Translating types and effects with state monads and linear logic

Paolo Tranquilli

To cite this version:

Paolo Tranquilli. Translating types and effects with state monads and linear logic. 2010. hal-00465793

HAL Id: hal-00465793
https://hal.science/hal-00465793
Preprint submitted on 21 Mar 2010

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 destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Translating Types and Effects with State Monads and Linear Logic

Paolo Tranquilli
LIP, ENS Lyon, Université de Lyon (UMR 5668 CNRS ENS Lyon UCBL INRIA)
Email: paolo.tranquilli@ens-lyon.fr

Abstract—We study a lambda-calculus with references and a types and effects system. In the first part of the paper, we translate it into the ordinary lambda-calculus with products, implementing an interacting family of state monads localized at sets of regions. In general the target language must be endowed with recursive types. However we prove that the stratification condition on regions, already used in type and effect systems to assure termination, is equivalent to completely avoid the use of recursion in the types used in the translation. We thus obtain a logical characterization of stratification, and by simulation we also provide a new proof that it yields termination. In the second part of the paper we extend the call-by-value translation of ordinary lambda-terms in linear logic proof nets to the calculus with references. This allows for a parallel evaluation of the calculus that preserves its sequential semantics.

I. INTRODUCTION

Mainstream programming paradigms are pervaded with side effects. The great majority of programs do not simply calculate a function, but carry out a whole lot of other actions that may influence the result: interacting with the user or with other processes, jumping to particular parts of its code, accessing memory,… There is a lot of research in computer science that goes towards controlling such side effects. Indeed programs that make large, uncontrolled use of side effects are harder to understand, verify or optimize.

Among the abstract tools that have been developed to this end and that are of interest to this work are types and effects systems [1] and monads [2]. The objective of the former is to analyze statically side effects by annotating in some way the ordinary types of programs. A typical way to analyze memory access is abstract memory into different entities called regions; then one decorates types with the set of regions which the typed program can access, possibly specifying what kind of access it needs. The annotated types become then informative on what and where can something happen when calling the function. A suitable level of abstraction from the actual workings of memory management allow to carry out a static analysis. For example such an approach has been successfully used to analyze the problem of heap memory deallocation ([3], leading to the so-called region based memory management).

Monads are a tool directly coming from category theory which envisages to encapsulate and abstract away the details of side effects while remaining in a “clean” typed world. The idea is that a monad T can be seen as a type constructor modeling a computational paradigm where (effect-less) values of type A are separated from computations of type T(A). All the details are left to the monad’s unit A → T(A), embedding values into computations, and its multiplication T^2(A) → T(A), determining how computations should compose, possibly interacting with one another. Since their inception they made it to be a highlight of Haskell’s type system and way of programming.

Both approaches rely on a common ground: types as a tool to study and/or discipline programs. To this end when it comes to memory access, the typical result is either allowing effective parallelization (like in the original type and effect proposal [1]), or ensure type safety (e.g. no “wrong” data occurs during execution), or allow timely memory deallocation as already mentioned. However there is another property that in general type systems have been studied to deliver: termination, i.e. a certificate that the program will eventually yield a result.

Until recently this particular aspect has not been much studied in the presence of side effects involving memory access, especially when higher order types are possibly referenced. Indeed it was long known [4] that apart from the classical way of obtaining a (diverging) fix-point operator through self application, which is easily forbidden by types, such a term can be encoded through well-typed self reference. Using the syntax we will show in Figure 1, a diverging term can be easily written following this idea:

$$\nu r \leftarrow \lambda x. \text{get}(r) x \cdot \text{get}(r) () .$$

Such a term can be read as “store in the location r the higher order function that reads from r what it should do, then apply it". Indeed, marking as $F = \lambda x. \text{get}(r)x$ the execution yields

$$\nu r \leftarrow F \cdot \text{get}(r) () \rightarrow \epsilon r \cdot \text{get}(r) () , r \leftarrow F$$

$$\rightarrow \epsilon r \cdot F (), r \leftarrow F \\rightarrow \epsilon r \cdot \text{get}(r) () , r \leftarrow F \rightarrow \cdots$$

r \leftarrow F is detached in a store accessible from the term. The $\epsilon r$ is a feature of our syntax which acts as a place-holder to garbage-collect values of the store once computation has ended (more details in section II). Returning to the self-referencing, divergent term, we can set r to hold functions of type 1 → 1, and the resulting term will be typed as 1. We may get a hint as to why the program loops (but a priori no solution) by annotating types and seeing that in fact r stores functions 1 \( \xrightarrow{1} r \), 1: the set added to the arrow indicates that functions stored in r may access r, so circularity may ensue.

Recent works explored the idea of stratification of regions to avoid such circularities [5], [6] and yield termination not only for sequential but also for cooperative
multithreading programs. The idea is that one must follow a precise order when assigning types to regions, which induces an ordering on regions so that, intuitively, a region may affect or read only regions that are strictly smaller. This has a distinct logical scent to it: even more so when one see their proof technique, which they carry via reducibility candidates.

In this work we set out to study types and effects from the logical point of view, and stratification together with them. We first chose the viewpoint of Girard’s linear logic (LL) [7], which has already been employed in the study of \( \lambda \)-calculus. One of the theoretical notions in LL’s toolbox are two translations of intuitionistic logic into LL (also first described in [7]). These two mappings are based on two different encodings of the intuitionistic arrow \( A \rightarrow B \) (corresponding via the Curry-Howard proofs-as-program paradigm to the type of functions from \( A \) to \( B \)): \( !(A \rightarrow B) \) and \( !A \rightarrow B \). The \( \rightarrow \) is the linear arrow, typing proofs/programs which use their hypotheses exactly once. The power of duplication is regained (and controlled) via the exponential modality \( ! \) ("off course"). The two translation then mark two different perspectives: in \( !(A \rightarrow B) \) we are saying that functions are the duplicable objects, and thus the values that can be passed around, while in the other we are saying that being an argument suffices to be duplicated. Indeed it was shown in [8] that the two translation are intimately linked with two paradigms of evaluation of functional programs, respectively call-by-value and call-by-name. We concentrate on the first, which is used more often in calculi with references.

The syntax of choice for LL are proof nets, graphical-theoretical representation of proofs that have the advantage of exposing parallel features of deterministic and sequential computation. Its recent developments in the direction of non-deterministic differential extensions [9] reaching concurrency [10] make this kind of investigation the ideal launching pad towards extending logical interpretations of concurrent computation, in the sense of Curry-Howard. For now we restrain to the sequential case which is used more often in calculi with references.

In section III we implement localized monads in \( \Lambda \), a simple typed \( \lambda \)-calculus with products. We then use them to completely translate \( \Lambda_{reg} \), proving two results: stratification is equivalent to using simple types without fixpoints of formulae (Proposition 12), and a \( \Lambda_{reg} \) terms evaluates to a value \( V \) iff its translation evaluates too to the translation of \( V \) (Theorem 14). In particular we get a new proof that stratification yields termination (Corollary 15).

In section IV we pass to LL proof nets. We redefine the translation, that is essentially what done with \( \Lambda \) passed through the call-by-value translation; we then show simulation (Theorem 23) and that we can follow any reduction strategy (limited to depth 0) in the proof net corresponding to a term \( M \); we are guaranteed that we will find the value of \( M \) if there is one (Theorem 24).

In section V we make some final remarks and present our future objectives.

Notations: We will use multisets (i.e. functions from a set to natural numbers, the multiplicities) with additive notation, so that \( \mu_1 + \mu_2 \) is disjoint union, \( \mu_1 \leq \mu_2 \) means that \( \mu_1 \) is a submultiset of \( \mu_2 \), and \( \mu_1 - \mu_2 \) is multiset subtraction. Given a relation \( \rightarrow \), the notation \( \overset{*}{\rightarrow} \) is for the transitive reflexive closure of \( \rightarrow \).

II. The \( \lambda \)-CALCULUS WITH REGIONS

In this section we present the \( \lambda \)-calculus with regions we will use for our results.

A. Syntax and Reduction

Figure 1 presents the syntax of terms, stores and the reduction of their interaction. A \( \nu \)-step is one reducing a \( \nu \nu \leftrightarrow V.N \) subterm. As usual, we associate both abstractions and applications, i.e. \( \lambda x.y.M = \lambda x.\lambda y. M \) and \( MN_1N_2 = (MN_1)N_2 \). We also use the imperative notation \( Mn \) to denote \( (\lambda d.N)M \) with \( d \notin FV(N) \).
A first abstraction with respect to other calculi with references is that we do not directly employ true references that can be passed around. In fact we identify regions with locations: every region in a given moment provides only one value. Notice indeed that though there may be multiple values for \( r \) in the store \( S \), as stores are not commutative in general, there will always be a single value “on the surface” for a given region: reduction is completely deterministic.

Stores are therefore functions assigning stacks to regions. This feature is introduced by the interaction between \( \nu r = V \), that pushes a value in the store, and the \( \nu r = V \) it leaves behind. The latter is a helper constructor that waits until the term it is attached to becomes a value and then removes the entry from the store possibly revealing what was assigned to \( r \) before. \( \nu r / \nu r \) thus implement a kind of local entry in the store. However it must not be confused with a private region (like the PRIVATE constructor from \([1]\)), as it does not bind \( r \) in any way. In particular any reference to \( r \) inside the body of a function is unaffected by the \( \nu r / \nu r \) reductions and may be evaluated later to refer to other values of \( r \). Also the value at the top of the stack can “leak” below after that it has been destroyed if a function passes it around.

We take the opportunity to present an example using all the reduction rules in Figure 1 and exposing what we just wrote. Let \( tt \) and \( ff \) be \( \lambda x, y. x \) and \( \lambda x, y. y \) respectively. Then

\[
\begin{align*}
\nu r & \mapsto \text{tt}(r)(\nu r \mapsto \text{ff} \cdot (\lambda x, y. \text{set}(r, x) \cdot x) \cdot \text{get}(r) ) \cdot () \\
\nu r & \mapsto \text{tt}(r)(\nu r \mapsto \text{ff} \cdot (\lambda x, y. \text{set}(r, x) \cdot x) \cdot \text{get}(r) ) \cdot () , r \mapsto \text{tt} \\
\nu r & \mapsto \text{er}(r)(\nu r \mapsto \text{ff} \cdot (\lambda x, y. \text{set}(r, x) \cdot x) \cdot \text{get}(r) ) \cdot () , r \mapsto \text{tt} \\
\nu r & \mapsto \text{er}(r)(\lambda y. \text{set}(r, f) \cdot f) \cdot () , r \mapsto \text{ff} , r \mapsto \text{tt} \\
\nu r & \mapsto \text{er}(r)(\lambda y. \text{set}(r, f) \cdot f) \cdot () , r \mapsto \text{ff} , r \mapsto \text{tt} \\
\nu r & \mapsto \text{er}(r)(\lambda y. \text{set}(r, f) \cdot f) \cdot () , r \mapsto \text{tt} \\
\nu r & \mapsto \text{er}(r)(\text{ff} \cdot f) , r \mapsto \text{tt} \\
\end{align*}
\]

Notice how the “internal” \( ff \) got to be the final result.
system, together with the \( \nu r \) construct we employ, allow to avoid this kind of situations. We just need to start from a closed term with no pending effects (i.e. \( R; \vdash M : A, \emptyset \)), provided \( M \) does not use any \( \nu r \). Nevertheless in order to reason inductively on programs and prove their properties we also need to describe the intermediate states between the starting program and (hopefully) the value it reaches.

In the following we will do exactly so introducing the notion of **external state**, checking on what regions and how many of them a term must have access to.

The domain \( \text{dom}(S) \) of a store \( S \) is defined as the **multiset** of its \( r \)'s for which there is \( r \leftarrow V \in S \). Formally, \( \text{dom}(\varepsilon) = [\emptyset] \), \( \text{dom}(r \leftarrow V) = [r] \) and \( \text{dom}(S, T) = \text{dom}(S) + \text{dom}(T) \). Let \( \text{ar}(M) \) (the **active regions**) be the partial function taking terms to multisets of regions defined inductively as follows (\( \perp \) stands for undefined).

\[
\begin{align*}
\text{ar}(x) &= \text{ar}(\varepsilon) = \text{ar}(\text{get}(r)) := [\emptyset], \\
\text{ar}(\text{set}(r, M)) &= \text{ar}(M), \\
\text{ar}(MN) &= \begin{cases} \\
\text{ar}(N) & \text{if } M \text{ is a value}, \\
\perp & \text{otherwise}, \\
\end{cases} \\
\text{ar}(\lambda x. M) &= \begin{cases} \\
\perp & \text{if } \text{ar}(M) = [\emptyset], \\
\perp & \text{otherwise}, \\
\end{cases} \\
\text{ar}(\nu r \leftarrow M, N) &= \begin{cases} \\
\text{ar}(M) & \text{if } \text{ar}(N) = [\emptyset], \\
\perp & \text{otherwise}, \\
\end{cases} \\
\text{ar}(\varepsilon r) &= \text{ar}(M) + [r]. 
\end{align*}
\]

What this function does is check how many \( \nu r \)'s were activated and turned into \( \varepsilon r \)'s waiting for an evaluation to end. Non-definedness marks that something is wrong: there is an \( \varepsilon r \) that could not possibly be generated during evaluation (for example under a \( \lambda \)).

**Definition 2.** A **state** is a pair \( M, S \) of a term \( M \) and a store \( S \) such that

- \( M, S \) is typable with some type and effects \( A, e \),
- \( \text{ar}(M) \) is defined and \( \text{ar}(M) \leq \text{dom}(S) \), and
- \( e \subseteq \text{dom}(S) \) and \( \text{ar}(M) \).

A state \( S, M \) is **external** if \( \text{dom}(S) = \text{ar}(M) \) (in particular it has \( e = \emptyset \)). A **program** is an external state \( M, \varepsilon \); in particular \( M, \varepsilon \) is a program iff \( M \) is closed, typable with some \( A, \emptyset \), and not containing any subterm \( \varepsilon r.N \), so that \( \text{ar}(M) = [\emptyset] \). A **result** is a state \( V, S \) whose term is a value. We call external results \( V, \varepsilon \) directly values.

While asking that a program do not contain \( \varepsilon r \) constructs may seem sensible, marking it as a helper constructor used for evaluation but not available for programming (similar to the \( \text{*PRIVATE*} \) constructor of [1]), the condition on states by means of the “\( \text{ar}^* \)” function might seem a bit awkward. However the stability of external states (Lemma 3) and the one we will present later (Lemma 8) indeed characterize external states as exactly the residuals of programs. Non-external states are needed to carry out some proofs by induction: intuitively, memory access operations are always evaluated in an internal state, otherwise they would fail in retrieving or setting a value.

The following result states that the conditions imposed on programs/states are stable under reduction and that they guarantee that either we have divergence or get a value/result. In particular no deadlock related to memory occurs: memory access (\( \text{get}(r) \) and \( \text{set}(r, V) \)) and deallocation (\( \varepsilon r.V \)) do not produce “segmentation faults”, i.e. are always evaluated when there is an \( r \leftarrow V \) in the store, so their reduction is defined. Moreover if \( M, \varepsilon \) is a program and evaluates to a result \( V, S \), then it will be necessarily a value \( V, \varepsilon \), i.e. garbage collection will have been done.

**Lemma 3.** If \( M, S \) is a state, then either it is a result \( V, S \) or \( M, S \rightarrow M', S' \) with \( M', S' \) a state too. Moreover \( \text{dom}(S') - \text{ar}(M') = \text{dom}(S) - \text{ar}(M); \) in particular if \( M, S \) is external so is \( M', S' \).

**C. Alternatives**

In this section we discuss some alternatives for the syntax, either coming from the literature, or necessary later in the paper.

1) **Subtyping:** The reader could notice the lack of subtyping in our system, as in [1], [6]: we retained just the possibility to add dummy effects. We will here explain how this does not really affect the expressiveness (though it may affect the conciseness of terms when subtyping is needed).

Subtyping is given by the following inductive definition:

\[
A' \leq A \quad B \leq B' \quad e \subseteq f
\]

\[
\begin{array}{c}
A \leq A' \\
A \preceq B \leq A' \leadsto B' \\
R; \Gamma \vdash_s M : A, e \quad A \leq B
\end{array}
\]

Transitivity follows from a proof by induction. Let \( \vdash_s \) be the type system with the same rules done in Figure 2 and the following one for subtyping:

\[
R; \Gamma \vdash_s M : A, e
\]

**Lemma 4.** For every derivation of \( R; \Gamma \vdash_s M : A, e \) there is one of the same assertion where the subtyping rule appears only under axioms (namely the rules for variable and for \( \text{get} \)).

The subtyping rule cannot be completely removed preserving the same assertion \( M : A \). Nevertheless one may notice that \( \eta \)-expansion allows some form of supertyping: e.g. we have \( x : 1 \xrightarrow{\cdot} 1 \leftarrow \lambda y. xy : 1 \xrightarrow{\cdot} 1 \) with \( e \subseteq e' \), without recurring to the explicit subtyping rule but just using the dummy effects one. However \( \eta \)-expansion behaves very badly in general with call-by-value, as it may turn a non-value into a value. Though \( \eta \)-expansion of values is acceptable, it does not suffice here. For example, if we want to cast \( x : 1 \rightarrow 1 \rightarrow 1 \) to its supertype \( 1 \rightarrow 1 \xrightarrow{\cdot} 1 \), we would need to \( \eta \)-expand to \( \lambda y, z. xyz \), in particular expanding \( xy \) which is not a value. We thus provide a particular combination of \( \eta \) and \( \beta \) expansions which do the trick.

Let \( \rightsquigarrow \) be the reflexive and compatible closure of

\[
V \rightsquigarrow \lambda x.I(Vx), \quad x \notin \text{FV}(V),
\]

\[
\text{get}(r) \rightsquigarrow \text{I get}(r),
\]

where \( I = \lambda x.x \), the identity. Notice that under non-weak reduction, the right hand side of \( \rightsquigarrow \) reduces to the \( \eta \)-expansion of the right hand side. Notice also that \( M \rightsquigarrow M' \)

\[1\]For example, if \( M \) is a diverging term, its \( \eta \)-expansion is a value and is thus terminating.
implies that $M$ is a value iff $M'$ is one too. We extend $\rightsquigarrow$ also to stores. Finally, by compatibility one easily has that if $M \rightsquigarrow M'$ and $V \rightsquigarrow V'$ then $M[V/x] \rightsquigarrow M'[V'/x]$.

**Lemma 5.** If $R; \Gamma \vdash_\nu M : A, e$ is derivable, then there is $M'$ with $M \leadsto M'$ with $R; \Gamma \vdash_\nu M' : A, e$ without subtyping.

**Lemma 6.** If $M \rightsquigarrow M'$ and $S \rightsquigarrow S'$, then $M, S \Downarrow V, V_0$ iff $M', S' \Downarrow V', V_0'$ with $V \rightsquigarrow V'$ and $S' \rightsquigarrow S_0'$.

The above two lemmas combined together say that the system without subtyping we presented is expressive as much as the one with subtyping, modulo doing an expansion on terms which allows mimicking subtyping by just adding dummy effects.

2) **Reference types:** Another feature that might seem strange to have missing are explicit types for references, and the possibility to treat references/regions as data, possibly to be passed between programs, like in [1]. The language presented in this paper must mainly be seen as a tool to abstract away some specific features of references, for example with the objective of proving termination.

In any case given enough expressiveness one can encode reference types. In fact if we suppose to have an implementation in $\lambda$-calculus of lists and natural numbers (for example using polymorphic $\lambda$-calculus, see the discussion we make in section V), it is not hard to implement general references. We here give an informal description of it.

For references of type $A$, let be given a region $r : \text{List}_A$ (of list type). Then let

\[
\begin{align*}
\text{new}_{r} &::= \lambda v. (\ell. \text{set}(r, \ell); \text{length} \ell) \text{get}(r) \\
\text{write}_{r} &::= \lambda n. v. \text{set}(r, \text{update} \text{get}(r)nv) \\
\text{read}_{r} &::= \lambda n. \text{pick} \text{get}(r)n,
\end{align*}
\]

where the new terms employed ($\text{length}$, $\text{update}$ and $\text{pick}$) are rather self-explanatory. Then $\text{new}$ can be interpreted to assign a value to a new slot in the store and pass a reference to it (which quite bluntly is the size of the list and thus the index of the last element inserted in it). Given such an integer $\text{write}$ and $\text{read}$ can then update and obtain the values from the list. The term must only be wrapped into $\nu r \ll \text{empty}, M$, initializing the list to be empty.

3) **Storeless reduction:** We will here present an alternative definition of reduction that internalizes stores and does not use the helper $c$ construct. We will use such a syntax to define the translation of states into linear logic proof nets in section IV.

Let $\nu$-evaluation contexts be generated by the same rules as evaluation contexts (Figure 1), adding however $\nu r \ll E$. Given a $\nu$-evaluation context $E$, let $\text{PR}(E)$ (the private regions of $E$) be the set of $r$’s so that $E$’s hole is in the scope of a $\nu r$. Now given a program $M$ (in particular without $\epsilon r$’s), we define the storeless reduction $M \rightarrow M'$ as:

\[
\begin{align*}
E[(\lambda x.M)V] &\rightarrow E[N(V/x)],
E[\nu r \ll V.U] &\rightarrow E[U]
E[\nu r \ll U.F[\text{set}(r, V)]] &\rightarrow E[\nu r \ll V.F[\emptyset]]
E[\nu r \ll U.F[\text{get}(r)]] &\rightarrow E[\nu r \ll V.F[V]],
\end{align*}
\]

where $E$ and $F$ are $\nu$-evaluation contexts such that $r \notin \text{PR}(F)$.

Intuitively, the $\nu r$ in $\nu r \ll U.F$ is the first value for $r$ whose scope captures the location we are evaluating. We recall that a $\nu$-step is one that in regular reduction reduces a $\nu r \ll V.N$ subterm adding $V$ to the store.

**Syntax**

\[
\begin{align*}
U, V &::= x \mid \emptyset \mid \lambda x.M \mid (U.V) & \text{(values)} \\
M, N &::= V \mid MN \mid \pi_r M \mid \langle M, N \rangle & \text{(terms)} \\
E, F &::= [] \mid EM \mid VE \mid \pi_r E \mid \langle E, N \rangle \mid \langle V, E \rangle & \text{(eval. contexts)}
\end{align*}
\]

**Reduction**

\[
\begin{align*}
(\lambda x.M)V &\rightarrow M(V/x), & \pi_r \langle V_1, V_2 \rangle &\rightarrow V_i.
\end{align*}
\]

Figure 3. Syntax and reduction of $\Lambda \times$.  

Now we will show how to lift a state to a program that reduces to it via $\nu$-steps (which, we recall, are those reducing $\nu r$’s), and which will be able to simulate the reduction of the state via $\rightarrow$ (Lemma 9). It will be then the case that the lifted program perfectly simulates the evolution of the state it lifted from by means of storeless reduction.

**Definition 7.** The lifting $(M, S)''$ of a state be defined as $M$ if $M = V$ or $M = \text{get}(r)$, and otherwise:

\[
(MN, S)'' := \begin{cases} M(N, S)'' & \text{if } M \text{ is a value,} \\
(M, S)'' & \text{otherwise.}
\end{cases}
\]

\[
(\nu r \ll M, N, S)'' := \nu r \ll (M, S)'' \ll N, \\
(\text{set}(r, M, S))'' := \text{set}(r, (M, S)'') \\
(\epsilon r, M, S, r \ll V)'' := \nu r \ll V(M, S)''.
\]

**Lemma 8.** For every external state $M, S$, $(M, S)''$ is defined and is the unique program such that $(M, S)''\epsilon \rightarrow M, S$ using only $\nu$-steps.

**Lemma 9.** Let $(M, S)$ be an external state. Then $(M, S) \rightarrow (M', S'')$ with a $\nu$-step iff $(M, S)'' \rightarrow (M', S'')''$. If $(M, S) \rightarrow (M', S')$ with a $\nu$-step, then $(M, S)'' \rightarrow (M', S'')''$.

### III. Types and Effects into Monads

In this section we define the translation of $\Lambda_{\text{reg}}$ into the ordinary $\lambda$-calculus with products. As it turns out, on the type level this corresponds to introducing state monads [2]. Indeed, the annotated arrow $A \Rightarrow B$ will correspond to the arrow $A \rightarrow T_e(B)$ where $T_e$ is a state monad indexed by the set of regions.

In Figure 3 we show the syntax of such calculus, which we denote by $\Lambda \times$. Types and typing rules for $\Lambda \times$ are shown in Figure 3. As usual, $FV(A)$ denotes the set of variables appearing in $A$. For $x$ and $y$ distinct variables.
we will denote \( \lambda(x, y).M \) to mean \( \lambda p.((\lambda x . y . M)(\pi_1 p))\pi_2 p \).
We will define the generalized product (parenthesized on the left) by \( \prod_{i \in I} A_i \), if \( I \) has an order associated with it.
We define the empty product as \( 1 \), and generalized tuples by \( \langle M_1, \ldots, M_{k+1} \rangle := \langle \langle M_1, \ldots, M_{k} \rangle, M_{k+1} \rangle \) for \( k \geq 2 \), and \( \langle M \rangle := M \). The corresponding projections \( \pi_i^k \) are obtained by combining the two projections \( \pi_i \).

As we will want to account also for the unstratified case, we have also introduced type variables and systems of equations, which are considered here as functions (possibly with infinite domain) from some type variables to non-atomic types, presented as sets of pairs \( X \equiv E(X) \).
Given such a system of equations, it can be used to define recursive types by considering the structural equivalence \( \equiv_E \) generated by \( X \equiv_E E(X) \) for \( X \in \text{dom}(E) \) (i.e. \( \equiv_E \) is the equivalence relation generated by the context closure of the equations \( \equiv \) appearing in \( E \)).

**Definition 10.** We say that \( E \) is **solvable** if there is an assignment \( \sigma_E \) from \( \text{dom}(E) \) to closed (i.e. variable-free) types so that for all \( X \in \text{dom}(E) \) we have \( X \equiv_E \sigma_E(X) \).

The above is equivalent to asking \( \sigma_E(X) = \sigma_E(E(X)) \), where \( \sigma_E(\ ) \) is extended on all types as usual, letting it be the identity on variables outside \( \text{dom}(E) \) and proceeding by induction. Notice that if \( E \) is solvable, then \( \text{FV}(E(X)) \subseteq \text{dom}(E) \) for all \( X \in \text{dom}(E) \), the solution \( \sigma_E \) is unique, and the quotient by \( \equiv_E \) gives just the types \( A \) with \( \text{FV}(A) \cap \text{dom}(E) = \emptyset \), in particular no truly recursive types (such as \( X = 1 \times X \)) are induced.

### A. State Monads

In this section we will implement side effects in \( \Lambda_\chi \) by using state monads. Let there be a distinguished type variable \( X_r \) for each region \( r \), and let \( E \) be a system of equations on the \( X_r \)'s. From now on, types will be considered modulo \( E \). Let there be also a fixed order on regions, so that sets of regions are considered presented according to this order.

Given a finite set \( e \) of regions, the **type of e-stores** is \( P_e := \prod_{r \in e} X_r \). The **state monad** localized at \( e \) is defined by the type constructor \( T_e(A) = P_e \rightarrow (P_e \times A) \). This is the classic state monad, modeling the fact that a computation will start with a certain state and return possibly another one together with the result. We just parametrize it by a finite product of types, indicating to what values it will have access.

Let us first introduce some \( \Lambda_\chi \) terms working with stores. Given \( r \) we define \( \pi^k_r M \) as \( \pi^k_r M \) where \( k = \# e \) and \( i \) is \( r \)'s position in \( e \). We generalize to \( e = \{ r_1, \ldots, r_k \} \subseteq f \) by setting \( \pi^k_r M = \pi^k_{r_1} M_{r_1} \ldots \pi^k_{r_k} M_{r_k} \).

We will now prove some of the main properties of the terms presented in **Figure 5**. We call e-stores the values of type \( P_e \). Given an e-store \( S \) and an f-store \( T \) then if \( e \cap f = \emptyset \), \( S + T \) is defined as the \( e \cup f \)-store given by joining the two; if \( e \subseteq f \) then \( T|_e \) is the store \( T \) restricted to regions in \( e \). In fact, \( S + T \) and \( T|_e \) are the values of \( \text{upd}_{e,f} ST \) and \( \pi^k_T \) respectively.

**Lemma 11.** We have the following properties on the terms introduced in **Figure 5**.

- If \( S : P_{e \cup \{ r \}} \), \( V : X_r \) is a value (so \( \langle V \rangle \) is an \( \{ r \} \)-store) and \( M : T_{e \cup \{ r \}}(A) \) then \( \pi^k_r V M S \overset{\ast}{\Rightarrow} \langle S', U \rangle \iff M S|_e \overset{\ast}{\Rightarrow} \langle S'|_e, U \rangle \) and \( S'|(f \setminus e) = S|_{f \setminus e} \).
- If \( S : P_{e \cup f} \), \( M : T_e(A) \) then \( \text{cast}_{e,f} MS \overset{\ast}{\Rightarrow} \langle S', U \rangle \iff M S|_e \overset{\ast}{\Rightarrow} \langle S'|_e, U \rangle \) and \( S'|(f \setminus e) \overset{\ast}{\Rightarrow} \langle T, V \rangle \) and \( M S|_{(V/x)}(T)|_{f \setminus e} \overset{\ast}{\Rightarrow} S|_{f \setminus e} \).

### B. Monadic structure

**Monadic structure**

\[
\text{let } x \text{ be } M \text{ in } N := \lambda s.((\lambda (s_1, x).N s_1)(M s))
\]

**Derived typing rules**

\[
\begin{align*}
\Gamma & \vdash M : A \\
\Gamma & \vdash [M] : T_e(A) \\
\Gamma & \vdash M : T_e(A) \quad x : A, \Gamma \vdash N : T_f(B) \\
\Gamma & \vdash \text{let } x \text{ be } M \text{ in } N : T_e(B)
\end{align*}
\]

**Additional projections**

\[
\pi^k_r M := \begin{cases} M & \text{if } i = k = 1, \\
\pi^k_r M & \text{if } i = k > 1, \\
\pi^k_{r-1} \pi^k_1 M & \text{if } i < k \text{ and } k > 2,
\end{cases}
\]

\[
\pi^k_r e, \text{ where } i \text{ is } r \text{'s place in } e,
\]

\[
\pi^k_r f, \text{ if } f \subseteq e.
\]

**Additional terms**

\[
\begin{align*}
\text{upd}_{e,f} & := \lambda s, t.\langle r_e, \text{let } \langle c_r \rangle e \text{ in } \text{let } c_r = \{ \pi^k_{r e} s_i \text{ if } i \in r, \pi^k_{r f} t \text{ otherwise} \};
\text{upd}_{r, e} & := \text{upd}_{(r), e},
\text{g} & := \lambda x. (x, x),
\text{s} & := \lambda x, d. (\langle x, e \rangle),
\text{n}_e^f & := \lambda r, p, s. (\lambda (s_1, v). \langle \pi^k_e \pi^k_f (s_1, v) \rangle (p(\text{upd}_{e,f} s_1, s_1, v)))
\text{cast}_{e,f} & := \lambda \lambda s, r. (\langle x, v \rangle). \langle \text{upd}_{e,f} s_1, s_1, v \rangle (p(\pi^k_e \pi^k_f s))
\end{align*}
\]

**Types of additional terms**

\[
\begin{align*}
\vdash \text{upd}_{e,f} & : P_e \rightarrow P_f \rightarrow P_{e \cup f},
\vdash g & : T_{[r]}(X_r),
\vdash s & : X_r \rightarrow T_{[r]}(1),
\vdash n_e^f & : X_r \rightarrow T_{e \cup \{ f \}}(A) \rightarrow T_e(\{ f \})(A),
\vdash \text{cast}_{e,f} & : T_e(A) \rightarrow T_{e \cup \{ f \}}(A)
\end{align*}
\]

**Mixing monads**

\[
\begin{align*}
\text{let } e, f & \text{ x be } M \text{ in } N := \lambda s, t. \langle c_r \rangle e \text{ in } \text{let } c_r = \{ \pi^k_{e s} s_i \text{ if } i \in e, \pi^k_{e f} t \text{ otherwise} \};
\end{align*}
\]

\[
\begin{align*}
\Gamma & \vdash M : T_e(A) \\
\Gamma & \vdash \text{let } x \text{ be } M \text{ in } N : T_{e \cup f}(B)
\end{align*}
\]

Figure 5. Implementation of localized state monads.
As it can be seen, the annotated function type $A \xrightarrow{\epsilon} B$ gets translated, in category theoretic terms, to arrows of the Kleisli category for the monad $T_e$. The region context just sets a system of equations that equates a variable $X_r$ with the translation of the type associated with $r$.

**Stratification:** We will account for stratification by showing that via our translation it is equivalent to avoiding the use of recursive types, as the associated system of equations is solvable (Definition 10). We will thus give a strong logical justification as to why stratification ensures termination, even if the result is not new: it allows to internalize all in an ordinary $\lambda$-calculus.

**Proposition 12.** $R^\circ$ is solvable iff the stratification condition $R \vdash$ holds.

In fact, the proof of the above proposition shows how stratification gives an order in which each indeterminate of $R^\circ$ find its value.

C. Translating the Terms

We will now turn our attention to terms. In the following we fix a region context $R$ and consider all $\Lambda_\times$ types under the structural equivalence $\equiv_E$ (possibly as non-recursive types if, as seen, $R$ is stratified). In Figure 6 we define the translation of $\Lambda_{\text{reg}}$ programs (to be more precise type derivations of programs) to $\Lambda_\times$ terms. Notice in particular that no translation is given for $e \cdot M$: as we will prove the simulation of an entire evaluation rather than a step by step one, this does not pose particular problems. Notice that the translation of a value $V$ typed with $A, \emptyset$ is necessarily $[V']$ for a value $V'$.

**Proposition 13.** Let $\Gamma^\circ(x) := (\Gamma(x))^\circ$. Then:

- if $R; \Gamma \vdash M : A, e \rightarrow M'$ then $\Gamma^\circ \vdash M' : T_e(A^\circ)$ is derivable in $\Lambda_\times$ modulo $\equiv_R$; in particular programs $M, \varepsilon : A, \emptyset$ are mapped to closed terms of type $A^\circ$;
- $\Gamma \vdash x : A \rightarrow M : A, e \rightarrow M'$ and $\Gamma \vdash \Gamma[V/x] : A, \emptyset \rightarrow [V']$ then $R; \Gamma \vdash M[V/x] : A, e \rightarrow M'[V'/x]$.

Here follows the main result of this section, stating that the $\Lambda_\times$ term associated with each $\Lambda_{\text{reg}}$ term evaluates to the same result (up to translation).

**Theorem 14.** If $R; \vdash M, \varepsilon : A, \emptyset \rightarrow M'$ is a $\Lambda_{\text{reg}}$ program with its associated $M'$ term, then $M$ evaluates to the value $V, \varepsilon$ iff $M' \xrightarrow{\tau} V'$ with $V \rightarrow [V']$.

**Corollary 15.** If $R ; \vdash M, \varepsilon : A, \emptyset$ then $M$ terminates to a value.

IV. TYPES AND EFFECTS INTO LINEAR LOGIC

In this section we draw from the intuitions gained from the translation of $\Lambda_{\text{reg}}$ into $\Lambda_\times$ to translate $\Lambda_\times$ into LL proof nets. We have two starting points: the translation of call-by-value $\lambda$-calculus [7], [8], and the exponential isomorphism $!((A \times B) \cong !A \otimes !B)$ that can be used for pairs.

A. The nets

First of all, in Figure 7 we define LL’s formulæ (and provide already the translation of $\Lambda_{\text{reg}}$ types). As usual, the dual is involutive ($A^{\perp \perp} = A$) and defined via De Morgan laws $\perp \perp = \bot$ and $(A \otimes B)^\perp = A^\perp \nabla B^\perp$. The linear arrow $A \nrightarrow B$ is defined as $A^\perp \nabla B$. For example changing dualities on the translation of the arrow with effects we have

$$(A \xrightarrow{\{r_i\}} B)^\bullet = \left(\left((A^\bullet)^\perp \nabla X^\perp_r \right) \cdot X^\perp_r \nabla (\otimes_i !X^\perp_r \otimes B^\bullet)\right).$$

Again, in order to be able to translate also in absence of stratification, we consider systems of equations, and the induced structural equivalence. Once again, $X_r$ are special variables marked with regions. The definition of solvability of such a system is identical to what done in section III: the only difference is one takes into account substitution of dual variables. We will present LL proof nets in the interaction net style [11], and range over them with letters such as $\pi, \sigma$.

**Definition 16.** LL nets\(^2\) are, intuitively, cells linked with wires. A net $\pi$ is thus given by a set of cells, to each of

\[X, Y\] $A, B := X \mid X^\perp \mid 1 \mid \bot \mid A \otimes B \mid A \nabla B$ (types)

$E, F := X_1 \vdash A_1, \ldots, X_k \vdash A_k$ (systems of eq.)

**Translation**

\begin{align*}
1^\bullet & : 1!, \quad \{r_1, \ldots, r_k\}^\bullet := \bigotimes_i !X^\perp_r,
(A \xrightarrow{\epsilon} B)^\bullet & := !((A^\bullet \otimes \ast^\bullet) \rightarrow (e^\bullet \otimes B^\bullet)),
(\emptyset)^\bullet & = \emptyset, \quad (R, r : A)^\bullet = R^\bullet, X^\perp_r \rightarrow A^\bullet.
\end{align*}

Figure 7. Recursive linear logic types and type and effect translation.
which a number of disjoint ports and a symbol is assigned; each port, belonging to a cell or free (i.e. a conclusion) belongs exactly to one wire, which in fact is a set of two ports. A net is typed if there is an assignment to directed wires such that reversing the direction of the wire we get the dual type, and such that other properties are satisfied.

The graphical representation of cells, together with their typing rules.

### Definition 17

Figure 9 shows the reduction and equivalence rules of LL.

B. Translating the Types

While introducing LL types in Figure 7 we also defined the translation of $\Lambda_{reg}$ types. Now we explain a bit informally how the translation we presented is related to the one we gave for $\Lambda_x$ in section III. Let $A^*$ be the translation of $\Lambda_x$ types into LL’s ones, defined by

$$1^* := !1, \quad X^* := !X, \quad (A \to B)^* := !(A^* \to B^*), \quad (A \times B)^* = A^* \otimes B^*.$$  

$A^*$ is in fact the classical call-by-value translation with pairs added in: seen that all $A^*$ start with an $!$, $A^* \otimes B^*$ is indeed isomorphic to an LL product. Now if we compose the translation given in section III with this one (before any system of equations is applied), we obtain

$$(A \nrightarrow B)^{\circ *} = (A^* \to P_e \to (P_e \times B^*))^* = !(A^{*\circ} \to !(e^* \to (e^* \otimes B^{\circ^*}))).$$

Here we will skip the subtleties linked to reduction modulo an equivalence. However the results of Lemma 19 are valid in this framework.
However we define from the intended behaviour of the translation that the function taking stores $P_s$ is duplicated only when part of a function taking actual values: in terms of monads, it is a computation, not a value. In other words, the inner! above is useless to our objective. So we pass to
\[(A^s \rightarrow e^s \rightarrow (e^s \otimes B^{v^s})) \cong !(\!\!(A^s \otimes e^s) \rightarrow (e^s \otimes B^{v^s})\!\!),\]
where the uncurrying isomorphism $A \rightarrow B \rightarrow C \cong (A \otimes B) \rightarrow C$ (monoidal closedness) shows that our translation is essentially the one we presented into $\Lambda_\times$ passed through the call-by-value translation.

The following result has the same statement and proof of Proposition 12.

**Proposition 20.** $R \vdash$ is stratified iff $R^\bullet$ is solvable.

**C. Translating the Terms**

We will define the translation as a mapping $M \mapsto M^\circ$ between typed terms and nets. Even more explicitly than we have done before, we will identify a term with its type derivation. This poses problems of representation: a type derivation may have dummy variables in the context; similarly it may also have dummy effects. We sidestep the problem by considering $y : D, \Gamma(x) \vdash M : A, e \equiv \Gamma \vdash M : A, e \equiv \Gamma \vdash, e \cup \{r\}$, if the center one is derivable. Clearly similar equivalences will have to be considered on nets also.

Given a term
\[R; x_1 : A_1, \ldots, x_k : A_k \vdash M : B, \{r_1, \ldots, r_k\}\]
its translation $M^\bullet$ will have the following general form.

\[
\begin{array}{l}
\begin{array}{c}
A^1_1 \mid \ldots \mid A^1_n \mid \langle X_{r_1} \rangle \mid \ldots \mid \langle X_{r_k} \rangle \\
M^\bullet \\
\langle X_{r_1} \rangle \mid \ldots \mid \langle X_{r_k} \rangle \mid B^\bullet
\end{array}
\end{array}
\] (1)

In particular, we have on top a wire for every variable (labelled with it) and one for every affected region, “entering” the net. Below there are corresponding wires for regions, and one for the output on the right. Informally, a translated term may be seen graphically as a unit processing a stream (the region wires passing through it) based on inputs (the variables) and giving out an output. With this graphical convention in fact the parts of the net that are evaluated beforehand are always on top. At times for the sake of space we may also draw proof nets from left to right rather than from top to bottom.

Given a context $\Gamma$ (resp. a set of regions $e$) a wire labelled by $\Gamma$ (resp. by $e$) will stand for multiple wires labelled by variables in $\text{dom}(\Gamma)$ (resp. regions in $e$), typed accordingly. In Figure 10 we show the rules defining the translation $M^\bullet$. Again, notice that no rule is given for $\text{cr.m}$, like for the $\Lambda_\times$ translation. However we use lifting to extend the translation to all external states by setting $(M, S)^\bullet := ((M, S)'^\bullet)^\bullet$. We refer to Definition 7 and the subsequent results for the definition and the properties of the lifting $(M, S)^\bullet$.

First, the upcoming lemma shows that the translation is “statically” correct: it indeed yields proof nets, that is switching acyclic nets.

**Lemma 21.** For every typed term $R; \Gamma \vdash M : A, e$, the net $M^\bullet$ is typed (modulo $R^\bullet$) and switching acyclic.

The following is a standard result when translating calculi into nets.

**Lemma 22** (substitution).

\[\begin{array}{c}
\begin{array}{c}
\Gamma \vdash M^\bullet \\
\Gamma \vdash e \rightarrow \{M_1 \rightarrow \cdots \rightarrow M_N\}
\end{array}
\end{array}\]

Now we show the main results of this part of the paper.

**Theorem 23** (Simulation). Let $M, S$ be an external state. Then:
- if $M, S = V, \varepsilon$ is a value, then $(V, \varepsilon)^\bullet$ is in 0-depth normal form.
- if $M, S \rightarrow M', S'$ with a non-$\nu$-step then $(M, S)^\bullet \vdash \rightarrow (M', S')^\bullet$ with exactly one dereliction on box step;
- if $M, S \rightarrow M', S'$ with a $\nu$-step, then $(M, S)^\bullet = (M', S')^\bullet$.

The following theorem finally tells that we can in fact calculate directly with proof nets: we can reduce in parallel the net while preserving the sequential semantics enforced by effects.

**Theorem 24.** If $(M, S)^\bullet \vdash \pi$, with $\pi$ a 0-depth normal form, then there is a value $V$ such that $M, S \rightarrow V, \varepsilon$ and $\pi = V^\bullet$.

An informal example: Let us show the point we made in the introduction with an informal example. Suppose we have a state $(\text{set}(r, V); F)((G \text{get}(r))((H \text{get}(r))), r = U)$ and $F$ is typed with effects not containing $r$. Then its translation will be (omitting $U$ that is erased any way):

*Even supposing that the term $F$ is undergoing some heavy calculations, the translation exposes the fact that the store containing $V$ can not only interact with the $\text{get}(r)$ in argument position for $G$ (possibly starting computation in $G$, it can be delivered even to $H^\bullet$, even before $G$’s $\text{get}$ “accepts” to take the value. Wires expose directly what dependencies are present in the term and where values can arrive even before the evaluation strategy permits it, all this while guaranteeing the same final result.*

V. **Concluding Remarks**

In this paper we gave a logical account of a $\lambda$-calculus with references, interpreting it as monads in ordinary $\lambda$-calculus and as proof nets in LL. There are some final points and future perspectives that can be discussed.
Polymporphism: Indeed we did not include any kind of polymorphism in our treatment. However type polymorphism (generalization to \( \forall A.A \) and instantiation to \( A[B/X] \)) can straightforwardly be added to the type system and does not entail any difficulty in the translation, though the types of regions need to be closed. Polymorphism of regions is probably also possible to handle, but needs some more investigation.

Multithreading: what is lacking the most with respect to other proposals of calculi (or type systems) is multithreading and concurrency. Indeed the starting objective of this work was to combine call-by-value translation of \( \lambda \)-calculus together with the communication zones which were employed in [10] for a bisimulation between (a fragment of) \( \pi \)-calculus and differential nets. Indeed by slightly generalizing to differential nets and non-determinism the translation presented in this work and combining it with elements of [10], one gets a translation of a multithreaded version of the calculus. However the target nets are very easily cyclic. For example \( \text{set}(r, \text{get}(r)) \), which may in general be any two threads cooperatively updating a shared variable, is (it seems) necessarily cyclic. No particular computational property can be therefore entailed, save for simulation. The problem seems to linked with how logic in general and proof nets in particular handle dependency. In proof nets dependency (which may be tracked with switching paths) can never be created. In particular in \( \text{set}(r, \text{get}(r)) \) there is a potential dependency of each of the \( \text{get} \)'s from the other \( \text{set} \), so that from the logical point of view there is a circular dependency which is somewhat hidden by prefixing. Indeed also in \( \pi \)-calculus' translation a simple process like \( c(x).\sigma(x) \equiv c(x).\sigma(x) \equiv c(x) \) is mapped to a cyclic net.

It seems then the only direction for truly using linear logic with concurrency is either to restrict programs in order to fall within LL's scope (such as forbidding processes like the one pointed above), or rather find a new meaning to correctness to account for such concurrent behaviours.

**REFERENCES**


**PROOFS**

A. The \( \Lambda \)-Calculus with Regions

**Lemma 1.**
Lemma 4.

Proof: Standard inductions on the height of the type derivation. For the second point for each axiom $R;\Gamma \vdash x : A, e$ and $x \notin \text{dom}(\Gamma)$, then $R;\Gamma, x : A \vdash M : e$; if $R;\Gamma, V : A, \emptyset$ and $R; x : A, \Gamma \vdash M : B, e$, then $R;\Gamma \vdash M[V/x] : B, e$; if $R;\Gamma \vdash M, S : A$ and $M, S \to M', S'$, then $R;\vdash M', S' : A$.

Proof: Standard inductions on the height of the type derivation. For the second point for each axiom $R;\Gamma, x : A \vdash x : A, \emptyset$ one has that $\Gamma' \supseteq \Gamma$, so an application of the first point can yield $R;\Gamma' \vdash V : A$ which thus can replace the axiom. The third point is also proved by induction, where the case when reducing $(\lambda x.M)V$ follows from the second point. For memory access operations subject reduction is straightforward.

Lemma 3.

Proof: Suppose $M$ is not a result. Let $\mu(M,S) := \text{dom}(S) - \text{ar}(M)$: $M, S$ is a state (resp. an external state) if $\mu$ is defined (i.e. positive) and contains the effects of $M$ (resp. if $\mu(M,S) = [\cdot]$ with no effects). We will show by induction on $M$ that $M, S \to M', S'$ with $\mu(M', S') = \mu(M,S)$. Checking that the reduc is typed with the same effects of $M$ will be omitted as it is guaranteed by Lemma 1. The cases where there is a subterm of $M$ which is not a value and should be evaluated are handled similarly to the proof of Lemma 4. For example, if $M = VN$ then $N, S$ is an (external) state and not a result, so $N, S \to N', S'$ and thus $M, S \to VN', S'$, an (external) state.

Particular care must only be reserved for $\rho$. In this case, if $N$ is typed with effects $e$ then $\text{cr}(N)$ will be with $f \supseteq e \setminus \{r\}$. Now $\mu(N,S) = \mu(\text{cr}(N), S) + [r]$, so $e \subseteq f \cup [r] \subseteq \mu(N,S)$ and $N, S$ is a state (necessarily non-external). By inductive hypothesis $N, S \to N', S'$, so $\text{cr}(N, S) = \text{cr}(N', S')$ where $\mu$ is invariant.

Suppose then that $M$ has no direct subterm to be evaluated. If $M = V_1V_2$, then $V_1 = \lambda x. N$ as it must be closed and typed with a function space. Then $M, \varepsilon \to N[V_2/x], \varepsilon$, which and $\mu$ cannot have changed as value substitution leaves $\text{ar}(N) = [\cdot]$ unchanged, and the store is the same.

If $M = \pi r \cdot V.N$ then $M, S \to \text{cr}(N, S), r \cdot V, \mu$ remains constant as the $\pi r \cdot V$ balances the new value in the store. If on the other hand $M = \text{cr}(V), r \in \text{ar}(\text{cr}(V)) \subseteq \text{dom}(S)$ and thus $S = T, r \in U$ and $M, S \to V, T$ which is a result (with $\mu(V,T) = \text{dom}(T) = \text{dom}(S) - [r] = \mu(M,S)$).

Finally, if $M = \text{get}(r)$ or $\text{set}(r, V)$, then $M$ must be typed with an effect containing $r$, so $r \in \mu(M,S) = \text{dom}(S)$ and the reduction of the two can take place giving in fact the result. The domain of the store and the inexistent active regions remain unchanged. ■

Lemma 4.

Proof: For every derivation of $R;\Gamma \vdash M : A, e$ there is one of the same assertion where the subtyping rule appears only under axioms (namely the rules for variable and for $\text{get}$).

Proof: Standard induction on the size of the starting inference. By size we take the number of non-subtyping rules, and we assume all adjacent subtyping rules are merged together into one. Supposing the inference ends with a subtyping rule, the proof is split by cases on the rule immediately preceding it. If the subtyping rule can be pushed up on the premises, the inductive hypothesis yields the result. The only interesting cases are application and abstraction. Omitting $R$ and $\Gamma$, one transforms the inferences in the following way.

Lemma 5.

Proof: One starts by applying Lemma 4 to get an inference where subtypings are just below axioms. Then for every $B \leq C$ let $F_{B,C}[\cdot]$ be the one-hole context (not an evaluation one) defined inductively by $F_{B,B}[\cdot] := [\cdot]$ and

\[
F_{B,C}[\cdot] := \lambda y. (\lambda x. F_{C,E}[x])([\cdot] F_{B,C}[\cdot]),
\]

with $y$ and $z$ fresh. Then by induction on the subtyping one sees that $x : B \vdash F_{B,C}[x] : C, \emptyset$ and $x \succeq F_{B,C}[x]$. Now substituting every variable occurrence $x$ in $M$ (resp. every $\text{get}(r)$ occurrence) with $F_{B,C}[x]$ (resp. with $(\lambda x. F_{B,C}[x]) \text{get}(r)$) where $B$ is its type in the context at the moment of introduction, (resp. the type of $r$) and $C$ the one after any subtyping following its introduction, we get an $M'$ with $M \rightsquigarrow M'$ and the same type under the $\vdash$ inference. ■

Lemma 6.

Proof: First suppose $M, S \vdash V, S_0$ if $M', S' \vdash V', S'_0$ with $V \rightsquigarrow V'$ and $S' \rightsquigarrow S'_0$.

Proof: First suppose $M, S \vdash V, S_0$ and let us reason by induction on the length of the normalization. If $M$ is itself a value we are done. Let us split by cases otherwise. All cases where $M$ is not the redefired immediately are handled by the compatibility of $\rightsquigarrow$.

If $M = \text{set}(r, U)$ and $\text{cr}(U)$ we are easily done, as both sides reduce in just one step.

If $S = r \cdot U, T$ and $M = \text{get}(r)$, then $S' = r \cdot U', T'$ with $U \rightsquigarrow U'$, and $M'$ is either $\text{get}(r)$, or $I \text{get}(r)$. In both cases after one or two step we get to $U'$ and we are done.
If $M = (\lambda x M_1)V_1 \rightarrow M_2[V_1/x]$ then $M' = V_2V_1'$
where $V_1 \rightsquigarrow V_1'$, and either $V_2' = \lambda x M_1$ with $M_2 \rightarrow M_1'$,
or $V_2' = \lambda y I(\lambda x M_1)\eta y$ with $M_2' = M_1$ (and in particular $M_2 \rightsquigarrow M$). In any case by inducive hypothesis, as $M_1'\{V_2'/x\} \rightsquigarrow M_2\{V_1'/x\} \downarrow V$ (turning the store $S$ into $S'$), we have $M_1'\{V_1'/x\} \downarrow V'$ as by the thesis. In both cases we conclude: in particular in the latter one we have $S',V_2'V_1' \rightarrow S', I((\lambda x M_1)\eta y) S_0IV' \rightarrow S_0[V].$

For the if part, the reasoning follows in reverse the steps taken for the only if part.

**Lemma 8.** For every external state $M,S$, $(M,S)^\nu$ is defined and is the unique program such that $(M,S)^\nu, e \dashv \vdash M$ using only $\nu$-steps.

Proof: By induction on $M$. If $(M,S)^\nu = M$ we notice that $S = \varepsilon$ (as $ar(M) = \emptyset$) and we are done. If $M = V_1N_2$ with $V_1$ a value, then $\nuS = N_2, S$ is an external state, and by inductive hypothesis $N_2, S \vdash (N_2, S)^\nu, e$ by $\nu$’s. Then as $N_2, S \vdash (N_2, S)^\nu, e \vdash N_1N_2, S$ we are done. The other case for application, for $\nuS \vdash N_1, N_2$ and for $set(r,M)$ are similar. For $M = \varepsilon, N$, it must be the case that $S = T, s \varepsilon V$ (as $s \in ar(M) = dom(S)$). As $N,T$ is an external state inductive hypothesis gives $(N,T)^\nu, e \vdash N,T$ by $\nu$-steps. Then $(M,S)^\nu = \varepsilon \varepsilon S = V, (N,T)^\nu$, apart from being provable, has the desired property: $\varepsilon \varepsilon S = V, (N,T)^\nu, e \varepsilon S = V, \varepsilon, N,T = s \varepsilon V$.

Uniqueness follows from the fact that if two programs reduce to the same external state $M, S$ just by $\nu$-steps, then such reductions must be exactly the same: their number is the cardinality of $S$, the position of reduced $\nu$’s are marked by $\nu r$’s in $M$, and the values assigned by the reduced $\nu$’s are determined by their order in $S$.

**Lemma 9.** Let $(M,S)$ be an external state. Then $(M,S) \rightarrow (M',S')$ with a non-$\nu$-step if $(M,S)^\nu \rightarrow (M',S')^\nu$. If $(M,S) \rightarrow (M',S')$ with a $\nu$-step, then $(M,S)^\nu \rightarrow (M',S')^\nu$.

Proof: Let $E[R] = M$ with $E$ a regular evaluation context and $R$ the redex fired in the reduction. Then there is a $\nu$-context $E'$ such that $E''[R] = (M',S')^\nu$, and such that $E''$ differs from $E$ by having $\nu$’s in place of $\nu r$’s. Moreover if $S'$ is the sequence of $r \varepsilon V$ obtained from each context $\nu r \varepsilon V$ building $E''$, starting from the hole up, we see that $S' = S$ (all this is easily shown by induction on $E$). In particular the first $r \varepsilon V$ in $S$ for any given $r$ is characterized by having $E'' = E''[\nu r \varepsilon V, E''^r]$ with $r \notin PR(E'')$. In fact such construction can also be reversed: every $\nu$-context $E$ such that $(M,S)^\nu = F[R]$ with $R$ a redex turns to a regular context $F''$ by stripping all $\nu$’s, so both sides of the equivalence are valid.

B. Types and effects into Monads

**Lemma 11.** We have the following properties on the terms introduced in Figure 5.

- If $S : P_{e,f}$, $V : X_r$ is a value (so $(V)$ is an $(r)$-store) and $M : T_{e,f}(A)$ then $\pi_r V M S \Rightarrow (S', U)$ if $M(S + (V)) \Rightarrow (S', U)$ for some $V' : X_r$.
- If $S : P_{e,f}$, $M : T_e(A)$ then $cast_{e,f} MS \Rightarrow (S', U)$ if $M[S_e] \Rightarrow (S', U)$ and $S'_{[f\Re]} = S'_{[f\Re]}$.
- If $S : P_{e,f}$, $M : T_e(A)$, $x : A \vdash N : T_f(B)$, then $(\text{let}_{e,f} x = M) \in N(S + (V)) \Rightarrow (S', U)$ iff $MS[e] \Rightarrow (T, V)$ and $N[V/x] \Rightarrow (T, V)$.

Proof: For $\pi_r V M S$, it reduces to $F(M(S + (V)))$ where $F = \lambda x (M) \cdot (\pi_r x M) s_1, v$. This reduces to some $F(S' + (V'))$ if $M(S + (V))$ evaluates to that value, then $F(S' + (V'))$ evaluates to that value, and then $F(S' + (V')) \Rightarrow (S', U)$.

cast_{e,f} MS follows similarly: it reduces to $(\lambda x (M) \cdot cast_{e,f} S, v)(MS[e])$, which goes to $(S'_e + S'_{[f\Re]}) \Rightarrow (S'_e, U)$.

The third point comines the expected behaviour of the implemented let construct with the one for cast. Indeed $(\text{let}_{e,f} x = M) \Rightarrow (\lambda x (S), cast_{e,f} S, v)(M S)$, which by the above reduces to $cast_{e,f} N(V/x) \Rightarrow (S'_e, U)$, and it will then reduce to $\Rightarrow (S'_e, U)$ iff $N[V/x] \Rightarrow (T, V)$.

**Proposition 12.** $R^o$ is solvable if the stratification condition $R^o \vdash$ holds.

Proof: Let $\Xi$ denote either $R \vdash A$ or $R \vdash \emptyset$, and let $[\Xi]$ be defined by $[R \vdash | := \bigcup_{r \in dom(R)} [1 + \pi_r r])$ and $[R \vdash \emptyset] := [R \vdash |] + [\emptyset]$, with the size $|$, defined on types as usual. Resoning by induction on $[\Xi]$ we show that $\Xi$ is derivable iff $R^o$ is solvable and $FV(A) \subseteq dom(R^o)$, if $A$ is present. Let us reason by cases on $\Xi$.

- $\Xi = R \vdash 1$: inductive hypothesis yields that $R \vdash R^o$ solvable. As $FV(1) = \emptyset$ and $R \vdash R^o$ iff $R = \emptyset$ we are done.
- $\Xi = R \vdash A \vdash B$: $\Xi$ is derivable iff $R \vdash R \vdash B$ and $e \subseteq dom(R)$, with the latter equivalent to $\forall r \in e : X_r \in dom(R^o)$. Then inductive hypothesis gives that $\Xi$ is derivable iff $R^o$ is solvable and $FV((A \Rightarrow B)^o) = FV(A) \cup FV(B)$ and $X_r \in dom(R^o)$.
- $\Xi = R \vdash \emptyset$: if $R = \emptyset$ there is nothing to prove, as both ends of the equivalence are always true. Otherwise suppose first that $R \vdash \emptyset$ is derivable, so that $R = R_0, r : A$ and $R_0 \vdash A$. By inductive hypothesis (as $[R_0, r : A \vdash | = [R_0 \vdash A] + 1$) $R_0$ is solvable and $FV(A^o) \subseteq dom(R_0^o)$, which entails that $\sigma_{R_0}(A^o)$ is closed. Assigning such a value to $X_r$ gives then a solution for $R^o$.

Let us start on the other hand with $R^o$ solvable. Take then a region $r \in dom(R)$ so that $\sigma_{R^o}(R^o(r))$ is maximal in size, and consider $R_0$ to be $R$ restricted to $dom(R) \backslash \{r\}$. Now we see that $X_r \notin FV(R^o(s))$ for all $s \in dom(R)$: if it was the case, then $\sigma_{R^o}(R^o(s))$ would contain $\sigma_{R^o}(r^o)$ as a proper subformula, which would violate maximality. This entails on one side that $\sigma_{R^o}$ provides a solution also for $R_0^o$, restricted to its domain; on the other that $FV(R^o(r)) \subseteq dom(R^o) \backslash \{X_r \} = dom(R_0^o)$. By inductive hypothesis we conclude that $R_0 \vdash R^o$, from which $R \vdash \emptyset$ can be inferred.

**Proposition 13.** $\Gamma^0(x) := (\Gamma(x))^o$. Then:

- if $R : \Gamma \vdash M : A, e \vdash M' \Gamma \vdash M' : T_e(A)^{o}$ is derivable in $\Lambda \times$ modulo $\equiv_{R^o}$; in particular programs $M, e : A, \emptyset$ are mapped to closed terms of type $A^o$.
- if $R : \Gamma \vdash \Lambda \times M : A, e \vdash M' \Gamma \vdash V : A, \emptyset \vdash [V']$ then $R : \Gamma \vdash M(V/x) : A, e \vdash M'(V'/x)$.

Proof: Straightforward induction on the derivation, using the derived typing rules shown in Figure 5. The
equivalence $\equiv_{\mathbb{R}}$ is used with set and get, to equate $A^c$ to $X$, if $r : A \in R$. For the point about substitution, it suffices to see that replacing all axioms $x : A \vdash x : A \rightarrow [x]$ with $\vdash V : A \rightarrow [V]$ gives exactly what needed in the end.

**Theorem 14.** If $R \vdash M, e : A, \theta \rightarrow M'$ is a $\Lambda_{\mathbb{R}}$ program with its associated $M'$ term, then $M$ evaluates to the value $V : e$ if $M' \rightarrow^* V'$ with $V \rightarrow [V]$.

**Proof:** Given a $\Lambda_{\mathbb{R}}$ store $S$ (typed according to $R$) and a set of regions $e \subseteq |\text{dom}(S)|$, there is a unique partition of $S = S_1, S_2$ so that $|\text{dom}(S_1)| = e$ and $S_1$ is made by singletons (in a way, $\text{dom}(S_1)$ is $e$). Let us define $t_e(S)$ as the translation of such an $S_1$ into a $\Lambda_e$-store: for each $r = V_r \in S_1$ ($V_r$ is uniquely determined by $r$) we have that $R \vdash V_r : T(r), \theta \rightarrow [V_r]$ for some $\Lambda_e$-value $V_r' ; R(r)^o = X_r$, so we define $t_e(S)$ as $\langle V_r', r \in e \rangle$. Clearly $t_e(\emptyset) = \emptyset$; moreover if $e \subseteq f$ then $t_f(S) = t_e(S) \upharpoonright f$.

Now we will prove that every $\Lambda_{\mathbb{R}}$ state $M, S$ with $R \vdash M ; A, e \rightarrow M'$ evaluates to a result $V, S'$ iff $M', t_e(S) \rightarrow$ evaluates to $(T, V')$ with $T = t_e(S')$ and $R \vdash V : A, \theta \rightarrow [V']$ (recall that by the condition imposed on states $e \subseteq |\text{dom}(S)|$). In particular for a program $M, e$ this amounts to saying that $M$ evaluates to $V$ iff $M' \upharpoonright_e \rightarrow (\emptyset, V', V')$ with $V \rightarrow [V']$, which is what requested.

**Proof of only if:** We will proceed by induction on the length of the reduction of $M, S$: for the base case in which $M$ is already a value then the only difference with the expected result is that the type derivation might have added effects in the end, i.e. $e \neq \emptyset$. Supposing no constructive rules adding effects are used, this amounts to having $M' = \text{cast}_{\theta, e}[V']$ with $M : A, \theta \rightarrow [V']$. Then $M', t_e(S) \rightarrow (t_e(S), V')$ which is what required.

For the inductive step we again settle first the case where the last rule of the derivation of $M$ just adds effects, $M' = \text{cast}_{\theta, e}[M'']$ with $R \vdash M : A, e \rightarrow M''$. Then Lemma 11 reduces the problem to $M \rightarrow M''$, with the same starting term as before. Now we go on depending on the shape of $M$.

\[
M = \text{let}_{e_1, e_2, e_3} f \text{ be } N_1 \text{ in let}_{e_2, e_3} a \text{ be } N_2 \text{ in fa} . \]

As $M, S$ evaluates, then $N_1, S \rightarrow_\lambda \lambda x.N_3, S''$, $N_2, S'' \rightarrow U, S'''$ and $N_3 \{U/x\}, S''' \rightarrow V, S'$, all with reductions strictly shorter than the global one (as the sum must include also the $\beta$-reduction). So inductive hypothesis gives $N_1, t_e(S) \rightarrow (t_e(S''), \lambda x.N_3')$ with $N_3 \rightarrow N_3'$ and $N_2, t_e(S''') \rightarrow \star (t_e(S'''), \lambda U . [U])$ with $U \rightarrow [U]$. By Proposition 13 $N_3 \{U/x\} \rightarrow N_3' \{U'/x\}$. so a third application of inductive hypothesis yields $N_3', \{U'/x\} t_e(S''') \rightarrow (t_e(S'''), V')$ with $V \rightarrow [V']$. Applying two times Lemma 11 gives what needed.

\[
M = \text{let}_{e_1, e_2} f \text{ be } N_1 \text{ in let}_{e_2} a \text{ be } N_2 \text{ in fa} . \]

We will have a reduction $N_1, S \rightarrow_\lambda V_1, S''$, $N_2 \rightarrow V_2, S'''$. A value for $r \in V_2, S'$. A value for $r$ must remain in the store because of Lemma 3, so that we have the final step $r, V, r \rightarrow V, S', V', S''$. By inductive hypothesis we get $N_1, t_e(S) \rightarrow (t_e(S''), \lambda x.N_3')$ and $N_2, t_e(S''') \rightarrow \star (t_e(S'''), \lambda U . [U])$ with $U \rightarrow [U]$. Then applying two times Lemma 11 yields first that $N_1, \{U'/x\} t_e(S'') \rightarrow (t_e(S''), V')$ and then that the let construction of $M$ gives that $M', t_e(S) \rightarrow (t_e(S'), V')$, all with $V \rightarrow [V']$.

\[
M = \text{set}(r, N) \quad (N \rightarrow N') \text{ then } N, S \rightarrow U_1, S'' \quad \text{and with a further step } M, S'' \rightarrow (r \equiv U_1, T'') \text{ (Lemma 3)}. \]

By inductive hypothesis we just obtain $N', t_e(S) \rightarrow (t_e(r), T'''') + \{U_2, U_1', \} \text{ with } U_1 \rightarrow U_1'$. Now as $s_1 U_1' U_2' \rightarrow \{U_1', \} \text{ Lemma 11 for the let construction yields } M', t_e(S) = (\text{let}_{e_1, r, v \text{ be } N'} \text{ in } s_1 v) t_e(S) \rightarrow (t_e(r), T'''') + \{U_1', \} \rightarrow (t_e(S'), \{\})$, and $(\emptyset) \rightarrow (\emptyset)$.

\[
M = \text{get}(r) ; \quad \text{then } S = r \equiv V, T \text{ (with } V \rightarrow [V']) \text{ and } M, S \rightarrow V, S' \text{ and } M', t_e(S') \rightarrow \mathbb{G} V' \rightarrow (V', V'') \text{ and we are done.} \]

**Proof of if:** In fact the opposite direction retraces exactly the same steps, only doing an induction on the length of the reduction of $M'$ to $S$ using the opposite directions of the equivalences of Lemma 11.

**C. Types and effects into linear logic**

**Lemma 19.** In untyped LL (and so also in presence of recursive types) one has the following properties.

- $\vdash$ is strongly normalizing;
- $\rightarrow$ is confluent;
- $\pi$ is strongly normalizing for $\rightarrow$ if it is weakly so.

**Proof:** The reduction $\vdash$ is strongly normalizing by the finite developments theorem, which with equivalences has been shown in [14]. It follows with a quick check that $\rightarrow$ is confluent. Now $\pi$ and $e$ are trivially strongly confluent, and the three strongly commute with one another (e.g. $\pi \cdot \vdash \subseteq \vdash \cdot e$), so the three together are confluent.

For strong normalization, there is a proof with a slightly different syntax in.

**D. De Carvalho, M. Pagani, and L. Tortora de Falco, “A semantic measure of the execution time in linear logic,” 2008, to appear on Theoretical Computer Science.**

One can alternatively show it by introducing a counter increasing at every $m$ or $e$ reduction, which cannot decrease at $s$ ones. Here one proves that reduction is still confluent, and conclude: the counter of the normal form bounds the number of total $e$ or $m$ steps that can be done, and there cannot be an infinite number of $s$ steps either.

**Lemma 22 (substitution).**

\[
\begin{array}{c}
V \quad \frac{e}{\rightarrow} & (M[V/x])
\end{array}
\]

**Proof (sketch):** After noticing that values are always boxes, the proof follows by induction. Equivalence on contractions commuting with box borders are needed to make the trailing contractions enter boxes in the $\lambda x.M$ case.

**Theorem 23 (Simulation).** Let $M, S$ be an external state. Then:

- if $M, S \rightarrow V, e$ is a value, then $(V, e)$ is in 0-depth normal form.
- if $M, S \rightarrow M', S'$ with a non-$\nu$-step then $(M, S)^* \rightarrow (M', S')^*$ with exactly one dereliction on box step;
- if $M, S \rightarrow M', S'$ with a $\nu$-step, then $(M, S)^* = (M', S')^*$. 

Proof: The first and the last points are straightforward from the definition. For the second we show that if \( M \rightarrow N \) then \( M^\bullet \xrightarrow{\perp} N^\bullet \) with exactly one dereliction on box reduction, and conclude by Lemma 9.

First notice that \( \nu \)-evaluation contexts translate to proof net contexts with the hole at depth 0. Moreover we can prove that if \( r \notin PR(F[\ ]\ ) \) then the context \( (\nu r \leftarrow V.F[\ ]\ ))^\bullet \) is of the form

![Diagram](image)

i.e. the translation of \( V \) is directly available to the hole. This follows from the definition of \( \nu \)-evaluation contexts: all the parts of the term the during the translation would be on top (or on the left) of the hole are necessarily values. In particular the effect \( r \) is present in them only as a wire (via the \( \equiv \) relation). The only exception would be another \( \nu r \leftarrow U \), which would interrupt it, but it is explicitly forbidden by \( r \notin PR(F) \). We can thus suppose such part of the net when carrying out the cases.

Indeed it suffices now to reduce each case separately, employing Lemma 22 for the \((\lambda x.M)V\) reduction.

**Theorem 24.** If \((M,S)^\bullet \xrightarrow{\perp} \pi\), with \( \pi \) a 0-depth normal form, then there is a value \( V \) such that \( M, S \rightarrow V, \varepsilon \) and \( \pi = V^\bullet \).

Proof: By Lemma 19 \((M,S)^\bullet \) is strongly normalizing for the 0-depth reduction we employ. So in particular applying Theorem 23 we obtain that \((M,S)^\bullet \) normalizes to \( V^\bullet \) (as \( M, S \) cannot make infinite \( \nu \)-steps). Unicity of 0-depth normal form entails \( \pi = V^\bullet \).