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 $\hat{t}$ 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:

Terms $t, u ::= x | tu | \lambda x.t$
Stacks $\pi ::= \varepsilon | \hat{t} \cdot \pi$
Environments $\tau ::= \varepsilon | \tau[x ::= t]$

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 $\hat{t}^x$ that is $\alpha$-equivalent to $t$ and such that any bound name in $\hat{t}^x$ 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

\(^1\)In other words, we assume implicit $\alpha$-conversion for terms, which stand for the equivalence class of raw syntactic codes up to $\alpha$-conversion.
Within the updated environment

\[
\begin{align*}
\tilde{t}u \star \pi \star \tau & \rightarrow_c \tilde{t} \star \tilde{u} \cdot \pi \star \tau \\
\lambda x.\tilde{t} \star \tilde{u} \cdot \pi \star \tau & \rightarrow_\beta \tilde{t} \star \tilde{u} \cdot \pi \star \tau [x := \tilde{u}] \\
x \star \pi \star \tau [x := \tilde{t}]\tau' & \rightarrow_a \tilde{t} \star \tilde{u} \star \pi \star \tau [x := \tilde{t}]\tau'
\end{align*}
\]

(a) Milner Abstract Machine

\[
\begin{align*}
\tilde{t}u \star S \star E & \rightarrow_c \tilde{t} \star (\tilde{u}, E) \cdot S \star E \\
\lambda x.\tilde{t} \star (\tilde{u}, E') \cdot S \star E & \rightarrow_\beta \tilde{t} \star S \star E [x := (\tilde{u}, E')] \\
x \star S \star E [x := \tilde{t}] \tilde{E''} & \rightarrow_a \tilde{t} \star S \star E'
\end{align*}
\]

(b) Krivine Abstract Machine

\begin{figure}[h]
\begin{center}
\includegraphics[width=\textwidth]{figure1.png}
\end{center}
\caption{MAM vs KAM}
\end{figure}

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

Terms \[ t, u ::= x \mid tu \mid \lambda x. t \]

Stacks \[ S ::= \varepsilon \mid (t, E) \cdot S \]

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 α-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 λ-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-needD (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 \( \nu \) in an environment \( \tau'_1 \), the machine goes back to the former computation within the updated environment \( \tau'_1 [x := \nu] \tau_2 \). 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

\[
\begin{align*}
\tilde{t}u \star \pi \star \tau \star D & \rightarrow_c, 1 \tilde{t} \star \tilde{u} \cdot \pi \star \tau \star D \\
\lambda x.\tilde{t} \star \tilde{u} \cdot \pi \star \tau \star D & \rightarrow_\beta \tilde{t} \star \tilde{u} \cdot \pi \star \tau [x := \tilde{u}] \star D \\
x \star \pi \star \tau [x := \tilde{t}] \tau' \star D & \rightarrow_c, 2 \tilde{t} \star h(x, \tau') \cdot \pi \star \tau \\
\overline{\nu} \star h(x, \tau') \cdot \pi \star \tau & \rightarrow_a, 3 \overline{\nu} \star \overline{\nu} \star \pi \star \tau [x := \overline{\nu}] \tau' \star D
\end{align*}
\]

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

\[
\begin{align*}
x \star \pi \star \tau [x := \tilde{t}] \tau' & \rightarrow_c, 1 \tilde{t} \star h(x, \tau') \cdot \pi \star \tau \\
\overline{\nu} \star h(x, \tau') \cdot \pi \star \tau & \rightarrow_a, 3 \overline{\nu} \star \overline{\nu} \star \pi \star \tau [x := \overline{\nu}] \tau'
\end{align*}
\]

This is for instance the approach chosen in Sestoft’s machine for lazy evaluation [33] or in Accattoli, Barendbaum 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, Barendbaum and Mazza’s paper [2].

1.3 The \( \overline{\lambda} \mu \nu \)-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 λμ-fragment (that is without the classical control \( \overline{\lambda} \nu \)-calculus with environments, see Appendix A.)
We formalize the MAD as a call-by-name calculus with global environments, which we call $\tilde{\mathcal{L}}\tilde{\mu}\tilde{\mu}$-calculus.

Syntax of stacks to $t \cdot E$ for call-by-name evaluation rather than the more general $te$. Observe that the reduction rules for $\tilde{\mu}$ is restricted to co-values, which enforces the call-by-name reduction strategy. Call-by-value is obtained by relaxing the prefix of the environment $\tilde{\mu}$, which allows to capture the current stack into a continuation, is very natural, it is less obvious to determine 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 $\lambda$-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 $\tilde{\lambda}\tilde{\mu}\tilde{\mu}$-calculus, they finally obtain a small-step sequent calculus, the $\tilde{\lambda}_{\tilde{t}\tilde{v}_\star\star}$-calculus, from which they get an untyped CPS translation almost for free\(^1\). The $\tilde{\lambda}_{\tilde{t}\tilde{v}_\star\star}$-calculus can be understood as a refinement of the $\tilde{\lambda}\tilde{\mu}\tilde{\mu}$-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:

$$\langle \mu \alpha.c \parallel \tilde{\mu}x.c.c' \rangle \rightarrow c'[x := \mu \alpha.c]$$

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 $\tilde{\mu}[x].(x \parallel F)\tau'$:

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

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 $\tilde{\mu}[x]$. $\langle x \parallel F \parallel \tau' \rangle$ where the $\tilde{\mu}[x]$ binder is waiting for a value. This context keeps track of the place 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:

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

The brackets in $\tilde{\mu}[x].c$ are used to express the fact that the variable $x$ is forced at top-level\(^2\). 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 $\tilde{\lambda}_{\tilde{t}\tilde{v}_\star\star}$-calculus are close to the ones of the MAD\(^3\).

\(^1\)See Appendix B.1 for the original definition of the $\tilde{\lambda}_{\tilde{t}\tilde{v}_\star\star}$-calculus and the corresponding untyped CPS.

\(^2\)Unlike meta-contexts of the shape $\tilde{\mu}x.C[(x \parallel F)]$ in the $\tilde{\lambda}_{\tilde{t}\tilde{v}_\star}$-calculus, see [5].

\(^3\)In fact, it is an easy exercise to simulate the MAD within the $\tilde{\lambda}_{\tilde{t}\tilde{v}_\star\star}$-calculus. We outline this construction in Appendix A.


| Strong values | $v ::= k \mid \lambda x_i.t$ |
| Weak values   | $V ::= v \mid x_i$ |
| Terms         | $t, u ::= V \mid \mu a_i.c$ |
| Stores        | $r ::= \epsilon \mid r[x_i := t] \mid r[a_i := E]$ |
| Commands      | $c ::= (t \parallel c)$ |
| Closures      | $l ::= c \tau$ |
| Forcing contexts | $F ::= \kappa \mid t \cdot E$ |
| Catchable contexts | $E ::= F \mid a_i \mid \mu[x_i].(x_i \parallel F)\tau$ |
| Evaluation contexts | $e ::= E \mid \mu x_i.c$ |

(LET) $\langle t \parallel \mu x_i.c \tau \rangle \tau \rightarrow^\dagger c[x_n/x_i]r[x_n := t]$  
(CATCH) $\langle \mu a_i.c \parallel E \tau \rangle \tau \rightarrow^\dagger c[a_n/a_i]r[a_n := E]$  
(LOOKUP) $(V \parallel a_n)\tau \rightarrow (V \parallel (\alpha r)\tau)$  
(LOOKUP) $(x_n \parallel F)\tau_0[x_n := t]r_1 \rightarrow (t \parallel \mu x_i[x_n \rightleftharpoons F]r_1)\tau_0$  
(RESTORE) $\langle V \parallel \mu x_i[x_i \parallel F]r' \tau \rangle \tau \rightarrow^\dagger (\mu \parallel F)\tau[x_n := V]r_2 \tau^\dagger$  
(BETA) $(\lambda x_i.t \parallel u \cdot E)\tau \rightarrow^\dagger (u \parallel \mu x_i, \lambda(x_n/x_i) \parallel E)\tau$  

$^\dagger$ with $|\tau| = n$  

$\dagger F \triangleq \uparrow_i^{(n-i)} F$ and $\tau^\dagger \triangleq \uparrow_i^{(n-i)} \tau'$

| Figure 4. The $\lambda_{\forall \tau \exists \tau}^*$-calculus with de Bruijn levels |

Last but not least, the different syntactic categories can be understood as different levels of alternation in a context-free abstract machine (see [5]): the priority is first given to contexts at level $\epsilon$ (lazy storage of terms), then to terms at level $t$ (evaluation of $\mu \alpha$ 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 $\lambda_{\forall \tau \exists \tau}^*$-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 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 $a_i$, where, again, $a$ 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 $\uparrow_i^n t$ as the term $t$ where the free variables $x_j$ (resp. $a_j$) with $j \geq i$ have been replaced by $x_{j+n}$ (resp. $a_{j+n}$). 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 $(n + 1)^{st}$ 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 $v, V, t, F, e, l, c, r$:

\[
\begin{align*}
\Gamma \vdash l & \quad \Gamma \vdash t : T & \quad \Gamma \vdash e : T^\bot \\
\Gamma \vdash c & \quad \Gamma \vdash V : T & \quad \Gamma \vdash E : T^\bot \\
\Gamma \vdash r & \quad \Gamma \vdash u : T & \quad \Gamma \vdash F : T^\bot
\end{align*}
\]

where types and typing contexts are defined by:

\[
T, U ::= X \mid T \rightarrow U \quad \Gamma ::= \epsilon \mid \Gamma, x : T \mid \Gamma, \alpha : T^\bot
\]

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 $T^\bot$; 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 $\kappa$ and co-constants $\lambda$ 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 $\Gamma \vdash l \tau$ and $\epsilon \tau \rightarrow c^*\tau'$ then $\Gamma \vdash l c^*\tau'$.
we illustrate each of them with the translation of the sequent\(^9\)
\(a : A, \alpha : A^\downarrow, b : B \tau_e e : C.\)

**Step 1 – Continuation-passing style.** In a first approximation, let us look only at the continuation-passing style part of the translation of a \(\lambda_{(\tau,v)}\) sequent. As emphasized in [5, 26], there are 6 different levels of control in the \(\lambda_{(\tau,v)}\) calculus (corresponding to the 6 nested syntactic categories), leading to 6 mutually defined levels of interpretation. We define \([A \to B]_v\) for strong values as \([A]_v \to [B]_v\), we define \([A]_{\tau}^\downarrow\) for forcing contexts as \(\lnot [A]_v\), \([A]_v\) for weak values as \(\lnot [A]_{\tau}^\downarrow\), and so on until \([A]_v = [\downarrow A]_v\), (where we use the notations \(\downarrow A \rightleftharpoons A \to \bot\) and \(\uparrow A \rightleftharpoons \lnot \bot\).

As observed in the realizability interpretation [26], hypotheses from a context \(\Gamma\) of the form \(\alpha : A^\downarrow\) are to be translated as \([\alpha]_v = [\downarrow A]_v\) while hypotheses of the form \(x : A\) are to be translated as \([\alpha]_v = [\downarrow A]_v.\) Up to this point, if we denote this translation of \(\Gamma\) by \([\Gamma]_v\), in the particular case of \(\Gamma \vdash \tau A\) the translation is \([\Gamma]_v \vdash [A]_v\), and similarly for other levels.

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

\[
\begin{align*}
[a : A, \alpha : A^\downarrow, b : B \tau_e e : C] & = a : [A]_v, \alpha : [A]_{\tau}^\downarrow, b : [B]_v \vdash [e]_v : [C]_v \\
&a = [\downarrow A]_v, \alpha = [\downarrow A]_v, b = [B]_v \vdash [e]_v = [\downarrow C]_v.
\end{align*}
\]

**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 \(\Gamma \vdash \tau A\) is not anymore a sequent \([\Gamma]_v \vdash [A]_v\), but instead a sequent roughly of the form \(\Gamma \vdash [\Gamma]_v \vdash [A]_{\tau}^\downarrow\), with actually \([\Gamma]_v\) being passed around not only at the top-level of \([\Gamma]_v\), but also each time a negation is used. We write this sequent \(\Gamma \vdash [\Gamma]_v \vdash [A]_v\) where \(\vdash_{\Gamma} A\) is defined by induction on \(t\) and \(A\):

\[
\begin{align*}
[\Gamma]_v \vdash_{\Gamma} A & = [\Gamma]_v \vdash ([\Gamma]_v \vdash [A]_v) \to \bot \\
& = [\Gamma]_v \vdash ([\Gamma]_v \vdash ([\Gamma]_v \vdash [A]_v) \to \bot) \to \bot \\
& \vdots
\end{align*}
\]

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

$$\begin{align*}
a : A, \alpha : A^4, b : B \vdash_e e : C \\
\Rightarrow \Gamma \vdash [e]_{\tau} : \left[ a : A, \alpha : A^4, b : B \right] \vdash e C \\
\Rightarrow \Gamma \vdash [e]_{\tau} : \left[ a : A, \alpha : A^4, b : B \right] \vdash e C \\
\Rightarrow \forall Y : \vdash (Y \vdash \alpha) \to \bot \\
\Rightarrow \Rightarrow \end{align*}$$

where:

$$\begin{align*}
\left[ a : A, \alpha : A^4, b : B \right] &\Rightarrow [a : A, \alpha : A^4, b : B] \vdash e C \\
\left[ a : A, \alpha : A^4 \right] &\Rightarrow [a : A, \alpha : A^4] \vdash e C \\
\left[ a : A, \alpha : A^4 \right] &\Rightarrow [a : A, \alpha : A^4] \vdash e C \\
\left[ a : A \right] &\Rightarrow [a : A] \vdash e C \\
\left[ a : A \right] &\Rightarrow [a : A] \vdash e C \\
\end{align*}$$

**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 $F_C$. [7] extended with stores, defined as lists of assignations $[x := t]$. Store types, denoted by $Y$, 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 $\vdash_e A$ as a list of types of the form $\left[ a : A, \alpha : A^4, b : B \right] \vdash_e e C$.

$$\begin{align*}
\left[ a : A, \alpha : A^4, b : B \right] &\Rightarrow [a : A, \alpha : A^4, b : B] \vdash e C \\
\left[ a : A, \alpha : A^4 \right] &\Rightarrow [a : A, \alpha : A^4] \vdash e C \\
\left[ a : A, \alpha : A^4 \right] &\Rightarrow [a : A, \alpha : A^4] \vdash e C \\
\left[ a : A \right] &\Rightarrow [a : A] \vdash e C \\
\left[ a : A \right] &\Rightarrow [a : A] \vdash e C \\
\end{align*}$$

Such a quantification is reminiscent of Kripke forcing [16]: thinking of store types $Y$ as worlds, the accessible worlds from $Y$ are precisely the store types $Y'$ such that $Y' < Y$. To emphasize this correspondence, we give here the translation of the arrow both in Kripke models and in our setting, where the forcing translation is interleaved with the continuation/environment-passing parts:

$$\begin{align*}
Y \vdash_e T &\Rightarrow U \iff \forall Y' : \vdash Y, Y' \to (Y \vdash_e T) \to (Y \vdash_e U) \to \bot \\
\omega \vdash_e A &\Rightarrow B \iff \forall \omega' \geq \omega : \omega' \vdash e A \Rightarrow \omega' \vdash e B \\
\end{align*}$$

**Example 2.3 (Translation, step 3).** The translation, now taking into account store extensions, of $a : A, \alpha : A^4, b : B \vdash_e e : C$ becomes:

$$\begin{align*}
\left[ a : A, \alpha : A^4, b : B \vdash_e e : C \right] \\
\Rightarrow \exists \Gamma, \forall Y : \vdash (Y \vdash \alpha) \to \bot \\
\Rightarrow \Rightarrow \end{align*}$$

where:

$$\begin{align*}
\left[ a : A, \alpha : A^4, b : B \right] &\Rightarrow [a : A, \alpha : A^4, b : B] \vdash e C \\
\left[ a : A, \alpha : A^4 \right] &\Rightarrow [a : A, \alpha : A^4] \vdash e C \\
\left[ a : A, \alpha : A^4 \right] &\Rightarrow [a : A, \alpha : A^4] \vdash e C \\
\left[ a : A \right] &\Rightarrow [a : A] \vdash e C \\
\left[ a : A \right] &\Rightarrow [a : A] \vdash e C \\
\end{align*}$$

**Step 4 – Explicit coercions** The only remaining step is to take into account de Bruijn levels both inside the source and target languages. In the target language, stores will then simply be defined as lists of terms (that is $[t, u, \ldots]$ rather than $[x := t, y := u, \ldots]$) while store types will simply be lists of types (i.e. $A, A^4, \ldots$ instead of $a : A, \alpha : A^4, \ldots$).

Interestingly, this requires giving computational content to the subtyping relation $\vdash_Y : Y$ through explicit coercions $\sigma : Y' : Y$ mapping each type in $Y$ to the corresponding type in $Y'$. In other words, considering a store $\tau' : Y'$ extending a store $\tau : Y$, a coercion $\sigma : Y' : Y$ indicates where each element of $\tau$ can be found in $\tau'$.

**Remark 1.** Looking carefully at the first three steps, we observe that the translation of a type $A$ at level $t$ is defined by applying a transformation on its translation at level $t$, which is itself defined as the same transformation applied to the translation at level $t$ and so on. Each step precisely consists in refining this transformation. Formally, if $F$ is a function taking a store type $Y$ and returning a type, let us define:

$$\Box F : Y \Rightarrow \forall Y' : Y, Y' \to (FY') \to \bot$$

which is also a function mapping store types $Y$ to types in the target of the translation. Then, writing $\vdash_e A$ for the function associating to any store type $Y$ the type $\vdash_e A$ (for $\vdash_e A$ a level among $e, t, \ldots$), the definition of the translation can be simply expressed by:

$$\vdash_e A = \Box (\vdash_e A) = \Box (\vdash_e A) = \ldots$$

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

- at step 1, $\Box F$ is $\vdash_e A = \Box (\vdash_e A) = \ldots$
- at step 2, $\Box F$ is $\vdash_e A = \Box (\vdash_e A) = \ldots$
- at step 3, $\Box F$ is $\vdash_e A = \Box (\vdash_e A) = \ldots$

3 $F_\gamma$: 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 $F_\gamma$. Each of the translations that we
A calculus of expandable stores

Hugo Herbelin and Étienne Miquey

<table>
<thead>
<tr>
<th>λ-calculus</th>
<th>( (k : A) \in S )</th>
<th>( (x : A) \in \Gamma )</th>
<th>( \Gamma \vdash x : A )</th>
<th>( \Gamma \vdash \lambda x.t : A \rightarrow B )</th>
<th>( \Gamma \vdash t : A \rightarrow B )</th>
<th>( \Gamma \vdash u : A )</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>( \Gamma \vdash k : A )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Stores**

<table>
<thead>
<tr>
<th>( \Gamma \vdash [\cdot] : \emptyset \tau \emptyset )</th>
<th>( \Gamma \vdash t : Y_0 \triangleright T )</th>
<th>( \Gamma \vdash \tau : Y_0 \triangleright Y )</th>
<th>( \Gamma \vdash \tau' : (Y_0; Y) \triangleright Y' )</th>
<th>( \Gamma \vdash \sigma : Y_1 \triangleright Y_0 )</th>
<th>( \Gamma \vdash \tau : Y_0 \triangleright Y )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \Gamma \vdash t : Y_0 \triangleright T )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Coercions**

<table>
<thead>
<tr>
<th>( \Gamma \vdash \varepsilon : \emptyset &lt; \emptyset )</th>
<th>( \Gamma \vdash \sigma' : \sigma' &lt; \sigma' &lt; \sigma' &lt; \sigma' )</th>
<th>( \Gamma \vdash \sigma : \sigma &lt; \sigma &lt; \sigma &lt; \sigma )</th>
<th>( \Gamma \vdash \sigma : \sigma &lt; \sigma &lt; \sigma &lt; \sigma )</th>
<th>( \Gamma \vdash \sigma : \sigma &lt; \sigma &lt; \sigma &lt; \sigma )</th>
<th>( \Gamma \vdash \sigma : \sigma &lt; \sigma &lt; \sigma &lt; \sigma )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \Gamma \vdash \sigma : \sigma &lt; \sigma &lt; \sigma &lt; \sigma )</td>
<td>( \Gamma \vdash \sigma : \sigma &lt; \sigma &lt; \sigma &lt; \sigma )</td>
<td>( \Gamma \vdash \sigma : \sigma &lt; \sigma &lt; \sigma &lt; \sigma )</td>
<td>( \Gamma \vdash \sigma : \sigma &lt; \sigma &lt; \sigma &lt; \sigma )</td>
<td>( \Gamma \vdash \sigma : \sigma &lt; \sigma &lt; \sigma &lt; \sigma )</td>
<td>( \Gamma \vdash \sigma : \sigma &lt; \sigma &lt; \sigma &lt; \sigma )</td>
</tr>
</tbody>
</table>

**Core**

<table>
<thead>
<tr>
<th>( \delta : Y_0 \triangleright Y )</th>
<th>( \delta : Y_0 \triangleright Y )</th>
<th>( \delta : Y_0 \triangleright Y )</th>
<th>( \delta : Y_0 \triangleright Y )</th>
<th>( \delta : Y_0 \triangleright Y )</th>
<th>( \delta : Y_0 \triangleright Y )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \Gamma \vdash \delta : Y_0 \triangleright Y )</td>
<td>( \Gamma \vdash \lambda \delta.t : Y_0 \triangleright Y \rightarrow B )</td>
<td>( \Gamma \vdash t : Y_0 \triangleright Y \rightarrow B )</td>
<td>( \Gamma \vdash \tau : Y_0 \triangleright Y \rightarrow B )</td>
<td>( \Gamma \vdash \tau : Y_0 \triangleright Y \rightarrow B )</td>
<td>( \Gamma \vdash \tau : Y_0 \triangleright Y \rightarrow B )</td>
</tr>
</tbody>
</table>

\[ \therefore \quad \Gamma \vdash t : A \quad \Gamma \vdash \lambda \delta.t : Y_0 \triangleright Y \rightarrow B \]

**Figure 6.** \( F_I \): Type system

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 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 \( F_I \). 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 \( F_I \). As we explained, we will focus on the case of a simply typed source calculus, whose types are defined by:

**Source types**

| \( A := X \mid A \rightarrow B \) | \( F := A \mid A^2 \) |

As explained above, a store \( \tau \) is simply given as a list whose type, written \( Y \), is defined as the list of the types of the elements \( \tau \) provides. Observe that if we consider the concatenation of such two stores \( \tau_0; \tau_1 \) of type \( Y_0; Y_1 \), thinking of them as substitutions, \( \tau_1 \) provides elements for \( Y_1 \) only if it is given with a prefix providing \( Y_0 \) (see also the Step 2 described earlier). We denote its type with \( Y_0 \triangleright Y_1 \) (the type of a “self-sufficient” store, which we will abbreviate by \( Y_0 \)). Obviously, such a store should also be compatible with any extension of \( Y_0 \), which justifies the introduction of the constructor \( Y_0 \triangleright Y_1 \) where \( \sigma \) is of type \( Y_0 \triangleright Y_1 \) and the resulting store is of type \( Y_0 \triangleright Y_1 \).

Coercions are simply defined through the natural structure witnessing list inclusion: \( \sigma^+ \) (resp. \( \uplus \sigma \)) witnesses the fact that \( Y, F \) (resp. \( Y \)) is included in \( Y', F \) provided that \( \sigma \) witnesses that \( Y \) is included in \( Y' \). Having in mind that list inclusion corresponds to a subtyping relation for stores, we denote it by \( Y' \triangleright Y \). We denote by \( \sigma^0 \circ \sigma \) the composition of two coercions, and by \( \sigma^+ \) (resp. \( \uplus \sigma \)) the twin of the previous coercions witnessing the addition of a list of type \( Y \).

Finally, System \( F_I \) 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...
to split a given store using a coercion. The resulting syntax is given by the following grammar:

\[
\begin{align*}
\text{Store type} & : Y ::= Y | \emptyset | Y, F | Y; Y' \\
\text{Stores} & : \tau ::= \delta | [\cdots] | \{ \cdots \} | r; \tau' | \Gamma; \tau \\
\text{Coercions} & : \sigma ::= s \mid \epsilon \mid \sigma' \mid \sigma \circ \sigma' \mid \sigma^+ \mid \|\| \tau \sigma
\end{align*}
\]

\[\text{Contexts} \Gamma ::= \Gamma, s : Y' < Y | \Gamma, \delta : Y < Y' \mid \Gamma, x : T\]

\[\text{Types} \quad T ::= X | T \rightarrow U | \forall Y.T \mid Y < : T \rightarrow Y' \mid Y > : T \rightarrow T\]

\[\text{Terms} \quad t ::= k | x \mid \lambda x. t \mid u \mid \lambda x. t \mid \Gamma \mid \lambda \delta.t \mid \tau \mid \epsilon \mid \sigma\]

We require a concrete list of types (defined in the next section) and where \(\forall\) the current store type (\(\delta\)) is given by the following grammar:

\[
\begin{align*}
\text{Eq.} & : \vdash \epsilon : Y, \lambda \quad | \quad \vdash \sigma : \forall \downarrow X, Y
\end{align*}
\]

Assume that for any \(\forall\) \(\delta\) is a type. The following rules are admissible:

\[
\begin{align*}
\Gamma, s : Y < : Y, \delta : \emptyset \Rightarrow \Gamma \vdash \lambda s \delta x. t : \forall \downarrow Y \\
\Gamma \vdash \tau \Rightarrow \forall \downarrow Y \\
\Gamma \vdash r : \forall \downarrow Y \Rightarrow \Gamma \vdash u : \forall \downarrow Y \quad (\varepsilon)
\end{align*}
\]

As we shall see in the next sections, we will mainly use these "packed" abstractions and applications to define the different translations (observe that \(\square F Y\) satisfies (Eq.)). 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 \(\tau \at \delta\) and \(\forall\) is expected from the source calculus, where \(\epsilon\) 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\(^2\), which will be translated as such). Since our syntax implicitly assume that stores of types \(\emptyset\) can be lifted to match extensions of \(T_0\), for our system to be sound, we need to assume that terms in the store can be lifted as well. Formally, we require that \(Y \Rightarrow F\) is of the shape\(^3\):

\[
\text{(Eq.\(\Rightarrow\))} \quad Y \Rightarrow F \iff \forall Y < : Y, \forall Y (F, Y)
\]

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

- **split \(\tau\) at \(n\)** along \(\sigma\) is of the shape \([\Gamma_0] T \mid [\Gamma_1]\) where \(\epsilon\) replaces \(\epsilon\).
- **Alternative**, a coercion \(\sigma : \forall \downarrow Y\) can actually be identified with a partial monotone function \([\sigma] N\) from \([0, \forall\downarrow Y]\) to \([0, \forall\downarrow Y]\) which intuitively maps the index of every type \(\forall\) \(\epsilon\) to its corresponding index in \(\forall\) \(\epsilon\). (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 \(\{\{\}^\epsilon\}^\epsilon\) which is in normal form, we have:

- **normal form**: \(T_0, T, U, T_1 \Rightarrow T, U\)
- **domain**: \(\sigma = 2\), \(\text{codomain}(\sigma) = 4\)
- **as \(\sigma\)** from \([0, \forall\downarrow Y]\) to \([0, \forall\downarrow Y]\)

Visually, this corresponds to the situation pictured on the right.
A calculus of expandable stores

Hugo Herbelin and Étienne Miquey

Parameter $\text{Ty} : \text{Type}$.

Inductive $\text{hlist} :=$
| $\text{nil}$ : $\text{hlist}$
| $\text{hcons} : \forall A, A \rightarrow \text{hlist} \Rightarrow \text{hlist}$

Definition $\text{store} := \text{hlist}$.

Inductive $\llbracket \text{store} \rightarrow \text{Type} \rrbracket :=$
| $\text{empty} : \text{nil} \llbracket \text{nil} \rrbracket$
| $\text{lift} : \forall Y, Y, A, Y <: [Y, A] <: Y$

Parameter $\triangleright : \text{store} \rightarrow \text{Ty} \rightarrow \text{Type}$.

Context $(F : \text{store} \rightarrow \text{Ty} \rightarrow \text{Type})$

$\triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangleright \triangle...
A calculus of expandable stores

4.1 A typed call-by-need translation for the \( \Lambda_{(\tau \leftarrow \tau \star)} \)-calculus

4.1.1 Translation of terms

We can now take advantage of the features of system \( F_T \) to type Ariola et al.'s untyped translation for the \( \Lambda_{(\tau \leftarrow \tau \star)} \)-calculus (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 it can be decided which reduction rule to apply by analyzing only the term or the context independently) [5]. The translation of terms is nothing more than the untyped translation of 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 \( \tau[t]; \tau' \), \( t \) has its levels coherent with its prefix \( \tau \), and ignores its suffix \( \tau' \). In terms of types, if \( \tau[t] \) is of type \( Y \), \( A \) then \( t \) will be of a type \( Y \bowtie A \).
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 \( \| x \|_V \) and \( \| \bar{\mu}[x_i]. (x \parallel F) \tau' \|_E \). In the untyped translation (see Appendix B.1), we have:

\[
\| \bar{\mu}[x_i]. (x \parallel F) \tau' \|_E = \forall \bar{x} \forall x (x : \tau[t]; \tau'[t]) \| F \|_F
\]

\[
\| x \|_V = \forall \bar{x} \forall x (x : \tau[t]; \tau'[t]) \| F \|_F
\]

Let us first focus on the \( \| \bar{\mu}[x_i]. (x \parallel F) \tau' \|_E \). 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 \( \tau[x := \| V \|_V] \tau' \) and passes it to \( V \) with the continuation \( \| F \|_E \). Now, when using de Bruijn levels, the continuation was expecting a store \( \tau_0 \) of type \( Y_0 \) that \( \tau \) (the actual store, of type \( Y \)) is extending, hence \( \tau \) comes together with a coercion \( \sigma : Y < Y_0 \) witnessing that \( Y \) is an extension of \( Y_0 \). Let us loosely identify the stores with their types and write \( \sigma : \tau < \tau_0 \) to simplify our explanation. The value \( V \) has its de Bruijn levels consistent with \( \tau \), but \( \| F \|_E \) and \( \| \tau' \|_E \) have to be updated. In detail, \( \| \tau' \|_E \) was expecting \( \tau_0[\tau[t]] \), we thus update it with \( \sigma \tau' \) which witnesses \( \tau_0[\tau[t]] \tau < \tau_0[\tau[t]] \). On the other hand, \( F \) was waiting for \( \tau_0[\tau[t]] \tau' \), we thus need to update it with \( \sigma \tau' = (\sigma + \tau') \tau' \). Finally, we need to give to \( V \) a coercion witnessing the extension of \( \tau \) into \( \tau_0[\tau[t]] \tau' \), that is to say \( \| \mu \|_E \). In the end, we obtain the following definition:

\[
\| \bar{\mu}[x_i]. (x \parallel F) \tau' \|_E = \forall \bar{x} \forall x (x : \tau[t]; \tau'[t]) \| F \|_F
\]

where \( \| \mu \|_E = \| \bar{\mu} \|_E \) and \( \tau' : \Gamma' \) in the source of the translation.
type $T$ in the signature of the target language that we also denote by $k$ (resp. $\kappa$ of type $T \rightarrow \perp$).

### 4.1.2 Translation of types

Regarding the translation of types, it follows exactly the intuition we presented in Section 2.1, so that we mostly said everything about it already. To summarize the construction, we start by embedding the types and typing contexts of the source calculus thanks to the $\tau$ function. A typing context $\Gamma = x_1 : T_1, \ldots, x_n : T_n$ is then translated into the store type $\llbracket \Gamma \rrbracket = T_1, \ldots, T_n$. This allows us to translate a sequent $e.g., \Gamma \vdash t : T$, into a judgment $\llbracket t \rrbracket : \llbracket \Gamma \rrbracket \vdash T$. The type $\llbracket \Gamma \rrbracket \vdash T$ can be understood as the types of terms translated at level $\tau$, which are waiting for any store extending $\llbracket \Gamma \rrbracket$ and a continuation at the inferior level (i.e. $E$) for the very same type $T$ but interpreted with the extended store type $Y$:

$$\llbracket \Gamma \rrbracket \vdash T \triangleq \forall Y <: \llbracket \Gamma \rrbracket : Y \rightarrow (Y \llbracket \Gamma \rrbracket \vdash T) \rightarrow \perp$$

It is worth noting that the translation $\llbracket \Gamma \rrbracket \vdash T$ is defined internally in system $F_t$, which allows in particular the recursive definition $Y \llbracket \Gamma \rrbracket \vdash T$ to make sense (since $Y$ is at the moment an interleaving of types in $\Gamma$ and second-order variables that are not the images of types in the source calculus). As we already explained, the different levels $e, t, E, V, F, \nu$ of translation reflect the dynamics of the (context-free) reduction system of the $\overline{\lambda \mu \nu \xi \tau}$-calculus, that is to say the different syntactic categories which are examined successively during the reduction\(^\text{16}\).

The resulting translation, which is given in Figure 9, is sound, i.e. the provability of a sequent in the source calculus (say $\Gamma \vdash t : T$) entails the provability of its translation ($\llbracket \Gamma \vdash t : T \rrbracket$) in $F_t$, which is the main result of this section:

**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

---

\(^\text{16}\)The context-free reduction rules are given in Appendix C.
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 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 and thus there is no need for an extra layer of alternation to handle their (shared) evaluation. Both translations are given in Figure 10, and again, we have:

**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. \(\square\)

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 $[t]$, 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 $x : A, y : B \vdash u : C$, through the translation we will thus have $\vdash [u]_t : A, B \vdash \lambda \tau u : C$. 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, $t_0$ is going to produce arbitrary computations (and in particular store arbitrarily many terms, let us denote the resulting store by $\tau_0 : \bar{U}_1$) before returning $V_1$ to its continuation. These terms can thus be assigned the types ($A \rightarrow D$) $→ D$, ($B \rightarrow D$) $→ D$, ($C \rightarrow D$) $→ D$, and the closed term $t_u \triangleq t_0(x,t_1(y,t_2u))$ can thus be typed by $t_u : D$. Now, if $t_u$ is evaluated in an initially empty store, at the moment where $uV_2$ will be evaluated, the store will be $\tau_0[x := V_0]t_1[y := V_1]t_2$ of type $\bar{U}_0, A, \bar{U}_1, B, \bar{U}_2$.

4.3 Using System F as source calculus

In addition to being compatible with different evaluation strategies, $F_t$ 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]:

$$
\forall X.F \triangleq \forall(X : Y \rightarrow T).Y \triangleright F \\
Y \triangleright X \triangleq X \triangleright Y
$$

5 Conclusion

**Conclusion** Through the definition of $F_t$, 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 $\lambda[l]_{\lambda \tau_{\downarrow}}$-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 $F_\ll$ [7] and dependently typed calculi (to manipulate sized lists). Yet, the precise logical strength of $F_\ll$ is unclear and is still to determine.

Last but not least, we would like to investigate whether the $\Box$ can be considered as a modality, and in particular whether we could optimize the translation by using a polarized source calculus, inserting the $\Box$ 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 $\lambda$-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


A calculus of expandable stores

A.1 The MAM and the call-by-name \( \mu \bar{\mu} \)-calculus with global environments

It is quite obvious that the call-by-name \( \mu \bar{\mu} \)-calculus with global environments allows us to faithfully simulate reductions of the MAM (which we recall in Fig. 11). We first define the following compilation function from states of the MAM to closures of the \( \mu \bar{\mu} \)-calculus:

\[
\begin{align*}
\llbracket t \star \pi \star \tau \rrbracket & \triangleq \langle \llbracket t \rrbracket \| \llbracket \pi \rrbracket \| \llbracket \tau \rrbracket \rangle, \\
\end{align*}
\]

with:

\[
\begin{align*}
\llbracket x \rrbracket & \triangleq x, \\
\llbracket \lambda x.t \rrbracket & \triangleq \lambda x.\llbracket t \rrbracket, \\
\llbracket tu \rrbracket & \triangleq \mu \alpha.\llbracket u \rrbracket \| \llbracket \pi \rrbracket \| \llbracket \alpha \rrbracket,
\end{align*}
\]

where \( \kappa \) is a fixed co-constant materializing the end of the execution.

It is then quite easy to verify that reductions of the MAM are preserved through the compilation process (modulo the fact that we consider terms of the \( \mu \bar{\mu} \)-calculus up to \( \alpha \)-conversion). Formally, to avoid considering the contexts stored in the environment, we first define a substitution function for co-variables. We write \( c(\tau) \) for the closure \( c\tau \) in which all the co-variables \( \alpha \) bound in \( \tau \) are recursively substituted by the terms to which they are bound and where \( \tau' \) consists of the fragment of \( \tau \) binding only variables:

\[
c(\epsilon) \triangleq c \\
\llbracket c(\tau[x := t]) \rrbracket \triangleq (c(\tau))[x := t] \\
\llbracket c(\tau[\alpha := E]) \rrbracket \triangleq (c(E/\alpha))(\tau)
\]

We then say that two closures \( c\tau \) and \( c'\tau' \) are equal up to co-variables substitutions, which we denote by \( c\tau \equiv c'\tau' \), whenever \( c\tau = c'\tau' \).

**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 \( c'\tau' \) such that we have \( \llbracket S \rrbracket \xrightarrow{1} c'\tau' \) and \( (c'\tau') \equiv \llbracket S' \rrbracket \).

**Proof.** Trivial induction on reduction rules of the MAM. \( \square \)

In other words, we showed that a variant of the \( \mu \bar{\mu} \)-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 \( \bar{\mu}[t \star \tau \star \pi] \)-calculus

Similarly, we can prove that the \( \bar{\mu}[t \star \tau \star \pi] \)-calculus allows us to simulate reductions of the MAD. The compilation function from states of the MAD to closures of the \( \bar{\mu}[t \star \tau \star \pi] \)-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 \( \bar{\mu}[t \star \tau \star \pi] \)-calculus through the binder \( \bar{\mu}[x].(x \parallel F)\tau' \). Following this intuition, the definition of the translation is almost direct:

\[
\begin{align*}
\llbracket t \star \pi \star \tau \star D \rrbracket & \triangleq \langle \llbracket t \rrbracket \| \llbracket \pi \rrbracket \| \llbracket D \rrbracket \rangle \| \llbracket \tau \rrbracket \\
\end{align*}
\]
A calculus of expandable stores

Hugo Herbelin and Étienne Miquey

with:

\[ J \equiv x \]

\[ \lambda x. [r] \]

\[ [tx] \equiv \mu \alpha. ([r] \parallel [u] \cdot \alpha) \]

\[ J \equiv \begin{array}{c}
\llbracket x \rrbracket \triangleq x \\
\llbracket \lambda x. [r] \rrbracket \triangleq \lambda x. [r] \\
\llbracket tx \rrbracket \triangleq \mu \alpha. ([r] \parallel [u] \cdot \alpha) \\
\end{array} \]

\[ J \equiv \begin{array}{c}
\llbracket t[x := t] \rrbracket \triangleq \llbracket t \rrbracket \\
\llbracket \tau \rrbracket \triangleq \epsilon \]

\[ J \equiv \begin{array}{c}
\llbracket (\pi, \tau) \mapsto D \rrbracket \triangleq \bar{\mu}[x].(x \parallel [\pi]^{D} \parallel \tau) \rrbracket \\
\llbracket \epsilon \rrbracket \triangleq \kappa \]

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 \( \llbracket S \rrbracket \xrightarrow{c' \tau'} \llbracket S' \rrbracket \).

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

Hugo Herbelin and Étienne Miquey

B The $\overline{\lambda_{[\ell r\star]}}$-calculus

B.1 Definitions

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

We recall here the definition of Ariola et al.’s $\overline{\lambda_{[\ell r\star]}}$-calculus [5]. The syntax and reduction rules are given in Fig. 12, while the type system, defined in [26], is given in Fig. 13. Finally, Ariola et al.’s original untyped CPS translation is given in Fig. 14.

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

The original presentation of the $\overline{\lambda_{[\ell r\star]}}$-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 $t = \mu x.(u \parallel \#x.(x \parallel \alpha))$ and a context of the shape $e = \#x.(x \parallel F)$. 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:

\[
\Gamma \vdash \mu \lambda \alpha. \langle u \| \phi x. \langle \alpha \| F \rangle \rangle \rightarrow \langle x \| F \rangle [\alpha := \mu \lambda \alpha. \langle u \| \phi x. \langle \alpha \| F \rangle \rangle] \\
\rightarrow \mu \alpha. \langle u \| \phi x. \langle \alpha \| F \rangle \rangle \rightarrow \langle x \| F \rangle [\alpha := \mu \lambda \alpha. \langle u \| \phi x. \langle \alpha \| F \rangle \rangle] \\
\rightarrow \langle u \| \phi x. \langle \alpha \| F \rangle \rangle [\alpha := \mu \lambda \alpha. \langle u \| \phi x. \langle \alpha \| F \rangle \rangle, x := u] \\
\rightarrow \langle x \| F \rangle [\alpha := \mu \lambda \alpha. \langle u \| \phi x. \langle \alpha \| F \rangle \rangle, x := u] \\
\rightarrow \langle u \| \phi x. \langle \alpha \| F \rangle \rangle [\alpha := \mu \lambda \alpha. \langle u \| \phi x. \langle \alpha \| F \rangle \rangle, x := u] \\
\rightarrow \langle x \| F \rangle [\alpha := \mu \lambda \alpha. \langle u \| \phi x. \langle \alpha \| F \rangle \rangle, x := u, x := x] \rightarrow \ldots
\]

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. \(\llbracket \langle t \| e \rangle \rrbracket\) is defined from \(\llbracket e \rrbracket\) and \(\llbracket t \rrbracket\)), 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:

\[
\begin{array}{l}
\text{let } \mu x \cdot (x \parallel F) \text{ in } (x \parallel F) \\
\text{let } \lambda x . (x \parallel \alpha) \text{ in } (x \parallel (\mu x . (x \parallel F)) \parallel (x \parallel (\lambda x . (x \parallel \alpha)) \parallel (x \parallel F))) \\
\text{let } \lambda x . (x \parallel \alpha) \text{ in } (\mu x . (x \parallel F) \parallel (x \parallel (\lambda x . (x \parallel \alpha)) \parallel (x \parallel F))) \\
\text{let } \lambda x . (x \parallel \alpha) \text{ in } (x \parallel F) \parallel (x \parallel (\lambda x . (x \parallel \alpha)) \parallel (x \parallel F)) \\
\text{let } \lambda x . (x \parallel \alpha) \text{ in } (x \parallel F) \parallel (x \parallel (\lambda x . (x \parallel \alpha)) \parallel (x \parallel F)) \\
\text{let } \lambda x . (x \parallel \alpha) \text{ in } (x \parallel F) \parallel (x \parallel (\lambda x . (x \parallel \alpha)) \parallel (x \parallel F))
\end{array}
\]

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 \(\alpha\)-conversion to prevent the formation of the cyclic reference \([x := [x]_V]\). This is why we need either to be able to perform \(\alpha\)-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 \(\overline{\alpha} \text{[\![\tau \tau \tau \tau]!]_{\overline{\sigma}}\text{,}}\) using de Bruijn levels. As we observed in the previous example, the issue arises when adding a binding \([x := \ldots]\) 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:

\[
\begin{array}{l}
\text{let } \mu x . (x \parallel \alpha) \text{ in } (x \parallel F) \parallel (x \parallel (\mu x . (x \parallel F)) \parallel (x \parallel (\lambda x . (x \parallel \alpha)) \parallel (x \parallel F))) \\
\text{let } \lambda x . (x \parallel \alpha) \text{ in } (\mu x . (x \parallel F) \parallel (x \parallel (\lambda x . (x \parallel \alpha)) \parallel (x \parallel F))) \\
\text{let } \lambda x . (x \parallel \alpha) \text{ in } (x \parallel F) \parallel (x \parallel (\lambda x . (x \parallel \alpha)) \parallel (x \parallel F)) \\
\text{let } \lambda x . (x \parallel \alpha) \text{ in } (x \parallel F) \parallel (x \parallel (\lambda x . (x \parallel \alpha)) \parallel (x \parallel F)) \\
\text{let } \lambda x . (x \parallel \alpha) \text{ in } (x \parallel F) \parallel (x \parallel (\lambda x . (x \parallel \alpha)) \parallel (x \parallel F))
\end{array}
\]

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 \([\alpha]_\mu^\sigma\) where \(\sigma\) is a substitution used to rename variables. To compact the notations, we write \([x]_{\mu}^\sigma[\ldots]_\mu^\sigma\) for the renaming substitution \([x := m, \alpha := \gamma, \ldots,]\), 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 \([x]_{\mu}^\sigma_\mu^\sigma\) instead of \([x]_{\mu}^\sigma_\mu^\sigma\). Using this trick, the translation of the former command would be (where \(m\) and \(n\)
are fresh names generated during the translation):
\[
\begin{align*}
[ce]_t^i &= [e]_t^i \epsilon [t]_t^i = [\tilde{\mu} x. (x \parallel F)]_c^i \epsilon [t]_t^i \\
&= [[(x \parallel F)]_c^i m := [t]_t^i] \\
&= [[x]_t^i m := [t]_t^i] \parallel [F]_c^i \\
&= [[\mu a. (u \parallel \tilde{\mu} x. (x \parallel a))]_t^i J = [\lambda \tau \lambda V. V \tau [m := \tilde{\iota} V] [F]_F^{\tilde{\iota} V}] \\
&= [[(u \parallel \tilde{\mu} x. (x \parallel a))]_t^i J = [\lambda \tau \lambda V. V \tau [m := \tilde{\iota} V] [F]_F^{\tilde{\iota} V}] \\
&= [[\tilde{\mu} x. (x \parallel a)]_t^i J = [\lambda \tau \lambda V. V \tau [m := \tilde{\iota} V] [F]_F^{\tilde{\iota} V}] \\
&= [[(x \parallel a)]_c^i x := m, a := y, x := n J = [\lambda \tau \lambda V. V [m := \tilde{\iota} V] [F]_F^{\tilde{\iota} V}, n := [u]_t^i \eta] \\
&= [[\alpha]_c^i \eta \eta] J = [\lambda \tau \lambda V. V [m := \tilde{\iota} V] [F]_F^{\tilde{\iota} V}, n := [u]_t^i \eta, m := [x]_v^i \eta] \\
&= [(\lambda \tau \lambda V. V \tau [m := \tilde{\iota} V] [F]_F^{\tilde{\iota} V}, n := [u]_t^i \eta, m := [x]_v^i \eta)] \\
&= [[x]_v^i \eta, \eta] J = [\lambda \tau \lambda V. V [m := \tilde{\iota} V] [F]_F^{\tilde{\iota} V}, n := [u]_t^i \eta, m := [x]_v^i \eta] \\
&= [[x]_v^i \eta, \eta] J = [\lambda \tau \lambda V. V [m := \tilde{\iota} V] [F]_F^{\tilde{\iota} V}, n := [u]_t^i \eta, m := [x]_v^i \eta]
\end{align*}
\]

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 reformulation 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 \( \uparrow_i^n t \), 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:

\[
\begin{align*}
\uparrow_i^n (ct) &= \Delta (\uparrow_i^n c)(\uparrow_i^n t) \\
\uparrow_i^n (t \parallel e) &= \Delta (\uparrow_i^n t \parallel \uparrow_i^n e) \\
\uparrow_i^n (\kappa) &= \Delta \kappa \\
\uparrow_i^n (t \cdot E) &= \Delta (\uparrow_i^n t) \cdot (\uparrow_i^n E) \\
\uparrow_i^n (\alpha_j) &= \Delta \alpha_j \quad \text{(if } j < i \text{)} \\
\uparrow_i^n (\alpha_j) &= \Delta \alpha_{j+n} \quad \text{(if } j \geq i \text{)} \\
\uparrow_i^n (\tilde{\mu}[x_j]. (x_j \parallel F) t) &= \Delta \tilde{\mu}[\uparrow_i^n x_j]. (\uparrow_i^n (x_j \parallel F) t) \\
\uparrow_i^n (\tilde{\mu} x_j. c) &= \Delta \tilde{\mu}[\uparrow_i^n x_j]. (\uparrow_i^n c) \\
\uparrow_i^n (r[x_j := t]) &= \Delta \uparrow_i^n (r)[\uparrow_i^n x_j := \uparrow_i^n t] \\
\uparrow_i^n (r[\alpha_j := E]) &= \Delta \uparrow_i^n (r)[\uparrow_i^n \alpha_j := \uparrow_i^n E] \\
\uparrow_i^n (\kappa) &= \Delta \kappa \\
\uparrow_i^n (\lambda x_j. t) &= \Delta \lambda[\uparrow_i^n x_j]. (\uparrow_i^n t) \\
\uparrow_i^n (x_j) &= \Delta x_j \quad \text{(if } j < i \text{)} \\
\uparrow_i^n (x_j) &= \Delta x_{j+n} \quad \text{(if } j \geq i \text{)} \\
\uparrow_i^n (\mu a_j. c) &= \Delta \mu[\uparrow_i^n a_j]. (\uparrow_i^n c)
\end{align*}
\]
C  Context-free abstract machines

C.1  The named context-free abstract machine for the $\lambda_{\tau^\star}$-calculus

<table>
<thead>
<tr>
<th>Expression</th>
<th>Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\langle t \parallel \mu x.c \rangle_e \tau$</td>
<td>$\rightarrow c_e[x := t]$</td>
</tr>
<tr>
<td>$\langle t \parallel E \rangle_e \tau$</td>
<td>$\rightarrow \langle t \parallel E \rangle_t \tau$</td>
</tr>
<tr>
<td>$\langle \mu \alpha.c \parallel E \rangle_t \tau$</td>
<td>$\rightarrow c_e[\alpha := E]$</td>
</tr>
<tr>
<td>$\langle V \parallel E \rangle_t \tau$</td>
<td>$\rightarrow \langle V \parallel E \rangle_v \tau$</td>
</tr>
<tr>
<td>$\langle V \parallel \mu[x].\langle x \parallel F \rangle \tau \rangle_t \tau$</td>
<td>$\rightarrow \langle V \parallel \mu[x].\langle x \parallel F \rangle \tau \rangle_v \tau$</td>
</tr>
<tr>
<td>$\langle V \parallel F \rangle_t \tau$</td>
<td>$\rightarrow \langle V \parallel F \rangle_v \tau$</td>
</tr>
<tr>
<td>$\langle V \parallel \langle x \parallel F \rangle \tau \rangle_t \tau$</td>
<td>$\rightarrow \langle V \parallel \langle x \parallel F \rangle \tau \rangle_v \tau$</td>
</tr>
<tr>
<td>$\langle V \parallel u \cdot E \rangle_t \tau$</td>
<td>$\rightarrow \langle V \parallel u \cdot E \rangle_v \tau$</td>
</tr>
<tr>
<td>$\langle \lambda x.t \parallel u \cdot E \rangle_v \tau$</td>
<td>$\rightarrow \langle u \parallel \mu x.(\langle t \parallel E \rangle) \rangle_e \tau$</td>
</tr>
</tbody>
</table>

Figure 15. Context-free abstract machine for the $\lambda_{\tau^\star}$-calculus [5]

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

<table>
<thead>
<tr>
<th>Expression</th>
<th>Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\langle t \parallel \mu x.c \rangle_e \tau$</td>
<td>$\rightarrow c_e[n/x]_e \tau[x_n := t]$ with $</td>
</tr>
<tr>
<td>$\langle t \parallel E \rangle_e \tau$</td>
<td>$\rightarrow \langle t \parallel E \rangle_t \tau$</td>
</tr>
<tr>
<td>$\langle \mu \alpha.c \parallel E \rangle_t \tau$</td>
<td>$\rightarrow c[n/\alpha]_e \tau[\alpha_n := E]$ with $</td>
</tr>
<tr>
<td>$\langle V \parallel \mu x.c \rangle_e \tau$</td>
<td>$\rightarrow \langle V \parallel \mu x.\langle x \parallel E \rangle \rangle_t \tau$</td>
</tr>
<tr>
<td>$\langle V \parallel E \rangle_t \tau$</td>
<td>$\rightarrow \langle V \parallel E \rangle_v \tau$</td>
</tr>
<tr>
<td>$\langle V \parallel \mu[\alpha][E] \rangle_t \tau$</td>
<td>$\rightarrow \langle V \parallel \mu[\alpha][E] \rangle_v \tau$</td>
</tr>
<tr>
<td>$\langle V \parallel u \cdot E \rangle_t \tau$</td>
<td>$\rightarrow \langle V \parallel u \cdot E \rangle_v \tau$</td>
</tr>
<tr>
<td>$\langle \lambda x.t \parallel u \cdot E \rangle_v \tau$</td>
<td>$\rightarrow \langle u \parallel \mu x.\langle t \parallel E \rangle \rangle_e \tau$</td>
</tr>
</tbody>
</table>

Figure 16. Context-free abstract machine for the call-by-name $\hat{\lambda} \mu \hat{\mu}$-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 $\sigma_I$ is in normal form, then the following rule is admissible:

$$\frac{\Gamma \vdash \sigma_0 : Y_0' \preceq Y_0 \quad \Gamma \vdash \sigma_I : Y_I' \preceq Y_I}{\Gamma \vdash \sigma_0 ; \sigma_I : Y_0' ; Y_I' \preceq Y_0 ; Y_I}$$

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

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

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 $\rightarrow_{\sigma}$. In other word, we can define the composition function $- \odot -$ between coercions in normal form by:

$$\begin{align*}
\sigma_1^+ \odot \sigma_0^+ &\triangleq (\sigma_1 \odot \sigma_0)^+ \\
\uplus \sigma_1 \odot \sigma_0 &\triangleq \uplus (\sigma_1 \odot \sigma_0) \\
\sigma_1^+ \uplus \sigma_0 &\triangleq \uplus (\sigma_1 \odot \sigma_0) \\
\varepsilon \odot \sigma_0 &\triangleq \sigma_I^1 \odot \varepsilon \triangleq \varepsilon
\end{align*}$$

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 $\vdash \sigma : Y <\: Y'$ and $\vdash \sigma' : Y' <\: Y''$, then $\vdash \sigma' \odot \sigma : Y <\: Y''$.

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

$$\sigma ::= \varepsilon \mid \sigma^+ \mid \uplus \sigma \mid \sigma' \odot \sigma$$

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 $\Gamma \vdash \sigma : Y <\: Y$ then there exists $\sigma_n$ in normal form such that $\Gamma \vdash \sigma_n : Y' <\: Y$.

Proof. By induction on typing derivations, using the previous lemma for the ($\preceq_{\sigma}$)-rule.

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

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

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 $\uplus_1 \sigma_n$ and $\sigma_n^+$ where $Y$ 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 $\Uparrow((\Uparrow t)++)$ which is in normal form, we have:

- $\vdash \Uparrow((\Uparrow t)++) : T_0, T, U, T_1 <: T, U$
- $\text{dom}(\sigma) = 2$, $\text{codom}(\sigma) = 4$
- $\|\sigma\| : \begin{cases} 
 0 \mapsto 1 \\
 1 \mapsto 2 \\
 2 \mapsto 4 
\end{cases}$

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. $\vdash \sigma : Y' <: Y$, then:

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

Proof. The first two items are proved by a straightforward induction on typing derivations. The third and fourth items are then proved together, again by induction on typing derivations: the case $(<_{\text{id}})$ is trivial; while for $(<_{\text{w}})$ and $(<_{\text{w}})$ it suffices to unfold the definition, using the first items to connect $|Y|$ and $\text{dom}(\sigma)$.

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

1. For any $Y$, we have $\vdash 1 : Y <: \Uparrow Y$ is admissible.
2. If $\vdash \sigma : Y <: Y'$ and $\vdash \sigma' : Y' <: Y''$, then $\vdash \sigma \circ \sigma' : Y <: Y''$.
3. If $\vdash \sigma' : Y <: Y'$ and $\vdash \sigma' : Y' <: Y$, 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 $[\|\sigma\|$ and $[\|\sigma'\|$ 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:

$$\frac{\Gamma \vdash t : A}{\Gamma' \vdash t : A} \quad (\text{id})$$

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 $Y' <: Y$ and a term $t$ whose type is of the shape $\forall Y <: Y.A$, we defined:

$$(\Uparrow t) \triangleq \lambda Ys.t\ Y\ (s \circ \sigma)$$

Lemma D.9. The following rule is admissible:

$$\frac{\Gamma \vdash \lambda Ys.t\ Y\ (s \circ \sigma) : \forall Y <: Y'.A}{\Gamma \vdash \Uparrow t : \forall Y <: Y'.A} \quad (\Uparrow)$$

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

$$\frac{\Gamma \vdash t : \forall Y <: Y_0.A \quad \Gamma \vdash \sigma : Y_1 <: Y_0 \quad \Gamma, s : Y <: Y_1 \vdash t \circ s : X <: Y_1'}{\Gamma, s : Y <: Y_1 \vdash \Uparrow t : \forall Y <: Y_1'.A} \quad (\Uparrow)$$

$$\frac{\Gamma, s : Y <: Y_1 \vdash \Uparrow t : \forall Y <: Y_1'.A}{\Gamma \vdash \lambda Ys.t\ Y\ (s \circ \sigma) : \forall Y <: Y_1'.A} \quad (\text{over})$$

$$\frac{\Gamma, s : Y <: Y_1 \vdash \Uparrow t : \forall Y <: Y_1'.A \quad \text{Y} \notin \text{FV}(\Gamma)}{\Gamma \vdash \lambda Ys.t\ Y\ (s \circ \sigma) : \forall Y <: Y_1'.A} \quad (\text{over})$$
where we use Lemma D.8 to weaken $\Gamma, \sigma : X <: Y_1$. 

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

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

$$
\Gamma \vdash t : Y_0 \triangleright F \quad \Gamma \vdash \sigma : Y_1 <: Y_0 \\
\Gamma \vdash (\langle t \rangle_\sigma) : Y_1 \triangleright F
$$

**Lemma D.11.** If $\sigma_1$ is in normal form, then the following rule is admissible:

$$
\Gamma \vdash \sigma_0 : Y_0 <: Y_0 \quad \Gamma \vdash \sigma_1 : Y_1' <: Y_1 \\
\Gamma \vdash \sigma_0; \sigma_1 : [Y_0; Y_1'] <: Y_0; Y_1
$$

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 $\Gamma, \delta : Y_0 \triangleright Y_1, \Gamma' \vdash t : B$ and $\Gamma \vdash \tau : \delta \rightarrow \delta$, then $\Gamma, \Gamma' \vdash t[\tau/\delta] : B$.
3. If $\Gamma, s : Y, \Gamma \vdash t : B$ 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:

$$
\Gamma \vdash \tau \vdash \tau [r] \rightarrow \tau (\langle \tau \rangle_\tau \triangleright \tau[t] t)
$$

Indeed, if we have:

$$
\Gamma \vdash \sigma : Y_1 <: Y_0 \quad \Gamma \vdash t : Y_0; Y \triangleright F \\
\Gamma \vdash \tau[t] : Y_0 \triangleright \tau, Y, F
$$

we can derive (using Corollary D.10):

$$
\Gamma \vdash \sigma[Y_1] : Y_0 \triangleright Y \quad \Gamma \vdash t[Y_0] : Y_0; Y \triangleright F \\
\Gamma \vdash \tau \triangleright \tau[t] \vdash \tau[Y_1] \triangleright \tau, Y, F
$$

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

$$
\Gamma \vdash \tau : Y' \quad \Gamma \vdash \sigma : Y' <: Y \quad \Gamma = \Gamma_0[F, \Gamma] \\
\Gamma \vdash \text{split } \tau \text{ at } n \text{ along } \sigma : Y' <: Y \text{ as } (Y_0, s_0, \delta_0), x, (Y_1, s_1, \delta_1) \text{ in } t : A'
$$

where $\Gamma' = \Gamma[Y_0, F; Y_1/Y']$ and $A' = \mathcal{A}[Y_0, F; Y_1/Y']$ (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 $s_0, s_1, \ldots$ thus referring to $Y_0, Y_1$ and terms referring 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 $s_0 : Y_0, F; Y_1 ; s_1 : Y' : Y_0, F; Y_1$ in the premise. In addition to giving access to subterm in $t$ to both representations of $Y'$, it also enforces the equality between $Y'$ and $Y_0, F; Y_1$ (remember that $<: \text{ induces an order relation, Proposition D.7}$). In particular, the reduction rule for split should then instantiate those two coercions with $\text{id}_{Y'}$. This approach would result in the following typing rule:

$$
\Gamma \vdash \tau : Y' \quad \Gamma \vdash \sigma : Y' <: Y \quad \Gamma = \Gamma_0[F, \Gamma] \\
\Gamma \vdash \text{split } \tau \text{ at } n \text{ along } \sigma : Y' <: Y \text{ as } (Y_0, s_0, \delta_0), x, (Y_1, s_1, \delta_1), s_i, s_j \text{ in } t : A'
$$

\[\text{ (split)}\]
together with the following reduction rule:

\[
\text{split } r_0[u]; r_1 \text{ at } n \text{ along } \sigma : Y_0, A, Y_1 <\!\!\!: [\Gamma_0], A, [\Gamma_1] \text{ as } (Y_0, s_0, \delta_0), x, (Y_1, s_1, \delta_1), s_i, s_j \text{ in } t \to t[Y_0/Y_0][\sigma_0/s_0][r_0/\delta_0][u/x][Y_1/Y_1][\tau_1/\delta_1][\sigma_1/s_1][id_{\Gamma_0, A, Y_1}/s_i][id_{\Gamma_0, A, Y_1}/s_j]
\]

where \( n = |\Gamma_0|, |r_0| = |\Gamma_0| \) 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 \( F_\tau \) 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\(^1\). 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:

- **Terms** \( t ::= k \mid x \mid \lambda Y.t \mid t Y \mid \lambda s.t \mid t \sigma \mid \lambda \delta.t \mid t \tau \mid \lambda x.t \mid t u \)

- **Stacks** \( \pi ::= \star \mid Y \cdot \pi \mid \sigma \cdot \pi \mid \tau \cdot \pi \mid t \cdot \pi \)

- **Process** \( p ::= t \cdot \pi \)

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

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

to which we add a rule for splitting stores:

\[
\text{split } r_0[u]r_1 \text{ at } n \text{ along } \sigma : Y_0, A, Y_1 <\!\!\!: [\Gamma_0], A, [\Gamma_1] \text{ as } (Y_0, s_0, \delta_0), x, (Y_1, s_1, \delta_1), s_i, s_j \text{ in } t \star \pi \\
\to t[Y_0/Y_0][\sigma_0/s_0][r_0/\delta_0][u/x][Y_1/Y_1][\tau_1/\delta_1][\sigma_1/s_1] \star \pi
\]

where \( n = |\Gamma_0| \) and \( Y_0, Y_1, \sigma_0, \sigma_1 \) are as in Lemma 3.2 (i.e. \( |\Gamma_0| = |\sigma|(n), \sigma_0 : Y_0 <\!\!\!: \Gamma_0 \), etc.), and \( |r_0| = |\Gamma_0| \).

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

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

\[
\begin{align*}
    \text{split } r_n \text{ at } n \text{ along } \sigma : \ldots & \text{ as } \ldots \text{ in } t \star \pi \triangleright \text{split } r' \text{ at } n \text{ along } \sigma' : \ldots \text{ as } \ldots \text{ in } t \star \pi \\
    \text{(if } \sigma \rightarrow \sigma' \text{ \ \ \ \ } )
\end{align*}
\]

where \( r_n \) 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 \( p \triangleright p' \) 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 \( \rho, Y := Y \)).

We write \( \rho(t) \) (resp. \( \rho(A), \rho(Y) \), 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:

- \( \|X\| = \{\cdot\} \)
- \( \|Y.T\| = \bigcup \{\text{for } \gamma \} \{\gamma : \pi : \pi \in \|T[Y/Y]\|}\)
- \( \|Y <: Y \rightarrow T\| = \{\sigma \cdot \pi : \sigma \vdash Y <: Y \land \pi \in \|T\|}\)
- \( \|Y \vdash Y \rightarrow T\| = \{\tau \cdot \pi : \tau \vdash Y \vdash Y \land \pi \in \|T\|}\)
- \( \|U \rightarrow T\| = \{\upsilon \cdot \pi : \upsilon \in [U] \land \pi \in \|T\|\}\)
- \( \|T\| \neq \{t : \forall \pi \in \|T\|, t \star \pi \in \perp\} \)

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

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

1. \( \sigma \vdash Y <: Y \) if \( \vdash \sigma : Y <: Y \)
2. \( \tau \vdash Y \vdash Y \) if \( \forall \tau', \tau' \vdash Y \implies \tau \vdash Y \)
3. \( [\cdot] \vdash 0 \)
4. \( \tau[\cdot] \vdash Y, F \) if \( \tau \vdash Y \) and \( t \in [Y \Rightarrow F] \)

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

\[
\sigma \rightarrow_{\sigma} \sigma' \land \sigma' \vdash Y <: Y \implies \sigma \vdash Y <: Y \quad \text{and} \quad \tau \rightarrow_{\tau} \tau' \land \tau' \vdash Y \implies \tau \vdash Y
\]

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 \( \delta : Y \vdash Y \in \Gamma \), we have \( \rho(\delta) \vdash \rho(Y) \vdash \rho(\delta) \).
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. \( \Gamma \vdash \sigma : Y <: Y \), \( \Gamma \vdash \tau : Y \vdash Y \)) is valid with respect to the interpretation if for any substitution \( \rho \) such that \( \rho \vdash \Gamma \), then \( \rho(t) \vdash \rho(A) \) (resp. \( \rho(\sigma) \vdash \rho(Y) <: \rho(Y), \rho(\tau) \vdash \rho(Y) \vdash \rho(\tau) \)).

We say that a typing rule \( \frac{\ldots}{\Delta} \) is adequate if the validity of the premises \( J_1, \ldots, J_n \) entails the validity of the conclusion \( \Delta \).

**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. \( \rho(A) \)).

- **Case** \( (x : A) \in \Gamma \)
  - **Case** \( \Gamma \vdash t : A \) (Ax).
    - **Case** \( \Gamma, x : A \vdash t : B \) (\( \lambda x.t \in [A \rightarrow B] \), i.e. \( u : \pi \in [A \rightarrow B] \). Then \( \lambda x.t \mu u : \pi > t_\rho[u/x] \star \pi \in \perp \) by induction hypothesis, since \( t_\rho[u/x] \mu _\rho[\pi = u/x] \) and \( \rho(x := u) \vdash \Gamma, x : A \). We conclude by anti-reduction.
  - **Case** \( \Gamma \vdash t : A \rightarrow B \rightleftharpoons \Gamma \vdash u : A \rightarrow \) (\( \gamma \)). Let \( \pi \in [B] \), by induction hypothesis we have \( t_\rho \vdash A \rightarrow B \) and \( u_\rho \vdash A \). Therefore, \( t_\rho u_\rho \star \pi > t_\rho u_\rho \star \pi \vdash \perp \) since \( u_\rho \cdot \pi \in [A \rightarrow B] \). We conclude by anti-reduction.
- **Case** \( \Gamma \vdash [\cdot] : \emptyset \vdash \emptyset \) (\( \emptyset \)). Trivial: for all \( \tau \vdash 0 \), we have that \( \tau[\cdot] = \tau \) and thus \( \tau ; [\cdot] \vdash 0 \).
- **Case** \( \Gamma \vdash [\cdot] : Y_0 \rightarrow F \) (\( \emptyset \)). Let \( t_0 \vdash Y_0 \). By induction hypothesis, we have that \( t_0 \vdash Y_0 \rightarrow F \). Hence, by definition, \( \tau[t_0] \vdash Y_0, F \).
- **Case** \( \Gamma \vdash [\cdot] : Y_0 \rightarrow T \) (\( \gamma \)). Let \( t_0 \vdash Y_0 \). By induction hypothesis, we have that \( t_0 \vdash Y_0 \rightarrow F \). Hence, by definition, \( \tau[t_0] \vdash Y_0, F \).

- **Case** \( \Gamma \vdash [\cdot] : Y_0 \rightarrow Y' \) (\( \gamma \)). Let \( \tau_0 \vdash Y_0 \). By induction hypothesis, we have that \( \tau_0 \vdash Y_0 \rightarrow Y' \). Since \( \tau_0 \) is closed, we have that \( \tau_0 \rightarrow (\tau_0 \rightarrow \tau) \rightarrow (\tau_0 \rightarrow \tau) \rightarrow (\tau_0 \rightarrow \tau) \). (by easy induction the structure of \( \tau_0 \)), hence \( \rightarrow \) (\( \gamma \)).
- **Case** \( (\cdot) \) rules. By definition, in all cases we have that \( \sigma_\rho \) is closed, hence \( \vdash \sigma_\rho : Y' \) \( \star \text{sub} \ Y_\rho \) is well-typed, thus \( \vdash \sigma_\rho : Y' \) \( \star \text{sub} \ Y_\rho \).
A calculus of expandable stores

Hugo Herbelin and Étienne Miquey

(δ : Y ▷τ Y′) ∈ Γ. By definition, since ρ ⊢ Γ and (δ : Y ▷τ Y′) ∈ Γ, we have that ρ(δ) ⊢ δ : Yρ ▷τ Yρ′.

• Case Γ ⊢ δ : Y ▷τ Y′ ∈ Γ(τa).

Γ, δ : Y0 ▷τ Y ⊢ t : B

• Case Γ ⊢ λδ.t : Y0 ▷τ Y → B(τb). Same proof as for the (λ) case.

Γ ⊢ t : Y0 ▷τ Y → B

• Case Γ ⊢ τ : B(τc). Same proof as for the (@) case.

Γ ⊢ τ : B

• Case Γ ⊢ λY.t : ∀Y. A(τe). Same proof as for the (λ) case.

Γ ⊢ λY.t : ∀Y. A

• Case Γ ⊢ τ Y : τ / Y ∈ Γ(τf). Same proof as for the (λ) case.

Γ ⊢ τ Y : τ / Y

• Case Γ ⊢ σ : Y′ ∈ Γ(σf).

Γ ⊢ σ : Y′

• Case Γ ⊢ split τ at n along σ : Y′ ∈ Γ as (Y0, s0, δ0), x, (Y1, s1, δ1) in t : A(spl1t). By induction hypothesis, we get that:

1. τρ ⊢ Yρ′
2. σρ ⊢ Yρ′
3. for any σ0 ⊢ Y0, u ⊢ Y0 ▷ F, σ1 ⊢ (Y0, F; Y1 ⊢ τ) ⊢ τ, if we define ρ′ = ρ, s0 := σ0, δ0 := τ0, x := u, s1 := σ1, δ1 := r1 then we have τρ′ ⊢ A

In particular, by definition, we have that ⊢ σρ ⊢ Yρ′ ⊢ τ, hence Lemma 3.3 applies and we get that: σp = σ0 ; σ1 and Yp′ = Y0, F; Y1 with ⊢ σ0 ⊢ Y0 : Γ0 and ⊢ σ1 : Y1 : Γ1. Besides, since τp ⊢ Yp, F; Yp, necessarily we have that τp = τp[u]; r1 with |τ0| = |Y0|, r0 ⊢ r1, r1 ⊢ Y1 and u ⊢ Y0 ▷ F (this is a simple induction on the structure of τp). Therefore, if π ∈ |A|, we have:

split τ0[u]τ1 at n along σ : Y0, A, Y1 ∈ Γ as (Y0, s0, δ0), x, (Y1, s1, δ1) in t * π

According to the third item above, this process belongs to the pole, and we can thus conclude by anti-reduction.

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

Proof. Easy verification: if p > p′ and p′ normalizes, then p normalizes too. Besides, for any (k : A) ∈ S, if π ∈ |A| then k * π is blocked hence belongs to □.

□
E Shallow embedding in Coq

We give here an overview of our take to define a shallow embedding of $F_t$ 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 $F_t$ is actually orthogonal to the choice of this translation.

\begin{verbatim}
Parameter Ty:Type.
Inductive hlist :=
| hnil : hlist |
| hcons : ∀ A, A → hlist → hlist.
Definition storeT := list Ty.

Inductive ::= storeT → storeT → Type :=
| empty : nil ≤ nil |
| lift : ∀ Y Y A, Y ≤ Y → [Y;A] ≤ Y |
| plus : ∀ Y Y A, Y ≤ Y → [Y;A] ≤ [Y;A].

Fixpoint (Y Y Y : Y ; Y ; Y := (\[ Y ; Y ; Y :=
match Y with
| nil ⇒ σ
| [Y;A] ⇒ lift A (σ \[ Y ; Y
end.

Lemma liftN_lift Y Y : (σ [(Y;A) σ] = lift A (σ \[ Y σ).
Proof. reflexivity.
Qed.

Definition o : (σ (σ ; Y Y ; Y :=
∀ σ Y Y ; Y ; Y (σ ; Y Y ; Y := (σ τ)
(σ (σ τ)).
Proof. (* Definition by induction on Y 2 *)
Defined

Lemma plus_lift Y Y : (σ (σ τ) Y Y ; Y :=
(σ (σ τ) (σ (σ τ) Y Y ; Y :=
Proof. reflexivity.
Qed.
\end{verbatim}

The full Coq development illustrating these ideas (and proving most of the properties we stated on $F_t$) 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:

\[
\frac{\Gamma \vdash \tau : \tau_0 \vdash \Sigma \quad \Gamma \vdash t : \tau_0, \Sigma \vdash T}{\Gamma \vdash \tau[t] : \tau_0 \vdash \Sigma, T} \quad (\tau[t])
\]

The same holds for \( \Gamma \vdash t : \tau_0, \Sigma \vdash T \) and \( \Gamma \vdash \tau[t] : \tau_0, \Sigma \vdash T \).

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

\[
\frac{\Gamma \vdash \tau \vdash \tau_0 \vdash \Sigma \quad \Gamma \vdash \tau[t] : \tau_0 \vdash \Sigma \quad \tau \vdash \tau'}{\Gamma \vdash \tau[t] \vdash \tau_0 \vdash \Sigma, \tau'} \quad (\tau, \tau')
\]

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:

\[
\frac{\Gamma \vdash V : \Sigma \vdash T}{\Gamma \vdash \uparrow V : \Sigma \vdash T} \quad (\uparrow)
\]

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

\[
\Pi_E, \Gamma, s : \Sigma \vdash \uparrow V : \Sigma \vdash T
\]

where we used Lemma D.9 and \( \Pi_E \) is the following derivation:

\[
\frac{E : \Sigma \vdash \Sigma \vdash T \vdash \Sigma \vdash T}{\uparrow E : \Sigma \vdash \Sigma \vdash T} \quad \text{(Ax)}
\]

\[
\frac{\delta : \Sigma \vdash \Sigma \vdash T \vdash \Sigma \vdash T}{\uparrow \delta : \Sigma \vdash \Sigma \vdash T} \quad \text{(Ax)}
\]

We are finally equipped to prove the main theorem:

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

1. If \( \Gamma \vdash \tau \vdash : T \) then \( \Gamma \vdash \tau \vdash : T \)
2. If \( \Gamma \vdash F : T \) then \( \Gamma \vdash F : T \)
3. If \( \Gamma \vdash V : T \) then \( \Gamma \vdash V : T \)
4. If \( \Gamma \vdash E : T \) then \( \Gamma \vdash E : T \)
5. If \( \Gamma \vdash t : T \) then \( \Gamma \vdash t : T \)
6. If \( \Gamma \vdash e : T \) then \( \Gamma \vdash e : T \)
7. If \( \Gamma \vdash c \) then \( \Gamma \vdash c \)
8. If \( \Gamma \vdash \lambda \) then \( \Gamma \vdash \lambda \)
9. If \( \Gamma \vdash \tau \vdash : \tau \) then \( \Gamma \vdash \tau \vdash : \tau \)

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 \((\uparrow E)\) and \((\lambda)\) rules in one rule.

1. Strong values \( [k]_\circ = k \), which has the desired type by hypothesis.
Therefore, we have by induction hypothesis that

\[ \vdash \Pi_t \vdash [t]_1 : [\Gamma, x_i : T] \vdash t : U \]

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

\[ \vdash [t]_1 : [\Gamma, x_i : T] \vdash Y' \vdash Y' \vdash E U \vdash \bot \quad \Pi_s \]

(\( \Pi_E \))

\[ \vdash s : Y < [\Gamma, \Gamma'] \vdash [t]_1 \quad \vdash s : Y < [\Gamma, \Gamma'] \vdash [t]_1 \quad (\lambda) \]

\[ \vdash [t]_1 \vdash [\Gamma, \Gamma'] \vdash s : Y < [\Gamma, \Gamma'] \vdash [t]_1 \quad (\lambda) \]

where:

- \( \Pi_E \) is a proof of \( E : T \vdash \bot \) (derivable according to Lemma D.9);
- \( \Pi_s \) is a proof of \( \delta : Y, u : Y \vdash T ; \vdash [t]_1 ; \vdash \delta[u] : Y, T \) (derivable according to Lemma F.1);
- \( \sigma_{\Gamma, \Gamma'} : (\circ [\Gamma] \circ [\Gamma])^\ast \) and \( \Pi_s \) is:

\[ \vdash \Pi_{\Gamma, \Gamma'} : [\Gamma] < [\Gamma'] \quad (\lessdot) \]

\[ \vdash \Pi_{\Gamma, \Gamma'} : [\Gamma] < [\Gamma'] \quad (\lessdot) \]

\[ \vdash \Pi_{\Gamma, \Gamma'} : [\Gamma] < [\Gamma'] \quad (\lessdot) \]

2. Forcing contexts

- **Case \([k]_F\).** \( [k]_F = \kappa \), which has the desired type by hypothesis.
- **Case \([t.E]_F\).** In the source language, we have:

\[ \Gamma \vdash t : T \quad \Gamma \vdash E : U \]

\[ \Gamma \vdash t : T \quad \Gamma \vdash E : U \]

Therefore, we have by induction hypothesis that \( \vdash [t]_1 : [\Gamma] \vdash t : T \) and \( \vdash [E]_1 : [\Gamma] \vdash E : U \), so that we can derive:

\[ \vdash [t]_1 : [\Gamma] \vdash t : U \quad \vdash [E]_1 : [\Gamma] \vdash E : U \]

\[ \vdash [t]_1 : [\Gamma] \vdash t : U \quad \vdash [E]_1 : [\Gamma] \vdash E : U \]

where:

- \( \Pi_E \) is a proof of \( s : Y < [\Gamma] \vdash [t]_1 ; \vdash [E]_1 ; \vdash \bot \) derived from the induction hypothesis for \( t \) and Lemma D.9;
- \( \Pi_t \) is a proof of \( s : Y < [\Gamma] \vdash [t]_1 ; \vdash [E]_1 ; \vdash \bot \) derived from the induction hypothesis for \( E \) and Lemma D.9;
- \( \Pi_\delta \) is the axiom rule \( \delta : Y \vdash \delta : Y ");
- \( \Pi_s \) is the proof of \( \vdash \Pi_{\Gamma, \Gamma'} : [\Gamma] < [\Gamma'] \).

3. Weak values

- **Case \([v]_V\).** In the source language, we have:

\[ \Gamma \vdash v : T \quad \Gamma \vdash v : T \]
Hence, we have by induction hypothesis that \( \vdash [v]_\Pi : \Gamma \vdash T \) and we can derive:

\[
F : Y \vdash \Pi T + F : Y T' < Y, Y' \rightarrow Y' \vdash \Pi T' \rightarrow \bot \quad (\oplus)
\]

\[
s : Y \vdash \Gamma \vdash F : Y \vdash \Pi T + F \vdash Y T' \vdash \bot
\]

\[
\delta : Y \vdash \delta : Y \quad (\oplus)
\]

\[
\Pi Y
\]

\[
\delta : Y \vdash \delta : Y \quad (\oplus)
\]

where:

- \( \Pi \alpha \) is a proof of \( s : Y \vdash \Gamma \vdash \top \)
- \( \Pi \beta \) is the axiom rule \( \delta : Y \vdash \delta : Y \)
- \( \Pi \gamma \) is a proof of \( \vdash \delta : Y \vdash \Gamma \)

\[\text{Case } [v]_\Pi.\] In the source language, we have:

\[\Gamma(i) = (x_i : T)\]

\[\Gamma \vdash T x_i : T\]

so that \( \Gamma \) is of the form \( \Gamma_0, x_i : T, \Gamma_1 \) with \( i = |\Gamma_0| \). By definition, we have:

\[T \vdash \sigma' : (s')_+ s' \]

where \( \sigma' = (s')_+ s' \).

\[\text{Case } [v]_\Pi.\] In the source language, we have:

\[\Gamma(i) = (x_i : T)\]

\[\Gamma \vdash T x_i : T\]

so that \( \Gamma \) is of the form \( \Gamma_0, x_i : T, \Gamma_1 \) with \( i = |\Gamma_0| \). By definition, we have:

\[\Gamma(i) = (x_i : T)\]

\[\Gamma \vdash T x_i : T\]

so that \( \Gamma \) is of the form \( \Gamma_0, x_i : T, \Gamma_1 \) with \( i = |\Gamma_0| \). By definition, we have:

\[\Gamma(i) = (x_i : T)\]

\[\Gamma \vdash T x_i : T\]

so that \( \Gamma \) is of the form \( \Gamma_0, x_i : T, \Gamma_1 \) with \( i = |\Gamma_0| \). By definition, we have:

\[\Gamma(i) = (x_i : T)\]

\[\Gamma \vdash T x_i : T\]
• $\Pi^\gamma_\gamma$ is the following derivation, where we use Lemmas F.1 and F.2:

$$\delta^\gamma_\gamma: Y^\gamma_0 + \delta^\gamma_\gamma: Y^\gamma_0 \quad (\text{ta})$$

$$\frac{V: Y^\gamma_v T + \exists^\gamma_\gamma: Y^\gamma_0 \quad (\tau^\gamma_\gamma) \quad \delta^\gamma_\gamma: (Y^\gamma_0, T)\tau^\gamma_\gamma Y^\gamma_1 + \delta^\gamma_\gamma: (Y^\gamma_0, T)\tau^\gamma_\gamma Y^\gamma_1 \quad (\text{ta})}{s^\gamma_\gamma: Y^\gamma_0 < Y_0 \vdash s: Y^\gamma_0 < Y_0} \text{ (<ax)}$$

$$\frac{\delta^\gamma_\gamma: Y^\gamma_0 \vdash \delta^\gamma_\gamma: Y^\gamma_0 \quad \delta^\gamma_\gamma: (Y^\gamma_0, T)\tau^\gamma_\gamma Y^\gamma_1 + \delta^\gamma_\gamma: (Y^\gamma_0, T)\tau^\gamma_\gamma Y^\gamma_1 \quad (\text{ta}) \quad \delta^\gamma_\gamma: (Y^\gamma_0, T)\tau^\gamma_\gamma Y^\gamma_1 \quad (\text{ta})}{\frac{\delta^\gamma_\gamma: (Y^\gamma_0, T)\tau^\gamma_\gamma Y^\gamma_1}{\delta^\gamma_\gamma: (Y^\gamma_0, T)\tau^\gamma_\gamma Y^\gamma_1 \quad (\tau^\gamma_\gamma)}}$$

4. Catchable contexts

• Case $[[F]]_E$. This case is similar to the case $[[v]]_V$.

• Case $[[\mu x_1. (x_1 \parallel F) \tau^\gamma]]_E$. In the source language, we have:

$$\frac{\Gamma, x_1 : T, \Gamma' \parallel F : T \quad \Gamma, x_1 : T \quad \Gamma' \quad |\Gamma| = i}{\Gamma, \Gamma'' \vdash E\mu x_1. (x_1 \parallel F) \tau^\gamma : T} \text{ (Ax)}$$

We have by induction hypothesis a proof of $\vdash [\tau^\gamma']_E : [\Gamma, x_1 : T] \parallel [\Gamma']_E$ and a proof $\Pi_F$ of $\vdash [F]_E : [\Gamma, x_1 : T, \Gamma']_E \parallel_T T$.

We can thus derive:

$$\frac{\vdash [\tau^\gamma']_E : [\Gamma, x_1 : T] \parallel [\Gamma']_E \quad \Pi_F \quad \Pi_E}{\vdash [\tau^\gamma']_E : [\Gamma, x_1 : T, \Gamma']_E \parallel_T T} \text{ (Ax)}$$

where:

• $\sigma = (so [[\tau^\gamma]]_E \mu \gamma_1 \gamma_1 \text{id}_E)^\gamma_\gamma$, $\sigma_F = \sigma = [[\gamma_1 \gamma_1 \text{id}_E]]_E$ and $\sigma_E = [[\gamma_1 \gamma_1 \text{id}_E]]_E$.

• $\Pi_F$ is the following proof, obtained by Lemma D.9:

$$\frac{s: Y < [[\Gamma, \Gamma'']]_E \vdash s: Y < [[\Gamma, \Gamma'']]_E \quad (\text{ta})}{\vdash F : ([\Gamma, \Gamma''])_E \parallel_T T} \text{ (Ax)}$$

5. Terms

• Case $[[V]]_1$. This case is similar to the case $[[v]]_V$.

• Case $[[\mu c \cdot c]]_1$. In the $\tilde{\lambda}_{[\text{t} \text{c} \text{r}]}$-calculus, we have:

$$\frac{\Gamma, \alpha_i : T \quad \text{ta} \quad \mu \alpha_i, c : T}{\Gamma, \Gamma' \parallel 1 \quad \mu \alpha_i, c : T} \text{ (Ax)}$$
Hence we have by induction a proof of \( \vdash [c]_e : [\Gamma, x_1 : T^1] \Rightarrow_e \bot \) and we can derive:

\[
\begin{align*}
\Pi_x \\
\vdash [c]_e : [\Gamma, x_1 : T^1] \Rightarrow_e \bot \\
\frac{s : Y < : [\Gamma, \Gamma'] \vdash (s \circ [\Gamma, \Gamma']^1))^1 : Y, T < : [\Gamma, T]}{s : Y < : [\Gamma, \Gamma'], \delta : Y \vdash [c]_e (Y, A^1) \Rightarrow_{e, r^1} (Y, T^1) \Rightarrow \bot} \\
\frac{s : Y < : [\Gamma, \Gamma'], \delta : Y, E : Y \Rightarrow_e T \vdash [c]_e (Y, A^1) \Rightarrow_{e, r^1} \delta[E]_e : \bot}{s : Y < : [\Gamma, \Gamma'], \delta : Y, E : Y \Rightarrow_e T \vdash \lambda Y \delta e \Rightarrow_{e, r^1} \delta[E]_e (Y, A^1) \Rightarrow_{e, r^1} \delta[E]_e : [\Gamma, \Gamma'] \Rightarrow_e T}
\end{align*}
\]

where \( \Pi_x \) is as in the first case for \( \lambda x_1.t \).

6. Contexts
- Case \( [E]_e \). This case is similar to the case \( [v]_v \).
- Case \( [\mu x_1.c]_e \). This case is similar to the case \( [\mu a_1.c]_e \).

7. Commands
- Case \( \langle t \parallel e \rangle_e \). In the \( \lambda_{\{t \mid r\ast\}} \)-calculus we have:

\[
\begin{align*}
\Gamma \vdash_e t : T & \quad \Gamma \vdash_e e : T^1 \\
\frac{}{\Gamma \vdash_e \langle t \parallel e \rangle}
\end{align*}
\]

thus we get by induction two proofs of \( \vdash [t]_e : [\Gamma] \Rightarrow_e T \) and \( \vdash [e]_e : [\Gamma] \Rightarrow_e T \). We can then derive:

\[
\begin{align*}
\vdash [e]_e : [\Gamma] \Rightarrow_e T \\
\frac{s : Y < : [\Gamma], \delta : Y \vdash [e]_e Y s : Y \Rightarrow_e T}{s : Y < : [\Gamma], \delta : Y \vdash [e]_e Y \delta \Rightarrow_e Y \Rightarrow_e T} & \quad (\text{r}_e) \\
\frac{s : Y < : [\Gamma], \delta : Y \vdash [e]_e Y \delta s \delta < [t]_e}{s : Y < : [\Gamma], \delta : Y \vdash [e]_e Y \delta \Rightarrow_e [t]_e} & \quad (\text{r}_e)
\end{align*}
\]

8. Closures
- Case \( [ct^r]_e \). In the \( \lambda_{\{t \mid r\ast\}} \)-calculus, we have:

\[
\begin{align*}
\Gamma, \Gamma' \vdash_e c & \quad \Gamma \vdash_e t^r : \Gamma^r \\
\frac{}{\Gamma \vdash t \parallel t^r}
\end{align*}
\]

We thus get by induction two proofs \( \vdash [t^r]_e : [\Gamma] \Rightarrow_e \Gamma^r \) and \( \vdash [e]_e : [\Gamma, \Gamma'] \Rightarrow_e \bot \). We can derive:

\[
\begin{align*}
\vdash [e]_e : [\Gamma, \Gamma'] \Rightarrow_e \bot \\
\frac{s : Y < : [\Gamma] \vdash [e]_e Y s : Y < : [\Gamma] \vdash (s^{[t^r]}) (Y, \Gamma') \Rightarrow \bot}{s : Y < : [\Gamma] \vdash [e]_e Y \vdash (s^{[t^r]}) (Y, \Gamma') \Rightarrow \bot} & \quad (\text{r}_e) \\
\frac{s : Y < : [\Gamma], \delta : Y \vdash [e]_e Y \delta (s^{[t^r]}) (Y, \Gamma') \Rightarrow \bot}{s : Y < : [\Gamma], \delta : Y \vdash [e]_e Y \delta \Rightarrow (s^{[t^r]}) (Y, \Gamma')} & \quad (\text{r}_e)
\end{align*}
\]

9. Stores
- Case \( [\lambda x_1.t]_e \). We only consider the case \( \lambda x_1.t \), the proof for the case \( \lambda a_1.E \) is identical. This corresponds to the typing rules:

\[
\begin{align*}
\Gamma \vdash_e t : T & \quad [\Gamma, \Gamma^r] = i \\
\frac{}{\Gamma \vdash \lambda x_1.t : [\Gamma, \Gamma^r]}
\end{align*}
\]

By induction, we obtain two proofs of \( \vdash [\lambda x_1.t]_e : [\Gamma] \Rightarrow_e \Gamma^r \) and \( \vdash [t]_e : [\Gamma, \Gamma'] \Rightarrow_e T \). We can thus derive by Lemma F.1:

\[
\begin{align*}
\vdash [\lambda x_1.t]_e : [\Gamma] \Rightarrow_e \Gamma^r \\
\vdash [t]_e : [\Gamma, \Gamma'] \Rightarrow_e T \vdash [\lambda x_1.t]_e [\Gamma] \Rightarrow_e [\Gamma, \Gamma'] \Rightarrow_e T \quad (\text{r}[t])
\end{align*}
\]
We first rephrase the reduction rules to use de Bruijn levels:

\[
\begin{align*}
\Gamma, \Gamma' \vdash \lambda x_i \cdot t : A \rightarrow B \mid V \ Y \sigma_\tau u E & \triangleq [t], (\Gamma, A) \sigma_{\tau \tau} \tau [u] \uparrow \delta \vdash E \\
\end{align*}
\]

\[
\begin{align*}
[t : E]_E \ Y \sigma \tau \upsilon \triangleq \upsilon \ Y \text{id}_\tau \tau \ (\uparrow \sigma \upsilon) (\uparrow \delta \upsilon) E & \triangleq \kappa \\
\end{align*}
\]

\[
\begin{align*}
[x_i : E]_s \ Y \sigma \tau \upsilon \triangleq \uparrow \text{id}_\tau \tau \ (\uparrow \delta \upsilon) x_i & \triangleq \kappa \\
\end{align*}
\]

\[
\begin{align*}
[V]_E \ Y \sigma \tau \upsilon \triangleq \upsilon \ Y \text{id}_\tau \tau \ (\uparrow \delta \upsilon) V & \triangleq \kappa \\
\end{align*}
\]

\[
\begin{align*}
[t \vdash E]_E \ Y \sigma \tau \upsilon \triangleq \upsilon \ Y \text{id}_\tau \tau \ (\uparrow \delta \upsilon) t & \triangleq \kappa \\
\end{align*}
\]

\[
\begin{align*}
[t_0 \alpha_i := \epsilon]_E \ Y \sigma \tau \upsilon \triangleq \upsilon \ Y \text{id}_\tau \tau \ (\uparrow \delta \upsilon) t_0 \alpha_i & \triangleq \kappa \\
\end{align*}
\]

where \( \text{id}_\tau = \epsilon^{\uparrow \tau} \), \( \sigma_{\tau \tau} \triangleq (\sigma \triangleright \uparrow \tau \text{id}_\tau) \), and \( \Gamma_i \) indicates that \( \Gamma_i \) is in \( \Gamma \) in the source of the translation.

![Translation of terms](image)

![Translation of types and judgments](image)

**Figure 17.** Call-by-name continuation-and-environment-passing style translation

### G A typed call-by-name translation

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

\[
\begin{align*}
\langle \tau \mu x_i . c \rangle \tau & \rightarrow \ c[x_n/x_i][x_n := \epsilon] \quad \text{with} \ |\tau| = n \\
\langle \mu x_i . c \ E \rangle \tau & \rightarrow \ c[\alpha_i/\alpha_i][\alpha_i := \epsilon] \quad \text{with} \ |\tau| = n \\
\langle \chi_i \cdot E \rangle \tau & \rightarrow \ \langle \tau(n) \ E \rangle \tau \\
\langle V \times \alpha_i \rangle \tau & \rightarrow \ \langle V \ | \alpha_i \rangle \tau \\
\langle \lambda x_i . t \ U \cdot E \rangle \tau & \rightarrow \ \langle u \mu x_j . (t \ E) \rangle \tau \\
\end{align*}
\]

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

**Theorem 4.2.** The translation is well-typed, i.e.:

1. If \( \Gamma \vdash_V V : T \) then \( \Gamma \vdash_V V : T \)
2. If \( \Gamma \vdash_E E : T^+ \) then \( \Gamma \vdash_E E : T^+ \)
3. If \( \Gamma \vdash_I t : T \) then \( \Gamma \vdash_I t : T \)
4. If \( \Gamma \vdash_e e : T^+ \) then \( \Gamma \vdash_e e : T^+ \)
5. If \( \Gamma \vdash_c c \) then \( \Gamma \vdash_c c \)
6. If \( \Gamma \vdash_I I \) then \( \Gamma \vdash_I I \)
7. If \( \Gamma \vdash_r r \) then \( \Gamma \vdash_r r : \Gamma \)

**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 \( \langle \bar{t} \rangle \), 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 $\tau_i : \bar{U}_i$) 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 $\bar{U}_0, A, \bar{U}_1, B, \bar{U}_2$. 
Theorem H.1. The translation is well-typed, i.e.:

1. If $\Gamma \vdash T$ then $\llbracket T \rrbracket_T = \top$
2. If $\Gamma \vdash c$ then $\llbracket c \rrbracket_T = \bottom$
3. If $\Gamma \vdash t$ then $\llbracket t \rrbracket_T = \top$

\[ \llbracket \alpha \rrbracket_T = \top \]
\[ \llbracket \beta \rrbracket_T = \bot \]

Theorem H.2. The translation follows the same hierarchy. Again, we have:

1. If $\Gamma \vdash V : T$ then $\llbracket V \rrbracket_T = \top$
2. If $\Gamma \vdash c$ then $\llbracket c \rrbracket_T = \bottom$
3. If $\Gamma \vdash t$ then $\llbracket t \rrbracket_T = \top$

\[ \llbracket \alpha \rrbracket_T = \top \]
\[ \llbracket \beta \rrbracket_T = \bot \]