Higher-Order Superposition for Dependent Types

Roberto Virga
May 9, 1995
CMU-CS-95-150

School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213

Abstract

In this paper we extend the higher-order critical pair criterion, as described in [9], to the LF framework [10], a calculus with dependent types. The notion of dependence relation is introduced, and used to restrict rewriting to those cases where well-typedness is preserved.

This work was supported by NSF Grant CCR-9303383

The views and conclusions contained in this document are those of the author and should not be interpreted as representing the official policies, either expressed or implied, of NSF or the U.S. government

Keywords: meta logic, logical frameworks, rewriting, superposition, lambda calculus, type theory

1. Historical background

In the study of Term Rewriting Systems (TRS), the two key properties that we are mostly interested with are *termination* and *confluence*, which imply existence and uniqueness, respectively, of normal forms. In presence of these conditions, the test for convertibility of two terms, undecidable in the general case, reduces to a simple test for equality of their respective normal forms.

One of the central results in this study is certainly the Critical Pair Lemma for first-order TRSes [6], which provides a computational method to check for *local confluence* in a TRS, together with a way to extend any TRS to an equivalent locally confluent one. This fact, in conjunction with Newman's lemma [4], which says that in presence of termination local confluence and confluence coincide, has led in the last decade to a series of important breakthroughs in the field of automated equational reasoning.

Until fairly recently, all attempts to lift the theory of TRSes to the higher-order case seemed to be undermined by the presence of some well-known negative results in this setting, first among these the undecidability of the general unification problem. The first important advance in order to overcome these difficulties is due to D. Miller [8], who identified a subclass of higher-order terms, called *higher-order patterns* for which the unification problem is decidable, and moreover uniqueness of most general unifiers hold. Making use of this result, T. Nipkow [7, 9] was able to state and prove an analogous of the Critical Pair Lemma for the case of higher-order, simply-typed TRSes. Nipkow's Higher Order Term Rewriting Systems (HTRS) are similar to Klop's Combinatory Reduction Systems (CRS). For a detailed analysis of the relation between these two, see [16]. In this paper we extend higher-order rewriting to a calculus with dependent types, as presented in [3]. Our approach in the proof of most results, notably the Critical Pair Lemma, will follow Nipkow's one, though significant modifications are necessary due to the fact that here terms may appear inside types.

2. Preliminaries

Definition 2.1. The LF calculus is a three-level calculus for *terms*, *type families*, and *kinds*

$$\begin{array}{llll} \textit{Kinds} & K & := & \mathrm{type} \mid \Pi x : A.K \\ \textit{Families} & A & := & a \mid \Pi x : A.B \mid AM \\ \textit{Terms} & M & := & c \mid x \mid \lambda x : A.M \mid MN \end{array}$$

In the following, K denotes kinds, A, B families, M, N terms; a stands for constants at the level of type families, c for constants at the level of terms, x, y, z for variables.

We assume the usual notions of α, β and η-reduction. All these notions, although defined on terms, extend naturally by congruence to type families and kinds. All objects will be considered equal modulo α-conversion.

We denote by $\to_\gamma^{RF}$, $\to_\gamma^*$ and $=_\gamma$ the reflexive, reflexive-transitive, and reflexive-symmetric-transitive closure, respectively, of $\to_\gamma$, $\gamma \in \{\alpha, \beta, \eta\}$; $\equiv$ is the smallest equivalence relation including $=_\alpha$, $=_\beta$, $=_\eta$.

By $[N/x]M$ ($[N/x]A$, $[N/x]K$ respectively) we intend, as usual, the replacement of all the free occurrences of x by N inside M (A, K, respectively). As usual, α-conversion will be used, if necessary, to ensure the that no free variable occurrence is captured inside the scope of a quantifier.

The notation $\mathcal{FV}(E)$ and $\mathcal{BV}(E)$ is used to denote the set of free and bound variables, respectively, in E, where E may be a term, a type family or a kind.

Definition 2.2. To define the class of well-typed kinds, type families, and terms we make use of signatures and contexts:

$$\begin{array}{llll} \textit{Signatures} & \Sigma & := & \cdot \mid \Sigma, a : K \mid \Sigma, c : A \\ \textit{Contexts} & \Gamma & := & \cdot \mid \Gamma, x : A \end{array}$$

We will use Γ and Δ to range over contexts.

Well-formed terms of a given type, type families, and kinds are then formed accordingly to the judgements

$$\Gamma \vdash_\Sigma M : A \ \Gamma \qquad\qquad \vdash_\Sigma A : K$$

$$\Gamma \vdash_\Sigma K \ Kind$$

These in turn are defined in terms of the auxiliary judgements

$$\vdash \Sigma \; Sig$$
$$\vdash_\Sigma \Gamma \; Ctx$$

which specify how valid signatures and contexts are formed.

The rules for the calculus are listed below:

$$\frac{\Sigma(c){=}A}{\Gamma{\vdash_\Sigma}c{:}A} \quad \frac{\Gamma(x){=}A}{\Gamma{\vdash_\Sigma}x{:}A}$$

$$\frac{\Gamma{\vdash_\Sigma}A{:}\mathrm{type} \quad \Gamma{,}x{:}A{\vdash_\Sigma}M{:}B}{\Gamma{\vdash_\Sigma}\lambda x{:}A.M{:}\Pi x{:}A.B}$$

$$\frac{\Gamma{\vdash_\Sigma}M{:}A \quad A{\equiv}B \quad \Gamma{\vdash_\Sigma}B{:}\mathrm{type}}{\Gamma{\vdash_\Sigma}M{:}B}$$

$$\frac{\Gamma{\vdash_\Sigma}M{:}\Pi x{:}A.B \quad \Gamma{\vdash_\Sigma}N{:}A}{\Gamma{\vdash_\Sigma}MN{:}[N/x]B}$$

$$\frac{\Sigma(a){=}K}{\Gamma{\vdash_\Sigma}a{:}K}$$

$$\frac{\Gamma{\vdash_\Sigma}A{:}\Pi x{:}B.K \quad \Gamma{\vdash_\Sigma}M{:}B}{\Gamma{\vdash_\Sigma}AM{:}[M/x]K}$$

$$\frac{\Gamma{\vdash_\Sigma}A{:}\mathrm{type} \quad \Gamma{,}x{:}A{\vdash_\Sigma}B{:}\mathrm{type}}{\Gamma{\vdash_\Sigma}\Pi x{:}A.B{:}\mathrm{type}}$$

$$\frac{}{\Gamma{\vdash_\Sigma}\mathrm{type}\; Kind} \quad \frac{\Gamma{\vdash_\Sigma}A{:}\mathrm{type} \quad \Gamma{,}x{:}A{\vdash_\Sigma}K \; Kind}{\Gamma{\vdash_\Sigma}\Pi x{:}A.K \; Kind}$$

$$\frac{}{\vdash_\Sigma \cdot \; Ctx} \qquad \frac{\vdash_\Sigma\Gamma \; Ctx \quad \Gamma{\vdash_\Sigma}A{:}\mathrm{type}}{\vdash_\Sigma\Gamma{,}x{:}A \; Ctx}$$

$$\frac{\Gamma{\vdash_\Sigma}A{:}K \quad K{\equiv}K' \quad \Gamma{\vdash_\Sigma}K' \; Kind}{\Gamma{\vdash_\Sigma}A{:}K'}$$

$$\frac{}{\vdash \cdot \; Sig}$$

$$\frac{\vdash_\Sigma K \; Kind \quad \vdash\Sigma \; Sig}{\vdash\Sigma{,}a{:}K \; Sig} \quad \frac{\vdash_\Sigma A{:}\mathrm{type} \quad \Gamma{\vdash}\Sigma \; Sig}{\vdash\Sigma{,}c{:}A \; Sig}$$

We will use $M\ \overline{N}$ to denote the repeated application $M\ N_1\ N_2 \ldots\ N_n$; similarly for type families. The notation $[\overline{N}/\overline{x}]$ will stand for the repeated replacement $[N_n/x_n]\ldots[N_1/x_1]$ rather than, as traditionally, for the simultaneous one $[N_1/x_1,\ldots,N_n/x_n]$, which we will not need to use in this paper.

3. Dependency Relations

Differently from the simply-typed lambda-calculus, in the LF calculus replacing a subterm with another of the same type inside a term may affect the type of the overall expression. The reason for this lies in the definition of the rule for application:

$$\frac{\Gamma{\vdash_\Sigma}M{:}\Pi x{:}A.B \quad \Gamma{\vdash_\Sigma}N{:}A}{\Gamma{\vdash_\Sigma}M\ N{:}[N/x]B}$$

If we replace N by another term $\Gamma \vdash_\Sigma N' : A$ we get an expression of a different (and not necessarily equivalent) type:

$$\frac{\Gamma \vdash_\Sigma M : \Pi x{:}A.B \quad \Gamma \vdash_\Sigma N' : A}{\Gamma \vdash_\Sigma M N' : [N'/x]B}$$

Worse than that, the resulting expression may not be well-typed at all. Suppose that the expression above was in turn a subterm in the expression:

$$\frac{\Gamma \vdash_\Sigma M' : \Pi y{:}[N/x]B.C \quad \Gamma \vdash_\Sigma M\ N : [N/x]B}{\Gamma \vdash_\Sigma M'\ (M\ N) : [(M\ N)/y]C}$$

Since in general $\Gamma \vdash_\Sigma M' : \Pi y : [N'/x]B.C$ may not hold, the expression we obtain after the replacement is ill-typed.

This problem is concretely illustrated by the following:

Example 1. Consider the following representation of a fragment of arithmetic:

$$\mathbf{nat} : \mathrm{type}$$

$$\begin{aligned} \mathbf{0} &: \mathbf{nat} \\ \mathbf{s} &: \mathbf{nat} \Rightarrow \mathbf{nat} \\ \mathbf{+} &: \mathbf{nat} \Rightarrow (\mathbf{nat} \Rightarrow \mathbf{nat}) \end{aligned}$$

where we used the notation $A \Rightarrow B$ and $A \Rightarrow K$ for the abstractions $\Pi x : A.B$ and $\Pi x : A.K$ where $x \notin \mathcal{FV}(B)$ and $x \notin \mathcal{FV}(K)$, respectively.

We want now to formalize the (first-order) predicate "n is even", together with some inference rules that allow us to decide if a number is even:

$$\begin{aligned} \mathbf{o} &: \mathrm{type} \\ \mathbf{proof} &: \mathbf{o} \Rightarrow \mathrm{type} \\ \mathbf{even} &: \mathbf{nat} \Rightarrow \mathbf{o} \end{aligned}$$

$$\begin{aligned} \mathbf{even}_0 &: \mathbf{proof}(\mathbf{even}\ \mathbf{0}) \\ \mathbf{even}_{ss} &: \Pi x : \mathbf{nat}.\ \mathbf{proof}(\mathbf{even}\ x) \Rightarrow \mathbf{proof}(\mathbf{even}\ (\mathbf{s}\ (\mathbf{s}\ x))) \\ \mathbf{even}_+ &: \Pi x : \mathbf{nat}.\ \Pi y : \mathbf{nat}.\ \mathbf{proof}(\mathbf{even}\ x) \Rightarrow (\mathbf{proof}(\mathbf{even}\ y) \Rightarrow \mathbf{proof}(\mathbf{even}\ (\mathbf{+}\ x\ y))) \\ \mathbf{even}_{s+} &: \Pi x : \mathbf{nat}.\ \Pi y : \mathbf{nat}.\ \mathbf{proof}(\mathbf{even}\ (\mathbf{+}\ x\ y)) \Rightarrow \mathbf{proof}(\mathbf{even}\ (\mathbf{+}\ (\mathbf{s}\ x)\ (\mathbf{s}\ y))) \end{aligned}$$

In this signature, for example, the term

$$\mathbf{even}_+\ \mathbf{0}\ (\mathbf{+}\ \mathbf{0}\ \mathbf{0})\ \mathbf{even}_0\ (\mathbf{even}_+\ \mathbf{0}\ \mathbf{0}\ \mathbf{even}_0\ \mathbf{even}_0)$$

is well typed, but rewriting $(\mathbf{+}\ \mathbf{0}\ \mathbf{0}) \to \mathbf{0} : \mathbf{nat}$ we get

$$\mathbf{even}_+\ \mathbf{0}\ \mathbf{0}\ \mathbf{even}_0\ (\mathbf{even}_+\ \mathbf{0}\ \mathbf{0}\ \mathbf{even}_0\ \mathbf{even}_0)$$

which is not.

In defining a notion of rewriting, we must therefore be careful to rule out all these pathological cases that lead to ill-typed expressions. A natural way to do this is to make use of dependency relations.

A signature Σ implicitly describes a hierarchy of type families: more complex families may depend on terms belonging to simpler ones defined before. For example, formalizing a proof system, one may start by defining basic type families, one for terms and the other for formulas; the family of proofs may depend on formulas, and, if some predicate symbols are defined, through these on terms. Dependency relations formalize mathematically this idea by defining preorders over type constants, constructed by looking (recursively) at the signature.

The idea of using dependency relations is not completely new in LF. They have also been used in [13] to prove well-foundedness of proofs by structural induction. In this paper, we will use them to obtain information about the type of objects appearing inside types, and in turn we will use this information to define a notion of rewriting which is sound with respect to type checking.

Definition 3.1. Define

$$\mathrm{head}(\Pi x_1 : A_1 \dots \Pi x_n : A_n.a\overline{M}) = a,$$

let Σ_0 be a signature, a pair $\prec_0 = (\prec_0^A, \prec_0^M)$ of binary transitive relations over the set of type constants of Σ_0 is called a dependency relation if it satisfies the following conditions:

- $a_i \prec_0^A a$ if $\Sigma_0(a) = \Pi x_1 : A_1 \dots . \Pi x_n : A_n.\mathrm{type}$, $\mathrm{head}(A_i) = a_i$, $1 \le i \le n$;
- $a \prec_0^A a'$ if, for some b, $a \prec_0^A b \prec_0^M a'$ or $a \prec_0^M b \prec_0^A a'$;
- $a \prec_0^M b$ if $a \prec_0^A b$;
- $\vdash^{\prec_0} \Sigma_0\ Sig$;

where $\vdash^{\prec_0} \Sigma\ Sig$ is defined (recursively) by the judgements

$$\frac{}{\vdash^{\prec_0} \cdot\ Sig}$$

$$\frac{\vdash_\Sigma K\ Kind \quad \vdash^{\prec_0} \Sigma\ Sig}{\vdash^{\prec_0} \Sigma, a{:}K\ Sig} \qquad \frac{\vdash_\Sigma^{\prec_0} A{:}\mathrm{type} \quad \vdash^{\prec_0} \Sigma\ Sig}{\vdash^{\prec_0} \Sigma, c{:}A\ Sig}$$

$$\frac{\Sigma(a) = K}{\Gamma \vdash_\Sigma^{\prec_0} a{:}K}$$

$$\frac{\Gamma \vdash_\Sigma^{\prec_0} A{:}\Pi x{:}B.K \quad \Gamma \vdash_\Sigma^{\prec_0} M{:}B}{\Gamma \vdash_\Sigma^{\prec_0} A\ M{:}[M/x]K}$$

$$\frac{\Gamma \vdash_\Sigma^{\prec_0} A{:}\mathrm{type} \quad \Gamma, x{:}A \vdash_\Sigma^{\prec_0} B{:}\mathrm{type}}{\Gamma \vdash_\Sigma^{\prec_0} \Pi x{:}A.B{:}\mathrm{type}}\ , \text{ where } \mathrm{head}(A) \prec_0^M \mathrm{head}(B) \text{ or } \mathrm{head}(A) = \mathrm{head}(B)$$

$$\frac{\Gamma \vdash_\Sigma^{\prec_0} A{:}\quad K \equiv K' \quad \Gamma \vdash_\Sigma^{\prec_0} K'\ Kind}{\Gamma \vdash_\Sigma^{\prec_0} A{:}K'}$$

$$\frac{\Sigma(c) = A}{\Gamma \vdash_\Sigma^{\prec_0} c{:}A} \qquad \frac{\Gamma(x) = A}{\Gamma \vdash_\Sigma^{\prec_0} x{:}A}$$

$$\frac{\Gamma \vdash_\Sigma^{\prec_0} A{:}\mathrm{type} \quad \Gamma, x{:}A \vdash_\Sigma^{\prec_0} M{:}B}{\Gamma \vdash_\Sigma^{\prec_0} \lambda x{:}A.M{:}\Pi x{:}A.B}\ , \text{ where } \mathrm{head}(A) \prec_0^M \mathrm{head}(B) \text{ or } \mathrm{head}(A) = \mathrm{head}(B)$$

$$\frac{\Gamma \vdash_\Sigma^{\prec_0} M{:}\Pi x{:}A.B \quad \Gamma \vdash_\Sigma^{\prec_0} N{:}A}{\Gamma \vdash_\Sigma^{\prec_0} M\ N{:}[N/x]B}$$

$$\frac{\Gamma \vdash_\Sigma^{\prec_0} M{:}A \quad A \equiv A' \quad (\Gamma \vdash_\Sigma^{\prec_0} A'{:}\mathrm{type}}{\Gamma \vdash_\Sigma^{\prec_0} M{:}A'}$$

$$\frac{}{\Gamma \vdash_{\Sigma}^{\prec 0} \text{type}\ Kind} \qquad \frac{\Gamma \vdash_{\Sigma}^{\prec 0} A{:}\text{type} \quad \Gamma, x{:}A \vdash_{\Sigma}^{\prec 0} K\ Kind}{\Gamma \vdash_{\Sigma}^{\prec 0} \Pi x{:}A.K\ Kind}$$

$$\frac{}{\vdash_{\Sigma}^{\prec 0} \cdot\ Ctx} \qquad \frac{\vdash_{\Sigma}^{\prec 0} \Gamma\ Ctx \quad \Gamma \vdash_{\Sigma}^{\prec 0} A{:}\text{type}}{\vdash_{\Sigma}^{\prec 0} \Gamma, x{:}A\ Ctx}$$

Notation. By abuse of notation, given two type families A, B, we will write $A \prec^A B$ and $A \prec^M B$ for head$(A) \prec^A$ head(B) and head$(A) \prec^M$ head(B), respectively. We will use $A \preceq_{\Sigma}^{M} B$ to say that $A \prec^M B$ or $head(A) = head(B)$.

The idea underlying the introduction of the relations $\prec^A$ and $\prec^M$ is to restrict, using the $\vdash_{\Sigma}^{\preceq}$ judgements, the generation of valid terms and type families to those which preserve the dependencies generated by the signature Σ; in particular, we want terms of type A to be allowed to appear inside B only if $A \prec^A B$, and similarly terms of type A will be subterms of terms of type B only if $A \preceq^M B$.

When looking for a dependency relation, we will usually prefer coarser ones, so that the class of dependency-preserving terms (i.e. terms well typed according to the $\vdash_{\Sigma}^{\preceq}$ judgement) is as wide as possible. In practice, given a derivation of $\vdash \Sigma\ Sig$, we will compute the minimum $\prec$ such that $\vdash^{\prec} \Sigma\ Sig$ holds.

Example 1. In our previous example about even numbers, the following is easily seen to be a dependency relation:

$$\prec = (\{\mathbf{nat} \prec^A \mathbf{proof}, \mathbf{o} \prec^A \mathbf{proof}\}, \{\mathbf{nat} \prec^M \mathbf{o}, \mathbf{nat} \prec^A \mathbf{proof}, \mathbf{o} \prec^M \mathbf{proof}\})$$

The condition $\mathbf{o} \prec^A \mathbf{proof}$ comes from the type of **proof**; $\mathbf{nat} \prec^M \mathbf{o}$ is obtained from type checking on **even**; finally $\mathbf{nat} \prec^A \mathbf{proof}$ since $\prec^A \supseteq \prec^M \cdot \prec A$, and all the others pair in $\prec^M$ follow from $\prec^M \supseteq \prec^A$.

Example 2. To demonstrate the gain in expressive power that the use of dependent types allows, we show how the simply-typed lambda calculus can be formalized in this calculus. We will need two type families: one, called **type**, for types, and the second, **term**, indexed by objects of the first, for terms.

$$\begin{aligned} \mathbf{type} &: \mathbf{type} \\ \mathbf{arrow} &: \mathbf{type} \Rightarrow (\mathbf{type} \Rightarrow \mathbf{type}) \end{aligned}$$

$$\begin{aligned} \mathbf{term} &: \mathbf{type} \Rightarrow \text{type} \\ \mathbf{lambda} &: \Pi x : \mathbf{type}.\Pi y : \mathbf{type}.((\mathbf{term}\ x) \Rightarrow (\mathbf{term}\ y)) \Rightarrow \mathbf{term}(\mathbf{arrow}\ x\ y)) \\ \mathbf{app} &: \Pi x : \mathbf{type}.\Pi y : \mathbf{type}.(\mathbf{term}(\mathbf{arrow}\ x\ y)) \Rightarrow ((\mathbf{term}\ x) \Rightarrow (\mathbf{term}\ y)) \end{aligned}$$

For this system, a dependency relation is simply

$$\prec = (\{\mathbf{type} \prec^A \mathbf{term}\}, \{\mathbf{type} \prec^M \mathbf{term}\})$$

Notation. In what follows, we will assume that a signature Σ and a dependency relation $\prec$ for Σ have been fixed. Moreover, wherever a context Γ is mentioned, we will will tacitly assume it is well-typed and dependency-preserving, i.e. $\vdash_{\Sigma}^{\preceq} \Gamma\ Ctx$.

We state below a few properties of the LF calculus that continue to hold when restricting ourselves to dependency-preserving terms:

Proposition 3.2. *If $\Gamma \vdash_{\Sigma}^{\preceq} M : A$ and N is a subterm of M, then there is $\Gamma' \supseteq \Gamma$ and type A' such that $\Gamma' \vdash_{\Sigma}^{\preceq} N : A'$.*

Proof. By induction on the derivation of $\Gamma \vdash_{\Sigma}^{\preceq} M : A$. □

Notation. In the rest of this paper, we will write $\Gamma(M, N)$ and $A(M, N)$ for the context Γ' and type A', respectively, obtained by the Proposition above. Note that these are not unique, but depend on the particular derivation of $\Gamma \vdash_{\Sigma}^{\preceq} M : A$ considered. However, all these are easily seen to be equivalent when conversion and variable renaming are taken into account.

Proposition 3.3 (Weakening). *Let $\Sigma' \subseteq \Sigma$, $\Gamma' \subseteq \Gamma$, and $\vdash^{\preceq}_{\Sigma} \Gamma\ Ctx$, then:*

1. *If $\Gamma' \vdash^{\preceq}_{\Sigma'} M : A$ then $\Gamma \vdash^{\preceq}_{\Sigma} M : A$.*
2. *If $\Gamma' \vdash^{\preceq}_{\Sigma'} A : K$ then $\Gamma \vdash^{\preceq}_{\Sigma} A : K$.*
3. *If $\Gamma' \vdash^{\preceq}_{\Sigma'} K\ Kind$ then $\Gamma \vdash^{\preceq}_{\Sigma} K\ Kind$.*

Proof. By an easy induction on the derivations. □

Lemma 3.4 (Substitution). *Let $\Gamma \vdash^{\preceq}_{\Sigma} N : C$, then:*

1. *if $\Gamma, y : C, \Delta \vdash^{\preceq}_{\Sigma} M : A$ then $\Gamma, [N/y]\Delta \vdash^{\preceq}_{\Sigma} [N/y]M : [N/y]A$;*
2. *if $\Gamma, y : C, \Delta \vdash^{\preceq}_{\Sigma} A : K$ then $\Gamma, [N/y]\Delta \vdash^{\preceq}_{\Sigma} [N/y]A : [N/y]K$;*
3. *if $\Gamma, y : C, \Delta \vdash^{\preceq}_{\Sigma} K\ Kind$ then $\Gamma, [N/y]\Delta \vdash^{\preceq}_{\Sigma} [N/y]K\ Kind$.*

Proof. By (simultaneous) induction on the size of the derivations. For term and type abstractions, one has to observe that $\mathrm{head}([N/y]A) = \mathrm{head}(A)$. □

Lemma 3.5. *We have:*

1. *$\Gamma \vdash^{\preceq}_{\Sigma} M : A$ implies $\Gamma \vdash^{\preceq}_{\Sigma} A : \mathrm{type}$;*
2. *$\Gamma \vdash^{\preceq}_{\Sigma} A : K$ implies $\Gamma \vdash^{\preceq}_{\Sigma} K\ Kind$.*

Proof. Both are proved by induction on the derivation.

- Type constant:

$$\frac{\Sigma(a)=K}{\Gamma\vdash^{\preceq}_{\Sigma} a:K}$$

By inversion on the derivation of $\vdash \Sigma\ Sig$ and Weakening.

- Type application:

$$\frac{\Gamma\vdash^{\preceq}_{\Sigma} A:\Pi x{:}B.K \qquad \Gamma\vdash^{\preceq}_{\Sigma} M:B}{\Gamma\vdash^{\preceq}_{\Sigma} A\ M:[M/x]K}$$

By inductive hypothesis we get $\Gamma \vdash^{\preceq}_{\Sigma} \Pi x : B.K\ Kind$. By inversion $\Gamma, x : B \vdash^{\preceq}_{\Sigma} K\ Kind$, hence by Substitution the result.

- Type abstraction:

$$\frac{\Gamma\vdash^{\preceq}_{\Sigma} A{:}\mathrm{type} \quad \Gamma,x{:}A\vdash^{\preceq}_{\Sigma} B{:}\mathrm{type}}{\Gamma\vdash^{\preceq}_{\Sigma}\Pi x{:}A.B{:}\mathrm{type}}\ A\preceq^{M}_{\Sigma} B$$

Trivial.

- Kind conversion:

$$\frac{\Gamma\vdash^{\preceq}_{\Sigma} A{:}K' \quad K'\equiv K \quad \Gamma\vdash^{\preceq}_{\Sigma} K\ Kind}{\Gamma\vdash^{\preceq}_{\Sigma} A{:}K}$$

Trivial.

- Term constant:

$$\frac{\Sigma(c)=A}{\Gamma\vdash^{\preceq}_{\Sigma} c{:}A}$$

By inversion on the derivation of $\vdash \Sigma\ Sig$ and Weakening.

- Term variable:

$$\frac{\Gamma(x)=A}{\Gamma\vdash^{\preceq}_{\Sigma} x{:}A}$$

By inversion on the derivation of $\vdash^{\preceq}_{\Sigma} \Gamma\ Ctx$ and Weakening.

- Term application:

$$\frac{\Gamma\vdash^{\preceq}_{\Sigma}M{:}\Pi x{:}B.A \quad \Gamma\vdash^{\preceq}_{\Sigma}N{:}B}{\Gamma\vdash^{\preceq}_{\Sigma}M\ N{:}[N/x]A}$$

By inductive hypothesis we get $\Gamma \vdash^{\preceq}_{\Sigma} \Pi x : B.A$: type. By inversion, $\Gamma, x : B \vdash^{\preceq}_{\Sigma} A$: type, hence by Substitution the result.

- Term abstraction:

$$\frac{\Gamma\vdash^{\preceq}_{\Sigma}A{:}\mathrm{type} \quad \Gamma,x{:}A\vdash^{\preceq}_{\Sigma}M{:}B}{\Gamma\vdash^{\preceq}_{\Sigma}\lambda x{:}A.M{:}\Pi x{:}A.B}\ A\preceq^{M}_{\Sigma}B$$

By inductive hypothesis we get $\Gamma, x : A \vdash^{\preceq}_{\Sigma} B$: type, and, applying the type abstraction rule, the result.

- Type conversion:

$$\frac{\Gamma\vdash^{\preceq}_{\Sigma}M{:}A' \quad A'{\equiv}A \quad \Gamma\vdash^{\preceq}_{\Sigma}A{:}\mathrm{type}}{\Gamma\vdash^{\preceq}_{\Sigma}M{:}A}$$

Trivial.

□

Corollary 3.6. *The following holds:*

1. *If* $\Gamma \vdash^{\preceq}_{\Sigma} \Pi x : A.B$: type *then* $A \preceq^{M}_{\Sigma} B$.
2. *If* $\Gamma \vdash^{\preceq}_{\Sigma} M : \Pi x : A.B$ *then* $A \preceq^{M}_{\Sigma} B$.

Proof. (1) is obtained immediately by inversion. For (2) we use the Lemma to conclude $\Gamma \vdash^{\preceq}_{\Sigma} \Pi x : A.B$: type, and hence by (1) the result. □

The following result clarifies the motivating property of the two relations $\prec^{A}$ and $\prec^{M}$:

Lemma 3.7. *Let* $\vdash^{\preceq}_{\Sigma} \Gamma, x : C\ Ctx$,

1. *if* $\Gamma, x : C, \Delta \vdash^{\preceq}_{\Sigma} A : K$ *and* $x \in \mathcal{FV}(A)$ *then* $C \prec^{A} A$
2. *if* $\Gamma, x : C, \Delta \vdash^{\preceq}_{\Sigma} M : A$ *and* $x \in \mathcal{FV}(M)$ *then* $C \preceq^{M}_{\Sigma} A$

Proof. By (simultaneous) induction on both derivations. The cases when either A or M are constants, or M is a variable are trivial. So are those for the conversion rules. The only interesting cases are, for both terms and type families, application and abstraction:

- Type application:

$$\frac{\Gamma, x : C, \Delta \vdash^{\preceq}_{\Sigma} A : \Pi y : B.K \qquad \Gamma, x : C, \Delta \vdash^{\preceq}_{\Sigma} M : B}{\Gamma, x : C, \Delta \vdash^{\preceq}_{\Sigma} A\ M : [M/y]K}$$

If $x \in \mathcal{FV}(A)$ we are done by inductive hypothesis on $\Gamma, x : C, \Delta \vdash^{\preceq}_{\Sigma} A : \Pi y : B.K$, since head$(A\ M)$ = *head*(A). Otherwise, if $x \in \mathcal{FV}(M)$, then by the inductive hypothesis on $\Gamma, x : C, \Delta \vdash^{\preceq}_{\Sigma} M : B$ we get $C \preceq^{M}_{\Sigma} B$. By inversion, we easily see $A = a\overline{N}$ for some terms $\overline{N}$ and type family constant a = head(A); then $\Sigma(a) = \Pi x_1 : C_1 \ldots \Pi x_n : C_n$.type and head$(B)$ = head(C_i) for some i, so $B \prec^{A} A$; hence, we conclude $C \prec^{A} A$.
- Type abstraction:

$$\frac{\Gamma, x : C, \Delta \vdash^{\preceq}_{\Sigma} A : \mathrm{type} \qquad \Gamma, x : C, \Delta, y : A \vdash^{\preceq}_{\Sigma} B : \mathrm{type}}{\Gamma, x : C, \Delta \vdash^{\preceq}_{\Sigma} \Pi y : A.B : \mathrm{type}}\ A \preceq^{M}_{\Sigma} B$$

If $x \in \mathcal{FV}(B)$ we are done by inductive hypothesis on $\Gamma, x : C, \Delta, y : A \vdash_{\Sigma} B$: type, since head$(\Pi y : A.B)$ = head(B). Otherwise, if $x \in \mathcal{FV}(A)$, then by the inductive hypothesis on $\Gamma, x : C, \Delta \vdash_{\Sigma} A$: type we get $C \prec^{A} A$, and hence by the side condition the result.
- Term application:

$$\frac{\Gamma, x : C, \Delta \vdash^{\preceq}_{\Sigma} M : \Pi y : B.A \qquad \Gamma, x : C, \Delta \vdash^{\preceq}_{\Sigma} N : B}{\Gamma, x : C, \Delta \vdash^{\preceq}_{\Sigma} M\ N : [N/y]A}$$

If $x \in \mathcal{FV}(M)$ we are done by inductive hypothesis on $\Gamma, x : C, \Delta \vdash_\Sigma M : \Pi y : B.A$, since $\text{head}([N/y]A) = \text{head}(\Pi y : B.A)$. Otherwise, if $x \in \mathcal{FV}(N)$ by the inductive hypothesis on $\Gamma, x : C, \Delta \vdash_\Sigma N : B$ we get $C \preceq^M_\Sigma B$. By Corollary 3.6, $B \preceq^M_\Sigma A$, and by transitivity we conclude $C \preceq^M_\Sigma [N/y]A$.

- Term abstraction:

$$\frac{\Gamma, x : C, \Delta \vdash_\Sigma A : \text{type} \qquad \Gamma, x : C, \Delta, y : A \vdash_\Sigma M : B}{\Gamma \vdash_\Sigma \lambda y : A.M : \Pi y : A.B} \; A \preceq^M_\Sigma B.$$

If $x \in \mathcal{FV}(M)$ we are done by inductive hypothesis on $\Gamma, x : C, \Delta, y : A \vdash_\Sigma M : B$, since $\text{head}(\Pi y : A.B) = \text{head}(B)$. Otherwise, if $x \in \mathcal{FV}(A)$, then by the inductive hypothesis on $\Gamma, x : C, \Delta \vdash_\Sigma A : \text{type}$ we get $C \preceq^M_\Sigma A$, hence by the side condition and transitivity we conclude $C \preceq^M_\Sigma \Pi y : A.B$.

$\square$

Definition 3.8. Environments are expressions with a "hole", which we will denote by $\circ$, constructed according to the following syntax:

$$\textit{Environments} \quad E \quad := \quad \circ \mid \lambda x : A.E \mid M\ E \mid E\ N$$

Well-typed environments are constructed by means of the judgement

$$\Gamma \vdash^{\preceq}_\Sigma E[\![\Gamma_\circ \vdash \circ : A_\circ]\!] : A,$$

and the rules

$$\frac{\Gamma_\circ \vdash^{\preceq}_\Sigma A_\circ : \text{type} \quad \Gamma_\circ \subseteq \Gamma}{\Gamma \vdash^{\preceq}_\Sigma \circ\ [\![\Gamma_\circ \vdash \circ : A_\circ]\!] : A_\circ}$$

$$\frac{\Gamma \vdash^{\preceq}_\Sigma A : \text{type} \quad \Gamma, x : A \vdash^{\preceq}_\Sigma E[\![\Gamma_\circ \vdash \circ : A_\circ]\!] : B}{\Gamma \vdash^{\preceq}_\Sigma \lambda x : A.E[\![\Gamma_\circ \vdash \circ : A_\circ]\!] : \Pi x : A.B} \quad A \preceq^M_\Sigma B$$

$$\frac{\Gamma \vdash^{\preceq}_\Sigma E[\![\Gamma_\circ \vdash \circ : A_\circ]\!] : \Pi x : A.B \quad \Gamma \vdash^{\preceq}_\Sigma N : A}{\Gamma \vdash^{\preceq}_\Sigma (E[\![\Gamma_\circ \vdash \circ : A_\circ]\!])\ N : [N/x]B}$$

$$\frac{\Gamma \vdash^{\preceq}_\Sigma M : \Pi x : A.B \quad \Gamma \vdash^{\preceq}_\Sigma E[\![\Gamma_\circ \vdash \circ : A_\circ]\!] : A}{\Gamma \vdash^{\preceq}_\Sigma M\ (E[\![\Gamma_\circ \vdash \circ : A_\circ]\!]) : B} \quad A_\circ \not\preceq^A B$$

$$\frac{\Gamma \vdash^{\preceq}_\Sigma E[\![\Gamma_\circ \vdash \circ : A_\circ]\!] : A \quad A \equiv B \quad \Gamma \vdash^{\preceq}_\Sigma B : \text{type}}{\Gamma \vdash^{\preceq}_\Sigma E[\![\Gamma_\circ \vdash \circ : A_\circ]\!] : B}$$

Example 1. The environments

$$\mathbf{even}_+\ \mathbf{0}\ (\circ[\![\vdash \circ : \mathbf{nat}]\!]),$$

and

$$\mathbf{even}_+\ \mathbf{0}\ (\circ[\![\vdash \circ : \mathbf{nat}]\!])\ (\mathbf{even}_+\ \mathbf{0}\ \mathbf{0}\ \mathbf{even}_0\ \mathbf{even}_0)$$

are not well-typed. This because in the application

$$\frac{\vdash^{\preceq}_\Sigma \mathbf{even}_+\ \mathbf{0} : \Pi y : \mathbf{nat}.\mathbf{proof}(\mathbf{even}\ 0) \Rightarrow (\mathbf{proof}(\mathbf{even}\ y) \Rightarrow \mathbf{proof}(\mathbf{even}\ (+\ 0\ y))) \quad \vdash^{\preceq}_\Sigma \circ\ [\![\vdash \circ : \mathbf{nat}]\!] : \mathbf{nat}}{\vdash^{\preceq}_\Sigma \mathbf{even}_+\ \mathbf{0}\ (\circ\ [\![\vdash \circ : \mathbf{nat}]\!]) : \mathbf{proof}(\mathbf{even}\ 0) \Rightarrow (\mathbf{proof}(\mathbf{even}\ \circ) \Rightarrow \mathbf{proof}(\mathbf{even}\ (+\ 0\ \circ)))}$$

the side condition $\mathbf{nat} \not\preceq^A \mathbf{even}$ is violated.

Notation. Given an environment E and a term M, we will write $E[\![M]\!]$ for the term obtained by replacing the hole $\circ$ with M. Conversely, let M be a term and N an occurrence of one of its subterm, we will write $M[\![\circ]\!]_N$ for the environment (not necessarily well-typed) obtained from M by replacing that occurrence of N by $\circ$.

The type of an environment depends, by the relation $\prec^M$, on the type of its hole:

Proposition 3.9. *If* $\Gamma \vdash_\Sigma^{\preceq} E[\![\Gamma_\circ \vdash \circ : A_\circ]\!] : A$ *then* $A_\circ \preceq_\Sigma^M A$.

Proof. By induction on the derivation of $\Gamma \vdash_\Sigma^{\preceq} E[\![\Gamma_\circ \vdash \circ : A_\circ]\!] : A$. All cases are trivial, except perhaps

$$\frac{\Gamma \vdash_\Sigma^{\preceq} M_1 : \Pi x{:}B.A \quad \Gamma \vdash_\Sigma^{\preceq} E_2[\![\Gamma_\circ \vdash \circ : A_\circ]\!] : B}{\Gamma \vdash_\Sigma^{\preceq} M_1(E_2[\![\Gamma_\circ \vdash \circ : A_\circ]\!]) : A} \quad A_\circ \not\prec^A A$$

By inductive hypothesis, $A_\circ \preceq_\Sigma^M B$. From $\Gamma \vdash_\Sigma^{\preceq} M_1 : \Pi x : B.A$ one concludes $B \preceq_\Sigma^M A$. Hence by transitivity $A_\circ \preceq_\Sigma^M A$. □

As expected, when the hole is replaced by an expression of compatible type, environments produce well-typed expressions:

Lemma 3.10. *If* $\Gamma \vdash_\Sigma^{\preceq} E[\![\Gamma_\circ \vdash \circ : A_\circ]\!] : A$, *and* $\Delta \vdash_\Sigma^{\preceq} M : A_\circ$ *with* $\Delta \subseteq \Gamma_\circ$, *then* $\Gamma \vdash_\Sigma^{\preceq} E[\![M]\!] : A$.

Proof. By induction on $\Gamma \vdash_\Sigma^{\preceq} E[\![\Gamma_\circ \vdash \circ : A_\circ]\!] : A$. The only interesting case is, as before,

$$\frac{\Gamma \vdash_\Sigma^{\preceq} M_1 : \Pi x{:}B.A \quad \Gamma \vdash_\Sigma^{\preceq} E_2[\![\Gamma_\circ \vdash \circ : A_\circ]\!] : B}{\Gamma \vdash_\Sigma^{\preceq} M_1(E_2[\![\Gamma_\circ \vdash \circ : A_\circ]\!]) : A} \quad A_\circ \not\prec^A A,$$

By induction hypothesis we get

$$\frac{\Gamma \vdash_\Sigma^{\preceq} M_1 : \Pi x{:}B.A \quad \Gamma \vdash_\Sigma^{\preceq} E_2[\![M]\!] : B}{\Gamma \vdash_\Sigma^{\preceq} M_1\ (E_2[\![M]\!]) : [E_2[\![M]\!]/x]A}$$

We are left to show that $x \notin \mathcal{FV}(A)$, so that $[E_2[\![M]\!]/x]A = A$. From $\Gamma \vdash_\Sigma^{\preceq} M_1 : \Pi x : B.A$ we deduce $\Gamma \vdash_\Sigma^{\preceq} \Pi x : B.A : \mathrm{type}$, and by inversion $\Gamma, x : B \vdash_\Sigma^{\preceq} A : \mathrm{type}$. Suppose $x \in \mathcal{FV}(A)$, then $B \prec^A A$, and, since from $\Gamma \vdash_\Sigma^{\preceq} E_2[\![\Gamma_\circ \vdash \circ : A_\circ]\!] : A$ we get $A_\circ \preceq_\Sigma^M B$, we conclude $A_\circ \prec^A A$, a contradiction. □

In general the composition of two well-typed environment does not produce a well-typed environment. A sufficient condition for this to happen is given by the following:

Proposition 3.11. *Let* $\Gamma \vdash_\Sigma^{\preceq} E[\![\Gamma_\circ \vdash \circ : A_\circ]\!] : A$, $\Delta \vdash_\Sigma^{\preceq} E'[\![\Gamma \vdash \circ : A]\!] : A'$ *two environments, if* $A \preceq_\Sigma^M A_\circ$ *then* $\Delta \vdash_\Sigma^{\preceq} E'[\![E[\![\Gamma_\circ \vdash \circ : A_\circ]\!]]\!] : A'$.

Proof. By an easy induction on $\Delta \vdash_\Sigma^{\preceq} E'[\![\Gamma \vdash \circ : A]\!] : A'$. We show the case

$$\frac{\Delta \vdash_\Sigma^{\preceq} M_1' : \Pi x{:}B'.A' \quad \Delta \vdash_\Sigma^{\preceq} E_2'[\![\Gamma \vdash \circ : A]\!] : B'}{\Delta \vdash_\Sigma^{\preceq} M_1'\ (E_2'[\![\Gamma \vdash \circ : A]\!]) : A'} \quad A \not\prec^A A'.$$

By inductive hypothesis we obtain $\Delta \vdash_\Sigma^{\preceq} E_2'[\![E[\![\Gamma_\circ \vdash \circ : A_\circ]\!]]\!] : B'$. If $A_\circ \prec^A A'$ from the assumption $A \preceq_\Sigma^M A_\circ$ we get $A \prec^A A'$, a contradiction. Hence

$$\frac{\Delta \vdash_\Sigma^{\preceq} M_1' : \Pi x{:}B'.A' \quad \Delta \vdash_\Sigma^{\preceq} E_2'[\![E[\![\Gamma_\circ \vdash \circ : A_\circ]\!]]\!] : B'}{\Delta \vdash_\Sigma^{\preceq} M_1'\ (E_2'[\![E[\![\Gamma_\circ \vdash \circ : A_\circ]\!]]\!]) : A'} \quad A_\circ \not\prec^A A'.$$

□

The following shows that environments behave nicely with respect to β-reduction:

Lemma 3.12. *Let* $\Gamma, x : C, \Delta \vdash_\Sigma^{\preceq} M : A$ *be any term and* $\Gamma \vdash_\Sigma^{\preceq} E[\![\Gamma_\circ \vdash \circ : A_\circ]\!] : C$ *an environment, if* $A_\circ \not\prec^A A$, *then for any occurrence of* x *in* M *we have* $\Gamma, x : C, \Delta \vdash_\Sigma^{\preceq} M[\![E[\![\Gamma_\circ \vdash \circ : A_\circ]\!]]\!]_x : A$.

Proof. By induction on the derivation of $\Gamma, x : C, \Delta \vdash^{\preceq}_{\Sigma} M : A$. Most of the cases are trivial; one interesting case is abstraction, since we have in particular to make sure that x cannot appear inside the type:

$$\frac{\Gamma,x{:}C,\Delta\vdash^{\preceq}_{\Sigma}A{:}\mathrm{type} \quad \Gamma,x{:}C,\Delta,y{:}A\vdash^{\preceq}_{\Sigma}M{:}B}{\Gamma,x{:}C,\Delta\vdash^{\preceq}_{\Sigma}\lambda y{:}A.M{:}\Pi y{:}A.B} \quad A\preceq^{M}_{\Sigma}B$$

If $x \in \mathcal{FV}(A)$ then $C \prec^{A} A$, and, by the side condition $C \prec^{A} \Pi y : A.B$. From $\Gamma \vdash^{\preceq}_{\Sigma} E[\![\Gamma_\circ \vdash \circ : A_\circ]\!] : C$ we get $A_\circ \preceq^{M}_{\Sigma} C$, hence $A_\circ \prec^{A} \Pi y : A.B$, contradiction to the assumptions. So it must be $x \in \mathcal{FV}(M)$, and the result follows by induction hypothesis.

Another interesting case is application, where x appears on the right-hand-side:

$$\frac{\Gamma,x{:}C,\Delta\vdash^{\preceq}_{\Sigma}M{:}\Pi y{:}B.A \quad \Gamma,x{:}C,\Delta\vdash^{\preceq}_{\Sigma}N{:}B}{\Gamma,x{:}C,\Delta\vdash^{\preceq}_{\Sigma}M\ N{:}[N/y]A}$$

Note that the side condition in the corresponding rule for environments is automatically guaranteed by the hypotheses. We are left to show that y does not appear in A and that $A_\circ \not\prec^{A} B$.

Since we are assuming $x \in \mathcal{FV}(N)$, $C \preceq^{M}_{\Sigma} B$. If $y \in \mathcal{FV}(A)$ then $B \prec^{A} A$, hence $C \prec^{A} A$, and, since $A_\circ \preceq^{M}_{\Sigma} C$, we obtain a contradiction. Similarly $A_\circ \not\prec^{A} B$, because otherwise we would get, from $B \preceq^{M}_{\Sigma} A$, $A_\circ \prec^{A} A$, again a contradiction. Having shown these two simple facts, the result follows by inductive hypothesis on $\Gamma, x : C, \Delta \vdash^{\preceq}_{\Sigma} N : A$. □

Corollary 3.13. *If $\Gamma \vdash^{\preceq}_{\Sigma} (\lambda x : A.M)\ (E[\![\Gamma_\circ \vdash \circ : A_\circ]\!]) : B$ then for all the occurrences of x in M we have $\Gamma, x : A \vdash^{\preceq}_{\Sigma} M[\![E[\![\Gamma_\circ \vdash \circ : A_\circ]\!]]\!]_x : B$.*

Proof. By inversion (and type conversion, if necessary), we get $\Gamma, x : A \vdash^{\preceq}_{\Sigma} M : B$, $\Gamma \vdash^{\preceq}_{\Sigma} E[\![\Gamma_\circ \vdash \circ : A_\circ]\!] : A$, and $A_\circ \not\prec^{A} B$. The result then follows by the Lemma. □

4. Substitutions

In [9], the definition of substitution makes use of the existence and uniqueness of long $\beta\eta$ normal forms. In the LF calculus, these find an analogue in the concept of canonical form:

Definition 4.1. We define canonical forms for terms and type families by the judgements

$\Gamma \vdash_\Sigma M \Downarrow A$	M is canonical of type A
$\Gamma \vdash_\Sigma A \Downarrow \mathrm{type}$	A is a canonical type
$\Gamma \vdash_\Sigma M \downarrow A$	M is atomic of type A
$\Gamma \vdash_\Sigma A \downarrow K$	A is atomic of type K

formed according to the following inference rules:

$$\frac{\Gamma\vdash_\Sigma A \Downarrow \mathrm{type} \quad \Gamma,x{:}A\vdash_\Sigma M \Downarrow B}{\Gamma\vdash_\Sigma \lambda x{:}A.M \Downarrow \Pi x{:}A.B}$$

$$\frac{\Gamma\vdash_\Sigma A \downarrow \mathrm{type} \quad \Gamma\vdash_\Sigma M \downarrow A}{\Gamma\vdash_\Sigma M \Downarrow A}$$

$$\frac{\Gamma\vdash_\Sigma M \Downarrow A \quad A{\equiv}B \quad \Gamma\vdash_\Sigma B{:}\mathrm{type}}{\Gamma\vdash_\Sigma M \Downarrow B}$$

$$\frac{\Sigma(c){=}A}{\Gamma{\vdash_\Sigma}c\downarrow A}\qquad\frac{\Gamma(x){=}A}{\Gamma{\vdash_\Sigma}x\downarrow A}$$

$$\frac{\Gamma{\vdash_\Sigma}M\downarrow\Pi x{:}A.B\quad\Gamma{\vdash_\Sigma}N\Downarrow A}{\Gamma{\vdash_\Sigma}M\ N\downarrow[N/x]B}$$

$$\frac{\Gamma{\vdash_\Sigma}M\downarrow A\quad A{\equiv}B\quad\Gamma{\vdash_\Sigma}B{:}\text{type}}{\Gamma{\vdash_\Sigma}M\downarrow B}$$

$$\frac{\Sigma(a){=}K}{\Gamma{\vdash_\Sigma}a\downarrow K}$$

$$\frac{\Gamma{\vdash_\Sigma}A\downarrow\Pi x{:}B.K\quad\Gamma{\vdash_\Sigma}M\Downarrow B}{\Gamma{\vdash_\Sigma}A\ M\downarrow[M/x]K}$$

$$\frac{\Gamma{\vdash_\Sigma}A\downarrow K\quad K{\equiv}K'\quad\Gamma{\vdash_\Sigma}K'\ Kind}{\Gamma{\vdash_\Sigma}A\downarrow K'}$$

$$\frac{\Gamma{\vdash_\Sigma}A\Downarrow\text{type}\quad\Gamma,x{:}A{\vdash_\Sigma}B\Downarrow\text{type}}{\Gamma{\vdash_\Sigma}\Pi x{:}A.B\Downarrow\text{type}}$$

$$\frac{\Gamma{\vdash_\Sigma}A\downarrow\text{type}}{\Gamma{\vdash_\Sigma}A\Downarrow\text{type}}$$

Theorem 4.2. *Let $\vdash_\Sigma \Gamma\ Ctx$, then*

1. *If $\Gamma\vdash_\Sigma M\downarrow A$ then $\Gamma\vdash_\Sigma M : A$.*
2. *If $\Gamma\vdash_\Sigma A\downarrow K$ then $\Gamma\vdash_\Sigma A : K$.*
3. *If $\Gamma\vdash_\Sigma M\Downarrow A$ then $\Gamma\vdash_\Sigma M : A$.*
4. *If $\Gamma\vdash_\Sigma A\Downarrow\text{type}$ then $\Gamma\vdash_\Sigma A : \text{type}$.*
5. *If $\Gamma\vdash_\Sigma M : A$ then there is a unique M' such that $M'\equiv M$ and $\Gamma\vdash_\Sigma M\Downarrow A$.*
6. *If $\Gamma\vdash_\Sigma A : \text{type}$ then there is a unique A' such that $A\equiv A'$ and $\Gamma\vdash_\Sigma A'\Downarrow\text{type}$.*

Proof. See [1], [2], [15]. □

In light of the previous section, our goal is to show that if a well-typed term or type family respects the dependencies, so does its canonical form.

Notation. We will make use of the following abbreviations:

$$\Gamma\vdash^{\preceq}_\Sigma M\Downarrow A \overset{\text{def}}{\Longleftrightarrow} \Gamma\vdash_\Sigma M\Downarrow A \text{ and } \Gamma\vdash^{\preceq}_\Sigma M : A$$

$$\Gamma\vdash^{\preceq}_\Sigma A\Downarrow\text{type} \overset{\text{def}}{\Longleftrightarrow} \Gamma\vdash_\Sigma A\downarrow\text{type} \text{ and } \Gamma\vdash^{\preceq}_\Sigma A : \text{type}$$

$$\Gamma\vdash^{\preceq}_\Sigma M\downarrow A \overset{\text{def}}{\Longleftrightarrow} \Gamma\vdash_\Sigma M\downarrow A \text{ and } \Gamma\vdash^{\preceq}_\Sigma M : A$$

$$\Gamma\vdash^{\preceq}_\Sigma A\downarrow K \overset{\text{def}}{\Longleftrightarrow} \Gamma\vdash_\Sigma A\downarrow K \text{ and } \Gamma\vdash^{\preceq}_\Sigma A : K$$

The inversion properties for the judgements $\Gamma\vdash^{\preceq}_\Sigma M\downarrow A$ and $\Gamma\vdash^{\preceq}_\Sigma M\Downarrow A$ are non-trivial enough to be worth being stated and proved explicitly:

Proposition 4.3 (Inversion)**.** *We have:*

1. *If $\Gamma\vdash^{\preceq}_\Sigma M : \Pi x : A.B$, $\Gamma\vdash^{\preceq}_\Sigma N : A$, and $\Gamma\vdash_\Sigma M\ N\downarrow C$ then $\Gamma\vdash^{\preceq}_\Sigma M\downarrow\Pi x : A.B$ and $\Gamma\vdash^{\preceq}_\Sigma N\Downarrow A$.*
2. *If $\Gamma, x : A\vdash^{\preceq}_\Sigma M : B$, and $\Gamma\vdash_\Sigma(\lambda x : A.M)\Downarrow C$ then $\Gamma, x : A\vdash^{\preceq}_\Sigma M\Downarrow B$.*
3. *If $\Gamma\vdash^{\preceq}_\Sigma M : A$, $A\equiv A'$, $\Gamma\vdash_\Sigma A'\downarrow\text{type}$, and $\Gamma\vdash_\Sigma M\Downarrow C$ then $\Gamma\vdash^{\preceq}_\Sigma M\downarrow A$.*

Proof. (1) By induction on the derivation of $\Gamma\vdash_\Sigma M\ N\downarrow C$. There are only two cases:

- Application:

$$\frac{\Gamma \vdash_\Sigma M \downarrow \Pi x{:}A'.B' \quad \Gamma \vdash_\Sigma N \Downarrow A'}{\Gamma \vdash_\Sigma M\ N \downarrow [N/x]B'}$$

From $\Gamma \vdash_\Sigma^\preceq M : \Pi x : A.B$ we get $\Gamma \vdash_\Sigma^\preceq \Pi x : A.B$: type, and by inversion $\Gamma \vdash_\Sigma^\preceq A$: type. The result then follows from $\Gamma \vdash_\Sigma M \downarrow \Pi x : A'.B'$ and $\Gamma \vdash_\Sigma N \Downarrow A'$ by conversion, since $A \equiv A'$ and $B \equiv B'$.

- Conversion:

$$\frac{\Gamma \vdash_\Sigma M\ N \downarrow C' \quad C' \equiv C \quad \Gamma \vdash_\Sigma C{:}\text{type}}{\Gamma \vdash_\Sigma M\ N \downarrow C}$$

Immediate by inductive hypothesis.

The proofs of (2) and (3) are similar. □

The following (quite technical) lemmas show that the class of dependency-preserving terms is closed with respect to β- and η-reduction, and also, under some circumstances, under η-expansion.

Lemma 4.4. *If $\Gamma \vdash_\Sigma^\preceq M : A$ and $M \to_\beta M'$ then $\Gamma \vdash_\Sigma^\preceq M' : A$.*

Proof. By induction on the derivation of $\Gamma \vdash_\Sigma^\preceq M : A$. Application is the only interesting case:

$$\frac{\Gamma \vdash_\Sigma^\preceq M_1{:}\Pi x{:}B.A \quad \Gamma \vdash_\Sigma^\preceq M_2{:}B}{\Gamma \vdash_\Sigma^\preceq M_1\ M_2{:}[M_2/x]A}$$

We have to distinguish three possible subcases:

- $M_1\ M_2 \to_\beta M_1'\ M_2$
  By inductive hypothesis $\Gamma \vdash_\Sigma^\preceq M_1' : \Pi x : B.A$, hence the result.
- $M_1\ M_2 \to_\beta M_1\ M_2'$
  By inductive hypothesis $\Gamma \vdash_\Sigma^\preceq M_2' : B$. From $\Gamma \vdash_\Sigma^\preceq M_1\ M_2 : [M_2/x]A$ we get $\Gamma \vdash_\Sigma^\preceq [M_2/x]A$: type, and clearly $[M_2'/x]A \equiv [M_2/x]A$, so

$$\frac{\dfrac{\Gamma \vdash_\Sigma^\preceq M_1{:}\Pi x{:}B.A \quad \Gamma \vdash_\Sigma^\preceq M_2'{:}B}{\Gamma \vdash_\Sigma^\preceq M_1\ M_2'{:}[M_2'/x]A} \quad [M_2'/x]A \equiv [M_2/x]A \quad \Gamma \vdash_\Sigma^\preceq [M_2/x]A{:}\text{type}}{\Gamma \vdash_\Sigma^\preceq M_1\ M_2'{:}[M_2/x]A}$$

- $(\lambda x : B.M_1')M_2 \to_\beta [M_2/x]M_1'$
  By inversion and type conversion, $\Gamma, x : B' \vdash_\Sigma^\preceq M_1' : A$ and $\Gamma \vdash_\Sigma^\preceq M_2 : B'$. The result then follows by Substitution.

□

Corollary 4.5. *If $\Gamma \vdash_\Sigma^\preceq M : A$ and $M \to_\beta^* M'$ then $\Gamma \vdash_\Sigma^\preceq M' : A$.*

Lemma 4.6. *If $\Gamma \vdash_\Sigma^\preceq M : A$ and $M \to_\eta M'$ then $\Gamma \vdash_\Sigma^\preceq M' : A$.*

Proof. By induction on the derivation of $\Gamma \vdash_\Sigma^\preceq M : A$. Abstraction is the only interesting case:

$$\frac{\Gamma \vdash_\Sigma^\preceq A{:}\text{type} \quad \Gamma, x{:}B \vdash_\Sigma^\preceq M_1{:}A}{\Gamma \vdash_\Sigma^\preceq \lambda x{:}B.M_1{:}\Pi x{:}B.A}\ A \preceq_\Sigma^M B$$

We have to distinguish two possible subcases:

- $\lambda x : A.M_1 \to_\eta \lambda x : A.M_1'$
  By inductive hypothesis $\Gamma, x : B \vdash_\Sigma^\preceq M_1' : A$, hence the result.
- $\lambda x : A.M_1 = \lambda x : B.(M_1'\ x) \to_\eta M_1'$
  By inversion (and type conversion, if necessary) $\Gamma \vdash_\Sigma^\preceq M_1' : \Pi x : B.A$.

□

Corollary 4.7. *If $\Gamma \vdash_\Sigma^\preceq M : A$ and $M \to_\eta^* M'$ then $\Gamma \vdash_\Sigma^\preceq M' : A$.*

Lemma 4.8. *If $\Gamma \vdash_\Sigma^\preceq M \downarrow C$, then there is $M' \to_\eta^* M$ such that $\Gamma \vdash_\Sigma^\preceq M' \Downarrow C$.*

Proof. The induction is on the structure of C:

- Case $C = \Pi x : A.B$:

  From the assumptions, one gets $\Gamma \vdash_{\Sigma}^{\preceq} \Pi x : A.B : \mathrm{type}$, and by inversion, $\Gamma \vdash_{\Sigma}^{\preceq} A : \mathrm{type}$, so $\Gamma, x : A \vdash_{\Sigma}^{\preceq} x \downarrow A$ and by inductive hypothesis we get a $N \to_{\eta}^{*} x$ such that $\Gamma, x : A \vdash_{\Sigma}^{\preceq} N \Downarrow A$.

  By inversion again, from $\Gamma \vdash_{\Sigma}^{\preceq} \Pi x : A.B : \mathrm{type}$ one also gets $\Gamma, x : A \vdash_{\Sigma}^{\preceq} B : \mathrm{type}$, and since $\Gamma, x : A \vdash_{\Sigma}^{\preceq} M\ N \downarrow B$, we can apply the inductive hypothesis once more to get a $M' \to_{\eta}^{*} M\ N$ such that $\Gamma, x : A \vdash_{\Sigma}^{\preceq} M' \Downarrow B$. Then $\lambda x : A.M'$ is as required.
- Case $C = A\ N$ or $C = a$

  From the assumptions $\Gamma \vdash_{\Sigma}^{\preceq} C : \mathrm{type}$, and by Theorem 4.2 there is $C' \equiv C$ such that $\Gamma \vdash_{\Sigma} C' \Downarrow \mathrm{type}$. By inversion then $\Gamma \vdash_{\Sigma} C' \downarrow \mathrm{type}$, and, since $\Gamma \vdash_{\Sigma} M \downarrow C'$ by type conversion, we get $\Gamma \vdash_{\Sigma} M \Downarrow C'$. By conversion again, we get finally $\Gamma \vdash_{\Sigma} M \Downarrow C$.

□

Proposition 4.9. *Let $C \equiv C'$, $\Gamma \vdash_{\Sigma}^{\preceq} C' : \mathrm{type}$, then:*

1. *If $\Gamma, x : C, \Delta \vdash_{\Sigma}^{\preceq} M \Downarrow A$ then $\Gamma, x : C', \Delta \vdash_{\Sigma}^{\preceq} M \Downarrow A$.*
2. *If $\Gamma, x : C, \Delta \vdash_{\Sigma}^{\preceq} A \Downarrow \mathrm{type}$ then $\Gamma, x : C', \Delta \vdash_{\Sigma}^{\preceq} A \Downarrow \mathrm{type}$.*
3. *If $\Gamma, x : C, \Delta \vdash_{\Sigma}^{\preceq} M \downarrow A$ then $\Gamma, x : C', \Delta \vdash_{\Sigma}^{\preceq} M \downarrow A$.*
4. *If $\Gamma, x : C, \Delta \vdash_{\Sigma}^{\preceq} A \downarrow K$ then $\Gamma, x : C', \Delta \vdash_{\Sigma}^{\preceq} A \downarrow K$.*

Proof. By an easy induction on the derivations. Replace

$$\frac{}{\Gamma, x{:}C, \Delta \vdash_{\Sigma}^{\preceq} x \downarrow C}$$

with

$$\frac{\dfrac{}{\Gamma, x{:}C', \Delta \vdash_{\Sigma}^{\preceq} x \downarrow C'} \quad C' \equiv C \quad \Gamma, x{:}C, \Delta \vdash_{\Sigma}^{\preceq} C{:}\mathrm{type}}{\Gamma \vdash_{\Sigma}^{\preceq} x \downarrow C}$$

□

Theorem 4.10. *We have:*

1. *If $\Gamma \vdash_{\Sigma}^{\preceq} M : A$ then there is a $M' \equiv M$ such that $\Gamma \vdash_{\Sigma}^{\preceq} M' \Downarrow A$.*
2. *If $\Gamma \vdash_{\Sigma}^{\preceq} A : \mathrm{type}$ then there is a $A' \equiv A$ such that $\Gamma \vdash_{\Sigma}^{\preceq} A' \Downarrow \mathrm{type}$.*
3. *If $\Gamma \vdash_{\Sigma}^{\preceq} M : A$ and $M = h\overline{N}$ where h constant or variable, then there is a $M' \equiv M$ such that $\Gamma \vdash_{\Sigma}^{\preceq} M' \downarrow A$.*
4. *If $\Gamma \vdash_{\Sigma}^{\preceq} A : K$ and $A = a\overline{N}$, then there is a $A' \equiv A$ such that $\Gamma \vdash_{\Sigma}^{\preceq} A' \downarrow K$.*

Proof. By (simultaneous) inductions on the derivations. By Corollary 4.5, in (1) and (3) we will furthermore assume, without loss of generality, M in β-normal form.

- Type constant:

  $$\frac{\Sigma(a) = K}{\Gamma \vdash_{\Sigma}^{\preceq} a{:}K}$$

  We have immediately $\Gamma \vdash_{\Sigma}^{\preceq} a \downarrow K$. If $K = \mathrm{type}$, we have also $\Gamma \vdash_{\Sigma}^{\preceq} a \Downarrow \mathrm{type}$.

- Type application:

  $$\frac{\Gamma \vdash_{\Sigma}^{\preceq} A{:}\Pi x{:}B.K \quad \Gamma \vdash_{\Sigma}^{\preceq} M{:}B}{\Gamma \vdash_{\Sigma}^{\preceq} A\ M{:}[M/x]K}$$

  By inversion we easily see $A = a\overline{N}$, hence by inductive hypothesis we get $A' \equiv A$ and $M' \equiv M$ such that $\Gamma \vdash_{\Sigma}^{\preceq} A' \downarrow \Pi x : B.K$ and $\Gamma \vdash_{\Sigma}^{\preceq} M' \Downarrow B$, and therefore $\Gamma \vdash_{\Sigma}^{\preceq} A'M' \downarrow [M'/x]K$.

  From $\Gamma \vdash_{\Sigma}^{\preceq} A : \Pi x : B.K$ we get $\Gamma \vdash_{\Sigma}^{\preceq} \Pi x : B.K\ Kind$, and by inversion $\Gamma, x : B \vdash_{\Sigma}^{\preceq} K\ Kind$. Therefore by Substitution $\Gamma \vdash_{\Sigma}^{\preceq} [M/x]K\ Kind$, and hence by conversion $\Gamma \vdash_{\Sigma}^{\preceq} A'M' \downarrow [M/x]K$. If $K = \mathrm{type}$, we have also $\Gamma \vdash_{\Sigma}^{\preceq} A'M' \Downarrow \mathrm{type}$.

- Type abstraction:

$$\frac{\Gamma \vdash^{\preceq}_{\Sigma} A\text{:type} \quad \Gamma, x{:}A \vdash^{\preceq}_{\Sigma} B\text{:type}}{\Gamma \vdash^{\preceq}_{\Sigma} \Pi x{:}A.B\text{:type}} \; A \preceq^{M}_{\Sigma} B$$

  From the inductive hypotheses we get $A' \equiv A$ and $B' \equiv B$ such that $\Gamma \vdash^{\preceq}_{\Sigma} A' \Downarrow \text{type}$ and $\Gamma, x : A \vdash^{\preceq}_{\Sigma} B' \Downarrow \text{type}$. Using Proposition 4.9 we conclude $\Gamma \vdash^{\preceq}_{\Sigma} \Pi x : A'.B' \Downarrow \text{type}$.

- Kind conversion:

$$\frac{\Gamma \vdash^{\preceq}_{\Sigma} A{:}K \quad K \equiv K' \quad \Gamma \vdash^{\preceq}_{\Sigma} K' \; Kind}{\Gamma \vdash^{\preceq}_{\Sigma} A{:}K'}$$

  Immediate from inductive hypothesis.

- Term constant:

$$\frac{\Sigma(c) = A}{\Gamma \vdash^{\preceq}_{\Sigma} c{:}A}$$

  We get immediately $\Gamma \vdash^{\preceq}_{\Sigma} c \downarrow A$; (1) then follows from Lemma 4.8.

- Term variable:

$$\frac{\Gamma(x) = A}{\Gamma \vdash_{\Sigma} x{:}A}$$

  We get immediately $\Gamma \vdash^{\preceq}_{\Sigma} x \downarrow A$; (1) then follows from Lemma 4.8.

- Term application:

$$\frac{\Gamma \vdash^{\preceq}_{\Sigma} M{:}\Pi x{:}B.A \quad \Gamma \vdash^{\preceq}_{\Sigma} N{:}B}{\Gamma \vdash^{\preceq}_{\Sigma} M\ N{:}[N/x]A}$$

  Since M in β-normal form, by inductive hypothesis we get $M' \equiv M$ and $N' \equiv N'$ such that $\Gamma \vdash^{\preceq}_{\Sigma} M' \downarrow \Pi x : B.A$ and $\Gamma \vdash^{\preceq}_{\Sigma} N' \Downarrow B$, and hence $\Gamma \vdash^{\preceq}_{\Sigma} M'N' \downarrow [M'/x]A$.

  From $\Gamma \vdash^{\preceq}_{\Sigma} M : \Pi x : B.A$ we get $\Gamma \vdash^{\preceq}_{\Sigma} \Pi x : B.A$ type, and by inversion $\Gamma, x : B \vdash^{\preceq}_{\Sigma} A$ type. Therefore by Substitution $\Gamma \vdash^{\preceq}_{\Sigma} [M/x]A \; Kind$, and hence by type conversion $\Gamma \vdash^{\preceq}_{\Sigma} M'N' \downarrow [M/x]A$. Once again, (1) follows from Lemma 4.8.

- Term abstraction:

$$\frac{\Gamma \vdash^{\preceq}_{\Sigma} A\text{:type} \quad \Gamma, x{:}A \vdash^{\preceq}_{\Sigma} M{:}B}{\Gamma \vdash^{\preceq}_{\Sigma} \lambda x{:}A.M{:}\Pi x{:}A.B} \; A \preceq^{M}_{\Sigma} B$$

  From the inductive hypotheses we get $A' \equiv A$ and $M' \equiv M$ such that $\Gamma \vdash^{\preceq}_{\Sigma} A' \Downarrow \text{type}$ and $\Gamma, x : A \vdash^{\preceq}_{\Sigma} M' \Downarrow B$. By Proposition 4.9 one obtain $\Gamma \vdash^{\preceq}_{\Sigma} \lambda x : A'.M' \Downarrow \Pi x : A'.B$.

  From $\Gamma \vdash^{\preceq}_{\Sigma} \lambda x : A.M : \Pi x : A.B$ we get $\Gamma \vdash^{\preceq}_{\Sigma} \Pi x : A.B$ type, and therefore by type conversion $\Gamma \vdash^{\preceq}_{\Sigma} \lambda x : A'.M' \Downarrow \Pi x : A.B$.

- Type conversion:

$$\frac{\Gamma \vdash^{\preceq}_{\Sigma} M{:}A \quad A \equiv A' \quad \Gamma \vdash^{\preceq}_{\Sigma} A'\text{:type}}{\Gamma \vdash^{\preceq}_{\Sigma} M{:}A'}$$

  Immediate by inductive hypothesis.

□

Corollary 4.11. *If $\Gamma \vdash^{\preceq}_{\Sigma} M : A$ then there are M', M'' such that $M \to^{*}_{\beta} M'$, $M'' \to^{*}_{\eta} M'$, $\Gamma \vdash^{\preceq}_{\Sigma} M'' \Downarrow A$*

Proof. By inspection of the proof of Theorem 4.10 and commutativity of β reduction and η expansion. □

Notation. Given a well-typed term M or a type family A, we will denote their canonical form by $M_{\Downarrow}$ and $A_{\Downarrow}$, respectively.

Lemma 4.12. *Let $\Gamma \vdash^{\preceq}_{\Sigma} E[\![\Gamma_{\circ} \vdash \circ : A_{\circ}]\!] : A$ an environment and $\Gamma_{\circ} \vdash^{\preceq}_{\Sigma} M : A_{\circ}$ a compatible term.*

1. *If $\Gamma \vdash^{\preceq}_{\Sigma} E[\![M]\!] \Downarrow A$ then $\Gamma_{\circ} \vdash^{\preceq}_{\Sigma} M \Downarrow A_{\circ}$ or $\Gamma_{\circ} \vdash^{\preceq}_{\Sigma} M \downarrow A_{\circ}$. Moreover, if $\Gamma_{\circ} \vdash^{\preceq}_{\Sigma} M \Downarrow A_{\circ}$ ($\Gamma_{\circ} \vdash^{\preceq}_{\Sigma} M \downarrow A_{\circ}$) then for all $\Gamma_{\circ} \vdash^{\preceq}_{\Sigma} N \Downarrow A_{\circ}$ ($\Gamma_{\circ} \vdash^{\preceq}_{\Sigma} N \downarrow A_{\circ}$) we have $\Gamma \vdash^{\preceq}_{\Sigma} E[\![N]\!] \Downarrow A$.*

2. *If* $\Gamma \vdash^{\preceq}_{\Sigma} E[\![M]\!] \downarrow A$ *then* $\Gamma_\circ \vdash^{\preceq}_{\Sigma} M \Downarrow A_\circ$ *or* $\Gamma_\circ \vdash^{\preceq}_{\Sigma} M \downarrow A_\circ$. *Moreover, if* $\Gamma_\circ \vdash^{\preceq}_{\Sigma} M \Downarrow A_\circ$ *(*$\Gamma_\circ \vdash^{\preceq}_{\Sigma} M \downarrow A_\circ$*) then for all* $\Gamma_\circ \vdash^{\preceq}_{\Sigma} N \Downarrow A_\circ$ *(*$\Gamma_\circ \vdash^{\preceq}_{\Sigma} N \downarrow A_\circ$*) we have* $\Gamma \vdash^{\preceq}_{\Sigma} E[\![N]\!] \downarrow A$.

Proof. By induction on $\Gamma \vdash^{\preceq}_{\Sigma} E[\![\Gamma_\circ \vdash \circ : A_\circ]\!] : A$, using Lemma 3.10 and Inversion. □

Definition 4.13. Given two contexts Γ and Δ, a substitution from Γ to Δ is a type-preserving, finite-support mapping from variables to terms $\theta : \Gamma \rightharpoondown \Delta$ formed according to the following rules:

$$\frac{}{\cdot : \cdot \rightharpoondown \Delta}$$

$$\frac{\{\overline{x} \mapsto \overline{M}\} : \Gamma \rightharpoondown \Delta \quad \Delta \vdash_\Sigma N \Downarrow [\overline{M}/\overline{x}]A}{\{\overline{x} \mapsto \overline{M}, y \mapsto N\} : (\Gamma, y{:}A) \rightharpoondown \Delta}$$

Dependency-preserving substitution are defined by the rules:

$$\frac{}{\cdot : \cdot \overset{\preceq}{\rightharpoondown} \Delta}$$

$$\frac{\{\overline{x} \mapsto \overline{M}\} : \Gamma \overset{\preceq}{\rightharpoondown} \Delta \quad \Delta \vdash^{\preceq}_\Sigma N \Downarrow [\overline{M}/\overline{x}]A}{\{\overline{x} \mapsto \overline{M}, y \mapsto N\} : (\Gamma, y{:}A) \overset{\preceq}{\rightharpoondown} \Delta}$$

Definition 4.14. Given any well-typed term $\Gamma \vdash_\Sigma M : A$ and substitution $\theta = \{\overline{x} \mapsto \overline{N}\} : \Gamma \rightharpoondown \Delta$, define θM to be the (unique) canonical form of

$$\Delta \vdash_\Sigma [\overline{N}/\overline{x}]M : [\overline{N}/\overline{x}]A$$

Similarly, given $\Gamma \vdash_\Sigma A : \mathrm{type}$ we also define θA.

Note that here, in analogy to [9], we define the result of a substitution application to be a canonical term. This will simplify considerably some proofs in the next section.

Definition 4.15. We define:

1. Given two substitutions $\theta_1 = \{\overline{x} \mapsto \overline{M}\} : \Gamma_1 \rightharpoondown \Gamma_2$ and $\theta_2 : \Gamma_2 \rightharpoondown \Gamma_3$, the *composition* $\theta_2 \circ \theta_1$ is the substitution $\theta_2 \circ \theta_1 = \{\overline{x} \mapsto \overline{\theta_2 M}\} : \Gamma_1 \rightharpoondown \Gamma_3$.
2. A substitution $\theta = \{\overline{x} \mapsto \overline{M}\} : \Gamma \rightharpoondown \Delta$ is a *renaming* if all the terms M_i are (convertible to) distinct variables.
3. A substitution $\theta_1 : \Gamma \rightharpoondown \Delta$ is said to be *more general* than $\theta_2 : \Gamma \rightharpoondown \Delta'$ if there is $\rho : \Delta \rightharpoondown \Delta'$ such that $\theta_2 = \rho \circ \theta_1$.
4. Given two well typed terms $\Gamma \vdash_\Sigma M : A$ and $\Gamma \vdash_\Sigma N : A'$, a substitution $\theta : \Gamma \rightharpoondown \Delta$ is said to be a *unifier* of M and N if $\theta M = \theta N$; M and N are then said to unify.

The class of dependency-preserving terms is closed with respect to substitution application:

Proposition 4.16. *Let* $\theta = \{\overline{x} \mapsto \overline{N}\} : \Gamma \overset{\preceq}{\rightharpoondown} \Delta$*,*

1. *If* $\Gamma \vdash^{\preceq}_\Sigma M : A$ *then* $\Delta \vdash^{\preceq}_\Sigma \theta M : [\overline{N}/\overline{x}]A$.
2. *If* $\Gamma \vdash^{\preceq}_\Sigma A : \mathrm{type}$ *then* $\Delta \vdash^{\preceq}_\Sigma \theta A : [\overline{N}/\overline{x}]K$.

Proof. (1) First assume $\mathrm{dom}\,\Gamma \cap \mathrm{dom}\,\Delta = \emptyset$. Then by Weakening one gets $\Delta, \Gamma \vdash^{\preceq}_\Sigma M : A$ and $\Delta \vdash^{\preceq}_\Sigma N_i : B_i$ for all i. By repeated applications of Weakening and Substitution from these one gets the result.

If $\mathrm{dom}\,\Gamma \cap \mathrm{dom}\,\Delta \neq \emptyset$, let $\rho : \Delta \overset{\preceq}{\rightharpoondown} \Delta'$ a renaming into a set of fresh variables. Using the proof above, one easily show, by induction on $\theta : \Gamma \overset{\preceq}{\rightharpoondown} \Delta$ that $\theta' = \rho \circ \theta : \Gamma \overset{\preceq}{\rightharpoondown} \Delta'$. Moreover, it is immediate to see $\rho^{-1} : \Delta' \overset{\preceq}{\rightharpoondown} \Delta$ and $\theta M = \rho^{-1}(\theta' M)$, hence, by using again (twice) the proof above, one gets the result.

(2) Similar. □

Corollary 4.17. *If* $\theta_1 : \Gamma_1 \overset{\preceq}{\rightharpoondown} \Gamma_2$ *and* $\theta_2 : \Gamma_2 \overset{\preceq}{\rightharpoondown} \Gamma_3$*, then* $\theta_2 \circ \theta_1 : \Gamma_1 \overset{\preceq}{\rightharpoondown} \Gamma_3$.

Proof. By induction on the derivation of $\theta_1 : \Gamma_1 \overset{\preceq}{\rightharpoondown} \Gamma_2$. □

Definition 4.18. A canonical term $\Gamma \vdash_\Sigma M \Downarrow A$ is said to be a pattern if each $x \in \mathrm{dom}\,\Gamma$ can appear in M and A only applied to terms η-equivalent to distinct bound variables.

Theorem 4.19. *Unification of patterns is decidable; if two patterns unify, there is a unique (up to conversion) most general unifier.*

Proof. See [11]. $\square$

5. Higher-Order Term Rewriting

In this section we extend the notion of term rewriting system and rewriting relation to a higher-order setting with dependent types.

Definition 5.1. A rewrite rule $\Gamma \vdash^{\preceq}_{\Sigma} l \to r : A$ is a pair of well typed terms such that

- $\Gamma \vdash^{\preceq}_{\Sigma} l \Downarrow A$ is a pattern, $\Gamma \vdash^{\preceq}_{\Sigma} r : A$,
- $\Gamma \vdash^{\preceq}_{\Sigma} A \downarrow \mathrm{type}$,
- $\mathcal{FV}(l) \supseteq \mathcal{FV}(r)$.

A higher-order term rewriting system (HTRS) R is a finite set of rewrite rules, such that, for each pair of rules $\Gamma_1 \vdash^{\preceq}_{\Sigma} l_1 \to r_1 : A_1, \Gamma_2 \vdash^{\preceq}_{\Sigma} l_2 \to r_2 : A_2 \in R$, $A_1 \not\preceq^A A_2$.

The condition above translates to the requirement that it is not possible to use a rewrite rule to rewrite the type of another. This is therefore consistent with the original goal to define rewriting in such a way that it does not modify types, and hence preserve well-typedness of expressions.

Moreover, under this assumption, as we will see, the critical pair criterion will involve, precisely like the first order case, a check for overlaps only among the left-hand-sides of the rules.

Example 2. In the formalization of the simply-typed lambda calculus given before, β and η reductions can be expressed as rewrite rules:

$$A : \mathbf{type}, B : \mathbf{type}, F : (\mathbf{term}\ A) \Rightarrow (\mathbf{term}\ B), U : \mathbf{term}\ A \vdash^{\preceq}_{\Sigma} (\mathbf{app}\ (\mathbf{lambda}\ F)\ U) \to (F\ U) : \mathbf{term}\ B$$

$$A : \mathbf{type}, B : \mathbf{type}, G : \mathbf{term}\ (\mathbf{arrow}\ A\ B) \vdash^{\preceq}_{\Sigma} \mathbf{lambda}(\lambda x : \mathbf{term}\ A.\mathbf{app}\ G\ x) \to G : \mathbf{term}(\mathbf{arrow}\ A\ B)$$

The check that both rules are well-typed and preserve dependencies is left to the reader.

Definition 5.2. Given a HTRS R and two terms $\Gamma \vdash^{\preceq}_{\Sigma} M : A$ and $\Gamma \vdash^{\preceq}_{\Sigma} N : A$ we define R-rewriting as follows:

$$\Gamma \vdash^{\preceq}_{\Sigma} M \xrightarrow{R} N : A \overset{def}{\Longleftrightarrow} M_{\Downarrow} = E[\![\theta l]\!], N_{\Downarrow} = E[\![\theta r]\!] \text{ for some } (\Delta \vdash l \to r : B) \in R, \theta : \Delta \xrightarrow{\preceq} \Gamma(M_{\Downarrow}, \theta l),$$
$$\text{and } \Gamma \vdash^{\preceq}_{\Sigma} E[\![\Gamma(M_{\Downarrow}, \theta l) \vdash \circ : A(M_{\Downarrow}, \theta l)]\!] : A.$$

We furthermore define R-conversion as the judgement $\Gamma \vdash^{\preceq}_{\Sigma} M \xleftrightarrow{R} N : A$ formed according to the following rules:

$$\frac{\Gamma \vdash^{\preceq}_{\Sigma} M : A \quad M \equiv N \quad \Gamma \vdash^{\preceq}_{\Sigma} N : A}{\Gamma \vdash^{\preceq}_{\Sigma} M \xleftrightarrow{R} N : A} \qquad \frac{\Gamma \vdash^{\preceq}_{\Sigma} M \xrightarrow{R} N : A}{\Gamma \vdash^{\preceq}_{\Sigma} M \xleftrightarrow{R} N : A}$$

$$\frac{\Gamma \vdash^{\preceq}_{\Sigma} M \xleftrightarrow{R} N : A}{\Gamma \vdash^{\preceq}_{\Sigma} N \xleftrightarrow{R} M : A} \qquad \frac{\Gamma \vdash^{\preceq}_{\Sigma} M \xleftrightarrow{R} N' : A \quad \Gamma \vdash^{\preceq}_{\Sigma} N' \xleftrightarrow{R} N : A}{\Gamma \vdash^{\preceq}_{\Sigma} M \xleftrightarrow{R} N : A}$$

In addition to R-conversion, we introduce a more natural notion of equality modulo R, as a congruence relation containing all instances of R, and closed with respect to conversion:

Definition 5.3. Let R be a HTRS, congruence modulo R is defined by the judgement

$$\Gamma \vdash^{\preceq}_{\Sigma} M \overset{R}{=} N : A \rhd \mathcal{D} \qquad M \text{ and } N \text{ of type } A \text{ are congruent modulo } R$$

where $\mathcal{D}$ is a set of type constants used to keep track of the dependency constraints. The rules associated to this judgement are the following:

$$\frac{\Gamma \vdash_\Sigma^\preceq M:A}{\Gamma \vdash_\Sigma^\preceq M \stackrel{R}{=} M:A \rhd \emptyset} \quad \frac{\Gamma \vdash_\Sigma^\preceq M \stackrel{R}{=} N:A \rhd \mathcal{D}}{\Gamma \vdash_\Sigma^\preceq N \stackrel{R}{=} M:A \rhd \mathcal{D}}$$

$$\frac{\Gamma \vdash_\Sigma^\preceq M \stackrel{R}{=} N':A \rhd \mathcal{D} \quad \Gamma \vdash_\Sigma^\preceq N' \stackrel{R}{=} N:A \rhd \mathcal{D}'}{\Gamma \vdash_\Sigma^\preceq M \stackrel{R}{=} N:A \rhd (\mathcal{D} \cup \mathcal{D}')}$$

$$\frac{\Delta \vdash_\Sigma^\preceq l \to r:A \in R \quad \theta:\Delta \stackrel{\preceq}{\to} \Gamma}{\Gamma \vdash_\Sigma^\preceq \theta l \stackrel{R}{=} \theta r:\theta A \rhd \{\mathrm{head}(A)\}}$$

$$\frac{\Gamma \vdash_\Sigma^\preceq A:\mathrm{type} \quad \Gamma, x:A \vdash_\Sigma^\preceq M \stackrel{R}{=} N:B \rhd \mathcal{D}}{\Gamma \vdash_\Sigma^\preceq \lambda x:A.M \stackrel{R}{=} \lambda x:A.N:\Pi x:A.B \rhd \mathcal{D}} \ A \preceq_\Sigma^M B$$

$$\frac{\Gamma \vdash_\Sigma^\preceq M \stackrel{R}{=} M':\Pi x:A.B \rhd \mathcal{D} \quad \Gamma \vdash_\Sigma^\preceq N \stackrel{R}{=} N':A \rhd \mathcal{D}'}{\Gamma \vdash_\Sigma^\preceq M\ N \stackrel{R}{=} M'\ N':[N/x]B \rhd (\mathcal{D} \cup \mathcal{D}')} \ a \not\preceq^A B \text{ for all } a \in \mathcal{D}'$$

$$\frac{\Gamma \vdash_\Sigma^\preceq M \stackrel{R}{=} N':A \rhd \mathcal{D} \quad N' \equiv N \quad \Gamma \vdash_\Sigma^\preceq N':A}{\Gamma \vdash_\Sigma^\preceq M \stackrel{R}{=} N:A \rhd \mathcal{D}}$$

The only place the set of dependency $\mathcal{D}$ above plays a role is in the application rule: there, it restricts the rule to those cases where well-typedness of both sides is guaranteed. An analogous set is defined for R-rewriting:

Definition 5.4. The set of dependency constraints generated by a R-rewriting step is defined as

$$(\Gamma \vdash_\Sigma^\preceq M \stackrel{R}{\longrightarrow} N : A) \Vdash \{\mathrm{head}(B)\}$$

if $(\Delta \vdash_\Sigma^\preceq l \to r : B) \in R$ was the rewriting rule used in its definition.

This definition is extended to R-conversion:

$$\frac{\Gamma \vdash_\Sigma^\preceq M:A \quad M \equiv N \quad \Gamma \vdash_\Sigma^\preceq N:A}{(\Gamma \vdash_\Sigma^\preceq M \stackrel{R}{\longleftrightarrow} N:A) \Vdash \emptyset} \qquad \frac{(\Gamma \vdash_\Sigma^\preceq M \stackrel{R}{\longrightarrow} N:A) \Vdash \mathcal{D}}{(\Gamma \vdash_\Sigma^\preceq M \stackrel{R}{\longleftrightarrow} N:A) \Vdash \mathcal{D}}$$

$$\frac{(\Gamma \vdash_\Sigma^\preceq M \stackrel{R}{\longleftrightarrow} N:A) \Vdash \mathcal{D}}{(\Gamma \vdash_\Sigma^\preceq N \stackrel{R}{\longleftrightarrow} M:A) \Vdash \mathcal{D}} \qquad \frac{(\Gamma \vdash_\Sigma^\preceq M \stackrel{R}{\longleftrightarrow} N':A) \Vdash \mathcal{D} \quad (\Gamma \vdash_\Sigma^\preceq N' \stackrel{R}{\longleftrightarrow} N:A) \Vdash \mathcal{D}'}{(\Gamma \vdash_\Sigma^\preceq M \stackrel{R}{\longleftrightarrow} N:A) \Vdash (\mathcal{D} \cup \mathcal{D}')}$$

The main theorem of this section will be the following:

Theorem 5.5. *Let R be a HTRS, then for all M, N,*

$$(\Gamma \vdash_\Sigma^\preceq M \stackrel{R}{\longleftrightarrow} N : A) \Vdash \mathcal{D} \Leftrightarrow \Gamma \vdash_\Sigma^\preceq M \stackrel{R}{=} N : A \rhd \mathcal{D}.$$

One direction is easy to prove:

Lemma 5.6. *If $\Gamma \vdash_\Sigma^\preceq E[\![\Gamma_\circ \vdash \circ : A_\circ]\!] : A$ and $\Gamma_\circ \vdash_\Sigma^\preceq M \stackrel{R}{=} N : A_\circ \rhd \{head(A_\circ)\}$ then $\Gamma \vdash_\Sigma^\preceq E[\![M]\!] \stackrel{R}{=} E[\![N]\!] : A \rhd \{head(A_\circ)\}$.*

Proof. By an easy induction on the derivation of $\Gamma \vdash_\Sigma^\preceq E[\![\Gamma_\circ \vdash \circ : A_\circ]\!] : A$. We check the case:

$$\frac{\Gamma \vdash_\Sigma^\preceq M_1:\Pi x:B.A \quad \Gamma \vdash_\Sigma^\preceq E_2[\![\Gamma_\circ \vdash \circ:A_\circ]\!]:B}{\Gamma \vdash_\Sigma^\preceq M_1(E_2[\![\Gamma_\circ \vdash \circ:A_\circ]\!]):A} \quad A_\circ \not\preceq^A A$$

By reflexivity, $\Gamma \vdash_\Sigma^{\preceq} M_1 \overset{R}{=} M_1 : \Pi x : B.A \rhd \emptyset$, and by inductive hypothesis $\Gamma \vdash_\Sigma^{\preceq} E_2[\![M]\!] \overset{R}{=} E_2[\![N]\!] : B \rhd \{head(A_\circ)\}$. By hypothesis $A_\circ \not\prec^A A$, hence by the application rule:

$$\frac{\Gamma\vdash_\Sigma^{\preceq} M_1 \overset{R}{=} M_1 : \Pi x{:}B.A \rhd \emptyset \quad \Gamma\vdash_\Sigma^{\preceq} E_2[\![M]\!] \overset{R}{=} E_2[\![N]\!] : B \rhd \{head(A_\circ)\}}{\Gamma\vdash_\Sigma^{\preceq} (M_1\ E_2[\![M]\!]) \overset{R}{=} (M_1\ E_2[\![N]\!]) : [E_2[\![M]\!]/x]A \rhd \{head(A_\circ)\}}$$

To conclude the proof we have to show that $x \notin \mathcal{FV}(A)$, so that $[E_2[\![M]\!]/x]A = A$. If not, then $B \prec^A A$, and since we know $A_\circ \preceq^M B$ from $\Gamma \vdash_\Sigma^{\preceq} E_2[\![\Gamma_\circ \vdash \circ : A_\circ]\!] : B$, we conclude $A_\circ \prec^A A$, a contradiction. □

Corollary 5.7. *Let R be a HTRS, if $(\Gamma \vdash_\Sigma^{\preceq} M \overset{R}{\longleftrightarrow} N : A) \Vdash \mathcal{D}$ then $\Gamma \vdash_\Sigma^{\preceq} M \overset{R}{=} N : A \rhd \mathcal{D}$.*

Proof. By induction on the derivation of $(\Gamma \vdash_\Sigma^{\preceq} M \overset{R}{\longleftrightarrow} N : A) \Vdash \mathcal{D}$. We consider two cases:

- Conversion:

$$\frac{\Gamma\vdash_\Sigma^{\preceq} M{:}A \quad M\equiv N \quad \Gamma\vdash_\Sigma^{\preceq} N{:}A}{(\Gamma\vdash_\Sigma^{\preceq} M \overset{R}{\longleftrightarrow} N{:}A) \Vdash \emptyset}$$

  From $\Gamma \vdash_\Sigma^{\preceq} M : A$ by reflexivity we get $\Gamma \vdash_\Sigma^{\preceq} M \overset{R}{=} M : A \rhd \emptyset$ and by the term conversion rule the result:

$$\frac{\Gamma\vdash_\Sigma^{\preceq} M \overset{R}{=} M{:}A \rhd \emptyset \quad M\equiv N \quad \Gamma\vdash_\Sigma^{\preceq} N{:}A}{\Gamma\vdash_\Sigma^{\preceq} M \overset{R}{=} N{:}A \rhd \emptyset}$$

- R-rewriting:

$$\frac{(\Gamma\vdash_\Sigma^{\preceq} M \overset{R}{\longrightarrow} N{:}A) \Vdash \mathcal{D}}{(\Gamma\vdash_\Sigma^{\preceq} M \overset{R}{\longleftrightarrow} N{:}A) \Vdash \mathcal{D}}$$

  By definition, $\Gamma \vdash_\Sigma^{\preceq} M \overset{R}{\longrightarrow} N : A$ if there are $(\Delta \vdash_\Sigma^{\preceq} l \to r : B) \in R$, $\theta : \Delta \overset{\preceq}{\to} \Gamma(M_\Downarrow, \theta l)$, and $\Gamma \vdash_\Sigma^{\preceq} E[\![\Gamma(M_\Downarrow, \theta l) \vdash \circ : A(M_\Downarrow, \theta l)]\!] : A$ such that $M_\Downarrow = E[\![\theta l]\!], N_\Downarrow = E[\![\theta r]\!]$.

  By reflexivity and conversion, like the previous case, we get $\Gamma \vdash_\Sigma^{\preceq} M \overset{R}{=} E[\![\theta l]\!] : A \rhd \emptyset$ and $\Gamma \vdash_\Sigma^{\preceq} E[\![\theta r]\!] \overset{R}{=} N : A \rhd \emptyset$. Also, $\Gamma(M_\Downarrow, \theta l) \vdash_\Sigma^{\preceq} \theta l \overset{R}{=} \theta r : A(M_\Downarrow, \theta l) \rhd \mathcal{D}$, where $\mathcal{D} = \{\text{head}(B)\} = \{\text{head}(A(M_\Downarrow, \theta l))\}$, so applying the Lemma we get $\Gamma \vdash_\Sigma^{\preceq} E[\![\theta l]\!] \overset{R}{=} E[\![\theta r]\!] : A \rhd \{\text{head}(B)\}$, and by transitivity the result.

□

To prove the other direction of Theorem 5.5 we follow the same approach used in [9], which goes through the definition of a weaker notion of rewriting:

Definition 5.8. For terms $\Gamma \vdash_\Sigma^{\preceq} M : A$ and $\Gamma \vdash_\Sigma^{\preceq} N : A$, we define weak R-rewriting as:

$$\Gamma \vdash_\Sigma^{\preceq} M \overset{[R]}{\longrightarrow} N : A \overset{def}{\Longleftrightarrow} M = E[\![M_\circ]\!], N = E[\![N_\circ]\!], M_\circ \equiv \theta l, N_\circ =_\eta \theta r, \text{ for some } (\Delta \vdash l \to r : B) \in R,$$
$$\theta : \Delta \overset{\preceq}{\to} \Gamma(M, M_\circ), \text{ and } \Gamma \vdash_\Sigma^{\preceq} E[\![\Gamma(M, M_\circ) \vdash \circ : A(M, M_\circ)]\!] : A.$$

We furthermore define weak R-conversion as the judgement $\Gamma \vdash_\Sigma^{\preceq} M \overset{[R]}{\longleftrightarrow} N : A$ formed according to the following rules:

$$\frac{\Gamma\vdash_\Sigma^{\preceq} M{:}A \quad M\equiv N \quad \Gamma\vdash_\Sigma^{\preceq} N{:}A}{\Gamma\vdash_\Sigma^{\preceq} M \overset{[R]}{\longleftrightarrow} N{:}A} \qquad \frac{\Gamma\vdash_\Sigma^{\preceq} M \overset{[R]}{\longrightarrow} N{:}A}{\Gamma\vdash_\Sigma^{\preceq} M \overset{[R]}{\longleftrightarrow} N{:}A}$$

$$\frac{\Gamma\vdash_\Sigma^{\preceq} M \overset{[R]}{\longleftrightarrow} N{:}A}{\Gamma\vdash_\Sigma^{\preceq} N \overset{[R]}{\longleftrightarrow} M{:}A} \qquad \frac{\Gamma\vdash_\Sigma^{\preceq} M \overset{[R]}{\longleftrightarrow} N'{:}A \quad \Gamma\vdash_\Sigma^{\preceq} N' \overset{[R]}{\longleftrightarrow} N{:}A}{\Gamma\vdash_\Sigma^{\preceq} M \overset{[R]}{\longleftrightarrow} N{:}A}$$

The set of dependency constraints generated by a weak R-rewriting step is defined as

$$(\Gamma \vdash_\Sigma^{\preceq} M \xrightarrow{[R]} N : A) \Vdash \{\mathrm{head}(B)\}$$

if $(\Delta \vdash_\Sigma^{\preceq} l \to r : B) \in R$ was the rewriting rule used.

This definition is extended to weak R-conversion:

$$\frac{\Gamma\vdash_\Sigma^{\preceq} M{:}A \quad M\equiv N \quad \Gamma\vdash_\Sigma^{\preceq} N{:}A}{(\Gamma\vdash_\Sigma^{\preceq} M\xleftrightarrow{[R]}N{:}A)\Vdash\emptyset} \qquad \frac{(\Gamma\vdash_\Sigma^{\preceq} M\xrightarrow{[R]}N{:}A)\Vdash\mathcal{D}}{(\Gamma\vdash_\Sigma^{\preceq} M\xleftrightarrow{[R]}N{:}A)\Vdash\mathcal{D}}$$

$$\frac{(\Gamma\vdash_\Sigma^{\preceq} M\xleftrightarrow{[R]}N{:}A)\Vdash\mathcal{D}}{(\Gamma\vdash_\Sigma^{\preceq} N\xleftrightarrow{[R]}M{:}A)\Vdash\mathcal{D}} \qquad \frac{(\Gamma\vdash_\Sigma^{\preceq} M\xleftrightarrow{[R]}N'{:}A)\Vdash\mathcal{D} \quad (\Gamma\vdash_\Sigma^{\preceq} N'\xleftrightarrow{[R]}N{:}A)\Vdash\mathcal{D}'}{(\Gamma\vdash_\Sigma^{\preceq} M\xleftrightarrow{[R]}N{:}A)\Vdash(\mathcal{D}\cup\mathcal{D}')}$$

One relation between these two notions of rewriting is easily derived from their respective definitions:

Proposition 5.9. *$(\Gamma \vdash_\Sigma^{\preceq} M \xleftrightarrow{R} N : A) \Vdash \mathcal{D}$ if and only if $(\Gamma \vdash_\Sigma^{\preceq} M_\Downarrow \xleftrightarrow{[R]} N_\Downarrow : A) \Vdash \mathcal{D}$.*

Proof. By definition and Lemma 4.12, $(\Gamma \vdash_\Sigma^{\preceq} M \xrightarrow{R} N : A) \Vdash \mathcal{D}$ if and only if $(\Gamma \vdash_\Sigma^{\preceq} M_\Downarrow \xrightarrow{[R]} N_\Downarrow : A) \Vdash \mathcal{D}$, and the result follows by a trivial induction on the two derivations. $\square$

Our next goal is to show that $(\Gamma \vdash_\Sigma^{\preceq} M \xleftrightarrow{R} N : A) \Vdash \mathcal{D}$ whenever $(\Gamma \vdash_\Sigma^{\preceq} M \xleftrightarrow{[R]} N : A) \Vdash \mathcal{D}$. The proof of this fact relies on a series of technical lemmas.

Lemma 5.10. *If $\Gamma, x : C, \Gamma' \vdash_\Sigma^{\preceq} E[\![\Gamma_\circ, x : C, \Gamma'_\circ \vdash \circ : A_\circ]\!] : A$ then for all terms $\Gamma \vdash_\Sigma^{\preceq} N : C$ there is an environment $\Gamma, [N/x]\Gamma' \vdash_\Sigma^{\preceq} E'[\![\Gamma_\circ, [N/x]\Gamma'_\circ \vdash \circ : [N/x]A_\circ]\!] : [N/x]A$ such that for all compatible terms $\Gamma_\circ, x : C, \Gamma'_\circ \vdash M : A_\circ$ we have $[N/x]E'[\![M]\!] = E'[\![[N/x]M]\!]$.*

Proof. By a trivial induction on the derivation of $\Gamma, x : C, \Gamma' \vdash_\Sigma^{\preceq} E[\![\Gamma_\circ, x : C, \Gamma'_\circ \vdash \circ : A_\circ]\!] : A$, using Substitution. We consider the case:

$$\frac{\Gamma,x{:}C,\Gamma'\vdash_\Sigma^{\preceq} M_1{:}\Pi x{:}B.A \quad \Gamma,x{:}C,\Gamma'\vdash_\Sigma^{\preceq} E_2[\![\Gamma_\circ,x{:}C,\Gamma'_\circ\vdash\circ{:}A_\circ]\!]{:}B}{\Gamma\vdash_\Sigma^{\preceq} M_1(E_2[\![\Gamma_\circ\vdash\circ{:}A_\circ]\!]){:}A} \quad A_\circ \not\preceq^A A$$

By Substitution, $\Gamma, [N/x]\Gamma'_\circ \vdash_\Sigma^{\preceq} [N/x]M : [N/x]\Pi x : B.A$, and by inductive hypothesis $\Gamma, [N/x]\Gamma' \vdash_\Sigma^{\preceq} E'_2[\![\Gamma_\circ, [N/x]\Gamma'_\circ \vdash \circ : [N/x]A_\circ]\!] : [N/x]B$. Since $\mathrm{head}([N/x]A_\circ) = \mathrm{head}(A_\circ)$, $\mathrm{head}([N/x]A) = \mathrm{head}(A)$, and $[N/x]A_\circ \not\preceq^A [N/x]A$, the result follows. $\square$

Notation. In the sequel, we will denote the environment obtained from Lemma 5.10 by $[N/x]E$.

Corollary 5.11. *If $(\Gamma, x : C \vdash_\Sigma^{\preceq} M \xrightarrow{[R]} N : A) \Vdash \mathcal{D}$ then for all terms $\Gamma \vdash_\Sigma^{\preceq} M' : C$ there is a term $\Gamma \vdash_\Sigma^{\preceq} N' : A$ such that $[M'/x]N \to_\beta^* N'$ and $(\Gamma \vdash_\Sigma^{\preceq} [M'/x]M \xrightarrow{[R]} N' : [M'/x]A) \Vdash \mathcal{D}$.*

Proof. By definition, $\Gamma, x : C \vdash_\Sigma^{\preceq} M \xrightarrow{R} N : A$ means there are

$$(\Delta \vdash_\Sigma^{\preceq} l \to r : B) \in R,$$
$$\theta : \Delta \xrightarrow{\preceq} \Gamma(M, M_\circ),$$
$$\Gamma, x : C \vdash_\Sigma^{\preceq} E[\![\Gamma(M, M_\circ) \vdash \circ : A(M, M_\circ)]\!] : A$$

such that

$$M = E[\![M_\circ]\!], \qquad N = E[\![N_\circ]\!],$$
$$M_\circ \equiv \theta l, \qquad N_\circ =_\eta \theta r.$$

By Lemma 5.10,

$$\Gamma \vdash^{\preceq}_{\Sigma} ([M'/x]E)[\![\Gamma([M'/x]M, [M'/x]M_\circ) \vdash \circ : A([M'/x]M, [M'/x]M_\circ)]\!] : [M'/x]A$$

Let $\theta' = \theta \circ \{x \mapsto M'\}$, pick $N_0' =_\eta \theta' r$ such that $[M'/x]N_0 \to^*_\beta N_0'$; then $N' = ([M'/x]E)[\![N_0']\!]$ is as required. $\square$

Lemma 5.12. *If $\Gamma, x : C \vdash^{\preceq}_{\Sigma} M' : A$, $(\Gamma \vdash^{\preceq}_{\Sigma} M \xrightarrow{[R]} N : C) \Vdash \mathcal{D}$, and $a \not\succ^A A$ if $a \in \mathcal{D}$, then there is a rewrite sequence $(\Gamma \vdash^{\preceq}_{\Sigma} M^{(i)} \xrightarrow{[R]} M^{(i+1)} : A) \Vdash \mathcal{D}$ $(0 \leq i < n)$ such that $M^{(0)} = [M/x]M'$, $M^{(n)} = [N/x]M'$.*

Proof. By definition, $\Gamma \vdash^{\preceq}_{\Sigma} M \xrightarrow{R} N : C$ if there are

$$(\Delta \vdash^{\preceq}_{\Sigma} l \to r : B) \in R,$$
$$\theta : \Delta \xrightarrow{\preceq} \Gamma(M, M_\circ),$$
$$\Gamma \vdash^{\preceq}_{\Sigma} E[\![\Gamma(M, M_\circ) \vdash \circ : A(M, M_\circ)]\!] : C$$

such that

$$M = E[\![M_\circ]\!], \qquad N = E[\![N_\circ]\!],$$
$$M_\circ \equiv \theta l, \qquad N_\circ =_\eta \theta r.$$

By progressively replacing all the occurrences of x in M by N using Lemma 3.12, we get a sequence of terms $M^{(i)'}$ $(0 \leq i \leq n)$ such that (by Lemma 5.10) $(\Gamma \vdash^{\preceq}_{\Sigma} [M/x]M^{(i)'} \xrightarrow{[R]} [M/x]M^{(i+1)'} : A) \Vdash \mathcal{D}$, $M^{(0)'} = M'$, $M^{(n)'} = [N/x]M'$. $\square$

Proposition 5.13. *We have:*

1. *If $(\Gamma, x : A \vdash^{\preceq}_{\Sigma} M \xrightarrow{[R]} M' : B) \Vdash \mathcal{D}$ and $A \preceq^M_{\Sigma} B$ then $(\Gamma \vdash^{\preceq}_{\Sigma} \lambda x : A.M \xrightarrow{[R]} \lambda x : A.M' : \Pi x : A.B) \Vdash \mathcal{D}$.*
2. *If $(\Gamma \vdash^{\preceq}_{\Sigma} M \xrightarrow{[R]} M' : \Pi x : A.B) \Vdash \mathcal{D}$ and $\Gamma \vdash^{\preceq}_{\Sigma} N : A$ then $(\Gamma \vdash^{\preceq}_{\Sigma} M\ N \xrightarrow{[R]} M'\ N : [N/x]B) \Vdash \mathcal{D}$.*
3. *If $\Gamma \vdash^{\preceq}_{\Sigma} M : \Pi x : A.B$, $(\Gamma \vdash^{\preceq}_{\Sigma} N \xrightarrow{[R]} N' : A) \Vdash \mathcal{D}$, and $a \not\succ^A B$ if $a \in \mathcal{D}$, then $(\Gamma \vdash^{\preceq}_{\Sigma} M\ N \xrightarrow{[R]} M\ N' : B) \Vdash \mathcal{D}$.*

Proof. (3) By definition, $\Gamma \vdash^{\preceq}_{\Sigma} N \xrightarrow{[R]} N' : A$ means there are

$$(\Delta \vdash^{\preceq}_{\Sigma} l \to r : C) \in R,$$
$$\theta : \Delta \xrightarrow{\preceq} \Gamma(N, N_\circ),$$
$$\Gamma \vdash^{\preceq}_{\Sigma} E[\![\Gamma(N, N_\circ) \vdash \circ : A(N, N_\circ)]\!] : A$$

such that

$$N = E[\![N_\circ]\!], \qquad N' = E[\![N_\circ']\!],$$
$$N_\circ \equiv \theta l, \qquad N_\circ' =_\eta \theta r.$$

and $\mathcal{D} = \{\mathrm{head}(C)\} = \{\mathrm{head}(A(N, N_\circ))\}$. Then

$$\Gamma \vdash^{\preceq}_{\Sigma} M\ (E[\![\Gamma(N, N_\circ) \vdash \circ : A(N, N_\circ)]\!]) : B$$

and hence by definition $(\Gamma \vdash^{\preceq}_{\Sigma} M\ N \xrightarrow{[R]} M\ N' : B) \Vdash \mathcal{D}$.

The proofs of (1) and (2) are similar. $\square$

Corollary 5.14. *We have:*

1. *If $(\Gamma, x : A \vdash^{\preceq}_{\Sigma} M \xleftrightarrow{[R]} M' : B) \Vdash \mathcal{D}$ and $A \preceq^M_{\Sigma} B$ then $(\Gamma \vdash^{\preceq}_{\Sigma} \lambda x : A.M \xleftrightarrow{[R]} \lambda x : A.M' : \Pi x : A.B) \Vdash \mathcal{D}$.*
2. *If $(\Gamma \vdash^{\preceq}_{\Sigma} M \xleftrightarrow{[R]} M' : \Pi x : A.B) \Vdash \mathcal{D}$ and $\Gamma \vdash^{\preceq}_{\Sigma} N : A$ then $(\Gamma \vdash^{\preceq}_{\Sigma} M\ N \xleftrightarrow{[R]} M'\ N : [N/x]B) \Vdash \mathcal{D}$.*
3. *If $\Gamma \vdash^{\preceq}_{\Sigma} M : \Pi x : A.B$, $(\Gamma \vdash^{\preceq}_{\Sigma} N \xleftrightarrow{[R]} N' : A) \Vdash \mathcal{D}$, and $a \not\succ^A B$ if $a \in \mathcal{D}$, then $(\Gamma \vdash^{\preceq}_{\Sigma} M\ N \xleftrightarrow{[R]} M\ N' : B) \Vdash \mathcal{D}$.*

Proof. By an easy induction on the derivations. $\square$

Lemma 5.15. *If* $(\Gamma \vdash_\Sigma^\preceq M \xrightarrow{[R]} N : C) \Vdash \mathcal{D}$ *and* $M \to_\beta M'$, *then there is a rewrite sequence* $(\Gamma \vdash_\Sigma^\preceq M^{(i)} \xrightarrow{[R]} M^{(i+1)} : A) \Vdash \mathcal{D}$ $(0 \le i < n)$ *such that* $M' = M^{(0)}$, $N \to_\beta^* M^{(n)}$.

In pictures:

$$\begin{tikzcd} M \arrow[rrr, "{[R]}"'] \arrow[d, "\beta"'] & & & N \arrow[d, dashed, "\beta\,|\,*"'] \\ M^{(0)} \arrow[r, dashed, "{[R]}"'] & \cdots \arrow[rr, dashed, "{[R]}"'] & & M^{(n)} \end{tikzcd}$$

Proof. By definition, $\Gamma \vdash_\Sigma^\preceq M \xrightarrow{[R]} N : A$ if there are

$$(\Delta \vdash_\Sigma^\preceq l \to r : B) \in R,$$
$$\theta : \Delta \xrightarrow{\preceq} \Gamma(M, M_\circ),$$
$$\Gamma \vdash_\Sigma^\preceq E[\![\Gamma(M, M_\circ) \vdash \circ : A(M, M_\circ)]\!] : A$$

such that

$$\begin{array}{ll} M = E[\![M_\circ]\!], & N = E[\![N_\circ]\!], \\ M_\circ \equiv \theta l, & N_\circ =_\eta \theta r. \end{array}$$

The proof proceeds by induction on $\Gamma \vdash_\Sigma^\preceq E[\![\Gamma(M, M_\circ) \vdash \circ : A(M, M_\circ)]\!] : A$. The most interesting cases are the two application rules:

- Case:

$$\frac{\Gamma \vdash_\Sigma^\preceq E_1[\![\Gamma_\circ \vdash \circ : A_\circ]\!] : \Pi x{:}B.A \quad \Gamma \vdash_\Sigma^\preceq M_2 : B}{\Gamma \vdash_\Sigma^\preceq (E_1[\![\Gamma_\circ \vdash \circ : A_\circ]\!])\ M_2 : A}$$

  There are three possible subcases:
  - $M = (E_1[\![M_\circ]\!]\ M_2) \to_\beta (E_1[\![M_\circ]\!]\ M_2') = M'$
    It is easily checked that

$$\Gamma \vdash_\Sigma^\preceq (E_1[\![\Gamma(M, M_\circ) \vdash \circ : A(M, M_\circ)]\!])\ M_2' : A,$$
$$\Gamma \vdash_\Sigma^\preceq (E_1[\![M_\circ]\!]\ M_2') \xrightarrow{[R]} (E_1[\![N_\circ]\!]\ M_2') : A,$$
$$N = (E_1[\![N_\circ]\!]\ M_2) \to_\beta (E_1[\![N_\circ]\!]\ M_2') = M^{(1)}$$

  - $M' = (M_1'\ M_2)$ and $E_1[\![M_\circ]\!] \to_\beta M_1'$
    Then, since

$$\Gamma \vdash_\Sigma^\preceq E_1[\![M_\circ]\!] \xrightarrow{[R]} E_1[\![N_\circ]\!] : \Pi x : B.A,$$

    the result follows by inductive hypothesis and repeated applications of Proposition 5.13.(2).
  - $M = (\lambda y : B'.E_1[\![M_\circ]\!])\ M_2 \to_\beta [M_2/y]E_1[\![M_\circ]\!]$
    By inversion (and type conversion, if necessary) $\Gamma, y : B' \vdash_\Sigma^\preceq E_1[\![\Gamma_\circ \vdash \circ : A_\circ]\!] : A$, $\Gamma \vdash_\Sigma^\preceq M_2 : B'$, and the result follows directly by Corollary 5.11.

- Case:

$$\frac{\Gamma \vdash_\Sigma^\preceq M_1 : \Pi x{:}B.A \quad \Gamma \vdash_\Sigma^\preceq E_2[\![\Gamma_\circ \vdash \circ : A_\circ]\!] : B}{\Gamma \vdash_\Sigma^\preceq M_1\ (E_2[\![\Gamma_\circ \vdash \circ : A_\circ]\!]) : A} \quad A_\circ \not\prec^A A$$

  There are again three possible subcases:

– $M = (M_1\ E_2[\![M_\circ]\!]) \to_\beta (M_1'\ E_2[\![M_\circ]\!]) = M'$
  It is easily checked that

$$\Gamma \vdash_\Sigma^\preceq M_1'\ (E_2[\![\Gamma(M,M_\circ) \vdash \circ : A(M,M_\circ)]\!] : A,$$
$$\Gamma \vdash_\Sigma^\preceq (M_1'\ E_2[\![M_\circ]\!]) \xrightarrow{[R]} (M_1'\ E_2[\![N_\circ]\!]) : A,$$
$$N = (M_1\ E_2[\![N_\circ]\!]) \to_\beta (M_1'\ E_2[\![N_\circ]\!]) = M^{(1)}$$

– $M' = (M_1\ M_2')$ and $E_2[\![M_\circ]\!] \to_\beta M_2'$
  Then, since

$$\Gamma \vdash_\Sigma^\preceq E_2[\![M_\circ]\!] \xrightarrow{[R]} E_2[\![N_\circ]\!] : B,$$

  the result follows by inductive hypothesis and repeated applications of Proposition 5.13.(3).

– $M = (\lambda y : B'.M_1')\ E_2[\![M_\circ]\!] \to_\beta [E_2[\![M_\circ]\!]/y]M_1'$
  By inversion and type conversion, $\Gamma, y : B' \vdash_\Sigma^\preceq M_1' : A$, $\Gamma \vdash_\Sigma^\preceq E_2[\![\Gamma_\circ \vdash \circ : A_\circ]\!] : B'$, and the result follows directly by Lemma 5.12.

□

Lemma 5.16. *Let $\xrightarrow{1}$, $\xrightarrow{2}$, and $>$ be relations on some set S such that $>$ is a terminating partial order, $s \xrightarrow{1} t$ implies $s \geq t$, and $s \xrightarrow{2} t$ implies $s > t$. Then*

$$\forall x, x', y \quad x' \xleftarrow{2} x \xrightarrow{1} y \ \Rightarrow \exists y' \quad x' \xrightarrow{1}{}^{*} x \,{}^{*}\!\xleftarrow{2} y$$

implies

$$\forall x, x', y \ \ x'\ x' \,{}^{*}\!\xleftarrow{2} x \xrightarrow{1}{}^{*} y \ \Rightarrow \exists y' \quad x' \xrightarrow{1}{}^{*} x \,{}^{*}\!\xleftarrow{2} y \ .$$

In pictures

$$\begin{tikzcd} x \arrow[r, "1"'] \arrow[d, "2"'] & y \arrow[d, dashed, "2 \mid *"] \\ y \arrow[r, dashed, "*"', "1"] & y' \end{tikzcd} \quad \Rightarrow \quad \begin{tikzcd} x \arrow[r, "*", "1"'] \arrow[d, "2"', "*"] & y \arrow[d, dashed, "2 \mid *"] \\ y \arrow[r, dashed, "*"', "1"] & y' \end{tikzcd}$$

Proof. By a double induction argument. The primary induction is on $(x, >)$, the secondary one on the length of the derivation $x \xrightarrow[1]{*} y$.

The cases when $x = x'$ or $x = y$ are trivial. In the induction case we have the following diagram:

$$\begin{tikzcd} x \arrow[r, "1"'] \arrow[d, "2"'] & u \arrow[r, "*", "1"'] \arrow[d, dashed, "2 \mid *"] & y \arrow[d, dashed, "2 \mid *"] \\ v \arrow[r, dashed, "*", "1"'] \arrow[d, "2"', "*"] & u' \arrow[r, dashed, "*", "1"'] \arrow[d, dashed, "2 \mid *"] & w \arrow[d, dashed, "2 \mid *"] \\ x' \arrow[r, dashed, "*", "1"'] & u'' \arrow[r, dashed, "*", "1"'] & y' \end{tikzcd}$$

where the existence of u' and w are given by hypothesis and secondary inductive hypothesis ($x \geq u$ but $u \xrightarrow[1]{}{}^{*} y$ is shorter than $x \xrightarrow[1]{}{}^{*} y$), respectively, while the existence of u'' and y' come from primary inductive hypothesis ($x > v \geq u'$). □

Corollary 5.17. *If $(\Gamma \vdash_\Sigma^\preceq M \xrightarrow{[R]} N : A) \Vdash \mathcal{D}$ and $M \to_\beta^* M'$, then there is a rewrite sequence $(\Gamma \vdash_\Sigma^\preceq M^{(i)} \xrightarrow{[R]} M^{(i+1)} : A) \Vdash \mathcal{D}$ $(0 \leq i < n)$ such that $M' = M^{(0)}$, $N \to_\beta^* M^{(n)}$.*

Proof. Define, for any terms $\Gamma \vdash^{\precsim}_{\Sigma} M : A$ and $\Gamma \vdash^{\precsim}_{\Sigma} N : A$,

$$m(M) = \text{ maximal length of } \beta\text{-reductions starting from } M,$$

and $M < N$ if and only if $m(M) < m(N)$, then

$$M \to_{\beta} N \Rightarrow M > N$$

$$\Gamma \vdash^{\precsim}_{\Sigma} M \xrightarrow{[R]} N : A \Rightarrow M \geq N$$

and the result follows by the previous Lemma and 4.12. $\square$

Lemma 5.18. *If* $(\Gamma \vdash^{\precsim}_{\Sigma} M \xrightarrow{[R]} N : A) \Vdash \mathcal{D}$ *then for all* $\Gamma \vdash^{\precsim}_{\Sigma} M' : A$ *such that* $M' \to_{\eta} M$ *there is a* $\Gamma \vdash^{\precsim}_{\Sigma} N' : A$ *such that* $N' \to^{RF}_{\eta} N$ *and* $(\Gamma \vdash^{\precsim}_{\Sigma} M' \xrightarrow{[R]} N' : A) \Vdash \mathcal{D}$.

In pictures:

$$\begin{tikzcd} M' \arrow[r, dashed, "{[R]}"'] \arrow[d, "\eta"'] & N' \arrow[d, dashed, "\eta \mid RF"] \\ M \arrow[r, dashed, "{[R]}"'] & N \end{tikzcd}$$

Proof. By definition, $\Gamma \vdash^{\precsim}_{\Sigma} M \xrightarrow{[R]} N : A$ if there are

$$(\Delta \vdash^{\precsim}_{\Sigma} l \to r : B) \in R,$$

$$\theta : \Delta \overset{\precsim}{\to} \Gamma(M, M_{\circ}),$$

$$\Gamma \vdash^{\precsim}_{\Sigma} E[\![\Gamma(M, M_{\circ}) \vdash \circ : A(M, M_{\circ})]\!] : A$$

such that

$$\begin{array}{ll} M = E[\![M_{\circ}]\!], & N = E[\![N_{\circ}]\!], \\ M_{\circ} \equiv \theta l, & N_{\circ} =_{\eta} \theta r. \end{array}$$

We will construct, by induction on $\Gamma \vdash^{\precsim}_{\Sigma} E[\![\Gamma(M, M_{\circ}) \vdash \circ : A(M, M_{\circ})]\!] : A$, an environment $\Gamma \vdash^{\precsim}_{\Sigma} E'[\![\Gamma(M, M_{\circ}) \vdash \circ : A(M, M_{\circ})]\!] : A$ and term $\Gamma \vdash^{\precsim}_{\Sigma} N' : A$ such that

$$\begin{array}{ll} M' = E'[\![M'_{\circ}]\!], & N' = E'[\![N'_{\circ}]\!], \\ M'_{\circ} \equiv \theta l, & N'_{\circ} =_{\eta} \theta r, \end{array}$$

$$N' \to^{RF}_{\eta} N.$$

We show some representative cases:

- Case:

$$\frac{\Gamma_{\circ} \vdash^{\precsim}_{\Sigma} A_{\circ} : \text{type} \quad \Gamma_{\circ} \subseteq \Gamma}{\Gamma \vdash^{\precsim}_{\Sigma} \circ[\![\Gamma_{\circ} \vdash \circ : A_{\circ}]\!] : A_{\circ}}$$

  Then $M' \equiv \theta l$, hence picking $E' = E$ and $N' = N$ we have the result.

- Case:

$$\frac{\Gamma \vdash^{\precsim}_{\Sigma} M_1 : \Pi x : A.B \quad \Gamma \vdash^{\precsim}_{\Sigma} E_2[\![\Gamma_{\circ} \vdash \circ : A_{\circ}]\!] : A}{\Gamma \vdash^{\precsim}_{\Sigma} M_1 \ (E_2[\![\Gamma_{\circ} \vdash \circ : A_{\circ}]\!]) : B} \quad A_{\circ} \not\precsim^{A} B$$

  We have three different subcases:

  – $B = \Pi x : A'.B'$ and $M' = \lambda y : A'.(M_1 \ M_2) \ y \to_{\eta} M_1 \ M_2 = M$
    It is easily checked that

$$\Gamma \vdash^{\precsim}_{\Sigma} \lambda y : A'.(M_1 \ E_2[\![\Gamma(M, M_{\circ}) \vdash \circ : A(M, M_{\circ})]\!] \ y) : B$$

    and $\lambda y : A'.(E[\![N_{\circ}]\!] \ y) \to_{\eta} N$.

– $M' = (M'_1\ M_2) \to_\eta (M_1\ M_2) = M$
  By inversion (and type conversion, if necessary), $\Gamma \vdash^{\preceq}_{\Sigma} M'_1 : \Pi x : A.B$, and $E' = M'_1\ E_2$, $N' = E'[\![N_\circ]\!]$ are as required.
– $M' = (M_1\ M'_2) \to_\eta (M_1\ M_2) = M$
  By inductive hypothesis on $\Gamma \vdash^{\preceq}_{\Sigma} E_2[\![\Gamma_\circ \vdash \circ : A_\circ]\!] : A$ we get E'_2 and N'_2; defining $E' = M_1\ E'_2$ and $N' = M_1\ N'_2$ we have the result.

- Case:

$$\frac{\Gamma\vdash^{\preceq}_{\Sigma}E[\![\Gamma_\circ\vdash\circ:A_\circ]\!]:A \quad A\equiv B \quad \Gamma\vdash^{\preceq}_{\Sigma}B:\text{type}}{\Gamma\vdash^{\preceq}_{\Sigma}E[\![\Gamma_\circ\vdash\circ:A_\circ]\!]:B}$$

  Immediate by inductive hypothesis and type conversion.

□

Corollary 5.19. *If* $(\Gamma \vdash^{\preceq}_{\Sigma} M \xrightarrow{[R]} N : A) \Vdash \mathcal{D}$ *then for all* $\Gamma \vdash^{\preceq}_{\Sigma} M' : A$ *such that* $M' \to^*_\eta M$ *there is a* $\Gamma \vdash^{\preceq}_{\Sigma} N' : A$ *such that* $N' \to^*_\eta N$ *and* $(\Gamma \vdash^{\preceq}_{\Sigma} M' \xrightarrow{[R]} N' : A) \Vdash \mathcal{D}$

Proof. By induction on the length of the reduction $M' \to^*_\eta M$, using the Lemma. □

Lemma 5.20. *If* $(\Gamma \vdash^{\preceq}_{\Sigma} M \xrightarrow{[R]} N : A) \Vdash \mathcal{D}$ *then* $(\Gamma \vdash^{\preceq}_{\Sigma} M \xleftrightarrow{R} N : A) \Vdash \mathcal{D}$.

Proof. Immediate from Corollaries 4.11, 5.17, 5.19. □

Corollary 5.21. *If* $(\Gamma \vdash^{\preceq}_{\Sigma} M \xleftrightarrow{[R]} N : A) \Vdash \mathcal{D}$ *then* $(\Gamma \vdash^{\preceq}_{\Sigma} M \xleftrightarrow{R} N : A) \Vdash \mathcal{D}$.

Proof of Theorem 5.5. One direction has already been proved by Corollary 5.7. The proof of the other is by induction on the derivation of $\Gamma \vdash^{\preceq}_{\Sigma} M \stackrel{R}{=} N : A \rhd \mathcal{D}$. Most of the cases are immediate. The only two requiring some work are application and abstraction:

- Abstraction:

$$\frac{\Gamma\vdash^{\preceq}_{\Sigma}A:\text{type} \quad \Gamma,x{:}A\vdash^{\preceq}_{\Sigma}M\stackrel{R}{=}N{:}B\rhd\mathcal{D}}{\Gamma\vdash^{\preceq}_{\Sigma}\lambda x{:}A.M\stackrel{R}{=}\lambda x{:}A.N{:}\Pi x{:}A.B\rhd\mathcal{D}}\ A\preceq^M_\Sigma B$$

  By inductive hypothesis,

$$(\Gamma, x : A \vdash^{\preceq}_{\Sigma} M \xleftrightarrow{R} N : B) \Vdash \mathcal{D}.$$

  By Proposition 5.9,

$$(\Gamma, x : A \vdash^{\preceq}_{\Sigma} M_\Downarrow \xleftrightarrow{[R]} N_\Downarrow : B) \Vdash \mathcal{D},$$

  and by Proposition 5.13.(1) and Corollary 5.21

$$(\Gamma \vdash^{\preceq}_{\Sigma} (\lambda x : A.M_\Downarrow) \xleftrightarrow{R} (\lambda x : A.N_\Downarrow) : \Pi x : A.B) \Vdash \mathcal{D}.$$

  By conversion

$$(\Gamma \vdash^{\preceq}_{\Sigma} (\lambda x : A.M) \xleftrightarrow{R} (\lambda x : A.M_\Downarrow) : \Pi x : A.B) \Vdash \mathcal{D},$$

$$(\Gamma \vdash^{\preceq}_{\Sigma} (\lambda x : A.N_\Downarrow) \xleftrightarrow{R} (\lambda x : A.N) : \Pi x : A.B) \Vdash \mathcal{D},$$

  hence by transitivity the result.

- Application:

$$\frac{\Gamma\vdash^{\preceq}_{\Sigma}M\stackrel{R}{=}M'{:}\Pi x{:}A.B\rhd\mathcal{D} \quad \Gamma\vdash^{\preceq}_{\Sigma}N\stackrel{R}{=}N'{:}A\rhd\mathcal{D}'}{\Gamma\vdash^{\preceq}_{\Sigma}M\ N\stackrel{R}{=}M'\ N'{:}B\rhd(\mathcal{D}\cup\mathcal{D}')}\ a\not\preceq^A B \text{ for all } a\in\mathcal{D}'$$

  By inductive hypothesis,

$$(\Gamma \vdash^{\preceq}_{\Sigma} M \xleftrightarrow{R} M' : \Pi x : A.B) \Vdash \mathcal{D},$$

$$(\Gamma \vdash^{\preceq}_{\Sigma} N \xleftrightarrow{R} N' : A) \Vdash \mathcal{D}'.$$

By Proposition 5.9,

$$(\Gamma \vdash^{\preceq}_{\Sigma} M_{\Downarrow} \xleftrightarrow{[R]} M'_{\Downarrow} : \Pi x : A.B) \Vdash \mathcal{D},$$
$$(\Gamma \vdash^{\preceq}_{\Sigma} N_{\Downarrow} \xleftrightarrow{[R]} N'_{\Downarrow} : A) \Vdash \mathcal{D}';$$

by Proposition 5.13 and Corollary 5.21

$$(\Gamma \vdash^{\preceq}_{\Sigma} (M_{\Downarrow}\, N_{\Downarrow}) \xleftrightarrow{R} (M'_{\Downarrow}\, N_{\Downarrow}) : B) \Vdash \mathcal{D}$$
$$(\Gamma \vdash^{\preceq}_{\Sigma} (M'_{\Downarrow}\, N_{\Downarrow}) \xleftrightarrow{R} (M'_{\Downarrow}\, N'_{\Downarrow}) : B) \Vdash \mathcal{D}',$$

and by conversion and transitivity the result.

□

6. Critical Pairs

As in the first order case, the check for local confluence of $\xleftrightarrow{R}$ goes through the search for critical pairs generated by the rules of the HTRS R. The definition of critical pairs here, however, is complicated by the presence of dependent types. Before giving the precise definition of critical pair, we need some additional machinery:

Definition 6.1. Let $\theta : \Gamma \rightharpoondown \Delta$ be a substitution, the support of θ ($\mathrm{supp}(\theta)$) is the set

$$\{x \in \mathrm{dom}\,\Gamma \mid \neg(\theta(x) \equiv x)\}.$$

Given two substitutions $\theta : \Gamma \rightharpoondown \Delta$ and $\theta' : \Gamma' \rightharpoondown \Delta'$, we will say that they are equivalent, and write $\theta \doteq \theta'$, if $\mathrm{supp}(\theta) = \mathrm{supp}(\theta')$ and $\theta(x) = \theta'(x)$ for all $x \in \mathrm{supp}(\theta)$.

Proposition 6.2. *Let $\theta = \{\overline{x} \mapsto \overline{M}\} : \Gamma \overset{\preceq}{\rightharpoondown} \Delta$ be a substitution, $\Gamma \vdash^{\preceq}_{\Sigma} \lambda y : A.M : \Pi y : A.B$ any term , then there is a substitution $\theta' : \Gamma, y : A \overset{\preceq}{\rightharpoondown} \Delta, y : [\overline{M}/\overline{x}]A$ such that $\theta' \doteq \theta$ and*

$$\theta(\lambda y : A.M) = \lambda y : \theta A.\theta' M$$

Proof. From $\Delta \vdash^{\preceq}_{\Sigma} \theta M : [\overline{M}/\overline{x}](\Pi y : A.B)$ we get $\Delta \vdash^{\preceq}_{\Sigma} [\overline{M}/\overline{x}](\Pi y : A.B) : \mathrm{type}$ and by inversion $\Delta \vdash^{\preceq}_{\Sigma} [\overline{M}/\overline{x}]A : \mathrm{type}$.

Also, by inversion (using type conversion, if necessary), $\Gamma \vdash^{\preceq}_{\Sigma} A : \mathrm{type}$, $\Gamma, y : A \vdash^{\preceq}_{\Sigma} M : B$, and $A \preceq^{M}_{\Sigma} B$; hence $\Delta \vdash^{\preceq}_{\Sigma} \theta A \Downarrow \mathrm{type}$.

Let $\Delta, y : \theta A \vdash^{\preceq}_{\Sigma} N \Downarrow [\overline{M}/\overline{x}]A$ be such that $N \equiv y$, then $\theta' = \{\overline{x} \mapsto \overline{M}, y \mapsto N\} : \Gamma, y : A \overset{\preceq}{\rightharpoondown} \Delta, y : [\overline{M}/\overline{x}]A$, so

$$\frac{\Delta \vdash^{\preceq}_{\Sigma} \theta A \Downarrow \mathrm{type} \quad \Delta, y{:}\theta A \vdash^{\preceq}_{\Sigma} \theta' M \Downarrow [\overline{M}/\overline{x}]B}{\Delta \vdash^{\preceq}_{\Sigma} \lambda y{:}\theta A.\theta M \Downarrow \Pi y{:}\theta A.[\overline{M}/\overline{x}]B} \; \theta A \preceq^{M}_{\Sigma} [\overline{M}/\overline{x}]B.$$

By type conversion $\Delta \vdash^{\preceq}_{\Sigma} \lambda y : \theta A.\theta M \Downarrow [\overline{M}/\overline{x}](\Pi y : \theta A.B$ and, observing that $\theta(\lambda y : A.M) \equiv (\lambda y : \theta A \,.\, \theta' M)$, by uniqueness of canonical forms we get the result. □

Definition 6.3. Let $\theta : \Gamma \overset{\preceq}{\rightharpoondown} \Delta$ be a substitution, an atomic term $\Gamma \vdash_{\Sigma} M \downarrow A$ is said to be stable for θ if $M = h\overline{N}$ where h is either a constant c or a variable $x \notin \mathrm{supp}(\theta)$.

Stability implies that the head of a canonical term is preserved by the application of a substitution, i.e. that $\theta(h\overline{N}) = h\overline{\theta N}$.

Lemma 6.4. *Let $\theta = \{\overline{x} \mapsto \overline{M}\} : \Gamma \overset{\preceq}{\rightharpoondown} \Delta$ be a substitution, $\Gamma \vdash^{\preceq}_{\Sigma} M \downarrow A$ stable for θ, then there exists an atomic term $\Delta \vdash^{\preceq}_{\Sigma} M' \downarrow [\overline{M}/\overline{x}]A$ such that $\theta M \to^{*}_{\eta} M'$.*

Proof. By Lemma 4.8 and uniqueness of canonical forms, it suffices to show $M' \equiv \theta M$. Moreover, by Proposition 4.16 and Corollary 4.7, we need only to show $\Delta \vdash_{\Sigma} M' \downarrow [\overline{M}/\overline{x}]A$. The proof goes by induction on the derivation $\Gamma \vdash_{\Sigma} M \downarrow A$:

- Case

$$\frac{\Sigma(c)=A}{\Gamma\vdash_\Sigma c \downarrow A}$$

It is immediately verified that $\theta c \equiv c$, and for each $x \in \mathrm{dom}\,\Gamma$, $x \notin \mathcal{FV}(A)$. Hence $[\overline{M}/\overline{x}]A = A$ and therefore

$$\frac{\Sigma(c)=[\overline{M}/\overline{x}]A}{\Delta\vdash_\Sigma c \downarrow [\overline{M}/\overline{x}]A}$$

- Case

$$\frac{\Gamma(x)=A}{\Gamma\vdash_\Sigma x \downarrow A}$$

By stability, $\theta(x) \equiv x$; by inversion on $\theta : \Gamma \xrightarrow{\preceq} \Delta$ we have $\Delta(x) = [\overline{M}/\overline{x}]A$, hence

$$\frac{\Delta(x)=[\overline{M}/\overline{x}]A}{\Delta\vdash_\Sigma x \downarrow [\overline{M}/\overline{x}]A}.$$

- Case

$$\frac{\Gamma\vdash_\Sigma M \downarrow \Pi y{:}A.B \quad \Gamma\vdash_\Sigma N \Downarrow A}{\Gamma\vdash_\Sigma M\ N \downarrow [N/y]B}$$

Since by hypothesis $M\ N$ is stable for θ, so is M, so by inductive hypothesis there is an atomic term $\Delta \vdash_\Sigma M' \downarrow [\overline{M}/\overline{x}](\Pi y : A.B)$ such that $\theta M \to_\eta^* M'$. Then

$$\frac{\Delta\vdash_\Sigma M' \downarrow [\overline{M}/\overline{x}](\Pi y{:}A.B) \quad \Delta\vdash_\Sigma \theta N \Downarrow [\overline{M}/\overline{x}]A}{\Gamma\vdash_\Sigma M\ \theta N \downarrow [\theta N/y][\overline{M}/\overline{x}]B}$$

From $\Delta \vdash_\Sigma^\preceq \theta(M\ N) \Downarrow [\overline{M}/\overline{x}][N/y]B$ we get $\Delta \vdash_\Sigma^\preceq [\overline{M}/\overline{x}][N/y]B$: type and, since $[\overline{M}/\overline{x}][N/y]B \equiv [\theta N/y][\overline{M}/\overline{x}]B$, by type conversion the result.

- Case

$$\frac{\Gamma\vdash_\Sigma M \downarrow A \quad A\equiv B \quad \Gamma\vdash_\Sigma B{:}\mathrm{type}}{\Gamma\vdash_\Sigma M \downarrow B}$$

Immediate by inductive hypothesis and type conversion.

$\square$

Definition 6.5. Let $\theta = \{\overline{x} \mapsto \overline{M}\} : \Gamma \xrightarrow{\preceq} \Delta$ be a substitution, an environment $\Gamma \vdash_\Sigma^\preceq E[\![\Gamma_\circ \vdash \circ : A_\circ]\!] : A$ is stable for θ if whenever the rule

$$\frac{\Gamma\vdash_\Sigma^\preceq M_1{:}\Pi x{:}A.B \quad \Gamma\vdash_\Sigma^\preceq E_2[\![\Gamma_\circ\vdash\circ{:}A_\circ]\!]{:}A}{\Gamma\vdash_\Sigma^\preceq M_1(E_2[\![\Gamma_\circ\vdash\circ{:}A_\circ]\!]){:}B} \quad A_\circ \not\preceq^A B$$

is applied, $\Gamma \vdash_\Sigma^\preceq M \downarrow \Pi x : A.B$ and M is stable for θ.

Since all the applications contained in it involve stable terms, one would expect that a stable environment preserves most of its structure when the substitution is applied to it. The following Lemma shows that this is actually the case:

Lemma 6.6. *Let*

$$\theta = \{\overline{x} \mapsto \overline{M}\} : \Gamma \xrightarrow{\preceq} \Delta$$
$$\Gamma \vdash_\Sigma^\preceq E[\![\Gamma_\circ \vdash \circ : A_\circ]\!] : A \textit{ stable for } \theta,$$
$$\Gamma_\circ \vdash_\Sigma^\preceq M_\circ \Downarrow A_\circ, \Gamma_\circ \vdash_\Sigma^\preceq A_\circ \downarrow \mathrm{type},$$

and $M = E[\![M_\circ]\!]$, *then there are*

$$\theta' : \Gamma_\circ \stackrel{\preceq}{\rightarrow} \Delta_\circ \ \textit{with}\ \theta' \doteq \theta,$$
$$\Delta \vdash^{\preceq}_{\Sigma} E'[\![\Delta_\circ \vdash \circ : [\overline{M}/\overline{x}]A_\circ]\!] : [\overline{M}/\overline{x}]A$$

such that:

1. *if* $\Gamma \vdash^{\preceq}_{\Sigma} E[\![M_\circ]\!] \Downarrow A$ *then* $\theta M = E'[\![\theta' M_\circ]\!]$ *and* $\Delta \vdash^{\preceq}_{\Sigma} E'[\![\theta' M_\circ]\!] \Downarrow [\overline{M}/\overline{x}]A$*;*
2. *if* $\Gamma \vdash^{\preceq}_{\Sigma} E[\![M_\circ]\!] \downarrow A$ *then* $\theta M \rightarrow^{*}_{\eta} E'[\![\theta' M_\circ]\!]$ *and* $\Delta \vdash^{\preceq}_{\Sigma} E'[\![\theta' M_\circ]\!] \downarrow [\overline{M}/\overline{x}]A$*.*

Proof. By induction on the derivation of $\Gamma \vdash^{\preceq}_{\Sigma} E[\![\Gamma_\circ \vdash \circ : A_\circ]\!] : A$:

- Case

$$\frac{\Gamma_\circ \vdash^{\preceq}_{\Sigma} A_\circ{:}\mathrm{type} \quad \Gamma_\circ \subseteq \Gamma}{\Gamma \vdash^{\preceq}_{\Sigma} [\![\Gamma_\circ \vdash \circ{:}A_\circ]\!]{:}A_\circ}$$

  (1) By Weakening $\Gamma \vdash^{\preceq}_{\Sigma} M_\circ : A_\circ$, so $\Delta \vdash^{\preceq}_{\Sigma} \theta M_\circ \Downarrow [\overline{M}/\overline{x}]A_\circ$, hence by letting $E' = E = \circ$, $\theta' = \theta$ we have the result.

  (2) By hypothesis $\Gamma \vdash^{\preceq}_{\Sigma} A_\circ \downarrow \mathrm{type}$ and therefore $[\overline{M}/\overline{x}]A_\circ \equiv A''$, $\Delta \vdash^{\preceq}_{\Sigma} A'' \downarrow \mathrm{type}$. Hence by Inversion $\Delta \vdash^{\preceq}_{\Sigma} \theta M \downarrow [\overline{M}/\overline{x}]A_\circ$, and the proof follows from (1).

- Case:

$$\frac{\Gamma \vdash^{\preceq}_{\Sigma} A{:}\mathrm{type} \quad \Gamma, x{:}A \vdash^{\preceq}_{\Sigma} E_1[\![\Gamma_\circ \vdash \circ{:}A_\circ]\!]{:}B}{\Gamma \vdash^{\preceq}_{\Sigma} \lambda x{:}A.E_1[\![\Gamma_\circ \vdash \circ{:}A_\circ]\!]{:}\Pi x{:}A.B} \quad A \preceq^{M}_{\Sigma} B$$

  (1) Since $\Gamma, x : A \vdash^{\preceq}_{\Sigma} E_1[\![M_\circ]\!] : B$, by Inversion $\Gamma, x : A \vdash^{\preceq}_{\Sigma} E_1[\![M_\circ]\!] \Downarrow B$. By Proposition 6.2 there is $\theta_1 : \Gamma, x : A \stackrel{\preceq}{\rightarrow} \Delta, x : [\overline{M}/\overline{x}]A$ such that $\theta_1 = \theta$ and $\theta(\lambda x : A.E_1[\![M_\circ]\!]) = (\lambda x : \theta A.\theta_1 E_1[\![M_\circ]\!])$, hence we can apply the inductive hypothesis obtaining

$$\theta' : \Gamma_\circ \stackrel{\preceq}{\rightarrow} \Delta_\circ,$$
$$\Delta, x : [\overline{M}/\overline{x}]A \vdash^{\preceq}_{\Sigma} E'_1[\![\Delta_\circ \vdash \circ : [\overline{M}/\overline{x}]A_\circ]\!] : [\overline{M}/\overline{x}]B$$

  such that $\theta E_1[\![M_\circ]\!] = E'_1[\![\theta' M_\circ]\!]$ and $\Delta, x : [\overline{M}/\overline{x}]A \vdash^{\preceq}_{\Sigma} E'_1[\![\theta' M_\circ]\!] \Downarrow [\overline{M}/\overline{x}]B$. Let E' be

$$\Delta \vdash^{\preceq}_{\Sigma} \lambda x : [\overline{M}/\overline{x}]A.E'_1[\![\Delta_\circ \vdash \circ : [\overline{M}/\overline{x}]A_\circ]\!] : [\overline{M}/\overline{x}]\Pi x : A.B,$$

  it is as required.

- Case:

$$\frac{\Gamma \vdash^{\preceq}_{\Sigma} E_1[\![\Gamma_\circ \vdash \circ{:}A_\circ]\!]{:}\Pi x{:}B.A \quad \Gamma \vdash^{\preceq}_{\Sigma} M_2{:}B}{\Gamma \vdash^{\preceq}_{\Sigma} (E_1[\![\Gamma_\circ \vdash \circ{:}A_\circ]\!])M_2{:}A}$$

  (2) Since $\Gamma \vdash^{\preceq}_{\Sigma} E_1[\![M_\circ]\!] : \Pi x : B.A$, by Inversion $\Gamma \vdash^{\preceq}_{\Sigma} E_1[\![M_\circ]\!] \downarrow \Pi x : B.A$. By inductive hypothesis there are

$$\theta' : \Gamma_\circ \stackrel{\preceq}{\rightarrow} \Delta_\circ,$$
$$\Delta \vdash^{\preceq}_{\Sigma} E'_1[\![\Delta_\circ \vdash \circ : [\overline{M}/\overline{x}]A_\circ]\!] : [\overline{M}/\overline{x}]\Pi x : B.A$$

  such that $\theta E_1[\![M_\circ]\!] \rightarrow^{*}_{\eta} E'_1[\![\theta' M_\circ]\!]$ and $\Delta \vdash^{\preceq}_{\Sigma} E'_1[\![\theta' M_\circ]\!] \downarrow [\overline{M}/\overline{x}](\Pi x : B.A)$. Let E' be

$$\Delta \vdash^{\preceq}_{\Sigma} (E'_1[\![\Delta_\circ \vdash \circ : [\overline{M}/\overline{x}]A_\circ]\!])\theta M_2 : [\overline{M}/\overline{x}]A,$$

  it is as required.

  (1) By inversion, we must have $A \equiv A'$, $\Gamma \vdash^{\preceq}_{\Sigma} A' \downarrow \mathrm{type}$; it is not difficult then to verify that $[\overline{M}/\overline{x}]A \equiv A''$, $\Delta \vdash^{\preceq}_{\Sigma} A'' \downarrow \mathrm{type}$. Hence by Inversion $\Gamma \vdash^{\preceq}_{\Sigma} E[\![M_\circ]\!] \downarrow A$, and the result follows from (1) and uniqueness of canonical forms.

- Case:

$$\frac{\Gamma \vdash^{\preceq}_{\Sigma} M_1{:}\Pi x{:}B.A \quad \Gamma \vdash^{\preceq}_{\Sigma} E_2[\![\Gamma_\circ \vdash \circ{:}A_\circ]\!]{:}B}{\Gamma \vdash^{\preceq}_{\Sigma} M_1(E_2[\![\Gamma_\circ \vdash \circ{:}A_\circ]\!]){:}A} \quad A_\circ \not\preceq^{A} A$$

(2) Since $\Gamma \vdash_\Sigma^{\preceq} E_2[\![M_\circ]\!] : B$, by Inversion $\Gamma \vdash_\Sigma^{\preceq} M_1 \downarrow \Pi x : B.A$ and $\Gamma \vdash_\Sigma^{\preceq} E_2[\![M_\circ]\!] \Downarrow B$. By inductive hypothesis there are

$$\theta' : \Gamma_\circ \stackrel{\preceq}{\rightarrow} \Delta_\circ,$$
$$\Delta \vdash_\Sigma^{\preceq} E_2'[\![\Delta_\circ \vdash \circ : [\overline{M}/\overline{x}]A_\circ]\!] : [\overline{M}/\overline{x}]B$$

such that $\theta E_2[\![M_\circ]\!] = E_2'[\![\theta' M_\circ]\!]$ and $\Delta \vdash_\Sigma^{\preceq} E_2'[\![\theta' M_\circ]\!] \Downarrow [\overline{M}/\overline{x}]B$. By stability of M_1, there is a M_1' such that $\theta M_1 \rightarrow_\eta^* M_1'$ and $\Delta \vdash_\Sigma^{\preceq} M_1' \downarrow [\overline{M}/\overline{x}](\Pi x : B.A)$. Let then E' be the environment

$$\Delta \vdash_\Sigma^{\preceq} M_1'(E_2'[\![\Delta_\circ \vdash \circ : [\overline{M}/\overline{x}]A_\circ]\!]) : [\overline{M}/\overline{x}]A,$$

it is as required.

(1) Similar to (1) of the previous case.

- Case:

$$\frac{\Gamma \vdash_\Sigma^{\preceq} E[\![\Gamma_\circ \vdash \circ : A_\circ]\!] : B \quad B \equiv A \quad \Gamma \vdash_\Sigma^{\preceq} B : \text{type}}{\Gamma \vdash_\Sigma^{\preceq} E[\![\Gamma_\circ \vdash \circ : A_\circ]\!] : A}$$

Both (1) and (2) follow trivially from inductive hypothesis and type conversion.

□

Notation. For the rest of this paper, we will write $E(\theta, M_\circ)$ and $\theta(E, M_\circ)$ to denote the environments E' and substitutions θ' obtained from Lemma 6.6.(1).

Definition 6.7 (Critical Pair). Let R be a HTRS, $\Gamma_1 \vdash_\Sigma^{\preceq} l_1 \rightarrow r_1 : C_1$, $\Gamma_2 \vdash_\Sigma^{\preceq} l_2 \rightarrow r_2 : C_2$ two rules in R, $\theta_1 : \Gamma_1 \stackrel{\preceq}{\rightarrow} \Delta$, $\theta_2 : \Gamma_2 \stackrel{\preceq}{\rightarrow} \Delta$, $\theta_1 = \{\overline{x} \mapsto \overline{N}\}$, and $\Gamma_1 \vdash_\Sigma^{\preceq} E[\![\Gamma_\circ \vdash \circ : A_\circ]\!] : A$ such that $l_1 = E[\![M_\circ]\!]$, $\theta_1(E_1, M_\circ)M_\circ = \theta_2 l_2$, then

$$\Delta \vdash_\Sigma^{\preceq} < E(\theta_1, M_\circ)[\![\theta_2 r_2]\!], \theta_1 r_1 >: [\overline{N}/\overline{x}]C_1$$

is a *critical pair*

Remark. By applying a renaming substitution and using α-conversion, we can assume, without loss of generality, $\Gamma_1 \cap \Gamma_2 = \emptyset$. The by Weakening it is easily verified that $\theta_1 \cup \theta_2 : \Gamma_1, \Gamma_2 \stackrel{\preceq}{\rightarrow} \Delta$ is a unifier of l_1 and $M_\circ$, and the definition above appears as a generalization of the familiar one for first-order TRSs.

Example 2. In the HTRS for the typed lambda calculus given before, letting

$$\Gamma_1 = A : \textbf{type}, B : \textbf{type}, F : (\textbf{term}\ A) \Rightarrow (\textbf{term}\ B), U : \textbf{term}\ A$$
$$\Gamma_2 = A : \textbf{type}, B : \textbf{type}, G : \textbf{term}\ (\textbf{arrow}\ A\ B)$$
$$\Delta = A : \textbf{type}, B : \textbf{type}, G : \textbf{term}\ (\textbf{arrow}\ A\ B), U : \textbf{term}\ A$$

$$\theta_1 = \{A \mapsto A, B \mapsto B, F \mapsto (\lambda x : \textbf{term}\ A.\textbf{app}\ G\ x), U \mapsto U\}$$
$$\theta_2 = \{A \mapsto A, B \mapsto B, G \mapsto G\}$$

$$E = \textbf{app}\ \circ\ U$$

we get the (trivial) critical pair

$$\Delta \vdash_\Sigma^{\preceq} < \textbf{app}\ G\ U, \textbf{app}\ G\ U >: \ \textbf{term}\ B$$

Proposition 6.8. *Let $\theta = \{\overline{x} \mapsto \overline{M}\} : \Gamma \stackrel{\preceq}{\rightarrow} \Delta$ be a substitution, $\Gamma \vdash_\Sigma^{\preceq} M \downarrow C$ stable for θ, $\theta M \rightarrow_\eta^* M_1'\ M_2'$, $\Delta \vdash_\Sigma^{\preceq} M_1' M_2' \downarrow [\overline{M}/\overline{x}]C$, then $M = M_1\ M_2$, $\theta M_1 \rightarrow_\eta^* M_1'$, $\theta M_2 = M_2'$.*

Proof. If $M = c$ or $M = x$ where $x \notin \text{supp}(\theta)$, then $\theta M \equiv M$, contradiction to uniqueness of atomic forms. Therefore $M = M_1\ M_2$. By inversion, there are types A, B such that $\Gamma \vdash_\Sigma^{\preceq} M_1 \downarrow \Pi x : A.B$, $\Gamma \vdash_\Sigma^{\preceq} M_2 : A$, $C \equiv [M_2/x]B$. Since M_1 is also stable for θ, by Lemma 6.4 there is an atomic term $\Delta \vdash_\Sigma^{\preceq} M_1' \downarrow [\overline{M}/\overline{x}](\Pi x : A.B)$ such that $\theta M_1 \rightarrow_\eta^* M_1''$. Then $\Delta \vdash_\Sigma^{\preceq} M_1'\ \theta M_2 : [\theta M_2/x][\overline{M}/\overline{x}]B$, and by type conversion, since $[\theta M_2/x][\overline{M}/\overline{x}]B \equiv [\overline{M}/\overline{x}][M_2/x]B$, the result. □

By definition, the only non-stable subterms of a pattern M have a very specific form, i.e. the must consist of a free variable, possibly applied to a sequence of terms equivalent to distinct bound variables. Unfortunately, this property is not preserved by subterms, since bound variables may become free. Proposition 6.2, however, suggests a slightly different definition of pattern, which relies on the support of a substitution rather than on on the set of free variables of the term.

Definition 6.9. Let $\theta : \Gamma \rightharpoondown \Delta$ be a substitution. A term $\Gamma \vdash_\Sigma M \Downarrow A$ ($\Gamma \vdash_\Sigma M \downarrow A$) is said to be a pattern for θ if each $x \in \mathrm{supp}(\theta)$ appears in M applied to terms η-equivalent to distinct bound variables.

Proposition 6.10. *If $\Gamma \vdash_\Sigma M \Downarrow A$ is a pattern, then it is a pattern for any substitution $\theta : \Gamma \rightharpoondown \Delta$.*

The following theorem says that any subterm N' of θM, where M is a pattern for θ, either corresponds to a subterm N of M (such that $\theta' N = N'$ for some $\theta' \doteq \theta$) or it is a subterm of $\theta(x)$ for some $x \in \mathrm{supp}\,\theta$. This key fact will play a central role in the proof of the Critical Pair Lemma.

Lemma 6.11. *Let*

$$\theta = \{\overline{x} \mapsto \overline{M}\} : \Gamma \overset{\preceq}{\rightharpoondown} \Delta$$
$$\Delta \vdash^{\preceq}_{\Sigma} E'[\![\Delta_\circ \vdash \circ : A'_\circ]\!] : C'$$
$$\Delta_\circ \vdash^{\preceq}_{\Sigma} M'_\circ \Downarrow A'_\circ,$$
$$\Gamma \vdash^{\preceq}_{\Sigma} M : C,$$

then

1. *if $\theta M = E'[\![M'_\circ]\!]$, $\Delta_\circ \vdash^{\preceq}_{\Sigma} E'[\![M'_\circ]\!] \Downarrow C'$ and $\Gamma \vdash^{\preceq}_{\Sigma} M \Downarrow C$ pattern for θ, or*
2. *if $\theta M \to^*_\eta E'[\![M'_\circ]\!]$, $\Delta_\circ \vdash^{\preceq}_{\Sigma} E'[\![M'_\circ]\!] \downarrow C'$, and $\Gamma \vdash^{\preceq}_{\Sigma} M \downarrow C$ both pattern and stable for θ,*

then either there is an environment E stable for θ such that $M = E[\![M_\circ]\!]$, $E' = E(\theta, M_\circ)$, $M'_\circ = \theta(E, M_\circ)M_\circ$, or there are well-typed environments E_M, E_θ and variable $x \in \mathrm{supp}(\theta)$ such that $M = E_M[\![x\overline{N}]\!]$, $N_i \equiv y_i$, $\theta(x) = \lambda\overline{y} : \overline{C}.E_\theta[\![M'_\circ]\!]$, $E' = E_M(\theta, x\overline{N})[\![E_\theta]\!]$.

Proof. By induction on the derivation of $\Delta \vdash^{\preceq}_{\Sigma} E'[\![\Delta_\circ \vdash \circ : A'_\circ]\!] : C'$, where $C' \equiv [\overline{M}/\overline{x}]C$:

- Case

$$\frac{\Delta_\circ \vdash^{\preceq}_{\Sigma} A'_\circ\text{:type} \quad \Delta_\circ \subseteq \Delta}{\Delta \vdash^{\preceq}_{\Sigma} [\![\Delta_\circ \vdash \circ : A'_\circ]\!] : A'_\circ}$$

  (1), (2) Immediate, by letting $E = \circ$.

- Case:

$$\frac{\Delta \vdash^{\preceq}_{\Sigma} A'\text{:type} \quad \Delta, x{:}A' \vdash^{\preceq}_{\Sigma} E'_1[\![\Delta_\circ \vdash \circ : A'_\circ]\!] : B}{\Delta \vdash^{\preceq}_{\Sigma} \lambda x{:}A'.E'_1[\![\Delta_\circ \vdash \circ : A'_\circ]\!] : \Pi x{:}A'.B'} \quad A \preceq^M_\Sigma B$$

  (1) By Inversion on $\Delta \vdash^{\preceq}_{\Sigma} \lambda x : A'.E'_1[\![M'_\circ]\!] \Downarrow \Pi x : A'.B'$ we obtain immediately $\Delta, x : A' \vdash^{\preceq}_{\Sigma} E'_1[\![M'_\circ]\!] \Downarrow B$. From the derivation of $\Gamma \vdash_\Sigma M \Downarrow C$ we get types A, B such that $M = \lambda x : A.M_1$, $C \equiv \Pi x : A.B$ and $\Gamma, x : A \vdash^{\preceq}_{\Sigma} M_1 \Downarrow B$. By Proposition 6.2 and uniqueness of canonical forms we conclude $A' = [\overline{M}/\overline{x}]B$. The result then follows by inductive hypothesis.

- Case:

$$\frac{\Delta \vdash^{\preceq}_{\Sigma} E'_1[\![\Delta_\circ \vdash \circ : A'_\circ]\!] : \Pi x{:}B'.A' \quad \Delta \vdash^{\preceq}_{\Sigma} M'_2 : B'}{\Delta \vdash^{\preceq}_{\Sigma} (E'_1[\![\Delta_\circ \vdash \circ : A'_\circ]\!])M'_2 : [M'_2/x]A'}$$

  (2) By Inversion on $\Delta \vdash^{\preceq}_{\Sigma} (E'_1[\![M'_\circ]\!])M'_2 \downarrow [M'_2/x]A'$ we obtain immediately $\Delta, x : A' \vdash^{\preceq}_{\Sigma} E'_1[\![M'_\circ]\!] \downarrow B$. By Proposition 6.8, $M = M_1\ M_2$ and inversion on the derivation of $\Gamma \vdash^{\preceq}_{\Sigma} M \Downarrow C$ there are types A, B such that $\Gamma \vdash^{\preceq}_{\Sigma} M_1 \Downarrow \Pi x : B.A$, $\Gamma \vdash^{\preceq}_{\Sigma} M_2 \Downarrow B$, and $C \equiv [M_2/x]B$. From Lemma 6.4, by uniqueness of atomic forms we deduce $\theta M_2 = M'_2$, $\theta M_1 \to^*_\eta E'_1[\![M'_\circ]\!]$, hence the result follows by inductive hypothesis.

  (1) We must have $\Delta \vdash^{\preceq}_{\Sigma} C'_{\Downarrow} \downarrow$ type. It is not difficult then to verify that $\Gamma \vdash^{\preceq}_{\Sigma} C_{\Downarrow} \downarrow$ type, and therefore by Inversion $\Gamma \vdash^{\preceq}_{\Sigma} M \downarrow C$. If M is stable for θ, the result follows from (1). Otherwise, by definition, it is easy to verify $M = x\overline{N}$, $N_i \equiv y_i$, $x \in \mathrm{supp}(\theta)$, $\theta(x) = \lambda\overline{y} : \overline{C}.E'[\![M'_\circ]\!]$. Hence $E_M = \circ$, $E_\theta = E'$ are as required.

- Case:

$$\frac{\Delta \vdash_{\Sigma}^{\preceq} M_1' : \Pi x : B'.A' \quad \Delta \vdash_{\Sigma}^{\preceq} E_2'[\![\Delta_\circ \vdash \circ : A_\circ']\!] : B'}{\Delta \vdash_{\Sigma}^{\preceq} M_1'(E_2'[\![\Delta_\circ \vdash \circ : A_\circ']\!]) : A'} \quad A_\circ' \not\preceq^A A'$$

(2) By Inversion on $\Delta \vdash_{\Sigma}^{\preceq} M_1'(E_2'[\![M_\circ']\!]) \downarrow A'$ we obtain immediately $\Delta \vdash_{\Sigma}^{\preceq} E_1'[\![M_\circ']\!] \Downarrow B$. By Proposition 6.8, $M = M_1\ M_2$, and by inversion on the derivation of $\Gamma \vdash_{\Sigma}^{\preceq} M \Downarrow C$ there are types A, B such that $\Gamma \vdash_{\Sigma}^{\preceq} M_1 \Downarrow \Pi x : B.A$, $\Gamma \vdash_{\Sigma}^{\preceq} M_2 \Downarrow B$, and $C \equiv [M_2/x]B$. From Lemma 6.4, by uniqueness of atomic forms we deduce $\theta M_2 = E_2'[\![M_\circ']\!]$, $\theta M_1 \rightarrow_\eta^* M_1'$, hence the result follows by inductive hypothesis. Notice that $head(A') = head(A)$.

(1) We must have $\Delta \vdash_{\Sigma}^{\preceq} C_{\Downarrow}' \downarrow$ type. It is not difficult then to verify that $\Gamma \vdash_{\Sigma}^{\preceq} C_{\Downarrow} \downarrow$ type, and therefore by Inversion $\Gamma \vdash_{\Sigma}^{\preceq} M \downarrow C$. If M is stable for θ, the result follows from (1). Otherwise, by definition, it is easy to verify $M = x\overline{N}$, $N_i \equiv y_i$, $x \in \mathrm{supp}(\theta)$, $\theta(x) = \lambda \overline{y} : \overline{C}.E'[\![M_\circ']\!]$. Hence $E_M = \circ$, $E_\theta = E'$ are as required.

- Case:

$$\frac{\Delta \vdash_{\Sigma}^{\preceq} E'[\![\Delta_\circ \vdash \circ : A_\circ']\!] : B' \quad B' \equiv A' \quad \Delta \vdash_{\Sigma}^{\preceq} B' : \mathrm{type}}{\Delta \vdash_{\Sigma}^{\preceq} E[\![\Delta_\circ \vdash \circ : A_\circ']\!] : A'}$$

Both (1) and (2) follow trivially from inductive hypothesis and type conversion.

□

Theorem 6.12 (Critical Pair Lemma). *Let R be a HTRS, if $\Gamma \vdash_{\Sigma}^{\preceq} M \overset{R}{\rightarrow} N_1 : A$ and $\Gamma \vdash_{\Sigma}^{\preceq} M \overset{R}{\rightarrow} N_2 : A$ then either there is a critical pair in R, or there are rewriting sequences $\Gamma \vdash_{\Sigma}^{\preceq} N_1^{(i)} \overset{R}{\rightarrow} N_1^{(i+1)}$ $(0 \leq i < n_1)$, $\Gamma \vdash_{\Sigma}^{\preceq} N_2^{(i)} \overset{R}{\rightarrow} N_2^{(i+1)}$ $(0 \leq i < n_2)$ such that $N_1^{(0)} \equiv N_1$, $N_2^{(0)} = N_2$, $N_1^{(n_1)} \equiv N_2^{(n_2)}$.*

Proof. By definition, $\Gamma \vdash_{\Sigma}^{\preceq} M \overset{R}{\rightarrow} N_k$ if and only if there are

$$\Delta_k \vdash_{\Sigma}^{\preceq} l_k \rightarrow r_k : C_k \in R, \theta_k : \Delta_k \overset{\preceq}{\rightarrow} \Gamma, \Gamma \vdash_{\Sigma}^{\preceq} E^{(k)}[\![\Gamma_\circ^{(k)} \vdash \circ : A_\circ^{(k)}]\!] : A$$

such that $M_{\Downarrow} = E^{(k)}[\theta_k l_k]$, $(N_k)_{\Downarrow} = E^{(k)}[\theta_k r_k]$, $(k = 1, 2)$.

The proof proceeds on induction on the size of the environments $E^{(1)}, E^{(2)}$. We show some representative cases:

- $E^{(1)} = \lambda x : A.E_1^{(1)}$, $E^{(2)} = \lambda x : A.E_1^{(2)}$:

  Using type conversion, if necessary, we can assume that the type derivations of $E^{(1)}, E^{(2)}$ are:

$$\frac{\Gamma \vdash_{\Sigma}^{\preceq} A : \mathrm{type} \quad \Gamma, x : A \vdash_{\Sigma}^{\preceq} E_1^{(1)}[\![\Gamma_\circ^{(1)} \vdash \circ : A_\circ^{(1)}]\!] : B}{\Gamma \vdash_{\Sigma}^{\preceq} \lambda x : A.E_1^{(1)}[\![\Gamma_\circ^{(1)} \vdash \circ : A_\circ^{(1)}]\!] : \Pi x : A.B} \quad A \preceq_{\Sigma}^{M} B \qquad \frac{\Gamma \vdash_{\Sigma}^{\preceq} A : \mathrm{type} \quad \Gamma, x : A \vdash_{\Sigma}^{\preceq} E_1^{(2)}[\![\Gamma_\circ^{(2)} \vdash \circ : A_\circ^{(2)}]\!] : B}{\Gamma \vdash_{\Sigma}^{\preceq} \lambda x : A.E_1^{(2)}[\![\Gamma_\circ^{(2)} \vdash \circ : A_\circ^{(2)}]\!] : \Pi x : A.B} \quad A \preceq_{\Sigma}^{M} B$$

  Then $M_{\Downarrow} = \lambda x : A.M_1$, and by Inversion on $\Gamma, x : A \vdash_{\Sigma}^{\preceq} E_1^{(1)}[\![\theta_1 l_1]\!] : B$ we have $\Gamma, x : A \vdash_{\Sigma}^{\preceq} M_1 \Downarrow B$. Therefore

$$\Gamma, x : A \vdash_{\Sigma}^{\preceq} M_1 \overset{R}{\rightarrow} E_1^{(k)}[\![\theta_k r_k]\!] \quad (k = 1, 2),$$

  and the result follows by inductive hypothesis.

- $E^{(1)} = E_1^{(1)}\ N$, $E^{(2)} = E_1^{(2)}\ N$:

  Using type conversion, if necessary, we can assume that the type derivations of $E^{(1)}, E^{(2)}$ are:

$$\frac{\Gamma \vdash_{\Sigma}^{\preceq} E_1^{(1)}[\![\Gamma_\circ^{(1)} \vdash \circ : A_\circ^{(1)}]\!] : \Pi x : A.B \quad \Gamma \vdash_{\Sigma}^{\preceq} N : A}{\Gamma \vdash_{\Sigma}^{\preceq} (E_1^{(1)}[\![\Gamma_\circ^{(1)} \vdash \circ : A_\circ^{(1)}]\!]) N : [N/x]B} \qquad \frac{\Gamma \vdash_{\Sigma}^{\preceq} E_1^{(2)}[\![\Gamma_\circ^{(2)} \vdash \circ : A_\circ^{(2)}]\!] : \Pi x : A.B \quad \Gamma \vdash_{\Sigma}^{\preceq} N : A}{\Gamma \vdash_{\Sigma}^{\preceq} (E_1^{(2)}[\![\Gamma_\circ^{(2)} \vdash \circ : A_\circ^{(2)}]\!]) N : [N/x]B}$$

  By inversion, $M_{\Downarrow} = (h\ \overline{M})\ N$. Since all rules are of atomic type, it is easy to see that there are indexes i_k such that

$$E_1^{(k)} = h\ M_1 \ldots M_{i_k - 1}\ E_{i_k}^{(k)}\ M_{i_k + 1} \ldots M_m \quad (k = 1, 2)$$

  There are two subcases:

– $i_1 = i_2$
By inversion on the derivation of $\Gamma \vdash^{\preceq}_{\Sigma} M_{\Downarrow} \Downarrow [N/x]B$ we get $\Gamma(M_{\Downarrow}, M_{i_1}) \vdash^{\preceq}_{\Sigma} M_{i_1} \Downarrow A(M_{\Downarrow}, M_{i_1})$, and the result follows by induction hypothesis.

– $i_1 \neq i_2$
Assuming $i_1 < i_2$, it is easy to verify that

$$\Gamma \vdash^{\preceq}_{\Sigma} (h\ M_1 \ldots M_{i_1-1}\ E^{(1)}_{i_1}\ M_{i_1+1} \ldots M_{i_2-1}\ E^{(2)}_{i_2}[\![\theta_2 r_2]\!]\ M_{i_2+1} \ldots M_m)\ N : [N/x]B$$
$$\Gamma \vdash^{\preceq}_{\Sigma} (h\ M_1 \ldots M_{i_1-1}\ E^{(1)}_{i_1}[\![\theta_1 r_1]\!]\ M_{i_1+1} \ldots M_{i_2-1}\ E^{(2)}_{i_2}\ M_{i_2+1} \ldots M_m)\ N : A$$

are well-typed contexts, hence letting

$$N^{(1)}_1 = N^{(2)}_1 = (h\ M_1 \ldots M_{i_1-1}\ E^{(1)}_{i_1}[\![\theta_1 r_1]\!]\ M_{i_1+1} \ldots M_{n_2-1}\ E^{(2)}_{n_2}[\![\theta_2 r_2]\!]\ M_{n_2+1} \ldots M_m)\ N$$

we have

$$\Gamma \vdash^{\preceq}_{\Sigma} N_k \xrightarrow{R} N^{(k)}_1 : A \quad (k = 1, 2)$$

- $E^{(1)} = \circ$:
  Then $\theta_1 l_1 = E^{(2)}[\![\theta_2 l_2]\!]$. By Lemma 6.11 we have two possible subcases:
  – There is E stable for θ_1 such that $l_1 = E[\![M_\circ]\!]$, $E^{(2)} = E(\theta_1, M_\circ)$, $\theta_2 r_2 = \theta_1(E, M_\circ)M_\circ$.
  Then by definition

$$\Gamma \vdash^{\preceq}_{\Sigma} < E(\theta_1, M_\circ)[\![\theta_2 r_2]\!], \theta_1 r_1 >: A$$

  is a critical pair.
  – There are well-typed environments $E_{\theta_1 l_1}, E_{\theta_1}$ and variable $x \in \mathrm{supp}(\theta_1)$ such that $\theta_1 l_1 = E_{\theta_1 l_1}[\![x\overline{M}]\!]$, $M_i \equiv y_i$, $\theta_1(x) = \lambda\overline{y} : \overline{C}.E_{\theta_1}[\![\theta_2 l_2]\!]$, $E' = E_{\theta_1 l_1}(\theta_1, x\overline{N})[\![E_{\theta_1}]\!]$.
  Let $\theta'_1 : \Delta_1 \xrightarrow{\preceq} \Gamma$ defined as

$$\theta'_1(y) = \begin{cases} \theta_1(y) & y \neq x \\ \lambda\overline{y} : \overline{C}.E_{\theta_1}[\![\theta_2 r_2]\!] & y = x, \end{cases}$$

  we want to show that both $N_1 = \theta_1 l_1$ and $N_2 = E^{(2)}[\![\theta_2 l_2]\!]$ both rewrite to $\theta'_1 r_1$.
  Assume $\Delta_1 \vdash^{\preceq}_{\Sigma} \theta_1(x) : C$, let z be a fresh variable, define $\theta^z_1 : \Delta_1 \xrightarrow{\preceq} \Gamma, z : C$ by

$$\theta^z_1(y) = \begin{cases} \theta_1(y) & y \neq x \\ z & y = x. \end{cases}$$

  By replacing progressively all the occurrences of z in $\theta^z_1 l_1$, starting from the occurrence in $E_{\theta_1 l_1}(\theta^z_1, x\overline{N})$, with $\lambda\overline{y} : \overline{C}.E_{\theta_1}[\![\theta_2 r_2]\!]$, we get a rewrite sequence $N^{(i)}_1$ such that $N^{(0)}_1 \equiv N_1$, $N^{(n_1-1)}_1 \equiv \theta'_1 l_1$. Similarly, by replacing all the occurrences of z in $\theta^z_1 r_1$ with $\lambda\overline{y} : \overline{C}.E_{\theta_1}[\![\theta_2 r_2]\!]$ we get a rewrite sequence $N^{(i)}_2$ such that $N^{(0)}_2 = [\theta_1(x)/y]\theta^z_1 r_1 \equiv N_2$, $N^{(n_2)}_2 \equiv \theta'_1 r_1$. The result then follows by a single additional rewrite step.

□

Definition 6.13. Let R be a HTRS, if whenever $\Gamma \vdash^{\preceq}_{\Sigma} M \xrightarrow{R} N_1 : A$ and $\Gamma \vdash^{\preceq}_{\Sigma} M \xrightarrow{R} N_2 : A$ there are rewriting sequences $\Gamma \vdash^{\preceq}_{\Sigma} N^{(i)}_1 \xrightarrow{R} N^{(i)}_1$ $(0 \leq i \leq n_1)$, $\Gamma \vdash^{\preceq}_{\Sigma} N^{(i)}_2 \xrightarrow{R} N^{(i)}_2$ $(0 \leq i \leq n_2)$ such that $N^{(0)}_1 \equiv N_1$, $N^{(0)}_2 = N_2$, $N^{(n_1)}_1 \equiv N^{(n_2)}_2$, R is said to be locally confluent.

Corollary 6.14. *If for all critical pairs $\Gamma \vdash^{\preceq}_{\Sigma} < M, N > : A$ of a HTRS R both M and N R-rewrite to a common term, then R it is locally confluent.*

7. Future Developments

The Critical Pair Lemma gives us a criterion to check for local confluence of a HTRS. As said before, local confluence assumes a great relevance in presence of termination, since by Newman's Lemma, it provides a simple and computationally-effective way to check for confluence. Very recently, in [5] and [12] two methods of proving the termination of a HTRS have been proposed for simple types; it is our hope that these will translate to dependent types, and that perhaps the richer type structure will allow to obtain better results.

Another interesting line of research is R-rewriting modulo a (higher-order) equational theory E. In LF, where the relation $\prec^A$ define a hierarchy of types, it is possible to define a suggestive notion of "multi-staged completion": once a terminating HTRS, defined on some set S of type classes, has been checked for local confluence, it becomes part of the underlying equational theory E modulo over which a new HTRS, defined of a set S' of "higher" type classes (i.e. $\forall A \in S \exists B \in S'\ A \prec^A B$, or at least $\forall A \in S \forall B \in S'\ B \not\preceq^A_\Sigma A$) is in turn tested for confluence, and so on.

8. Acknowlegments

I would like to thank Prof. Frank Pfenning for his help, suggestions, and support. I also thank E. Rohwedder and W. Gehrke for their valuable comments.

References

[1] Coquand, T. *An algorithm for testing conversion in type theory.* Logical Frameworks, Cambridge University Press, 1991, pp. 155-279

[2] Geuvers, H. *The Church-Rosser Property for $\beta\eta$-Reduction in Typed λ-Calculi.* Seventh. Ann. IEEE Symp. on Lofic in Comp. Sci., IEEE Computer Society Press, 1992, pp. 453-460

[3] Harper, R. , Honsell F., Plotkin, G. *A framework for defining logics.* Journal of the Association for Computing Machinery, January 1993, pp. 143-184

[4] Klop, J. *Combinatory Reduction Systems.* Mathematical Centre Tracts 127. Stichting Mathematisch Centrum, Amsterdam, 1980.

[5] Kahrs, D.*Towards a Domain Theory for Termination Proofs.* Sixth International Conference on Rewriting Techniques and Applications (RTA), 1994

[6] Knuth, D. and Bendix, P. *Simple Word Problems in Universal Algebra.* Computational Problems in Abstract Algebra, Pergamon Press, 1972, pp. 263-297

[7] Mayr, R. , Nipkow, T. *Higher-Order Rewrite Systems and their Confluence.* Tech. Report, Technische Universität München, 1994

[8] Miller, D. *A Logic Programming Language With Lambda abstraction, Function Variables, and Simple Unification.* LFCS report series, University of Edinburgh, 1991, pp. 253-281

[9] Nipkow, T. *Higher-Order Critical Pairs.* Proceedings of the 5th IEEE Conference of Logic In Computer Science (LICS), 1990, pp. 342-348

[10] Pfenning, F. *Logic Programming in the LF Logical Framework.* G. Huet, G. Plotkin ed., Logical Frameworks, Cambridge University Press, 1991, pp. 149-181

[11] Pfenning, F. *Unification and ant-unification in the Calculus of Constructions.*, Proceedings of the 6th IEEE Conference of Logic In Computer Science (LICS), 1991, pp. 149-181

[12] Rohwedder, E. , Pfenning, F. *Mode and Termination analysis for Higher-Order Logic.*, to appear at ESOP 96

[13] Snyder, W. *A Proof Theory for General Unification.* Birkhauser, 1991

[14] Salvesen, A. *The Church-Rosser Property for Pure Systems with $\beta\eta$-Reduction.* Tech. Rep., University of Oslo, 1992

[15] Van de Pol, J. *Termination Proofs for Higher-Order Rewrite Systems*, J. Heering, K. Meinke, B. Möller, T. Nipkow ed., Higher Order Algebra, Logic and Term Rewriting, Lect. Notes in Comp. Sci., Vol 816, Springer Verlag, 1994

[16] Van Oostrom, V. , Van Raamsdonk, F. *Comparing Combinatory Reduction Systems and Other Systems.* J. Heering, K. Meinke, B. Möller, T. Nipkow ed., Higher Order Algebra, Logic and Term Rewriting, Lect. Notes in Comp. Sci., Vol 816, Springer Verlag, 1994, pp. 305-325