A Generic Normalisation Proof for Pure Type Systems

Paul-André Melliès
paulm@dcs.ed.ac.uk

Benjamin Werner
benjamin.werner@inria.fr

September 1, 1996

Abstract

We prove the strong normalisation for any PTS, provided the existence of a certain Λ-set $\mathfrak{A}^{\Uparrow}(s)$ for every sort s of the system. The properties verified by the $\mathfrak{A}^{\Uparrow}(s)$'s depend of the axiom and rules of the type system.

1 Introduction

1.1 Brief History

This work is an attempt to deal with the structure of complex Type Theories. Historically, once Girard had transposed the Burali-Forti paradox to type theory, Martin-Lof replied by suppressing the guilty Type : Type rule and remediated to the resulting loss of expressiveness by introducing a new concept of stratified *universes* [10]. Today this notion can be found, in different forms and variants, in most Type Theories, especially the ones with foundational ambitions. For example, it appears in the theories used in actually implemented proof-checkers (NuPRL, Coq, Lego...).

The main idea is that all types are no longer equal. Each one inhabits a certain *universe* (Martin-Lof) or *sort* (Pure Type Systems). In general, universes are embedded in each other following a monotone hierarchy. The key point is that quantification inside a given type is restricted to types of the same (or smaller) universes[1].

Since, this episode has often been presented as part of a long-going predicative vs. non-predicative debate. It however had another consequence for type theories viewed as practical and actually usable logical formalisms: The fact that all types are no longer equal puzzles the newcomer and makes it more difficult to grasp the underlying intuitions of the formalisms. This may become particularly acute when types are used as propositions: for some formalisms, depending upon in which universe it is done, proving "there exists an element x of type A" will not have the same meaning, i.e. we may or may not exhibit a constructive witness.

More generally, lots of very technical choices have to be made; in particular:

- Concerning the theory itself: as mentioned above, and would it be only for pragmatic reasons, most up-to-date type theories are build on top of a more or less complex structure defining the interactions between the different kinds of types. The corresponding rules are however almost always, if slightly, different from one theory to another. No current mathematical tools deal with the study of these structures and are thus likely to provide objective comparison criterions.

[1] With the exception of the impredicative universe when there is one; but even then, elimination has to be restricted for the existential quantifier.

- When formalizing a piece of mathematics in such a theory, one has to decide at which level the objects, respectively the propositions, of the work to be formalized have to be put. There is, for now, no canonical way of deciding this, and this choice will depend upon the way the objects are going to be used. Schematizing, we might say that if every piece of known mathematics seems to be, more or less, formalizable in a powerful type theory, there is no uniform and canonical way of doing so since it requires non-trivial choices to be made concerning the status of its objects. From the outsider's point of view, these choices often have to be made be a Type Theory wizard.

For these reasons, the world of Type Theories might, at first glance, bear some similitude with the late Ptolemeic astronomy. We hope to demonstrate that what seems to be chaotic actually yields some order and structure[2].

1.2 Why Pure Type systems ?

In the process of studying the structure of type theories, a first clarification attempt has been the introduction of *Pure Type Systems* (PTSs). The concept is due to Terlouw and Berardi and largely owes its fame to Henk Barendregt.

We refer to the bibliography [2] and to the definitions below for more details. The formalisms of PTSs allows to describe a wide range of λ-calculi like simple types, F, F_ω, the Calculus of Constructions, but also non-normalizable systems, especially Girard's system U or Martin-Lof's Type:Type. Until now, with the notable exception of Terlouw's work [12], the only properties proved on large classes of PTSs were of combinatorial nature (confluence, subject reduction) and did not deal with normalization and its counterpart, logical consistency.

The techniques presented in the present work do apply to extensions of Pure Type Systems (inductive types...). Since our main aim was to confront with complex structures, a generic study of PTSs was the natural first step.

1.3 About this paper

Technically, the main difficulty, when trying to build up a generic normalization proof for PTSs, is that syntactically similar operations (abstraction, application) have to be interpreted in different ways, depending upon the sort in which they are performed: whereas basic types are always treated like in Girard's original work [6], functions from types to types (object of type $* \to *$ in F_ω) have to be seen as extensional functions mapping sets of terms to sets of terms. Thus the homogeneity of the syntax is lost.

An answer was proposed by Altenkirch [1] with the introduction of Λ-sets. These are ω-sets [8] modified for normalization proofs. The advantage is that if types are interpreted by Λ-sets, function types can be treated in a fully generic way.

What is done in the present work is therefore merely the next step: we axiomatize, for every PTS, the properties of a structure of Λ-sets (sect. 4), which allows the carrying through of a generic normalization proof (sect. 5). The existence of such a structure is therefore a sufficient condition for strong normalization. We construct such structures for well-known PTSs like F, CC, ECC (sect. 6). In other words, we specify a particular model of type systems, whose existence is sufficient for strong normalization. A difference with [12] is that the specification of the model directly reflects the structure (i.e. sorts, axioms and rules) of the PTS.

[2]This was originally *not* suposed to be a quotation of Jean-Yves Girard.

2 Definition

In the whole paper, we will consider a single pure type system, described by a *set of sorts* $\mathcal{S}$, a set of *axioms* $\mathcal{A} \subset \mathcal{S} \times \mathcal{S}$ and a set of *rules* $\mathcal{R} \subset \mathcal{S} \times \mathcal{S} \times \mathcal{S}$.

We give ourselves a countable set $\mathcal{V}$ of variables (generally denoted by $x, y, \ldots$).

In the meta-theoretic study hereafter, we will consider a variant of the usual presentation of Pure Type Systems: the terms will carry more type information than usual in the cases of λ-abstraction and application. This approach can be seen as related to the labeled terms used in [4]. However, here, we will use these labels to restrict the usual formulation of β-reduction, see [1, 3]. In section 7, we will verify that, provided the strong normalization property holds, our definition of PTS's is equivalent to the usual ones, and hence strong normalization itself is inherited by the "unlabeled" PTS.

Definition 1 *A term is described by*

$$M \quad := \quad x \mid s \mid \mathtt{app}_{x:M.M}(M, M) \mid \lambda_{x:M.M} x.M \mid (x : M)M.$$

The set of terms is written $\mathcal{T}$. A context (Γ) is a list of pairs $(x : A) \in \mathcal{V} \times \mathcal{T}$, $[]$ being the empty context.

The letters $M, N, A, B, C, T, U, V, t, u, v$, etc will be used to denote terms, greek capitals Γ, Δ for contexts and a, b, c, x, y, z for variables.

Term conversion will here be taken care of by the following reduction, due to Torsten Altenkirch:

Definition 2 (tight reduction) *We define $\triangleright_\beta$ as the contextual closure of:*

$$\mathtt{app}_{y:A.B}((\lambda_{y:A.B} x.M), N) \triangleright_\beta M[x \setminus N]$$

As usual, we will write $\triangleright_\beta^+$ (respectively $\triangleright_\beta^*$, $=_\beta$) for the transitive (respectively transitive-reflexive, symmetric-transitive-reflexive) closure of $\triangleright_\beta$.

Remark The tight-reduction does *not* enjoy the Church-Rosser property on non well-typed terms. We do not give the proof, but it is quite easy to adapt the counter examples for confluence for λ-calculi with surjective pairing. See [7] for details. Of course, Church-Rosser will hold for terms well-typed in a strongly normalizing PTS.

Definition 3 (Strong Normalization) *A term t is said to be strongly normalizing if and only if there is no infinite sequence of reductions starting from t.*

The typing rules

We use two kind of judgements: $\vdash \Gamma \;\; wf$ expresses that the context Γ is well-formed, $\Gamma \vdash t : T$ that the term t is of type T in the context Γ. The set of *derivable judgements* is inductively defined by the following inference rules:

(Start)	$\vdash [] \;\; wf$	
(Axiom)	$\dfrac{\vdash \Gamma \;\; wf}{\Gamma \vdash s_1 : s_2}$	if $(s_1, s_2) \in \mathcal{A}$
(Weak)	$\dfrac{\Gamma \vdash A : s}{\vdash \Gamma, x : A \;\; wf}$	
(Var)	$\dfrac{\vdash \Gamma, x : A, \Gamma' \;\; wf}{\Gamma, x : A, \Gamma' \vdash x : A}$	if $\mathsf{binder}(\Gamma') \cap \mathsf{free}(\mathsf{A}) = \emptyset$
(Prod)	$\dfrac{\Gamma \vdash A : s_1 \Gamma, x : A \vdash B : s_2}{\Gamma \vdash (x : A)B : s_3}$	if $(s_1, s_2, s_3) \in \mathcal{R}$
(Lambda)	$\dfrac{\Gamma, x : A \vdash M : B \Gamma \vdash (x : A)B : s}{\Gamma \vdash \lambda_{x:A.B} x.M : (x : A)B}$	
(App)	$\dfrac{\Gamma \vdash M : (x : A)B \Gamma \vdash N : A}{\Gamma \vdash \mathtt{app}_{x:A.B}(M, N) : B[x \setminus N]}$	
(Conv)	$\dfrac{\Gamma \vdash M : A \Gamma \vdash B : s A \rhd_\beta^* B \text{ or } B \rhd_\beta^* A}{\Gamma \vdash M : B}$	

Remark We consider that each judgement represents an α-conversion class: for instance, $x : s \vdash x : s$ and $y : s \vdash y : s$ should be considered as two α-equivalent judgements. The judgement $\Gamma \vdash \lambda_{x:A.B} x.M : (x : A)B$ obtained with the rule (Lambda) is also equivalent to $\Gamma \vdash \lambda_{x:A.B} x.M : (y : A)B'$ or $\Gamma \vdash \lambda_{y:A.B'} x.M : (x : A)B$ where $B' = B[x \setminus y]$ and y is not free in B.

We can now state some elementary syntactic results. The proofs are quite similar to their counter-parts for usual PTSs and they are often simplified by the presence of labels. We therefore do not detail the proofs; actually, all the following lemmas are proved by inductoin over the structure of the corresponding derivation. For matters of space, we also only state the results which will be necessary in the rest of the paper.

Lemma 1 (Free Variables) *Given any derivable judgement $\Gamma \vdash t : T$, every free variable of t or T is bound in Γ.*

Lemma 2 (Subterms) *Any subterm of any derivable judgement is well-formed.*

Lemma 3 (Substitution) *Given the two following derivable judgements:*

$$\Gamma, x : A, \Delta \vdash t : T \qquad \textit{and} \qquad \Gamma \vdash u : A$$

there exists a derivation of:

$$\Gamma, \Delta[x \setminus u] \vdash t[x \setminus u] : T[x \setminus u].$$

Provided, of course there is no other binding occurrence of x in Δ; in this case, we have:

$$\Gamma, \Delta[x \setminus u] \vdash t : T.$$

Lemma 4 (Weakening) *Given the two following derivable judgements* $\Gamma, \Delta \vdash t : T$ *and* $\Gamma \vdash A : s$*, there exists a derivation of* $\Gamma, x : A, \Delta \vdash t : T$ *for any variable* x *which is not free in* Δ*,* t *and* T*.*

Lemma 5 (Subject Reduction) *Let* $\Gamma \vdash t : T$ *be a derivable judgement. If* $t \triangleright_\beta t'$ *and* $\Gamma \triangleright_\beta \Gamma'$*, then the two following judgements are derivable:*

$$\Gamma \vdash t' : T \qquad \textit{and} \qquad \Gamma' \vdash t : T.$$

3 Structures for the interpretation

3.1 Λ-sets

As mentioned before, one of the main steps of this work will be to interpret each type of the system by a Λ-set. This section is devoted to the definition of this notion, and is therefore largely inspired by the work of Altenkirch [1].

Definition 4 (Atomic terms) *A term is said to be atomic if it is of the form*

$$\mathtt{app}_{x_n:A_n.B_n}(\ldots(\mathtt{app}_{x_1:A_1.B_1}(P, Q_1), \ldots, Q_n)$$

with P *of one of the following forms:* s*,* x*,* $(x : A)B$*. We write* $\mathcal{AT}$ *for the set of atomic terms.*

The following is essentially Tait's (and Krivine's and other's) [11, 5] version of reducibility candidates [6].

Definition 5 (Saturated sets) *A set* $\mathcal{C}$ *of terms is said to be saturated, if and only if*

1. $\mathcal{C} \subset \mathcal{SN}$
2. $(\mathcal{SN} \cap \mathcal{AT}) \subset \mathcal{C}$
3. *if* $(A, B, P) \in \mathcal{SN}^3$ *and*

$$\mathtt{app}_{x_n:A_n.B_n}(\ldots(\mathtt{app}_{x_1:A_1.B_1}(M[x \setminus P], Q_1), \ldots, Q_n) \in \mathcal{C}$$

then

$$\mathtt{app}_{x_n:A_n.B_n}(\ldots(\mathtt{app}_{x_1:A_1.B_1}(\mathtt{app}_{x:A.B}(\lambda_{x:A.B}x.M, P), Q_1), \ldots, Q_n) \in \mathcal{C}$$

Definition 6 (Λ-set) *A* Λ*-set is a couple* $(X_0, \models)$*, where*

- X_0 *is some set,*
- *and* $\models$ *a relation between* X_0 *and the set of terms:* $\models \subset X_0 \times \mathcal{T}$*.*

The elements of X_0 *are called the* carriers *of* X *and* X_0 *is the* carrier-set*. The terms* M *such that* $M \models_X \alpha$ *for some* $\alpha \in X_0$ *are called the* realizers *of* α *(or more generally the realizers of* X*).*

Another way to view a Λ-set is that it is a family of sets of terms indexed over X_0.

Notation If X is a Λ-set, we write X_0 for its first component and $\models_X$ for the second.

Definition 7 (saturated Λ-set) *A* Λ*-set* X *is said to be* saturated *if and only if:*

1. *Every realizer is strongly normalizable.*

2. *There is one element of X_0 which is realized by any atomic strongly normalizable term.*

3. *For every $\alpha \in X_0$, the set of realizers of α is closed by reverse head β-expansion, i.e. verifies the condition 3 of definition 5:*

$$\forall (A,B,P) \in \mathcal{SN} \ . \ \mathtt{app}_{x_n:A_n.B_n}(\ldots(\mathtt{app}_{x_1:A_1.B_1}(M[x \setminus P], Q_1), \ldots, Q_n) \models_X \alpha \Longrightarrow$$
$$\mathtt{app}_{x_n:A_n.B_n}(\ldots(\mathtt{app}_{x_1:A_1.B_1}(\mathtt{app}_{x:A.B}(\lambda_{x:A.B}x.M, P), Q_1), \ldots, Q_n) \models_X \alpha.$$

Remark If a Λ-set is saturated, the set of its realizers is a saturated set.

This means we can also see a saturated Λ-set as a saturated set of terms with some additional information given by the carriers.

Notation Let X be a Λ-set. We write $x \sqsubset X$ for $x \in X_0$.

Definition 8 (Λ-morphism) *Let X and Y be two Λ-sets. A morphism p from X to Y is a function $p : X_0 \to Y_0$ such that $M \models_X f \Longrightarrow M \models_Y p(f)$.*

Definition 9 (Λ-isos) *Let X and Y be two Λ-sets. An Λ-iso p from X to Y is a one-to-one function $p : X_0 \to Y_0$ such that $M \models_X f \iff M \models_Y p(f)$.*

3.2 $\mathfrak{C}$-sets

A usual difficulty when building a model of a typed λ-calculus is to restrict the size of the function spaces, in order not to "get lost in a sea of set-theoretic functions" (Girard). One radical possibility is to assume the existence of inaccessible cardinals; here, we prefer to avoid this by defining a finer structure on our Λ-sets using adapted equivalence relations. The underlying idea should appear more clearly in the next sections. For a first reading, it is possible to forget about the details of these relations.

Hereafter we give ourselves a fixed set $\mathfrak{C}$ which will index the equivalence relations.

Definition 10 ($\mathfrak{C}$-set) *An $\mathfrak{C}$-set $\mathfrak{A}$ is a set of Λ-sets which, for every $i \in \mathfrak{C}$, is enriched with:*

1. *an equivalence relation $\left\| \begin{smallmatrix} i \\ \mathfrak{A} \end{smallmatrix} \right\|$ over $\mathfrak{A}$,*

2. *an equivalence relation $\left| \begin{smallmatrix} i \\ \mathfrak{A} \end{smallmatrix} \right|$ over $\bigcup_{X \in \mathfrak{A}} X_0$ (i.e. a relation between the carriers α of elements of $\mathfrak{A}$).*

Definition 11 (product) *Let $\mathfrak{A}_1$ and $\mathfrak{A}_2$ be two $\mathfrak{C}$-sets. Let X be a Λ-set element of $\mathfrak{A}_1$, and $Y \equiv (Y_\alpha)_{\alpha \in X_0}$ a family of Λ-sets elements of $\mathfrak{A}_2$ (and indexed over X_0). We define the Λ-set $\Pi(X,Y)$ by:*

$$\Pi(X,Y)_0 \quad \equiv \quad \{f \in \Pi_{\alpha \in X_0}(Y_\alpha)_0 \mid \forall \alpha, \alpha' \in X_0, \forall i \in \mathfrak{C}, \alpha \left| \begin{smallmatrix} i \\ \mathfrak{A}_1 \end{smallmatrix} \right| \alpha' \Longrightarrow f(\alpha) \left| \begin{smallmatrix} i \\ \mathfrak{A}_2 \end{smallmatrix} \right| f(\alpha')\}$$

$$M \models_{\Pi(X,Y)} f \iff \forall \alpha \in X_0, \ \forall N \models_X \alpha \ . \ \forall A, B \in \mathcal{SN} \ . \ \forall x \in \mathcal{V} \ . \ \mathtt{app}_{x:A.B}(M,N) \models_{Y_\alpha} f(\alpha)$$

Lemma 6 *If X and every Y_x is saturated, then so is $\Pi(X,Y)$.*

PROOF We separate the proofs of the three conditions:

1. If $M \models_{\Pi(X,Y)} f$, we know there exists $\alpha \sqsubset X$ such that (for example) $x \models_X \alpha$. Thus $\mathtt{app}_{x:x.x}(M,x) \models_{Y_\alpha} f(\alpha)$ which implies that M is strongly normalizable.

2. For any $\alpha \sqsubset X$, we know there exists a carrier $\underline{Y_\alpha}$ of Y_α which is realized by any atomic strongly normalizable term. We define f as the function which to any $\alpha \sqsubset X$ associates Y_α. Since $\left|\begin{matrix} i \\ \mathfrak{A}_1 \end{matrix}\right|$ and $\left|\begin{matrix} i \\ \mathfrak{A}_2 \end{matrix}\right|$ are equivalence relations, it is easy to check that $f \sqsubset \Pi(X, Y)$. Now let M be a strongly normalizable atomic term; we have
$$\forall \alpha \sqsubset X \ .\ \forall N \models_X \alpha \ .\ \forall A, B \in \mathcal{SN} \ .\ \mathtt{app}_{x:A.B}(M, N) \in \mathcal{SN} \cap \mathcal{AT}$$
and hence
$$\mathtt{app}_{x:A.B}(M, N) \models_{Y_\alpha} \underline{Y_\alpha}.$$
Which is sufficient for $M \models_{\Pi(X,Y)} f$.
3. The proof is easy and simillar to its counterpart for saturated sets. See [1, 5] for example. ∎

Definition 12 ($\mathfrak{E}$-relation product) *Let $\mathfrak{A}_1$ and $\mathfrak{A}_2$ be two $\mathfrak{E}$-set. Let there be elements X and X' of $\mathfrak{A}_1$, and two families $(Y_\alpha)_{\alpha \in X_0}$ and $(Y'_{\alpha'})_{\alpha' \in X'_0}$ of Λ-sets elements of $\mathfrak{A}_2$ indexed over X_0 and X'_0. The following definitions extend the $\left\|\begin{matrix} i \\ \mathfrak{A} \end{matrix}\right\|$ and $\left|\begin{matrix} i \\ \mathfrak{A} \end{matrix}\right|$ to $\Pi(X, Y)$ and $\Pi(X', Y')$, for $i \in \mathfrak{E}$:*

1. $$\Pi(X,Y) \left\|\begin{matrix} i \\ \Pi(\mathfrak{A}_1, \mathfrak{A}_2) \end{matrix}\right\| \Pi(X', Y') \quad \Leftrightarrow \quad \begin{cases} X \left\|\begin{matrix} i \\ \mathfrak{A}_1 \end{matrix}\right\| X' \text{ and} \\ \forall \alpha \sqsubset X, \forall \alpha' \sqsubset X', \alpha \left|\begin{matrix} i \\ \mathfrak{A}_1 \end{matrix}\right| \alpha' \ \Rightarrow \ Y_\alpha \left\|\begin{matrix} i \\ \mathfrak{A}_2 \end{matrix}\right\| Y'_\alpha \end{cases}$$
2. *when* $\Pi(X,Y) \left\|\begin{matrix} i \\ \Pi(\mathfrak{A}_1, \mathfrak{A}_2) \end{matrix}\right\| \Pi(X', Y')$, *the relation* $\left|\begin{matrix} i \\ \Pi(\mathfrak{A}_1, \mathfrak{A}_2) \end{matrix}\right|$ *can be defined as:*
$$f \left|\begin{matrix} i \\ \Pi(\mathfrak{A}_1, \mathfrak{A}_2) \end{matrix}\right| g \Leftrightarrow \quad (\forall \alpha \sqsubset X, \forall \alpha' \sqsubset X', \alpha \left|\begin{matrix} i \\ \mathfrak{A}_1 \end{matrix}\right| \alpha' \Rightarrow f(\alpha) \left|\begin{matrix} i \\ \mathfrak{A}_2 \end{matrix}\right| g(\alpha'))$$

Note that the relations $\left\|\begin{matrix} i \\ \Pi(\mathfrak{A}_1, \mathfrak{A}_2) \end{matrix}\right\|$ and $\left|\begin{matrix} i \\ \Pi(\mathfrak{A}_1, \mathfrak{A}_2) \end{matrix}\right|$ are not expected to live in any $\mathfrak{E}$-set $\Pi(\mathfrak{A}_1, \mathfrak{A}_2)$.

4 The universes of the interpretations

This is the key of the proof. We suppose that for every sort s, there exists an $\mathfrak{E}$-set $\mathfrak{A}^{\Uparrow}(s)$ and a saturated Λ-set $\mathfrak{A}_{\Downarrow}(s)$. We shall construct in $\mathfrak{A}^{\Uparrow}(s)$ the interpretation of types A of sort s ; and in $\mathfrak{A}_{\Downarrow}(s)$ the interpretation of terms M of type s. One notable difficulty is that a type A of sort s is at the same time a term A of type s (and vice-versa). Thus, for every sort s we suppose the existence of two one-to-one mappings $\Downarrow_s \colon \mathfrak{A}^{\Uparrow}(s) \to \mathfrak{A}_{\Downarrow}(s)_0$ and $\Uparrow_s \colon \mathfrak{A}_{\Downarrow}(s)_0 \to \mathfrak{A}^{\Uparrow}(s)$ such that:
$$\Uparrow_s \circ \Downarrow_s = Id_{\mathfrak{A}^{\Uparrow}(s)} \qquad \Downarrow_s \circ \Uparrow_s = Id_{\mathfrak{A}_{\Downarrow}(s)_0}$$
In fact, if α is the "type" interpretation of $\Gamma \vdash A$ in $\mathfrak{A}^{\Uparrow}(s)$ then $\Downarrow_s \langle a \rangle$ is its "term" interpretation in $\mathfrak{A}_{\Downarrow}(s)$. In the other direction, the "term" interpretation μ of $\Gamma \vdash M$ in $\mathfrak{A}_{\Downarrow}(s)$ can be lifted to its "type" interpretation $\Uparrow_s \langle \mu \rangle$ in $\mathfrak{A}^{\Uparrow}(s)$. The two equations above imply that the lift and unlift operations are revertible:
$$\Uparrow_s \langle \Downarrow_s \langle \alpha \rangle \rangle = \alpha \text{ and } \Downarrow_s \langle \Uparrow_s \langle \mu \rangle \rangle = \mu$$

In all the literature, the two denotational universes $\mathfrak{A}^{\Uparrow}(s)$ and $\mathfrak{A}_{\Downarrow}(s)$ are identified to a unique $\mathfrak{A}(s)$, with $\Downarrow_s = \Uparrow_s = Id_{\mathfrak{A}(s)}$. Our forthcoming interpretation of derivations shows that the distinction we introduce is natural — moreover it shall play an important role in circular Pure Type Systems.

The structure of the PTS is reflected in the fact that $\mathfrak{A}^{\Uparrow}(s)$, $\mathfrak{A}_{\Downarrow}(s)$, $\Downarrow_s$ and $\Uparrow_s$ shall verify the conditions described below.

Condition 1 (hierarchy of universe) *We require that for any sort s, $\mathfrak{A}^{\Uparrow}(s)$ and $\mathfrak{A}_{\Downarrow}(s)$ verify the following conditions:*

1. *The elements of $\mathfrak{A}^{\Uparrow}(s)$ are* saturated *Λ-sets; every carrier of $\mathfrak{A}_{\Downarrow}(s)$ is realized by any strongly normalizing term.*
2. *If $(s_1, s_2) \in \mathcal{A}$, then*
$$\mathfrak{A}_{\Downarrow}(s_1) \in \mathfrak{A}^{\Uparrow}(s_2).$$
3. *If $(s_1, s_2, s_3) \in \mathcal{R}$, then let there be $X \in \mathfrak{A}^{\Uparrow}(s_1)$ and a family $(Y_\alpha)_{\alpha \in X_0}$ with $Y_\alpha \in \mathfrak{A}^{\Uparrow}(s_2)$ such that:*
$$\forall (\alpha, \alpha') \in X_0^2 . \forall i \in \mathfrak{C} . \alpha \left| \begin{array}{c} i \\ \mathfrak{A}^{\Uparrow}(s_1) \end{array} \right| \alpha' \Longrightarrow Y_\alpha \left\| \begin{array}{c} i \\ \mathfrak{A}^{\Uparrow}(s_2) \end{array} \right\| Y_{\alpha'}$$
there exists a Λ-iso $\downarrow_{\Pi(X,Y)}$ from $\Pi(X,Y)$ to an element $\Pi_{\downarrow}(X,Y) \in \mathfrak{A}^{\Uparrow}(s_3)$:
$$\downarrow_{\Pi(X,Y)} : \Pi(X,Y) \to \Pi_{\downarrow}(X,Y) \in \mathfrak{A}^{\Uparrow}(s_3).$$

We ask here that $\Pi_{\downarrow}(X,Y)$ and $\downarrow_{\Pi(X,Y)}$ do not depend on (s_1, s_2, s_3). However a quick look at the definition of products 11 shows that the construction $\Pi(X,Y)$ depends on the equivalence relations $\left| \begin{array}{c} i \\ \mathfrak{A}^{\Uparrow}(s_1) \end{array} \right|$ and $\left| \begin{array}{c} i \\ \mathfrak{A}^{\Uparrow}(s_2) \end{array} \right|$. In order to ensure that the construction of $\Pi(X,Y)$ itself does not depend on the universes $\mathfrak{A}^{\Uparrow}(s_1)$ and $\mathfrak{A}^{\Uparrow}(s_2)$ we impose the following uniformity condition:

Condition 2 (uniformity of equivalence relations)

1. *if $X, X' \in \mathfrak{A}^{\Uparrow}(s_1)$ and $\mathfrak{A}_{\Downarrow}(s_1) \in \mathfrak{A}^{\Uparrow}(s_2)$ then*
$$\forall i \in \mathfrak{C}, \quad X \left\| \begin{array}{c} i \\ \mathfrak{A}^{\Uparrow}(s_1) \end{array} \right\| X' \Leftrightarrow \Downarrow_{s_1} \langle X \rangle \left| \begin{array}{c} i \\ \mathfrak{A}^{\Uparrow}(s_2) \end{array} \right| \Downarrow_{s_1} \langle X' \rangle$$
2. *if $\alpha \sqsubset X_1 \in \mathfrak{A}^{\Uparrow}(s_1)$, $\alpha' \sqsubset X_1' \in \mathfrak{A}^{\Uparrow}(s_1)$ and $\alpha \sqsubset X_2 \in \mathfrak{A}^{\Uparrow}(s_2)$, $\alpha' \sqsubset X_2' \in \mathfrak{A}^{\Uparrow}(s_2)$ then*
$$\forall i \in \mathfrak{C} : \quad \alpha \left| \begin{array}{c} i \\ \mathfrak{A}^{\Uparrow}(s_1) \end{array} \right| \alpha' \iff \alpha \left| \begin{array}{c} i \\ \mathfrak{A}^{\Uparrow}(s_2) \end{array} \right| \alpha'.$$

The required properties on the equivalence relations $\left\| \begin{array}{c} i \\ \mathfrak{A}^{\Uparrow}(s_3) \end{array} \right\|$ and $\left| \begin{array}{c} i \\ \mathfrak{A}^{\Uparrow}(s_3) \end{array} \right|$ in the case of a (collapsed) product construction are expressed by the following condition.

Condition 3 (collapsed products)
if $i \in \mathfrak{C}$ and $(s_1, s_2, s_3) \in \mathcal{R}$, then given any elements $X, X' \in \mathfrak{A}^{\Uparrow}(s_1)$ and $Y_\alpha, Y_{\alpha'} \in \mathfrak{A}^{\Uparrow}(s_2)$ respectively indexed by $\alpha \sqsubset X$ and $\alpha' \sqsubset X'$:

1. $$\Pi(X,Y) \left\| \begin{matrix} i \\ \Pi(\mathfrak{A}^{\Uparrow}(s_1),\mathfrak{A}^{\Uparrow}(s_2)) \end{matrix} \right\| \Pi(X',Y') \Longrightarrow \Pi_{\downarrow}(X,Y) \left\| \begin{matrix} i \\ \mathfrak{A}^{\Uparrow}(s_3) \end{matrix} \right\| \Pi_{\downarrow}(X',Y')$$

2. *if* $\Pi(X,Y) \left\| \begin{matrix} i \\ \Pi(\mathfrak{A}^{\Uparrow}(s_1),\mathfrak{A}^{\Uparrow}(s_2)) \end{matrix} \right\| \Pi(X',Y')$ *then* $f \sqsubset \Pi(X,Y)$ *and* $g \sqsubset \Pi(X',Y')$ *imply that:*
$$f \left| \begin{matrix} i \\ \Pi(\mathfrak{A}^{\Uparrow}(s_1),\mathfrak{A}^{\Uparrow}(s_2)) \end{matrix} \right| g \iff \downarrow_{\Pi(X,Y)} \langle f \rangle \left| \begin{matrix} i \\ \mathfrak{A}^{\Uparrow}(s_3) \end{matrix} \right| \downarrow_{\Pi(X',Y')} \langle g \rangle$$

The last condition tells that the lift and unlift procedures should not depend on the universe they proceed in.

Condition 4 (uniformity of lift/unlift procedures)
We require that the $\Downarrow_s$ *and the* $\Uparrow_s$ *verify the following conditions:*

1. *if* $\alpha \in \mathfrak{A}^{\Uparrow}(s)$ *and* $\alpha \in \mathfrak{A}^{\Uparrow}(s')$ *then* $\Downarrow_s \langle \alpha \rangle = \Downarrow_{s'} \langle \alpha \rangle$

2. *if* $\alpha \sqsubset \mathfrak{A}_{\Downarrow}(s)$ *and* $\alpha \sqsubset \mathfrak{A}_{\Downarrow}(s')$ *then* $\Uparrow_s \langle \alpha \rangle = \Uparrow_{s'} \langle \alpha \rangle$

Remark This means that instead of considering a the family of $\Uparrow_s$ isos (resp. $\Downarrow_s$), we might assume the existence of a single $\Uparrow \equiv \bigcup_{s \in \mathcal{S}} \Uparrow_s$ respectively $\Downarrow \equiv \bigcup_{s \in \mathcal{S}} \Downarrow_s$. In other words, the sort in $\Uparrow_s$, respectively $\Downarrow_s$, may simply be seen as an annotation.
We define for any Λ-iso $\downarrow_{\Pi(X,Y)}$ the inverse Λ-iso $\uparrow_{\Pi(X,Y)}$ such that $\uparrow_{\Pi(X,Y)} \circ \downarrow_{\Pi(X,Y)} = Id_{\Pi(X,Y)}$ and $\downarrow_{\Pi(X,Y)} \circ \uparrow_{\Pi(X,Y)} = Id_{\Pi_{\downarrow}(X,Y)}$.

5 The Interpretation

This section follows the usual pattern of reducibility proofs. For any derivable judgement, we will define an interpretation. Like in [1], the interpretation of a type will be a Λ-set and the interpretations of its terms will be carriers of this Λ-set. Strong normalization being assured by the fact that every well-typed term realizes its interpretation.

5.1 Definition

We will associate two interpretations $[\Gamma \vdash M]$ and $[\![\Gamma \vdash M]\!]$ to any judgement $\Gamma \vdash M : A$. We also associate an interpretation $[\![\Gamma]\!]$ to any well formed context Γ.

The construction is by structural induction on Γ and M:

Definition 13

$$
\begin{aligned}
[\![[]]\!] &\equiv \{\emptyset\} && (1)\\
[\![\Gamma, x : A]\!] &\equiv \{(\gamma,\alpha), \gamma \in [\![\Gamma]\!] \wedge \alpha \sqsubset [\![\Gamma \vdash A]\!](\gamma)\} && (2)\\
[\![\Gamma \vdash s]\!](\gamma) &\equiv \mathfrak{A}_{\Downarrow}(s) && (3)\\
[\![\Gamma \vdash (x:A)B]\!](\gamma) &\equiv \Pi_{\downarrow}([\![\Gamma \vdash A]\!](\gamma), [\![\Gamma, x : A \vdash B]\!](\gamma, \_)) && (4)\\
[\Gamma \vdash x_i](\gamma) &\equiv \gamma_i && (5)\\
[\Gamma \vdash \lambda_{x:A.B} x.M](\gamma) &\equiv \downarrow_{\Pi([\![\Gamma \vdash A]\!](\gamma), [\![\Gamma, x:A \vdash B]\!](\gamma,\_))} \langle [\Gamma, x : A \vdash M](\gamma, \_) \rangle && (6)\\
[\Gamma \vdash \mathtt{app}_{x:A.B}(M,N)](\gamma) &\equiv \uparrow_{\Pi([\![\Gamma \vdash A]\!](\gamma), [\![\Gamma, x:A \vdash B]\!](\gamma,\_))} \langle [\Gamma \vdash M](\gamma) \rangle \ ([\Gamma \vdash N](\gamma)) && (7)
\end{aligned}
$$

and for all the other cases:

$$
\begin{aligned}
[\![\Gamma \vdash A]\!](\gamma) &\equiv \Uparrow_s \langle [\Gamma \vdash A](\gamma) \rangle && (8)\\
[\Gamma \vdash A](\gamma) &\equiv \Downarrow_s \langle [\![\Gamma \vdash A]\!](\gamma) \rangle && (9)
\end{aligned}
$$

In the above, and the rest of the paper, $[\![\Gamma, x : A \vdash B]\!](\gamma, \_)$*, respectively* $[\Gamma, x : A \vdash M](\gamma, \_)$ *is a short-cut for the function*

$$\alpha \sqsubset [\![\Gamma \vdash A]\!](\gamma) \mapsto [\![\Gamma, x : A \vdash B]\!](\gamma, \alpha)$$

respectively

$$\alpha \sqsubset [\![\Gamma \vdash A]\!](\gamma) \mapsto [\Gamma, x : A \vdash M](\gamma, \alpha).$$

The definition is not total. We explicit the sufficient properties for each interpretation step:

- *for all cases but (1) we require that* $[\![\Gamma]\!]$ *is defined.*

(2) *both* $[\![\Gamma]\!]$ *and* $[\![\Gamma \vdash A]\!]$ *are defined and* $[\![\Gamma \vdash A]\!](\gamma)$ *there exists a sort* s *such that* $[\![\Gamma \vdash A]\!](\gamma) \in \mathfrak{A}^{\Uparrow}(s)$ *for any* $\gamma \in [\![\Gamma]\!]$.

(4,6 and 7) *there exist* $(s_1, s_2, s_3) \in \mathcal{R}$ *such that for any* $\gamma \in [\![\Gamma]\!]$*:*

- $[\![\Gamma \vdash A]\!](\gamma) \sqsubset \mathfrak{A}^{\Uparrow}(s_1)$
- $\forall \alpha \sqsubset [\![\Gamma \vdash A]\!](\gamma) \;.\; [\![\Gamma, x : A \vdash B]\!](\gamma, \alpha) \sqsubset \mathfrak{A}^{\Uparrow}(s_2)$
- $\forall i \in \mathfrak{E} \;.\; \forall (\alpha, \alpha') \in [\![\Gamma \vdash A]\!](\gamma)^2 \;.\; \alpha \left| \begin{matrix} i \\ \mathfrak{A}^{\Uparrow}(s_1) \end{matrix} \right| \alpha' \Longrightarrow$

$$[\![\Gamma, x : A \vdash B]\!](\gamma, \alpha) \left\| \begin{matrix} i \\ \mathfrak{A}^{\Uparrow}(s_2) \end{matrix} \right\| [\![\Gamma, x : A \vdash B]\!](\gamma, \alpha')$$

(6) *for any* $\gamma \in [\![\Gamma]\!]$*, for any* $\alpha \sqsubset [\![\Gamma \vdash A]\!](\gamma)$*,* $[\Gamma, x : A \vdash M](\gamma, \alpha)$ *is defined, and:*

$$(\alpha \sqsubset [\![\Gamma \vdash A]\!](\gamma) \mapsto [\Gamma, x : A \vdash M](\gamma, \alpha)) \sqsubset \Pi([\![\Gamma \vdash A]\!](\gamma), [\![\Gamma, x : A \vdash B]\!](\gamma, \_))$$

(7) $[\Gamma \vdash M](\gamma) \sqsubset [\![\Gamma \vdash (x : A)B]\!](\gamma)$ *and* $[\Gamma \vdash N](\gamma) \sqsubset [\![\Gamma \vdash A]\!](\gamma)$ *for any* $\gamma \in [\![\Gamma]\!]$

(8) $[\Gamma \vdash A](\gamma) \sqsubset \mathfrak{A}_{\Downarrow}(s)$ *for any* $\gamma \in [\![\Gamma]\!]$

(9) $[\![\Gamma \vdash A]\!](\gamma) \in \mathfrak{A}^{\Uparrow}(s)$ *for any* $\gamma \in [\![\Gamma]\!]$.

From now on, the main work will be to state and prove the soundness of our interpretation. The strong normalization will follow quite easily, as it is usual in reducibility proofs.

5.2 Subject reduction properties

Lemma 7 (Subject reduction A)

$$[\Gamma \vdash \mathtt{app}_{x:A.B}((\lambda_{x:A.B} x.M), N)](\gamma) = [\Gamma, x : A \vdash M](\gamma, [\Gamma \vdash N](\gamma))$$

Proof using that

$$\uparrow_{\Pi([\![\Gamma \vdash A]\!](\gamma), [\![\Gamma, x:A \vdash B]\!](\gamma, \_))} \circ \downarrow_{\Pi([\![\Gamma \vdash A]\!](\gamma), [\![\Gamma, x:A \vdash B]\!](\gamma, \_))} = \mathtt{id}_{\Pi([\![\Gamma \vdash A]\!](\gamma), [\![\Gamma, x:A \vdash B]\!](\gamma, \_))}$$

■

Lemma 8 (Weakening for the interpretation, A) *Suppose that* $[\![\Gamma \vdash C]\!](\gamma) \in \mathfrak{A}^{\Uparrow}(s)$*. We prove three results in one:*

1) *if* $[\![\Gamma, \Delta]\!]$ *is defined and* z *is not free in* Δ *then* $[\![\Gamma, z : C, \Delta]\!]$ *is defined and*

$$[\![\Gamma, z : C, \Delta]\!] = \{(\gamma, \zeta, \delta) \mid (\gamma, \delta) \in [\![\Gamma, \Delta]\!] \text{ and } \zeta \in [\![\Gamma \vdash C]\!](\gamma)\}$$

2) if $[\Gamma, \Delta \vdash M](\gamma, \delta)$ is defined and z is not free in Δ or in M then $[\Gamma, z : C, \Delta \vdash M](\gamma, \zeta, \delta)$ is defined and furthermore

$$[\Gamma, z : C, \Delta \vdash M](\gamma, \zeta, \delta) = [\Gamma, \Delta \vdash M](\gamma, \delta).$$

3) if $[\![\Gamma, \Delta \vdash M]\!](\gamma, \delta)$ is defined and z is not free in Δ or in M then $[\![\Gamma, z : C, \Delta \vdash M]\!](\gamma, \zeta, \delta)$ is also defined and:

$$[\![\Gamma, z : C, \Delta \vdash M]\!](\gamma, \zeta, \delta) = [\![\Gamma, \Delta \vdash M]\!](\gamma, \delta).$$

Proof We proceed by induction over the constructions of $[\![\Gamma, \Delta]\!]$, $[\Gamma, \Delta \vdash M](\gamma, \delta)$, $[\![\Gamma, \Delta \vdash M]\!](\gamma, \delta)$. We do not detail all the cases

- Suppose that $[\![\Gamma, \Delta]\!]$ is defined: then it either comes from $[\![\Gamma, \Delta' \vdash A]\!](\gamma, \delta')$ when Δ is of the form $(\Delta', x : A)$; or permits to construct $[\![\Gamma, z : C]\!]$ from $[\![\Gamma \vdash C]\!](\gamma)$ when Δ is empty. In the latter case, the definition of $[\![\Gamma, z : C]\!]$ leads to the assertion (1). In the first case, when Δ is not empty, we have by induction that:
$$[\![\Gamma, z : C, \Delta']\!] \text{ exists}$$
$$[\![\Gamma, z : C, \Delta' \vdash A]\!](\gamma, \zeta, \delta') = [\![\Gamma, \Delta' \vdash A]\!](\gamma, \delta')$$
which induces the assertion (1) from:
$$[\![\Gamma, z : C, \Delta']\!] = \{(\gamma, \zeta, \delta') \mid (\gamma, \delta') \in [\![\Gamma, \Delta']\!] \text{ and } \zeta \in [\![\Gamma \vdash C]\!](\gamma)\}$$
and the definition of $[\![\Gamma, z : C, \Delta]\!]$ as:
$$[\![\Gamma, z : C, \Delta]\!] = \{(\gamma, \zeta, \delta', \alpha) \mid (\gamma, \zeta, \delta') \in [\![\Gamma, z : C, \Delta']\!] \text{ and } \alpha \sqsubset [\![\Gamma, \Delta' \vdash A]\!](\gamma, \delta')\}$$

- Suppose that $[\Gamma, \Delta \vdash x_i](\gamma, \delta)$ is defined for x_i bound by Γ or Δ. It was necessarily constructed from $(\gamma, \delta) \in [\![\Gamma, \Delta]\!]$; by induction, $[\![\Gamma, z : C, \Delta]\!]$ is defined and verifies the assertion (1). Hence $[\Gamma, z : C, \Delta \vdash x_i](\gamma)$ also exists with $[\Gamma, z : C, \Delta \vdash x_i](\gamma) = [\Gamma, \Delta \vdash x_i](\gamma, \delta)$ — since z is different from x_i.

- Suppose that $[\![\Gamma, \Delta \vdash (x : A)B]\!](\gamma, \delta)$ is defined: its definition then comes from the definition of $[\![\Gamma, \Delta \vdash A]\!](\gamma, \delta)$ and $[\![\Gamma, \Delta, x : A \vdash B]\!](\gamma, \delta, \alpha)$. Remember that we consider α-equivalence classes of judgement: it follows that we can choose x such that $x \neq z$. We then use our induction hypothesis and obtain from the assertion (3) that both $[\![\Gamma, z : C, \Delta \vdash A]\!](\gamma, \zeta, \delta)$ and $[\![\Gamma, z : C, \Delta, x : A \vdash B]\!](\gamma, \zeta, \delta, \alpha)$ exist and verify:
$$[\![\Gamma, z : C, \Delta \vdash A]\!](\gamma, \zeta, \delta) = [\![\Gamma, \Delta \vdash A]\!](\gamma, \delta)$$
$$[\![\Gamma, z : C, \Delta, x : A \vdash B]\!](\gamma, \zeta, \delta, \alpha) = [\![\Gamma, \Delta, x : A \vdash B]\!](\gamma, \delta, \alpha)$$
These equalities permits to insure that:
$$[\![\Gamma, z : C, \Delta \vdash A]\!](\gamma, \zeta, \delta) \in \mathfrak{A}^{\Uparrow}(s_1)$$
$$[\![\Gamma, z : C, \Delta, x : A \vdash B]\!](\gamma, \zeta, \delta, \alpha) \in \mathfrak{A}^{\Uparrow}(s_2)$$
for some $(s_1, s_2, s_3) \in \mathcal{R}$. Hence $[\![\Gamma, z : C, \Delta \vdash (x : A)B]\!](\gamma, \zeta, \delta)$ exists and verifies the assertion (3). The other cases are similar.

■

Lemma 9 (Weakening for the interpretation, B) *If $[\Gamma \vdash M](\gamma)$ and $[\![\Gamma, \Delta]\!]$ are defined and all the variables bound by Δ do not occur free in M then $[\Gamma, \Delta \vdash M](\gamma, \delta)$ is defined and furthermore*
$$[\Gamma, \Delta \vdash M](\gamma, \delta) = [\Gamma \vdash M](\gamma).$$
And similarly for $[\![\Gamma \vdash M]\!](\gamma)$.

Proof using the lemma 8 as many times there are variables in Δ. ■

Lemma 10 (Substitution for the interpretation) *If $\Gamma, x : A, \Delta \vdash M : B$ and $\Gamma \vdash P : A$ are derivable, $\gamma \in [\![\Gamma]\!]$, $\pi \equiv [\Gamma \vdash P](\gamma)$ is defined, $(\gamma, \pi, \delta) \in [\![\Gamma, x : A, \Delta]\!]$ and $[\Gamma, x : A, \Delta \vdash M](\gamma, \pi, \delta)$ is defined, then $[\Gamma, \Delta[x \setminus P] \vdash M[x \setminus P]](\gamma, \delta)$ is defined, and*

$$[\Gamma, \Delta[x \setminus P] \vdash M[x \setminus P]](\gamma, \delta) = [\Gamma, x : A, \Delta \vdash M](\gamma, \pi, \delta).$$

Similarly, if $[\![\Gamma, x : A, \Delta \vdash M]\!](\gamma, \pi, \delta)$ is defined:

$$[\![\Gamma, \Delta[x \setminus P] \vdash M[x \setminus P]]\!](\gamma, \delta) = [\![\Gamma, x : A, \Delta \vdash M]\!](\gamma, \pi, \delta).$$

Proof By induction over the structure of M. The key case is $M = x$ which is treated by the previous lemma. We also detail the case of λ-abstraction; if $M = \lambda_{x:A.B} x.N$ ... ■

Lemma 11 (Subject Reduction for the interpretation) *If $\Gamma \vdash M : A$, $M \triangleright_\beta M'$ and $[\Gamma \vdash M](\gamma)$ is defined then so is $[\Gamma \vdash M'](\gamma)$ and*

$$[\Gamma \vdash M](\gamma) = [\Gamma \vdash M'](\gamma).$$

And similarly for $[\![\Gamma \vdash M]\!](\gamma)$ and $[\![\Gamma \vdash M']\!](\gamma)$.

Proof By induction over the structure of M, or more precisely over the proof that $M \triangleright_\beta M'$. The key case is of course the one where M is itself the reduced redex. It is treated by the previous lemma. ■

5.3 Soundness

Definition 14 *Let $i \in \mathfrak{C}$ and $[\![\Gamma]\!]$ be well-defined. The relation $\left|\begin{smallmatrix} i \\ \mathfrak{C} \end{smallmatrix}\right|$ between the sequences γ of $[\![\Gamma]\!]$ is constructed by structural induction on Γ:*

- $\forall \alpha, \alpha' \in [\![x : A]\!]$:

$$\alpha \left|\begin{matrix} i \\ \mathfrak{C} \end{matrix}\right| \alpha' \Leftrightarrow \exists s \in \mathcal{S}, \alpha \left|\begin{matrix} i \\ \mathfrak{A}^{\Uparrow}(s) \end{matrix}\right| \alpha'$$

- $\forall (\gamma, \alpha), (\gamma', \alpha') \in [\![\Gamma, x : A]\!]$:

$$(\gamma, \alpha) \left|\begin{matrix} i \\ \mathfrak{C} \end{matrix}\right| (\gamma', \alpha') \Leftrightarrow \gamma \left|\begin{matrix} i \\ \mathfrak{C} \end{matrix}\right| \gamma' \text{ and } \exists s \in \mathcal{S}, \alpha \left|\begin{matrix} i \\ \mathfrak{A}^{\Uparrow}(s) \end{matrix}\right| \alpha'$$

Theorem 1 (Well-formedness and soundness of the interpretation) *If Γ wf is derivable, then $[\![\Gamma]\!]$ is defined. If the judgement $\Gamma \vdash M : A$ is derivable, then for any $\gamma \in [\![\Gamma]\!]$ the following holds:*

1. *$[\Gamma \vdash M](\gamma)$ and $[\![\Gamma \vdash A]\!](\gamma)$ are defined with*

$$[\Gamma \vdash M](\gamma) \sqsubset [\![\Gamma \vdash A]\!](\gamma).$$

Moreover, if there exists a sort s such that $[\![\Gamma \vdash A]\!](\gamma) \in \mathfrak{A}^{\Uparrow}(s)$, then:

$$\forall i \in \mathfrak{C} \,.\, \gamma \left|\begin{matrix} i \\ \mathfrak{C} \end{matrix}\right| \gamma' \Rightarrow [\Gamma \vdash M](\gamma) \left|\begin{matrix} i \\ \mathfrak{A}^{\Uparrow}(s) \end{matrix}\right| [\Gamma \vdash M](\gamma')$$

2. if $A = s$ then $\llbracket\Gamma \vdash M\rrbracket(\gamma)$ is defined, and $\llbracket\Gamma \vdash M\rrbracket(\gamma) \in \mathfrak{A}^{\Uparrow}(s)$. Moreover:

$$\forall i \in \mathfrak{E} \,.\, \gamma \left| \begin{matrix} i \\ \mathfrak{E} \end{matrix} \right| \gamma' \Rightarrow \llbracket\Gamma \vdash M\rrbracket(\gamma) \left\| \begin{matrix} i \\ \mathfrak{A}^{\Uparrow}(s) \end{matrix} \right\| \llbracket\Gamma \vdash M\rrbracket(\gamma')$$

Remark We remark that clause 2 is equivalent to clause 1, provided $A = s_1$ and the Λ-set $\mathfrak{A}_{\Downarrow}(s_1)$ is element of an $\mathfrak{E}$-set $\mathfrak{A}^{\Uparrow}(s_2)$. This is typically the case when $A = s_1$ and $(s_1, s_2) \in \mathcal{A}$.

PROOF

$2 \Rightarrow 1$ Suppose that clause 2 applies and that $A = s_1$. Then $[\Gamma \vdash M](\gamma)$ is defined either directly or as $\Downarrow_{s_1} \langle\llbracket\Gamma \vdash M\rrbracket(\gamma)\rangle$. In both cases, by $\Downarrow_{s_1} \circ \Uparrow_{s_1} = Id_{\mathfrak{A}_{\Downarrow}(s_1)_0}$, we have:

$$[\Gamma \vdash M](\gamma) = \Downarrow_{s_1} \langle\llbracket\Gamma \vdash M\rrbracket(\gamma)\rangle$$

and therefore:

$$[\Gamma \vdash M](\gamma) \sqsubset \mathfrak{A}_{\Downarrow}(s_1) = \llbracket\Gamma \vdash A\rrbracket(\gamma)$$

Suppose now that $\mathfrak{A}_{\Downarrow}(s_1)$ is element of $\mathfrak{A}^{\Uparrow}(s)$ for some sort s. The condition 2(1) infers from

$$\llbracket\Gamma \vdash M\rrbracket(\gamma) \left\| \begin{matrix} i \\ \mathfrak{A}^{\Uparrow}(s_1) \end{matrix} \right\| \llbracket\Gamma \vdash M\rrbracket(\gamma')$$

that:

$$[\Gamma \vdash M](\gamma) \left| \begin{matrix} i \\ \mathfrak{A}^{\Uparrow}(s) \end{matrix} \right| [\Gamma \vdash M](\gamma')$$

when $\gamma \left| \begin{matrix} i \\ \mathfrak{E} \end{matrix} \right| \gamma'$; we conclude clause 1.

$1 \Rightarrow 2$ conversely, suppose that clause 1 applies and that $A = s_1$ with $\mathfrak{A}_{\Downarrow}(s_1) \in \mathfrak{A}^{\Uparrow}(s_2)$. Then for every $\gamma \in \llbracket\Gamma\rrbracket$, $\llbracket\Gamma \vdash M\rrbracket(\gamma)$ is defined either directly or as $\Uparrow_{s_1} \langle[\Gamma \vdash M](\gamma)\rangle$. In both cases, by $\Uparrow_{s_1} \circ \Downarrow_{s_1} = Id_{\mathfrak{A}^{\Uparrow}(s_1)}$, we have $\llbracket\Gamma \vdash M\rrbracket(\gamma) = \Uparrow_{s_1} \langle[\Gamma \vdash M](\gamma)\rangle$, hence

$$\llbracket\Gamma \vdash M\rrbracket(\gamma) \in \mathfrak{A}^{\Uparrow}(s_1)$$

Moreover, by clause 1 and $\mathfrak{A}_{\Downarrow}(s_1) \in \mathfrak{A}^{\Uparrow}(s_2)$ we have:

$$\forall i \in \mathfrak{E}. \quad \gamma \left| \begin{matrix} i \\ \mathfrak{E} \end{matrix} \right| \gamma' \Rightarrow [\Gamma \vdash M](\gamma) \left| \begin{matrix} i \\ \mathfrak{A}^{\Uparrow}(s_2) \end{matrix} \right| [\Gamma \vdash M](\gamma')$$

therefore by condition 2(1) we deduce:

$$\forall i \in \mathfrak{E}. \quad \gamma \left| \begin{matrix} i \\ \mathfrak{E} \end{matrix} \right| \gamma' \Rightarrow \llbracket\Gamma \vdash M\rrbracket(\gamma) \left\| \begin{matrix} i \\ \mathfrak{A}^{\Uparrow}(s_1) \end{matrix} \right\| \llbracket\Gamma \vdash M\rrbracket(\gamma')$$

■

PROOF **(theorem 1)** Not surprisingly, the proof proceeds by induction over the structure of the derivation.

WEAK

The judgement is $\vdash \Gamma, x : A$ *wf*. The induction hypothesis applied to the premises yields:

- $\llbracket\Gamma\rrbracket$ is defined
- for any $\gamma \in \llbracket\Gamma\rrbracket$ we have $\llbracket\Gamma \vdash A\rrbracket(\gamma) \in \mathfrak{A}^{\Uparrow}(s)$

hence $\llbracket\Gamma \vdash A\rrbracket(\gamma)$ is a saturated Λ-set and $\llbracket\Gamma, x : A\rrbracket$ is defined.

SORT

the judgement is $\Gamma \vdash s_1 : s_2$ with $(s_1, s_2) \in \mathcal{A}$; we prove clause 2. $\llbracket\Gamma \vdash s_1\rrbracket(\gamma)$ is directly defined as $\mathfrak{A}_{\Downarrow}(s_1)$, which is an element of $\mathfrak{A}^{\Uparrow}(s_2)$ by condition 1(2). Hence clause 1.

Var

the judgement is $\Gamma, x : A, \Delta \;\vdash\; x : A$; we prove clause 1, whichh implies clause 2 because $A = s$ implies that A has a sort. The induction hypothesis applied to the premises yields that $[\![\Gamma, x : A, \Delta]\!]$ is defined. Iterating the induction, it is easy to see that its elements are of the form (γ, α, δ) with $\gamma \in [\![\Gamma]\!]$ and $\alpha \sqsubset [\![\Gamma \vdash A]\!](\gamma)$.

By definition, we have

$$[\Gamma, x : A, \Delta \vdash x](\gamma, \alpha, \delta) = \alpha$$

and hence

$$[\Gamma, x : A, \Delta \vdash x](\gamma, \alpha, \delta) \sqsubset [\![\Gamma \vdash A]\!](\gamma).$$

On the other hand, by the weakening lemma, we have that $[\![\Gamma, x : A, \Delta \vdash A]\!](\gamma, \alpha, \delta)$ is defined and also:

$$[\![\Gamma, x : A, \Delta \vdash A]\!](\gamma, \alpha, \delta) = [\![\Gamma \vdash A]\!](\gamma).$$

The result follows:

$$[\Gamma, x : A, \Delta \vdash x](\gamma, \alpha, \delta) \sqsubset [\![\Gamma, x : A, \Delta \vdash A]\!](\gamma, \alpha, \delta).$$

Suppose moreover that there is a sort s such that for every $\gamma \in [\![\Gamma]\!]$, $[\![\Gamma \vdash A]\!](\gamma) \in \mathfrak{A}^{\Uparrow}(s)$. Let $i \in \mathfrak{C}$. $(\gamma, \alpha, \delta) \left| \begin{array}{c} i \\ \mathfrak{C} \end{array} \right| (\gamma', \alpha', \delta')$ implies by definition of $\left| \begin{array}{c} i \\ \mathfrak{C} \end{array} \right|$ that there is an $\mathfrak{C}$-set $\mathfrak{A}^{\Uparrow}(s_2)$ such that $\alpha \left| \begin{array}{c} i \\ \mathfrak{A}^{\Uparrow}(s_2) \end{array} \right| \alpha'$. The property

$$(\gamma, \alpha, \delta) \left| \begin{array}{c} i \\ \mathfrak{C} \end{array} \right| (\gamma', \alpha', \delta') \Rightarrow [\Gamma, x : A, \Delta \vdash x](\gamma, \alpha, \delta) \left| \begin{array}{c} i \\ \mathfrak{A}^{\Uparrow}(s) \end{array} \right| [\Gamma, x : A, \Delta \vdash x](\gamma, \alpha, \delta)$$

follows condition 2(2).

Prod

The judgement is $\Gamma \;\vdash\; (x : A)B : s_3$ with $(s_1, s_2, s_3) \in \mathcal{R}$; we prove clause 2 (which implies clause 1). The induction hypothesis applied to the premises yield:

1. $[\![\Gamma]\!]$ is defined
2. for any $\gamma \in [\![\Gamma]\!]$ we have $[\![\Gamma \vdash A]\!](\gamma) \in \mathfrak{A}^{\Uparrow}(s_1)$
3. for any $\alpha \sqsubset [\![\Gamma \vdash A]\!](\gamma)$, $[\![\Gamma, x : A \vdash B]\!](\gamma, \alpha) \in \mathfrak{A}^{\Uparrow}(s_2)$
4. for any $i \in \mathfrak{C}$, for any $\gamma' \in [\![\Gamma]\!]$, if
$$\gamma \left| \begin{array}{c} i \\ \mathfrak{C} \end{array} \right| \gamma'$$
then
$$[\![\Gamma \vdash A]\!](\gamma) \left\| \begin{array}{c} i \\ \mathfrak{A}^{\Uparrow}(s_1) \end{array} \right\| [\![\Gamma \vdash A]\!](\gamma').$$
5. for any $\alpha' \sqsubset [\![\Gamma \vdash A]\!](\gamma')$, if
$$\alpha \left| \begin{array}{c} i \\ \mathfrak{C} \end{array} \right| \alpha'$$
then
$$[\![\Gamma, x : A \vdash B]\!](\gamma, \alpha) \left\| \begin{array}{c} i \\ \mathfrak{A}^{\Uparrow}(s_2) \end{array} \right\| [\![\Gamma, x : A \vdash B]\!](\gamma', \alpha').$$

By choosing $\gamma = \gamma'$ in 5, we obtain:

$$\forall i \in \mathfrak{C} \;.\; \forall \alpha \in [\![\Gamma \vdash A]\!](\gamma) \;.\; \alpha \left| \begin{array}{c} i \\ \mathfrak{C} \end{array} \right| \alpha' \Longrightarrow$$

$$[\![\Gamma, x : A \vdash B]\!](\gamma, \alpha) \left\| \begin{array}{c} i \\ \mathfrak{A}^{\Uparrow}(s_2) \end{array} \right\| [\![\Gamma, x : A \vdash B]\!](\gamma, \alpha')$$

which, by condition 2(2) is equivalent to:

$$\forall i \in \mathfrak{E} \;.\; \forall \alpha \in [\![\Gamma \vdash A]\!](\gamma) \;.\; \alpha \left| \begin{array}{c} i \\ \mathfrak{A}^{\Uparrow}(s_1) \end{array} \right| \alpha' \Longrightarrow$$
$$[\![\Gamma, x : A \vdash B]\!](\gamma, \alpha) \left\| \begin{array}{c} i \\ \mathfrak{A}^{\Uparrow}(s_2) \end{array} \right\| [\![\Gamma, x : A \vdash B]\!](\gamma, \alpha').$$

This last proposition, combined with 1, 2 and 3 above, guarantees that $[\![\Gamma \vdash (x : A)B]\!](\gamma)$ is defined as

$$[\![\Gamma \vdash (x : A)B]\!](\gamma) = \Pi_{\downarrow}([\![\Gamma \vdash A]\!](\gamma), [\![\Gamma, x : A \vdash B]\!](\gamma, \_))$$

and thus

$$[\![\Gamma \vdash (x : A)B]\!](\gamma) \in \mathfrak{A}^{\Uparrow}(s_3).$$

It remains to be proved:

$$\forall i \in \mathfrak{E}, \quad \gamma \left| \begin{array}{c} i \\ \mathfrak{E} \end{array} \right| \gamma' \Rightarrow [\![\Gamma \vdash (x : A)B]\!](\gamma) \left\| \begin{array}{c} i \\ \mathfrak{A}^{\Uparrow}(s_3) \end{array} \right\| [\![\Gamma \vdash (x : A)B]\!](\gamma').$$

By definition and condition 3(1), when $\gamma \left| \begin{array}{c} i \\ \mathfrak{E} \end{array} \right| \gamma'$, this is a consequence of:

$$\Pi([\![\Gamma \vdash A]\!](\gamma), [\![\Gamma, x : A \vdash B]\!](\gamma, \_)) \left\| \begin{array}{c} i \\ \Pi(\mathfrak{A}^{\Uparrow}(s_1), \mathfrak{A}^{\Uparrow}(s_2)) \end{array} \right\| \Pi([\![\Gamma \vdash A]\!](\gamma'), [\![\Gamma, x : A \vdash B]\!](\gamma', \_))$$

and unfolding the definition of the equivalence relation of definition 12:

$$[\![\Gamma \vdash A]\!](\gamma) \left\| \begin{array}{c} i \\ \mathfrak{A}^{\Uparrow}(s_1) \end{array} \right\| [\![\Gamma \vdash A]\!](\gamma')$$

and

$$\forall \alpha \sqsubset [\![\Gamma \vdash A]\!](\gamma) \;.\; \forall \alpha' \sqsubset [\![\Gamma \vdash A]\!](\gamma') \;.\; \alpha \left| \begin{array}{c} i \\ \mathfrak{A}^{\Uparrow}(s_1) \end{array} \right| \alpha' \Longrightarrow$$
$$[\![\Gamma, x : A \vdash B]\!](\gamma, \alpha) \left\| \begin{array}{c} i \\ \mathfrak{A}^{\Uparrow}(s_2) \end{array} \right\| [\![\Gamma, x : A \vdash B]\!](\gamma', \alpha').$$

These two propositions are immediate consequences of the induction hypothesis 4 (respectively 5), using condition 2(2).

Lambda

The judgement is $\Gamma \vdash \lambda_{x:A.B}x.M : (x : A)B$; we prove clause 1 (which implies clause 2 because $(x : A)B$ is not a sort). The premises are

$$\Gamma, x : A \vdash M : B$$

and

$$\Gamma \vdash (x : A)B : s.$$

We first prove that $[\Gamma \vdash \lambda_{x:A.B}x.M](\gamma)$ is defined as an index of $[\![\Gamma \vdash (x : A)B]\!](\gamma)$ for any $\gamma \sqsubset [\![\Gamma]\!]$. Some of the necessary conditions are common to the definition of $[\![\Gamma \vdash (x : A)B]\!](\gamma)$; they are of course an immediate consequence of the induction hypothesis for the second premise.

It is important hereafter that the derivation of the second premise contains a (Prod) derivation step of the form:

$$\frac{\Gamma \vdash A : s_1 \Gamma, x : A \vdash B : s_2}{\Gamma \vdash (x : A)B : s_3}$$

with $(s_1, s_2, s_3) \in \mathcal{R}$.

For any $\gamma \in [\![\Gamma]\!]$, the induction hypothesises yield, among others:

1. $[\![\Gamma \vdash A]\!](\gamma) \in \mathfrak{A}^{\Uparrow}(s_1)$
2. for any $\alpha \sqsubset [\![\Gamma \vdash A]\!](\gamma)$
$$[\![\Gamma, x : A \vdash B]\!](\gamma, \alpha) \in \mathfrak{A}^{\Uparrow}(s_2)$$
3. for any $\gamma \in [\![\Gamma]\!]$, for any $\alpha \sqsubset [\![\Gamma \vdash A]\!](\gamma)$
$$[\Gamma, x : A \vdash M](\gamma, \alpha) \sqsubset [\![\Gamma, x : A \vdash B]\!](\gamma, \alpha)$$

4. for any $i \in \mathfrak{C}$, for any $(\gamma', \alpha') \in [\![\Gamma, x : A]\!]$, if

$$(\gamma, \alpha) \left| \begin{matrix} i \\ \mathfrak{C} \end{matrix} \right| (\gamma', \alpha')$$

then

$$[\Gamma, x : A \vdash M](\gamma, \alpha) \left| \begin{matrix} i \\ \mathfrak{A}^{\Uparrow}(s_2) \end{matrix} \right| [\Gamma, x : A \vdash M](\gamma', \alpha').$$

5. for any $i \in \mathfrak{C}$, for any $(\gamma', \alpha') \in [\![\Gamma, x : A]\!]$, if

$$(\gamma, \alpha) \left| \begin{matrix} i \\ \mathfrak{C} \end{matrix} \right| (\gamma', \alpha')$$

then

$$[\![\Gamma \vdash A]\!](\gamma) \left\| \begin{matrix} i \\ \mathfrak{A}^{\Uparrow}(s_1) \end{matrix} \right\| [\![\Gamma \vdash A]\!](\gamma')$$

and

$$[\![\Gamma, x : A \vdash B]\!](\gamma, \alpha) \left\| \begin{matrix} i \\ \mathfrak{A}^{\Uparrow}(s_2) \end{matrix} \right\| [\![\Gamma, x : A \vdash B]\!](\gamma', \alpha')$$

If we chose $\gamma' = \gamma$ in the fourth proposition above, we obtain:
$\forall i \in \mathfrak{C} \,.\, \forall \alpha' \sqsubset [\![\Gamma \vdash A]\!](\gamma) \,.\, \alpha \left| \begin{matrix} i \\ \mathfrak{C} \end{matrix} \right| \alpha' \Longrightarrow$

$$[\Gamma, x : A \vdash M](\gamma, \alpha) \left| \begin{matrix} i \\ \mathfrak{A}^{\Uparrow}(s_2) \end{matrix} \right| [\Gamma, x : A \vdash M](\gamma, \alpha').$$

This is exactly what is necessary for having (see definition 10):

$$(\alpha \sqsubset [\![\Gamma \vdash A]\!](\gamma) \mapsto [\Gamma, x : A \vdash M](\gamma, \alpha)) \;\sqsubset\; \Pi([\![\Gamma \vdash A]\!](\gamma), [\![\Gamma, x : A \vdash B]\!](\gamma, \_))$$

since $\alpha \left| \begin{matrix} i \\ \mathfrak{C} \end{matrix} \right| \alpha'$ is equivalent to $\alpha \left| \begin{matrix} i \\ \mathfrak{A}^{\Uparrow}(s) \end{matrix} \right| \alpha'$ for any sort s (here s_1) such that $\alpha \sqsubset [\![\Gamma \vdash A]\!](\gamma) \in \mathfrak{A}^{\Uparrow}(s)$ and $\alpha' \sqsubset [\![\Gamma \vdash A]\!](\gamma') \in \mathfrak{A}^{\Uparrow}(s)$ — see condition 2(2).

Thus $[\Gamma \vdash \lambda_{x:A.B} x.M](\gamma)$ exists and is an index of $[\![\Gamma \vdash (x : A)B]\!](\gamma)$.

Suppose now that for some sort s, for every $\gamma \in [\![\Gamma]\!]$, $[\![\Gamma \vdash (x : A)B]\!](\gamma) \in \mathfrak{A}^{\Uparrow}(s)$. We have to check that:

$$\forall (\gamma, \gamma') \in [\![\Gamma]\!]^2 \,.\, \gamma \left| \begin{matrix} i \\ \mathfrak{C} \end{matrix} \right| \gamma' \Longrightarrow [\Gamma \vdash \lambda_{x:A.B} x.M](\gamma) \left| \begin{matrix} i \\ \mathfrak{A}^{\Uparrow}(s_3) \end{matrix} \right| [\Gamma \vdash \lambda_{x:A.B} x.M](\gamma')$$

which by definition 12 and condition 3(2$\Rightarrow$) and hypothesis 5, this proposition is a consequence of:
$\forall (\gamma, \gamma') \in [\![\Gamma]\!]^2 \,.\, \forall \alpha \sqsubset [\![\Gamma \vdash A]\!](\gamma) \,.\, \gamma \left| \begin{matrix} i \\ \mathfrak{C} \end{matrix} \right| \gamma' \Longrightarrow$

$$\forall \alpha' \sqsubset [\![\Gamma \vdash A]\!](\gamma') \,.\, \alpha \left| \begin{matrix} i \\ \mathfrak{C} \end{matrix} \right| \alpha' \Longrightarrow$$

$$[\Gamma, x : A \vdash M](\gamma, \alpha) \left| \begin{matrix} i \\ \mathfrak{A}^{\Uparrow}(s_2) \end{matrix} \right| [\Gamma, x : A \vdash M](\gamma', \alpha')$$

which is exactly the fourth induction hypothesis enumerated above.

App

The judgement is $\Gamma \vdash \mathtt{app}_{x:A.B}(M, N) : B[x \setminus N]$; we prove clause 1. The three premises are

$$\Gamma \vdash M : (x : A)B$$

and

$$\Gamma \vdash N : A$$

and

$$\Gamma \vdash (x : A)B : s$$

Once again we use the fact that the derivation of the second premise contains a (Prod) derivation step of the form:

$$\frac{\Gamma \vdash A : s_1 \Gamma, x : A \vdash B : s_2}{\Gamma \vdash (x : A)B : s_3}$$

with $(s_1, s_2, s_3) \in \mathcal{R}$.

The induction hypothesises yield, among others:

1. $[\![\Gamma]\!]$ is defined
2. for any $\gamma \in [\![\Gamma]\!]$, $[\![\Gamma \vdash (x : A)B]\!](\gamma)$ is defined and
$$[\![\Gamma \vdash (x : A)B]\!](\gamma) \in \mathfrak{A}^{\Uparrow}(s_3)$$
3. $[\![\Gamma \vdash A]\!](\gamma) \in \mathfrak{A}^{\Uparrow}(s_1)$
4. for any $\alpha \sqsubset [\![\Gamma \vdash A]\!](\gamma)$
$$[\![\Gamma, x : A \vdash B]\!](\gamma, \alpha) \in \mathfrak{A}^{\Uparrow}(s_2)$$
5. $\uparrow_{\Pi([\![\Gamma \vdash A]\!](\gamma), [\![\Gamma, x:A \vdash B]\!](\gamma, \_))} \langle [\Gamma \vdash M](\gamma) \rangle \sqsubset \Pi([\![\Gamma \vdash A]\!](\gamma), [\![\Gamma, x : A \vdash B]\!](\gamma))$
6. $[\Gamma \vdash N](\gamma) \sqsubset [\![\Gamma \vdash A]\!](\gamma)$
7. for any $i \in \mathfrak{C}$, for any $\gamma' \in [\![\Gamma]\!]$ if
$$\gamma \,\Big|\, \overset{i}{\mathfrak{C}} \,\Big|\, \gamma'$$
then
$$[\Gamma \vdash N](\gamma) \,\Big|\, \overset{i}{\mathfrak{A}^{\Uparrow}(s_1)} \,\Big|\, [\Gamma \vdash N](\gamma')$$
and
$$[\Gamma \vdash M](\gamma) \,\Big|\, \overset{i}{\mathfrak{A}^{\Uparrow}(s_2)} \,\Big|\, [\Gamma \vdash M](\gamma')$$
8. for any $i \in \mathfrak{C}$, for any $(\gamma', \alpha') \in [\![\Gamma, x : A]\!]$, if
$$(\gamma, \alpha) \,\Big|\, \overset{i}{\mathfrak{C}} \,\Big|\, (\gamma', \alpha')$$
then
$$[\![\Gamma \vdash A]\!](\gamma) \,\Big\|\, \overset{i}{\mathfrak{A}^{\Uparrow}(s_1)} \,\Big\|\, [\![\Gamma \vdash A]\!](\gamma')$$
and
$$[\![\Gamma, x : A \vdash B]\!](\gamma, \alpha) \,\Big\|\, \overset{i}{\mathfrak{A}^{\Uparrow}(s_2)} \,\Big\|\, [\![\Gamma, x : A \vdash B]\!](\gamma', \alpha')$$

An immediate consequence of the clauses 5 and 6 is that $[\Gamma \vdash \mathsf{app}_{x:A.B}(M, N)](\gamma)$ is defined and

$$[\Gamma \vdash \mathsf{app}_{x:A.B}(M, N)](\gamma) \sqsubset [\![\Gamma, x : A \vdash B]\!](\gamma, [\Gamma \vdash N](\gamma)).$$

By the lemma 10, we then have:

$$[\Gamma \vdash \mathsf{app}_{x:A.B}(M, N)](\gamma) \sqsubset [\![\Gamma \vdash B[x \setminus N]]\!](\gamma).$$

We now have to prove that for any $i \in \mathfrak{C}$,

$$\forall \gamma' \in [\![\Gamma]\!] \,.\, \gamma \,\Big|\, \overset{i}{\mathfrak{C}} \,\Big|\, \gamma' \Longrightarrow [\Gamma \vdash \mathsf{app}_{x:A.B}(M, N)](\gamma) \,\Big|\, \overset{i}{\mathfrak{A}^{\Uparrow}(s_2)} \,\Big|\, [\Gamma \vdash \mathsf{app}_{x:A.B}(M, N)](\gamma')$$

Which is a quite immediate consequence of the clauses 6, 7 and 8 of the induction hypothesises above, of condition 3(2$\Leftarrow$) and of definition 12.

This proves clause 1. To prove clause 2, note that if $B[x \setminus N]$ is a sort t, then $\mathfrak{A}_{\Downarrow}(t) \in \mathfrak{A}^{\Uparrow}(s_2)$ by clauses 4 and 6 in the hypothesis.

Conv

The judgement is $\Gamma \vdash M : B$; we prove clause 1. Clause 2 follows from the fact that $\Gamma \vdash B : s$ stands among the premises. Applied to the premises, the induction hypothesis yields that $[\![\Gamma]\!]$ is defined, and for any $\gamma \in [\![\Gamma]\!]$,

- $[\Gamma \vdash M](\gamma) \sqsubset [\![\Gamma \vdash A]\!](\gamma)$
- $[\![\Gamma \vdash B]\!](\gamma) \in \mathfrak{A}^{\Uparrow}(s)$

Furthermore, lemma 11 guarantees that

$$[\![\Gamma \vdash A]\!](\gamma) = [\![\Gamma \vdash B]\!](\gamma)$$

and thus

$$[\Gamma \vdash M](\gamma) \sqsubset [\![\Gamma \vdash B]\!](\gamma) \in \mathfrak{A}^{\Uparrow}(s).$$

The proposition

$$\forall i \in \mathfrak{E} \;.\; \gamma \left| \begin{array}{c} i \\ \mathfrak{E} \end{array} \right| \gamma' \Longrightarrow [\Gamma \vdash M](\gamma) \left| \begin{array}{c} i \\ \mathfrak{A}^{\Uparrow}(s) \end{array} \right| [\Gamma \vdash M](\gamma')$$

is already an induction hypothesis. ■

5.4 Strong Normalisation

Definition 15 *Let $(\gamma_1, ..., \gamma_n) \in [\![\Gamma]\!]$. We define $(P_1, ..., P_n) \models (\gamma_1, ..., \gamma_n)$ by induction on n:*

- *if $\Gamma, x_{n+1} : A_{n+1}$ is well formed and $\gamma_1, ..., \gamma_{n+1} \in [\![\Gamma, x_{n+1} : A_{n+1}]\!]$ then $(P_1, ..., P_{n+1}) \models (\gamma_1, ..., \gamma_{n+1})$ iff $(P_1, ..., P_n) \models (\gamma_1, ..., \gamma_n)$ and $P_{n+1} \models [\![\Gamma \vdash A]\!](\gamma_1, ..., \gamma_{n+1})$.*

If $(\gamma_1, ..., \gamma_n) \in [\![x_1 : A_1, ..., x_n : A_n]\!]$ and $(P_1, ..., P_n) \models (\gamma_1, ..., \gamma_n)$ then $\{\{M\}\}(P_1, ..., P_n)$ is defined as $M[x_n \setminus P_n, \ldots, x_1 \setminus P_1]$.

Lemma 12 *Let $\Gamma \vdash M : A$ be derivable. If $(\gamma_1, ..., \gamma_n) \in [\![\Gamma]\!]$ and $(P_1, ..., P_n) \models \gamma$ then*

$$\{\{M\}\}(P_1, ..., P_n) \models_{[\![\Gamma \vdash A]\!](\gamma)} [\Gamma \vdash M](\gamma)$$

Proof By induction over the structure of the derivation. We only detail two cases:

Lambda We have to check that

$$\{\{\lambda_{x:A.B} x.M\}\}(P_1, ..., P_n) \models_{[\![\Gamma \vdash (X:A)B]\!](\gamma)} [\Gamma \vdash \lambda_{x:A.B} x.M](\gamma)$$

because $\downarrow_{\Pi([\![\Gamma \vdash A]\!](\gamma), [\![\vdash \Gamma, x:A \vdash B]\!](\gamma, \_))}$ is a Λ-iso, and unfolding the definitions, we see this is equivalent to

$$\{\{\lambda_{x:A.B} x.M\}\}(P_1, ..., P_n, N) \models_{\Pi([\![\Gamma \vdash A]\!](\gamma), [\![\Gamma, x:A \vdash B]\!](\gamma, \_)} [\Gamma, x : A \vdash M](\gamma, \_)$$

or equivalently,

$$\forall \alpha \sqsubset [\![\Gamma \vdash A]\!](\gamma) \;.\; \forall N \models_{[\![\Gamma \vdash A]\!](\gamma)} \alpha \;.\; \forall A', B' \in \mathcal{SN} \;.$$
$$\{\{\mathsf{app}_{x:A'.B'}(\lambda_{x:A.B} x.M\}\}(P_1, ..., P_n), N) \models_{[\![\Gamma, x:A \vdash B]\!](\gamma, \alpha)} [\Gamma, x : A \vdash M](\gamma, \alpha).$$

Now, the induction hypothesis ensures that

$$\{\{M\}\}(P_1, \ldots, P_n, N) \models_{[\![\Gamma, x:A \vdash B]\!](\gamma, \alpha)} [\Gamma, x : A \vdash M](\gamma, \alpha)$$

which, since $[\![\Gamma, x : A \vdash B]\!](\gamma, \alpha)$ is a saturated Λ-set, is equivalent to the previous proposition.

Prod We simply have to check (condition 1(1)), that $\{\{(x : A)B\}\}(p_1, \ldots, P_n)$ is strongly normalizing. It is an immediate consequence of the induction hypothesis, which states that $\{\{A\}\}(p_1, \ldots, P_n)$ and $\{\{B\}\}(P_1, \ldots, P_n, x)$ are both strongly normalizing. ■

Theorem 2 *If $\Gamma \vdash M : A$ is derivable, then M is strongly normalizable.*

Proof Let $\Gamma = [x_1 : A_1; \ldots; x_n : A_n]$. We know that $[\![x_a : A_1]\!]$ is a saturated Λ-set; thus the second clause of definition 7 ensures there exists $\gamma_1 \sqsubset [\![x_1 : A_1]\!]$ such that γ_1 is realized by any strongly normalizing atomic term. Iterating this construction we obtain $\gamma \equiv (\gamma_1, \ldots, \gamma_n)$ such that $\gamma \in [\![\Gamma]\!]$ and $(x_1, \ldots, x_n) \models (\gamma_1, \ldots, \gamma_n)$. The previous lemma then ensures that $M[x_n \setminus P_n, \ldots, x_1 \setminus P_1] \models_{[\![\Gamma \vdash A]\!](\gamma)}$ and hence M is strongly normalizing. ■

6 Universe Constructions for Different Type Systems

Definition 16 (degenerated Λ-sets) *A Λ-set X is said to be degenerated if X_0 is a singleton $\{\mathcal{C}\}$ where $\mathcal{C}$ is a saturated set of terms and*

$$M \models_X \mathcal{C} \iff M \in \mathcal{C}.$$

There is of course a trivial one-to-one correspondence between saturated degenerated Λ-sets and saturated sets of terms. **Remark** The family of degenerated Λ-sets is a set.

Any non-empty set X can be viewed as a Λ-set $J(X)$ whose indexes are the elements of X and such that

$$\forall x \in J(X) \ . \ \forall M \in \Lambda \ . \ M \models_{\mathfrak{A}(*)} \mathcal{C} \iff M \in \mathcal{SN}.$$

Hereafter we usually identify the set X and the (saturated) Λ-set $J(X)$.

6.1 System F

Girard's system F, also called second order polymorphic λ-calculus is defined as a PTS by:

$$\mathcal{S} \equiv \{*, \Box\} \qquad \mathcal{A} \equiv \{(*, \Box)\} \qquad \mathcal{R} \equiv \{(*, *, *), (\Box, *, *)\}$$

Here, the set $\mathfrak{C}$ is empty, which means that we do not care about the relations. For every sort s we take $\mathfrak{A}^{\Uparrow}(s) = \mathfrak{A}_{\Downarrow}(s) = \mathfrak{A}(s)$ and thus $\Uparrow_s = \Downarrow_s = Id_{\mathfrak{A}^{\Uparrow}(s)}$. We define $\mathfrak{A}(*)$ as the set of saturated degenerated Λ-sets ; the set $\mathfrak{A}(\Box)_0$ is the singleton $\{\mathfrak{A}(*)\}$.

Conditions 2, 3 and 4 are trivial because $\mathfrak{C}$ is empty. The first two points in condition 1 are easy:

1. all elements of $\mathfrak{A}(\star)$ and $\mathfrak{A}(\Box)$ are saturated Λ-sets
2. $\mathfrak{A}(\star)$ is (the only) element of $\mathfrak{A}(\Box)$.

Let us prove the point 3. Suppose that X is a Λ-set either element of $\mathfrak{A}(*)$ or $\mathfrak{A}(\Box)$, and $(Y_\alpha)_{\alpha \in X_0}$ is a family of saturated degenerated Λ-sets $Y_\alpha \in \mathfrak{A}*$. Since all the Y_α have exactly one carrier y_α, the saturated Λ-set $\Pi_{\downarrow}(X, Y)$ is naturally defined as the degenerated Λ-set corresponding to the following saturated set:

$$\{M, \forall (A, B, N) \in \mathcal{SN}^3 \ . \ \forall \alpha \sqsubset X \ . \ \forall N \models_X \alpha \ . \ \mathtt{app}_{x:A.B}(M, N) \models_{Y_\alpha} y_\alpha\}.$$

The element of this set are exactly the realisers of the only index of $\pi \sqsubset \Pi(X, Y)$. Thus we have defined a Λ-iso

$$\downarrow_{\Pi(X,Y)}: \Pi(X, Y) \to \Pi_{\downarrow}(X, Y) \in \mathfrak{A}^{\Uparrow}(*).$$

which associates π to $\emptyset$. This proves criterion 1.

6.2 CC

The Calculus of Construction which extends system F is defined as a PTS by:

$$\mathcal{S} \equiv \{*, \Box\} \qquad \mathcal{A} \equiv \{(*, \Box)\} \qquad \mathcal{R} \equiv \{(*, *, *), (\Box, *, *), (*, \Box, \Box), (\Box, \Box, \Box)\}$$

Our model extends the model of system F. We use a singleton set $\mathfrak{C} = \{1\}$ to treat the rule $(\Box, \Box, \Box)$ inside set theory. For every sort s we take $\mathfrak{A}^{\Uparrow}(s) = \mathfrak{A}_{\Downarrow}(s) = \mathfrak{A}(s)$ and thus $\Uparrow_s = \Downarrow_s = Id_{\mathfrak{A}^{\Uparrow}(s)}$. $\mathfrak{A}(*)$ is the set of saturated degenerated Λ-sets. $\mathfrak{A}(\Box)$ is constructed as the union of all level_n for $n \in \omega^+$, where ω^+ is the set of strictly positive natural numbers.

1. level_1 is the singleton $\{\mathfrak{A}(*)\}$,

2. $\mathsf{level}_{\leq n}$ is defined as the union of all level_k for $1 \leq k \leq n$,

3.
$$\begin{array}{rcl} \mathsf{level}_{n+1} & = & \{\Pi(X,Y), X \in \mathfrak{A}(*), Y_\alpha \in \mathsf{level}_n\} \\ & \cup & \{\Pi(X,Y), X \in \mathsf{level}_n, Y_\alpha \in \mathsf{level}_{\leq n}\} \\ & \cup & \{\Pi(X,Y), X \in \mathsf{level}_{\leq n}, Y_\alpha \in \mathsf{level}_n\} \end{array}$$

We check easily that the level_n are disjoint sets. Let us introduce the equivalence relations:

1. $\left\| \begin{array}{c} 1 \\ \mathfrak{A}(*) \end{array} \right\|$ relates every two elements of $\mathfrak{A}(*)$, and $\left| \begin{array}{c} 1 \\ \mathfrak{A}(*) \end{array} \right|$ relates every two indexes $\emptyset$ of saturated degenerated Λ-set $X, X' \in \mathfrak{A}(*)$,

2. two elements of $\mathfrak{A}^{\Uparrow}(\Box)$ are related by $\left\| \begin{array}{c} 1 \\ \mathfrak{A}(\Box) \end{array} \right\|$ if and only if they are in the same set level_n,

3. every two indexes α and α' of X and X' in $\mathfrak{A}^{\Uparrow}(\Box)$ are related by $\left| \begin{array}{c} 1 \\ \mathfrak{A}(\Box) \end{array} \right|$.

The isos
$$\downarrow_{\Pi(X,Y)}: \Pi(X,Y) \to \Pi_{\downarrow}(X,Y)$$
are defined:

1. as in system F for the rules $(*,*,*)$ and $(\Box,*,*)$

2. as the identity $\Pi(X,Y) = \Pi_{\downarrow}(X,Y)$ for the rules $(*,\Box,\Box)$ and $(\Box,\Box,\Box)$.

Remark that the Λ-iso $\downarrow_{\Pi(X,Y)}$ does not depend on the rules because $\mathfrak{A}^{\Uparrow}(*)$ and $\mathfrak{A}^{\Uparrow}(\Box)$ are disjoint sets.
Let us check that the definition fulfills our conditions. First, conditions 2(2) and 4 are trivial ; condition 2(1) means $\left\| \begin{array}{c} 1 \\ \mathfrak{A}^{\Uparrow}(*) \end{array} \right\|$ and $\left| \begin{array}{c} 1 \\ \mathfrak{A}^{\Uparrow}(\Box) \end{array} \right|$ are identical on $\mathfrak{A}^{\Uparrow}(*) = \mathfrak{A}_{\Downarrow}(*)$, which is true.

On the other hand, conditions 3(1) and 3(2) are true on the rules $(*,*,*)$ and $(\Box,*,*)$ because $\left\| \begin{array}{c} 1 \\ \mathfrak{A}(*) \end{array} \right\|$ and $\left| \begin{array}{c} 1 \\ \mathfrak{A}(*) \end{array} \right|$ relate all elements and indexes of elements of $\mathfrak{A}(*)$, respectively. Condition 1(3) is true on $(*,*,*)$ and $(\Box,*,*)$ for the same reason as in system F.

At that point, let us check conditions 3(1), 3(2) and 1(3) on the rules $(*,\Box,\Box)$ and $(\Box,\Box,\Box)$. Condition 3(1) is true because the relation $\left\| \begin{array}{c} 1 \\ \mathfrak{A}(\Box) \end{array} \right\|$ mirrors the levels of $\mathfrak{A}(\Box)$. In fact, a product $\Pi(X,Y)$ is in level_p when there are natural numbers m and n such that:

- $X \in \mathsf{level}_m$ and $Y_\alpha \in \mathsf{level}_n$ for any $\alpha \sqsubset X$: then $p = max(m,n)+1$,
- or $X \in \mathfrak{A}^{\Uparrow}(*)$ and $Y_\alpha \in \mathsf{level}_n$ for any $\alpha \sqsubset X$: then $p = n+1$.

Condition 3(2) is true for another simple reason. Suppose that
$$\Pi(X,Y) \left\| \begin{array}{c} 1 \\ \Pi(\mathfrak{A}^{\Uparrow}(s_1), \mathfrak{A}^{\Uparrow}(\Box)) \end{array} \right\| \Pi(X',Y')$$

for $s_1 = *$ or $s_1 = \square$. Remark (see points 1 and 3 in our definition of equivalence) that all indexes in $\alpha \sqsubset X$, $\alpha' \sqsubset X'$ and indexes $\beta \sqsubset Y_\alpha$ and $\beta' \sqsubset Y_{\alpha'}$ are equivalent. As a consequence, all indexes f and g of $\Pi(X, Y)$ and $\Pi(X', Y')$ respectively, verify:

$$f \left| \begin{array}{c} 1 \\ \Pi(\mathfrak{A}^{\Uparrow}(s_1), \mathfrak{A}^{\Uparrow}(\square)) \end{array} \right| g$$

On the other hand, by point 2 in the definition of equivalence relations, all indexes in $\Pi_{\downarrow}(X, Y)$ and $\Pi_{\downarrow}(X', Y')$ are equivalent:

$$\downarrow_{\Pi(X,Y)} \langle f \rangle \left| \begin{array}{c} 1 \\ \mathfrak{A}^{\Uparrow}(\square) \end{array} \right| \downarrow_{\Pi(X',Y')} \langle g \rangle$$

The condition 3(2) follows.
Let us check condition 1(3) on $(*, \square, \square)$ and $(\square, \square, \square)$. It is of the highest importance here that every two indexes α and α' of a Λ-set $X \in \mathfrak{A}^{\Uparrow}(s_1)$ are related by $\left| \begin{array}{c} 1 \\ \mathfrak{A}^{\Uparrow}(s_1) \end{array} \right|$ — for $s_1 = *$ or $s_1 = \square$. As a consequence, if $(Y_\alpha)_{\alpha \in X_0}$ is a family of elements in $\mathfrak{A}(\square)$ such that

$$\forall (\alpha, \alpha') \in X_0^2 . \alpha \left| \begin{array}{c} 1 \\ \mathfrak{A}^{\Uparrow}(s_1) \end{array} \right| \alpha' \Longrightarrow Y_\alpha \left\| \begin{array}{c} 1 \\ \mathfrak{A}^{\Uparrow}(\square) \end{array} \right\| Y_{\alpha'}$$

then all Y_α's are on the same level level_n. It follows that $\Pi(X, Y)$ is an element of level_{n+1} and as such, an element of $\mathfrak{A}(\square)$.

6.3 ECC

The Extended Calculus of Construction is defined as a PTS by:

$$\mathcal{S} \equiv \{*, \square_i \mid i \in \omega^+\} \qquad \mathcal{A} \equiv \{(*, \square_i), (\square_i, \square_{i+1}) \mid i \in \omega^+\}$$

$$\mathcal{R} \equiv \{(*, *, *), (\square_i, *, *), (*, \square_i, \square_i), (\square_j, \square_k, \square_m) \mid i, j, k \in (\omega^+)^3, m = max(j, k)\}$$

The construction of the $\mathfrak{A}(\square_i)$'s extends the construction of $\mathfrak{A}(\square)$ in the case of ECC. Here, $\mathfrak{C}$ is the set ω^+. For every sort s we take $\mathfrak{A}^{\Uparrow}(s) = \mathfrak{A}_{\Downarrow}(s) = \mathfrak{A}(s)$ and thus $\Uparrow_s = \Downarrow_s = Id_{\mathfrak{A}^{\Uparrow}(s)}$. Again, the set $\mathfrak{A}(*)$ is the set of saturated degenerated Λ-sets. The sets $\mathfrak{A}(\square_i)$'s are defined as the union of all $\mathsf{level}_{(i,n)}$ for $n < \omega$:

1. $\mathsf{level}_{(1,0)}$ is the singleton $\{\mathfrak{A}(*)\}$,
2. $\mathsf{level}_{\leq(i,n)}$ is defined as the union of all $\mathsf{level}_{(j,p)}$ for (j, p) lexicographically[3] less than (i, n),
3. $$\begin{array}{rcl} \mathsf{level}_{(i,n+1)} & = & \{\Pi(X, Y), X \in \mathfrak{A}(*), Y_\alpha \in \mathsf{level}_{(i,n)}\} \\ & \cup & \{\Pi(X, Y), X \in \mathsf{level}_{(i,n)}, Y_\alpha \in \mathsf{level}_{\leq(i,n)}\} \\ & \cup & \{\Pi(X, Y), X \in \mathsf{level}_{\leq(i,n)}, Y_\alpha \in \mathsf{level}_{(i,n)}\} \end{array}$$
4. $\mathsf{level}_{(i+1,0)}$ is the singleton $\{\mathfrak{A}(\square_i)\}$.

All sets $\mathsf{level}_{(i,n)}$ are disjoint sets. In the case of CC we were able to give a direct definition of the relations $\left| \begin{array}{c} 1 \\ \mathfrak{A}^{\Uparrow}(\square) \end{array} \right|$ and $\left\| \begin{array}{c} 1 \\ \mathfrak{A}^{\Uparrow}(\square) \end{array} \right\|$ in terms of the levels in $\mathfrak{A}(\square)$. This would be very

[3] That is $j < i$ or ($j = i$ and $p \leq n$).

hard indeed in the case of ECC. As a consequence at some point the definition of $\left|\begin{matrix} j \\ \mathfrak{A}^{\Uparrow}(s)\end{matrix}\right|$ and $\left\|\begin{matrix} j \\ \mathfrak{A}^{\Uparrow}(s)\end{matrix}\right\|$ for $j \in \mathfrak{C}$ and $s \in \mathcal{S}$ makes use of an induction argument on the construction steps $\mathsf{level}_{(i,n)}$.

For the universe $\mathfrak{A}(*)$

$\left\|\begin{matrix} j \\ \mathfrak{A}(*)\end{matrix}\right\|$ relates all elements of $\mathfrak{A}(*)$, and $\left|\begin{matrix} j \\ \mathfrak{A}(*)\end{matrix}\right|$ relates all indexes $\emptyset$ of saturated degenerated Λ-set $X, X' \in \mathfrak{A}(*)$,

For the universe $\mathfrak{A}(\Box_i)$ when $i < j$

$\left\|\begin{matrix} j \\ \mathfrak{A}(\Box_i)\end{matrix}\right\|$ relates all elements X and X' of $\mathfrak{A}^{\Uparrow}(\Box_i)$ and $\left|\begin{matrix} j \\ \mathfrak{A}(\Box_i)\end{matrix}\right|$ relates every two indexes $\alpha \sqsubset X$ and $\alpha \sqsubset X'$.

For the universe $\mathfrak{A}(\Box_j)$

Two elements X and X' of $\mathfrak{A}^{\Uparrow}(\Box_j)$ are related by $\left\|\begin{matrix} j \\ \mathfrak{A}(\Box_j)\end{matrix}\right\|$ if and only they are in the same set $\mathsf{level}_{(j,n)}$. $\left|\begin{matrix} j \\ \mathfrak{A}(\Box_j)\end{matrix}\right|$ relates every two indexes $\alpha \sqsubset X$ and $\alpha' \sqsubset X'$ in any two Λ-sets X, X' in $\mathfrak{A}(\Box_j)$.

For the universe $\mathfrak{A}(\Box_i)$ when $i > j$

The two relations $\left|\begin{matrix} j \\ \mathfrak{A}(\Box_i)\end{matrix}\right|$ and $\left\|\begin{matrix} j \\ \mathfrak{A}(\Box_i)\end{matrix}\right\|$ are defined by induction on the construction steps $\mathsf{level}_{(i,n)}$. The first step in the construction is to impose that

1. two Λ-sets Z and Z' related by $\left\|\begin{matrix} j \\ \mathfrak{A}(\Box_i)\end{matrix}\right\|$ are at the same level $\mathsf{level}_{(i,n)}$,
2. two indexes $\alpha \sqsubset Z$ and $\alpha' \sqsubset Z'$ related by $\left|\begin{matrix} j \\ \mathfrak{A}(\Box_i)\end{matrix}\right|$ have their Λ-sets Z and Z' at the same level $\mathsf{level}_{(i,n)}$.

Thus, it is enough to construct $\left\|\begin{matrix} j \\ \mathfrak{A}(\Box_i)\end{matrix}\right\|$ and $\left|\begin{matrix} j \\ \mathfrak{A}(\Box_i)\end{matrix}\right|$ at each level $\mathsf{level}_{(i,n)}$. Let there be two elements Z and Z' of $\mathsf{level}_{(i,n)}$:

1. if $n = 0$ then by construction of $\mathfrak{A}(\Box_i)$, Z and Z' are equal to $\mathfrak{A}_{\Downarrow}(\Box_{i-1})$ and thus related by $\left\|\begin{matrix} j \\ \mathfrak{A}(\Box_i)\end{matrix}\right\|$. Let there be two indexes f and g of $\mathfrak{A}_{\Downarrow}(\Box_{i-1})$. Then

$$f \left|\begin{matrix} j \\ \mathfrak{A}(\Box_i)\end{matrix}\right| g \quad \text{if and only if} \quad f \left\|\begin{matrix} j \\ \mathfrak{A}(\Box_{i-1})\end{matrix}\right\| g$$

2. if $n = p + 1$ then Z and Z' are of the form:

$$Z = \Pi(X, Y) \quad \text{and} \quad Z' = \Pi(X', Y')$$

where X, X' and $Y_\alpha, Y'_{\alpha'}$ are elements of $\mathsf{level}_{\leq(i,p)}$, for any $\alpha \sqsubset X$ and $\alpha' \sqsubset X'$. We impose that the relation $\left\| \begin{matrix} j \\ \mathfrak{A}(\Box_i) \end{matrix} \right\|$ only relates the Λ-sets Z and Z' when there are two sorts s_1 and s_2 among $\{*, \Box_m \mid m \leq i\}$ such that

   - both Λ-sets X and X' elements of $\mathfrak{A}(s_1)$,
   - for any $\alpha \sqsubset X$ and $\alpha' \sqsubset X'$, both Λ-sets Y_α and $Y_{\alpha'}$ are elements of $\mathfrak{A}(s_2)$.

   The relation $\left\| \begin{matrix} j \\ \mathfrak{A}^{\Uparrow}(\Box_i) \end{matrix} \right\|$ is defined as follows:

$$\Pi(X, Y) \left\| \begin{matrix} j \\ \mathfrak{A}^{\Uparrow}(\Box_i) \end{matrix} \right\| \Pi(X', Y')$$

   if and only if:

$$X \left\| \begin{matrix} j \\ \mathfrak{A}^{\Uparrow}(\Box_i) \end{matrix} \right\| X'$$

   and for any $\alpha \sqsubset X$ and $\alpha' \sqsubset X'$,

$$\alpha \left| \begin{matrix} j \\ \mathfrak{A}(s_1) \end{matrix} \right| \alpha' \Longrightarrow Y_\alpha \left\| \begin{matrix} j \\ \mathfrak{A}(s_2) \end{matrix} \right\| Y'_{\alpha'}$$

3. the relation $\left| \begin{matrix} j \\ \mathfrak{A}(\Box_i) \end{matrix} \right|$ is defined on any index $f \sqsubset Z$ and $g \sqsubset Z'$ with $Z, Z' \in \mathsf{level}_{(i,n)}$ as follows:

$$f \left| \begin{matrix} j \\ \mathfrak{A}(\Box_i) \end{matrix} \right| g$$

   if and only if

$$Z \left\| \begin{matrix} j \\ \mathfrak{A}(\Box_i) \end{matrix} \right\| Z' \quad \text{and} \quad f \left| \begin{matrix} j \\ \Pi(\mathfrak{A}(s_1), \mathfrak{A}(s_2)) \end{matrix} \right| g$$

Once having expressed the equivalence relation, we introduce the isos

$$\downarrow_{\Pi(X,Y)} : \Pi(X, Y) \to \Pi_\downarrow(X, Y)$$

which are defined like in CC:

1. as in system F for the rules $(*, *, *)$ and $(\Box_i, *, *)$
2. as the identity $\Pi(X, Y) = \Pi_\downarrow(X, Y)$ for the rules $(*, \Box_i, \Box_i)$ and $(\Box_j, \Box_k, \Box_m)$ with $m = max(k, m)$.

Again, the Λ-iso $\downarrow_{\Pi(X,Y)}$ does only depend on X and Y since $\mathfrak{A}^{\Uparrow}(*)$ and the $\mathfrak{A}^{\Uparrow}(\Box_i)$'s are all disjoint.
Let us check the conditions on our model. Conditions 1(1), 1(2) and 4 are trivial, condition 2(2) is true because the $\mathfrak{A}^{\Uparrow}(s)$'s are disjoint and condition 2(1) is the consequence of the fact that

1. $\left\| \begin{array}{c} j \\ \mathfrak{A}^{\Uparrow}(*) \end{array} \right\|$ and $\left| \begin{array}{c} 1 \\ \mathfrak{A}_{\Downarrow}(\Box_1) \end{array} \right|$ are the same relation on $\mathfrak{A}^{\Uparrow}(*) = \mathfrak{A}_{\Downarrow}(*)$,

2. $\left\| \begin{array}{c} j \\ \mathfrak{A}^{\Uparrow}(\Box_i) \end{array} \right\|$ and $\left| \begin{array}{c} j \\ \mathfrak{A}_{\Downarrow}(\Box_i) \end{array} \right|$ are the same relation on $\mathfrak{A}^{\Uparrow}(\Box_i) = \mathfrak{A}_{\Downarrow}(\Box_i)$, for $i, j < \omega$.

Condition 1(3) is true:

1. on the rules $(*, *, *)$ and $(\Box_i, *, *)$ because every product $\Pi(X, Y)$ of saturated degenerated Λ-sets Y_α is collapsed by $\downarrow_{\Pi(X,Y)}$ to the saturated degenerated Λ-set $\Pi_{\downarrow}(X, Y)$;

2. on the rules $(\Box_i, \Box_j, \Box_j)$ when $i \leq j$ because the equivalence relation $\left| \begin{array}{c} j \\ \mathfrak{A}(\Box_i) \end{array} \right|$ is designed so as to relate every two indexes α and α' in a Λ-set X element of $\Box_i$. As a consequence, if $(Y_\alpha)_{\alpha \in X_0}$ is a family of elements in $\mathfrak{A}(\Box)$ such that
$$\forall(\alpha, \alpha') \in X_0^2 . \alpha \left| \begin{array}{c} 1 \\ \mathfrak{A}^{\Uparrow}(s_1) \end{array} \right| \alpha' \Longrightarrow Y_\alpha \left\| \begin{array}{c} 1 \\ \mathfrak{A}^{\Uparrow}(\Box) \end{array} \right\| Y_{\alpha'}$$
then all Y_α's are in the same level level_n. It follows that $\Pi(X, Y)$ is an element of level_{n+1} and as such, an element of $\mathfrak{A}(\Box)$.

3. on the rules $(\Box_j, \Box_i, \Box_j)$ for $i \leq j$ because all products $\Pi(X, Y)$ where X is element of $\mathsf{level}_{(j,n)}$ and $(Y_\alpha)_{\alpha \sqsubset X}$ is a family of elements of $\mathfrak{A}(\Box_i)$ indexed by indexes of X, are in $\mathsf{level}_{(j,n+1)}$, and hence in $\mathfrak{A}(\Box_j)$.

Let us check condition 3 on the relations $\left| \begin{array}{c} j \\ \mathfrak{A}(s) \end{array} \right|$ and $\left\| \begin{array}{c} j \\ \mathfrak{A}(s) \end{array} \right\|$ for a given element j of $\mathfrak{C}$:

For the rules (s_1, s_2, s_3) **where** $s_2 = s_3 = *$ **or** $s_3 = \Box_i$ **with** $i < j$

The conditions 3(1) and 3(2) are true here for the same reasons as in CC:

- $\left\| \begin{array}{c} j \\ \mathfrak{A}(s_2) \end{array} \right\|$ and $\left\| \begin{array}{c} j \\ \mathfrak{A}(s_3) \end{array} \right\|$ relate all elements of $\mathfrak{A}(s_2)$ and $\mathfrak{A}(s_3)$,
- $\left| \begin{array}{c} j \\ \mathfrak{A}(s_2) \end{array} \right|$ and $\left| \begin{array}{c} j \\ \mathfrak{A}(s_3) \end{array} \right|$ relate all indexes of elements of $\mathfrak{A}(s_2)$ and $\mathfrak{A}(s_3)$.

For the rules $(s_1, s_2, \Box_j)$

The proof of conditions 3(1) follows the same line as in the case of CC: A product $\Pi(X, Y)$ is in $\mathsf{level}_{(j,p)}$ if and only if there are (i_1, n_1) and (i_2, n_2) such that

1. $X \in \mathsf{level}_{(i_1,n_1)}$ and $Y_\alpha \in \mathsf{level}_{(i_2,n_2)}$ for any $\alpha \sqsubset X$, and (j, p) is the (lexicographical) maximum of (i_1, n_1) and (i_2, n_2),

2. or $X \in \mathfrak{A}^{\Uparrow}(*)$ and $Y_\alpha \in \mathsf{level}_{(j,p-1)}$ for any $\alpha \sqsubset X$.

The reasons for condition 3(2) are the same as in the previous case since all indexes of elements of $\mathfrak{A}(\Box_j)$ are related by $\left| \begin{array}{c} j \\ \mathfrak{A}(\Box_j) \end{array} \right|$.

For the rules $(s_1, s_2, \Box_i)$ **for** $i > j$

The inductive definition of $\left\| \begin{array}{c} j \\ \mathfrak{A}(\Box_i) \end{array} \right\|$ and $\left| \begin{array}{c} j \\ \mathfrak{A}(\Box_i) \end{array} \right|$ for $i > j$ follows explicitly the requirements of conditions 2(1) and 3. For this reason both conditions are fulfilled.

6.4 System U^-

It is well-known that Girard's system U^- yields non-normalizable terms, and thus we cannot find a collection of $\mathfrak{A}^{\Uparrow}(s)$ fitting its rules. However, it is reassuring to check that the rules do *not* allow the usual model construction.

As a PTS, system U^- is defined with three sorts $\mathcal{R} \equiv \{*, \Box, \triangle\}$ and the following axioms and rules:
$\mathcal{A} = \{(*, \Box), (\Box, \triangle)\}$ and $\mathcal{R} = \{(*, *, *), (\Box, *, *), (\Box, \Box, \Box), (\triangle, \Box, \Box)\}$.

The three first rules are exactly the rules of system F_ω. The last one however is obviously problematic:

- because of the second axiom, we need to have completed the construction of $\mathfrak{A}(\Box)$ in order to define $\mathfrak{A}(\triangle)$,
- on the other hand, because of the last rule, we need to quantify over all elements of $\mathfrak{A}(\triangle)$ while constructing $\mathfrak{A}(\Box)$.

It is obviously not possible to break this vicious circle. In other words, we see how polymorphism cannot be authorized for higher sorts.

6.5 Cyclic F

The following PTS does not seem more expressive than system F. It might however be worth noting that it fits easily in our pattern. $\mathcal{A} = \{(*, \Box), (\Box, *)\}$ and $\mathcal{R} = \{(*, *, *), (\Box, *, *)\}$

$\mathfrak{A}(*)$ is the Λ-set of degenerated Λ-sets. $\mathfrak{A}^{\Uparrow}(\Box)$ is the singleton $\mathfrak{A}(*)$. $\mathfrak{A}_{\Downarrow}(\Box)$ is a degenerated Λ-set. It is easy to finish the proof.

7 The Church-Rosser Property

We now focus on the relation between the labeled PTSs considered in this paper and the usual presentation. The first step is to verify the Church-Rosser property for the first one.

From now on, we suppose given a PTS (i.e. the sets $\mathcal{S}$, $\mathcal{A}$ and $\mathcal{R}$) and we assume it verifies the strong normalization property. We will make another assumption (uniqueness of type) just before lemma 15.

Definition 17 (loose reduction) *Loose reduction (written $\triangleright_l$) is the contextual closure of*

$$\mathtt{app}_{x:A.B}(\lambda_{x:A'.B'}x.M, N) \triangleright_l M[x \setminus N].$$

Again, we write $\triangleright_l^*$ (respectively $=_l$) for the reflexive-transitive (respectively reflexive transitive and symmetric) closure of $\triangleright_l$.

Lemma 13 *The $\triangleright_l$ property enjoys the Church-Rosser property on pseudo-terms:*

$$\forall t, t' \,.\, t =_l t' \Longrightarrow \exists t'' \,.\, t \triangleright_l^* t'' \wedge t' \triangleright_l^* t''.$$

PROOF The usual Tait–Martin-Lof style proofs apply. ∎

Lemma 14 *Let* $\mathsf{app}_{x:A.B}(\lambda_{x:A'.B'}x.M, N)$ *be a well-typed term in some context* Γ. *We have* $A =_l A'$ *and* $B =_l B'$.

PROOF Looking at the derivation, it is clear that $(x : A)B =_\Gamma (x : A')B'$, and thus we also have $(x : A)B =_l (x : A')B'$. The previous lemma ensures that there exists a $(x : A'')B''$ which is a common (loose) reduct of $(x : A)B$ and $(x : A')B'$. Hence, $A \rhd_l^* A''$, $A' \rhd_l^* A''$ $B \rhd_l^* B''$ $B \rhd_l^* B''$. ∎

Theorem 3 (Church-Rosser) *Let there be two derivable judgements* $\Gamma \vdash t : T$ *and* $\Gamma \vdash t' : T'$, *such that* $t =_l t'$ *and* t *and* t' *are in normal form (for* $\rhd_\beta$*). Then* $t = t'$.

PROOF We proceed by mutual induction over the size of t and t'. We start by proving that t (respectively t') is in normal form for $\rhd_l$: suppose t yields a loose redex, i.e. contains a subterm of the form

$$\mathsf{app}_{x:A.B}(\lambda_{x:A'.B'}x.M, N)$$

by the previous lemma, we have $A =_l A'$ and $B =_l B'$ and by induction hypothesis $A = A'$ and $B = B'$. But then we have exhibited and tight redex, and this is impossible since t is in normal form.

Now lemma 13 states there exists t'' such that $t \rhd_l^* t''$ and $t' \rhd_l^* t''$. But since t and t' are normal with respect to $\rhd_l$, we have $t = t'' = t'$. ∎

Corollary 1 *Let* t *and* t' *be two well-formed terms in a same context* Γ. *If* $t =_l t'$, *then* t *and* t' *have a common unique normal form.*

What now follows is a little boring and straightforward, but necessary to extend the previous results to usual PTSs.

We can now define the usual PTSs and state our equivalence theorem. The *unlabeled terms* are defined by the following grammar:

$$M \quad := \quad x \mid s \mid (M\ M) \mid \lambda x : M.M \mid (x : M)M.$$

We overload the symbol $\rhd_l$ (respectively $\rhd_l^*$, etc) by defining reduction on unlabeled terms:

$$(\lambda x : A.M\ N) \rhd_l M[x \setminus N].$$

The rules for unlabeled judgements $\Gamma \vdash_l M : T$ are then defined as usual (see [2] for example). The main point is of course that the conversion rule now goes:

$$(\textsc{conv})\ \frac{\Gamma \vdash_l M : A \Gamma \vdash_l B : s A =_l B}{\Gamma \vdash_l M : B}$$

Definition 18 (Unstripped term) *We define the map* $||\_||$ *from terms to the usual, naked terms of PTS's:*

$$\begin{array}{rcl} ||x|| & \equiv & x \\ ||s|| & \equiv & s \\ ||\mathsf{app}_{A.B}(M, N)|| & \equiv & (||M||\ ||N||) \\ ||\lambda_{x:A.B}x.M|| & \equiv & \lambda x : ||A||.||t|| \end{array}$$

It is straightforward to extend this map to contexts.

The following results are quite immediate:

- $t =_\beta t' \Longrightarrow ||t|| =_l ||t'||$

- $t =_l t' \Longrightarrow ||t|| =_l ||t'||$
- $\Gamma \vdash t : T \Longrightarrow ||\Gamma|| \vdash_l ||t|| : ||T||$.

But we are mainly interested in the reverse assertion, i.e. theorem 4. Since we do not want to get lost in technical details without much interest, we make the following assumption.
Assumption *If the judgements $\Gamma \vdash_l t : T$ and $\Gamma \vdash_l t : T'$ are derivable, then $T =_l T'$.*

The first thing to check is:

Lemma 15 *Let $\Gamma \vdash t : T$ and $\Gamma \vdash t' : T'$ be two derivable (tight) judgements. If $||t|| =_l ||t'||$, then $t =_\beta t'$.*

Proof Thanks to strong normalization, we might restrict ourselves to the case were t and t' are both normal. Thanks to previous results, this implies that $||t|| = ||t'||$. We may then proceed by mutual structural induction over t and t'. The only non-trivial cases are:

- $t = \lambda_{x:A.B} x.M$ and $t' = \lambda_{x:A'.B'} x.M'$. Since both terms are normal and $=_l$-convertible, we have $A =_l A'$, $B =_l B'$ and $M =_l M'$. The induction thus implies that $A = A'$ and also $B = B'$ (respectively $M = M'$), since B and B' (respectively M and M') are well-typed in $\Gamma, x : A$.
- $t = \mathtt{app}_{x_1:A_1.B_1}(\mathtt{app}_{x_2:A_2.B_2}(\ldots \mathtt{app}_{x_n:A_n.B_n}(y, M_n)\ldots, M_2), M_1)$
  and
  $t' = \mathtt{app}_{x'_1:A'_1.B'_1}(\mathtt{app}_{x'_2:A'_2.B'_2}(\ldots \mathtt{app}_{x'_n:A'_n.B'_n}(y, M'_n)\ldots, M'_2), M'_1)$.
  We know that $(x_n : A_n)B_n$ and $(x'_n : A'_n)B'_n)$ are both correct types for y in $||\Gamma||$. They are therefore convertible and the induction hypothesis applies. We also know that $||M_n|| = ||M'_n||$ and may apply the induction hypothesis. We iterate these two steps n times to conclude $t = t'$. ∎

Theorem 4 *Given a derivable judgement $\Gamma \vdash_l t : T$, there exists a derivable judgement $\Delta \vdash u : V$ such that $||\Delta|| = \Gamma$, $||u|| = t$ and $||V|| = T$.*

Proof By induction over the derivation. All steps are straightforward but the conversion rule, which is taken care by the previous lemma. ∎

Corollary 2 *If $\Gamma \vdash_l t : T$ is derivable, then t and T are strongly normalizing with respect to $\triangleright_l$.*

8 Conclusion

We hope that this work might shed some new light on the interaction between model construction and strong normalization, which is the syntactical approach to logical consistency. We realize that the definition of the interpretation, as well as the construction of the universes for particular systems is complicated by the presence of the equivalence relations in the $\mathfrak{A}^{\Uparrow}(s)$. This seems the price to pay for avoiding the use of inaccessible cardinals. We however conjecture that inaccessible cardinals are necessary to prove normalization for more powerful theories, for instance when adding full inductive types to ECC. This leads to possible directions for future work:

- Give a clean categorical setting to this work, since most of the constructions seem to be of categorical nature.
- Extend this approach to other theories, especially to inductive types.
- Understand to what extent these construction might be used for more traditional applications of models, like consistency for additional axioms (excluded middle, choice) or new reductions.

Acknowledgements

We would like to thank Thorsten Altenkirch, Martin Hofmann, Ralph Loader and Thomas Streicher for useful comments and suggestions on earlier versions of this work.

References

[1] T. Altenkirch. *Constructions, Inductive Types and Strong Normalization.* Ph.D. Thesis, University of Edinburgh, 1993.

[2] H. Barendregt. Lambda Calculi with Types. In *Handbook of Logic in Computer Science*, Vol II, Elsevier, 1992

[3] G. Barthe, P.-A. Melliès. On the Subject Reduction property for algebraic type systems. In *Proceedings CSL'96*, LNCS 1258, Springer Verlag, 1996.

[4] G. Dowek, G. Huet and B. Werner. On the Definition of the η-long Normal Form in Type Systems of the Cube. Submitted to publication. See also `http://pauillac.inria.fr/~werner/`, 1996.

[5] H. Geuvers et M.-J. Nederhof. A modular proof of strong normalization for the Calculus of Constructions. *Journal of Functional Programming*, 1 (2):155–189, 1991.

[6] J.-Y. Girard. *Interprétation fonctionnelle et élimination des coupures de l'arithmétique d'ordre supérieur*, Thèse d'Etat, Université Paris 7, 1972.

[7] J. W. Klop, *Combinatory Reduction Systems.* Ph.D. Thesis, Utrecht University, 1980.

[8] G. Longo and E. Moggi. Constructive Natural Deduction and its ω-set Interpretation.

[9] Z. Luo. *An Extended Calculus of Constructions.* Ph.D. Thesis, University of Edinburgh, 1990.

[10] P. Martin-Löf. *Intuitionistic Type Theory.* Studies in Proof Theory, Bibliopolis, 1984.

[11] W. W. Tait. A realizability interpretation of the theory of species. In *Logic Colloquium*, R. Parikh Ed. LNM 453, Springer-Verlag, 1975.

[12] J. Terlouw. Strong Normalization in Type Systems: a model theoretical approach. In *Dirk van Dalen Festschrift*, Henk Barendregt, Marc Bezem and Jan Willem Klop Eds. Dept. of Philosophy, Utrecht University, 1993.