Strong Normalization of MLF via a Calculus of Coercions

Giulio Manzonetto, Paolo Tranquilli

Strong Normalization of ML^F via a Calculus of Coercions

Giulio Manzonetto[a,1], Paolo Tranquilli[b,2]

[a] Intelligent Systems,
Department of Computer Science, Radboud University, Nijmegen, The Netherlands
[b] LIP, CNRS UMR 5668, INRIA,
ENS de Lyon, Université Claude Bernard Lyon 1, France

Abstract

ML^F is a type system extending ML with first-class polymorphism as in system F. The main goal of the present paper is to show that ML^F enjoys strong normalization, i.e., it has no infinite reduction paths. The proof of this result is achieved in several steps. We first focus on xML^F, the Church-style version of ML^F, and show that it can be translated into a calculus of coercions: terms are mapped into terms and instantiations into coercions. This coercion calculus can be seen as a decorated version of system F, so that the simulation results entails strong normalization of xML^F through the same property of system F. We then transfer the result to all other versions of ML^F using the fact that they can be compiled into xML^F and showing there is a bisimulation between the two. We conclude by discussing what results and issues are encountered when using the candidates of reducibility approach to the same problem.

Keywords: ML^F, xML^F, calculus of coercions, strong normalization, coercions, polymorphic types.

1. Introduction

One of the most efficient techniques for assuring that a program "behaves well" is *static type-checking*: types are assigned to every subexpression of a program, so that consistency of such an assignment (checked at compile time) implies the program will be well-behaved at runtime. Such assignment may be *explicit*, i.e. requiring the programmer to annotate the types at key points in the program (e.g. variables), as in C or Java. Otherwise we can free the programmer of the hassle and leave the boring task of scattering the code with types to an automatic type reconstructor, part of the compiler. One of the most prominent

Email addresses: `g.manzonetto@cs.ru.nl` (Giulio Manzonetto), `paolo.tranquilli@ens-lyon.fr` (Paolo Tranquilli)

[1] Supported by NWO project CALMOC (612.000.936).

[2] Supported by ANR project COMPLICE (ANR-08-BLANC-0211-01).

examples of this approach is the functional programming language ML [1, 2, 3] and its dialects.

Polymorphism. In this context *type polymorphism* allows greater flexibility, as it makes it possible to reuse code that works with elements of different types. For example an identity function will have type $\alpha \to \alpha$ for any α, so one can give it the type $\forall\alpha.\alpha \to \alpha$. However full polymorphism (like in system F [4]) leads to undecidable type systems: no automatic reconstructor would be available [5]. For this reason ML employs the so called second-class polymorphism (i.e. available only for named variables), more restricted but allowing a type inference procedure. Unfortunately, the programmer is also *forced* to use only such restricted polymorphism, even when a fully-polymorphic typing is known and could be provided by hand. One could wish for a more flexible approach, where one would write just enough type annotations to let the compiler's type reconstructor do the job, while still being able to employ first-class polymorphism if desired.

Extending ML *with full polymorphism.* ML^F [6, 7] answers this call by providing a partial type annotation mechanism with an automatic type reconstructor. This extension allows to write system F programs, which is not possible in general in ML. Moreover it is a conservative extension: ML programs still typecheck without needing any annotation. An important feature are principal type schemata, lacking in system F, which are obtained by employing a downward bounded quantification $\forall(\alpha \geq \sigma)\tau$, called a *flexible* quantifier. Such a type intuitively denotes that τ may be instantiated to any $\tau\,[\sigma'/\alpha]$, *provided that* σ' *is an instantiation of* σ. Usual quantification is recovered by allowing $\bot$ as bound, where $\bot$ is morally equivalent to the usual $\forall\alpha.\alpha$. ML^F also uses a *rigid* quantifier $\forall(\alpha = \sigma)\tau$, fundamental for type inference but not for the semantics. Indeed $\forall(\alpha = \sigma)\tau$ can be regarded as being $\tau\,[\sigma/\alpha]$.

ML^F *and strong normalization.* One of the well-behaving properties that a type system can assure is *strong normalization* (SN), that is the termination of all typable programs whatever execution strategy is used. For example system F is strongly normalizing [4]. As already pointed out, system F is contained in ML^F. However it is not yet known, but it is conjectured [6], that the inclusion is strict. This makes the question of SN of ML^F a non-trivial one, to which we answer positively in this paper. The result is proved via a suitable simulation in system F, with additional decorations dealing with the complex type instantiations possible in ML^F.

ML^F*'s variants.* ML^F comes in three versions with a varying degree of explicit typing. What we briefly described above and we might refer to as the "real deal" is in fact eML^F(following the nomenclature of [7]). In eML^F there are just enough type annotations to allow the automatic reconstruction of the missing ones, so that we may place it midway between the Curry and Church styles. The former is covered by the "implicit" version iML^F, where no type annotation whatsoever is present. Going the Church-style way we have a completely explicit version, $\mathsf{xML^F}$, studied in [8]. In $\mathsf{xML^F}$ type inference and the rigid quantifier $\forall(\alpha = \sigma)\tau$ are abandoned, with the aim of providing an internal language to which a compiler might map the surface language $\mathsf{eML^F}$.

With respect to $\mathsf{ML^F}$ the $\mathsf{xML^F}$ system is the main object of study with this work. Compared to Church-style system F, the type reduction $\to_\iota$ of $\mathsf{xML^F}$ is more complex, and may *a priori* cause unexpected glitches: it could cause non-termination, or block the reduction of a β-redex. The main difficulty lies in the non-trivial nature of the *type instance* relation $\sigma \leq \tau$. In $\mathsf{xML^F}$ for the sake of complete explicitness such relations are testified by syntactic entities called *instantiations* (see Figure 2). Given an instantiation $\phi : \sigma \leq \tau$ taking σ to τ and a term a of type σ the new term $a\phi$ will have the type τ. In fact ϕ plays the role of a type conversion, or in other words a *coercion*.

The coercion calculus. These type conversions have a non-trivial *type reduction* $\to_\iota$, as opposed to the easy type reduction of system F. Such a reduction may *a priori* introduce unexpected glitches in the system, such as introducing non-termination even if the β-reduction of the underlying term terminates, or on the contrary keeping a β-reduction of the underlying term from happening. To prove that none of this happens, rather than translating directly into system F we use an intermediate language abstracting the concept of coercion: the *coercion calculus* $\mathsf{F_c}$.

The delicate point in $\mathsf{xML^F}$ is that some of the instantiations (the "abstractions" $!\alpha$) behave in fact as variables, abstracted when introducing a bounded quantifier: in a way, $\forall(\alpha \geq \sigma)\tau$ expects a coercion from σ to α, whatever the choice for α may be. A question naturally arising is: what does it mean to be a coercion in this context, where such operations of coercion abstraction and substitution are available? Our answer, which works for $\mathsf{xML^F}$, is in the form of a type system (Figure 6). In section 3 we will show the good properties enjoyed by $\mathsf{F_c}$: it is a decoration of system F, so it is SN; moreover it has a *coercion erasure* which ideally recovers the actual semantics of a term, and establishes a *weak bisimulation* with ordinary λ-calculus [9], where coercion reductions $\to_{\mathsf{c}}$ take the role of silent actions, while β-reduction $\to_\beta$ remains the observable one.

The generality of coercion calculus allows then to lift these results to $\mathsf{xML^F}$ via a translation of the latter into the former (section 4). Its main idea is the same as for the one shown for $\mathsf{eML^F}$ in [10], where however no dynamic property was studied. Here we produce a proof of SN for all versions of $\mathsf{ML^F}$. Moreover the bisimulation result establishes that $\mathsf{xML^F}$ can indeed be used as an internal language for $\mathsf{eML^F}$, as the additional structure cannot block reductions of the intended program.

Candidates of reducibility. Before entering the details of the work, one may wonder whether the candidates of reducibility deliver the same result — indeed it was the first approach we tried. The *naïve* interpretation where type instantiation is mapped to inclusion of saturated sets (much like what has been done

The Big Picture

$$\begin{tikzcd}
& \mathsf{xML^F} \arrow[r, "(\,.\,)^\circ"] \arrow[ddrr, "\lceil\,.\,\rceil"] & \mathsf{F_c} \arrow[r, "\lvert\,.\,\rvert"] \arrow[ddr, "\lfloor\,.\,\rfloor"] & \mathsf{F} \arrow[dd, hook] \\
\mathsf{eML^F} \arrow[ur, "(\,.\,)^*"] \arrow[dr, "\lceil\,.\,\rceil"'] \arrow[r, phantom, "="] & {} \arrow[r, phantom, "="] & = & \neq \\
& \mathsf{iML^F} \arrow[uu, "(\,.\,)^*"] \arrow[rr, hook] & & \Lambda
\end{tikzcd}$$

$(\,.\,)^*$ = compiling $(\,.\,)^\circ$ = translation
$\lceil\,.\,\rceil$ = type erasure $\lfloor\,.\,\rfloor$ = coercion erasure

Figure 1: Pre-existing relationships among the systems (solid arrows), plus our contribution (dashed arrows).

for $\mathsf{F}_{<:}$ [11]) works for the β-reduction of $\mathsf{xML^F}$, leaving outside the ι type reduction. As already explained, contrary to system F the latter is non-trivial, so its presence is another reason for embracing the system F translation approach. We will however give a presentation of the results using candidates of reducibility (or more precisely *saturated sets*) in section 7, and what glitches one encounters when dealing with the same approach with $\mathsf{eML^F}$ and $\mathsf{iML^F}$.

Outline. In Figure 1 we give a schematic representation of the interrelations among the various type systems that will be studied in the present paper. It is well known that the type erasure of $\mathsf{eML^F}$ terms gives $\mathsf{iML^F}$ terms [7] and that the two systems can be compiled into $\mathsf{xML^F}$ [8]. Obviously, we have that $\mathsf{iML^F}$ and system F are embeddable into the untyped λ-calculus, and the type erasure of $\mathsf{xML^F}$ terms gives ordinary λ-terms. This part of the picture was well-established in the literature.

We present $\mathsf{xML^F}$ in section 2 and the coercion calculus $\mathsf{F_c}$ in section 3. $\mathsf{F_c}$ is strongly normalizing as it can be seen as a decorated version of system F: $\lvert\,.\,\rvert$ denotes the *decoration erasure* (Definition 13), and moreover enjoys the usual properties one expects of a type system, namely subject reduction. As coercions denote type conversions which morally have no operational meaning, a *coercion erasure* $\lfloor\,.\,\rfloor$ is given (Definition 19) extracting the actual semantics of a term. As is shown in the diagram in Figure 1 the two mappings $\lvert\,.\,\rvert$ and $\lfloor\,.\,\rfloor$ to Λ are clearly different.

We then move to one of the main contributions of the paper by defining in section 4 a translation $(\,.\,)^\circ$ from the former to the latter (Figure 9). In this way we prove that $\mathsf{xML^F}$ is strongly normalizing: suppose indeed that there is an infinite reduction chain in $\mathsf{xML^F}$, then it is simulated via the translation $(\,.\,)^\circ$ in $\mathsf{F_c}$, which is impossible.

To entail the same result for $\mathsf{eML^F}$ and $\mathsf{iML^F}$ the sole simulation does not suffice: we need to be sure that any infinite reduction in one of the two systems can be lifted to an infinite one in $\mathsf{xML^F}$. This is achieved by proving that the type erasure $\lceil\,.\,\rceil$ from $\mathsf{xML^F}$ to the λ-calculus Λ (Definition 3) is in fact a

$$\begin{array}{lll}
\alpha, \beta, \dots & & \text{(type variables)} \\
\sigma, \tau & ::= \alpha \mid \sigma \to \tau \mid \bot \mid \forall(\alpha \geq \sigma)\tau & \text{(types)} \\
\phi, \psi & ::= \tau \mid \phi;\psi \mid \mathbf{1} \mid \& \mid \parr \mid !\alpha \mid \forall(\geq \phi) \mid \forall(\alpha \geq)\phi & \text{(instantiations)} \\
x, y, z, \dots & & \text{(variables)} \\
a, b, c & ::= x \mid \lambda(x : \tau)a \mid ab \mid \Lambda(\alpha \geq \tau)a \mid a\phi \mid \texttt{let}\ x = a\ \texttt{in}\ b & \text{(terms)} \\
A, B & ::= a \mid \phi & \text{(expressions)} \\
\Gamma & ::= \emptyset \mid \Gamma, \alpha \geq \tau \mid \Gamma, x : \tau & \text{(environments)}
\end{array}$$

Figure 2: Syntactic definitions of $\mathsf{xML^F}$.

(weak) bisimulation (Theorem 37). We prove this result from an analogous one for the *coercion erasure* $\lfloor . \rfloor$ of $\mathsf{F_c}$ (Theorem 26). Nevertheless a direct proof of bisimulation of $\mathsf{xML^F}$'s type erasure $\lceil . \rceil$ is provided at page 26.

Finally in section 7 we define a candidates of reducibility interpretation for $\mathsf{xML^F}$ types, implying SN of $\lceil a \rceil$ for $\mathsf{xML^F}$ terms a, but failing to directly provide the full result.

Notations and basic definitions. Given reductions $\to_1$ and $\to_2$, we write $\to_1\to_2$ (resp. $\to_{12}$) for their concatenation (resp. their union). Moreover $\leftarrow$, $\xrightarrow{+}$, $\xrightarrow{=}$ and $\xrightarrow{*}$ denote the transpose, the transitive, the reflexive and the transitive-reflexive closures of $\to$ respectively. A reduction $\to$ is *strongly normalizing* if there is no infinite chain $a_i \to a_{i+1}$; it is *confluent* if $\xleftarrow{*}\xrightarrow{*} \subseteq \xrightarrow{*}\xleftarrow{*}$. In confluence diagrams, solid arrows denote reductions one starts with, while dashed arrows are the entailed ones.

2. A Short Presentation of $\mathsf{xML^F}$

Currently, $\mathsf{ML^F}$ comes in a Curry-style version $\mathsf{iML^F}$, where no annotation is provided, and a type-inference version $\mathsf{eML^F}$ requiring partial annotations, though a large amount of type information is automatically inferred. A truly Church-style version of $\mathsf{ML^F}$, called $\mathsf{xML^F}$, has been recently introduced in [8] and will be our main object of study in this paper. However, in section 5, we will draw conclusions for $\mathsf{iML^F}$ and $\mathsf{eML^F}$ too.

We warn the reader that we will only present the definitions we need, while we refer to [8] for an in-depth discussion on $\mathsf{xML^F}$. Concerning the presentation of $\mathsf{iML^F}$ and $\mathsf{eML^F}$ we refer to [12, 13].

2.1. Syntax

All the syntactic definitions of $\mathsf{xML^F}$ can be found in Figure 2. To be consistent with the existing literature we use the same notations of [8], but we warn the reader that the instantiations $\&, \parr$ and $!\alpha$ have no connection whatsoever with the "par", "with" and "promotion" connectives of linear logic.

We assume fixed a countable set of **type variables** denoted by $\alpha, \beta, \dots$

Types include type variables and arrow types, as usual. Here types also contain a bottom type $\bot$ corresponding to system F's type $\forall\alpha.\alpha$ and the **flexible**

quantification $\forall(\alpha \geq \sigma)\tau$ generalizing $\forall\alpha.\tau$ of system F. Intuitively, $\forall(\alpha \geq \sigma)\tau$ restricts the variable α to range just over instances of σ. The variable α is bound in τ but not in σ. We write $\mathrm{ftv}(\tau)$ for the set of type variables appearing free in a type τ.

An **instantiation** ϕ maps a type σ to a type τ which is an instance of σ. Thus ϕ can be seen as a 'witness' of the instance relation holding between σ and τ. In $\forall(\alpha \geq)\phi$, α is bounded in ϕ. We write $\mathrm{ftv}(\phi)$ for the set of free type variables of ϕ.

Terms of $\mathsf{xML^F}$ extend the ordinary λ-terms with a constructor `let`, type instantiation and type application. Type instantiation $a\phi$ generalizes system F type application. Type abstractions are extended with an instance bound τ, written $\Lambda(\alpha \geq \tau)a$. The type variable α is bounded in a, but free in τ. We write $\mathrm{fv}(a)$ (resp. $\mathrm{ftv}(a)$) for the set of free term (resp. type) variables of a.

Expressions can be either terms or instantiations. They are not essential for the calculus, but will be used to state results holding for both syntactic categories in a more elegant and compact way.

Environments Γ are finite maps assigning types to term variables and bounds to type variables. We write: $\mathrm{dom}(\Gamma)$ for the set of all term and type variables that are bound by Γ; $\mathrm{ftv}(\Gamma)$ for the set of type variables appearing free in Γ. Environments Γ are **well-formed** if for every $\alpha \in \mathrm{dom}(\Gamma)$ (resp. $x \in \mathrm{dom}(\Gamma)$) so that we may write $\Gamma = \Gamma', \alpha \geq \tau, \Gamma''$ (resp. $\Gamma', x : \tau, \Gamma''$) we have $\mathrm{ftv}(\tau) \subseteq \mathrm{dom}(\Gamma')$. All environments in this paper are supposed to be well-formed.

2.2. Type System

Typing rules of $\mathsf{xML^F}$ are provided in Figure 3. **Typing judgments** are of the form $\Gamma \vdash a : \tau$, where a is an $\mathsf{xML^F}$ term, Γ a (well-formed) environment and τ a type. Especially focus on type abstraction and type instantiation that are the biggest novelties with respect to system F. Type abstraction $\Lambda(\alpha \geq \tau)a$ extends the environment Γ with the type variable α bounded by τ. Notice that the typing of a type instantiation $a\phi$ is similar to the typing of a coercion, as it just requires the instantiation ϕ to transform the type of a to the type of the result. This analogy will be formally developed in section 4. The `let`-binding `let` $x = a$ `in` b is morally equivalent to the immediate application $(\lambda(x : \tau)b)a$ except that in the `let` the variable x does not require type annotation. We will soon forget about the `let` (see Convention 2, below) as it is unnecessary for our study.

Type instance judgments have the shape $\Gamma \vdash \phi : \sigma \leq \tau$ stating that in the environment Γ the instantiation ϕ maps the type σ into the type τ.

The bottom instantiation states that every type τ is an instance of $\bot$, independently of the environment. The abstract instantiation $!\alpha$ is applicable in an environment containing $\alpha \geq \tau$ and abstracts the bound τ of α as the type variable α. The inside instantiation $\forall(\geq \phi)$ applies ϕ to the bound σ of a flexible quantification $\forall(\beta \geq \sigma)\tau$. Conversely, the under instantiation $\forall(\alpha \geq)\phi$ applies ϕ to the type τ under the quantification. The quantifier introduction $\parr$ introduces

Instantiation rules

$$\frac{}{\Gamma \vdash \tau : \bot \leq \tau}\textsc{IBot} \qquad \frac{\Gamma, \alpha \geq \tau \vdash \phi : \tau_1 \leq \tau_2}{\Gamma \vdash \forall(\alpha \geq)\phi : \forall(\alpha \geq \tau)\tau_1 \leq \forall(\alpha \geq \tau)\tau_2}\textsc{IUnder}$$

$$\frac{\alpha \geq \tau \in \Gamma}{\Gamma \vdash !\alpha : \tau \leq \alpha}\textsc{IAbs} \qquad \frac{\Gamma \vdash \phi : \tau_1 \leq \tau_2}{\Gamma \vdash \forall(\geq \phi) : \forall(\alpha \geq \tau_1)\tau \leq \forall(\alpha \geq \tau_2)\tau}\textsc{IInside}$$

$$\frac{\alpha \notin \mathrm{ftv}(\tau)}{\Gamma \vdash \parr : \tau \leq \forall(\alpha \geq \bot)\tau}\textsc{IIntro} \qquad \frac{}{\Gamma \vdash \& : \forall(\alpha \geq \sigma)\tau \leq \sigma\,[\tau/\alpha]}\textsc{IElim}$$

$$\frac{\Gamma \vdash \phi : \tau_1 \leq \tau_2 \qquad \Gamma \vdash \psi : \tau_2 \leq \tau_3}{\Gamma \vdash \phi; \psi : \tau_1 \leq \tau_3}\textsc{IComp} \qquad \frac{}{\Gamma \vdash \mathbf{1} : \tau \leq \tau}\textsc{IId}$$

Typing rules

$$\frac{\Gamma(x) = \tau}{\Gamma \vdash x : \tau}\textsc{Var} \qquad \frac{\Gamma \vdash a : \tau \qquad \Gamma, x : \tau \vdash b : \sigma}{\Gamma \vdash \texttt{let}\ x = a\ \texttt{in}\ b : \sigma}\textsc{Let}$$

$$\frac{\Gamma, x : \tau \vdash a : \sigma}{\Gamma \vdash \lambda(x : \tau)a : \tau \to \sigma}\textsc{Abs} \qquad \frac{\Gamma \vdash a : \sigma \to \tau \qquad \Gamma \vdash b : \sigma}{\Gamma \vdash ab : \tau}\textsc{App}$$

$$\frac{\Gamma, \alpha \geq \sigma \vdash a : \tau \qquad \alpha \notin \mathrm{ftv}(\Gamma)}{\Gamma \vdash \Lambda(\alpha \geq \sigma)a : \forall(\alpha \geq \sigma)\tau}\textsc{TAbs} \qquad \frac{\Gamma \vdash a : \tau \qquad \Gamma \vdash \phi : \tau \leq \sigma}{\Gamma \vdash a\phi : \sigma}\textsc{TApp}$$

Type instantiation

$$\tau(!\alpha) := \alpha, \qquad \bot\tau := \tau, \qquad \tau\mathbf{1} := \tau, \qquad \tau(\phi;\psi) := (\tau\phi)\psi,$$
$$\tau\parr := \forall(\alpha \geq \bot)\tau, \quad \alpha \notin \mathrm{ftv}(\tau), \qquad (\forall(\alpha \geq \sigma)\tau)(\forall(\geq \phi)) := \forall(\alpha \geq \sigma\phi)\tau,$$
$$(\forall(\alpha \geq \sigma)\tau)\& := \tau\,[\sigma/\alpha]\,, \qquad (\forall(\alpha \geq \sigma)\tau)(\forall(\alpha \geq)\phi) := \forall(\alpha \geq \sigma)(\tau\phi).$$

Figure 3: The typing rules of xML^F.

a fresh trivial quantification $\forall(\alpha \geq \bot)$. *Vice versa*, the quantifier elimination & eliminates the bound of a type of the form $\forall(\alpha \geq \tau)\sigma$ by substituting τ for α in σ. The composition $\phi;\psi$ provides a witness of the transitivity of type instance, while the identity instantiation $\mathbf{1}$ of reflexivity.

In iML^F flexible quantification allows us to recover the property of *principal typing* that was lost in system F. This phenomenon can be observed also in xML^F, e.g. in the following paradigmatic example. Let `choice` be a system F program of type $\forall\alpha.\alpha \to \alpha \to \alpha$, and id be an identity program of type $\forall\alpha.\alpha \to \alpha$. The application of `choice` to id has several types in system F that are incompatible: for instance it can be typed both with $(\forall\beta.\beta \to \beta) \to (\forall\beta.\beta \to \beta)$ and with $\forall\gamma.(\gamma \to \gamma) \to (\gamma \to \gamma)$.

In xML^F we write the polymorphic identity $\mathrm{id} = \Lambda(\alpha \geq \bot)\lambda(x : \alpha)x$ of type $\tau_{\mathrm{id}} = \forall(\alpha \geq \bot)(\alpha \to \alpha)$. A possible implementation of the aforementioned function `choice` is $\Lambda(\beta \geq \bot)\lambda(x : \beta)\lambda(y : \beta)x$ of type $\forall(\beta \geq \bot)\beta \to \beta \to \beta$. The application of `choice` to id can be defined as the program

$$\texttt{choice\_id} = \Lambda(\beta \geq \tau_{\mathrm{id}})\texttt{choice}\langle\beta\rangle(\mathrm{id}(!\beta)), \text{ where } \langle\beta\rangle = \forall(\geq \beta); \&.$$

We can give weaker types to `choice_id` by type instantiation; for instance

$$\begin{aligned}
(\lambda(x:\tau)a)b &\to_\beta a\,[b/x]\\
\texttt{let}\ x = b\ \texttt{in}\ a &\to_\beta a\,[b/x]\\
a\mathbf{1} &\to_\iota a\\
a(\phi;\psi) &\to_\iota (a\phi)\psi\\
a\parr &\to_\iota \Lambda(\alpha \geq \bot)a,\ \alpha \notin \mathrm{ftv}(a)\\
(\Lambda(\alpha \geq \tau)a)\& &\to_\iota a\,[\mathbf{1}/!\alpha]\,[\tau/\alpha]\\
(\Lambda(\alpha \geq \tau)a)(\forall(\alpha \geq)\phi) &\to_\iota \Lambda(\alpha \geq \tau)(a\phi)\\
(\Lambda(\alpha \geq \tau)a)(\forall(\geq \phi)) &\to_\iota \Lambda(\alpha \geq \tau\phi)a\,[\phi;!\alpha/!\alpha]
\end{aligned}$$

Figure 4: Reduction rules of $\mathsf{xML^F}$.

we can recover the two system F types mentioned above. Indeed the term $\texttt{choice\_id}\&$ has type $(\forall(\beta \geq \bot)\beta \to \beta) \to (\forall(\beta \geq \bot)\beta \to \beta)$, while the term $\texttt{choice\_id}(\parr;\forall(\gamma \geq)(\forall(\geq \langle\gamma\rangle);\&))$ has type $\forall(\gamma \geq \bot)(\gamma \to \gamma) \to (\gamma \to \gamma)$.

2.3. Operational Semantics

One of the main technical aspects of $\mathsf{xML^F}$ is presenting how type instantiations evolve during reduction. $\mathsf{xML^F}$'s reduction rules are presented in Figure 4. They are divided into $\to_\beta$ (regular β-reductions) and $\to_\iota$, reducing instantiations. We allow reductions to occur in any context, including under λ-abstractions. Note that one of the ι-steps uses the definition of type instantiation $\tau\phi$, giving the unique type such that $\Gamma \vdash \phi : \tau \leq \tau\phi$, if ϕ type-checks.

We recall, from [8, Sec. 2.1], that both $\to_\beta$ and $\to_\iota$ enjoy subject reduction.

Lemma 1 (Subject reduction)**.** *Let a be an* $\mathsf{xML^F}$ *term.*

(i) $\Gamma \vdash a : \sigma$ *and* $a \to_\beta b$ *entail* $\Gamma \vdash b : \sigma$*,*

(ii) $\Gamma \vdash a : \sigma$ *and* $a \to_\iota b$ *entail* $\Gamma \vdash b : \sigma$*.*

Hereafter, we will adopt the following convention.

Convention 2. Here we presented the original syntax of $\mathsf{xML^F}$ which also contains the `let` construct. However this instruction has been added mainly to accommodate $\mathsf{eML^F}$'s type reconstructor. Hence in the whole paper we can suppose that in all $\mathsf{xML^F}$ terms every $\texttt{let}\ x = a\ \texttt{in}\ b$ has been replaced by $(\lambda(x:\sigma)b)a$, with σ the correct type of a.

We end the section by defining the type erasure of an $\mathsf{xML^F}$ ($\mathsf{eML^F}$) term, which erases all type and instantiation annotations, mapping a to an ordinary λ-term.

Definition 3. The **type erasure** $\lceil a \rceil$ of an $\mathsf{xML^F}$ term a is defined by:

$$\lceil x \rceil := x, \quad \lceil \lambda(x:\tau)a \rceil := \lambda x.\lceil a \rceil, \quad \lceil ab \rceil := \lceil a \rceil \lceil b \rceil,$$
$$\lceil \Lambda(\alpha \geq \sigma)a \rceil := \lceil a \rceil, \quad \lceil a\phi \rceil := \lceil a \rceil.$$

The type erasure of an $\mathsf{eML^F}$ term a is defined analogously and will be denoted by $\lceil a \rceil$ too (no confusion arises, since the context will disambiguate). From [8, Lemma 7, Theorem 6 and §4.2] we know the following[3].

Theorem 4. *For every* $\mathsf{iML^F}$ *(resp.* $\mathsf{eML^F}$*) term a, there is an* $\mathsf{xML^F}$ *term a^* such that $\lceil a^* \rceil = a$ (resp. $\lceil a^* \rceil = \lceil a \rceil$).*

3. The Coercion Calculus $\mathsf{F_c}$

In this section we will introduce the *coercion calculus* $\mathsf{F_c}$, which is (as shown in subsection 3.5) a decoration of system F accompanied by a type system. Before introducing the details, we point out that the version of $\mathsf{F_c}$ presented here is tailored down to suit $\mathsf{xML^F}$. As such, there are natural choices that have been intentionally left out or restrained. If $\mathsf{F_c}$ is to serve as a good meta-theory of coercions, more liberal choices and constructs are needed, as discussed at page 31.

A note on $\mathsf{F_c}$ *and* DILL. The type system we will present can be said to be a subsystem of lambda calculus typed with *dual intuitionistic linear logic* derivations (DILL, [14]). Such a system, built on top of linear logic [15], is characterized by having judgments of the form $\Gamma; L \vdash A$, where the context is split in a linear part L whose assumptions may be used just once and a regular, non-linear part Γ. Here the linear context and the linear arrow $\multimap$ will capture the linearity aspect of coercions: they neither erase nor duplicate their arguments.

The language presented in [14] is the term calculus of the logical system, and as such has a constructor for every logical rule. Notably, that work provides no intuitionistic arrow, as the translation $A \to B \cong\ !A \multimap B$ is preferred. So technically speaking employing DILL as a type system for ordinary λ-terms leads to another system (which we might call F_ℓ) using types rather than terms to strictly differentiate between linear and regular constructs. This system is known in *folklore*[4] but, as far as we know, it has never been thoroughly presented in the literature.

3.1. Syntax

The syntactic categories of (Curry-style) coercion calculus are presented in Figure 5.

In **types** the difference from usual system F types lies in the presence of a new arrow for coercions, denoted by the lollipop $\multimap$. As already explained above, contrary to $\mathsf{xML^F}$'s notation here the use of the linear logic symbol is pertinent. These **coercion types** $\sigma \multimap \tau$ will type conversions from the type σ to the type τ and are allowed to appear in regular types only on the left of an arrow. These in fact leads to three distinguishable arrow types: regular with regular type on

[3] Notice that [8] uses the notation $[\![\,.\,]\!]$ for what we refer to with $(\,.\,)^*$.

[4] As an example we might cite [16], where a fragment of F_ℓ is used to characterize poly-time functions.

$$
\begin{array}{lr}
\alpha, \beta, \dots & \text{(type variables)} \\
\sigma, \tau ::= \alpha \mid \sigma \to \tau \mid \kappa \to \tau \mid \forall\alpha.\tau & \text{(types)} \\
\kappa \quad ::= \sigma \multimap \tau & \text{(coercion types)} \\
\zeta \quad ::= \tau \mid \kappa & \text{(type expressions)} \\
x, y, z, \dots & \text{(variables)} \\
a, b ::= x \mid \lambda x.a \mid \underline{\lambda} x.a \mid \underline{\angle} x.a \mid ab \mid a \triangleright b \mid a \triangleleft b & \text{(terms)} \\
u, v ::= \lambda x.a \mid \underline{\angle} x.u \mid x \triangleright u & \text{(}\mathtt{c}\text{-values)} \\
\Gamma \quad ::= \emptyset \mid x : \tau, \Gamma \mid x : \sigma \multimap \alpha, \Gamma & \text{(regular environments)} \\
L \quad ::= \emptyset \mid z : \tau & \text{(linear environments)} \\
\Gamma; L & \text{(environments)} \\
\Gamma; \vdash_{\mathtt{t}} a : \sigma & \text{(term judgements)} \\
\Gamma; \vdash_{\mathtt{c}} a : \kappa & \text{(coercion judgements)} \\
\Gamma; z : \tau \vdash_{\ell} a : \sigma & \text{(linear judgements)} \\
\vdash_{\mathtt{xy}},\ \mathtt{x}, \mathtt{y} \in \{\, \mathtt{t}, \mathtt{c}, \ell \,\} \text{ stands for } \vdash_{\mathtt{x}} \text{ or } \vdash_{\mathtt{y}}. &
\end{array}
$$

Figure 5: Syntactic definitions of coercion calculus.

the left, regular with coercion type on the left and finally the coercion arrow. For type polymorphism $\forall\alpha.\tau$ we employ a different typesetting convention with respect to $\mathsf{xML}^{\mathsf{F}}$'s types for the sake of clarity. **Type expressions** denote both sorts of types.

We reflect the three different kinds of arrow types in **terms** with three different abstraction/application pairs. These are to be intended as mere decorations of the usual pair, used both to distinguish regular reduction from coercion one (subsection 3.3) and to define coercion erasure (subsection 3.6) directly on terms without regarding their type derivation. The three different pairs of abstraction/application are

- the regular one with $\lambda x.a$ and ab, where no coercion is involved;
- the **linear abstraction** and **application** $\underline{\lambda} x.a$ and $a \triangleright b$: the former builds a coercion and the latter applies the coercion a to the term b;
- the **coercion abstraction** and **application** $\underline{\angle} x.a$ and $a \triangleleft b$: the former expects a coercion to be passed to it, which is achieved by the latter where the coercion b is passed to a.

Notice that in applications the side of the triangle indicates where the coercion is.

Here we moreover introduce a special subclass of terms which we call **$\mathtt{c}$-values**. Essentially they are regular abstractions wrapped in the "blocking" coercion operations: coercion abstraction and linear application with a variable in coercion position. Its role be made more clear when we will discuss F_{c}'s reductions.

Environments are of shape $\Gamma; L$, where Γ is a map from term variables to type expressions (a **regular environment**), and L is the **linear environment**,

$$\frac{\Gamma(y) = \zeta}{\Gamma; \vdash_{\mathtt{tc}} y : \zeta}\,\textsc{Ax} \qquad \frac{\Gamma, x : \tau; \vdash_{\mathtt{t}} a : \sigma}{\Gamma; \vdash_{\mathtt{t}} \lambda x.a : \tau \to \sigma}\,\textsc{Abs} \qquad \frac{\Gamma; \vdash_{\mathtt{t}} a : \sigma \to \tau \qquad \Gamma; \vdash_{\mathtt{t}} b : \sigma}{\Gamma; \vdash_{\mathtt{t}} ab : \tau}\,\textsc{App}$$

$$\frac{}{\Gamma; z : \tau \vdash_{\ell} z : \tau}\,\textsc{LAx} \qquad \frac{\Gamma; z : \tau \vdash_{\ell} a : \sigma}{\Gamma; \vdash_{\mathtt{c}} \underline{\lambda} z.a : \tau \multimap \sigma}\,\textsc{LAbs} \qquad \frac{\Gamma, x : \kappa; L \vdash_{\mathtt{t}\ell} a : \sigma}{\Gamma; L \vdash_{\mathtt{t}\ell} \underline{\not\lambda} x.a : \kappa \to \sigma}\,\textsc{CAbs}$$

$$\frac{\Gamma; \vdash_{\mathtt{c}} a : \sigma_1 \multimap \sigma_2 \qquad \Gamma; L \vdash_{\mathtt{t}\ell} b : \sigma_1}{\Gamma; L \vdash_{\mathtt{t}\ell} a \triangleright b : \sigma_2}\,\textsc{LApp} \qquad \frac{\Gamma; L \vdash_{\mathtt{t}\ell} a : \kappa \to \sigma \qquad \Gamma \vdash_{\mathtt{c}} b : \kappa}{\Gamma; L \vdash_{\mathtt{t}\ell} a \triangleleft b : \sigma}\,\textsc{CApp}$$

$$\frac{\Gamma; L \vdash_{\mathtt{t}\ell} a : \sigma \qquad \alpha \notin \mathrm{ftv}(\Gamma; L)}{\Gamma; L \vdash_{\mathtt{t}\ell} a : \forall \alpha.\sigma}\,\textsc{Gen} \qquad \frac{\Gamma; L \vdash_{\mathtt{t}\ell} a : \forall \alpha.\sigma}{\Gamma; L \vdash_{\mathtt{t}\ell} a : \sigma\,[\tau'/\alpha]}\,\textsc{Inst}$$

Figure 6: Typing rules of coercion calculus.

containing (contrary to DILL) *at most* one assignment. Notice the restriction to $\sigma \multimap \alpha$ for coercion variables, which might at first seem overtly restrictive. However, Theorem 26 relies on this restriction, though the preceding results do not. Alternative, more permissive restrictions preserving the bisimulation result are left for future work.

3.2. Typing Rules

In $\mathsf{F_c}$ typing judgments are of the general form $\Gamma; L \vdash M : \zeta$. However the shape of the environment L (which can be either empty or containing one assignment) and of the type ζ (which can be regular or a coercion one) gives four different general combinations. Of these only three will be allowed by the rules:

- no linear assignment and a regular type gives rise to a **term judgment**, i.e. the typing of a regular term, marked by $\vdash_{\mathtt{t}}$;
- no linear assignment and a coercion type is a **coercion judgment**, marked by $\vdash_{\mathtt{c}}$;
- a linear assignment and a regular type is a **linear judgment**, and denotes in fact the building in progress of a coercion, marked by $\vdash_{\ell}$.

So in fact the subscripts of $\vdash$ are there just as an aid to readability, as they can be completely recovered from the shape of the judgment.

The typing rules making up $\mathsf{F_c}$ are presented in Figure 6. With the rules at hand we can finally specify what exactly a coercion is in our framework.

Definition 5 (Coercion and regular terms)**.** An $\mathsf{F_c}$ term a is a **coercion** if $\Gamma; \vdash_{\mathtt{c}} a : \sigma \multimap \tau$. We say it is **regular** if $\Gamma; \vdash_{\mathtt{t}} a : \sigma$.

There are three main ideas behind the design of $\mathsf{F_c}$'s typing rules.

- Regular operations (i.e. not marked as coercion or linear ones) are allowed only while building a regular term and not in coercions, so Abs and App are only on $\vdash_{\mathtt{t}}$ judgments.

$$(\lambda x.a)b \quad \to_\beta a\,[b/x]\,, \quad (\underline{\reflectbox{λ}} x.a) \lhd b \to_{\mathsf{c}} a\,[b/x]\,, \quad (\underline{\lambda} x.a) \rhd b \to_{\mathsf{c}} a\,[b/x]\,,$$

$$(\underline{\reflectbox{λ}} x.u) \lhd b \to_{\mathsf{cv}} u\,[b/x]\,, \quad (\underline{\lambda} x.a) \rhd u \to_{\mathsf{cv}} a\,[u/x]\,, \quad \text{where } u \text{ is a } \mathsf{c}\text{-value.}$$

Figure 7: Reduction rules of coercion calculus.

- The linear variable stands for the term to be coerced, so going up the LApp and CApp rules the linear context will *not* go the coercion side.
- The system is tailored for the needs of xML^F, so some restrictions have been made: for example coercions cannot be themselves coerced and are not polymorphic.

Discussing the rules some more in detail, we see that Ax is the usual axiom which can also introduce coercion variables, while LAx is its linear version used to start building a coercion. LAbs is the only other rule (with Ax) introducing coercions, and together with LApp they type the linear abstraction-application pair, available both for terms and for coercions under construction. The third abstraction-application pair is left to the CAbs and CApp rules.

3.3. Operational Semantics

Regarding reduction rules there is in fact not much to say as the different kinds of abstraction/application pairs are decorations of the usual one and as such share its reduction rules. This is shown in Figure 7, and as usual the rules are to be intended closed by context. The only detail to observe is that we distinguish regular β-reductions (denoted by $\to_\beta$) from the **coercion reductions** (denoted by $\to_{\mathsf{c}}$) which as the name suggests concerns the coercion part of the terms.

The coercion reduction has a conditional subreduction $\to_{\mathsf{cv}}$ that fires c-redexes only when c-values are at the right of the $\rhd$ or left of the $\lhd$. Intuitively, this reduction is what is strictly necessary to "unearth" a λ-abstraction. As shown later in the proof of Theorem 26 and as a consequence of Lemma 25, cv-normalizing a term will necessarily "unblock" all abstractions. Its main role here is that it is general enough to have bisimulation (Theorem 26) and small enough to correspond to xML^F's ι-steps (Lemma 36).

3.4. Some Basic Properties of F_c

We start presenting some basic properties of the coercion calculus. The first statements restrain the shape and the behaviour of coercions.

Remark 6. A coercion a is necessarily either a variable or a coercion abstraction, as Ax and LAbs are the only rules having a coercion type in the conclusion.

Lemma 7. *If* $\Gamma; L \vdash_{\mathsf{c}\ell} a : \zeta$ *then no subterm of* a *is of the form* $\lambda x.b$ *or* bc*. In particular* a *is both* β*-normal and* cv*-normal.*

Proof. Let us here call *strictly regular* the terms of form $\lambda x.b$ or bc. We proceed by induction on the derivation of a. If $\Gamma;\vdash_{\mathtt{c}} a : \sigma \multimap \tau$ then the last rule is either Ax (in which case a is a variable and the result follows) or LAbs from $\Gamma; z : \sigma \vdash_{\ell} a' : \tau$ with $a = \underline{\lambda} z.a'$. Inductive hypothesis yields that no strict subterm of a (i.e. no subterm of a') is strictly regular.

If $\Gamma; z : \sigma \vdash_{\ell} a : \tau$ then we reason by cases on the last rule. If it is LAx then $a = z$ and we are done; in all other cases it is sufficient to note that:

- a is not strictly regular, and
- the premise or both the premises of the rule are of one of the two forms, so inductive hypothesis applies to every immediate subterm(s). □

Following are basic properties of type systems. Note that though there are two substitution results (points (i), (ii) of Lemma 9 below) to accommodate the two types of environment, no weakening property is available to add the linear assignment.

Lemma 8 (Weakening)**.** *We have that* $\Gamma; L \vdash_{\mathtt{tc}\ell} a : \zeta$ *and* $x \notin \mathrm{dom}(\Gamma; L)$ *entail* $\Gamma, x : \zeta'; L \vdash_{\mathtt{tc}\ell} a : \zeta$*;*

Proof. Trivial induction on the size of the derivation. As usual, one may have to change the bound variable in the Gen rule. □

Lemma 9 (Substitution)**.** *We have the following:*

(i) $\Gamma;\vdash_{\mathtt{tc}} a : \zeta'$ *and* $\Gamma, x : \zeta'; L \vdash_{\mathtt{tc}\ell} b : \zeta$ *entail* $\Gamma; L \vdash_{\mathtt{tc}\ell} b\,[a/x] : \zeta$*;*

(ii) $\Gamma; L \vdash_{\mathtt{t}\ell} a : \sigma$ *and* $\Gamma; x : \sigma \vdash_{\ell} b : \zeta$ *entail* $\Gamma; L \vdash_{\mathtt{t}\ell} b\,[a/x] : \zeta$*.*

Proof. Both substitution results are obtained by induction on the derivation for b, by cases on its last rule.

- Ax: for (i), if $b = x$ then the derivation of a is what looked for, as $\zeta' = \zeta$ and $b\,[a/x] = a$; otherwise $b\,[a/x] = b$ and we are done; (ii) does not happen.
- LAx: for (i) $L = z : \sigma$ and $b = z \neq x$, so $\Gamma; z : \sigma \vdash_{\ell} z = z\,[a/x] : \sigma$ and we are done; for (ii) necessarily $b = x$, $\zeta = \sigma$ and $b\,[a/x] = a$ and we are done.
- Abs, App and LAbs: trivial application of inductive hypothesis for (i), while it does not apply for (ii) as the judgment for b cannot be a linear one.
- CAbs, Gen and Inst: for these unary rules both (i) and (ii) are trivial.
- CApp and LApp: for (i) the substitution distributes as usual; for (ii) it must be noted that x does not appear free in one of the two subterms (as it does not appear in the assignment). Indeed we will have $(b_1 \triangleleft b_2)\,[a/x] = (b_1\,[a/x]) \triangleleft b_2$ (resp. $(b_1 \triangleright b_2)\,[a/x] = b_1 \triangleright (b_2\,[a/x])$) and inductive hypothesis is needed for just one of the two branches. □

The next standard lemma is used in some of the following results.

Lemma 10. *If $\Gamma; L \vdash_{\mathtt{tc}\ell} a : \zeta$, then there is a derivation of the same judgment where no* Inst *rule follows immediately a* Gen *one.*

Proof. One uses the following remark: if we have a derivation π of $\Gamma; L \vdash_{\mathtt{tc}\ell} a : \zeta$ then for any τ there is a derivation of the same size, which we will denote by $\pi\,[\tau/\alpha]$, giving $\Gamma\,[\tau/\alpha]\,; L\,[\tau/\alpha] \vdash_{\mathtt{tc}\ell} a : \zeta\,[\tau/\alpha]$. To show it, it suffices to substitute τ for all α's, possibly renaming bound variables along the process.

One then shows the result by structural induction on the size of the derivation π of $\Gamma; L \vdash_{\mathtt{tc}\ell} a : \zeta$. Suppose in fact that there is an Inst rule immediately after a Gen one. Then there is a subderivation π' of the following shape:

$$\dfrac{\dfrac{\begin{array}{c}\pi''\\ \vdots\\ \Gamma'; L' \vdash_{\mathtt{t}\ell} b : \sigma\end{array} \qquad \alpha \notin \mathrm{ftv}(\Gamma'; L')}{\Gamma'; L' \vdash_{\mathtt{t}\ell} b : \forall\alpha.\sigma}\,\textsc{Gen}}{\Gamma'; L' \vdash_{\mathtt{t}\ell} b : \sigma\,[\tau/\alpha]}\,\textsc{Inst}$$

By applying the above remark it suffices to substitute π' in π with $\pi''\,[\tau/\alpha]$, as $\Gamma'\,[\tau/\alpha]\,; L'\,[\tau/\alpha] = \Gamma'; L'$. The derivation thus obtained is smaller by two rules, so inductive hypothesis applies and we are done. □

We now show that the coercion calculus satisfies both subject reduction and confluence.

Proposition 11 (Subject reduction)**.** *If $\Gamma; L \vdash_{\mathtt{t}\ell\mathtt{c}} a : \zeta$ and $a \to_{\beta\mathtt{c}} b$ then $\Gamma; L \vdash_{\mathtt{t}\ell\mathtt{c}} b : \zeta$.*

Proof. By Lemma 10 we can suppose that in the derivation of $a : \zeta$ there is no Inst rule immediately following a Gen. One then reasons by induction on the size of the derivation to settle the context closure, stripping the cases down to when the last rule of the derivation is one of the application rules App, CApp or LApp which introduces the redex $(\lambda x.c)d$, $(\underline{\reflectbox{$\lambda$}}x.c) \triangleleft d$ or $(\underline{\lambda}x.c) \triangleright d$. Moreover we can see that no Gen or Inst rule is present between the abstraction rule and the application one: if there were any, then as no Inst follows Gen we would have a sequence of Inst rules followed by Gen ones. However the former cannot follow an abstraction, while the latter cannot precede an application on the function side.

- $(\lambda x.c)d \to_\beta c\,[d/x]$: then $\Gamma, x : \sigma; \vdash_{\mathtt{t}} c : \tau$, $\Gamma; \vdash_{\mathtt{t}} d : \sigma$ and Lemma 9(i) settles the case;
- $(\underline{\reflectbox{$\lambda$}}x.c) \triangleleft d \to_{\mathtt{c}} c\,[d/x]$: the rule introducing $\underline{\reflectbox{$\lambda$}}x.c$ must be CAbs, with $\Gamma, x : \kappa; L \vdash_{\mathtt{t}\ell} c : \sigma$ and $\Gamma; \vdash_{\mathtt{c}} d : \kappa$, and again Lemma 9(i) entails the result;
- $(\underline{\lambda}x.c) \triangleright d \to_{\mathtt{c}} c\,[d/x]$: here $\underline{\lambda}x.c$ is introduced by LAbs, so $\Gamma; x : \tau \vdash_\ell c : \sigma$ and $\Gamma; L \vdash_{\mathtt{t}\ell} d : \tau$, and it is Lemma 9(ii) that applies. □

Syntactic categories

$$\begin{array}{lr}
\alpha, \beta, \ldots & \text{(type variables)} \\
\sigma, \tau ::= \alpha \mid \sigma \to \tau \mid \forall \alpha.\tau & \text{(types)} \\
x, y, z, \ldots & \text{(variables)} \\
a, b \ ::= x \mid \lambda x.a \mid ab \mid & \text{(terms)} \\
\Gamma \quad ::= \emptyset \mid \Gamma, x : \tau & \text{(environments)}
\end{array}$$

Typing rules

$$\frac{\Gamma(y) = \tau}{\Gamma \vdash_{\mathsf{F}} y : \tau}\textsc{Ax} \qquad \frac{\Gamma, x : \tau \vdash_{\mathsf{F}} a : \sigma}{\Gamma; \vdash_{\mathsf{F}} \lambda x.a : \tau \to \sigma}\textsc{Abs} \qquad \frac{\Gamma; \vdash_{\mathsf{F}} a : \sigma \to \tau \qquad \Gamma; \vdash_{\mathsf{F}} b : \sigma}{\Gamma; \vdash_{\mathsf{F}} ab : \tau}\textsc{App}$$

$$\frac{\Gamma \vdash_{\mathsf{F}} a : \sigma \qquad \alpha \notin \mathrm{ftv}(\Gamma)}{\Gamma \vdash_{\mathsf{F}} a : \forall \alpha.\sigma}\textsc{Gen} \qquad \frac{\Gamma \vdash_{\mathsf{F}} a : \forall \alpha.\sigma}{\Gamma \vdash_{\mathsf{F}} a : \sigma\,[\tau'/\alpha]}\textsc{Inst}$$

Figure 8: Syntax and typing rules of Curry-style system F.

Proposition 12 (Confluence)**.** *All of $\to_\beta$, $\to_{\mathsf{c}}$, $\to_{\mathsf{cv}}$ and $\to_{\beta\mathsf{c}}$ are confluent.*

Proof. The proof by Tait-Martin Löf's technique of parallel reductions does not pose particular issues. □

3.5. Coercion Calculus as a Decoration of System F

The following definition presents the coercion calculus as a simple decoration of usual Curry-style system F [4], which for the sake of completeness is briefly recalled in Figure 8.

System F can be recovered by collapsing the extraneous constructs $\multimap$, $\underline{\lambda}$, $\underline{\not\lambda}$, $\triangleleft$ and $\triangleright$ to their regular counterpart. Notably this will lead to a strong normalization result.

Definition 13. The **decoration erasure** of F_{c} types and terms is defined by:

$$|\alpha| := \alpha, \quad |\zeta \to \tau| := |\zeta| \to |\tau|, \quad |\sigma \multimap \tau| := |\sigma| \to |\tau|,$$
$$|x| := x, \quad |\lambda x.a| = |\underline{\lambda} x.a| = |\underline{\not\lambda} x.a| := \lambda x.|a|, \quad |a \triangleleft b| = |a \triangleright b| = |ab| := |a||b|,$$
$$|\Gamma|(y) := |\Gamma(y)| \quad \text{for } y \in \mathrm{dom}(\Gamma), \qquad |\Gamma; z : \tau| := |\Gamma|, z : |\tau|.$$

Lemma 15 ensures that the decoration erasure is sound with respect to typability. We just need the standard weakening lemma for system F, which we state for completeness.

Lemma 14. *If $\Gamma \vdash_{\mathsf{F}} a : \sigma$ and $x \notin \mathrm{dom}(\Gamma)$ then $\Gamma, x : \tau \vdash_{\mathsf{F}} a : \sigma$.*

Lemma 15. *Let a be an F_{c} term. If $\Gamma; L \vdash_{\mathtt{tc}\ell} a : \zeta$ then $|\Gamma; L| \vdash_{\mathsf{F}} |a| : |\zeta|$.*

Proof. It suffices to see that through $|\,.\,|$ all the new rules collapse to their regular counterpart: LAx becomes Ax, CAbs, LAbs become Abs, and CApp, LApp become App. In the latter cases Lemma 14 will have to be applied to add the $z : |\tau|$ coming from the linear environment which will be missing in one of the two branches. □

It is now immediate to see how decoration erasure agrees with substitution and thus reduction.

Lemma 16. *Given an $\mathsf{F_c}$ term a we have $|a[b/x]| = |a|[|b|/x]$.*

Proof. Trivial by induction on the term. □

Lemma 17. *If $a \to_{\beta\mathsf{c}} b$ then $|a| \to |b|$. Vice versa $|a| \to c$ implies $c = |b|$ with $a \to_{\beta\mathsf{c}} b$.*

Proof. The first claim is immediate from Lemma 16. The converse needs typability of a: take $|a| = (\lambda x.b'_1)b'_2$, then there are b_i with $|b_i| = b'_i$ and a is one of nine combinations ($(\lambda x.b_1)b_2$, $(\underline{\lambda}x.b_1)b_2$, $(\lambda x.b_1) \triangleleft b_2$, etc.). However as a is typable only the three matching combinations are possible, giving rise to the three possible redexes in the coercion calculus. □

As an easy consequence we get that $\mathsf{F_c}$ is strongly normalizing.

Corollary 18 (Termination)**.** *The coercion calculus is strongly normalizing.*

Proof. Immediate by Lemmas 15 and 17, using the strong normalization property of system F [4, Sec. 14.3]. □

3.6. Preservation of the Semantics

We will now turn to establishing why coercions $a : \tau \multimap \sigma$ can be truly called such. First, we need a way to extract the semantics of a term, i.e., a way to strip it of the structure one may have added to it in order to manage coercions.

Definition 19. The **coercion erasure** is a map from $\mathsf{F_c}$ terms to regular λ-calculus defined by:

$$\lfloor x \rfloor := x, \quad \lfloor \lambda x.a \rfloor := \lambda x.\lfloor a \rfloor, \quad \lfloor ab \rfloor := \lfloor a \rfloor \lfloor b \rfloor,$$
$$\lfloor \underline{\angle} x.a \rfloor := \lfloor a \rfloor, \quad \lfloor a \triangleleft b \rfloor := \lfloor a \rfloor, \quad \lfloor a \triangleright b \rfloor := \lfloor b \rfloor.$$

Notice that it is undefined on $\underline{\lambda}x.a$ terms, as we will not apply it on coercions.

Lemma 20.

(i) If $\Gamma, x : \kappa; L \vdash_{\mathtt{t}\ell} a : \sigma$ (i.e. x is a coercion variable) then $x \notin \mathrm{fv}(\lfloor a \rfloor)$;

(ii) if $\Gamma; z : \tau \vdash_{\ell} a : \sigma$ then $\lfloor a \rfloor = z$.

Proof. Both are proved by induction on the derivation, by cases on the last rule.

(i) As the judgment is not a coercion one, Ax cannot yield $a = x$, nor can LAx. Inductive hypothesis applies seamlessly for rules Abs, App, CAbs, Gen and Inst. The LAbs rule cannot be the last one of the derivation. Finally, rule CApp (resp. LApp) gives $\lfloor a \rfloor = \lfloor b \triangleleft c \rfloor = \lfloor b \rfloor$ (resp. $\lfloor a \rfloor = \lfloor b \triangleright c \rfloor = \lfloor c \rfloor$), and inductive hypothesis applied to the left (resp. right) branch gives the result.

(ii) The judgment is required to be a linear one: Ax, Abs, App and LAbs do not apply. For LAx we have $a = z$ and we are done. For all the other rules the result follows by inductive hypothesis, possibly chasing the $\Gamma; z : \tau$ environment left or right in the CApp and LApp rules respectively. □

Notice that property (i) above entails that $\lfloor\,.\,\rfloor$ is well-defined with respect to α-equivalence on regular, typed terms: given a term $\measuredangle x.a$ issued from a coercion abstraction, $\lfloor \measuredangle x.a \rfloor = \lfloor a \rfloor$ is independent from x.

As for property (ii), it greatly restricts the form of a coercion: if $a : \sigma \multimap \tau$ then it is either a variable or an abstraction $\underline{\lambda} x.a'$ (as already written in Remark 6), with $\lfloor a' \rfloor = x$. Apart when they are variables, coercions are essentially identities.

The problem whether the erasure maps $\mathsf{F_c}$ to a larger set of terms than system F is an open one, probably related to the open question whether ML^{F} types more terms than System F.

A note on unrestricted coercion variables. If we dropped the condition on coercion variables, namely that they are typed $\sigma \multimap \alpha$ in the context, we would get way too many terms: indeed the coercion erasure would cover the whole of the untyped λ-calculus. It would suffice to use two coercion variables $y_{o \to o} : o \multimap (o \to o)$ and $y_o : (o \to o) \multimap o$ modelling the recursive type $o \to o \simeq o$. For example, we would have

$$\begin{aligned} a_\delta &:= y_o \triangleright (\lambda x.(y_{o \to o} \triangleright x)x) : o, \\ a_\Delta &:= (y_{o \to o} \triangleright a_\delta)a_\delta : o, \end{aligned}$$

though $\lfloor a_\Delta \rfloor = (\lambda x.xx)(\lambda x.xx)$ is the renown divergent term untypable in system F.

We turn back to study the properties of the coercion erasure, firstly by stating a fundamental and easy result on its interaction with substitution.

Lemma 21. *For $\mathsf{F_c}$ terms a and b we have that $\lfloor a\,[b/x] \rfloor = \lfloor a \rfloor\,[\lfloor b \rfloor/x]$, when both sides are defined*[5].

Proof. Immediate induction. □

The following result employs the linearity constraint in a crucial way: reductions in linear position can be neither erased nor duplicated.

Lemma 22. *If $\Gamma; x : \tau \vdash_\ell a : \sigma$ and $b \to_\beta c$, then $a\,[b/x] \to_\beta a\,[c/x]$.*

Proof. The proof is an easy induction on the derivation.

We proceed by cases on the last rule used: Ax, Abs, App and LAbs do not apply; LAx is trivial (as $a = x$); in CAbs, Gen and Inst the inductive hypothesis easily yields the inductive step; finally in CApp and LApp the inductive

[5] We regard the right-hand side to be defined even if $\lfloor b \rfloor$ is not defined but $x \notin \mathrm{fv}(\lfloor a \rfloor)$, in which case we simply take $\lfloor a \rfloor$.

hypothesis is applied only to the left and right premises respectively, giving the needed one step by context closure. □

Before going on we prove a property we will need later: c-values are stable by β-reduction.

Lemma 23. *If c is a c-value and $c \to_\beta d$ then d is a c-value too.*

Proof. Intuitively, it is due to the fact that the λ-abstraction buried under $\underline{\reflectbox{$\lambda$}}$'s and $x\triangleright$'s cannot be possibly destroyed by the β-reduction. Formally the proof is by straightforward induction on c. □

The following will state some basic dynamic properties of coercion reductions. Intuitively we will prove that β-steps are actual steps of the semantics (point (iii)) and that c-steps preserves it in a strong sense: they are collapsed to the equality (point (iv)) and they preserve β-steps (point (i)).

Proposition 24. *Suppose that a is an $\mathsf{F_c}$ term. Then:*

(i) if $b_1 \leftarrow_{\mathsf{c}} a \to_\beta b_2$ then there is c with $b_1 \to_\beta c \overset{*}{\leftarrow}_{\mathsf{c}} b_2$;

(ii) if $b_1 \leftarrow_{\mathsf{cv}} a \to_\beta b_2$ then there is c with $b_1 \to_\beta c \overset{*}{\leftarrow}_{\mathsf{cv}} b_2$;

(iii) if $a \to_\beta b$ then $\lfloor a \rfloor \to \lfloor b \rfloor$;

(iv) if $a \to_{\mathsf{c}} b$ then $\lfloor a \rfloor = \lfloor b \rfloor$.

$$\begin{tikzcd} a \arrow[r, "\beta"] \arrow[d, "\mathsf{c}"'] & b_2 \arrow[d, dashed, "\mathsf{c}*"] \\ b_1 \arrow[r, dashed, "\beta"] & c \end{tikzcd}$$

$$\begin{tikzcd} a \arrow[r, "\beta"] \arrow[d, "\mathsf{cv}"'] & b_2 \arrow[d, dashed, "\mathsf{cv}*"] \\ b_1 \arrow[r, dashed, "\beta"] & c \end{tikzcd}$$

Proof. (i–ii) We consider the case where the two redexes are not orthogonal: by non-overlapping one contains the other, and we can suppose that a is the biggest of the two, closing the diagram by context in the other cases.

If $a = (\lambda x.d)e$, then the diagram is closed straightforwardly, whether the c or cv-redex is in d or in e (in which case many or no steps may be needed to close the diagram).

When firing $a = (\underline{\lambda} x.d) \triangleright e$ then by typing $\underline{\lambda} x.d$ is a coercion (resp. a c-value), so we have a derivation ending in $\Gamma; x : \sigma \vdash_\ell d : \tau$, with $\Gamma; \vdash_{\mathsf{t}} e : \sigma$. As d cannot contain any β-redex, the other redex fired in the diagram is in e, so $e \to_\beta e'$, and if e is a c-value then by Lemma 23 e' is one too. Thus $b_1 = d\,[e/x]$ and $b_2 = (\underline{\lambda} x.d) \triangleright e' \to_{\mathsf{c}} d\,[e'/x]$ (resp. $b_2 \to_{\mathsf{cv}} d\,[e'/x]$). By Lemma 22 we have that $b_1 \to_\beta d\,[e'/x]$ and we are done.

If firing $a = (\underline{\reflectbox{λ}} x.d) \triangleleft e$ we have that e is a coercion, which cannot contain any β-redex, so we have $d \to_\beta d'$ (with d' a c-value if d is one by Lemma 23) and $b_2 = (\underline{\reflectbox{λ}} x.d') \triangleleft e$. We easily get $b_2 \to_{\mathsf{c}} d'\,[e/x] \leftarrow_\beta d\,[e/x] = b_1$ (resp. $b_2 \to_{\mathsf{cv}} d'\,[e/x] \leftarrow_\beta b_1$).

(iii) By induction and β-normality of coercions we can reduce to the case where $a = (\lambda x.c)d$. By Lemma 21, as $\lfloor (\lambda x.c)d \rfloor = (\lambda x.\lfloor c \rfloor)\lfloor d \rfloor \to \lfloor c \rfloor\,[\lfloor d \rfloor/x] = \lfloor c\,[d/x] \rfloor$.

(iv) Proceeding by context closure, suppose $a = (\measuredangle x.c) \triangleleft d$ (resp. $a = (\underline{\lambda} x.c) \triangleright d$), so $b = c\,[d/x]$. In the first case we will have $\lfloor a \rfloor = \lfloor c \rfloor$ and $\Gamma, x : \kappa; L \vdash_{\mathtt{t}\ell} c : \sigma$ for some typing derivation. Then by Lemmas 20(i) and 21 we have that $x \notin \mathrm{fv}(\lfloor c \rfloor)$ and $\lfloor b \rfloor = \lfloor c \rfloor\,[\lfloor d \rfloor / x] = \lfloor c \rfloor = \lfloor a \rfloor$ and we are done.

In the latter case we have $\lfloor a \rfloor = \lfloor d \rfloor$, and $\Gamma; x : \tau \vdash_{\ell} c : \sigma$. Lemmas 20(ii) and 21 entail $\lfloor b \rfloor = \lfloor c \rfloor\,[\lfloor d \rfloor / x] = x\,[\lfloor d \rfloor / x] = \lfloor d \rfloor = \lfloor a \rfloor$ and we are again done. □

In order to truly see coercions as additional information that is not strictly needed for reduction, one may ask that some converse of property (iii) should also hold. Here the condition on coercion variables $(x : \sigma \multimap \alpha)$ starts to play a role[6]. Indeed in general this is not the case: take $a = \measuredangle y.(y \triangleright I)I$ with $I = \lambda x.x$, that would be typable with $; \vdash a : (\sigma_{\mathrm{id}} \multimap \sigma_{\mathrm{id}}) \to \sigma_{\mathrm{id}}$ (where $\sigma_{\mathrm{id}} := \forall \alpha.(\alpha \to \alpha)$). Its coercion erasure is typable but it has a redex that is blocked by a coercion variable. Intuitively asking that a coercion variable y is always typed with the form $\sigma \multimap \alpha$ prevents terms of the form $y \triangleright a$ to be used in the functional position of a redex before y has the chance to be actually instantiated.

With the condition on coercion variables in place we are ready to prove a complete correspondence between the β-reductions of the coerced terms and the ones of their coercion erasure. In fact Theorem 26 states that $a \mapsto \lfloor a \rfloor$ is a weak bisimulation for $\to_\beta$, taking $\to_{\mathtt{cv}}$ as the silent actions on the side of coercion calculus. The proof uses the following lemma.

Lemma 25. *Every typable* $\mathtt{cv}$*-normal term* a *with* $\lfloor a \rfloor = \lambda x.b$ *is a* $\mathtt{c}$*-value. In particular if* a *has an arrow type then* $a = \lambda x.c$ *with* $\lfloor c \rfloor = b$*.*

Proof. We reason by structural induction on a. Notice a can be neither a variable nor a regular application, as its erasure is an abstraction. Following are the remaining cases.

- $a = \lambda y.d$: a is a $\mathtt{c}$-value.
- $a = \measuredangle y.d$: as $\lfloor d \rfloor = \lfloor a \rfloor = \lambda x.b$ inductive hypothesis applies and d is a $\mathtt{c}$-value, hence a is a $\mathtt{c}$-value too.
- $a = \underline{\lambda} y.d$: this case cannot happen, as no coercion has an abstraction as erasure.
- $a = d \triangleleft e$: by inductive hypothesis ($\lfloor d \rfloor = \lfloor a \rfloor = \lambda x.b$) we have that d is a $\mathtt{c}$-value. We arrive to a contradiction ruling out all the alternatives for d:
  - $d = \lambda y.f$ would make $d \triangleright e$ impossible to type;
  - $d = \measuredangle y.f$ with f a $\mathtt{c}$-value is impossible as $d \triangleright e$ would be a valid $\mathtt{cv}$-redex;

[6] All the results shown so far are valid also without such a condition.

  - $d = x \triangleright f$ with f a $\mathtt{c}$-value is impossible as, before the CApp introducing $d \triangleright e$, d would be typed by a type variable α (as x would necessarily have type $\sigma \multimap \alpha$), which in no way could lead to the necessary type $\kappa \to \tau$ (α is not generalizable as $x : \sigma \multimap \alpha$ would be in the context).

- $a = d \triangleright e$: by inductive hypothesis ($\lfloor e \rfloor = \lfloor a \rfloor = \lambda x.b$) e is a $\mathtt{c}$-value. As d is a coercion, by Remark 6 it can either be a variable (in which case we are done) or an abstraction. The latter however is impossible as a would be a valid $\mathtt{cv}$-redex.

For the consequence about an arrow-typed a, it suffices to see that $\underline{\angle} y.u$ gives rise to a (possibly generalized) type $\kappa \to \tau$, while $x \triangleright u$ gives a (non-generalizable) type variable. So in this case the only possibility for a is to be an abstraction $\lambda x.c$. The fact that $\lfloor c \rfloor = b$ follows from the definition of $\lfloor a \rfloor$. □

Theorem 26 (Bisimulation of $\lfloor\,.\,\rfloor$ with $\mathtt{cv}$-reduction)**.** *If $\Gamma; \vdash_{\mathtt{t}} a : \sigma$, then $\lfloor a \rfloor \to_\beta b$ if and only if $a \overset{*}{\to}_{\mathtt{cv}} \to_\beta c$ with $\lfloor c \rfloor = b$.*

$$\begin{tikzcd}
a \arrow[r, "\mathtt{cv}*"] \arrow[d, mapsto] & {} \arrow[r, "\beta"] \arrow[d, phantom, "\Updownarrow"] & c \arrow[d, mapsto] \\
\lfloor a \rfloor \arrow[rr, "\beta"'] & & b
\end{tikzcd}$$

Proof. The if part is given by Proposition 24. For the only if part we can suppose that $a = a_1 a_2$ with $\lfloor a_1 \rfloor = \lambda x.d$, so that $(\lambda x.d)\lfloor a_2 \rfloor$ is the redex fired in $\lfloor a \rfloor$, i.e. $b = d\,[\lfloor a_2 \rfloor / x]$. We can reduce to such a case reasoning by structural induction on a, discarding all the parts of the context where the reduction does not occur.

As a_1 is applied to a_2 there is a derivation giving $\Gamma'; \vdash_{\mathtt{t}} a_1 : \tau \to \tau'$ for some Γ', τ, τ'. We can then $\mathtt{cv}$-normalize a_1 to a_1' (Corollary 18), which by subject reduction has the same type. Moreover by Proposition 24(iv) $\lfloor a_1' \rfloor = \lfloor a_1 \rfloor = \lambda x.d$, and we conclude by Lemma 25 that $a_1' = \lambda x.e$ with $\lfloor e \rfloor = d$, and we finally get $a_1 a_2 \overset{*}{\to}_{\mathtt{cv}} (\lambda x.e) a_2 \to_\beta e\,[a_2/x]$. Now by Lemma 21 $\lfloor e\,[a_2/x] \rfloor = \lfloor e \rfloor\,[\lfloor a_2 \rfloor / x] = d\,[\lfloor a_2 \rfloor / x] = b$ and we are done. □

Notice that the above result entails straightforwardly bisimulation with $\to_{\mathtt{c}}$ as a more general silent action, as stated below.

Theorem 27 (Bisimulation of $\lfloor\,.\,\rfloor$)**.** *If $\Gamma; \vdash_{\mathtt{t}} a : \sigma$, then $\lfloor a \rfloor \to_\beta b$ if and only if $a \overset{*}{\to}_{\mathtt{c}} \to_\beta c$ with $\lfloor c \rfloor = b$.*

Proof. The only if part is given by $\to_{\mathtt{cv}} \subseteq \to_{\mathtt{c}}$ and Theorem 26, while the if part is again a consequence of Proposition 24. □

4. Strong Normalization of xML$^{\mathsf{F}}$ via Translation

A translation from xML$^{\mathsf{F}}$ terms and instantiations into the coercion calculus is given in Figure 9. The idea is that instantiations can be seen as coercions;

Types and contexts

$$\alpha^\bullet := \alpha, \qquad (\sigma \to \tau)^\bullet := \sigma^\bullet \to \tau^\bullet, \qquad (x : \tau)^\bullet := x : \tau^\bullet,$$
$$\bot^\bullet := \forall\alpha.\alpha, \quad (\forall(\alpha \geq \sigma)\tau)^\bullet := \forall\alpha.(\sigma^\bullet \multimap \alpha) \to \tau^\bullet, \quad (\alpha \geq \tau)^\bullet := i_\alpha : \tau^\bullet \multimap \alpha.$$

Instantiations

$$\tau^\circ := \underline{\lambda} x.x, \qquad (\parr)^\circ := \underline{\lambda} x.\underline{\measuredangle} i_\alpha.x, \qquad (\phi;\psi)^\circ := \underline{\lambda} z.\psi^\circ \triangleright (\phi^\circ \triangleright z),$$
$$(!\alpha)^\circ := i_\alpha, \qquad (\&)^\circ := \underline{\lambda} x.x \triangleleft \underline{\lambda} z.z, \qquad (\mathbf{1})^\circ := \underline{\lambda} z.z,$$
$$(\forall(\geq \phi))^\circ := \underline{\lambda} x.\underline{\measuredangle} i_\alpha.x \triangleleft (\underline{\lambda} z.i_\alpha \triangleright (\phi^\circ \triangleright z)),$$
$$(\forall(\alpha \geq)\phi)^\circ := \underline{\lambda} x.\underline{\measuredangle} i_\alpha.\phi^\circ \triangleright (x \triangleleft i_\alpha).$$

Terms

$$x^\circ := x, \qquad (\lambda(x : \tau)a)^\circ := \lambda x.a^\circ, \qquad (ab)^\circ := a^\circ b^\circ,$$
$$(\Lambda(\alpha \geq \tau)a)^\circ := \underline{\measuredangle} i_\alpha.a^\circ, \qquad (a\phi)^\circ := \phi^\circ \triangleright a^\circ.$$

Figure 9: Translation of types, instantiations and terms into the coercion calculus. For every type variable α we suppose fixed a fresh term variable i_α.

thus a term starting with a type abstraction $\Lambda(\alpha \geq \tau)$ becomes a term waiting for a coercion of type $\tau^\bullet \multimap \alpha$, and a term $a\phi$ becomes a° coerced by ϕ°. One can see how this translation shares the same base idea as the one given for $\mathsf{iML^F}/\mathsf{eML^F}$ in [10].

We can already state how the translation "preserves semantics". As this concept is represented by type erasure in $\mathsf{xML^F}$ and coercion erasure in $\mathsf{F_c}$, it is achieved by the following easy result.

Lemma 28. *The type erasure of an* $\mathsf{xML^F}$ *term* a *coincides with the coercion erasure of its translation, i.e.* $\lceil a \rceil = \lfloor a^\circ \rfloor$.

Proof. Immediate induction. □

The rest of this section lead to the first main result of this work, namely SN of $\mathsf{xML^F}$. The same result for $\mathsf{eML^F}$ and $\mathsf{iML^F}$ will be established in the next section. We first need to show that the translation is sound from the point of view of typing. We will thus show that it maps typed terms to typed terms and typed instantiations to typed coercions).

Lemma 29. *If* $\Gamma \vdash \phi : \sigma \leq \tau$ *then* $\Gamma^\bullet; \vdash_{\mathsf{c}} \phi^\circ : \sigma^\bullet \multimap \tau^\bullet$.

Lemma 30. *If* a *is an* $\mathsf{xML^F}$ *term with* $\Gamma \vdash a : \sigma$ *then* $\Gamma^\bullet; \vdash_{\mathsf{t}} a^\circ : \sigma^\bullet$.

Lemma 31. *Let* A *be an* $\mathsf{xML^F}$ *term or an instantiation. Then we have:*

(i) $(A\,[b/x])^\circ = A^\circ\,[b^\circ/x]$,

(ii) $(A\,[\mathbf{1}/!\alpha]\,[\tau/\alpha])^\circ = A^\circ\,[\underline{\lambda} z.z/i_\alpha]$,

(iii) $(A\,[\phi; !\alpha/!\alpha])^\circ = A^\circ\,[(\underline{\lambda} z.i_\alpha \triangleright (\phi^\circ \triangleright z))/i_\alpha]$.

The above lemmas are proved by a standard induction. The interested reader can find their proofs in Appendix A.

Theorem 32 (Coercion calculus simulates $\mathsf{xML^F}$)**.** *If $a \to_\beta b$ (resp. $a \to_\iota b$) in $\mathsf{xML^F}$, then $a^\circ \to_\beta b^\circ$ (resp. $a^\circ \overset{+}{\to}_{\mathsf{c}} b^\circ$) in $\mathsf{F_c}$.*

Proof. As the translation is contextual, it is sufficient to analyze each case of the reduction rules.

- $(\lambda(x:\tau)a)b \to_\beta a\,[b/x]$. We have $((\lambda(x:\tau)a)b)^\circ = (\lambda x.a^\circ)b^\circ$, β-reducing to $a^\circ\,[b^\circ/x]$, which is $(a\,[b/x])^\circ$ by Lemma 31(i).
- $a\mathbf{1} \to_\iota a$. We have $(a\mathbf{1})^\circ = \underline{\lambda} z.z \triangleright a^\circ \to_{\mathsf{c}} z\,[a^\circ/z] = a^\circ$.
- $a(\phi;\psi) \to_\iota a\phi\psi$. We have $(a(\phi;\psi))^\circ = (\underline{\lambda} z.\psi^\circ \triangleright (\phi^\circ \triangleright z)) \triangleright a^\circ \to_{\mathsf{c}} \psi^\circ \triangleright (\phi^\circ \triangleright a^\circ)$ which is equal to $(a\phi\psi)^\circ$.
- $a\parr \to_\iota \Lambda(\alpha \geq \bot)a$. Here we have $(a\parr)^\circ = (\underline{\lambda} x.\underline{\lambda} i_\alpha.x) \triangleright a^\circ \to_{\mathsf{c}} \underline{\lambda} i_\alpha.a = (\Lambda(\alpha \geq \bot)a)^\circ$.
- $(\Lambda(\alpha \geq \tau)a)\& \to_\iota a\,[\mathbf{1}/!\alpha]\,[\tau/\alpha]$. Here, we have:

$$\begin{aligned} ((\Lambda(\alpha \geq \tau)a)\&)^\circ &= (\underline{\lambda} x.x \triangleleft \underline{\lambda} z.z) \triangleright \underline{\not\lambda} i_\alpha.a^\circ \\ &\to_{\mathsf{c}} (\underline{\not\lambda} i_\alpha.a^\circ) \triangleleft \underline{\lambda} z.z \\ &\to_{\mathsf{c}} a^\circ\,[\underline{\lambda} z.z/i_\alpha] = (a\,[\mathbf{1}/!\alpha]\,[\tau/\alpha])^\circ, \text{ by Lemma 31(ii).} \end{aligned}$$

- $(\Lambda(\alpha \geq \tau)a)(\forall(\alpha \geq)\phi) \to_\iota \Lambda(\alpha \geq \tau)a\phi$. We have:

$$\begin{aligned} \big((\Lambda(\alpha \geq \tau)a)(\forall(\alpha \geq)\phi)\big)^\circ &= (\underline{\lambda} x.\underline{\not\lambda} i_\alpha.\phi^\circ \triangleright (x \triangleleft i_\alpha)) \triangleright (\underline{\not\lambda} i_\alpha.a^\circ) \\ &\to_{\mathsf{c}} \underline{\not\lambda} i_\alpha.\phi^\circ \triangleright ((\underline{\not\lambda} i_\alpha.a^\circ) \triangleleft i_\alpha)) \\ &\to_{\mathsf{c}} \underline{\not\lambda} i_\alpha.\phi^\circ \triangleright a^\circ = (\Lambda(\alpha \geq \tau)a\phi)^\circ. \end{aligned}$$

- $(\Lambda(\alpha \geq \tau)a)(\forall(\geq \phi)) \to_\iota \Lambda(\alpha \geq \tau\phi)a\,[\phi;!\alpha/!\alpha]$. We have:

$$\begin{aligned} &\big((\Lambda(\alpha \geq \tau)a)(\forall(\geq \phi))\big)^\circ \\ &\quad = \big(\underline{\lambda} x.\underline{\not\lambda} i_\alpha.x \triangleleft (\underline{\lambda} z.i_\alpha \triangleright (\phi^\circ \triangleright z))\big) \triangleright (\underline{\not\lambda} i_\alpha.a^\circ) \\ &\quad \to_{\mathsf{c}} \underline{\not\lambda} i_\alpha.(\underline{\not\lambda} i_\alpha.a^\circ) \triangleleft (\underline{\lambda} z.i_\alpha \triangleright (\phi^\circ \triangleright z)) \\ &\quad \to_{\mathsf{c}} \underline{\not\lambda} i_\alpha.a^\circ\,[(\underline{\lambda} z.i_\alpha \triangleright (\phi^\circ \triangleright z))/i_\alpha] \\ &\quad = \underline{\not\lambda} i_\alpha.(a\,[\phi;!\alpha/!\alpha])^\circ = (\Lambda(\alpha \geq \tau\phi)a\,[\phi;!\alpha/!\alpha])^\circ, \end{aligned}$$

  by Lemma 31(iii). □

Corollary 33 (Termination)**.** $\mathsf{xML^F}$ *is strongly normalizing.*

5. Transferring Strong Normalization from xML^F to ML^F

In the previous section we have already shown SN of $\mathsf{xML^F}$. However in order to prove that $\mathsf{eML^F}$ and $\mathsf{iML^F}$ are normalizing too we need to make sure that ι-redexes cannot block β ones: in other words, a bisimulation result that we will achieve with Theorem 4. In this section we will show it by seeing how β and cv-reductions can be lifted to xML^F along the translation $(\,.\,)^\circ$ and concluding by the bisimulation result contained in Theorem 26. An alternative proof of the same result can be carried out directly inside xML^F: we will discuss it in the following section.

5.1. The lifting lemma

We will show here how reductions in a translation a° lift to ones of a. Let us show the case where $a^\circ \to_\beta b$ with this first lemma.

Lemma 34. *Let a be an xML^F term. If $a^\circ \to_\beta b$ in F_c then there is c with $a \to_\beta c$ and $c^\circ = b$.*

$$\begin{tikzcd} a \arrow[r, dashed, "\beta"] \arrow[d, mapsto] & c \arrow[d, dashed, mapsto] \\ a^\circ \arrow[r, "\beta"] & b \end{tikzcd}$$

Proof. By structural induction on a.

- $a = x$ $(a^\circ = x)$: impossible.
- $a = \lambda(x : \tau)a_1$ $(a^\circ = \lambda x.a_1^\circ)$, $\Lambda(\alpha \geq \tau)a_1$ $(a^\circ = \underline{\lambda} i_\alpha.a_1^\circ)$: the reduction takes necessarily place in a_1° and the inductive step is completed.
- $a = a_1\phi$ $(a^\circ = \phi^\circ \triangleright a_1^\circ)$: we see that ϕ° is a coercion by Lemma 29 and is thus β-normal by Lemma 7, so the reduction takes place in a_1° and we proceed as above.
- $a = a_1a_2$: from $a^\circ = a_1^\circ a_2^\circ$ we can as above reduce to the case where a is the redex to be fired. We then have $a_1^\circ = \lambda x.a_3'$ and $b = a_3' \left[a_2^\circ/x\right]$, and necessarily $a_1 = \lambda(x : \tau)a_3$ with $a_3^\circ = a_3'$, so $a \to_\beta a_3 \left[a_2/x\right]$ and $(a_3 \left[a_2/x\right])^\circ = b$ by Lemma 31(i). □

When moving on we quickly discover that in general it is not always possible to lift c-reductions in the above sense. Take for example $x\&$: it is normal in xML^F, but $(x\&)^\circ = (\underline{\lambda} y.y) \triangleright x \to_\mathsf{c} x$. However what is important for bisimulation is that the function side of a redex be always ι-reducible or directly a λ-abstraction. Indeed the cv-reductions can be lifted, as shown below.

Lemma 35. *Let a be an xML^F term. If $a^\circ \to_\mathsf{cv} b$ in F_c then there is c with $a \to_\beta c$ and $b \overset{=}{\to}_\mathsf{cv} c^\circ$.*

$$\begin{tikzcd} a \arrow[rr, dashed, "\iota"] \arrow[d, mapsto] & & c \arrow[d, dashed, mapsto] \\ a^\circ \arrow[r, "\mathsf{cv}"] & b \arrow[r, dashed, "\mathsf{cv}^{=}"] & c^\circ \end{tikzcd}$$

Proof. We reason again by induction on a. We can exclude $a = x$, and the inductive steps are trivial for a equal to $\lambda(x : \tau)a_1$, a_1a_2 and $\Lambda(\alpha \geq \tau)a_1$, as the cv-reduction necessarily takes place in a strict subterm. It only remains the case $a = a_1\phi$, where $a^\circ = \phi^\circ \triangleright a_1^\circ$.

If a° is not the immediate redex of the reduction, then the latter must take place in a_1°, as ϕ° is typed as a coercion (Lemma 29) and is thus cv-normal (Lemma 7). Inductive hypothesis then applies to a_1 and we are done.

Suppose therefore that $\phi^\circ \triangleright a_1^\circ$ is the redex being fired. The only way for a_1° to be a c-value is that either $a_1 = \lambda(x : \tau)a_3$ for any a_3, or $a_1 = \Lambda(\alpha \geq \tau)a_2$ (resp. $a_1 = a_2!\alpha$) with a_2° a c-value. First, we prove that $a_1\phi$ is necessarily a redex in xML^F. It would not be a redex only in the following cases.

- $\phi = \tau$: impossible as it requires a_1 to be of type $\bot$, which is excluded by all three alternatives for a_1.
- $\phi = \,!\beta$: this is likewise impossible as $\phi^\circ \triangleright a_1^\circ = i_\beta \triangleright a_1^\circ$ would not be a redex.
- a_1 not of the form $\Lambda(\alpha \geq \tau)a_2$ and $\phi = \&$, $\forall(\geq \psi)$ or $\forall(\alpha \geq)\psi$: excluding that a_1 starts with a Λ, we have $a_1 = \lambda(x : \tau)a_2$ or $a_1 = a_2!\alpha$. The type of a_1 would then be an arrow type or a type variable respectively, which are both incompatible with all the listed instantiations, which require a quantifier.

So there is c with $a_1\phi \to_\iota c$ obtained by firing $a_1\phi$ itself. Now take the steps $\phi^\circ \triangleright a_1^\circ \overset{*}{\to}_{\mathtt{c}} c^\circ$ simulating $a_1\phi \to_\iota c$, as shown in the proof of Theorem 32. We can then inspect such a proof and see that the first step always fires the redex $\phi^\circ \triangleright a_1^\circ$ (i.e. is the step we started with), which is then followed by at most one $\mathtt{c}$-step, which is a $\mathtt{cv}$ one if a_1° is a $\mathtt{c}$-value. □

Combining the two results above and some other properties of $\mathsf{F_c}$ we arrive to the statement below, which will lead the way to the bisimulation result.

Lemma 36 (Lifting)**.** *Given a typed* $\mathsf{xML^F}$ *term a, we have that if $a^\circ \overset{*}{\to}_{\mathtt{cv}}\to_\beta b$ then $a \overset{*}{\to}_\iota\to_\beta c$ with $b \overset{*}{\to}_{\mathtt{c}} c^\circ$.*

$$\begin{tikzcd}
a \arrow[r, dashed, "\iota*"] \arrow[d, mapsto] & {} \arrow[rr, dashed, "\beta"] & & c \arrow[d, mapsto, dashed] \\
a^\circ \arrow[r, "\mathtt{cv}*"] & {} \arrow[r, "\beta"] & b \arrow[r, dashed, "\mathtt{cv}*"] & c^\circ
\end{tikzcd}$$

Proof. As $\to_{\mathtt{cv}}$ is strongly normalizing (Corollary 18), we can reason by well-founded induction on a° with respect to $\to_{\mathtt{cv}}$.

First let us suppose that $a^\circ \to_\beta b$: we then apply Lemma 34 and get the result directly. Suppose then that $a^\circ \overset{+}{\to}_{\mathtt{cv}}\to_\beta b$. We have the following diagram:

$$\begin{tikzcd}
a \arrow[r, dashed, "\iota"] \arrow[dd, mapsto] \arrow[ddr, phantom, "\text{(i)}"] & a_1 \arrow[rr, dashed, "\iota*"] \arrow[d, mapsto, dashed] \arrow[drrr, phantom, "\text{(iv)}"] & & {} \arrow[r, dashed, "\beta"] & c \arrow[d, mapsto, dashed] \\
& a_1^\circ \arrow[r, dashed, "\mathtt{cv}*"] & {} \arrow[r, dashed, "\beta"] & {} \arrow[r, dashed, "\mathtt{cv}*"] & c^\circ \\
a^\circ \arrow[r, "\mathtt{cv}"'] & {} \arrow[u, dashed, "\mathtt{cv}="] \arrow[r, "\mathtt{cv}*"'] \arrow[ur, phantom, "\text{(ii)}"] & {} \arrow[u, dashed, "\mathtt{cv}*"] \arrow[r, "\beta"'] \arrow[ur, phantom, "\text{(iii)}"] & b \arrow[u, dashed, "\mathtt{cv}*"'] &
\end{tikzcd}$$

where in succession (i) comes from Lemma 35, (ii) is by confluence (Proposition 12), (iii) is by Proposition 24(ii) and (iv) is by inductive hypothesis, as $a^\circ \overset{+}{\to}_{\mathtt{cv}} a_1^\circ$. □

5.2. From Bisimulation to Strong Normalization of $\mathsf{eML^F}$ *and* $\mathsf{iML^F}$

With the results of the previous section at hand we are ready to obtain the following weak bisimulation result.

Theorem 37 (Bisimulation of $\lceil\,.\,\rceil$)**.** *Given a typed* $\mathsf{xML^F}$ *term a, we have that $\lceil a\rceil \to_\beta b$ iff $a \overset{*}{\to}_\iota\to_\beta c$ with $\lceil c\rceil = b$.*

$$\begin{tikzcd}
a \arrow[r, "\iota*"] \arrow[d, mapsto] & {} \arrow[r, "\beta"] \arrow[d, phantom, "\Updownarrow"] & c \arrow[d, mapsto] \\
\lceil a\rceil \arrow[rr, "\beta"'] & & b
\end{tikzcd}$$

Proof. For the if part, by Theorem 32 we have $a^\circ \overset{*}{\rightarrow}_{\mathsf{c}}\rightarrow_\beta c^\circ$, which by Lemma 28 and Proposition 24 implies $\lceil a \rceil = \lfloor a^\circ \rfloor \rightarrow_\beta \lfloor c^\circ \rfloor = \lceil c \rceil$. For the only if part, as $\lfloor a^\circ \rfloor = \lceil a \rceil \rightarrow_\beta b$, by Theorem 26 $a^\circ \overset{*}{\rightarrow}_{\mathsf{cv}}\rightarrow_\beta b'$ with $\lfloor b' \rfloor = b$. Now by Lemma 36 we have that $b' \overset{*}{\rightarrow}_{\mathsf{c}} c^\circ$ with $a \overset{*}{\rightarrow}_\iota\rightarrow_\beta c$. To conclude, we see that $\lceil c \rceil = \lfloor c^\circ \rfloor = \lfloor b' \rfloor = b$, where we used Lemma 28 and Proposition 24(iv). □

In the next section we will show that the above proof may be completely carried out within $\mathsf{xML^F}$, by applying a suitably modified version of Lemma 25. We preferred this formulation here since it provides a better understanding of what happens on the side of the coercion calculus.

We are now ready to complete the main result of the paper for the other versions of $\mathsf{ML^F}$.

Corollary 38. *Terms typed in* $\mathsf{iML^F}$ *and* $\mathsf{eML^F}$ *are strongly normalizing.*

Proof. Suppose an $\mathsf{iML^F}$ term a has an infinite reduction. By Theorem 4 we have an $\mathsf{xML^F}$ term a^* such that $\lceil a^* \rceil = a$. Then by the bisimulation result above each step from a can iteratively be lifted to at least a step from a^*, giving rise to an infinite chain in $\mathsf{xML^F}$ which is impossible by Corollary 18.

For $\mathsf{eML^F}$ the reasoning is identical, there is only a further type erasure from $\mathsf{eML^F}$ to $\mathsf{iML^F}$. □

6. An Alternative Proof of Bisimulation

In this section we provide an alternative proof of Theorem 37, completely carried out within the $\mathsf{xML^F}$ system (given the SN result for $\mathsf{xML^F}$). This proof is provided as a comparison to the one using $\mathsf{F_c}$. We first need this intermediate lemma, which is a version of Lemma 25 in $\mathsf{xML^F}$.

Lemma 39. *If a is typable and ι-normal and $\lceil a \rceil = \lambda x.b$, then it is of one of the following forms, with c ι-normal:*

- *$a = \lambda(x : \tau)c$ with $\lceil c \rceil = b$;*
- *$a = \Lambda(\alpha \geq \tau)c$;*
- *$a = c!\alpha$.*

In particular if a is typed with some arrow type $\tau \rightarrow \sigma$, then $a = \lambda(x : \tau)c$.

Proof. By induction on a. As $\lceil a \rceil = \lambda x.b$ then a is neither an application nor a variable. Let us suppose that a is not of one of the above listed forms. The only remaining case is $a = a'\phi$ with a' ι-normal and $\phi \neq !\alpha$. By inductive hypothesis (as $\lceil a' \rceil = \lceil a \rceil = \lambda x.b$) we have that a' is one among $\lambda(x : \tau)c'$, $\Lambda(\alpha \geq \tau)c'$ and $c'!\alpha$, with c' ι-normal.

Now let us rule out all the cases for ϕ.

- $\phi = \sigma$: impossible as none of the three alternatives for a' is typable by $\bot$;

- $\phi = \mathbf{1}$, $\psi_1; \psi_2$ or $\invamp$: impossible as $a'\phi$ would not be ι-normal;
- $\phi = \forall(\alpha \geq)\psi$, $\forall(\geq \psi)$ or &: by typing a' must be $\Lambda(\alpha \geq \tau)c'$, as the other two alternatives would give an arrow and a variable type respectively, which is not compatible with these instantiations; however this is not possible as $a'\phi$ would form a ι-redex.

This concludes the proof. In case a has an arrow type $\tau \to \sigma$, the only compatible form is $a = \lambda(x : \tau)c$. □

Alternative proof of Theorem 37. The if part is immediate by verifying that $a \to_\iota^* a'$ implies $\lceil a \rceil = \lceil a' \rceil$, and $a' \to_\beta c$ implies $\lceil a' \rceil \to_\beta \lceil c \rceil$.

For the only if part, let a_0 be the ι-normal form of a (which exists as $\to_\iota$ is SN by Theorem 32). We have that $\lceil a_0 \rceil = \lceil a \rceil \to_\beta b$: if we prove that $a_0 \to_\beta c$ with $\lceil c \rceil = b$ we are done. Let us reason by induction on a_0.

- $a_0 = x$: impossible, as $\lceil a_0 \rceil = x$ is not reducible.
- $a_0 = \lambda(x : \tau)a_1$, $\Lambda(\alpha \geq \tau)a_1$ or $a_1\phi$: the reduction takes place in $\lceil a_1 \rceil$ and inductive hypothesis applies smoothly giving a β-reduction in a_1, and thus in a_0.
- $a_0 = a_1 a_2$: if the reduction takes place in $\lceil a_1 \rceil$ or $\lceil a_2 \rceil$ then the inductive hypothesis applies as above. Suppose then that $\lceil a_1 \rceil \lceil a_2 \rceil$ is itself the redex being fired, i.e. $\lceil a_1 \rceil = \lambda x.d$ and $b = d\,[\lceil a_2 \rceil / x]$. As a_1 is typed with some $\sigma \to \tau$ (in order to form the application) and $\lceil a_1 \rceil = \lambda x.d$, by Lemma 39 we have that $a_1 = \lambda(x : \sigma)a_3$ with $\lceil a_3 \rceil = d$, so $a_0 = (\lambda(x : \sigma)a_3)a_2 \to_\beta a_3\,[a_2/x]$ and $\lceil a_3\,[a_2/x] \rceil = d\,[\lceil a_2 \rceil / x] = b$. □

7. A Short Trip through Candidates of Reducibility

In this section we will show what results and difficulties one encounters if trying to adapt the proof by Girard and Tait's method of *candidates of reducibility* [4, 17] (or more precisely here *saturated sets*) to ML^F. The base idea is analogous to what done for $\mathsf{F}_{<:}$ in [11]: in a nutshell, interpret the instance bound by a subset of candidates. However, one stumbles into a difficulty and an unexpected glitch which are worth mentioning.

- The method shows the strong normalization of $\lceil a \rceil$ for every xML^F term a, but cannot say anything about the non-trivial type reduction $\to_\iota$. A separate proof of SN of $\to_\iota$ is needed, which together with the bisimulation result of Theorem 37 gives then SN for the whole of $\to_{\beta\iota}$. Probably a direct proof of SN of $\to_\iota$ is not overtly hard, but the simulation to system F via $\mathsf{F_c}$ wraps SN of the whole of $\to_{\beta\iota}$ together.
- As one proves SN of $\lceil a \rceil$ for xML^F terms a, the result applies to eML^F or iML^F via compilation. However using the same interpretation directly on terms in $\mathsf{eML}^\mathsf{F}/\mathsf{iML}^\mathsf{F}$ and their types *does not work* in general. The

apparent mismatch is due to the fact that the compilation a^* to $\mathsf{xML^F}$ described in [8] actually changes the type derivation of a before starting to build the $\mathsf{xML^F}$ term. So in fact there are some $\mathsf{iML^F}$ typings that do not survive the compilation process and which seem to pose serious issues to the candidates of reducibility argument. While we must admit it is quite confusing, we think this glitch may show some insight in $\mathsf{eML^F}$ and $\mathsf{iML^F}$'s type systems.

7.1. A Quick Recapitulation of Saturated Sets

We here briefly sketch the definitions and properties of *saturated sets* of ordinary λ-terms (whose set we denote by Λ). More details can be found in [18, 19]. We denote a sequence of terms $P_1 \cdots P_k$ by $\vec{P}$ and consequently the iterated application $MP_1 \cdots P_k$ by $M\vec{P}$.

Definition 40.

- Let $\mathsf{SN} := \{M \in \Lambda \mid M \text{ is strongly normalizable }\}$.
- For $\mathcal{A}, \mathcal{B} \subseteq \Lambda$ let $\mathcal{A} \to \mathcal{B} := \{M \in \Lambda \mid (\forall N \in A)\ MN \in B\}$.
- A set $\mathcal{A} \subseteq \mathsf{SN}$ is said to be **saturated** if

  S1) for all $\vec{P} \in \mathsf{SN}$ and any variable x we have $x\vec{P} \in \mathcal{A}$;

  S2) for all $\vec{P}, Q \in \mathsf{SN}$, if $M\,[Q/x]\,\vec{P} \in \mathcal{A}$ then $(\lambda x.M)Q\vec{P} \in \mathcal{A}$.

The set of saturated sets is denoted by SAT.

The following results are standard.

Lemma 41.

(i) SN *is saturated,*

(ii) $A, B \in \mathsf{SAT}$ *implies* $A \to B \in \mathsf{SAT}$,

(iii) Given a family $\{A_i\}_{i \in I}$ *such that* $A_i \in \mathsf{SAT}$ *we have* $\bigcap_{i \in I} A_i \in \mathsf{SAT}$.

7.2. Saturated Interpretation for $\mathsf{xML^F}$

In the following we will consider how to interpret types as saturated sets. As already hinted, the type instance relation $\leq$ will be modeled by set inclusion $\subseteq$ in SAT.

Definition 42. An **interpretation** Σ is a function from type variables to saturated sets. Let $\Sigma[\alpha \mapsto \mathcal{A}]$ be defined as Σ on $\beta \neq \alpha$ and as $\mathcal{A}$ on α. We extend an interpretation Σ to all $\mathsf{xML^F}$ types by the following recursion:

$$\Sigma(\sigma \to \tau) := \Sigma(\sigma) \to \Sigma(\tau),$$

$$\Sigma(\forall(\alpha \geq \sigma)\tau) := \bigcap_{\substack{\mathcal{A} \in \mathsf{SAT} \\ \mathcal{A} \supseteq \Sigma(\sigma)}} \Sigma[\alpha \mapsto \mathcal{A}](\tau), \qquad \Sigma(\bot) := \bigcap_{\mathcal{A} \in \mathsf{SAT}} \mathcal{A}.$$

Lemma 41 shows that indeed the above definition maps types to SAT.

The following lemma is also quite standard and shown by a trivial induction.

Lemma 43.

(i) If $\alpha \notin \mathrm{ftv}(\sigma)$ *then* $\Sigma[\alpha \mapsto \mathcal{A}](\sigma) = \Sigma(\sigma)$*;*

(ii) $\Sigma(\sigma\,[\tau/\alpha]) = \Sigma[\alpha \mapsto \Sigma(\tau)](\sigma)$*.*

Definition 44. A **substitution** S is a function from term variables to *ordinary* λ-terms, which is then extended to all λ-terms by setting

$$S(M) = M\,[S(x_1)/x_1] \cdots [S(x_n)/x_n] \text{ where } \{x_1, \dots, x_n\} = \mathrm{fv}(M).$$

Given a subsitution S and an evaluation Σ, we write

- $\Sigma, S \vDash M : \sigma$ for an $\mathsf{xML}^{\mathsf{F}}$ term M if $S(\lceil M \rceil) \in \Sigma(\sigma)$;
- $\Sigma, S \vDash \Gamma$ for an $\mathsf{xML}^{\mathsf{F}}$ context if
  - for all $x : \sigma \in \Gamma$ we have $\Sigma, S \vDash x : \sigma$, i.e. $S(x) \in \Sigma(\sigma)$;
  - for all $\alpha \geq \sigma \in \Gamma$ we have $\Sigma(\alpha) \supseteq \Sigma(\sigma)$.

We divide the adequacy of the interpretation with respect to the typing rules in two results: in one we settle instantiations, while the other is for terms.

Lemma 45. *If* $\Gamma \vdash \phi : \sigma \leq \tau$ *and* $\Sigma, S \vDash \Gamma$ *then* $\Sigma(\sigma) \subseteq \Sigma(\tau)$*.*

Proof. By induction on the derivation, splitting by cases on the last rule.

- IComp and IRef are trivial.
- IBot, $\Gamma \vdash \tau : \bot \leq \tau$. By definition $\Sigma(\bot)$ is the bottom element of the meet-semilattice SAT.
- IAbstr, $\Gamma \vdash !\alpha : \tau \leq \alpha$ where $\alpha \geq \tau \in \Gamma$. By definition of $\Sigma, S \vDash \Gamma$, we have $\Sigma(\tau) \subseteq \Sigma(\alpha)$.
- IUnder, $\Gamma \vdash \forall(\alpha \geq)\phi : \forall(\alpha \geq \sigma)\tau_1 \leq \forall(\alpha \geq \sigma)\tau_2$. By well-formedness of the context in $\Gamma, \alpha \geq \sigma \vdash \phi : \tau_1 \leq \tau_2$ we have $\alpha \notin \mathrm{ftv}(\Gamma)$. Hence from $\Sigma, S \vDash \Gamma$ and for any $\mathcal{A} \supseteq \Sigma(\sigma)$ we can deduce $\Sigma[\alpha \to \mathcal{A}], S \vDash \Gamma, \alpha \geq \sigma$ by Lemma 43(i). By inductive hypothesis we then have $\Sigma[\alpha \to \mathcal{A}](\tau_1) \subseteq \Sigma[\alpha \to \mathcal{A}](\tau_2)$ for all $\mathcal{A} \supseteq \Sigma(\sigma)$, so that

$$\Sigma(\forall(\alpha \geq \sigma)\tau_1) = \bigcap_{\mathcal{A} \supseteq \Sigma(\sigma)} \Sigma[\alpha \mapsto \mathcal{A}](\tau_1) \subseteq \bigcap_{\mathcal{A} \supseteq \Sigma(\sigma)} \Sigma[\alpha \mapsto \mathcal{A}](\tau_2) = \Sigma(\forall(\alpha \geq \sigma)\tau_2).$$

- IInside, $\Gamma \vdash \forall(\geq \phi) : \forall(\alpha \geq \tau_1)\sigma \leq \forall(\alpha \geq \tau_2)\sigma$. By inductive hypothesis $\Sigma(\tau_1) \subseteq \Sigma(\tau_2)$, so that

$$\{\, \mathcal{A} \in \mathsf{SAT} \mid \mathcal{A} \supseteq \Sigma(\tau_1) \,\} \supseteq \{\, \mathcal{A} \in \mathsf{SAT} \mid \mathcal{A} \supseteq \Sigma(\tau_2) \,\}$$

which entails

$$\Sigma(\forall(\alpha \geq \tau_1)\sigma) = \bigcap_{\mathcal{A}\supseteq\Sigma(\sigma)} \Sigma[\alpha \mapsto \mathcal{A}](\tau_1) \subseteq \bigcap_{\mathcal{A}\supseteq\Sigma(\sigma)} \Sigma[\alpha \mapsto \mathcal{A}](\tau_2) = \Sigma(\forall(\alpha \geq \tau_2)\sigma).$$

- IIntro, $\Gamma \vdash \parr : \tau \leq \forall(\alpha \geq \bot)\tau$ where $\alpha \notin \mathrm{ftv}(\tau)$. Lemma 43(i) entails

  $$\Sigma(\forall(\alpha \geq \bot)\tau) = \bigcap_{\mathcal{A}\in\mathsf{SAT}} \Sigma[\alpha \mapsto \mathcal{A}](\tau) = \bigcap_{\mathcal{A}\supseteq\Sigma(\sigma)} \Sigma(\tau) = \Sigma(\tau).$$

- IElim, $\Gamma \vdash \& : \forall(\alpha \geq \sigma)\tau \leq \tau\,[\sigma/\alpha]$. We have

  $$\Sigma(\forall(\alpha \geq \sigma)\tau) = \bigcap_{\mathcal{A}\supseteq\Sigma(\sigma)} \Sigma[\alpha \mapsto \mathcal{A}](\tau_1) \subseteq \Sigma[\alpha \mapsto \Sigma(\sigma)](\tau_2) = \Sigma(\forall(\alpha \geq \sigma)\tau_2).$$

  where the last equality comes from Lemma 43(ii). □

Lemma 46. *If $\Gamma \vdash a : \sigma$ and $\Sigma, S \vDash \Gamma$ then $\Sigma, S \vDash M : \sigma$.*

Proof. Again an induction on the derivation of $\Gamma \vdash a : \sigma$ settles the case. Var, Abs and App are as usual, but we include the cases for completeness.

- Var, $\Gamma \vdash x : \tau$, where $\Gamma(x) = \tau$. Directly from the definition $\Sigma, S \vDash \Gamma$.
- Abs, $\Gamma \vdash \lambda(x : \tau)a : \tau \to \sigma$. In order to show that $S(\lceil \lambda(x : \tau)a \rceil) \in \Sigma(\tau \to \sigma) = \Sigma(\tau) \to \Sigma(\sigma)$ we take any $b \in \Sigma(\tau)$. Without loss of generality we can set $S(x) = x$ and $x \notin \mathrm{fv}(b)$. Then clearly $\Sigma, S[x \mapsto b] \vDash \Gamma, x : \tau$, so that inductive hypothesis $S(\lceil a \rceil)\,[b/x] = S[x \mapsto b](\lceil M \rceil) \in \Sigma(\sigma)$. By definition of saturated set we obtain $S(\lceil \lambda(x : \tau)a \rceil)b = \lambda x.S(\lceil a \rceil))b \in \Sigma(\sigma)$ which concludes the case.
- App, $\Gamma \vdash ab : \tau$ with $\Gamma \vdash a : \sigma \to \tau$. By induction hypothesis we have $\lceil a \rceil \in \Sigma(\sigma) \to \Sigma(\tau)$ and $\lceil b \rceil \in \Sigma(\sigma)$, which by definition entails $\lceil ab \rceil = \lceil a \rceil \lceil b \rceil \in \Sigma(\tau)$.
- TApp, $\Gamma \vdash a\phi : \sigma$ with $\Gamma \vdash \phi : \tau \leq \sigma$. By Lemma 45 $\Sigma(\tau) \subseteq \Sigma(\sigma)$, and by inductive hypothesis we can obtain

  $$S(\lceil a\phi \rceil) = S(\lceil a \rceil) \in \Sigma(\tau) \subseteq \Sigma(\sigma).$$

  which concludes the proof. □

Corollary 47. *If $\Gamma \vdash a : \sigma$ then $\lceil a \rceil \in \mathsf{SN}$.*

Proof. It suffices to take $\Sigma(\alpha) = \mathsf{SN}$ for all α (which is correct by Lemma 41) and $S(x) = x$ for all x. Then necessarily $\Sigma, S \vDash \Gamma$ (as $x \in \mathsf{SN}$ and $\mathsf{SN} \supseteq \Sigma(\tau)$), so that by the above lemma we get $\lceil a \rceil = S(\lceil a \rceil) \in \Sigma(\sigma) \subseteq \mathsf{SN}$. □

Corollary 48. *If a is a typed $\mathsf{iML}^{\mathsf{F}}$ or $\mathsf{eML}^{\mathsf{F}}$ term then a is strongly normalizing.*

Proof. Even if a is in $\mathsf{eML^F}$ its reductions are exactly those of $\lceil a \rceil$. In any case by Theorem 4 we have $\lceil a \rceil = \lceil a^* \rceil \in \mathsf{SN}$. □

Notice however that a separate proof of SN of $\to_\iota$ is needed to obtain again the remaining main result about SN of $\mathsf{xML^F}$. This is one of the main reasons we preferred anyway the proof via translation, the other reason being the study of $\mathsf{F_c}$ which has its own interest in our view.

7.3. The Issue of the Interpretation in $\mathsf{eML^F}$ *and* $\mathsf{iML^F}$*.*

Here we will briefly sketch the problems one encounters when applying the interpretation depicted above directly in $\mathsf{eML^F}$ or $\mathsf{iML^F}$. For the sake of space we will not be able to completely present the systems. The interested reader is referred to the literature about $\mathsf{ML^F}$ [6, 12, 13, 7].

First, types in $\mathsf{eML^F}$ and $\mathsf{iML^F}$ are built also out of the *rigid quantification* $\forall(\alpha = \sigma)\tau$. The most sensible way to interpret it would be

$$\Sigma(\forall(\alpha = \sigma)\tau) = \Sigma[\alpha \mapsto \Sigma(\sigma)](\tau) = \Sigma(\sigma\,[\tau/\alpha]),$$

in accordance with the semantic meaning given to rigid quantification, which is needed for type inference only.

Apart from $\mathsf{xML^F}$, the instance relation on types is tiered in three parts: an equivalence $\equiv$ (for relations such as commutation of quantifiers or such as $\forall(\alpha \geq \sigma)\alpha \equiv \sigma$), an *abstraction* relation $\mathrel{-\!\!\!\sqsubset}$ which pertains operations concerning the rigid quantifier (so that for example $\Gamma \vdash \sigma \mathrel{-\!\!\!\sqsubset} \alpha$ if $\alpha = \sigma \in \Gamma$) and finally the instance relation $\sqsubseteq$. One has

$$\equiv \subseteq \mathrel{-\!\!\!\sqsubset} \subseteq \sqsubseteq, \qquad \sqsubseteq \cap \sqsupseteq = \equiv.$$

With respect to $\mathsf{xML^F}$ there is a subtle difference between $\sqsubseteq$ and $\leq$, paramount to type inference. In fact $\leq$ may be decomposed as

$$\sigma \leq \tau \iff \sigma \mathrel{\sqsupset\!\!\!-} \sqsubseteq \mathrel{\sqsupset\!\!\!-} \tau$$

using the inverse relation $\mathrel{\sqsupset\!\!\!-}$. The part $\sqsubseteq$ of $\leq$ is completely recoverable by the automatic type inferencer, and it is in fact the $\mathrel{\sqsupset\!\!\!-}$ parts that need explicit annotations in $\mathsf{eML^F}$. Notice that $\mathrel{-\!\!\!\sqsubset}$ from the point of view of full type instance will be contained both in $\leq$ and $\geq$, so it is in fact part of the equivalence relation associated with the preorder $\leq$. Semantically $\mathrel{-\!\!\!\sqsubset}$ is thus a completely reversible operation, while it is irreversible *vis-à-vis* the inferencer.

Because of the above reasons it is to be expected that the interpretation should enjoy the following (supposing $\Sigma, S \vDash \Gamma$):

- if $\Gamma \vdash \sigma \equiv \tau$ then $\Sigma(\sigma) = \Sigma(\tau)$;
- if $\Gamma \vdash \sigma \mathrel{-\!\!\!\sqsubset} \tau$ then $\Sigma(\sigma) = \Sigma(\tau)$;
- if $\Gamma \vdash \sigma \sqsubseteq \tau$ then $\Sigma(\sigma) \subseteq \Sigma(\tau)$.

In fact the point that fails is already the first. If σ is equivalent to a *monomorphic* type (i.e. quantifier free), then we have:

$$\alpha \geq \sigma \in \Gamma \implies \tau \equiv \tau\,[\sigma/\alpha]$$

by the Eq-Mono rule of [6] (or by the *similarity* relation in the graphic representation of ML^F types [13, Definition 5.3.12]). Now there is no way to pass from $\Sigma(\alpha) \supseteq \Sigma(\sigma)$ of the hypothesis $\Sigma, S \vDash \Gamma$ to $\Sigma(\tau) = \Sigma(\tau\,[\sigma/\alpha])$. In rough words, there is no way for the interpretation as we defined to distinguish between a truly polymorphic type and a monomorphic one.

While we did try to change the interpretation of types along several directions, we always found some of the rules failing. However presenting these trials is well outside the scope of this paper, also due to their failure.

Further works

We were able to prove new results for ML^F (namely SN and bisimulation of xML^F with its type erasure) by employing a more general calculus of coercions. It becomes natural then to ask whether its type system may be a framework to study coercions in general. A first natural target are the coercions arising from Leijen's translation of ML^F [10], which is more optimized than ours, in the sense that it does not add additional and unneeded structure to system F types. We plan then to study the coercions arising in F_η [20] or when using subtyping [21]. As explained at the beginning of section 3, $\mathsf{F_c}$ was purposely tailored down to suit xML^F, stripping it of natural features.

A first, easy extension would consist in more liberal types and typing rules, allowing coercion polymorphism, coercion abstraction of coercions or even coercions between coercions (i.e. allowing types $\forall\alpha.\kappa$, $\kappa_1 \to \kappa_2$ and $\kappa_1 \multimap \kappa_2$). To progress further however, one would need a way to build coercions of arrow types, which are unneeded in xML^F. Namely, given coercions $c_1 : \sigma_2 \multimap \sigma_1$ and $c_2 : \tau_1 \multimap \tau_2$, there should be a coercion $c_1 \Rightarrow c_2 : (\sigma_1 \to \tau_1) \multimap (\sigma_2 \to \tau_2)$, allowing a reduction $(c_1 \Rightarrow c_2) \triangleright \lambda x.a \to_\mathsf{c} \lambda x.c_2 \triangleright a\,[c_1 \triangleright x/x]$. This could be achieved either by introducing it as a primitive, by translation or by special typing rules. Indeed, if some sort of η-expansion would be available while building a coercion, one could write $c_1 \Rightarrow c_2 := \underline{\lambda} f.\lambda x.(c_2 \triangleright (f(c_1 \triangleright x)))$. However how to do this without loosing bisimulation is under investigation.

Acknowledgements. We thank Didier Rémy for stimulating discussions and remarks.

References

[1] R. Milner, M. Tofte, D. Macqueen, The definition of Standard ML, MIT Press, Cambridge, MA, USA, ISBN 0262631814, 1997.

[2] R. Milner, A theory of type polymorphism in programming, Journal of Computer and System Sciences 17 (1978) 348–75.

[3] F. Pottier, D. Rémy, The Essence of ML type inference, in: B. C. Pierce (Ed.), Advanced Topics in Types and Programming Languages, chap. 10, MIT Press, 389–489, 2005.

[4] J.-Y. Girard, Y. Lafont, P. Taylor, Proofs and Types, no. 7 in Cambridge tracts in theoretical computer science, Cambridge University Press, 1989.

[5] J. B. Wells, Typability and Type Checking in System F are Equivalent and Undecidable, Ann. Pure Appl. Logic 98 (1-3) (1999) 111–56.

[6] D. Le Botlan, D. Rémy, ML^{F}: Raising ML to the power of System F, in: Proc. of International Conference on Functional Programming (ICFP'03), 27–38, 2003.

[7] D. L. Botlan, D. Rémy, Recasting ML^{F}, Inf. Comput. 207 (6) (2009) 726–85.

[8] D. Rémy, B. Yakobowski, A Church-style intermediate language for ML^{F}, URL http://www.yakobowski.org/xmlf.html, submitted, 2009.

[9] H. Barendregt, The lambda calculus, its syntax and semantics, no. 103 in Studies in Logic and the Foundations of Mathematics, North-Holland, second edn., 1984.

[10] D. Leijen, A type directed translation of ML^{F} to System F, in: Proc. of International Conference on Functional Programming (ICFP'07), ACM Press, 2007.

[11] G. Ghelli, Termination of System F-bounded: A Complete Proof, Inf. Comput. 139 (1) (1997) 39–56.

[12] D. Le Botlan, ML^{F} : Une extension de ML avec polymorphisme de second ordre et instanciation implicite, Ph.D. thesis, École Polytechnique, Available at gallium.inria.fr/~remy/mlf/mlf.pdf, 2004.

[13] D. Le Botlan, Types et contraintes graphiques : polymorphisme de second ordre et inférence, Ph.D. thesis, Université Paris Diderot (Paris 7), Available at hal.inria.fr/tel-00357708/, 2008.

[14] A. Barber, G. Plotkin, Dual intuitionistic linear logic, Technical Report LFCS-96-347, University of Edinburgh, 1997.

[15] J.-Y. Girard, Linear logic, Th. Comp. Sc. 50 (1987) 1–102.

[16] P. Baillot, K. Terui, Light types for polynomial time computation in lambda calculus, Inf. Comput. 207 (1) (2009) 41–62.

[17] W. W. Tait, Intentional interpretation of functionals of finite type I, Journal of Symbolic Logic 32 (1967) 198–212.

[18] J.-L. Krivine, Lambda-calculus, Types and Models, Ellis Horwood, New York, ISBN 0-13-062407-1, translated from the ed. Masson, 1990, French original, 1993.

[19] H. Barendregt, S. Abramsky, D. M. Gabbay, T. S. E. Maibaum, H. P. Barendregt, Lambda Calculi with Types, in: Handbook of Logic in Computer Science, Oxford University Press, 117–309, 1992.

[20] J. C. Mitchell, Coercion and type inference, in: Proc. of 11th symposium on Principles of programming languages (POPL'84), ACM, ISBN 0-89791-125-3, 175–85, 1984.

[21] K. Crary, Typed compilation of inclusive subtyping, in: Proc. of International Conference on Functional Programming (ICFP'00), 68–81, 2000.

A. Technical Proofs

This technical appendix is devoted to provide the proofs of Lemmas 29, 30 and 31. These proofs are not particularly difficult, but long and require the following preliminary lemma.

Lemma 49. *Let σ, τ be $\mathsf{xML^F}$ types, then $(\sigma\,[\tau/\alpha])^\bullet = \sigma^\bullet\,[\tau^\bullet/\alpha]$.*

Proof. By structural induction on σ.

- $\sigma = \alpha$: $(\alpha\,[\tau/\alpha])^\bullet = \tau^\bullet = \alpha^\bullet\,[\tau^\bullet/\alpha]$.
- $\sigma = \beta \neq \alpha$: $(\beta\,[\tau/\alpha])^\bullet = \beta^\bullet = \beta^\bullet\,[\tau^\bullet/\alpha]$.
- $\sigma = \sigma_1 \to \sigma_2$: we have $((\sigma_1 \to \sigma_2)\,[\tau/\alpha])^\bullet = (\sigma_1\,[\tau/\alpha] \to \sigma_2\,[\tau/\alpha])^\bullet = (\sigma_1\,[\tau/\alpha])^\bullet \to (\sigma_2\,[\tau/\alpha])^\bullet$. By the induction hypothesis, this is equal to $\sigma_1^\bullet\,[\tau^\bullet/\alpha] \to \sigma_2^\bullet\,[\tau^\bullet/\alpha] = (\sigma_1^\bullet \to \sigma_2^\bullet)\,[\tau^\bullet/\alpha]$.
- $\sigma = \bot$: $(\bot\,[\tau/\alpha])^\bullet = \bot^\bullet = \forall\beta.\beta = (\forall\beta.\beta)\,[\tau^\bullet/\alpha] = \bot^\bullet\,[\tau^\bullet/\alpha]$.
- $\sigma = \forall(\beta \geq \sigma_1)\sigma_2$ (supposing $\beta \notin \mathrm{ftv}(\tau) \cup \{\alpha\}$):

$$\begin{aligned}((\forall(\beta \geq \sigma_1)\sigma_2)\,[\tau/\alpha])^\bullet &= (\forall(\beta \geq \sigma_1\,[\tau/\alpha])\sigma_2\,[\tau/\alpha])^\bullet\\ &= \forall\beta.((\sigma_1\,[\tau/\alpha])^\bullet \multimap \beta) \to \sigma_2^\bullet\,[\tau^\bullet/\alpha]\\ &= \forall\beta.(\sigma_1^\bullet\,[\tau^\bullet/\alpha] \multimap \beta) \to \sigma_2^\bullet\,[\tau^\bullet/\alpha]\\ &= (\forall\beta.(\sigma_1^\bullet \multimap \beta) \to \sigma_2^\bullet)\,[\tau^\bullet/\alpha] = (\forall(\beta \geq \sigma_1)\sigma_2)^\bullet\,[\tau^\bullet/\alpha]\end{aligned}$$

  where we applied inductive hypothesis for the third equality. □

Lemma 29. If $\Gamma \vdash \phi : \sigma \leq \tau$ then $\Gamma^\bullet;\vdash_{\mathsf{c}} \phi^\circ : \sigma^\bullet \multimap \tau^\bullet$.

Proof. By induction on the derivation of $\Gamma \vdash \phi : \sigma \leq \tau$.

- IBot, $\Gamma \vdash \tau : \bot \leq \tau$. We have to prove that $\Gamma^\bullet;\vdash_{\mathsf{c}} \underline{\lambda} x.x : (\forall\alpha.\alpha) \multimap \tau^\bullet$. This follows by applying LAbs, Inst and LAx.
- IAbstr, $\Gamma \vdash\, !\alpha : \tau \leq \alpha$ where $\alpha \geq \tau \in \Gamma$. We have to prove $\Gamma^\bullet;\vdash_{\mathsf{c}} i_\alpha : \tau^\bullet \multimap \alpha$, which follows from Ax since $i_\alpha : \tau^\bullet \multimap \alpha \in \Gamma^\bullet$.
- IUnder, $\Gamma \vdash \forall(\alpha \geq)\phi : \forall(\alpha \geq \sigma)\tau_1 \leq \forall(\alpha \geq \sigma)\tau_2$. By induction hypothesis we have a proof π of $\Gamma';\vdash_{\mathsf{c}} \phi^\circ : \tau_1^\bullet \multimap \tau_2^\bullet$ where $\Gamma' := \Gamma^\bullet, i_\alpha : \sigma^\bullet \multimap \alpha$. Let $L := x : \forall\alpha.(\sigma^\bullet \multimap \alpha) \to \tau_1^\bullet$.

$$\dfrac{\dfrac{\dfrac{}{\Gamma'; L \vdash_\ell x : (\forall(\alpha \geq \sigma)\tau_1)^\bullet}\,\text{LAx}}{\Gamma'; L \vdash_\ell x : (\sigma^\bullet \multimap \alpha) \to \tau_1^\bullet}\,\text{Inst} \qquad \dfrac{}{\Gamma';\vdash_{\mathsf{c}} i_\alpha : \sigma^\bullet \multimap \alpha}\,\text{Ax}}{\vdots}\,\text{CApp}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\begin{matrix}\pi\\ \vdots\\ \Gamma';\vdash_{\mathsf{c}} \phi^\circ : \tau_1^\bullet \multimap \tau_2^\bullet\end{matrix} \qquad \begin{matrix}\vdots\\ \Gamma'; L \vdash_\ell x \triangleleft i_\alpha : \tau_1^\bullet\end{matrix}}{\Gamma'; L \vdash_\ell \phi^\circ \triangleright (x \triangleleft i_\alpha) : \tau_2^\bullet}\,\text{LApp}}{\Gamma^\bullet; L \vdash_\ell \underline{\Lambda} i_\alpha.\phi^\circ \triangleright (x \triangleleft i_\alpha) : (\sigma^\bullet \multimap \alpha) \to \tau_2^\bullet}\,\text{CAbs}}{\Gamma^\bullet; L \vdash_\ell \underline{\Lambda} i_\alpha.\phi^\circ \triangleright (x \triangleleft i_\alpha) : \forall\alpha.(\sigma^\bullet \multimap \alpha) \to \tau_2^\bullet}\,\text{Gen}}{\Gamma^\bullet;\vdash_{\mathsf{c}} \underline{\lambda} x.\underline{\Lambda} i_\alpha.\phi^\circ \triangleright (x \triangleleft i_\alpha) : (\forall(\alpha \geq \sigma)\tau_1)^\bullet \multimap (\forall(\alpha \geq \sigma)\tau_2)^\bullet}\,\text{LAbs}$$

- ICOMP, $\Gamma \vdash \phi;\psi : \tau_1 \leq \tau_3$. By induction hypothesis we have a proof π_1 of $\Gamma^\bullet;\vdash_{\mathsf{c}} \phi^\circ : \tau_1^\bullet \multimap \tau_2^\bullet$, and a proof π_2 of $\Gamma^\bullet;\vdash_{\mathsf{c}} \psi^\circ : \tau_2^\bullet \multimap \tau_3^\bullet$. Then we can build the following proof:

$$\dfrac{\dfrac{\begin{matrix}\pi_2\\ \vdots\\ \Gamma^\bullet;\vdash_{\mathsf{c}} \psi^\circ : \tau_2^\bullet \multimap \tau_3^\bullet\end{matrix}\qquad \dfrac{\begin{matrix}\pi_1\\ \vdots\\ \Gamma^\bullet;\vdash_{\mathsf{c}} \phi^\circ : \tau_1^\bullet \multimap \tau_2^\bullet\end{matrix}\quad \dfrac{}{\Gamma^\bullet; z : \tau_1^\bullet \vdash_\ell z : \tau_1^\bullet}\,\text{LAx}}{\Gamma^\bullet; z : \tau_1^\bullet \vdash_\ell \phi^\circ \triangleright z : \tau_2^\bullet}\,\text{LApp}}{\Gamma^\bullet; z : \tau_1^\bullet \vdash_\ell \psi^\circ \triangleright (\phi^\circ \triangleright z) : \tau_3^\bullet}\,\text{LApp}}{\Gamma^\bullet;\vdash_{\mathsf{c}} \underline{\lambda} z.\psi^\circ \triangleright (\phi^\circ \triangleright z) : \tau_1^\bullet \multimap \tau_3^\bullet}\,\text{LAbs}$$

- IINSIDE, $\Gamma \vdash \forall(\geq \phi) : \forall(\alpha \geq \tau_1)\sigma \leq \forall(\alpha \geq \tau_2)\sigma$. We can suppose $\alpha \notin \mathrm{ftv}(\Gamma) = \mathrm{ftv}(\Gamma^\bullet)$. We set $L := x : (\forall(\alpha \geq \tau_1)\sigma)^\bullet$ and $\Gamma' := \Gamma^\bullet, i_\alpha : (\tau_2^\bullet \multimap \alpha)$. By induction hypothesis (and Lemma 8) we have a proof of $\Gamma';\vdash_{\mathsf{c}} \phi^\circ : \tau_1^\bullet \multimap \tau_2^\bullet$. By mixing it with $\Gamma';\vdash_{\mathsf{c}} i_\alpha : \tau_2^\bullet \multimap \alpha$ and going through the same derivation as above for ICOMP, we get a proof π of $\Gamma';\vdash_{\mathsf{c}} \underline{\lambda} z.i_\alpha \triangleright (\phi^\circ \triangleright z) : \tau_1^\bullet \multimap \alpha$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma'; L \vdash_\ell x : (\forall(\alpha \geq \tau_1)\sigma)^\bullet}\,\text{LAx}}{\Gamma'; L \vdash_\ell x : (\tau_1^\bullet \multimap \alpha) \to \sigma^\bullet}\,\text{Inst}\qquad \begin{matrix}\pi\\ \vdots\\ \Gamma';\vdash_{\mathsf{c}} \underline{\lambda} z.i_\alpha \triangleright (\phi^\circ \triangleright z) : \tau_1^\bullet \multimap \alpha\end{matrix}}{\Gamma'; L \vdash_\ell x \triangleleft (\underline{\lambda} z.i_\alpha \triangleright (\phi^\circ \triangleright z)) : \sigma^\bullet}\,\text{CApp}}{\Gamma^\bullet; L \vdash_\ell \underline{\measuredangle} i_\alpha.x \triangleleft (\underline{\lambda} z.i_\alpha \triangleright (\phi^\circ \triangleright z)) : (\tau_2^\bullet \multimap \alpha) \to \sigma^\bullet}\,\text{CAbs}}{\Gamma^\bullet; L \vdash_\ell \underline{\measuredangle} i_\alpha.x \triangleleft (\underline{\lambda} z.i_\alpha \triangleright (\phi^\circ \triangleright z)) : (\forall(\alpha \geq \tau_2)\sigma)^\bullet}\,\text{Gen}}{\Gamma^\bullet;\vdash_{\mathsf{c}} \underline{\lambda} x.\underline{\measuredangle} i_\alpha.x \triangleleft (\underline{\lambda} z.i_\alpha \triangleright (\phi^\circ \triangleright z)) : (\forall(\alpha \geq \tau_1)\sigma)^\bullet \multimap (\forall(\alpha \geq \tau_2)\sigma)^\bullet}\,\text{LAbs}$$

- IINTRO, $\Gamma \vdash \parr : \tau \leq \forall(\alpha \geq \bot)\tau$ where $\alpha \notin \mathrm{ftv}(\tau)$. By α-conversion we can choose any $\alpha \notin \mathrm{ftv}(\Gamma^\bullet; x : \tau^\bullet)$, so the GEN rule in the following proof is applicable:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma^\bullet, i_\alpha : (\forall\beta.\beta) \multimap \alpha; x : \tau^\bullet \vdash_\ell x : \tau^\bullet}\,\text{LAx}}{\Gamma^\bullet; x : \tau^\bullet \vdash_\ell \underline{\measuredangle} i_\alpha.x : ((\forall\beta.\beta) \multimap \alpha) \to \tau^\bullet}\,\text{CAbs}}{\Gamma^\bullet; x : \tau^\bullet \vdash_\ell \underline{\measuredangle} i_\alpha.x : (\forall(\alpha \geq \bot)\tau)^\bullet}\,\text{Gen}}{\Gamma^\bullet;\vdash_{\mathsf{c}} \underline{\lambda} x.\underline{\measuredangle} i_\alpha.x : \tau^\bullet \multimap (\forall(\alpha \geq \bot)\tau)^\bullet}\,\text{LAbs}$$

- IELIM, $\Gamma \vdash \& : \forall(\alpha \geq \sigma)\tau \leq \tau\,[\sigma/\alpha]$. Note that α can be chosen not in $\mathrm{ftv}(\sigma^\bullet)$ and that $(\tau\,[\sigma/\alpha])^\bullet = \tau^\bullet\,[\sigma^\bullet/\alpha]$ holds by Lemma 49. Let $L := x : \forall\alpha.(\sigma^\bullet \multimap \alpha) \to \tau^\bullet$.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma^\bullet; L \vdash_\ell x : \forall\alpha.(\sigma^\bullet \multimap \alpha) \to \tau^\bullet}\,\text{LAx}}{\Gamma^\bullet; L \vdash_\ell x : (\sigma^\bullet \multimap \sigma^\bullet) \to \tau^\bullet\,[\sigma^\bullet/\alpha]}\,\text{Inst}\qquad \dfrac{\dfrac{}{\Gamma^\bullet; z : \sigma^\bullet \vdash_\ell z : \sigma^\bullet}\,\text{LAx}}{\Gamma^\bullet;\vdash_{\mathsf{c}} \underline{\lambda} z.z : \sigma^\bullet \multimap \sigma^\bullet}\,\text{LAbs}}{\Gamma^\bullet; L \vdash_\ell x \triangleleft \underline{\lambda} z.z : \tau^\bullet\,[\sigma^\bullet/\alpha]}\,\text{CApp}}{\Gamma^\bullet;\vdash_{\mathsf{c}} \underline{\lambda} x.x \triangleleft \underline{\lambda} z.z : (\forall(\alpha \geq \sigma)\tau)^\bullet \multimap (\tau\,[\sigma/\alpha])^\bullet}\,\text{LAbs}$$

- IID, $\Gamma \vdash \mathbf{1} : \tau \leq \tau$. We have $\Gamma^\bullet;\vdash_{\mathsf{c}} \underline{\lambda} z.z : \tau^\bullet \multimap \tau^\bullet$ by LABS and LAX. □

Lemma 30. If a is an $\mathsf{xML^F}$ term with $\Gamma \vdash a : \sigma$ then $\Gamma^\bullet; \vdash_{\mathtt{t}} a^\circ : \sigma^\bullet$.

Proof. By induction on the derivation of $\Gamma \vdash a : \sigma$.

- Var, $\Gamma \vdash x : \tau$, where $\Gamma(x) = \tau$. We then get $\Gamma^\bullet; \vdash_{\mathtt{t}} x : \tau^\bullet$ by Ax.
- Abs, $\Gamma \vdash \lambda(x : \tau)a : \tau \to \sigma$. By induction hypothesis we have a proof of $\Gamma^\bullet, x : \tau^\bullet; \vdash_{\mathtt{t}} a : \sigma^\bullet$ which by Abs gives $\Gamma^\bullet; \vdash_{\mathtt{t}} \lambda x.a : \tau^\bullet \to \sigma^\bullet$.
- App, $\Gamma \vdash ab : \tau$. By induction hypothesis we have proofs for $\Gamma^\bullet; \vdash_{\mathtt{t}} a : \tau^\bullet \to \sigma^\bullet$ and π_2 of $\Gamma^\bullet; \vdash_{\mathtt{t}} b : \tau^\bullet$ giving $\Gamma^\bullet; \vdash_{\mathtt{t}} ab : \sigma^\bullet$ by App.
- TAbs, $\Gamma \vdash \Lambda(\alpha \geq \sigma)a : \forall(\alpha \geq \sigma)\tau$ where $\alpha \notin \mathrm{ftv}(\Gamma)$. It follows that $\alpha \notin \mathrm{ftv}(\Gamma^\bullet)$, and as by induction hypothesis we have a proof π of $\Gamma^\bullet, i_\alpha : \sigma^\bullet \multimap \alpha; \vdash_{\mathtt{t}} a^\circ : \tau^\bullet$ we have

$$\dfrac{\dfrac{\begin{matrix}\pi \\ \vdots \\ \Gamma^\bullet, i_\alpha : \sigma^\bullet \multimap \alpha; \vdash_{\mathtt{t}} a^\circ : \tau^\bullet\end{matrix}}{\Gamma^\bullet; \vdash_{\mathtt{t}} \underline{\angle} i_\alpha . a^\circ : (\sigma^\bullet \multimap \alpha) \to \tau^\bullet}\,\textsc{CAbs}}{\Gamma^\bullet; \vdash_{\mathtt{t}} \underline{\angle} i_\alpha . a^\circ : \forall\alpha.(\sigma^\bullet \multimap \alpha) \to \tau^\bullet}\,\textsc{Gen}$$

- TApp, $\Gamma \vdash a\phi : \sigma$. Since $\Gamma \vdash \phi : \tau \leq \sigma$ holds we have a proof of $\Gamma^\bullet; \vdash_{\mathtt{c}} \phi^\circ : \tau^\bullet \multimap \sigma^\bullet$ by Lemma 29. By induction hypothesis we have also a proof of $\Gamma^\bullet; \vdash_{\mathtt{t}} a^\circ : \tau^\bullet$. The two together combined with a LApp rule give $\Gamma^\bullet; \vdash_{\mathtt{t}} \phi^\circ \triangleright a^\circ : \sigma^\bullet$. □

Lemma 31. Let A be a term or an instantiation. Then we have:

(i) $(A\,[b/x])^\circ = A^\circ\,[b^\circ/x]$,

(ii) $(A\,[\mathbf{1}/!\alpha]\,[\tau/\alpha])^\circ = A^\circ\,[\underline{\lambda} z.z/i_\alpha]$,

(iii) $(A\,[\phi; !\alpha/!\alpha])^\circ = A^\circ\,[(\underline{\lambda} z.i_\alpha \triangleright (\phi^\circ \triangleright z))/i_\alpha]$.

Proof. All three results are carried out by structural induction on A. The inductive steps of (i) are straightforward, taking into account that if $A = \phi$ then $\phi\,[b/x] = \phi$.

For (ii), when A is a term the inductive step is immediate. Otherwise:

- $A = \sigma$: we have $(\sigma\,[\mathbf{1}/!\alpha]\,[\tau/\alpha])^\circ = (\sigma\,[\tau/\alpha])^\circ = \underline{\lambda} x.x$, which is equal to $(\underline{\lambda} x.x)\,[\underline{\lambda} z.z/i_\alpha] = \sigma^\circ\,[\underline{\lambda} z.z/i_\alpha]$.
- $A = !\alpha$: we have $(!\alpha\,[\mathbf{1}/!\alpha]\,[\tau/\alpha])^\circ = (\mathbf{1})^\circ = \underline{\lambda} z.z = i_\alpha\,[\underline{\lambda} z.z/i_\alpha] = (!\alpha)^\circ\,[\underline{\lambda} z.z/i_\alpha]$.
- $A = \forall(\geq \phi)$: we have

$$\begin{aligned}
(\forall(\geq \phi)\,[\mathbf{1}/!\alpha]\,[\tau/\alpha])^\circ &= (\forall(\geq \phi\,[\mathbf{1}/!\alpha]\,[\tau/\alpha]))^\circ \\
&= \underline{\lambda} x.\underline{\angle} i_\beta.x \triangleleft (\underline{\lambda} z.i_\beta \triangleright ((\phi\,[\mathbf{1}/!\alpha]\,[\tau/\alpha])^\circ \triangleright z)) \\
\text{(inductive hypothesis)} \quad &= \underline{\lambda} x.\underline{\angle} i_\beta.x \triangleleft (\underline{\lambda} z.i_\beta \triangleright ((\phi^\circ\,[\underline{\lambda} z.z/i_\alpha]) \triangleright z)) \\
&= (\underline{\lambda} x.\underline{\angle} i_\beta.x \triangleleft (\underline{\lambda} z.i_\beta \triangleright (\phi^\circ \triangleright z)))\,[\underline{\lambda} z.z/i_\alpha] \\
&= (\forall(\geq \phi))^\circ\,[\underline{\lambda} z.z/i_\alpha]\,.
\end{aligned}$$

- $A = \forall(\beta \geq)\phi$: we have (supposing $\beta \notin \mathrm{ftv}(\tau) \cup \{\alpha\}$):

$$\begin{aligned}
((\forall(\beta \geq)\phi)\,[\mathbf{1}/!\alpha]\,[\tau/\alpha])^\circ &= (\forall(\beta \geq)\phi\,[\mathbf{1}/!\alpha]\,[\tau/\alpha])^\circ\\
&= \underline{\lambda} z.i_\beta.(\phi\,[\mathbf{1}/!\alpha]\,[\tau/\alpha])^\circ \triangleright (x \triangleleft i_\beta)\\
\text{(inductive hypothesis)} \quad &= \underline{\lambda} z.i_\beta.(\phi^\circ\,[\underline{\lambda} z.z/i_\alpha]) \triangleright (x \triangleleft i_\beta)\\
&= (\underline{\lambda} z.i_\beta.\phi^\circ \triangleright (x \triangleleft i_\beta))\,[\underline{\lambda} z.z/i_\alpha]\\
&= (\forall(\beta \geq)\phi)^\circ\,[\underline{\lambda} z.z/i_\alpha]\,.
\end{aligned}$$

- $A = \parr$: we have $(\parr\,[\mathbf{1}/!\alpha]\,[\tau/\alpha])^\circ = \parr^\circ = \underline{\lambda} x.\underline{\measuredangle} i_\beta.x = \parr^\circ\,[\underline{\lambda} z.z/i_\alpha]\,.$

- $A = \&$: we have $(\&\,[\mathbf{1}/!\alpha]\,[\tau/\alpha])^\circ = \&^\circ = \underline{\lambda} x.x \triangleleft \underline{\lambda} y.y = \&^\circ\,[\underline{\lambda} z.z/i_\alpha]\,.$

- $A = \phi;\psi$: we have

$$\begin{aligned}
((\phi;\psi)\,[\mathbf{1}/!\alpha]\,[\tau/\alpha])^\circ &= (\phi\,[\mathbf{1}/!\alpha]\,[\tau/\alpha]\,;\psi\,[\mathbf{1}/!\alpha]\,[\tau/\alpha])^\circ\\
&= \underline{\lambda} x.(\psi\,[\mathbf{1}/!\alpha]\,[\tau/\alpha])^\circ \triangleright ((\phi\,[\mathbf{1}/!\alpha]\,[\tau/\alpha])^\circ \triangleright x)\\
\text{(inductive hypothesis)} \quad &= \underline{\lambda} x.(\psi^\circ\,[\underline{\lambda} z.z/i_\alpha]) \triangleright ((\phi^\circ\,[\underline{\lambda} z.z/i_\alpha]) \triangleright x)\\
&= (\underline{\lambda} x.\psi^\circ \triangleright (\phi^\circ \triangleright x))\,[\underline{\lambda} z.z/i_\alpha]\\
&= (\phi;\psi)^\circ\,[\underline{\lambda} z.z/i_\alpha]\,.
\end{aligned}$$

- $A = \mathbf{1}$: we have $(\mathbf{1}\,[\mathbf{1}/!\alpha]\,[\tau/\alpha])^\circ = \mathbf{1}^\circ = \underline{\lambda} x.x = \mathbf{1}^\circ\,[\underline{\lambda} z.z/i_\alpha]$.

For (iii), once again, the inductive steps where A is a term are immediate. Otherwise:

- $A = \sigma$: we have $(\sigma\,[\phi;!\alpha/!\alpha])^\circ = \sigma^\circ = (\underline{\lambda} x.x)\,[(\underline{\lambda} z.i_\alpha \triangleright (\phi^\circ \triangleright z))/i_\alpha] = \sigma^\circ\,[(\underline{\lambda} z.i_\alpha \triangleright (\phi^\circ \triangleright z))/i_\alpha]$.

- $A = !\alpha$: we have

$$\begin{aligned}
(!\alpha\,[\phi;!\alpha/!\alpha])^\circ &= (\phi;!\alpha)^\circ\\
&= \underline{\lambda} z.i_\alpha \triangleright (\phi^\circ \triangleright z)\\
&= i_\alpha\,[\underline{\lambda} z.i_\alpha \triangleright (\phi^\circ \triangleright z)/i_\alpha]\\
&= (!\alpha)^\circ\,[\underline{\lambda} z.i_\alpha \triangleright (\phi^\circ \triangleright z)/i_\alpha]\,.
\end{aligned}$$

- $A = \forall(\geq \phi)$: we have

$$\begin{aligned}
(\forall(\geq \phi)\,[\phi;!\alpha/!\alpha])^\circ &= (\forall(\geq \phi\,[\phi;!\alpha/!\alpha]))^\circ\\
&= \underline{\lambda} x.\underline{\measuredangle} i_\beta.x \triangleleft (\underline{\lambda} z.i_\beta \triangleright ((\phi\,[\phi;!\alpha/!\alpha])^\circ \triangleright z))\\
\text{(ind. hyp.)} &= \underline{\lambda} x.\underline{\measuredangle} i_\beta.x \triangleleft (\underline{\lambda} z.i_\beta \triangleright ((\phi^\circ\,[\underline{\lambda} z.i_\alpha \triangleright (\phi^\circ \triangleright z)/i_\alpha]) \triangleright z))\\
&= (\underline{\lambda} x.\underline{\measuredangle} i_\beta.x \triangleleft (\underline{\lambda} z.i_\beta \triangleright (\phi^\circ \triangleright z)))\,[\underline{\lambda} z.i_\alpha \triangleright (\phi^\circ \triangleright z)/i_\alpha]\\
&= (\forall(\geq \phi))^\circ\,[\underline{\lambda} z.i_\alpha \triangleright (\phi^\circ \triangleright z)/i_\alpha]\,.
\end{aligned}$$

- $A = \forall(\beta \geq)\phi$: we have (with $\beta \notin \mathrm{ftv}(\phi) \cup \{\alpha\}$)

$$\begin{aligned}
((\forall(\beta \geq)\phi)\,[\phi;!\alpha/!\alpha])^\circ &= (\forall(\beta \geq)\phi\,[\phi;!\alpha/!\alpha])^\circ\\
&= \underline{\lambda} z.i_\beta.(\phi\,[\phi;!\alpha/!\alpha])^\circ \triangleright (x \triangleleft i_\beta)\\
\text{(ind. hyp.)} &= \underline{\lambda} z.i_\beta.(\phi^\circ\,[\underline{\lambda} z.i_\alpha \triangleright (\phi^\circ \triangleright z)/i_\alpha]) \triangleright (x \triangleleft i_\beta)\\
&= (\underline{\lambda} z.i_\beta.\phi^\circ \triangleright (x \triangleleft i_\beta))\,[\underline{\lambda} z.i_\alpha \triangleright (\phi^\circ \triangleright z)/i_\alpha]\\
&= (\forall(\beta \geq)\phi)^\circ\,[\underline{\lambda} z.i_\alpha \triangleright (\phi^\circ \triangleright z)/i_\alpha]\,.
\end{aligned}$$

- $A = \parr$: $(\parr\,[\phi; !\alpha/!\alpha])^\circ = \parr^\circ = \underline{\lambda}x.\underline{\reflectbox{λ}}i_\beta.x = \parr^\circ\,[\underline{\lambda}z.i_\alpha \triangleright (\phi^\circ \triangleright z)/i_\alpha]\,.$
- $A = \&$: we have $(\&\,[\phi; !\alpha/!\alpha])^\circ = \underline{\lambda}x.x \triangleleft \underline{\lambda}y.y = \&^\circ\,[\underline{\lambda}z.i_\alpha \triangleright (\phi^\circ \triangleright z)/i_\alpha]\,.$
- $A = \phi; \psi$: we have

$$\begin{aligned}
&((\phi;\psi) && [\phi; !\alpha/!\alpha])^\circ \\
& && = (\phi\,[\phi; !\alpha/!\alpha]\,; \psi\,[\phi; !\alpha/!\alpha])^\circ \\
& && = \underline{\lambda}x.(\psi\,[\phi; !\alpha/!\alpha])^\circ \triangleright ((\phi\,[\phi; !\alpha/!\alpha])^\circ \triangleright x) \\
&\text{(ind. hyp.)} && = \underline{\lambda}x.(\psi^\circ\,[\underline{\lambda}z.i_\alpha \triangleright (\phi^\circ \triangleright z)/i_\alpha]) \triangleright ((\phi^\circ\,[\underline{\lambda}z.i_\alpha \triangleright (\phi^\circ \triangleright z)/i_\alpha]) \triangleright x) \\
& && = (\underline{\lambda}x.\psi^\circ \triangleright (\phi^\circ \triangleright x))\,[\underline{\lambda}z.i_\alpha \triangleright (\phi^\circ \triangleright z)/i_\alpha] \\
& && = (\phi;\psi)^\circ\,[\underline{\lambda}z.i_\alpha \triangleright (\phi^\circ \triangleright z)/i_\alpha]\,.
\end{aligned}$$

- $A = \mathbf{1}$: we have $(\mathbf{1}\,[\phi; !\alpha/!\alpha])^\circ = \mathbf{1}^\circ = \underline{\lambda}x.x = \mathbf{1}^\circ\,[\underline{\lambda}z.i_\alpha \triangleright (\phi^\circ \triangleright z)/i_\alpha]$. □