A calculus of expandable stores
Hugo Herbelin, Étienne Miquey

To cite this version:

HAL Id: hal-02557823
https://hal.archives-ouvertes.fr/hal-02557823v2
Submitted on 29 Jun 2020

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.
A calculus of expandable stores
Continuation-and-environment-passing style translations

Hugo Herbelin
INRIA, IRIF (CNRS)
Université Paris-Diderot
France
hugo.herbelin@inria.fr

Étienne Miquey
CNRS, LSV, INRIA
ÉNS Paris-Saclay
France
emiquey@lsv.fr

Abstract
The call-by-need evaluation strategy for the \(\lambda\)-calculus is an evaluation strategy that lazily evaluates arguments only if needed, and if so, shares computations across all places where it is needed. To implement this evaluation strategy, abstract machines require some form of global environment. While abstract machines usually lead to a better understanding of the flow of control during the execution, facilitating in particular the definition of continuation-passing style translations, the case of machines with global environments turns out to be much more subtle.

The main purpose of this paper is to understand how to type a continuation-and-environment-passing style translation, that is to say how to soundly translate in continuation-passing style a calculus with global environment. To this end, we introduce \(F_\Upsilon\), a generic calculus to define the target of such translations. In particular, \(F_\Upsilon\) features a data type for typed stores and a mechanism of explicit coercions witnessing store extensions along environment-passing style translations. On the logical side, this broadly amounts to a Kripke forcing-like translation mixed with a negative translation (for the continuation-passing part). Since \(F_\Upsilon\) allows for the definition of such translations for different source calculi (call-by-need, call-by-name, call-by-value) with different type systems (simple types, system F), we claim that it precisely captures the computational content of continuation-and-environment-passing style translations.

Keywords  global environment, abstract machines, CPS translations, Kripke forcing, lazy evaluation, de Bruijn indices

This paper is an extended version of a conference paper available at: https://dx.doi.org/10.1145/3373718.3394792. Due to the original space constraints, most of the proof are given in appendices.

Introduction
Variable binding is one of these notions that seems really natural on the surface (especially to humans that have some habit of working with variables), while being much more subtle to define formally (computer scientists are well aware of that fact). In particular, the way programming languages handle bindings and environments has evolved a lot since the emergence of computers.

In the realm of the \(\lambda\)-calculus, most of the standard abstract machines evaluate terms within a local environment by using closures (e.g. Landin’s SECD machine [20], the Krivine Abstract Machine [18], etc.). Nonetheless, these machines do not allow the use of evaluation strategies such as call-by-need that require the ability to share computations. Instead, lazy evaluation strategies require abstract machines with a global environment [3, 33]. Such machines demand in particular to explicitly handle addresses (as in the Lazy Krivine [21]) or a renaming process (as in the Milner Abstract Machine [2]).

Continuation-passing style translations, that where first introduced by Sussman and Steel [35], constitute a great tool when it comes to studying operational semantics of calculi: by making explicit the order in which reduction steps are computed, CPS translations indirectly specify an evaluation strategy for the translated calculus. On a logical aspect, they are also very informative insofar as the translation they induce at the level of types mostly amounts to a syntactic model allowing to transfer logical properties (coherence, normalization) from the target calculus [6]. For instance, standard CPS translations are known to correspond to embeddings of classical logic into intuitionistic logic [14, 28].

If there exists a wide literature on (typed) CPS translations for call-by-name or call-by-value calculi [4, 13, 32], the situation is quite different for lazily evaluated calculi. Even though such strategies are used in practice, for instance in Haskell or Coq, no typed CPS allows to take them into account. The main difficulty in deriving a CPS translation for a call-by-need calculus is related to the necessity of a global environment: since the evaluation of terms is shared, the CPS translation actually has to be combined with an environment-passing style transformation. Also, since environments can grow during the execution, such a translation needs to handle this extensibility. Last but not least, the use of a global environment requires tackling problems related to the uniqueness of names.

This paper aims at bridging the gap between CPS translations and calculi with a global environment. Our main result is the introduction of \(F_\Upsilon\), a highly parametric calculus suitable as the target of several typed continuation-and-environment-passing style (CEPS) translations, taking into account source
calculi with different evaluation strategies or type systems. It features the architecture to manipulate typed expandable stores, whose elements are accessed via the careful use of de Bruijn levels. Store extensions are computationally witnessed by explicit coercions which allow us to update de Bruijn levels along the execution. In some sense, we make explicit the rewriting system underlying store management, in a similar way as explicit substitution calculi, as e.g. in [1], make explicit the computational structure of substitution.

Our results improve over the state-of-the-art in a previous paper by Ariola et al., in which they define an untyped CPS translation for a call-by-need calculus with control [5]. Besides just being able to type this translation, our setting solves a subtle issue of renaming in their translation. The de Bruijn presentation used in this paper formally addresses this issue by avoiding names altogether. Most importantly, this paper shows that a de Bruijn version of [5] is even possible. This fact was not obvious from the previous work, which depends deeply on name-based binding and lookup operations on an environment. Insofar as name-based environments are neither very practical nor efficient for most applications, demonstrating how the system of [5] can be statically compiled to numeric offsets into an ordered environment is a step forward toward a practical implementation strategy for call-by-need with control effects.

Let us begin this paper with a comprehensive introduction to abstract machines with global environments. This introduction shall then lead us to analyzing the technicalities that CEPS translations give rise to (Sec. 2) before introducing $F_1$ more in depth (Sec. 3), and illustrating its features by defining different typed CEPS (Sec. 4). We shall conclude with further perspectives arising from this work (Sec. 5).

1 Computing with global environments

In this section, we recall and introduce several calculi and abstract machines that have in common that they use a form of global environments to perform substitutions. As such, what we call global environments somewhat behave like (lazy) explicit substitutions or particular stores. To draw the comparison with the usual notions of stores and environments, two things should be observed. First, the usual notion of store refers to a structure of list that is fully mutable, in the sense that its cells can be updated at any time and thus values might be replaced. In the following examples, cells might be updated but only to replace an unevaluated term by its corresponding value. Second, the usual notion of environment designates a structure in which variables are bound to closures made of a term and an environment. In particular, terms and environments are duplicated, i.e. sharing is not allowed. Such a structure resembles a tree whose nodes are decorated by terms, as opposed to a machinery allowing sharing (like ours), whose underlying structure is broadly a directed acyclic graph.

1.1 The Milner Abstract Machine

Even though it is far from being the most well-known abstract machine, the Milner Abstract Machine (MAM) is probably the easiest presentation of an abstract machine for the (call-by-name) $\lambda$-calculus that uses a single global environment [2, 3]. A state of this machine is made of three components:

- a code $\tilde{t}$ for a term $t$ which is not considered up to $\alpha$-conversion$^1$,
- a stack $\pi$ which contains the arguments of the current code, that is to say a stack of codes,
- a global environment $\tau$, which is a list storing the (delayed) substitutions generated by the redexes encountered so far.

Formally, this corresponds to the following syntax:

\[
\begin{align*}
\text{Terms} & \quad t, u ::= x \mid tu \mid \lambda x.t \\
\text{Stacks} & \quad \pi ::= \varepsilon \mid \tilde{t} \cdot \pi \\
\text{Environments} & \quad \tau ::= \varepsilon \mid \tau[x := t]
\end{align*}
\]

The machine is given in Figure 1, where we follow the notations of Accattoli and Barras [3] to denote reduction rules: we write $\rightarrow_\beta$ for the $\beta$-reduction rule, $\rightarrow_s$ for the rule which somehow performs a substitution, and $\rightarrow_c$ for the commutative transition. By considering invariants of the machine, one can easily prove that the Milner Abstract Machine soundly implements the call-by-name evaluation strategy for the $\lambda$-calculus [2].

It is worth noting that the soundness of the execution crucially relies on the uniqueness of names in the environment. Incidentally, this requires the possibility of an on-the-fly $\alpha$-renaming process. Executing twice a term binding a variable $x$ in different contexts (say $(\lambda x.t)u$ and $(\lambda x.t)v$) could indeed result in linking two different terms to the same name in the environment. This is avoided by asking in the $\rightarrow_s$ rule that if $x$ is linked to some term $t$ in the environment $\tau$, accessing $x$ results in executing a code $\tilde{t}^x$ that is $\alpha$-equivalent to $t$ and such that any bound name in $\tilde{t}^x$ is fresh with respect to every other names in the term, in the current stack $\pi$ and in the environment $\tau$. In the sequel, we will explicitly use de Bruijn levels to handle this kind of issues.

On the contrary, most of the abstract machines of the literature implementing the call-by-name or call-by-value evaluation strategies for the $\lambda$-calculus use many local environments (e.g. the Krivine Abstract Machine [18], Landin’s SECD machine [20], Felleisen and Friedman’s CEK machine [12], Leroy’s ZINC machine [22]). In these machines, the concept of closure, that is a term taken with an environment under which it can be seen as a closed term, plays a central part. As an example, we give in Figure 1 the definition of the Krivine

\footnote{In other words, we assume implicit $\alpha$-conversion for terms, which stand for the equivalence class of raw syntactic codes up to $\alpha$-conversion.}
A calculus of expandable stores
Hugo Herbelin and Étienne Miquey

\[
\bar{\mu} \mu \pi \tau \rightarrow_c \bar{\mu} \mu \cdot \pi \cdot \tau
\]
\[
\lambda x. \bar{\mu} \pi \cdot \mu \cdot \tau \rightarrow_\beta \bar{\mu} \mu \cdot \pi \cdot \pi [x := \bar{\mu}]
\]
\[
x \pi \tau [x := \bar{\mu}] \rightarrow_\delta \bar{\mu} \mu \cdot \pi \cdot \pi [x := \bar{\mu}] r'
\]
(a) Milner Abstract Machine

\[
\bar{\mu} \pi \cdot \tau \rightarrow_c \bar{\mu} \pi \cdot \tau \cdot D
\]
\[
\lambda x. \bar{\mu} \pi \cdot \tau \cdot D \rightarrow_\beta \bar{\mu} \mu \cdot \pi \cdot \pi [x := \bar{\mu}] \cdot D
\]
\[
x \pi \tau [x := \bar{\mu}] \cdot D \rightarrow_\delta \bar{\mu} \mu \cdot \pi \cdot \pi [x := \bar{\mu}] \cdot D
\]
(b) Krivine Abstract Machine

Figure 1. MAM vs KAM

Abstract Machine (KAM), whose syntax is given by:

| Terms       | $t, u ::= x \mid tu \mid \lambda x. t$ |
| Stacks      | $S ::= \varepsilon \mid (E, E) \cdot S$ |
| Environments| $E ::= \varepsilon \mid E[x := (t, E')]$ |

In comparison with the MAM, it is interesting to observe that the definitions of environments and closures are mutually recursive. Notably, it presents the advantage that the locality of environments makes the $\alpha$-renaming process useless. While this design with a local environment presents some benefits over machines with global ones (among other things in terms of complexity [3]), it has the drawback of being incompatible with lazy evaluation strategies which require to share computations and memory bindings.

1.2 The Milner Abstract Machine By-Need

The call-by-need evaluation strategy of the $\lambda$-calculus evaluates arguments of functions only when needed, and, when needed, shares their evaluations across all places where the argument is required. Therefore, abstract machines implementing the call-by-need evaluation have to allow for some kind of global environment in order to share computations [8, 33]. The Milner Abstract Machine can easily be modified to obtain such an abstract machine, called the Milner Abstract machine by-need (MAD) [2]. The main idea consists in adding a *dump*, which is used whenever the code is some variable $x$ within an environment $\tau_1[x := t] \tau_2$: the machine momentarily focuses on the evaluation of $t$ in $\tau_1$ while saving the current stack together with the rest of the environment $\tau_2$ and the variable $x$ on the dump. Then, if this computation eventually produces a value $v$ in an environment $\tau'_1$, the machine goes back to the former computation within the updated environment $\tau'_1[x := v] \tau_2$. The machine is given Figure 2, where environments $\tau$ and stacks $\pi$ are defined as in the MAM, and where dumps are given by the following grammar:

\[
D ::= \varepsilon \mid (x, \pi, \tau) :: D
\]

Alternatively, one could also extend the syntax of stacks in order to add a constructor $h(x, \tau) \cdot \pi$ that holds the entries

Figure 2. The Milner Abstract machine by-need

that would otherwise go to the dump. The modified reduction rules could then be given by:

\[
x \pi \tau [x := \bar{\mu}] r' \rightarrow_\delta \bar{\mu} h(x, \tau') \cdot \pi \cdot \tau
\]
\[
\bar{\mu} h(x, \tau') \cdot \pi \cdot \tau \rightarrow_\delta \bar{\mu} h(x, \tau') \cdot \pi \cdot \tau
\]

This is for instance the approach chosen in Sestoft’s machine for lazy evaluation [33] or in Accattoli, Barenbaum and Mazza’s **Merged MAD** [2]. For a more detailed introduction to the subtleties related to the implementation of lazy abstract machines or a comparison between the different approaches (including Crégut’s lazy KAM [8] and Sestoft’s abstract machine), we refer the reader to Accattoli, Barenbaum and Mazza’s paper [2].

1.3 The $\bar{\lambda}\mu\bar{\mu}$-calculus with global environments

Let us briefly explain how the MAM could be expressed under the shape of a sequent calculus. We shall dwell on a lambda calculus extended with a global environment [9]. The syntax of the usual $\bar{\lambda}\mu\bar{\mu}$-calculus is divided in three categories: terms, which represent programs; evaluation contexts (or co-terms); commands, which are pairs of a term and a context representing a system that contains both the program and its environment. Then, as in the MAM, we extend the syntax with environments made of delayed substitutions. The notion of evaluation context is a generalization of the notion of stacks where $\bar{j}x.c$ can be read as a context let $x = \bar{x}$ in $c$. As for terms, the $\mu$ operator comes from Parigot’s $\bar{\lambda}\cdot\mu$-calculus [30]: $\mu x$ binds a context to a context variable $x$ in the same way $\bar{j}x$ binds a proof to some proof variable $x$. In particular, as we shall see now, it allows terms to capture evaluation contexts and as such plays the role of a control operator.

The syntax and reduction rules are given in Figure 3, in which terms and contexts are implicitly considered up to $\alpha$-conversion in order to preserve the uniqueness of names in the environment. It is easy to see that on its intuitionistic fragment (that is without the classical control $\mu a$), this calculus behaves exactly as the MAM\(^2\). As per [9], we restrict the

\[^2\text{The reader unfamiliar with the$\bar{\lambda}\mu\bar{\mu}$-calculus might be puzzled by the absence of a syntactic construction for the application of proof terms. Intuitively, the usual application $tu$ of the $\lambda$-calculus is replaced by the application of the proof $t$ to a stack of the shape $u :: E$. The usual application can be recovered through the following shorthand: $tu \triangleq \mu x. (r || u \cdot \alpha)$. It is then an easy exercise to show that the MAM can be simulated within the$\bar{\lambda}\mu\bar{\mu}$-calculus with environments, see Appendix A.}\]
A calculus of expandable stores

Hugo Herbelin and Étienne Miquey

Values

\[ V ::= \lambda x.t \]

Terms

\[ t, u ::= V \mid x \mid \mu \alpha.c \]

Co-values

\[ E ::= t \cdot E \mid \alpha \]

Contexts

\[ e ::= E \mid \mu x.c \]

Environments

\[ \tau ::= \epsilon \mid \tau[x ::= t] \mid \tau[\alpha ::= E] \]

Commands

\[ c ::= (t \circ e) \]

Closures

\[ l ::= \mu \]

---

Figure 3. By-name \( \lambda \mu \mu \)-calculus with global environments

The syntax of stacks to \( t \cdot E \) for call-by-name evaluation rather than the more general \( te \). Observe that the reduction rules for \( \mu \) is restricted to co-values, which enforces the call-by-name reduction strategy. Call-by-value is obtained by relaxing these constraints and by dually constraining the reduction of \( \bar{\mu} \) to values [9]. Note in particular our formulation of the (Beta) rule: by delegating the process of substitution of the argument to the \( \mu \) rule, it captures what is common to call-by-name \( \beta \) and call-by-value \( \bar{\beta} \), leaving the role of choosing between call-by-name and call-by-value to the rules \( \mu \) and \( \bar{\mu} \). As for the typing rules, they will be easy to deduce from the type system we will introduce for the \( \lambda [l \nu r \star] \)-calculus in the next section, we thus let them as an exercise for the reader.

### 1.4 The \( \lambda [l \nu r \star] \)-calculus

Although the MAD arguably provides us with the easiest presentation of a lazy abstract machine, it does not directly lead to an operational semantics for control operators (or, equivalently, to the definition of a continuation-passing style translation). While the addition to the KAM of the call/cc operator, which allows to capture the current stack into a continuation, is very natural, it is less obvious to determine its behavior in the MAD. Especially, it is not clear \textit{a priori} how control operators should handle the global environment and the dump. More generally, the problem of soundly defining a CPS translation for the call-by-need \( \lambda \tau \)-calculus turns out to be trickier than the call-by-value and call-by-name cases. In particular, a first attempt by Okasaki, Lee, Tarditi [29] was later shown to be non-normalizing on simply-typed terms [5].

In the latter, Ariola et al. apply the methodology of Danvy’s semantics artifacts to mechanically derive a continuation-passing style translation from a sequent calculus presentation of classical call-by-need. Starting from a specific evaluation strategy for the \( \lambda \mu \mu \)-calculus, they finally obtain a small-step sequent calculus, the \( \lambda [l \nu r \star] \)-calculus, from which they get an untyped CPS translation almost for free.\(^3\) The \( \lambda [l \nu r \star] \)-calculus can be understood as a refinement of the \( \lambda \mu \mu \)-calculus with explicit environments (see Section 1.3). Before introducing our variant of this calculus using de Bruijn levels, let us first stick to names in order to emphasize the main differences between both calculi, which are:

- a new binder, written \( \tilde{\mu} [x].(x \parallel F) \tau \), which is used to implement laziness as we shall explain;
- a subdivision of values (resp. co-values) into two categories of weak and strong values (resp. catchable and forcing contexts).

Strong values correspond to values strictly speaking. Weak values include variables, which force the evaluation of terms to which they refer into shared strong value. Their evaluation may require capturing a continuation. Dually, catchable contexts are co-values strictly speaking, while forcing contexts are contexts eagerly asking for a strong value, which may trigger the evaluation of terms lazily stored. In detail, the lazy evaluation of terms allows for the following reduction:

\[ (\mu \alpha.c \parallel \tilde{\mu} x.c) \rightarrow c'[x ::= \mu \alpha.c] \]

In this case, the term \( \mu \alpha.c \) is left unevaluated (“frozen”) in the environment, until possibly reaching a command in which the variable \( x \) is needed. When evaluation reaches a command of the form \( \langle x \parallel F \rangle \tau[x ::= \mu \alpha.c] \tau' \), the binding is opened and the term is evaluated in front of the context written \( \tilde{\mu} x.[x \parallel F] \tau' \):

\[ \langle x \parallel F \rangle \tau[x ::= \mu \alpha.c] \tau' \rightarrow (\mu \alpha.c \parallel \tilde{\mu} x.[x \parallel F] \tau') \tau \]

The reader can think of the previous rule as the “defrosting” operation of the frozen term \( \mu \alpha.c \) this term is evaluated in the prefix of the environment \( \tau \) which predates it, in front of the context \( \tilde{\mu} x.[x \parallel F] \tau' \) where the \( \tilde{\mu} x \) binder is waiting for a value. This context keeps trace of the part of the environment \( \tau' \) that was originally located after the binding \( [x ::= \ldots] \). This way, if a value \( V \) is indeed furnished for the binder \( \tilde{\mu} x \), the original command \( \langle x \parallel F \rangle \) is evaluated in the updated full environment:

\[ \langle V \parallel \tilde{\mu} x.[x \parallel F] \tau' \rangle \tau \rightarrow (\mu \alpha.c \parallel \tilde{\mu} x.[x \parallel F] \tau') \tau \]

The brackets in \( \tilde{\mu} x.[x \parallel F] \tau' \) are used to express the fact that the variable \( x \) is forced at top-level.\(^4\) Especially, it allows us to keep the standard redex at the top of a command and avoids searching through the meta-context for work to be done. As such, reduction rules of the \( \lambda [l \nu r \star] \)-calculus are close to the ones of the MAD.\(^5\)

---

\(^3\)See Appendix B.1 for the original definition of the \( \lambda [l \nu r \star] \)-calculus and the corresponding untyped CPS.

\(^4\)Unlike meta-contexts of the shape \( \tilde{\mu} x. C[\langle x \parallel F \rangle] \) in the \( \lambda [l \nu r] \)-calculus, see [5].

\(^5\)In fact, it is an easy exercise to simulate the MAD within the \( \lambda [l \nu r \star] \)-calculus. We outline this construction in Appendix A.
A calculus of expandable stores
Hugo Herbelin and Étienne Miquey

Last but not least, the different syntactic categories can be understood as the different levels of alternation in a context-free abstract machine (see [5]): the priority is first given to contexts at level e (lazy storage of terms), then to terms at level t (evaluation of μα into values), then back to contexts at level E and so on until level v. These different categories are directly reflected in the definition of the untyped continuation-passing style defined in [5] (see Appendix B.1), and will thus be involved in the definition of our typed translation as well.

1.5 De Bruijn levels
Ariola et al.’s presentation of the \( \Lambda_{[\text{ℓ} \tau \mu \alpha]^*} \)-calculus deeply relies on the assumption that names of variable are unique and thus on the possibility of performing \( \alpha \)-conversion on-the-fly. While this assumption, which is crucial to ensure the freshness of bindings added to the environment, is straightforward in the abstract machine model, it is not possible in the CPS translation. In turn, we will use de Bruijn levels\(^7\) for variables (and co-variables) that are bound in the environment. Just as de Bruijn indices are pointers to the correct binder, de Bruijn levels are pointers to the correct cell of the environment. We use the notation \( x_i \) to denote a term variable of de Bruijn level \( i \) where \( x \) is a fixed name whose sole purpose is to remind that the variable is binding terms. For binders of evaluation contexts, we similarly use de Bruijn levels, but with variables of the form \( α_i \), where, again, \( α \) is a fixed name whose sole purpose is to remind that the variable is binding evaluation contexts, and the relevant information is the index \( i \). The corresponding syntax is given in Figure 4. Note that typing rules for binders include a possible weakening of the context. In particular, giving a meaning to de Bruijn levels requires the knowledge of the length of the current context.

As the environment can be dynamically extended during the execution, the location of a term in the environment and the corresponding pointer are likely to evolve (monotonically). Therefore, we need to be able to update de Bruijn levels within terms (contexts, etc.). To this end, we define the lifted term \( ↑_i^nt \) as the term \( t \) where the free variables \( x_j \) (resp. \( α_j \)) with \( j \geq i \) have been replaced by \( x_{j+i} \) (resp. \( α_{j+i} \)). The reduction rules are given in Figure 4. Note that we choose to perform index substitutions as soon as they come, maintaining the property that \( x_n \) always refers to the \( (n+i)\text{th} \) element of the environment.

Regarding the type system, we consider nine kinds of sequents, one for typing each of the nine syntactic categories. We write them with an annotation on the \( \tau \) sign, using one of the letters \( v, V, t, F, E, e, l, c, r \).

\[
\begin{align*}
\Gamma & \vdash I & \Gamma & \vdash t : T & \Gamma & \vdash e : T^⊥ \\
\Gamma & \vdash c & \Gamma & \vdash V : T & \Gamma & \vdash E : T^⊥ \\
\Gamma & \vdash r : \Gamma' & \Gamma & \vdash v : T & \Gamma & \vdash F : T^⊥ 
\end{align*}
\]

where types and typing contexts are defined by:

\[
T, U ::= X \mid T \to U \quad \Gamma ::= \varepsilon \mid \Gamma, x : T \mid \Gamma, α : T^⊥
\]

Sequents typing values and terms are asserting a type, with the type written on the right; sequents typing contexts are expecting a type \( T \) with the type written \( T^⊥ \); sequents typing commands and closures are black boxes neither asserting nor expecting a type; sequents typing environments are instantiating a typing context.

The typing rules are given on Figure 5 where we adopt the convention that constants \( k \) and co-constants \( κ \) come with a signature \( S \) which assigns them a type. The typing rules are the same as for the named calculus [26], except for the one where indices should now match the length of the typing context. As in the named case, this type system enjoys the property of subject reduction.

**Theorem 1.1 (Subject reduction).** If \( \Gamma \vdash l \text{ and } c \rhd \rightarrow c'\tau' \) then \( \Gamma \vdash l \text{ and } c \rhd \rightarrow c'\tau' \).

\(^6\)See Appendix B.2 for more details on problems related to \( \alpha \)-conversion
\(^7\)De Bruijn levels were originally introduced as a reversed notation for de Bruijn indices [11]. While they are less common in the literature, levels have the significant benefit that variables referring to the same binder have the same name.
We shall now introduce System \(\Gamma\), we shall see, System \(\Upsilon\) A calculus of expandable stores Hugo Herbelin and Étienne Miquey

2 Towards typed CEPS translations

We shall now introduce System \(F_{\Upsilon}\), the calculus that we will use as the target of several continuation-and-environment-passing style translations. Our main objective here is to identify the core ingredients necessary to the definition of a generic target calculus, independently of the source languages we will consider afterwards. In particular, our calculus will be suitable to express translation of calculi with different evaluation strategies or different type systems. As we shall see, System \(F_{\Upsilon}\) is essentially Cardelli’s System \(F_{\omega}\) [7] extended with the necessary structure to handle typed (expandable) stores.

In order to ease the introduction of System \(F_{\Upsilon}\), we first focus on the case of the simply typed \(\Lambda_{\Upsilon}\)-calculus. We begin this section by explaining the rationale guiding the translation of types (which we only outline in this section) while taking advantage of this overview to highlight the different elements that such a translation requires.

2.1 Guidelines of the translation

Let us start by introducing step by step the intuitions guiding the definition of the translation. The main idea is that, due to the sharing of the evaluation of arguments, the environment associating terms to variables has to be passed around. Passing the environment amounts to combining the continuation-passing style translation with an environment-passing style translation. As we observed in Section 1, the environment is extensible, therefore, to anticipate extensions of the environment, Kripke style forcing has to be used too, in a way comparable to what is done in step-indexing translations. To facilitate the comprehension of the different steps, we illustrate each of them with the translation of the sequent\(^9\) \(\alpha : A, \alpha : A^\perp, b : B \tau e : C\).

Step 1 – Continuation-passing style. In a first approximation, let us look only at the continuation-passing style part of the translation of a \(\Lambda_{\Upsilon}\)-sequent. As emphasized in [5, 26], there are 6 different levels of control in the \(\Lambda_{\Upsilon}\)-calculus (corresponding to the 6 nested syntactic categories), leading to 6 mutually defined levels of interpretation. We define \(\llbracket A \rightarrow B \rrbracket_v\) for strong values as \(\llbracket A \rrbracket_v \rightarrow \llbracket B \rrbracket_v\), we define \(\llbracket A \rrbracket_F\) for forcing contexts as \(\neg \llbracket A \rrbracket\), \(\llbracket A \rrbracket_{V}\) for weak values as \(\neg \llbracket A \rrbracket_F = \llbracket A \rrbracket_{V}\), and so on until \(\llbracket A \rrbracket_v = \llbracket A \rrbracket_{\perp}\) (where we use the notations \(\downarrow A \triangleq A \rightarrow \perp\) and \(\uparrow A \triangleq \neg A\)).

As observed in the realizability interpretation [26], hypotheses from a context \(\Gamma\) of the form \(\alpha : A\) are to be translated as \(\llbracket A \rrbracket_{\perp}\) while hypotheses of the form \(A : x \rightarrow A\) are to be translated as \(\llbracket A \rrbracket_{\perp}\). Up to this point, if we denote this translation of \(\Gamma\) by \(\llbracket \Gamma \rrbracket\), in the particular case of \(\Gamma, A\) the translation is \(\llbracket \Gamma \rrbracket \rightarrow \llbracket A \rrbracket\), similarly for other levels.

Example 2.1 (Translation, step 1). Up to now, the translation taking into account the continuation-passing style of \(a : A, \alpha : A^\perp, b : B \tau e : C\) is simply:

\[
\begin{align*}
[a : A, \alpha : A^\perp, b : B \tau e : C] & = a : \llbracket A \rrbracket_{\perp}, \alpha : \llbracket A \rrbracket_{\perp}, b : \llbracket B \rrbracket_{\perp} \mapsto e : \llbracket C \rrbracket_{\perp} \\
& = a : \downarrow A_v, \alpha : \downarrow A_v, b : \downarrow B_v \mapsto e : \downarrow C_v
\end{align*}
\]

Step 2 – Environment-passing style. The continuation-passing style part being settled, the environment-passing style part should be considered. In particular, the translation of \(\Gamma, A\) is not anymore a sequent \(\llbracket \Gamma \rrbracket \rightarrow \llbracket A \rrbracket\), but instead a sequent roughly of the form \(\llbracket \Gamma \rrbracket \rightarrow \llbracket A \rrbracket\), with actually \(\llbracket \Gamma \rrbracket\) being passed around not only at the top-level of \(\llbracket A \rrbracket\), but also at each time a negation is used. We write this sequent \(\llbracket \Gamma \rrbracket \Rightarrow \llbracket A \rrbracket\) where \(\Rightarrow\) is defined by induction on \(\Gamma\) and \(A\):

\[
\begin{align*}
\llbracket \Gamma \rrbracket \Rightarrow \llbracket A \rrbracket & = \llbracket \Gamma \rrbracket \rightarrow (\llbracket \Gamma \rrbracket \Rightarrow \llbracket A \rrbracket) \rightarrow \perp \\
& = \llbracket \Gamma \rrbracket \rightarrow (\llbracket \Gamma \rrbracket \Rightarrow (\llbracket \Gamma \rrbracket \Rightarrow A) \rightarrow \perp) \rightarrow \perp \ldots
\end{align*}
\]

\(^9\)We omit de Bruijn levels for the moment and we write \(\alpha : A, b : B, \ldots\) instead of \(\alpha : T, y : U, \ldots\) for the sole purpose of easing readability.

Proof: The proof proceeds by induction on typing derivation, and is almost the same as in the case without de Bruijn levels [26, Theorem 1]. \(\square\)
Moreover, the translation of each type in $\Gamma$ should itself be abstracted over the environment at each use of a negation.

**Example 2.2** (Translation, step 2). Up to this point, the continuation-and-environment-passing style translation of $a : A, \alpha : A^4, b : B \vdash_e e : C$ is:

$$[a : A, \alpha : A^4, b : B] \vdash [e]_e : [\Gamma] \vdash [\Gamma] \vdash [\Gamma]_e A$$

$$= [a : A, \alpha : A^4] \vdash \beta [\Gamma] \vdash [\Gamma]_e A$$

where:

$$[a : A, \alpha : A^4, b : B] \vdash [e]_e : [\Gamma] \vdash [\Gamma] \vdash [\Gamma]_e A$$

$$= [a : A, \alpha : A^4] \vdash \beta [\Gamma] \vdash [\Gamma]_e A$$

**Step 3 – Extension of the environment** The environment-passing style part being settled, it remains to take into account that the environment is extensible. This is done by supporting arbitrary insertions of any term at any place in the environment. The extensibility is obtained by quantifying over all possible extensions of the environment at each level of the negation. In the realizability interpretation, this was reflected by the compatibility of realizers with any environment extension [26].

For this purpose, we use as a type system an adaptation of System $F_\varepsilon$ [7] extended with stores, defined as lists of assignations $[x := t]$. Store types, denoted by $\Upsilon$, are defined as a list of types of the form $(x : A)$ where $x$ is a name and $A$ is a (usual) type. Store types admit a subtyping notion $(\alpha)$. Each of the translations that we take into account store extensions of $a : A, \alpha : A^4, b : B \vdash e : C$ becomes:

$$[a : A, \alpha : A^4, b : B] \vdash [e]_e : [\Gamma] \vdash [\Gamma] \vdash [\Gamma]_e A$$

where:

$$[a : A, \alpha : A^4] = [a : A, \alpha : A^4] \vdash [\Gamma] \vdash [\Gamma]_e A$$

$$\vdash \beta [\Gamma] \vdash [\Gamma]_e A$$

This corresponds to the following refinement of the definition of $[\Gamma]_e A$:

$$[\Gamma]_e A = \forall \Upsilon : [\Gamma] \vdash [\Gamma]_e A$$

which is also a function mapping store types $\Upsilon$ to types in the target of the translation. Then, writing $\cdot_\Upsilon A$ for the function associating to any store type $\Upsilon$ the type $t \vdash (\forall \Upsilon : [\Gamma]_e A)$, the definition of the translation can be simply expressed by:

$$\forall \Upsilon : [\Gamma]_e A$$

Following this observation, the previous steps are successive refinements of the definition of $\Box F$:

- at step 1, $\Box F$ is $\forall Y : (F Y) \vdash \perp$,
- at step 2, $\Box F$ is $\forall Y : (F Y) \vdash \perp$,
- at step 3, $\Box F$ is $\forall Y : (F Y) \vdash \perp$,

### 3 $F_\varepsilon$: a calculus of expandable stores

#### 3.1 Core calculus

The elements necessary to properly define a continuation-and-environment passing style translation being now identified, we can formally introduce the corresponding calculus, which we dub System $F_\varepsilon$. Each of the translations that we
will introduce afterwards will rely on a target calculus defined as a particular instance of this system. The structure of these translations can be divided in three blocks:

1. A source calculus and its type system. For the moment, we will only consider simply-typed λ-calculi\(^\text{10}\) to ease notations, we shall explain afterwards in Section 4.3 how this scales to System F.

2. A syntax for stores and coercions. In this paper, we will simply consider lists and list inclusions, but one could also contemplate the possibility of using trees or different data structures. The type of a store will always be a list of types from the source calculus, while the way these types are translated will be a parameter of the target calculus depending on the chosen translation. In other words, the interpretation of a store of type \(A, A^2, B\) will depend on whether we consider a call-by-need or a call-by-value translation. As for the type of a coercion, it will simply be expressed as the inclusion relation for the corresponding lists of types.

3. The target calculus, which will be an instance of \(F_1\). This calculus should be as expressive as the source calculus (here, this will only mean to have the same constants) and should contain enough structure to manipulate stores and express extensions of stores. Our calculus will be parameterized by the base cases for translation of source types together with the translation of types in the store.

We are now ready to introduce the syntax of \(F_1\). As we explained, we will focus on the case of a simply typed source calculus, whose types are defined by:

**Source types**

\[
A ::= X \mid A \rightarrow B \quad F ::= A \mid A^2
\]

As explained above, a store \(\tau\) is simply given as a list whose type, written \(\Upsilon\), is defined as the list of the types of the elements \(\tau\) provides. Observe that if we consider the concatenation of two stores \(\emptyset\) and \(\tau_1\) of type \(\emptyset, \Upsilon_1\), thinking of them as substitutions, \(\tau_1\) provides elements for \(\Upsilon_1\) only if it is given with a prefix providing \(\emptyset\) (see also the Step 2 described earlier). We denote its type with \(\emptyset \succ \Upsilon_1\), expressing the fact that it is well-typed only when concatenated with a store of type \(\emptyset \succ \Upsilon_0\) (the type of a "self-sufficient" store, which we will abbreviate by \(\emptyset\)). Obviously, such a store should also be compatible with any extension of \(\emptyset\), which justifies the introduction of the constructor \(\Upsilon^n\) \(\tau\) where \(\sigma\) is of type \(\Upsilon^n\) \(\Upsilon_0\) and the resulting store is of type \(\Upsilon^n\) \(\Upsilon_1\).

Coercions are simply defined through the natural structure witnessing list inclusion: \(\sigma^*\) (resp. \(\downarrow^\top\sigma\)) witnesses the fact that \(\Upsilon, F\) (resp. \(\Upsilon\)) is included in \(\Upsilon', F\) provided that \(\sigma\) witnesses that \(\Upsilon\) is included in \(\Upsilon'\). Having in mind that list inclusion corresponds to a subtyping relation for stores, we denote\(^{11}\) it by \(\Upsilon' \prec \Upsilon\). We denote by \(\sigma \circ \sigma\) the composition of two coercions, and by \(\sigma^{+\tau}\) (resp. \(\uparrow^\top\sigma\)) the twin of the previous coercions witnessing the addition of a list of type \(\Upsilon\).

Finally, System \(F_1\) terms are defined as the usual λ-terms (with constants, to match the source calculus expressiveness) extended with abstractions (and the dual applications) over stores and coercions as well as a split instruction to be able

\(^{10}\)In fact, variants of the \(\lambda\mu\bar{\mu}\)-calculus with explicit stores, but which would naturally define an Intermediate Representation for the corresponding λ-calculi in the compilation chain.

\(^{11}\)This may read "\(\Upsilon'\) is more precise than \(\Upsilon\) as a list" since it contains all its elements.
to split a given store using a coercion. The resulting syntax is given by the following grammar:

**Store type** \( \Upsilon ::= Y | \emptyset | Y, F | \Upsilon, \Upsilon' \)**

**Stores** \( \tau ::= \delta | [t] | \{t\} | \tau; \tau' | [\Unlhd] \tau \)

**Coercions** \( \sigma ::= s | \varepsilon | \sigma' | \sigma \circ \sigma' | \sigma^{-1} | [\Unlhd] \sigma \)

**Contexts** \( \Gamma ::= \emptyset | \Gamma, s : \Upsilon' < Y | \Gamma, \Delta : \Upsilon \triangleright \Upsilon' | \Gamma, x : T \)

**Types** \( T ::= X | T \rightarrow U | \forall Y, T | Y : T \rightarrow Y ; \forall \tau, Y \rightarrow T \)

**Terms** \( t ::= k | x | \lambda \delta.t | t/u | \lambda \delta.t \mid t \sigma | \lambda \delta.t \mid t \tau \)

As for the typing rules, there are given in Figure 6 where \( \mathcal{S} \) is a signature for constants (which will be chosen in each instance so that constants types match the types expected from the source calculus), where \( \equiv \) is the congruent-transitive-symmetric-reflexive closure of the reduction \( \rightarrow \) (defined in the next section) and where \( \Upsilon \triangleright F \) is a parameter of the translation. Intuitively, its definition will specify how elements of the global environment are translated (e.g., in call-by-need the environment contains potentially unevaluated terms\(^{\ref{fn:split}}\), which will be translated as such). Since our syntax implicitly assume that stores of types \( Y_0 \triangleright \Upsilon \) can be lift to match extensions of \( \Upsilon_0 \), for our system to be sound, we need to assume that terms in the store can be lifted as well. Formally, we require that \( \Upsilon \triangleright F \) is of the shape\(^{\ref{fn:split}}\):

\[
\text{(Eq}\triangleright \text{)} \quad \Upsilon \triangleright F \equiv \forall Y < Y : Y, F(Y, F)
\]

for some \( F \), where we write \( \forall Y < Y : T \) as an abbreviation for \( \forall Y, Y < Y : T \rightarrow T \). All the typing rules are quite intuitive, but for the (split) rule, which requires special care. For a term:

\[
\text{split } \tau \text{ at } n \text{ along } \sigma : \Upsilon < Y \text{ as } (Y_0, \sigma_0, \delta_0), x, (Y_1, \sigma_1, \delta_1) \text{ in } t
\]

we need to ensure that \( \Upsilon \) is of the shape \([\Upsilon_0], F, [\Upsilon_1]\) where we abuse the notation \([\Upsilon_0]\) to express that we require a concrete list of types (i.e., without store variable \( Y \)). Besides, to allow the term \( t \) to contain coercions referring to the resulting split stores, we need to explicit name their types, hence\(^{\ref{fn:split}}\) the \( Y_0 \) and \( Y_1 \).

Before we present the operational semantics of the calculus, observe that we introduced enough structure to define terms whose type will match the transformation \( \Box \) evoked earlier (see Remark 1). Remember that we defined the formula \( \Box \mathcal{F} \mathcal{Y} \) as \( \forall Y < Y : \emptyset, \emptyset : \mathcal{F} \rightarrow \{\emptyset\} \rightarrow \bot \) for any \( Y \). We have:

**Lemma 3.1.** Assume that for any \( Y, \mathcal{F} \mathcal{Y} \) is a type. The following rules are admissible:

\[
\frac{\Gamma, s : Y < Y, \delta ; \emptyset \triangleright, Y, x : \mathcal{F} \mathcal{Y} \triangleright t \Downarrow}{\Gamma \vdash \lambda s.\delta \cdot x.t : \Box \mathcal{F} \mathcal{Y}} \quad \text{(E)}
\]

\[
\frac{\Gamma \vdash t : \Box \mathcal{F} \mathcal{Y} \quad \Gamma \vdash \sigma : \Upsilon < Y \quad \Gamma \vdash t : \Upsilon \triangleright \tau \quad \Gamma \vdash u : \mathcal{F} \mathcal{Y} \quad \Gamma \vdash t \sigma u : \bot}{\Gamma \vdash t \Upsilon \triangleright \tau \mathcal{F} \mathcal{Y} \text{ (s)}}
\]

As we shall see in the next sections, we will mainly use these "packed" abstractions and applications to define the different translations (observe that \( \Box \mathcal{F} \mathcal{Y} \) satisfies (Eq\triangleright)). This somehow suggests the use of lists for stores and the corresponding coercions is more a matter of implementation choices than a crucial point in the definition of \( F_1 \). Actually, we could have presented \( F_1 \) directly through these rules, but we choose to stick to a somewhat more atomic presentation.

### 3.2 Reduction rules

We shall now define the reduction rules of System \( F_1 \). If most of them are straightforward, some special care has to be given to define the reduction of terms of the shape \( \text{split}\ \tau \text{ at } n \text{ along } \sigma : \Upsilon < [\|] \text{ as } ... \text{ in } t \). To reduce such a term, we will need to use the coercion \( \sigma \) to split the store \( \tau \) correctly. In particular, we need \( \sigma \) (and \( \tau \)) to be in normal form, that is that it contains neither variables nor compositions of coercions:

**Normal forms**

\[
\begin{align*}
\tau_n & ::= [] | \tau_n[t] \\
\sigma_n & ::= \varepsilon | \sigma_n[t] | [\Unlhd] \sigma_n
\end{align*}
\]

As shown by the next lemma, a coercion in normal forms always allows us to split a store type and the coercion itself:

**Lemma 3.2.** If \( \Gamma \vdash \sigma : \Upsilon < [\|] \) where \( \sigma \) is a coercion in normal form then there exists \( \Upsilon_0, \sigma_0, \sigma_1 \) such that:

1. \( \Gamma \vdash \sigma_0 : \Upsilon_0 < [\|] \)
2. \( \Upsilon = \Upsilon_0, A : \Upsilon_1 \)
3. \( \sigma = \sigma_0 \circ \sigma_1 \)

where \( \sigma_0, \sigma_1 \) is the coercion \( \sigma_1 \) where \( \sigma_0 \) replaces \( \varepsilon \).

Alternatively, a coercion \( \sigma : \Upsilon < [\|] \) in normal form can actually be identified with a partial monotone function \( \| \sigma \|_\mathcal{N} \) from \([0, [\|]]\) to \([0, [\|]]\) which intuitively maps the index of every type in \( \Upsilon \) to its corresponding index in \( \Upsilon' \) (see Appendix D).1

**Example 3.3.** As an example, for any types \( T, U, T_0, T_1 \), if we write \( \sigma \) to denote the coercion \( \| \langle \| \varepsilon \| \rangle \) which is in normal form, we have:

- \( \vdash \langle \| \varepsilon \| \rangle : T_0, U, T_1 \rightarrow T, U \)
- \( \dim(\sigma) = 2, \text{codom}(\sigma) = 4 \)
- \( \| \sigma \|_\mathcal{N} : 1 \rightarrow 2, 2 \rightarrow 4 \)

Visually, this corresponds to the situation pictured on the right.

Similarly, it is easy to see that if a store \( \tau \) is in normal form and is of type \([\| \rangle, A : [\|] \) then we can divide it as expected into \( \tau = \tau_0[u ; \tau_1] \). This justifies the reduction rule for split:

\[
\text{split } \tau_0[u ; \tau_1] \text{ at } n \text{ along } \sigma : \Upsilon_0, A, Y_1 < [\|] \text{ as } (\Upsilon_0, \sigma_0, \delta_0), x, (Y_1, \sigma_1, \delta_1) \text{ in } t \rightarrow \]

\[
t([Y_0/Y_1]) \sigma_0/\sigma_0[\tau_0/\delta_0][u/x][Y_1/Y_1][\tau_1/\delta_1][\sigma_1/\sigma_1]
\]

\(\text{As opposed to values in call-by-value.}^{\ref{fn:split}}\)

\(\text{Where we use the notation } \forall Y < Y : T \text{ to abbreviate } \forall Y, Y < Y : T.\)

\(\text{As the reader will observe in the typing rules, we also need to identify the current store type } (\Upsilon') \text{ with its cutting } (Y_0, F, Y_1). \text{ See also Remark 2.}\)
where \( n = |I_0|, |P_0| = |Y_0| \) and \( Y_0, Y_1, \sigma_0, \sigma_1 \) are as in Lemma 3.2 (i.e. \( |I_0| = \|\sigma(n)\|_0 < I_0 = \|\Gamma_0 = \|\cdot \), etc.).

The rest of the reduction rules are easier and of four kinds:

a) Reductions that normalize coercions, stores and store types as much as possible:

\[
\begin{align*}
\sigma^+ \uplus \sigma_0 & \rightarrow \sigma \uplus (\sigma_1 \circ \sigma_0) & \varepsilon^+ \circ \varepsilon \rightarrow \varepsilon \\
\sigma^+ \circ \sigma_0 & \rightarrow (\sigma_1 \circ \sigma)^+ & \sigma \circ \varepsilon^+ \rightarrow \sigma \\
\uplus \sigma_1 \circ \sigma_0 & \rightarrow \sigma_1 \circ \sigma_0 & \tau ; (\tau' \zeta) \rightarrow \tau ; (\tau ; \tau' \zeta)[r] \\
\uplus \tau . \sigma & \rightarrow \uplus \uplus \sigma & \tau_1 ; \tau \rightarrow (\tau_1 \uplus \tau)[r] \\
\sigma^+ \uplus \uplus \uplus & \rightarrow (\sigma^+)^+ & \tau ; (\uplus \tau)[r] \rightarrow (\tau_1 \uplus \tau)[r] \\
\sigma^+ \uplus \uplus \uplus & \rightarrow (\sigma^+)^+ & \tau ; (\uplus \tau)[r] \rightarrow (\tau_1 \uplus \tau)[r] \\
\sigma^+ \uplus \uplus \uplus & \rightarrow (\sigma^+)^+ & \tau ; (\uplus \tau)[r] \rightarrow (\tau_1 \uplus \tau)[r]
\end{align*}
\]

where \( \uplus^ \triangleq \lambda Ys.t Y s \circ \sigma \).

b) Usual \( \beta \)-reduction steps for the different abstractions:

\[
\begin{align*}
(\lambda x.t) u & \rightarrow t[u/x] & (\lambda s.t) \sigma & \rightarrow t[\sigma/s] \\
(\lambda Y.t) Y & \rightarrow t[Y/x] & (\lambda \delta.t) \tau & \rightarrow t[\tau/\delta]
\end{align*}
\]

c) Contextual rules for store types in stores and coercions:

\[
U_{r}[Y] \xrightarrow{r} U_{r}[Y']
\]

where \( U_{r}[] \triangleq \sigma^+ [r] \) and \( U_{r}[] :\!(r \circ \tau) \)

d) Contextual rules for stores and coercions in split:

\[
C[\sigma] \xrightarrow{r} C[\sigma']
\]

where contexts are defined by:

\[
\begin{align*}
C[] & \triangleq \text{split}[] \text{ at } n \text{ along } \sigma : Y' :: Y \text{ as } \ldots \text{ in } t \\
D[] & \triangleq \text{split} \tau \text{ at } n \text{ along }[] : Y' :: Y \text{ as } \ldots \text{ in } t
\end{align*}
\]

\textbf{Theorem 3.4 (Subject reduction).} If \( \Gamma \vdash t : T \) and \( t \rightarrow t' \) then \( \Gamma \vdash t' : T \).

\textbf{Proof.} See Appendix D.2. \hfill \Box

\textbf{Theorem 3.5 (Normalization). Typed terms normalize.}

\textbf{Proof.} The proof is done by means of a realizability interpretation, see Appendix D.3. \hfill \Box

\textbf{3.3 Expressiveness}

Before introducing the different translations for which we will use \( F_T \) as target calculus, let us briefly discuss the expressiveness of the system. To be more precise, we are interested in the expressiveness that is required to define \( F_T \) (independently of the source calculus). As the reader would have observed, not only do we need to manipulate lists of types and their size, but our definition of coercions involves a form of dependent types (as in \( \sigma^+ \) and \( \uplus \sigma \)). Even if we could have thought to different presentations, it seems that there is a minimal form of dependent types (namely to have access to the size of lists) that we cannot get rid of. In particular, it seems very unlikely that our calculus could be embed into system \( F \) or Cardelli’s system \( F_{\bot} \).

In turn, it is clear that various dependent type theories are expressive enough to define \( F_T \). As an example, in Figure 7 we give an overview of how \( F_T \) can be expressed in Coq through a shallow embedding. We give more details in Appendix E\textsuperscript{13}.

\textbf{4 Implementation for simply typed calculi}

We are now equipped to define typed continuation-and-environment-passing style translations to system \( F_T \). These translations exactly follow the intuitions outlined in Section 2.1. We first focus on the case of the (call-by-name) \( \lambda[\text{for} \cdot \text{e}] \)-calculus, and then illustrate the generality of our method by giving a translation for the call-by-name \( \lambda[\mu] \)-calculus with environments. Theses translations also apply to the MAD and the MAM through the adequate embeddings (see Appendix A). A call-by-value translation is also given in Appendix H.

\textsuperscript{13}The Coq development illustrating these ideas is available at: https://gitlab.com/ermiquey/fupislon.
Let us first focus on the $\llbracket \hat{x} \rrbracket \cdot (x \parallel F)\tau' \rrbracket E$. In the named version, its translation is a term which waits for a store $\tau$ and a value $V$, then forms a store looking like $\langle t \tau | \hat{e}_{\tau} \rangle$ and passes it to $V$ with the continuation $\llbracket F \rrbracket E$. Now, when using de Bruijn levels, the continuation was expecting a store $\tau_0$ of type $\gamma_0$ that $\tau$ (the actual store, of type $Y$) is extending, hence $\tau$ comes together with a coercion $\sigma : \gamma < \gamma_0$ witnessing that $Y$ is an extension of $\gamma_0$. Let us loosely identify the stores with their types and write $\sigma : \gamma < \gamma_0$ to simplify our explanation. The value $V$ has its de Bruijn levels consistent with $\tau$, but $\llbracket F \rrbracket E$ and $\llbracket \tau' \rrbracket E$ have to be updated. In detail, $\llbracket \tau' \rrbracket E$ was expecting $\tau_0[\llbracket \tau' \rrbracket E]$, thus we update it with $\sigma^{+\tau'}$, which witnesses $\llbracket \tau' \rrbracket E < \tau_0[\llbracket \tau' \rrbracket E]$. On the other hand, $F$ was waiting for $\tau_0[\llbracket \tau' \rrbracket E]$, $\tau'$, we thus need to update it with $\sigma' = (\sigma^{+\tau'})^{+\tau}$. Finally, we need to give to $V$ a coercion witnessing the extension of $\tau$ into $\tau_0[\llbracket \tau' \rrbracket E];\llbracket \tau' \rrbracket E$, that is to say $\llbracket \tau' \rrbracket E$. In the end, we obtain the following definition:

$$\llbracket \hat{x} \rrbracket \cdot (x \parallel F)\tau' \rrbracket E \quad V \gamma < \gamma_0 \quad V \gamma \llbracket V \rrbracket E$$

$$\langle \gamma < \gamma_0 \rangle \langle \llbracket \tau' \rrbracket E \rangle \llbracket (\llbracket \tau' \rrbracket E);\llbracket \tau' \rrbracket E \rangle \llbracket \tau' \rrbracket E \rrbracket F$$

where $id_Y = \epsilon^{+\tau'}, \sigma' = (\sigma^{+\tau'})^{+\tau'}$ and $\tau' : \Gamma'$ in the source of the translation.

Let us now take advantage of the features of system $A$ calculus of expandable stores Hugo Herbelin and Étienne Miquey (given in Figure 14). This translation was obtained by refining the reduction system (see Figure 12) into a context-free abstract machine (that is to say an abstract machine in which type Ariola et al. rephrased to handle de Bruijn levels and coercions). Along the translation, we maintain two invariants on de Bruijn levels:

1. Stores are always consistent, that is, in a store $\tau[\tau']$, $\tau$ has its levels coherent with its prefix $\tau$, and ignores its suffix $\tau'$. In terms of types, if $\tau[\tau']$ is of type $Y$, $A$ then $\tau$ will be of a type $Y < A$.

2. The continuations/terms that are passed with a store are always consistent with it, that is they do not need to be lifted and their types always match the type of the store.

Let us spend a few lines to explain the definitions of two cases, namely $\llbracket x \rrbracket Y$ and $\llbracket \hat{x} \rrbracket Y \cdot (x \parallel F)\tau' \rrbracket E$. In the untyped translation (see Appendix B.1), we have:

$$\llbracket \hat{x} \rrbracket Y \cdot (x \parallel F)\tau' \rrbracket E \quad \llbracket V \parallel \tau \tau' \rrbracket E$$

$$\llbracket x \rrbracket \cdot t \tau F \llbracket t \rrbracket E$$

where $id_Y = e^{+\tau'}, \sigma' = (\sigma^{+\tau'})^{+\tau'}$ and $\tau' : \Gamma'$ in the source of the translation.

### Figure 8. Call-by-need translation of terms

#### 4.1 A typed call-by-need translation for the $\lambda_{\mu \sigma \tau \omega}^\text{-calculus}$

#### 4.1.1 Translation of terms

We can now take advantage of the features of system $A$ calculus of expandable stores Hugo Herbelin and Étienne Miquey (given in Figure 14). This translation was obtained by refining the reduction system (see Figure 12) into a context-free abstract machine (that is to say an abstract machine in which type Ariola et al. rephrased to handle de Bruijn levels and coercions). Along the translation, we maintain two invariants on de Bruijn levels:

1. Stores are always consistent, that is, in a store $\tau[\tau']$, $\tau$ has its levels coherent with its prefix $\tau$, and ignores its suffix $\tau'$. In terms of types, if $\tau[\tau']$ is of type $Y$, $A$ then $\tau$ will be of a type $Y < A$.

2. The continuations/terms that are passed with a store are always consistent with it, that is they do not need to be lifted and their types always match the type of the store.

Let us spend a few lines to explain the definitions of two cases, namely $\llbracket x \rrbracket Y$ and $\llbracket \hat{x} \rrbracket Y \cdot (x \parallel F)\tau' \rrbracket E$. In the untyped translation (see Appendix B.1), we have:

$$\llbracket \hat{x} \rrbracket Y \cdot (x \parallel F)\tau' \rrbracket E \quad \llbracket V \parallel \tau \tau' \rrbracket E$$

$$\llbracket x \rrbracket \cdot t \tau F \llbracket t \rrbracket E$$

where $id_Y = e^{+\tau'}, \sigma' = (\sigma^{+\tau'})^{+\tau'}$ and $\tau' : \Gamma'$ in the source of the translation.
Theorem 4.1 (Soundness). The translation is well-typed.

Proof. The proof is done by induction on typing derivations, and requires a few previous lemmas on the soundness of the constrictions $\uparrow^t_i$ and $\uparrow^t$. The complete proof is given in Appendix F. □

4.2 A typed call-by-name translation for the $\tilde{\lambda}_{[\nu r^*]}$-calculus

To emphasize that $F_1$ is a generic target calculus for typed continuation-and-environment-passing style translations, we give the example of a call-by-name translation for the call-by-name $\lambda \mu \tilde{\mu}$-calculus with environments (see Figure 3). A similar translation for the same calculus evaluated in call-by-value is given in Appendix H. We first rephrase its reduction rules to use de Bruijn levels:

$$\tilde{\lambda}(\nu x_1.c)t \rightarrow c[x_n/x_1]t$$
$$\tilde{\lambda}(\mu a_1.c)E \rightarrow c[a_2/x_1]t[a_n := E]$$
$$\tilde{\lambda}(x_n E) \rightarrow (\tau(\|E))\tau$$
$$\tilde{\lambda}(\nu x_1.\langle u \cdot E \rangle) \rightarrow \langle u \| \tilde{\lambda}(x_1, \langle u \| E \rangle) \rangle \tau$$

We spare the reader from the redefinition of a type system using de Bruijn levels, which is fully deducible from the type system of the $\tilde{\lambda}_{[\nu r^*]}$-calculus when considering only the levels $e, t, E, V$ and typing terms and contexts at the appropriate level.

Similarly, we do not wish to enter into too many details about the translation of terms. We follow the same process as for the $\tilde{\lambda}_{[\nu r^*]}$-calculus, by refining the dynamic of the calculus into a context-free abstract machine (see Appendix C.2). This machine only has four level of alternation, as reflected by the syntax, and so does the translation of terms. The definition of the translation for terms almost comes for free modulo the careful treatment of de Bruijn levels. Most of the definitions are identical (or simpler) than in the call-by-need case. In particular, the definition ensures that the same invariants about consistency with respect to de Bruijn levels and store extension are maintained.
Appendix G. A calculus of expandable stores Hugo Herbelin and Étienne Miquey

[54x738]A calculus of expandable stores Hugo Herbelin and Étienne Miquey

⊢ be assigned the types before returning V arbitrary computations (and in particular store arbitrarily of types imagine that we dispose of three values the translation we will thus have

Example 4.3. may contain arbitrarily more elements at that time (see Ex-

The system we propose has the benefits of being highly para-

The system we propose has the benefits of being highly para-

In addition to being compatible with different evaluation strategies, F₁ also allows for different type systems in the source calculus. Exploring this question in detail is beyond the scope of this paper, but we just want to illustrate how we could rather have chosen a source calculus typed with System F. Since the second-order quantification in System F is intended to be substituted by any type, through the translations second-order variables should behave as the translation of types. In particular, they should have access to the current store type. The corresponding translations, that have to be defined at the lowest level, are reminiscent of forcing translations where types are involved [15, 25]:

4.3 Using System F as source calculus

As for the translation of types and judgments, we hope that it should now look trivial to the reader: it follows the exact same guidelines than in the call-by-need case, except that it now only has four levels. It does not come as a surprise that the two translations are so so close: in both cases, terms remain unevaluated in the store environments (and contexts are stored at the same syntactic levels in the environments (t and E). The main difference lies in the fact that in call-by-name, terms remains unevaluated in the store at the lowest level. It does not come as a surprise

Theorem 4.2. The translation is well-typed.

Proof. The proof is similar (and easier) than the proof in the call-by-need case, by induction on typing derivations. See Appendix G.

It is interesting to observe that even though terms are stored once and for all in call-by-name, the use of a global environment forces us to quantify over arbitrary extensions of the store. Indeed, through the translation each (typed) term t is waiting for a store whose type should match its former typing context. Yet, many computations may happen before [t]i is evaluated, corresponding to other branches of the global typing derivation. As a consequence, the store may contain arbitrarily more elements at that time (see Example G.1).

Example 4.3. Consider a term x : A, y : B ⊢ u : C, through the translation we will thus have ⊢ [u]i : [A], B ⊢ C → D. Now, imagine that we dispose of three values V₀, V₁, V₂ respectively of types A, B, C, we can thus construct three closed terms t₀, t₁, t₂ such that, given a continuation, t₁ is going to produce arbitrary computations (and in particular store arbitrarily many terms, let us denote the resulting store by t₁ : [U₁]) before returning V₁ to its continuation. These terms can thus be assigned the types (A → D) → D, (B → D) → D, (C → D) → D, and the closed term t₂ ≜ t₀(x(t₁(y(t₂u)))) can thus be typed by ⊢ t₂ : D. Now, if t₂ is evaluated in an initially empty store, at the moment where uV₂ will be evaluated, the store will be t₀[x := V₀]t₁[y := V₁]t₂ of type U₀, A, U₁, B, U₂.

4.3 Using System F as source calculus

In addition to being compatible with different evaluation strategies, F₁ also allows for different type systems in the source calculus. Exploring this question in detail is beyond the scope of this paper, but we just want to illustrate how we could rather have chosen a source calculus typed with System F. Since the second-order quantification in System F is intended to be substituted by any type, through the translations second-order variables should behave as the translation of types. In particular, they should have access to the current store type. The corresponding translations, that have to be defined at the lowest level, are reminiscent of forcing translations where types are involved [15, 25]:

\[
Y \triangleright T \triangleq \triangleright \triangleright T
\]

\[
Y \triangleright T \triangleq \triangleright \triangleright T
\]

5 Conclusion

Conclusion Through the definition of F₁, we isolated the key ingredients necessary to the definition of well-typed continuation-and-environment-passing style translations:

1. terms to represent and manipulate typed stores,
2. explicit coercions to witness store extensions.

The system we propose has the benefits of being highly parametric: not only is it suitable for defining CEPS translations for simply typed source calculi with global environments evaluated in call-by-need, call-by-name or call-by-value; it is also compatible with different type systems. In addition, while we chose to implement stores with lists, we could as well have chosen to leave their concrete representation abstract. In particular, one could use the very same architecture to handle source calculi where environments are defined through different data structures (tree, records, etc).
A calculus of expandable stores

Hugo Herbelin and Étienne Miquey

About environments and forcing
On the logical side, the translation of types amounts to a (Kripke) forcing translation (for the environment-passing part), interleaved with a negative translation (for the continuation-passing part). Actually, the connection between forcing and the environment-passing style translation does not come as a surprise. It is folklore that the local state monad (used to give a meaning to memory states in functional programming) can be categorically interpreted by means of presheaves construction [24, 31]. Interestingly, presheaves also give a semantics to Kripke models or Cohen forcing [15, 23, 27]. Last but not least, the analysis of Cohen forcing in the framework of Krivine realizability [19, 25] relies on an extension of Krivine abstract machine with a cell (containing the forcing condition), which resembles the Krivine realizability interpretation of the $\lambda\nu\tau\#\#\$-calculus in [26]. In short, our typed environment-passing style translation is just another observation of the connection between forcing translations and explicit expandable environments as a side-effect.

Further work
This work should open the way to the definition of well-typed compilation transformations for lazily-evaluated calculi. For instance, the MetaCoq project managed to identify a type transformation of programs mapped to the call-by-value evaluation through the erasure procedure [34], but defining a similar transformation for the lazy evaluation will necessarily require to define a typed environment-passing style transformation. On the logical side, as we emphasized in Section 3.3, it seems that our system somehow lies in between Cardelli’s system $F_\prec$ [7] and dependently typed calculi (to manipulate sized lists). Yet, the precise logical strength of $F_\prec$ is unclear and is still to determine.

Last but not least, we would like to invest whether the □ can be considered as a modality, and in particular whether we could optimize the translation by using a polarized source calculus, inserting the □ in the translation only when polarity changes.

Acknowledgments
Both authors would like to thank the anonymous reviewers for their accurate remarks. Moreover, the first author thanks Keiko Nakata, as well as José Carlos Espirito Santo, Luís Pinto, Zena Ariola, Paul Downen, Alexis Saurin and Rossen Mikhov for initial discussions on typing the continuation-passing style semantics of call-by-need λ-calculus. The second author was supported by the Paris Ile-de-France Region and would like to thank Théo Winterhalter and Simon Boulier for their valuable comments on this work and the companion Coq development.

References
A calculus of expandable stores

Hugo Herbelin and Étienne Miquey


We then say that two closures \( c, c' \) are equal up to co-variables substitutions, which we denote by \( c \equiv c' \), whenever
\[
c(t) = c'(t).
\]

**Proposition A.1** (MAM simulation). If \( S, S' \) are two states of the MAM such that \( S \xrightarrow{1} S' \), then there exists a closure \( c' \) such that we have \( [[S]] \xrightarrow{1} c' \) and \( (c') \equiv [[S']] \).

**Proof.** Trivial induction on reduction rules of the MAM.

In other words, we showed that a variant of the \( \lambda \mu \mu \)-calculus with global environments where catchable contexts would be immediately substituted instead of being stored is exactly simulating the MAM through the compilation function.

### A.2 The MAD and the \( \bar{\lambda}_{x \mu \pi \tau} \)-calculus

Similarly, we can prove that the \( \bar{\lambda}_{x \mu \pi \tau} \)-calculus allows us to simulate reductions of the MAD. The compilation function from states of the MAD to closures of the \( \bar{\lambda}_{x \mu \pi \tau} \)-calculus is almost the same, except that we now need to take the dump into account. As we explain in Section 1.4, the dump is somehow inlined in the \( \bar{\lambda}_{x \mu \pi \tau} \)-calculus through the binder \( \bar{\mu}[x], (x \parallel F) \tau' \).

Following this intuition, the definition of the translation is almost direct:
\[
[[t \star \pi \star \tau \star D]] \triangleq [[[t]]_1 \parallel [[\pi]\sigma]_{\parallel \delta}]_1(\tau).\]
with:

\[
\begin{align*}
[x]_1 & \triangleq x \\
[\lambda x. t]_1 & \triangleq \lambda x. [t]_1 \\
[tv]_1 & \triangleq \mu \alpha. ([\alpha]_1 \cdot [v]_1) \\
[u \cdot \pi]_\pi & \triangleq [u]_1 \cdot [\pi]_\pi \\
[r[x := t]]_r & \triangleq [r]_r[x := [t]_1] \\
[\epsilon]_r & \triangleq \epsilon \\
[(x, \pi, \tau) :: D]_D & \triangleq \tilde{\mu}[x].(x \parallel [\pi]_D D \tau)_\tau \\
[\epsilon]_D & \triangleq \kappa
\end{align*}
\]

Once again, it is straightforward to check that:

**Proposition A.2 (MAD simulation).** If \(S, S'\) are two states of the MAD such that \(S \xrightarrow{1} S'\), then there exists a closure \(c' \tau'\) such that we have \([S] \xrightarrow{1} c' \tau'\) and \((c' \tau') \equiv [S']\).

**Proof.** Trivial induction on reduction rules of the MAD. \(\square\)
A calculus of expandable stores

Hugo Herbelin and Étienne Miquey

| Strong values  | $v ::= \lambda x.t \mid k$ |
| Weak values    | $V ::= v \mid x$ |
| Terms          | $t, u ::= V \mid \mu \alpha.c$ |
| Environments   | $\tau ::= \epsilon \mid \tau[x := t] \mid \tau[\alpha := E]$ |
| Forcing contexts | $F ::= t \cdot E \mid \kappa$ |
| Catchable contexts | $E ::= F \mid \alpha \mid \mu \tilde{x}.(x \parallel F)\tau$ |
| Evaluation contexts | $e ::= E \mid \mu \tilde{x}.c$ |

B.1 Definitions

B.2 The necessity of $\alpha$-renaming

The original presentation of the $\lambda[u.\tau\star]$-calculus deeply relies on the assumption that names of variable are unique and thus on the possibility of performing $\alpha$-conversion on-the-fly. Consider for instance a command formed by a term of the shape $t = \mu \alpha.\langle u \parallel \mu \tilde{x}.(x \parallel \alpha)\rangle$ and a context of the shape $e = \mu \tilde{x}.(x \parallel F)$. Such a command is perfectly typable (if $u$ and $F$ are) in the type system introduced in [26], however, reducing this command (without $\alpha$-conversion) would loop forever because of the...
auto-reference \([x := x]\) in the environment:

\[
\langle \mu \alpha. \langle u \parallel \tilde{\mu} x. \langle \alpha \parallel F \rangle \rangle \parallel \tilde{\mu} x. \langle \alpha \parallel F \rangle \rangle \rightarrow \langle x \parallel F \rangle [x := \mu \alpha. \langle u \parallel \tilde{\mu} x. \langle \alpha \parallel F \rangle \rangle]
\]

While a simple \(\alpha\)-conversion of one of the \(x\) binding solves the problem, this becomes much more subtle to handle through a CPS translation without renaming (as the one in Figure 14 originally defined in [5]). Indeed, since "different" variables named \(x\) (that is variables which are bound by different binders) are translated independently (e.g. \(\langle t \parallel e \rangle\) is defined from \(\parallel e\) and \(\parallel t\)), there is no hope to perform \(\alpha\)-conversion on the fly during the translation. Thus, the problem becomes unsolvable after the translation, and the problem of renaming should be tackled together with the definition of the translation of terms. For
instance, through this translation, the same closure is again a program that will loop forever:

\[
\llbracket \alpha \rrbracket = \llbracket \alpha \rrbracket_e \in \llbracket \epsilon \rrbracket_e = \llbracket \mu x \cdot (x \parallel F) \rrbracket_e \in \llbracket \epsilon \rrbracket_e
\]

\[
= \llbracket (x \parallel F) \rrbracket_e \in [x := \llbracket \epsilon \rrbracket]_{0}
\]

\[
= \llbracket x \rrbracket_{0} \cdot [x := \llbracket \epsilon \rrbracket]_{0} \llbracket F \rrbracket_{0}
\]

\[
= \llbracket \mu \alpha \cdot u \llbracket \mu x \cdot (x \parallel \alpha) \rrbracket_{e} \in \llbracket \lambda \tau \lambda V. \tau[\llbracket x := \lambda \tau E. E \tau V \rrbracket \llbracket F \rrbracket_{0} - \llbracket \epsilon \rrbracket_{0} \llbracket x \rrbracket_{0}]
\]

\[
= \llbracket (u \parallel \mu x \cdot (x \parallel \alpha))_{e} \llbracket x := \lambda \tau E. E \tau V \rrbracket \llbracket F \rrbracket_{0} , x := \llbracket \epsilon \rrbracket_{0}
\]

\[
= \llbracket a \rrbracket_{0} \llbracket x := \lambda \tau E. E \tau V \rrbracket \llbracket F \rrbracket_{0} , x := \llbracket \epsilon \rrbracket_{0}, x := \llbracket x \rrbracket_{0}
\]

\[
= \llbracket \lambda \tau \lambda V. \tau[\llbracket x := \lambda \tau E. E \tau V \rrbracket \llbracket F \rrbracket_{0} - \llbracket \epsilon \rrbracket_{0} \llbracket x \rrbracket_{0}]
\]

\[
\rightarrow \llbracket x \rrbracket_{0} \llbracket x := \lambda \tau E. E \tau V \rrbracket \llbracket F \rrbracket_{0} , x := \llbracket \epsilon \rrbracket_{0}, x := \llbracket x \rrbracket_{0}
\]

Observe that as the translation is defined modulo administrative reduction, the first equations indeed are equalities, and that when the reduction is performed, the two ”different” x are not bound anymore. Thus, there is no way to achieve any kind of α-conversion to prevent the formation of the cyclic reference [x := [x]V]. This is why we need either to be able to perform α-conversion while executing the translation of a command, assuming that we can find a smooth way to do it, or to explicitly handle the renaming.

In order to ensure the correctness of our translation, we address the problem at the source in the \(\bar{\lambda}_{\mu \alpha \cdot u}^{\theta} \vdash \), using de Bruijn levels. As we observed in the previous example, the issue arises when adding a binding [x := ...] in an environment that already contained a variable x. We thus need to ensure the uniqueness of names within the environment. A simple solution consists in renaming the variables bound in the environment by the position at which they occur in the environment, which is obviously unique. Before presenting formally the corresponding system and the adapted translation, let us reduce the same example using this idea. We use a mixed notation for names, writing x when a variable is bound by a \( \lambda \) or a \( \mu \), and \( x_i \) (where i is the relevant information) when it refers to a position in the environment. The same reduction is now safe if we replace stored variables by their de Bruijn levels:

\[
\left\langle \mu \alpha \cdot u \parallel \mu x \cdot (x \parallel \alpha) \right\rangle \rightarrow \left\langle \lambda \theta \parallel \mu \alpha \cdot u \parallel \mu x \cdot (x \parallel \alpha) \right\rangle
\]

\[
\rightarrow \left\langle \mu \alpha \cdot u \parallel \mu x \cdot (x \parallel \alpha) \right\rangle \rightarrow \left\langle \mu \alpha \cdot u \parallel \mu x \cdot (x \parallel \alpha) \right\rangle
\]

\[
\rightarrow \left\langle x_i \parallel \alpha_0 \right\rangle \rightarrow \left\langle \mu \alpha \cdot u \parallel \mu x \cdot (x \parallel \alpha) \right\rangle \rightarrow \left\langle x_i \parallel \mu \alpha \cdot u \parallel \mu x \cdot (x \parallel \alpha) \right\rangle
\]

where the exponents \(0, 1, \ldots\) to number the cells are only there to ease the readability.

Another solution would have consisted in defining the translation using an explicit renaming function. In broad lines, the translation of terms (resp. contexts, closures, etc.) should be of the form \( [\cdot]_{\nu}^{\sigma} \) where \( \sigma \) is a substitution used to rename variables. To compact the notations, we write \( [\cdot]_{\nu}^{\sigma} \vdash \) for the renaming substitution \( [x := m, \alpha := y, \ldots] \), where we adopt the convention that the most recent binding is on written on the right. As a binding \( [x := n] \) overwrites any former binding \( [x := m] \), we write \( [\alpha]_{\nu}^{m, n} \) instead of \( [\alpha]_{\nu}^{m} \). Using this trick, the translation of the former command would be (where m and n
are fresh names generated during the translation):

\[ [ce]_e^f = [c]_e^f \cdot [e]_e^f = [\hat{\mu}x.(x \parallel F)]_e^f \cdot [e]_e^f \]
\[ = [[x]_t^{[m]}_e \cdot [e]_e^f \cdot [\,[t]_t]_t^f \]
\[ = [[\mu\alpha.(\mu x.(\alpha \parallel a))]_e^{[m]}_n \cdot [\lambda\tau\lambda V.V \cdot y[m := \tau^t V]]_F^{[m]}_n \]
\[ = [\mu x.(\alpha \parallel a)]_e^{[m]}_n \cdot [\lambda\tau\lambda V.V \cdot y[m := \tau^t V]]_F^{[m]}_n \]
\[ = [[x]_t^{[m]}_e \cdot [e]_e^f \cdot [\,[t]_t]_t^f \]
\[ = [[x]_t^{[m]}_e \cdot [e]_e^f \cdot [\,[t]_t]_t^f \]
\[ = [\mu x.(\alpha \parallel a)]_e^{[m]}_n \cdot [\lambda\tau\lambda V.V \cdot y[m := \tau^t V]]_F^{[m]}_n \]
\[ = [\mu x.(\alpha \parallel a)]_e^{[m]}_n \cdot [\lambda\tau\lambda V.V \cdot y[m := \tau^t V]]_F^{[m]}_n \]
\[ = [\mu x.(\alpha \parallel a)]_e^{[m]}_n \cdot [\lambda\tau\lambda V.V \cdot y[m := \tau^t V]]_F^{[m]}_n \]
\[ = [\mu x.(\alpha \parallel a)]_e^{[m]}_n \cdot [\lambda\tau\lambda V.V \cdot y[m := \tau^t V]]_F^{[m]}_n \]
\[ = [\mu x.(\alpha \parallel a)]_e^{[m]}_n \cdot [\lambda\tau\lambda V.V \cdot y[m := \tau^t V]]_F^{[m]}_n \]
\[ = [\mu x.(\alpha \parallel a)]_e^{[m]}_n \cdot [\lambda\tau\lambda V.V \cdot y[m := \tau^t V]]_F^{[m]}_n \]
\[ = [\mu x.(\alpha \parallel a)]_e^{[m]}_n \cdot [\lambda\tau\lambda V.V \cdot y[m := \tau^t V]]_F^{[m]}_n \]

We observe that in the end, the variable \( m \) is bound to the variable \( n \), which is now correct. While this method has the benefit of avoiding the formulation of the source calculus with de Bruijn levels, it has the flaw of hiding a part of the computational content related to the renaming process (that is Kripke forcing).

### B.3 De Bruijn levels

We give here the formal definition of the lifted term \( \uparrow^i \), the term \( t \) where all the free variables \( x_j \) with \( j \geq i \) (resp. \( \alpha_j \)) have been replaced by \( x_{j+n} \) (resp. \( \alpha_{j+n} \)). Given \( i, n \) two natural numbers, we define:

\[ \uparrow^i_n (ct) \triangleq (\uparrow^i_n c)(\uparrow^i_n t) \]
\[ \uparrow^i_n ((t \parallel e)) \triangleq (\uparrow^i_n t \parallel \uparrow^i_n e) \]
\[ \uparrow^i_n (k) \triangleq k \]
\[ \uparrow^i_n (t \cdot E) \triangleq (\uparrow^i_n t) \cdot (\uparrow^i_n E) \]
\[ \uparrow^i_n (\alpha_j) \triangleq \alpha_j \text{ (if } j < i) \]
\[ \uparrow^i_n (\alpha_j) \triangleq \alpha_{j+n} \text{ (if } j \geq i) \]
\[ \uparrow^i_n (\mu[x_j].(x_j \parallel F) \cdot \tau) \triangleq (\uparrow^i_n \mu[x_j].(x_j \parallel F) \cdot \tau) \]
\[ \uparrow^i_n (\mu x_j, c) \triangleq (\uparrow^i_n c) \]
\[ \uparrow^i_n (r[x_j := t]) \triangleq (\uparrow^i_n r)[x_j := \uparrow^i_n t] \]
\[ \uparrow^i_n (r[\alpha_j := E]) \triangleq (\uparrow^i_n r)[\alpha_j := \uparrow^i_n E] \]
\[ \uparrow^i_n (k) \triangleq k \]
\[ \uparrow^i_n (\lambda x_j, t) \triangleq \lambda (\uparrow^i_n x_j).(\uparrow^i_n t) \]
\[ \uparrow^i_n (x_j) \triangleq x_j \text{ (if } j < i) \]
\[ \uparrow^i_n (x_j) \triangleq x_{j+n} \text{ (if } j \geq i) \]
\[ \uparrow^i_n (\mu \alpha_j, c) \triangleq (\uparrow^i_n \mu \alpha_j).(\uparrow^i_n c) \]
C Context-free abstract machines

C.1 The named context-free abstract machine for the \( \lambda_{[\ell \nu \tau \star]} \)-calculus

\[
\begin{align*}
\langle t \parallel \bar{\mu} x. c \rangle_{e \tau} & \rightarrow c_{e \tau}[x := t] \\
\langle t \parallel E \rangle_{e \tau} & \rightarrow \langle t \parallel E \rangle_{1 \tau} \\
\langle \mu \alpha . c \parallel E \rangle_{1 \tau} & \rightarrow c_{e \tau}[\alpha := E] \\
\langle V \parallel E \rangle_{e \tau} & \rightarrow \langle V \parallel E \rangle_{e \tau} \\
\langle V \parallel x . (x \parallel F) \rangle_{e \tau} & \rightarrow \langle V \parallel F \rangle_{V \tau}[x := V]_{\tau'} \\
\langle V \parallel F \rangle_{e \tau} & \rightarrow \langle V \parallel F \rangle_{e \tau} \\
\langle x \parallel F \rangle_{V \tau}[x := t]_{\tau'} & \rightarrow \langle t \parallel \bar{\mu} x . (x \parallel F) \rangle_{1 \tau} \\
\langle V \parallel E \rangle_{V \tau} & \rightarrow \langle V \parallel E \rangle_{V \tau} \\
\langle v \parallel u \cdot E \rangle_{e \tau} & \rightarrow \langle v \parallel u \cdot E \rangle_{e \tau} \\
\langle \lambda x . t \parallel u \cdot E \rangle_{e \tau} & \rightarrow \langle u \parallel \bar{\mu} x . (t \parallel E) \rangle_{e \tau}
\end{align*}
\]

Figure 15. Context-free abstract machine for the \( \lambda_{[\ell \nu \tau \star]} \)-calculus [5]

C.2 Context-free abstract machine for the call-by-name \( \bar{\lambda} \mu \bar{\mu} \)-calculus with environments

\[
\begin{align*}
\langle t \parallel \bar{\mu} x_i . c \rangle_{e \tau} & \rightarrow c_{[x_n/x_i]_{e \tau}[x_n := t]} \quad \text{with } |\tau| = n \\
\langle t \parallel E \rangle_{e \tau} & \rightarrow \langle t \parallel E \rangle_{1 \tau} \\
\langle \mu \alpha_i . c \parallel E \rangle_{1 \tau} & \rightarrow c_{[\alpha_n/\alpha_i]_{e \tau}[\alpha_n := E]} \quad \text{with } |\tau| = n \\
\langle x_n \parallel E \rangle_{e \tau} & \rightarrow \langle r(n) \parallel E \rangle_{1 \tau} \\
\langle V \parallel E \rangle_{e \tau} & \rightarrow \langle V \parallel E \rangle_{e \tau} \\
\langle V \parallel \bar{\mu} \alpha_n \rangle_{e \tau} & \rightarrow \langle V \parallel \bar{\mu} \alpha_n \rangle_{e \tau} \\
\langle V \parallel u \cdot E \rangle_{e \tau} & \rightarrow \langle V \parallel u \cdot E \rangle_{V \tau} \\
\langle \lambda x . t \parallel u \cdot E \rangle_{e \tau} & \rightarrow \langle u \parallel \bar{\mu} x . (t \parallel E) \rangle_{e \tau}
\end{align*}
\]

Figure 16. Context-free abstract machine for the call-by-name \( \bar{\lambda} \mu \bar{\mu} \)-calculus with environments
**D Properties of System** $F_Y$

We give here the properties of System $F_Y$ with their proofs.

### D.1 Coercions

**Lemma D.1.** If $\sigma_1$ is in normal form, then the following rule is admissible:

$$
\frac{
\Gamma \vdash \sigma_0 : \mathcal{Y}_0 < : \mathcal{Y}_0 \quad \Gamma \vdash \sigma_1 : \mathcal{Y}_1 < : \mathcal{Y}_1
}{
\Gamma \vdash \sigma_0 \circ \sigma_1 : \mathcal{Y}_0 < : \mathcal{Y}_1
}
$$

Remember that we say that a coercion is in normal form if it contains neither variables nor compositions of coercions. Formally, these coercions are given by the following grammar:

**Normal forms**

$$\sigma ::= \varepsilon \mid \sigma^+ \mid \uparrow \sigma$$

Interestingly, when two coercions are in normal form, it is possible to compose them to compute another normal form, by simply following the reduction rules $\rightarrow$. In other word, we can define the composition function $- \circ -$ between coercions in normal form by:

$$\sigma_1^+ \circ \sigma_0^+ \triangleq (\sigma_1 \circ \sigma_0)^+ \quad \uparrow \sigma_1 \circ \sigma_0 \triangleq \uparrow (\sigma_1 \circ \sigma_0)$$

$$\sigma_1^\uparrow \circ \| \sigma_0 \triangleq \| (\sigma_1 \circ \sigma_0) \quad \varepsilon \circ \sigma_0 = \sigma_1^\uparrow \circ \varepsilon \triangleq \varepsilon$$

It is easy to verify that this function is sound with respect to the typing rule for composing coercions:

**Lemma D.2 (Composition of normal forms).** If $\sigma, \sigma'$ are coercions in normal forms such that $\vdash \sigma : \mathcal{Y} < : \mathcal{Y}'$ and $\vdash \sigma' : \mathcal{Y}' < : \mathcal{Y}''$, then $\vdash \sigma' \circ \sigma : \mathcal{Y} < : \mathcal{Y}''$.

**Proof.** Direct by structural induction on $\sigma'$.

This suggests us that we can actually consider a slightly larger fragment that includes compositions, since we are able to compute them to get normal form\(^\dagger\). We then define **computable coercions** as being coercions of the shape:

**Computable coercions**

$$\sigma ::= \varepsilon \mid \sigma^+ \mid \uparrow \sigma \mid \sigma' \circ \sigma$$

We can in fact safely reduce properties of computable coercions to the ones of normal forms:

**Proposition D.3 (Computing normal forms).** For any computable $\sigma$, if $\Gamma \vdash \sigma : \mathcal{Y} < : \mathcal{Y}$ then there exists $\sigma_n$ in normal form such that $\Gamma \vdash \sigma_n : \mathcal{Y} < : \mathcal{Y}$.

**Proof.** By induction on typing derivations, using the previous lemma for the $(<:)$-rule.

It is worth noting that for any $\sigma, \mathcal{Y}, \mathcal{Y}'$, if $\vdash \sigma : \mathcal{Y} < : \mathcal{Y}$, then $\sigma$ is necessarily computable.

**Corollary D.4.** If $\vdash \sigma : \mathcal{Y} < : \mathcal{Y}$, then $|\mathcal{Y}| \leq |\mathcal{Y}'|$.

**Proof.** Using the previous proposition, we can reduce this to the case of $\sigma$ in normal forms. The proof then proceed by easy structural induction on $\sigma$.

\(^\dagger\)We could also include $\uparrow \sigma_n$ and $\sigma_n^{\uparrow\uparrow}$ where $\mathcal{Y}$ is in normal form, but for the sake of simplicity, let us just focus on this simpler fragment.
Example D.5. As an example, we let the reader verify that for any types \(T, U, T_0, T_1\), if we denote by \(\sigma\) for the coercion \(\uparrow((\uparrow e)^{++})\) which is in normal form, we have:

\[
\begin{align*}
\bullet & \vdash \uparrow((\uparrow e)^{++}) : T_0, T, U, T_1 \vdash T, U \\
\bullet & \text{dom}(\sigma) = 2, \text{codom}(\sigma) = 4
\end{align*}
\]

\[
\begin{align*}
\llbracket \sigma \rrbracket : & \begin{cases} 0 \mapsto 1 \\
1 \mapsto 2 \\
2 \mapsto 4
\end{cases}
\end{align*}
\]

Visually, this corresponds to the situation pictured on the right.

The previous definitions are indeed in adequacy with the intuition we gave above:

**Proposition D.6 (Associated function).** If \(\sigma\) is in normal form and s.t. \(\vdash \sigma : Y' \vdash Y\), then:

1. \(\text{dom}(\sigma) = |Y|\)
2. \(\text{dom}(\sigma) = |Y'|\)
3. \(\forall n < |Y|, Y'(|\llbracket \sigma \rrbracket(n)) = Y(n)\)
4. \(\llbracket \llbracket \sigma \rrbracket \rrbracket(|Y|) = |Y'|\)

**Proof.** The first two items are proved by a straightforward induction on typing derivations. The third and forth items are then proved together, again by induction on typing derivations: the case \(\llbracket \llbracket \sigma_0 \rrbracket \rrbracket\) is trivial; while for \(\llbracket \llbracket \sigma_+ \rrbracket \rrbracket\) and \(\llbracket \llbracket \sigma_{\uparrow} \rrbracket \rrbracket\) it suffices to unfold the definition, using the first items to connect \(|Y|\) and \(\text{dom}(\sigma)\).

The previous proposition opens the way for proving properties of computable coercions through their associated functions. For instance, we have (remember that we define \(\text{id}_Y = e^{++}\)):

**Proposition D.7 (Partial order).** In the empty context, the subtyping relation \(\llp\) is an order relation on store types.

1. For any \(Y\), we have \(\vdash \text{id}_Y : Y \llp Y\) is admissible.
2. If \(\vdash \sigma : Y \llp Y'\) and \(\vdash \sigma' : Y' \llp Y''\), then \(\vdash \sigma \circ \sigma : Y \llp Y''\).
3. If \(\vdash \sigma : Y \llp Y'\) and \(\vdash \sigma' : Y' \llp Y\), then \(Y = Y'\).

**Proof.** Straightforward using the previous lemma to reduce it to the case of coercions in normal forms. The first two items are straightforward. As for the third one, it is a direct consequence of Proposition D.6, since \(\llbracket \sigma \rrbracket\) and \(\llbracket \sigma' \rrbracket\) are two strictly monotone functions from \([0, |Y|]\) to itself (by Corollary D.4 we have \(|Y'| = |Y|\)), they are necessarily the identity. Equivalently, we could have seen that necessarily \(\sigma\) is of the shape \(\sigma_0^{++}\) (and so is \(\sigma'\)), so that \(Y = Y_0\), \(T\) and \(Y = Y_0, T\), from which we can conclude by an easy induction.

**D.2 Subject reduction**

First, it is clear that the type system is compatible with a weakening rule:

**Lemma D.8 (Weakening).** The following rule is admissible:

\[
\frac{\Gamma \vdash t : A \quad \Gamma \subseteq \Gamma'}{(\text{W})} \quad \frac{}{(\text{W})_\sigma}
\]

**Proof.** Easy induction on typing derivations. In the case of second-order quantification, we might need to rename the second-order variable \(X\) if it occurs in \(\Gamma'\) and not in \(\Gamma\).

Before proving subject reduction, we need to show how terms and stores can be lifted using coercions for their types to remain consistent while extended stores are passed in the translations. First, we show that the bounded quantification can be composed with a subtyping relation witnessed by a coercion \(\sigma\), by precomposing terms with \(\sigma\). Remember that given a coercion \(\sigma\) of type \(Y' \llp Y\) and a term \(t\) whose type is of the shape \(\forall Y < : Y.A\), we defined:

\[
(\uparrow^\sigma t) \triangleq \lambda Ys.t Y (s \circ \sigma)
\]

**Lemma D.9.** The following rule is admissible:

\[
\frac{\Gamma \vdash t : \forall Y < : Y.A \quad \Gamma \vdash \sigma : Y' \llp Y}{\Gamma \vdash (\uparrow^\sigma t) : \forall Y < : Y'.A} (\text{\text{W}})
\]

**Proof.** We assume that \(Y\) is fresh with respect to \(\text{FV}(\Gamma)\), otherwise it suffices to rename it. Unfolding the definition of \(\uparrow^\sigma t\), we can derive:

\[
\frac{\begin{align*}
\Gamma \vdash t : \forall Y < : Y_0.A & \quad \quad (\forall_E) \\
\Gamma \vdash t : \forall Y < : Y_0.A & \quad \quad (\forall_B) \\
\Gamma, s : Y < : Y_1 \vdash t : A & \quad \quad (\forall_\sigma) \\
\end{align*}}{\Gamma, s : Y < : Y_1 \vdash \lambda Ys.t Y (s \circ \sigma) : A} (\text{\text{W}}_\sigma) \quad \frac{\begin{align*}
\Gamma \vdash \sigma : Y_1 < : Y_0 & \quad \quad (\sigma_E) \\
\Gamma, s : Y < : Y_1, s \circ \sigma : Y < : Y_0 & \quad \quad (\llbracket \llbracket \sigma \rrbracket \rrbracket Y \notin \text{FV}(\Gamma)) \\
\end{align*}}{\Gamma \vdash \lambda Ys.t Y (s \circ \sigma) : \forall Y < : Y_1.A} (\text{\text{W}}_\sigma) \quad \frac{\begin{align*}
\end{align*}}{\text{\text{W}}_\sigma} \quad \frac{\begin{align*}
\end{align*}}{\text{\text{W}}_\sigma} \quad \frac{\begin{align*}
\end{align*}}{\text{\text{W}}_\sigma}
where we use Lemma D.8 to weaken \( \Gamma, \sigma : X <: Y_1 \). □

As a Corollary, since we require (Eq\( \uparrow \)) that \( Y \downarrow F \) is always of the shape \( \forall Y <: Y. \mathcal{F}(Y, F) \), we get that

**Corollary D.10.** The following rule is admissible:

\[
\frac{\Gamma \vdash t : Y_0 \rightarrow F \quad \Gamma \vdash \sigma : Y_1 <: Y_0}{\Gamma \vdash \tag{\( \uparrow t \)} \vdash Y_1 \rightarrow F}
\]

**Lemma D.11.** If \( \sigma \) is in normal form, then the following rule is admissible:

\[
\frac{\Gamma \vdash \sigma : Y_0 <: Y_0 \quad \Gamma \vdash \sigma_1 : Y_1 <: Y_1}{\Gamma \vdash \sigma; \sigma_1 : Y_0; Y_1 <: Y_0; Y_1}
\]

We can now verify type safety with respect to reductions:

**Theorem 3.4** (Subject reduction). For any context \( \Gamma \), any type \( T \) and any terms \( t, t' \), if \( \Gamma \vdash t : T \) and \( t \rightarrow t' \), then \( \Gamma \vdash t' : T \).

**Proof.** The proof is standard and does not bring much information. We start by proving the following statements for safe substitutions:

1. If \( \Gamma, x : A, \Gamma' \vdash t : B \) and \( \Gamma \vdash u : A \), then \( \Gamma, \Gamma' \vdash t[u/x] : B \).
2. If \( \Gamma, \delta : Y_0 \vdash_\theta Y_1, \Gamma' \vdash t : B \) and \( \Gamma \vdash \tau : Y_0 \vdash_\theta Y_1 \), then \( \Gamma, \Gamma' \vdash t[\tau/\delta] : B \).
3. If \( \delta, Y : \theta, \Gamma, \delta : Y \vdash t : B \) and \( \Gamma \vdash \sigma : Y <: Y \), then \( \Gamma, \Gamma'[Y'/Y] \vdash t[\sigma/s] : B[Y'/Y] \).
4. If \( \Gamma \vdash t : B \) then \( \Gamma[Y/Y] \vdash t[Y/Y] : B[Y/Y] \).

Each of the three statements is proved together with the similar statements for typing judgments for stores and coercions by mutual induction on typing derivations. The proof of subject reduction is then direct by induction on reduction rules using the previous statements to conclude. The (almost) only interesting case is the one induced by the following reduction rule:

\[
\frac{\Gamma \vdash \sigma : Y_1 <: Y_0 \quad \Gamma \vdash \tau : Y_0 \vdash_\theta Y \quad \Gamma \vdash t : Y_0; Y \vdash F}{\Gamma \vdash \tag{\( \uparrow \tau \)} \vdash Y_1 \vdash_\theta Y, F \quad (\tag{\( \uparrow \tau \)} \vdash Y_1 \vdash_\theta Y, F \vdash F}
\]

we can derive (using Corollary D.10):

\[
\frac{\Gamma \vdash \sigma : Y_1 <: Y_0 \quad \Gamma \vdash \tau : Y_0 \vdash_\theta Y \quad \Gamma \vdash t : Y_0; Y \vdash F}{\Gamma \vdash \tag{\( \uparrow \tau \)} \vdash Y_1 \vdash_\theta Y, F \quad (\tag{\( \uparrow \tau \)} \vdash Y_1 \vdash_\theta Y, F \vdash F}
\]

\[
\frac{\Gamma \vdash \tau : Y' \quad \Gamma \vdash \sigma : Y' <: Y \quad \Gamma = \Gamma_0 \vdash \Gamma_1 \quad |\Gamma_0| = n}{\Gamma \vdash \tag{\( \uparrow \tau \)} \vdash Y', \Gamma = \Gamma_0 \vdash \Gamma_1 \quad |\Gamma_0| = n}
\]

**Remark 2** (About the (\( \uparrow \tau \)) -rule). We shall attract the reader’s attention on a specificity of the (\( \uparrow \tau \)) that she may have observed. Remember that we defined the rule by:

\[
\frac{\Gamma \vdash \tau : Y' \quad \Gamma \vdash \sigma : Y' <: Y \quad \Gamma = \Gamma_0 \vdash \Gamma_1 \quad |\Gamma_0| = n}{\Gamma \vdash \tag{\( \uparrow \tau \)} \vdash Y', \Gamma = \Gamma_0 \vdash \Gamma_1 \quad |\Gamma_0| = n}
\]

where \( \Gamma' = \Gamma[Y_0; F; Y_1/Y'] \) and \( A' = A[Y_0; F; Y_1/Y'] \) (which is an abuse of notations to say that \( \Gamma' = \Gamma_0[Y'/\bullet] \)), \( \Gamma = \Gamma_0[Y_0; F; Y_1/\bullet] \) for some \( \Gamma_0 \), etc). The latter equalities are necessary for identifying \( Y' \) and its cutting in the typing derivation for \( t \), which may contain at the same time build on \( s_0, s_1 \), etc. thus refering to \( Y_0, Y_1 \) and terms refering directly to \( Y' \). To avoid more syntax, we chose to take this equality into account directly with a substitution, but we also could have simply considered two extra coercion variables \( s_1 : Y_0; F; Y_1 <: Y \), \( \delta_1 : (Y_0, F) \vdash_\theta Y_1 + t : A' \) (\( \uparrow \tau \)) -rule). In particular, the reduction rule for split should then instantiate those two coercions with id\( Y' \). This approach would result in the following typing rule:

\[
\frac{\Gamma \vdash \tau : Y' \quad \Gamma, s_0 : Y_0 <:\Gamma_0, \delta_0 : Y_0, x : Y_0 \vdash F, s_1 : (Y_0, F; Y_1 <: Y), \delta_1 : (Y_0, F) \vdash_\theta Y_1 + t : A'}{\Gamma \vdash \tag{\( \uparrow \tau \)} \vdash Y', \Gamma = \Gamma_0 \vdash \Gamma_1 \quad |\Gamma_0| = n}
\]

\[
\frac{\Gamma, s_0 : Y_0 <:\Gamma_0, \delta_0 : Y_0, x : Y_0 \vdash F, s_1 : (Y_0, F; Y_1 <: Y), \delta_1 : (Y_0, F) \vdash_\theta Y_1 + t : A'}{\Gamma \vdash \tag{\( \uparrow \tau \)} \vdash Y', \Gamma = \Gamma_0 \vdash \Gamma_1 \quad |\Gamma_0| = n}
\]
A calculus of expandable stores

Hugo Herbelin and Étienne Miquey

...together with the following reduction rule:

\[
\text{split } \tau_0[u]; \tau_1 \text{ at } n \text{ along } \sigma : \Gamma_0, A, \Gamma_1 <: \llbracket \Gamma_0 \rrbracket, A, \llbracket \Gamma_1 \rrbracket \text{ as } (Y_0, s_0, \delta_0), x, (Y_1, s_1, \delta_1), s_i, s_j \text{ in } t \\
\rightarrow \ t[Y_0/Y_1][\sigma_0/s_0][\tau_0/\delta_0][u/x][Y_1/Y_1][\tau_1/\delta_1][\sigma_1/s_1][\text{id}_{\llbracket \Gamma_0 \rrbracket, A, \llbracket \Gamma_1 \rrbracket}, s_j]] \text{id}_{\llbracket \Gamma_0 \rrbracket, A, \llbracket \Gamma_1 \rrbracket}, s_j]
\]

where \( n = |\llbracket \Gamma_0 \rrbracket |, \ |\llbracket \Gamma_0 \rrbracket | = |\llbracket Y_0 \rrbracket | \) and \( Y_0, Y_1, \sigma_0, \sigma_1 \) are again as in Lemma 3.2. This reduction is also safe with respect to typing.

D.3 Normalization

The proof of normalization for \( F_1 \) that we present in this section is inspired from techniques of Krivine’s classical realizability [18], whose notations we borrow. Actually, it is also very close to a proof by reducibility\(^{16}\). In a nutshell, to each type \( A \) is associated a set \( |A| \) of terms whose execution is guided by the structure of \( A \). These terms are the ones usually called realizers in Krivine’s classical realizability. Their definition is in fact indirect, and is done by orthogonality to a set of “correct” computations, called a pole. The choice of this set is central when studying models induced by classical realizability for second-order-logic, but in the present case we only pay attention to the particular pole of terminating computations. This is where lies one of the difference with usual proofs by reducibility, where everything is done with respect to SN, while our definition are parametric in the pole (which is chosen to be SN in the end). The adequacy lemma, which is the central piece, consists in proving that typed terms belong to the corresponding sets of realizers, and are thus normalizing.

We try to remain as concise as possible, for a comprehensive introduction to Krivine realizability and normalization proof in that context, we refer the reader to Dagand, Rieg and Scherer’s [10].

Abstract machine We begin by adapting the Krivine Abstract Machine to our calculus:

<table>
<thead>
<tr>
<th>Terms</th>
<th>( t \ := \ k \mid x \mid \lambda Y.t \mid t Y \mid \lambda s.t \mid t \sigma \mid \lambda \delta t \mid t \tau \mid \lambda x.t \mid t u )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stacks</td>
<td>( \pi \ := \ • \mid Y \cdot \pi \mid \sigma \cdot \pi \mid \tau \cdot \pi \mid t \cdot \pi )</td>
</tr>
<tr>
<td>Process</td>
<td>( p \ := \ t \star \pi )</td>
</tr>
</tbody>
</table>

We then define the reduction rules \( p > p' \). We first define the usual rules for abstractions/applications (where \( M \in Y \mid \sigma \mid \tau \mid u \)):

\[
\begin{align*}
M \star \pi & > M \cdot \pi \\
\lambda Y.t \star \cdot \pi & > t[Y/Y] \star \pi \\
\lambda s.t \star \sigma \cdot \pi & > t[\sigma/Y] \star \pi \\
\lambda \delta t \star \tau \cdot \pi & > t[\tau/Y] \star \pi \\
\lambda x.t \star u \cdot \pi & > t[u/Y] \star \pi
\end{align*}
\]

...to which we add a rule for splitting stores:

\[
\text{split } \tau_0[u]; \tau_1 \text{ at } n \text{ along } \sigma : \Gamma_0, A, \Gamma_1 <: \llbracket \Gamma_0 \rrbracket, A, \llbracket \Gamma_1 \rrbracket \text{ as } (Y_0, s_0, \delta_0), x, (Y_1, s_1, \delta_1), s_i, s_j \text{ in } t \star \pi \\
\rightarrow \ t[Y_0/Y_1][\sigma_0/s_0][\tau_0/\delta_0][u/x][Y_1/Y_1][\tau_1/\delta_1][\sigma_1/s_1] \star \pi
\]

where \( n = |\llbracket \Gamma_0 \rrbracket |, \ |\llbracket \Gamma_0 \rrbracket | = |\llbracket Y_0 \rrbracket | \) and \( Y_0, Y_1, \sigma_0, \sigma_1 \) are as in Lemma 3.2 (i.e. \( |\llbracket \Gamma_0 \rrbracket | = |\sigma|(n), \sigma_0 : \llbracket Y_0 \rrbracket \cdot \ldots \cdot \), etc.), and \( |\llbracket \Gamma_0 \rrbracket | = |\llbracket Y_0 \rrbracket | \).

Finally, we add two contextual rules for reducing coercions in stores in split:

\[
\begin{align*}
\text{split } \tau \text{ at } n \text{ along } ... \text{ as } ... \text{ in } t \star \pi & > \text{ split } \tau' \text{ at } n \text{ along } ... \text{ as } ... \text{ in } t \star \pi \quad \text{(if } \tau \rightarrow \tau' \text{)} \\
\text{split } \tau_0 \text{ at } n \text{ along } \sigma : ... \text{ as } ... \text{ in } t \star \pi & > \text{ split } \tau_0 \text{ at } n \text{ along } \sigma' : ... \text{ as } ... \text{ in } t \star \pi \quad \text{(if } \sigma \rightarrow \sigma' \text{)}
\end{align*}
\]

where \( \tau_0 \) is in normal form (in other words, we first reduce stores then coercions).

Realizability interpretation We now focus on the definition of the Krivine realizability interpretation, which relies on the definition truth and falsity values (which are themselves defined with respect to a pole).

Definition D.12 (Pole). A subset \( \bot \subseteq \Lambda \star \Pi \) is said to be closed under anti-reduction whenever for all closed \( p, p' \in \Lambda \star \Pi \), if \( p' \in \bot \) and \( p > p' \) then \( p \in \bot \). A pole is defined as any set of closed processes that is closed under anti-reduction.

Definition D.13 (Valuation). A substitution, written \( \rho \), is a function mapping term variables to closed terms (written \( \rho, x := t \)), coercion variables to closed coercions (written \( \rho, s := \sigma \)), store variables to closed stores (written \( \rho, \delta := \tau \)) and store type variable to closed store types (written \( \rho, Y := \llbracket Y \rrbracket \)).

We write \( \rho(t) \) (resp. \( \rho(A), \rho(Y), \text{etc.} \)) the term \( t \) where the substitution \( \rho \) has been performed.

\(^{16}\)See for instance the proof of normalization for system D presented in [17, 3.2].
Given a fixed pole $\perp$, we define the interpretation of closed types as follows:

$$
\begin{align*}
||X|| & = \{ \star \} \\
||Y.T|| & = \bigcup_{T \in \mathcal{T}} \{ Y : \pi : \pi \in ||T/Y|| \} \\
||Y' <: Y \rightarrow T|| & = \{ \sigma \cdot \pi : \sigma \vdash Y' <: Y \land \pi \in ||T|| \} \\
||Y \tau \rightarrow Y' \rightarrow T|| & = \{ \tau \cdot \pi : \tau \vdash Y' \tau Y \land \pi \in ||T|| \} \\
||U \rightarrow T|| & = \{ u \cdot \pi : u \in [U \land \pi \in ||T||] \} \\
|T| & = \{ t : \forall \pi \in ||T||, t \cdot \pi \in \perp \}
\end{align*}
$$

where $\mathcal{T}$ is defined as the set of closed store types (i.e. the set of lists of source types corresponding to the subsyntax $Y_0 = \emptyset | Y_0, F$).

We say that (where all terms and types are closed):

1. $\sigma \vdash Y' <: Y$ if $\exists \sigma : Y' <: Y$
2. $\tau \vdash Y' \tau Y$ if $\forall \tau' \vdash \tau' \tau Y$ and $\tau \vdash Y' ; Y$
3. $[\ ] \vdash \emptyset$
4. $\tau[\ ] \vdash Y, F$ if $\tau \vdash \emptyset$ and $t \in [Y \tau F]$

We close these relations by anti-reduction with respect to $\rightarrow_{\sigma}$ and $\rightarrow_{\tau}$, that is:

$$
\begin{align*}
\sigma & \rightarrow_{\sigma} \sigma' \land \sigma' \vdash Y' <: Y \Rightarrow \sigma \vdash Y' <: Y \\
\tau & \rightarrow_{\tau} \tau' \land \tau' \vdash Y \Rightarrow \tau \vdash Y
\end{align*}
$$

Given a closed context $\Gamma$, we say that a substitution $\rho$ realizes $\Gamma$, which we write $\rho \vdash \Gamma$, if:

1. for any $Y \in \Gamma$, $\rho(Y)$ is defined
2. for any $(s : Y' <: Y) \in \Gamma$, we have $\rho(s) \vdash \rho(Y') <: \rho(Y)$
3. for any $(\delta : Y' \tau Y) \in \Gamma$, we have $\rho(\delta) \vdash \rho(Y') \tau \rho(Y)$
4. for any $(x : A) \in \Gamma$, we have $\rho(x) \vdash \rho(A)$

**Definition D.14 (Adequacy).** We say that a typing judgment $\Gamma \vdash t : A$ (resp. $\Gamma \vdash \sigma : Y' <: Y$, $\Gamma \vdash \tau : Y' \tau Y$) is valid with respect to the interpretation if for any substitution $\rho$ such that $\rho \vdash \Gamma$, then $\rho(t) \vdash \rho(A)$ (resp. $\rho(\sigma) \vdash \rho(Y') <: \rho(Y)$, $\rho(\delta) \vdash \rho(Y') \tau \rho(\delta)$).

We say that a typing rule $J$ is adequate if the validity of the premises $J_1, \ldots, J_n$ entails the validity of the conclusion $J$.

**Proposition D.15 (Adequacy).** All the typing rules (except the rule (c) for constants) are adequate.

**Proof:** By case analysis. In each case we assume a substitution $\rho \vdash \Gamma$ and to ease readability, we write $t_\rho$ (resp. $A_\rho$) for $\rho(t)$ (resp. $\rho(A)$).

\begin{itemize}
\item \textbf{Case} $\Box x : A \vdash (Ax)$. By definition, since $\rho \vdash \Gamma$ and $(x : A) \in \Gamma$, we have that $\rho(x) \vdash A_\rho$.

\begin{align*}
\Gamma \vdash x : A & \vdash t : B \\
\Gamma \vdash t : A & \vdash \lambda x.t : A \rightarrow B
\end{align*}

\item \textbf{Case} $\Gamma \vdash \lambda x.t : A \rightarrow B$ (Ax). Let $u \cdot \pi \in ||A \rightarrow B||$, i.e. $u \vdash A$ and $\pi \in ||B||$. Then $\lambda x.t_\rho \star u \cdot \pi > t_\rho[u/x] \star \pi \in \perp$ by induction hypothesis, since $t_\rho[u/x] = t_\rho[x := u]$ and $\rho[x := u] \vdash \Gamma, x : A$. We conclude by anti-reduction.

\begin{align*}
\Gamma \vdash t : A & \vdash B \\
\Gamma \vdash u : B & \vdash \nu \vdash (\rho(A))
\end{align*}

\item \textbf{Case} $\Gamma \vdash [\ ] : \emptyset \vdash (\emptyset)$. Let $\pi \in ||\emptyset||$, by induction hypothesis we have $t_\rho \vdash A \rightarrow B$ and $u_\rho \vdash A$. Therefore, $t_\rho \cdot u_\rho \cdot \pi > t_\rho \star u_\rho \cdot \pi \in \perp$ since $u_\rho \cdot \pi \in ||A \rightarrow B||$. We conclude by anti-reduction.

\begin{itemize}
\item \textbf{Case} $\Gamma \vdash [\ ] : \emptyset \vdash (\emptyset)$. Trivial: for all $\tau \vdash \emptyset$, we have that $\tau[\ ] = \tau$ and thus $\tau[\ ] \vdash \emptyset$.

\begin{align*}
\Gamma \vdash t : Y_0 & \vdash F \\
\Gamma \vdash [t] : Y_0 & \vdash Y \\
\Gamma \vdash \tau : Y_0 & \vdash Y
\end{align*}

\item \textbf{Case} $\Gamma \vdash \tau : Y_0 \vdash Y$ (t). Let $t_\rho \vdash Y_0$. By induction hypothesis, we have that $t_\rho \vdash Y_0 \vdash F$. Hence, by definition, $t[t_\rho] \vdash Y_0, F$.

\begin{align*}
\Gamma \vdash \tau : Y_0 & \vdash Y \\
\Gamma \vdash \tau : Y_0 & \vdash Y
\end{align*}

\item \textbf{Case} $\Gamma \vdash \tau : Y_0 \vdash Y$. Let $\tau_0 \vdash Y_0$. By induction hypothesis, we have that $\tau_0 \vdash Y_0 \vdash Y$ and thus $(\tau_0 : \tau_0) ; \tau_0 \vdash Y_0 ; Y; Y'$. Since $\tau_0$ is closed, we have that $\tau_0 ; (\tau_0 : \tau_0) \rightarrow (\tau_0 ; \tau_0) ; \tau_0$ (by easy induction the structure of $\tau_0$), hence $\tau_0 \vdash \tau_0 \vdash Y_0 \vdash Y; Y'$.

\item \textbf{Case} $(<:) \text{ rules.}$ By definition, in all cases we have that $\sigma_\rho$ is closed, hence $\vdash \sigma_\rho : Y' \text{ subst } \sigma_\rho$ is well-typed, thus $\sigma_\rho \vdash Y' \text{ subst } \rho_\sigma$.}
\[ (\delta : Y \vdash Y') \in \Gamma \]

- **Case** \( \Gamma \vdash \delta : \Gamma \vdash Y' \). By definition, since \( \rho \vdash \Gamma \) and \( (\delta : Y \vdash Y') \in \Gamma \), we have that \( \rho(\delta) \vdash \delta : Y \vdash Y' \).

  \[
  \Gamma, \delta : \Gamma_0 \vdash Y \vdash t : B \\
  \Gamma \vdash \delta : \Gamma_0 \vdash Y \vdash \lambda Y.t : \forall Y.A
  \]

- **Case** \( \Gamma \vdash \lambda \delta.t : \Gamma_0 \vdash \Gamma \vdash B \). Same proof as for the \((\lambda)\) case.

  \[
  \Gamma \vdash \lambda \delta.t : \forall Y.A
  \]

- **Case** \( \Gamma \vdash t : \forall Y.A \). Same proof as for the \((\lambda)\) case.

  \[
  \Gamma \vdash t : \forall Y.A
  \]

- **Case** \( \Gamma \vdash \sigma : \forall Y.A \). Same proof as for the \((\lambda)\) case.

  \[
  \Gamma \vdash \sigma : \forall Y.A
  \]

- **Case** \( \Gamma \vdash \text{split } \tau \text{ at } n \) along \( \sigma : \forall Y.A \) as \( (Y_0, s_0, \delta_0), x, (Y_1, s_1, \delta_1) \) in \( t : A \).

By induction hypothesis, we get that:

1. \( \tau_0 \vdash \tau' \)
2. \( \sigma_0 \vdash \sigma_0' \)
3. for any \( \sigma_0 \vdash \sigma_0' \), \( \tau_0 \vdash \tau_0' \), \( u \vdash u \), \( F \vdash F \), \( \sigma_1 \vdash \sigma_1 \), \( (Y_0, F, Y_1) \vdash Y_1 \), \( \tau_1 \vdash \tau_1 \), \( \delta_0 \vdash \delta_0 \), \( \delta_1 \vdash \delta_1 \), then \( t_0 \vdash t_0 \)

In particular, by definition, we have that \( \tau_0 \vdash \tau' \), hence Lemma 3.2 applies and we get that: \( \sigma_0 : \sigma_0' \); \( \sigma_1 \) and \( \tau_0' \vdash \tau_1 \). Besides, since \( \tau_0 \vdash \tau_0 \), \( \delta_0 \vdash \delta_0 \), \( \delta_1 \vdash \delta_1 \). Besides, for any \( (k : A) \in \mathcal{S} \), if \( \pi \in \[A] \) then \( k \vdash \pi \) is blocked hence belongs to \( \vdash \).

\[ \square \]

**Proposition D.16.** The set \( \mathcal{M} = \{ p : p \text{ normalizes} \} \) is a valid pole. Besides, the typing rule \((c)\) is adequate for this pole.

**Proof.** Easy verification: if \( p \vdash p' \) and \( p' \) normalizes, then \( p \) normalizes too. Besides, for any \( (k : A) \in \mathcal{S} \), if \( \pi \in \[A] \) then \( k \vdash \pi \) is blocked hence belongs to \( \vdash \).

\[ \square \]
E  Shallow embedding in Coq

We give here an overview of our take to define a shallow embedding of $F_1$ in Coq. We define store types as list of types of the source calculus ($\Ty$), stores through heterogeneous lists of terms, while the corresponding typing relation is defined as an inductive relation. Observe that we do treat the translation $\triangleright$ of types in the store as a parameter, emphasizing that the structure of $F_1$ is actually orthogonal to the choice of this translation.

<table>
<thead>
<tr>
<th>Parameter $\Ty: \Type$.</th>
</tr>
</thead>
</table>

| Inductive $\hlist :=$
| $\mid \hnil : \hlist$
| $\mid \hcons \, \forall \, A, A \rightarrow \hlist \rightarrow \hlist$. |

| Definition $\storeT := \text{list } \Ty$. |

| Inductive $\ll :</ \storeT \rightarrow \storeT \rightarrow \Type :=$
| $\mid \text{empty} : \hnil : \ll$
| $\mid \text{lift} : \forall \, Y \, \forall \, A, Y <:\ll \rightarrow [Y;A] <:\ll$
| $\mid \text{plus} : \forall \, Y \, \forall \, A, Y <:\ll \rightarrow [Y;A] <:\ll;[Y;A]$. |

| Coercions |

Regarding coercions, we define them as the constructors of the inductive type defining the relation $\ll$. In other words, we only define the coercions in normal form, since through the shallow embedding variables will be Coq variables, while $\sigma \circ \sigma', \ll \sigma$ and $\ll \sigma'$ are easily definable as Coq functions. Similarly, $\ll \sigma$ is also defined through its reduction rules, that is by induction $\ll$. That way, the reductions rules easily matches Coq reductions: for instance, observe that $\ll \sigma$ is defined by its reduction rules. Similarly, the only subtle reduction we have to reduce split terms, will be precisely be the very definition of its embedding in Coq.

| Fixpoint $\ll Y \, \ll Y \, Y \, (\sigma;Y1<:\ll Y0):[Y1;Y]:Y0 := (\ldots Y \sigma \ldots)$ match $Y$ with
| $\mid \text{nil} \Rightarrow \sigma$
| $\mid [Y';A] \Rightarrow \text{lift } A (\ll Y' \sigma)$ end. |

| Lemma $\text{liftN}$ _lift $\{Y1 \, Y0 \, Y \, (\sigma;Y1<:\ll Y0): ([\ll Y1 \, A \, \sigma] = \ll (\ll Y \, \sigma)$.

| Proof. reflexivity. Qed. |

| Definition $\circ : \forall \, Y2 \, Y1 \, Y0 \, (\sigma2;Y2<:\ll Y1):(\sigma1;Y1<:\ll Y0), \, Y2 <:\ll Y0$. |

| Proof (* Definition by induction on $Y2$ *) Defined |

| Lemma $\text{plus_N}$ _lift $\{Y2 \, Y1 \, Y0 \, (\sigma1;Y2<:\ll Y1) : (\sigma0;Y0<:\ll Y0)$:
| $(\sigma1 \circ (\ll \sigma0) = \ll (\sigma1 \circ \sigma0))$. |

| Proof. reflexivity. Qed. |

| Definition $\text{precomp}_t$ _F$ : \forall \, Y \, Y \, Y \, (\sigma;Y1<:\ll Y0)$
| $(t;\forall \, Y2 \, Y2<:\ll Y1 \rightarrow F \, Y2):(\forall \, Y2 \, Y2<:\ll Y1 \rightarrow F \, Y2)$
| $\Rightarrow (\text{fun } Z \, (\sigma';Y2<:\ll Y1) \Rightarrow t \, Z \, (\sigma' \circ \sigma))$. (* $\ll \sigma \, t \sigma$ *) |

| Definition $\text{presig}_t Y \, Y \, T \, (\sigma;Y<:\ll T)$ $\Rightarrow (t;Y \Rightarrow T) \ll (\ll T$. |

| rewrite $\text{tr_sound}$ in *. apply (precomp $\triangleright$ _t_ _\sigma_). Defined. |

| Definition $\text{presig}_r Z$:
| $\forall \, r \, Y0 \, Y1 \, (\sigma;Y1<:\ll Y0)$ $(H;\text{typedStore } r \, Y0 \, Z)$, store. |

| Proof. induction $Z';\text{intros};\text{inversion}$ $H;\text{subst}$. |

| exact $\text{hnil}$. |

| exact $((\text{IH} \, Z \, \text{r0} \, Y0 \, Y1 \, \sigma) \, X,\text{presig}_t \, (\text{plus}_N \, Z \, \sigma) \, t1)$. |

| Defined. |

| Lemma $\text{store}_s$ $\text{presig}$ $\{A;\Ty\} (Y0 \, Y1 \, : \, \text{store}(r \, : \, \text{store}(\ldots Y0 \, Y1 \, \text{r} \, : \, A \, (\sigma;Y1<:\ll Y0): (\ll \sigma \, t) \Rightarrow (\ll \sigma \, t) \, (\ll \sigma' \, t)$.

| Proof. intros. reflexivity. Qed. |

The full Coq development illustrating these ideas (and proving most of the properties we stated on $F_1$) is available as supplementary material.
F  Proof of well-typedness

We give here the complete proof of the correction of the translation of terms with respect to types. We begin by making a few observations that will be useful in the proof of the main theorem.

First of all, it is easy to check that the rules for forming stores and witnessing extensions are safe through the translation:

**Lemma F.1** (Store formation). The following rules are admissible:

\[
\begin{array}{c}
\Gamma \vdash \tau : \nu \to \gamma \\
\Gamma \vdash t : \nu_0, \nu_1 \to T
\end{array}
\quad
\Gamma \vdash \tau[t] : \nu_0 \to \gamma, T
\]

The same holds for \(\Gamma \vdash t : \nu_0, \nu_1 \to T\) and \(\Gamma \vdash \tau[t] : \nu_0 \to \gamma, T^\perp\).

**Proof.** Straightforward typing derivations. For the left-hand side we have:

\[
\Gamma \vdash \tau : \nu_0 \to \gamma \\
\Gamma \vdash t : \nu_0, \nu_1 \to T \\
\Gamma \vdash \tau[t] : \nu_0 \to \gamma, T
\]

We then show that the construction lifting values to the level of terms is safe with respect to typing:

**Lemma F.2** (Lifting values). The following is derivable:

\[
\Gamma \vdash V : \nu_0 \to T \\
\Gamma \vdash \uparrow V : \nu_0 \to T
\]

**Proof.** We can derive (weakening contexts on-the-fly to ease readability):

\[\begin{array}{c}
\Pi_E \\
\Gamma \vdash V : \nu_0 \to T \\
\Gamma \vdash \uparrow V : \nu_0 \to T
\end{array}
\]

We are finally equipped to prove the main theorem:

**Theorem 4.1.** The translation is well-typed, i.e.:

1. If \(\Gamma \vdash \nu : T\) then \(\llbracket \Gamma \vdash \nu : T \rrbracket\)
2. If \(\Gamma \vdash F : T^\perp\) then \(\llbracket \Gamma \vdash F : T^\perp \rrbracket\)
3. If \(\Gamma \vdash \nu V : T\) then \(\llbracket \Gamma \vdash \nu V : T \rrbracket\)
4. If \(\Gamma \vdash E : T^\perp\) then \(\llbracket \Gamma \vdash E : T^\perp \rrbracket\)
5. If \(\Gamma \vdash t : T\) then \(\llbracket \Gamma \vdash t : T \rrbracket\)

**Proof.** We reason by induction over typing derivations. We (ab)use of Lemma D.8 to make the derivations more compact by systematically weakening contexts as soon as possible, and compact the first \((\nu)\) and \((\lambda)\) rules in one rule.

1. **Strong values** \(\llbracket k \rrbracket_\nu = k\), which has the desired type by hypothesis.
Case \(\lambda x_i.t\). In the source language, we have:

\[
\Gamma, x_i : T \vdash t : U \quad \boxed{\square = i}
\]

\[
\Gamma, \Gamma' \vdash \lambda x_i.t : T \to U
\]

Hence, we get by induction a proof \(\Pi_t\) of \([t]_1 : \boxed{\square, x_i : T} \vdash U\) and we can derive:

\[
\Pi_t \vdash [t]_1 : \forall Y' \vdash [\Gamma, x_i : T].Y' \to Y' \ni E U \to \perp \quad \Pi_s \quad \Pi_{\delta}
\]

\[
\vdash s : Y < [: \Gamma, \Gamma']. \delta : Y, u : Y \ni E U \vdash [t]_1 (Y, T) \sigma_{T, \Gamma'} \delta[u] : (Y, T) \ni E U \to \perp
\]

\[
\vdash \lambda Y \delta \nu E [t]_1 (Y, T) \sigma_{T, \Gamma'} \delta[u] \ni \delta \nu E \forall Y < [: \Gamma, \Gamma']. Y \to Y \ni E U \to \perp
\]

where:

- \(\Pi_E\) is a proof of \(E : Y \ni E U \ni \delta \nu E (Y, T) \ni E U\) (derivable according to Lemma D.9);
- \(\Pi_s\) is a proof of \(\delta : Y, u : Y \ni E U \vdash \delta[u] : Y, T\) (derivable according to Lemma F.1);
- \(\sigma_{T, \Gamma'} \triangleq (s \circ \ni \Gamma \ni \Gamma T)^{\nu E}\) and \(\Pi_s\) is:

\[
\vdash s : Y < [: \Gamma, \Gamma'] \vdash \boxed{\square} < \nu E \ni \Gamma T : [\Gamma] < [: \Gamma] \quad \Pi_s \quad \Pi_{\delta}
\]

\[
\vdash s : Y < [: \Gamma, \Gamma'] \vdash \boxed{\square} \ni \nu E \ni \Gamma T : [\Gamma] < [: \Gamma]
\]

\[
\vdash s : Y < [: \Gamma, \Gamma'] \vdash (s \circ \ni \Gamma \ni \Gamma T)^{\nu E} : Y, T < [: \Gamma, T]
\]

2. Forcing contexts

- Case \(\ni k\). \(\ni k\) is the desired type by hypothesis.
- Case \(\ni E\). In the source language, we have:

\[
\Gamma \ni E \ni T \ni U \ni L
\]

\[
\Gamma \ni E \ni T \ni (T \to U)\ni L
\]

Therefore, we have by induction hypothesis that \(\vdash [t]_1 : \boxed{\square} \ni E U\), and \(\boxed{\square} \ni E\), so that we can derive:

\[
\delta : Y, u : Y \ni E U \vdash \nu Y \ni \ni E Y, u : Y \ni E U \to \perp
\]

\[
\vdash s : Y < [: \Gamma, \Gamma]. \delta : Y, u : Y \ni E U \vdash \nu Y \ni Y \ni E U \to \perp
\]

\[
\vdash \lambda Y \delta \nu E u \ni Y \ni E Y, Y \ni E U \to \perp
\]

where:

- \(\Pi_E\) is a proof of \(s : Y < [: \Gamma] \ni \ni E U,\) derived from the induction hypothesis for \(t\) and Lemma D.9;
- \(\Pi_s\) is a proof of \(s : Y < [: \Gamma] \ni \ni E U,\) derived from the induction hypothesis for \(E\) and Lemma D.9;
- \(\Pi_{\delta}\) is the axiom rule \(\delta : Y \ni E U\);
- \(\Pi_s\) is the proof of \(\ni \ni E Y : Y < [: \Gamma].

3. Weak values

- Case \(\ni v\). In the source language, we have:

\[
\Gamma \ni \nu \ni v \ni T
\]

\[
\Gamma \ni \nu \ni v \ni T
\]
Hence, we have by induction hypothesis that $\Gamma \vdash \nu^\Psi, [\Gamma] \Gamma \vdash T$ and we can derive:

$$
\begin{align*}
F : Y &\Gamma T \vdash F : Y Y' \to Y', Y' \to Y' \Gamma \vdash T \to \bot \quad (\Psi) \\
\Gamma[\nu^\Psi] &\vdash Y : [\Gamma] F \Gamma T \vdash F : Y' \Gamma \vdash Y \to Y_0 Y \Gamma \vdash T \to \bot \quad (\Psi) \\
\Gamma[\nu^\Psi] &\vdash \delta : Y ; \delta : Y' \Gamma \vdash \delta : Y'. \quad (\Psi) \\
\Gamma[\nu^\Psi] &\vdash s : Y : [\Gamma] \Gamma \vdash Y : [\Gamma] \Gamma \vdash Y \to Y' \Gamma \vdash T \to \bot \quad (\Psi) \\
\Gamma[\nu^\Psi] &\vdash s \to [\Gamma] \Gamma \vdash Y : [\Gamma] \Gamma \vdash \delta : Y'. \quad (\Psi) \\
\Gamma[\nu^\Psi] &\vdash \lambda Y s \Gamma T \Gamma \vdash \delta : \delta' \Gamma \vdash Y \to Y' \Gamma \vdash T \to \bot \quad (\Psi)
\end{align*}
$$

where:

- $\Pi_\Gamma$ is a proof of $s : Y : [\Gamma] \Gamma \vdash Y : [\Gamma] \Gamma \vdash \delta : Y'$, derivable from the induction hypothesis and Lemma D.9.
- $\Pi_\delta$ is the axiom rule $\delta : Y \vdash \delta : Y'$.
- $\Pi_\delta'$ is a proof of $\Gamma \vdash \delta : Y.$ (Proposition D.7)

**Case $[\nu^\Psi]$.** In the source language, we have:

$$
\Gamma(i) = (x_i : T) \\
\Gamma \vdash \nu^\Psi, x_i : T
$$

so that $\Gamma$ is of the form $[\Gamma_0, x_i : T, \Gamma_1]$ with $i = [\Gamma_0]$. By definition, we have:

$$
\Gamma[\nu^\Psi] \vdash \lambda Y s \Gamma T \Gamma \vdash \delta \Gamma \vdash \delta' \Gamma \vdash (\Psi V) \Gamma \vdash (\Psi' F)
$$

where $\Psi^V = \lambda Y s \Gamma T \Gamma \vdash \delta \Gamma \vdash \delta' \Gamma \vdash (\Psi V)$ and $\Psi'$ is such derivation:

$$
\begin{align*}
V : Y' \to Y &\Gamma T \vdash V : (\Gamma[\nu^\Psi]) \Gamma \vdash Y_0 : Y_0 \to T \to \bot \\
\Gamma, V : Y &\Gamma[\nu^\Psi] T \vdash (\Gamma[\nu^\Psi]) \Gamma \vdash Y_0 : Y_0 \to T \to \bot \\
\Gamma, s_0' : Y_0 &\Gamma[\nu^\Psi] T \vdash (\Gamma[\nu^\Psi]) \Gamma \vdash Y_0 : Y_0 \to T \to \bot \\
\Gamma &\Gamma[\nu^\Psi] T \vdash (\Gamma[\nu^\Psi]) \Gamma \vdash Y_0 : Y_0 \to T \to \bot \\
\Gamma &\Gamma[\nu^\Psi] T \vdash (\Gamma[\nu^\Psi]) \Gamma \vdash Y_0 : Y_0 \to T \to \bot
\end{align*}
$$

where $\Gamma = F : Y_0, Y_1 \vdash T, s_0 : Y_0 \vdash Y_0, x : Y_0 \vdash T, s_1 : (Y_0, Y_1) \vdash (\Psi F)$. 

- $\Pi_\Psi$ is the axiom rule:

$$
\begin{align*}
\Gamma &\Gamma[\nu^\Psi] T \vdash (\Gamma[\nu^\Psi]) \Gamma \vdash Y_0 : Y_0 \to T \to \bot \\
\Gamma &\Gamma[\nu^\Psi] T \vdash (\Gamma[\nu^\Psi]) \Gamma \vdash Y_0 : Y_0 \to T \to \bot \\
\Gamma &\Gamma[\nu^\Psi] T \vdash (\Gamma[\nu^\Psi]) \Gamma \vdash Y_0 : Y_0 \to T \to \bot
\end{align*}
$$

- $\Pi_{\Psi'}$ is the following proof, obtained by Lemma D.9:

$$
\begin{align*}
F : (Y_0, Y_1) \Gamma T &\vdash F : (Y_0, Y_1) \Gamma T \Gamma \vdash (\Psi F) \\
\Gamma &\Gamma[\nu^\Psi] T \vdash \psi : Y_0 \to Y_0 \to T \to \bot \\
\Gamma &\Gamma[\nu^\Psi] T \vdash \psi : Y_0 \to Y_0 \to T \to \bot \\
\Gamma &\Gamma[\nu^\Psi] T \vdash \psi : Y_0 \to Y_0 \to T \to \bot
\end{align*}
$$

- $\Pi_{\Psi'}$ is the following proof, obtained by Lemma D.9:

$$
\begin{align*}
\Gamma &\Gamma[\nu^\Psi] T \vdash \psi : Y_0 \to Y_0 \to T \to \bot \\
\Gamma &\Gamma[\nu^\Psi] T \vdash \psi : Y_0 \to Y_0 \to T \to \bot \\
\Gamma &\Gamma[\nu^\Psi] T \vdash \psi : Y_0 \to Y_0 \to T \to \bot
\end{align*}
$$

- $\Pi_{\Psi'}$ is the following proof, obtained by Lemma D.9:

$$
\begin{align*}
\Gamma &\Gamma[\nu^\Psi] T \vdash \psi : Y_0 \to Y_0 \to T \to \bot \\
\Gamma &\Gamma[\nu^\Psi] T \vdash \psi : Y_0 \to Y_0 \to T \to \bot \\
\Gamma &\Gamma[\nu^\Psi] T \vdash \psi : Y_0 \to Y_0 \to T \to \bot
\end{align*}
$$

- $\Pi_{\Psi'}$ is the following proof, obtained by Lemma D.9:
\(\Pi'_t\) is the following derivation, where we use Lemmas F.1 and F.2:

\[
\frac{\delta_0': Y_0', \delta': Y_0}{V : Y_0' \triangleright V T + t'i' V : Y_0' \triangleright T'} \quad (\text{Ax}) \quad \frac{\delta_1 : (Y_0, T) \triangleright t, Y_1 : (t'i' Y) \triangleright Y_1}{(\text{?1})} \quad \frac{s^x_0 : Y_0' <: Y_0 + s : Y_0' <: Y_0}{(\text{<ax})}
\]

\[
\frac{Y_0' <: Y_0, \delta_0' : Y_0', V : Y_0' \triangleright V T + \delta_0'[t'i' V] : Y_0'}{Y_0'} \quad (\text{?l}) \quad \frac{\delta_1 : (Y_0, T) \triangleright t, s_0' : Y_0' <: Y_0 + t'i' s_0' : Y_0', \delta_1 : Y_0', T \triangleright Y_1}{(\text{?m})}
\]

\[
\delta_1 : (Y_0, T) \triangleright t, Y_1, s_0' : Y_0' <: Y_0, \delta_0' : Y_0', V : Y_0' \triangleright V T + \delta_0'[t'i' V] \equiv s_0' \triangleright Y_0, T, V_1, Y_1
\]

4. Catchable contexts

- **Case \([F]_E\)**. This case is similar to the case \([v]_v\).

- **Case \([m][x_i].(x_i \parallel T')_E\)**. In the source language, we have:

\[
\Gamma, x_i : T, \Gamma' \triangleright F : T' \quad \Gamma, x_i : T \triangleright T' : T' \\
\Gamma, \Gamma' \triangleright_E \mu[x_i].(x_i \parallel T') \quad (\text{Ax}) \quad (\text{Ax}) \quad \text{I} \quad (\text{Ax})
\]

We have by induction hypothesis a proof of \(\lambda \Gamma x_i . (x_i \parallel T') \triangleright \Gamma'\) and a proof \(\Pi_F\) of \(\lambda \Gamma x_i . (x_i \parallel T') \triangleright T\).

We can thus derive:

\[
\frac{V : Y \triangleright V T + \nu V \triangleright V : Y \triangleright T \quad \Gamma, x_i : T \triangleright \Gamma' \quad \Gamma \vdash \nu \Gamma' \quad (\text{Ax}) \quad (\text{Ax}) \quad \Pi_F \quad \Pi_F}{(\text{Ax})}
\]

\[
\frac{s : Y <: \Gamma', \Gamma'', \delta : V, Y \triangleright V T + \nu V \triangleright (Y, T, \Gamma'')} \sigma_V : (Y, T, \Gamma'') \triangleright \nu (Y, T, \Gamma''') \quad (\text{Ax}) \quad (\text{Ax}) \quad (\text{Ax}) \quad \Pi_F \quad \Pi_F
\]

\[
\frac{s : Y <: \Gamma', \Gamma'', \delta : V, Y \triangleright V T + \nu V \triangleright (Y, T, \Gamma'')} \sigma_V : (Y, T, \Gamma'') \triangleright \nu (Y, T, \Gamma''') \quad (\text{Ax}) \quad (\text{Ax}) \quad (\text{Ax}) \quad \Pi_F \quad \Pi_F
\]

\[
\frac{\lambda y \delta \nu \varphi \varphi \nu \varphi : \nu (Y, T, \Gamma''') \triangleright \nu \Gamma' \quad (\text{Ax}) \quad (\text{Ax}) \quad (\text{Ax}) \quad \Pi_F \quad \Pi_F
\]

• \(\Pi_\tau\) is the following proof:

\[
\frac{V : Y \triangleright V T + V : Y \triangleright V T \quad \delta : \nu V \triangleright \nu V \quad (\text{Ax}) \quad (\text{Ax}) \quad (\text{Ax}) \quad \Pi_F \quad \Pi_F}{(\text{Ax})}
\]

\[
\frac{s : Y <: \Gamma', \Gamma'', \delta : \nu V \triangleright \nu V \quad \Gamma', \Gamma'' \vdash \nu \Gamma' \quad (\text{Ax}) \quad (\text{Ax}) \quad (\text{Ax}) \quad \Pi_F \quad \Pi_F}{(\text{Ax})}
\]

5. Terms

- **Case \([v]_v\)**. This case is similar to the case \([v]_v\).

- **Case \([\lambda \mu \alpha . c]_v\)**. In the \(\bar{\lambda}[\nu \tau \ast]\)-calculus, we have:

\[
\Gamma, \alpha_i : T' \quad \mu \alpha_i . c : T \quad (\text{Ax}) \quad (\text{Ax}) \quad (\text{Ax})
\]

\[
\frac{\Gamma, \alpha_i : T' \quad \mu \alpha_i . c : T}{\Gamma, \Gamma' \triangleright \mu \alpha_i . c : T} \quad (\text{Ax}) \quad (\text{Ax}) \quad (\text{Ax})
\]
Hence we have by induction a proof of \(\vdash [e]_c : [\Gamma, x_i : T^A] \triangleright c \perp\) and we can derive:

\[
\Pi_y
\]

\[
\Pi_y : \frac{\vdash [c]_s : [\Gamma, x_i : T^A] \triangleright c \perp}{s : Y <: [\Gamma, \Gamma'] \vdash Y, T <: [\Gamma, \Gamma'], T} \quad (\lhd_c)
\]

\[
\Pi_y : \frac{\vdash [e]_c : [\Gamma, Y, \delta \vdash [e]_c : (Y, T^A) \triangleright \perp}{s : Y <: [\Gamma, \Gamma'], \delta : Y \vdash [e]_c : (Y, T^A) \triangleright \perp} \quad (\forall e)
\]

\[
\Pi_y : \frac{\delta : Y \vdash \delta : Y \vdash Y, E Y \vdash E T \vdash \delta[E] : \triangleright \perp \quad \Pi_y}{s : Y <: [\Gamma, \Gamma'], \delta : Y, E Y \vdash E T \vdash [e]_c : (Y, A^A) \triangleright \perp} \quad (\forall e)
\]

\[
\Pi_y : \frac{\lambda Ys \delta E [e]_c (Y, A^A) \triangleright \perp \vdash E T}{s : Y <: [\Gamma, \Gamma'], \delta : Y, E Y \vdash E T \vdash \delta[E] : \triangleright \perp} \quad (\forall e)
\]

where \(\Pi_y\) is as in the first case for \(\lambda x_i.t\).

6. Contexts

- Case \([E]_c\). This case is similar to the case \([v]_v\).
- Case \([\mu x_i.c]_c\). This case is similar to the case \([\mu \alpha_i.c]_c\).

7. Commands

- Case \(\llbracket (t \parallel e) \rrbracket_c\). In the \(\Lambda_{\llbracket t \parallel e \rrbracket}\)-calculus we have:

\[
\begin{align*}
\Gamma \vdash t : T & \quad \Gamma \vdash e : T^A \\
\Gamma \vdash (t \parallel e) : T
\end{align*}
\]

thus we get by induction two proofs of \(\vdash [t]_t : [\Gamma] \triangleright t \perp\) and \(\vdash [e]_c : [\Gamma] \triangleright e \perp\). We can then derive:

\[
\begin{align*}
\frac{\vdash [e]_c : [\Gamma] \triangleright e \perp \vdash [t]_t : [\Gamma] \triangleright t \perp}{s : Y <: [\Gamma] \vdash Y \vdash [e]_c : Y \vdash Y \vdash [t]_t : Y \vdash \perp} \quad (\forall e)
\end{align*}
\]

8. Closures

- Case \(\llbracket c t^* \rrbracket\). In the \(\Lambda_{\llbracket t \parallel e \rrbracket}\)-calculus, we have:

\[
\begin{align*}
\Gamma \vdash c t^* \gamma_c & \quad \Gamma \vdash c t^* \gamma' \\
\Gamma \vdash (c t^*)_t \gamma' : [\Gamma, \Gamma'] \\
\end{align*}
\]

We thus get by induction two proofs \(\vdash [t]_t : [\Gamma] \triangleright t \perp\) and \(\vdash [t^*]_t : [\Gamma] \triangleright t^* \perp\). We can derive:

\[
\begin{align*}
\frac{\vdash [c]_c : [\Gamma, \Gamma'] \triangleright c \perp \vdash [t]_t : [\Gamma] \triangleright t \perp \vdash [t^*]_t : [\Gamma] \triangleright t^* \perp}{s : Y <: [\Gamma] \vdash Y \vdash [t]_t : Y \vdash \perp \vdash [t^*]_t : Y \vdash \perp} \quad (\forall e)
\end{align*}
\]

9. Stores

- Case \(\llbracket \tau x_i := t \rrbracket\). We only consider the case \(\llbracket \tau x_i := t \rrbracket\), the proof for the case \(\llbracket \alpha_i := E \rrbracket\) is identical. This corresponds to the typing rules:

\[
\begin{align*}
\Gamma \vdash \tau : \Gamma' & \quad \Gamma, \Gamma' \vdash t : T \\
\Gamma \vdash \tau x_i := t : \Gamma', \Gamma' \vdash x_i : T
\end{align*}
\]

By induction, we obtain two proofs of \(\vdash [\tau x_i := t]_\tau : [\Gamma] \triangleright \tau \perp\) and \(\vdash [t]_t : [\Gamma] \triangleright t \perp\). We can thus derive by Lemma F.1:

\[
\begin{align*}
\vdash [\tau x_i := t]_\tau : [\Gamma] \triangleright \tau \perp \quad \vdash [t]_t : [\Gamma] \triangleright t \perp \quad \vdash [t]_t : [\Gamma] \triangleright t \perp
\end{align*}
\]

\(\square\)
A calculus of expandable stores

Hugo Herbelin and Étienne Miquey

G  A typed call-by-name translation

We first rephrase the reduction rules to use de Bruijn levels:

\[
\begin{align*}
\langle t \parallel \mu x. c \rangle & \leadsto c[x_n/x_i] \parallel [x_n := t] \quad \text{with } |\tau| = n \\
\langle \mu x. c \parallel E \rangle & \leadsto \langle [c/x_n] \parallel [a_n/x_i] \parallel [a_n := E] \rangle \quad \text{with } |\tau| = n \\
\langle V \parallel [\lambda a. c] \rangle & \leadsto \langle V \parallel \lambda a. \parallel [\lambda a \parallel [a_n := E]] \rangle \\
\langle \lambda x.t \parallel u \cdot E \rangle & \leadsto \langle u \parallel \lambda x. \parallel [x_n := t] \parallel [E] \rangle 
\end{align*}
\]

We give in Figure 17 the full translation for the call-by-name \(\lambda \mu \tau\)-calculus with global environment. Once again, we have:

\begin{itemize}
\item \(\Rightarrow\): The translation is well-typed, i.e.:
\end{itemize}

\begin{itemize}
\item If \(\Gamma \parallel V \parallel \Gamma \parallel V : T\) then \(\parallel \parallel \parallel \Gamma \parallel V \parallel V \parallel T\)
\item If \(\Gamma \parallel E : T^+\) then \(\parallel \parallel \parallel \Gamma \parallel E : T^+\)
\item If \(\Gamma \parallel t : T\) then \(\parallel \Gamma \parallel t : T\)
\item If \(\Gamma \parallel e : T^+\) then \(\parallel \parallel \parallel \Gamma \parallel e : T^+\)
\end{itemize}

\[\text{Proof.}\] The proof is very similar (and easier) than the proof in the call-by-need case, by induction on typing derivations. In particular, all the lemmas proved in Appendix F also hold for the call-by-name translation. \(\square\)

It is interesting to observe that even though terms are stored once and for all in call-by-name, the use of a global environment forces us to quantify over arbitrary extensions of the store. Indeed, through the translation each (typed) term \(t\) is waiting for a store whose type should match its former typing context. Yet, many computations may happen before \([\parallel]\), is evaluated, corresponding to other branches of the global typing derivation. As a consequence, the store may contain arbitrarily more elements at that time.
Example G.1. Consider a term \( x : A, y : B \vdash u : C \), through the translation we will thus have \( \vdash [u]_1 : A, B \vdash C \rightarrow D \). Now, imagine that we dispose of three values \( V_0, V_1, V_2 \) respectively of types \( A, B, C \), we can thus construct three closed terms \( t_0, t_1, t_2 \) such that, given a continuation, \( t_i \) is going to produce arbitrary computations (and in particular store arbitrarily many terms, let us denote the resulting store by \( \tau_i : \bigcirc U_i \)) before returning \( V_i \) to its continuation. These terms can thus be assigned the types \( (A \rightarrow D) \rightarrow D, (B \rightarrow D) \rightarrow D, (C \rightarrow D) \rightarrow D \), and the closed term \( t_u \triangleq t_0(\lambda x. t_1(\lambda y. t_2 u)) \) can thus be typed by \( \vdash t_u : D \). Now, if \( t_u \) is evaluated in an initially empty store, at the moment where \( uV_2 \) will be evaluated, the store will be \( \tau_0[x := V_0] \tau_1[y := V_1] \tau_2 \) of type \( \bigcirc U_0, A, \bigcirc U_1, B, \bigcirc U_2 \).
A calculus of expandable stores

Hugo Herbelin and Étienne Miquey

**Theorem H.1.** The translation is well-typed, i.e:

1. If $\Gamma \vdash_{\nu} V : T$ then $[\Gamma \vdash_{\nu} V : T]$
2. If $\Gamma \vdash_{\tau} e : T$ then $[\Gamma \vdash_{\tau} e : T]'$
3. If $\Gamma \vdash_{\tau} t : T$ then $[\Gamma \vdash_{\tau} t : T]$
4. If $\Gamma \vdash_{\epsilon} c$ then $[\Gamma \vdash_{\epsilon} c]$
5. If $\Gamma \vdash_{\epsilon} l$ then $[\Gamma \vdash_{\epsilon} l]$
6. If $\Gamma \vdash_{\tau} \tau$ then $[\Gamma \vdash_{\tau} \tau : \Gamma']$

---

**Figure 18.** Call-by-value continuation-and-environment-passing style translation

**H A typed call-by-value translation**

To illustrate the generality of our construction, we give one more example by giving a typed continuation-and-environment-passing style translation for the call-by-value $\lambda\mu\nu$-calculus with explicit environments. Its syntax is given by:

Values  $V ::= \lambda x : T \mid x \mid k$

Co-values  $E ::= t \cdot e \mid a : \kappa$

Environment  $\tau ::= \epsilon \mid \tau[x : V] \mid \tau[a_i : E]$

Terms  $t, u ::= V \mid \mu a : e$

Contexts  $e ::= E \mid \mu x : i$

Commands  $c ::= (t \parallel e)$

Closures  $l ::= cr$

while the reduction rules are given by:

(Catch)  $(\mu a : e) \tau \rightarrow c[a_\kappa / a][\tau[a_\kappa : e]]$ with $|\tau| = n$

(Let)  $(\lambda x : i) \tau \rightarrow c[x / i][\tau[x : V]]$ with $|\tau| = n$

(Lookup)  $(\lambda x : i) \parallel (t \parallel e) \tau \rightarrow (t \parallel \tau[i]) \tau$

(Beta)  $(\mu x : i) \parallel (t \parallel e) \tau \rightarrow (t \parallel \mu x : (i \parallel e)) \tau$

The main specificity of the translations is that since only values can be stored in environments, we define $Y \triangleright T = Y \triangleright_{\nu} T$. The translations of types and judgments, is very similar to the translation in the call-by-name and call-by-need settings, but adapted to match the alternation of levels in the operational semantics. Namely, since terms at level $t$ are first analyzed, then context at level $e$ and finally values, the translation follows the same hierarchy. Again, we have: