35] G. PLOTKIN, *LCF considered as a programming language*, Theoretical Comput. Sci. 5 (1977) 223-256.
- [36] G. PLOTKIN,  *$T^\omega$  as a universal domain*, J. of Computer and System Sciences 17 (1978) 209-236.
- [37] G. PLOTKIN, *Types and partial functions. A metalanguage. (Towards a) logic for computable functions*, manuscript, CSLI Summer School Notes (1985).
- [38] J.G. RIECKE, *A complete and decidable proof system for call-by-value equalities*, ICALP 90, Lecture Notes in Comput. Sci. 443 (1990) 20-31.
- [39] D. SCOTT, *Outline of a mathematical theory of computation*, 4<sup>th</sup> Ann. Princeton Conf. on Information Sciences and Systems, Princeton University (1970) 169-176.
- [40] D. SCOTT, *Data types as lattices*, SIAM J. Comput. 5 (1976) 522-587.
- [41] D. SCOTT, *Identity and existence in intuitionistic logic*, in Application of Sheaves, Lecture

Notes in Mathematics 753 (1979) 660-696.

- [42] D. SCOTT, *Lambda-calculus: some models, some philosophy*, The Kleene Symposium, North-Holland (1980) 223-265.
- [43] D. SCOTT, *Domains for denotational semantics*, ICALP 82, Lecture Notes in Comput. Sci. 140 (1982) 577-613.
- [44] A. STOUGHTON, *Fully Abstract Models of Programming Languages*, Research Notes in Theoretical Computer Science, Pitman, Wiley (1988).
- [45] C. WADSWORTH, *The relation between computational and denotational properties for Scott  $D_\infty$ -models of the lambda-calculus*, SIAM J. Comput. 5 (1976) 488-521.

Imprimé en France  
par  
l'Institut National de Recherche en Informatique et en Automatique



**ISSN 0249 - 6399**