LIF

Laboratoire d'Informatique Fondamentale
de Marseille

Unité Mixte de Recherche 6166
CNRS – Université de Provence – Université de la Méditerranée

An Effective Proof of the Well-Foundedness of the Multiset Path Ordering

Solange Coupet-Grimal
and William Delobel

Rapport/Report 27-2005

13 décembre 2005

An Effective Proof of the Well-Foundedness of the Multiset Path Ordering

Solange Coupet-Grimal
and William Delobel

LIF – Laboratoire d'Informatique Fondamentale de Marseille
UMR 6166
CNRS – Université de Provence – Université de la Méditerranée

CMI, 39 rue Joliot-Curie, F-13453, Marseille, France.

{Solange.Coupet, Delobel}@cmi.univ-mrs.fr.

Abstract/Résumé

The contribution of this paper is an effective proof of the well-foundedness of MPO, as a term of the Calculus of Inductive Constructions. This proof is direct, short and simple. It is a sequence of nested inductions and it only requires as preliminary results the transitivity of MPO and the fact that finite multisets whose elements are accessible for the basic relation are themselves accessible for the multiset order. The terms we consider are not supposed to be ground nor the signature to be finite. All the proofs have been carried out in the Coq proof-assistant.

Keywords: Termination, well-foundedness, proof-assistant.

La contribution de cet article est une preuve effective de la bonne fondation de l'ordre récursif multi-ensemble sur les chemins (Multiset Path Ordering (MPO)), comme terme du Calcul des Constructions Inductives. Cette preuve est directe, courte et simple. Elle ne fait appel qu'à des résultats préliminaires élémentaires et s'applique à des termes contenant des variables, construits sur une signature non nécessairement finie de symboles fonctionnels d'arité variable. Toutes les preuves présentées ici ont été vérifiées par l'assistant de preuves Coq.

Mots-clés : Terminaison, bonne fondation, assistant de preuves.

Relecteurs/Reviewers: Roberto Amadio et Pierre Lescanne.

1 Introduction

Termination is an important property of term rewriting systems (TRS), that is undecidable in general as shown by Huet and Lankford [HL78]. A standard method to prove the termination of a particular TRS consists in finding a well-founded order $>$ such that $s > t$ for each rewrite step $s \to t$. Recursive Path Orders (RPO), introduced by Dershowitz [Der82], are simplification orders, closed both under context and under substitutions. So, for such orders, it is sufficient to prove that the left hand sides of rewrite rules are greater than their right hand sides. They have some other interesting features. For example, it is decidable whether the termination of a finite TRS with a finite signature can be proved with RPO (see [BN98] for an overview of these properties). These orders compare terms by first comparing their head symbol, and then the lists of their immediate arguments. These lists can be compared either as multisets in the case of the Multiset Path Order (MPO), or lexicographically in the case of the Lexicographic Path Order (LPO), or by combining both approaches (RPO with status).
The contribution of this paper is an effective proof of the well-foundedness of MPO, as a term of the Calculus of Inductive Constructions (CIC). It has been carried out in the Coq proof-assistant [Tea04] [The] to be part of *CoLoR*, the Coq library on rewriting and termination [CoL]. This proof is direct in the sense that it is not obtained as an application of general theorems that have been produced recently ([GL01] [DG04] see section 5). It is short (30 lines of Coq), simple and exclusively relies on nested inductions. It only requires as preliminary results the transitivity of MPO and the fact that a finite multiset the elements of which are accessible for the basic relation is itself accessible for the multiset order. Our specification of MPO is general since the terms are not supposed to be ground nor the signature to be finite.
The paper is self-contained and organized as follows. Section 2 is devoted to the rules that specify in the CIC the key notions of this paper: accessibility, well-foundedness and well-founded induction. Section 3 treats the finite multisets and the multiset ordering. In section 4, MPO is defined and its well-foundedness is proved. We present related work and we conclude in section 5.

2 Well-Foundedness

Let $(A, <)$ be a set equipped with a binary relation. The key notion for expressing the well-foundedness of $<$ is *accessibility*. Intuitively, an element a of A is accessible for the relation $<$, and this is denoted by $(acc_< \ x)$, if and only if all descending chains starting with x are finite. In the CIC, this is expressed by a generalized inductive definition (1), associated with the induction principle (2) below:

$$\frac{\forall y : A,\ y < x \ \to\ (acc_< \ y)}{(acc_< \ x)} \tag{1}$$

$$\frac{(acc_< \ x) \quad (\forall y : A,\ y < x \ \to\ (P\ y)) \ \to\ (P\ x)}{(P\ x)} \tag{2}$$

Clearly, minimal elements are accessible, and this is the base case of the recursive definition (1). As far as the induction principle is concerned, it makes it possible to conclude that an accessible element x satisfies predicate P by using as *induction hypothesis* the fact that P is satisfied by all elements y less than x.

Now, the relation $<$ is well-founded if and only if all descending chains are finite, that is if and only if all elements are accessible. Therefore, the predicate WF is defined by:

$$(WF\ \ <) := \forall x : A,\ (acc_< \ x) \tag{3}$$

Consequently, the following principle of *well founded induction* holds for all well-founded relations $<$:

$$\frac{(\forall\, x : A) \quad (\forall y : A,\ y < x\ \rightarrow\ (P\ y))\ \rightarrow\ (P\ x)}{\forall x : A,\ (P\ x)} \tag{4}$$

3 Multiset Order

3.1 Finite Multisets

Let us consider a setoïd $(A, \sim_A)$, that is a set A equipped with an equivalence relation $\sim_A$. Let us assume that $\sim_A$ is decidable :

$$\forall a, b : A,\ (a\ \sim_A\ b)\ \vee\ \neg(a\ \sim_A\ b)$$

A multiset M of A is an application from A to the set $I\!N$ of natural numbers, compatible with $\sim_A$. For all elements a of A, $M(a)$ is called *multiplicity* of a in M. By definition, an element a belongs to M if and only if its multiplicity is greater than 0. Finite multisets are those that have only finitely many elements modulo $\sim_A$. We represent finite multisets by listing their elements modulo $\sim_A$ in double curly brackets. Each element occurs as many times as its multiplicity. For instance, $M = \{\!\{1, 1, 5, 5, 5, 6, 6, 7\}\!\}$ is the multiset on the setoïd $(I\!N, =)$ defined by $M(1) = 2$, $M(5) = 3$, $M(6) = 2$, $M(7) = 1$, and null elsewhere.

Finite multisets have been implemented in the CIC by Koprowski [CoL, Kop04]. Both subsections 3.1 and 3.2 refer to these Coq libraries, that we have slightly modified and complemented for our purpose.

The author gives an axiomatization for the finite multisets and proves its consistency by showing that it can be modelled by the set of the finite lists of elements of A. The axiomatization includes in particular the union and the difference operations, a special element $\emptyset$, and an equivalence relation $\sim_{mul}$.
The finiteness of the multisets is expressed by means of the following reasoning principle:

$$\frac{(P\ \emptyset) \qquad (\forall M\ : (Multiset\ A))(\forall a : A)\ (P\ M) \rightarrow (P\ M \cup \{\!\{a\}\!\})}{\forall M : (Multiset\ A)\ (P\ M)} \tag{5}$$

Note that type $Multiset$ is parameterized by the base set A. All throughout the paper the multisets we consider are finite and this precision will be omitted in the sequel.

Then, from these axiomatic definitions, several other operations are introduced. In particular, and this is of interest for our purpose, from a function *insert* that adds an element to a multiset, a function *list2multiset* transforms recursively each list in a multiset by inserting its head in the multiset resulting of the transformation of its tail.

We have added a function *multiset2list* which builds a list from a multiset M by induction on M (principle 5), and we have proved that for all multisets M, $(list2multiset\,(multiset2list\,M)) \sim_{mul} M$.

3.2 Order on Finite Multisets

Let us now consider a new binary relation $>_A$ on the setoïd $(A, \sim_A)$. This relation induces a relation $>_{mul,>_A}$ on the multisets of A. A multiset N is less than a multiset M if it is obtained by replacing finitely many elements of M by smaller elements. This relation is precisely defined by induction as follows:

$$\frac{\begin{array}{c} M\ \sim_{mul}\ Z \cup X \quad N \sim_{mul}\ Z \cup Y \quad \neg(X \sim_{mul} \emptyset) \\ (\forall y : A,\ y \in Y\ \rightarrow\ \exists x : A,\ x \in X\ \wedge\ x >_A y) \end{array}}{M\ >_{mul,>_A}\ N}$$

Let $<_A$ and $<_{mul,>_A}$ denote the transposed relations of $>_A$ and $>_{mul,>_A}$, respectively.

Lemma 1 *If $>_A$ is transitive, then $>_{mul,>_A}$ is transitive.*

In fact, in order to establish transitivity results by structural induction on the elements of the base set, we shall need a more general result, that we have added to the existing Coq libraries.

Lemma 2 *Let M be a multiset of elements of A. Let us assume that :*

$$\forall a : A,\, a \in M \;\rightarrow\; (\forall a_1,\, a_2\, :\, A,\, a_2 >_A a_1 \;\rightarrow\; a_1 >_A\, a \;\rightarrow\; a_2 >_A a)$$

Then for all multisets M_1 and M_2 :

$$M_2 >_{mul,>_A} M_1 \rightarrow M_1 >_{mul,>_A} M \;\rightarrow\; M_2 >_{mul,>_A} M.$$

If one assumes that the relation $>_A$ is transitive, it can be shown that the relation $>_{mul,<_A}$ on the multisets is the transitive closure of a reduction relation $>_{red,>_A}$ defined by:

$$\frac{M \sim_{mul} Z \cup \{\!\{a\}\!\} \quad N \sim_{mul} Z \cup Y \quad (\forall y : A,\; y \in Y \;\rightarrow\; a >_A y)}{M \;>_{red,>_A}\; N}$$

Lemma 3 *If the relation$>_A$ is transitive, then for all multisets M and N*

$$M \;>_{mul,>_A}\; N \;\leftrightarrow\; M(>_{red,>_A})^+\, N$$

Proof. The proof in the existing Coq libraries uses the additional decidability hypothesis : $\forall a, b : A,\; (a >_A b) \;\vee \neg\; (a >_A b)$ that is not trivial to prove in case of the relation MPO on first order terms. But in fact, this hypothesis can be weakened by using only the decidability of $\sim_A$ that is mandatory all throughout the development. So we have modified this proof in this way. □

Lemma 4 *For all multisets M of A, if all elements of M are accessible for the relation $<_A$, then M is accessible for the relation $(<_{red,>_A})^+$.*

An inductive proof of this lemma has been performed by Buchholtz, presented by Nipkow in [Nip98], and carried out in Coq by Koprowski. We have added to the Coq libraries the reciprocal property :

Lemma 5 *For all multisets M on A, if M is accessible for the relation $(<_{red,>_A})^+$, then all elements of M are accessible for the relation $<_A$.*

Proof. The proof is performed by induction on the accessibility hypothesis, following principle (2). So, we have to prove that all the elements of a multiset M are accessible under the induction hypothesis:

$$\forall N : (MultisetA), N(<_{red,<_A})^+ M \;\rightarrow\; \forall n : A,\; n \in N \;\rightarrow\; (acc_{<_A}\, n) \qquad .$$

Let m be an element of M. Proving that m is accessible for $<_A$, by definition 1, amounts to prove that all n such that $n <_A m$ are accessible. This is obtained by applying the induction hypothesis with $N = M - \{\!\{m\}\!\} + \{\!\{n\}\!\}$. □

Moreover, let us mention that an immediate consequence of lemma 4 is that the relation $(<_{red,>_A})^+$ on multisets is well-founded as soon as the relation $<_A$ on the base set A is well-founded.

3.3 Multiset Order on the Lists

Since we aim at studying first order terms, and since such terms are encoded as functional symbols applied to the list of their arguments (see section 4.1), we are led to convert the order on the multisets to a relation on the lists.

Let us consider a setoïd A equipped with a relation $>_A$ and let us define a relation $\ll_{>_A}$ as the inverse image of $<_{mul,\,>_A}$ by the function *list2multiset*:

$$\ll_{>_A} := \lambda l, l' : (\mathit{list}\,A).\,(\mathit{list2multiset}\,l) <_{mul,>_A} (\mathit{list2multiset}\,l')$$

We first establish a result slightly more general than the transitivity of $\ll_{>_A}$ under an hypothesis weaker than the transitivity of the relation $>_A$.

Lemma 6 *Let l be a list of elements of A. Let us assume that :*

$$\forall a : A,\, a \in l \to (\forall a_1, a_2 : A,\, a <_A a_1 \to a_1 <_A a_2 \to a <_A a_2)$$

Then :

$$\forall l_1, l_2 : (\mathit{list}\,A),\, l \ll_{>_A} l_1 \to l_1 \ll_{>_A} l_2 \to l \ll_{>_A} l_2.$$

Proof This lemma is a reformulation of lemma 2. □
The following lemmas are the key results for proving the well-foundedness of MPO.

Lemma 7 *Let us assume that the relation $>_A$ is transitive. For all lists l of elements of A, if $(\mathit{list2multiset}\,l)$ is accessible for the relation $(<_{red,<_A})^+$, then l is accessible for the relation $\ll_{>_A}$.*

Proof As $<_A$ is transitive, the relations $(<_{red,<_A})^+$ and $<_{mul,>_A}$ are equivalent (see lemma 3). Thus, it is sufficient to prove the result for the latter. It follows from the fact that for any function f and relation $<$, if $(f\,x)$ is accessible for $<$, then x is accessible for $(f^{-1}\ <)$ (this is proved in the standard Coq libraries). □
The converse is in the next lemma.

Lemma 8 *Let us assume that the relation $>_A$ is transitive. For all lists l of elements of A, if l is accessible for the relation $\ll_{>_A}$, then $(\mathit{list2multiset}\,l)$ is accessible for the relation $(<_{red,<_A})^+$.*

Proof As $<_{mul,>_A}$ is the inverse image of $\ll_{>_A}$, using the same approach as in the previous lemma, we would obtain that for all multiset M, if $(\mathit{multiset2list}\,M)$ is accessible for $\ll_{>_A}$, then M is accessible for $<_{mul,>_A}$, and thus for $(<_{red,<_A})^+$. Unfortunately, this does not allow to conclude, since list l is not equal, in general, to $(\mathit{multiset2list}\,(\mathit{list2multiset}\,l)))$. Function $\mathit{list2multiset}$ being not injective, its inverse is a non functional relation. Therefore, we must use the following lemma.

Lemma 9 *Let $(\mathcal{L}, \ll)$ and $(\mathcal{M}, <)$ be two sets equipped with binary relations. Let $r : \mathcal{L} \to \mathcal{M} \to Prop$ a relation such that:*

$$(\forall l : \mathcal{L})\ (\forall M, M' : \mathcal{M})\ (r\ l\ M) \to M' < M \to (\exists l' : \mathcal{L})\ (r\,l'\,M') \wedge l' \ll l$$

then

$$(\forall l : \mathcal{L})\ (\forall M : \mathcal{M})\ (r\ l\ M) \to\ (acc_{\ll}\ l)\ \to\ (acc_{<}\ M)$$

Proof The proof is performed by induction on hypothesis $(acc_{\ll}\ s)$. □
The proof of lemma 8 is done by applying lemma 9 with $\mathcal{L} = (list\ A)$, $\mathcal{M} = (Multiset\ A)$, and $r = \lambda l, M.\, M \sim_{mul} (\mathit{list2multiset}\ l)$. The hypothesis of lemma 9 is fulfilled by choosing $l' = (\mathit{multiset2list}\ M')$. □

Lemma 10 *Let us assume that the relation $>_A$ is transitive. For all lists l of elements of A, if all elements of l are accessible for the relation $<_A$, then l is accessible for the relation $\ll_{>_A}$.*

Proof From the transitivity of the relation $>_A$, we deduce the equivalence of the relation $<_{mul,>_A}$ on the multisets and the transitive closure of the reduction relation $<_{red,>_A}$. Therefore, using lemma 4, we deduce that $(\mathit{list2multiset}\ l)$ is accessible for $(<_{red,<_A})^+$. The result follows from lemma 7. □

Lemma 11 *Let us assume that the relation $>_A$ is transitive. For all lists l of elements of A, if l is accessible for the relation $\ll_{>_A}$, then all elements of l are accessible for the relation $<_A$.*

Proof It is similar to the previous one, but it relies on lemmas 5 and 8 . □
The following lemma will be instrumental in many proofs in the sequel.

Lemma 12 *Let l_1 and l_2 be two lists of elements of A, such that $l_1 \ll_{>_A} l_2$. Then, for all elements a_1 in l_1, there exists an element a_2 in l_2 such that $a_2 \geqslant_A a_1$.*

4 Multiset Path Ordering (MPO)

MPO is a binary relation on the first order terms. It has been introduced by Dershowitz [Der82] for proving termination of rewriting systems.

4.1 First order terms

Let us consider a set F of functional symbols, equipped with a well-founded transitive relation $<_F$ and X a set of variable names. The type *term* of first order terms on signature F can be defined inductively as follows:

$term\ :\ Set :=$
$\quad Var\ :\ X \to term\ |$
$\quad App\ :\ F \to (list\ term)\ \to\ term.$

where type *list* is classically defined by:

$(list\ term)\ :\ Set :=$
$\quad nil\ :\ (list\ term)\ |$
$\quad cons : term\ \to\ (list\ term)\ \to\ (list\ term).$

In the sequel, we shall use the usual simplified notations:

- $(s_1, \ldots, s_n)$ for $(cons\ s_1(\ldots(cons\ s_n\ nil)\ldots))$
- $\{\!\{s_1, \ldots, s_n\}\!\}$ for $(list2multiset\ (cons\ s_1(\ldots(cons\ s_n\ nil)\ldots)))$.
- $f(s_1, \ldots, s_n)$ for $(App\ f\ (cons\ s_1(\ldots(cons\ s_n\ nil)\ldots))$
- x for $(Var\ x)$
- $Vars(s)$ for the set of the variables that occur in term s.
- $s \in ss$ to express that s is an element of list ss.

An induction principle associated with type *term* can be stated by the following rule, in which P is a predicate on *term*.

$$\frac{\begin{array}{c}\forall x\ :\ X,\ P\,(Var\ x)\\ \forall f : F, \forall ss : (list\ term),\ (\forall s : term,\ s \in ss\ \to\ (P\ s))\ \to\ (P\ f(ss))\end{array}}{\forall s\ :\ term,\ (P\ s)} \tag{6}$$

This principle is an immediate consequence of the following lemma:

Lemma 13 *Let P be a predicate on term. Under the two hypotheses*

(i) $\forall x\ :\ X,\ P\,(Var\ x)$

(ii) $\forall f : F, \forall ss : (list\ term),\ (\forall s : term,\ s \in ss\ \to\ (P\ s))\ \to\ (P\ f(ss))$

one can prove that $\forall n\ :\ nat, \forall s\ :\ term, |s|\ =\ n\ \to\ (P\ s)$ where $|s|$ denotes the size of term s, that is the number of functional symbols in s.

Proof Following principle (4) for the strict order on the natural numbers, we proceed by well-founded induction on the size n of term s. If s is a variable, one applies hypothesis (i). If s is of the form $s = f(ss)$, the result follows from hypothesis (ii) and from the fact that the size of all the immediate subterms of s is less than n. □

4.2 Definition of MPO

The Multiset Recursive Ordering MPO (denoted here by $<_{MPO}$) is a relation on terms defined inductively by the 3 rules below:

$$\frac{g <_F f \quad \forall i \in \{1, \ldots, m\},\, t_i <_{MPO}\ f(s_1, \ldots, s_n)}{g(t_1, \ldots, t_m)\ <_{MPO}\ f(s_1, \ldots, s_n)} \qquad (MPO_1)$$

$$\frac{\{\!\{t_1, \ldots, t_m\}\!\}\ <_{mul,<_{MPO}}\ \{\!\{s_1, \ldots, s_n\}\!\}}{f(t_1, \ldots, t_m)\ <_{MPO}\ f(s_1, \ldots, s_n)} \qquad (MPO_2)$$

$$\frac{\exists i \in \{1, \ldots, n\},\, t \leqslant_{MPO}\ s_i}{t\ <_{MPO}\ f(s_1, \ldots, s_n)} \qquad (MPO_3)$$

Let us point out that the premise of rule (MPO$_2$) is recursive, since the relation $<_{mul,<_{MPO}}$ on the multisets of terms depends on the relation $<_{MPO}$ on terms. In the sequel, we will use a simplified notation $<_{mul}$ instead of $<_{mul,<_{MPO}}$. Moreover we define $\leq_{MPO} := \lambda s, t\ : term,\ s <_{MPO} t \vee s = t$.

4.3 Variables Behavior in MPO

The section is dedicated to some results related on the behavior of variables with respect to the relation $<_{MPO}$.

Lemma 14 *Variables are minimal terms for the relation* $<_{MPO}$.

Proof This is immediate from the definition of $<_{MPO}$, since no rule makes it possible to derive $s\ <_{MPO}\ x$, where s is a term and x is a variable. □

Lemma 15 *For all terms s and all variables x, if $x <_{MPO} s$ then $x \in Vars(s)$.*

Proof By induction on s. □

Lemma 16 *For all terms s and all variables x, if $x \in Vars(s)$ and $x \neq s$, then $x <_{MPO} s$.*

Proof By induction on s. □

Lemma 17 *Let s and t be two terms. If $t \leq_{MPO}\ s$ then $Vars(t) \subset Vars(s)$.*

Proof The case where $s = t$ is trivial. We have thus to establish that $\forall t : term, (P\ t)$ where:

$$P := \lambda t : term. \forall s : term,\ t\ <_{MPO}\ s\ \rightarrow\ Vars(t) \subset Vars(s) \qquad .$$

We proceed by induction on term t, following principle (6) in section 4.1.

- **Base Case** Let us prove $(P\ x)$ for any variable x. Let s be a term and let us assume that $x <_{MPO} s$. By lemma 15, x is a variable of s and then the result is immediate.
- **Induction Step** Let g be a functional symbol and ts a list of terms. Under the induction hypothesis

  HInd1: $\forall t\ : term,\ t \in ts\ \rightarrow\ (P\ t)$

  we have to prove $(P\ g(ts))$, that is $\forall s : term,\ (Q\ s)$ where:

  $Q := \lambda s : term. g(ts) <_{MPO}\ s \rightarrow Vars(g(ts)) \subset Vars(s)$.

  By induction on term s, we have now two cases to consider:

- **Base Case** Let us prove $(Q\ x)$ for any variable x. Let us assume that $g(ts) <_{MPO} x$. This is impossible from lemma (14). Therefore, the goal is proved by contradiction.
- **Induction Step** Let f be a functional symbol and ss a list of terms. We have to establish that $(Q\ f(ss))$ holds, under the induction hypothesis:

  HInd2: $\forall s \in ss,\ (Q\ s)$.

  Let us assume $g(ts) <_{MPO} f(ss)$. In this case, the proof is done by cases on the definition of the relation $<_{MPO}$.

  * From (MPO$_1$), we have **H**: $\forall t \in ts, t <_{MPO} f(ss)$. Let $x \in Vars(g(ts))$. Necessarily, there exists an element t of list ts such that $x \in Vars(t)$. But, from **HInd1** we know that $(P\ t)$ holds and from **H** we can deduce that $Vars(t) \subset Vars(f(ss))$. Therefore, $x \in Vars(f(ss))$
  * From (MPO$_2$), we have $ts \ll_{>_{MPO}} ss$. As in the previous case, a variable x in $Vars(g(ts))$ is in $Vars(t)$ for some t in ts. But, from lemma 12, there exists s in ss such that $t \leqslant_{mpo} s$. If $s = t$, $Vars(t) = Vars(s)$. If $t <_{MPO} s$, from **Hind1** $Vars(t) \subset Vars(s)$. In both cases, we can deduce that x is in $Var(s)$, and thus in $Vars(f(ss))$.
  * From (MPO$_3$), there exists a term s in list ss such that $g(ts) \leq_{MPO} s$. From **Hind2**, $(Q\ s)$ is satisfied. Therefore, all variables of $g(ts)$ belong to $Vars(s)$ and thus to $Vars(f(ss))$. □

4.4 Transitivity

The transitivity of the relation $<_{MPO}$ is proved by three nested inductions on terms following principle (6) in section 4.1. It requires lemma 17 above.

Lemma 18 *For all terms u, t, s, if $u <_{MPO} t$ and $t <_{MPO} s$ then $u <_{MPO} s$*

Proof The proof proceeds by inductions on terms u, t, and s successively. First, we have to establish that $\forall u : term,\ (P\ u)$ where:

$$P := \lambda u : term. \forall t : term,\ \forall s : term,\ u <_{MPO} t \wedge t <_{MPO} s \rightarrow u <_{MPO} s \qquad .$$

- **Base Case** Term u is a variable x. From lemma 15, x is in $Vars(t)$ and from lemma 17 below, $Vars(t) \subset Vars(s)$. Therefore, x is a variable of term s. Moreover s is not a variable since s is not minimal. Thus, from lemma 16, $x <_{MPO} s$.
- **Induction Step** Let h be a functional symbol and us a list of terms. We have to prove $(P\ h(us))$ under the induction hypothesis

  HInd1 : $\forall u : term,\ u \in us \rightarrow (P\ u)$.

  In fact, we have to establish that $\forall t : term,\ (Q\ t)$ where :

  $Q := \lambda t : term,\ \forall s : term,\ h(us) <_{MPO} t \wedge t <_{MPO} s \rightarrow h(us) <_{MPO} s$.

  - **Base Case** Term t is a variable. This is impossible since variables are minimal elements.
  - **Induction Step** Let g be a functional symbol and ts be a list of terms we have to prove $(Q\ g(ts))$ under the induction hypothesis

    HInd2: $\forall t : term,\ t \in ts \rightarrow (Q\ t)$.

    The goal is of the form $\forall s : term,\ (R\ s)$ where:

$R := \lambda s : term, h(us) <_{MPO} g(ts) \wedge g(ts) <_{MPO} s \rightarrow h(us) <_{MPO} s.$

- ∗ **Base Case** Term s is a variable. This is impossible since variables are minimal elements.
- ∗ **Induction Step** Let f be a functional symbol and ss be a list of terms we have to prove $(R\ f(ss))$ under the induction hypothesis

  HInd3: $\forall s : term,\ s \in ss \ \rightarrow\ (R\ s)$.

  By the definition of R, we have to prove that
  G: $h(us) <_{MPO} f(ss)$
  under the two hypotheses
  H1: $h(us) <_{MPO} g(ts)$
  H2: $g(ts) <_{MPO} f(ss)$.

  Each of these hypotheses leads to consider three cases. Thus, we have to examine nine cases. We only detail some of them that illustrate the need of various lemmas introduced previously. The others are routine.

  Case 1 Let us assume for example that **H1** follows from (MPO_1) and **H2** from (MPO_2). We have :
  (i) $h <_F g$
  (ii)$\forall u : term,\ u \in us \ \rightarrow\ u <_{MPO} g(ts)$
  (iii) $g = f$
  From (i) and (iii), $h <_F f$. Let be u any element of us. Let us prove that $u <_{MPO} f(ss)$. This comes from (ii), **H2**, and **HInd1**. The goal is proved by applying (MPO_1).

  Case 2 If **H1** and **H2** come from (MPO_2), we have $h = g = f$ and $us \ll_{>_{MPO}} ts \ll_{>_{MPO}} ss$. We conclude that $us \ll_{>_{MPO}} ss$ by applying lemma 6 in section 3.3 and hypothesis **Hind1**.

  Case 3 If **H1** comes from (MPO_3) and **H2** from (MPO_2), we have:
  (i)$\exists t : term,\ t \in ts \wedge h(us) \leqslant_{MPO} t$
  (ii) $g = f$
  (iii) $ts \ll_{>_{MPO}} ss$
  From lemma 12 and (iii), there exists s in ss such that $t \leqslant_{MPO} s$. If $t = s$, from (i) it results that $h(us) \leqslant_{MPO} s$. If $t <_{MPO} s$, from **Hind2** and (i) we deduce $h(us) <_{MPO} s$. Therefore, in both cases, $h(us) \leqslant_{MPO} f(ss)$ from (MPO_3).

  Let us point out that the transitivity of the relation $<_F$ is required when both **H1** and **H2** come from (MPO_1).

4.5 Well-Foundedness of the Multiset Path Ordering

We have now at our disposal all the tools instrumental for proving the well-foundedness of MPO.

Theorem 19 *Relation $<_{MPO}$ is well-founded.*

Proof Let s be a term, let us prove that s is accessible for $<_{MPO}$. We proceed by induction on s (principle 6).

- **Base Case** If s is a variable, from lemma 14 s is a minimal element, and thus it is accessible.

- **Induction Step** Let f be a functional symbol and ss a list of terms. We have to prove $(acc_{<_{MPO}}\ f(ss))$ under the induction hypothesis:

  HInd1: $(accs\ ss)$

  where $accs\ :=\ \lambda ss:\ (list\ term).\forall s: term, s \in ss \rightarrow (acc_{<_{MPO}}\ s)$.

  This amounts to proving that $\forall f: F,\ (P\ f)$ where predicate P is defined by:

  $P\ :=\ \lambda f: F.\forall ss:\ (list\ term),\ (accs\ ss)\ \rightarrow (acc_{<_{MPO}}\ f(ss))$.

  Let f be a functional symbol. As $<_F$ is supposed to be well-founded, f is accessible for this relation and then, using induction principle 2, we are led to prove $(P\ \ f)$ under the induction hypothesis

  Hind2: $\forall g: F,\ g <_F f\ \rightarrow\ (P\ g)$.

  The goal can be written $(\forall ss:\ (list\ term))\ (Q\ ss)$ where predicate Q is defined by

  $Q\ :=\ \lambda ss:\ (list\ term).\,(accs\ ss)\ \rightarrow (acc_{<_{MPO}}\ f(ss))$

  Let ss be a list of terms such that $(accs\ \ ss)$. From lemma 10 in section 3.3, this implies that ss is accessible for the relation $\ll_{<_{MPO}}$. Consequently, we have to prove that ss satisfies Q under the induction hypothesis

  HInd3: $\forall ts:\ (list\ term),\ ts\ \ll_{<_{MPO}}\ ss\ \rightarrow\ (Q\ ts)$.

  By the definition of predicate acc (rule 1), proving the goal $(Q\ \ ss)$ amounts to proving the proposition $(accs\ ss) \rightarrow \forall t: term, (R\ t)$ where R is defined by:

  $R\ :=\ \lambda t: term.\, t\ <_{MPO}\ f(ss)\ \rightarrow\ (acc_{<_{MPO}}\ t)$

  So, at this point, we have to prove $(R\ \ t)$ under the hypothesis **Hind1**. Let us do an induction on term t.

  - **Base Case** If t is a variable, from lemma 14 s is a minimal element, and thus it is accessible.
  - **Induction Step** Let g be a functional symbol and ts a list of terms. Let us prove $(R\ g(ts))$ under the induction hypothesis:

    HInd4 : $\forall t: term,\ t \in ts, \rightarrow\ (R\ t)$.

    By the definition of R, we have to establish that $(acc_{<_{MPO}}\ g(ts))$ under the hypothesis **H**: $g(ts)\ <_{MPO}\ f(ss)$. This assumption leads us to consider three cases, following the rule (MPO$_i$) from which the inequality is derived.

    Case MPO$_1$ We have: (i) $g\ <_F\ f$
    (ii) $\forall t: term,\ t \in ts \rightarrow\ t <_{MPO} f(ss)$

    From (i) and hypothesis **Hind2**, g satisfies predicate P. Thus, to demonstrate the accessibility of $g(ts)$, it is sufficient to prove $(accs\ ts)$. But all elements t of ts are less than $f(ss)$ by (ii) and thus are accessible from **HInd4**.

    Case MPO$_2$ The hypotheses are: (i) $f\ =\ g$
    (ii) $ts\ \ll_{>_{MPO}}\ ss$

From (i), the goal is now $(acc_{<_{MPO}}\ f(ts))$. From (ii) and **HInd3** we deduce that ts satisfies Q. Thus, proving the goal amounts to show that all terms t in ts are accessible. But from **HInd4**, t is accessible as soon as it is less than $f(ss)$. But $t <_{MPO} f(ts)$ from (MPO$_3$) and $f(ts) <_{MPO} f(ss)$ by **H**, thus by transitivity (lemma 18), $t <_{MPO} f(ss)$.

Case MPO$_3$ In this case, $g(ts)$ is less or equal than an element s of ss. Since by **HInd1** s is accessible, so is $g(ts)$. □

5 Related Work and Conclusion

The proof of the well-foundedness of RPO given in [Der82], relies on the fact that all simplification orders are well-founded since they contain the homeomorphic embedding that is a well partial order (and thus well-founded) from Kruskal's theorem. However, the proof of Kruskal's theorem is not constructive and only applies when the signature is finite.

In [Les82], Lescanne introduces a decomposition order (DO) on the terms, that he proves to be equivalent to MPO. Then, he establishes the well-foundedness of DO assuming that the precedence relation on the functional symbols is total and well-founded. His proof is elementary although not really constructive, but it seems that, with some efforts, it could be transformed into a constructive version, more intricate than ours. Moreover, Zorn's Lemma is required when the signature is infinite and the precedence non total, to embed it in a total one. However, this approach is interesting since it does not require the transitivity, and it provides an efficient algorithm for comparing two terms.

Ferreira and Zantema in [FZ95] demonstrate several theorems related to the well-foundedness of first order term orderings. Their results are quite general and even complete with respect to the termination of the term rewriting systems in the case of finite signatures. They can be applied straightforwardly to RPO. Although their proofs do not rely on Kruskal's theorem, they are not constructive.

In [JR99][JR03] Jouannaud and Rubio propose a constructive proof of termination of higher-order of recursive path ordering (horpo) by the Tait-Girard technique [GLT88] whose specialization to the case of first order terms leads to a proof of the well-foundedness of RPO by structural induction on terms as pointed out in [van01]. Our Coq proof relies on a simplification of this specialization to MPO, in the sense that it does not require the auxiliary lexicographic order on triples they use.

In [GL01], Goubault-Larrecq establishes a theorem the proof of which has been carried out in the Coq proof assistant. The result is general since it does not depend on the term structure, and therefore it applies to other algebras. The proof of the theorem is elementary. However, proving that it generalizes Ferreira and Zantema's results involves a non constructive step. Moreover, applying this theorem to MPO, and in particular, proving that hypothesis (iv) is satisfied is not simpler than our direct proof. Also, the definition of MPO has to be modified. The condition $\forall i \in \{1, \ldots, m\}, t_i <_{MPO}\ f(s_1, \ldots, s_n)$ must be added as a premise to the rule MPO_2 (see section 4.2), and that is cumbersome. An additional Coq proof that this condition is useless should be achieved.

Dawson and Goré [DG04] prove a general theorem for establishing the well-foundedness of relations closed under context. This theorem has been machine-checked in Isabelle. Again, proving that the hypotheses of the theorem are satisfied may be difficult and requires in particular to find out an appropriate auxiliary relation to be proved well-founded (that may be non trivial). The authors apply it to various examples including LPO. The proof obtained in this last case seems reasonably easy and it would be interesting to compare this approach for MPO with a direct one as ours.

Let us also mention the work of Leclerc [Lec95] who carries out in Coq a termination proof of term rewriting systems with MPO. However, the proof is achieved without using the well-foundedness of MPO, which is not established, but rather an embedding of the rewrite relations into some well-founded ordering based on the Grzegorczyk hierarchy of number theoretic functions.

We have designed a direct proof of the well-foundedness of MPO in the CIC. This proof is particularly short (30 lines). It only requires elementary preliminary results, and applies to terms on a (possibly infinite) signature of functional symbols with variable arity, including variables. It also applies when functional symbols have a fixed arity (*algebraic* terms). Indeed, Blanqui has integrated in CoLoR [CoL] a library that includes a conversion from algebraic terms to varyadic ones, that is proved to be termination-preserving. This work is a first step to be extended to the cases of LPO and RPO with status.

Acknowledgements The authors wish to thank Frédéric Blanqui for his collaboration, and Pierre Lescanne for having read and commented carefully this paper.

References

[BN98] Franz Baader and Tobias Niptow. *Term Rewriting and All That.* Cambridge University Press, New York, 1998.

[CoL] CoLoR: a Coq Library on Rewriting and Termination. http://color.loria.fr.

[Der82] Nachum Dershowitz. Orderings for Term Rewriting Systems. *Theoretical Computer Science*, 3(17):279–301, 1982.

[DG04] E.Jeremy Dawson and Rajeev Goré. A General Theorem on Termination of Rewriting. In *Computer Science Logic, CSL'04*, number 3210 in LNCS, pages 100–114. Springer-Verlag, 2004.

[FZ95] Maria.C.F. Ferreira and Hans Zantema. Well-foundedness of Term Orderings. In *4th International Workshop on Conditional Term Rewriting Systems (CTRS'94)*, number 968 in LNCS, pages 106–123. Springer-Verlag, 1995.

[GL01] Jean Goubault-Larrecq. Well-Founded Recursive Relations. In *15th Worshop on Computer Science Logic (CSL'01), Paris*, volume 2142 of *LNCS*, pages 484–497. Springer-Verlag, 2001.

[GLT88] Jean-Yves Girard, Yves Lafont, and Paul Taylor. *Proofs and Types.* Cambridge Tracts in Theoritical Computer, Science 7, 1988.

[HL78] Gérard Huet and Dallas Lankford. On the uniform halting problem for term rewriting systems. Technical Report 283, IRIA, 1978.

[JR99] Jean-Pierre Jouannaud and Albert Rubio. The Higher-Order Recursive Path Ordering. In *Proceedings of the 14th annual IEEE Symposium on Logic in Computer Science (LICS'99)*, pages 402–411, Trento, Italy, 1999.

[JR03] Jean-Pierre Jouannaud and Albert Rubio. Higher-Order Recursive Path Orderings 'à la carte'. Technical report, http://www.lix.polytechnique.fr/Labo/Jean-Pierre.Jouannaud/biblio.html, 2003.

[Kop04] Adam Koprowski. Well-foundedness of the Higher-Order Recursive Path Ordering in Coq. Master thesis, Free University of Amsterdam (The Netherlands) and Warsaw University (Poland), 2004.

[Lec95] François Leclerc. Termination Proof of Term Rewriting System with the Multiset Path Ordering. A Complete Development in the System Coq. In *TLCA*, pages 312–327, 1995.

[Les82] Pierre Lescanne. Some Properties of Decomposition Ordering, a Simplification Ordering to Prove Termination of Rewriting Systems. *R.A.I.R.O. Theoretical Informatics*, 14(4):331–347, 1982.

[Nip98] Tobias Nipkow. An Inductive Proof of the Well-foundedness of the Multiset Order. Due to Wilfried Buchholz. Technical report, http://www4.informatik.tu-muenchen.de/˜nipkow/misc/index.html, 1998.

[Tea04] The Coq Development Team. The Coq Proof Assistant Reference Manual – Version V8.0. Technical report, LogiCal Project-INRIA, 2004.

[The] The Coq Proof Assistant. http://coq.inria.fr.

[van01] Femke van Raamsdonk. On termination of higher-order rewriting. In *Proceedings of the 12th International Conference on Rewriting Techniques and Applications (RTA'01)*, pages 261–275, Utrecht, The Netherlands, 2001.