Associative-Commutative Reduction Orderings via Head-Preserving Interpretations*

Claude Marché
LIFAC - E.N.S. de Cachan
61, Av. du Président Wilson
94235 Cachan cedex
France
E-mail: `marche@lifac.ens-cachan.fr`
Phone: +33 1 47 40 23 75
Fax: +33 1 47 40 24 64

February 2, 1995

Abstract

We introduce a generic definition of reduction orderings on term algebras containing associative-commutative (hereafter denoted AC) operators. These orderings are *compatible* with the AC theory hence makes them suitable for use in deduction systems where AC operators are built-in. Furthermore, they have the nice property of being *total* on AC classes of ground terms, a required property for example to avoid failure in AC-completion, or to insure completeness of ordered strategies in first-order theorem proving with built-in AC operators. We show that the two definitions already known of such total and AC-compatible orderings [24, 25] are actually instances of our definition. Finally, we find new such orderings which have more properties, first an ordering based on an integer polynomial interpretation, answering positively to a question left open by Narendran and Rusinowitch, and second an ordering which allow to orient the distributivity axiom in the usual way, answering positively to a question of the RTA'93 open problems list [15].

1 Introduction

Orderings over term algebras have a very important role in automated deduction since they are the basis for ordered strategies: rewriting (ordered strategy of application of identities), where orderings can be used to ensure termination of reduction, ordered rewriting, ordered inference rules for deduction in first-order theories, systems involving ordering constraints, etc.

These automated reasoning techniques have been extended by building-in axioms, the most important of them being axioms of associativity and commutativity, and for that purpose, AC-compatible orderings are needed. Furthermore, in some cases one needs a *total* ordering: this is required to avoid failure in AC-ground completion [20, 24], this is also required to prove completeness of ordered strategies in first-order theorem proving involving

*This work is partly supported by the "GDR Programmation du CNRS", the ESPRIT Working Group "CCL" and the ESPRIT Basic Research Action "TYPES".

AC operators [28,29]. Solving *ordering constraints* is also known to be easier when using total orderings [6,13], hence having simply defined total AC-orderings is certainly a good basis for use in AC-ordering constraints.

Defining a total AC-compatible reduction ordering was a very difficult problem and has been solved only very recently (in 1991) by Narendran and Rusinowitch [24]. Unfortunately their definition is only on ground terms. Even more recently, Nieuwenhuis and Rubio [25] have defined such an ordering on terms with variables, which has the additional interesting property of being based on an operator precedence — like the well-known recursive path ordering — hence being more suitable for use in practise.

Nevertheless, neither the ordering defined by Narendran and Rusinowitch, nor the one of Nieuwenhuis and Rubio are able to orient the rule of distributivity in the right way. This was mentioned as an open question in the last RTA open problems list [15]. In fact, this problem makes these orderings unadapted for use in an application we have been interested in [21,22]: for deciding the word problem in equational theories defined by two AC operators $+$ and $*$, $*$ distributing over $+$, and arbitrary many ground equations, a problem related to Gröbner bases computation [5]. This is the main motivation of this work, and we detail it in Section 2.5.

Our thesis is that in both two definitions mentioned above, there is a key argument which makes the orderings total, that is the preservation of the head symbol by interpretation: we use an interpretation function I on terms such that $I(s) = I(t)$ implies $\mathcal{H}\mathrm{ead}(s) = \mathcal{H}\mathrm{ead}(t)$. We introduce a generic definition and show that the two definitions above are actually instances of our definition.

The main results are the propositions of Section 5.1 showing that our generic definition of orderings (Definition 5.2) builds a total AC-compatible reduction ordering. We then answer positively to a question asked by Narendran and Rusinowitch [24], that is the existence of total AC orderings based on integer polynomial interpretation (Section 5.2.2). Finally, we show how to build a total AC ordering which orients distributivity in the right way (Theorem 5.9).

This paper is organized as follows: Section 2 contains all preliminary definitions; Section 3 recalls the two main families of simplification orderings, that is polynomial orderings and path orderings; Section 4 recalls the already known ways of defining AC-compatible orderings; Section 5 exposes our results about total AC-orderings.

2 Preliminaries

We recall briefly notions about orderings. For more details, see the very complete article on termination written by Dershowitz [10].

2.1 Generalities about ordering relations

A relation $\to$ on a set $\mathcal{E}$ is *Noetherian* if there are no infinite sequences of related elements: $x_0 \to x_1 \to x_2 \to \cdots$. A *multiset* on $\mathcal{E}$ is a map M from $\mathcal{E}$ to $\mathbb{N}$ such that $\{x \in \mathcal{E} | M(x) \neq 0\}$ is finite. We call $M(x)$ the *multiplicity of x in M*. We denote multisets in extension, by enumerating $M(x)$ times every x, for example we denote $\{a, b, b\}$ the multiset on $\{a, b, c\}$ given by $M(a) = 1$, $M(b) = 2$ and $M(c) = 0$. We denote $\mathcal{M}(\mathcal{E})$ the set of multisets on $\mathcal{E}$.

We call *multiset extension* of a relation $\to$ on $\mathcal{E}$ the transitive closure of the relation $\to_{mul}$ given by $\{s_1, \ldots, s_i, \ldots, s_n\} \to_{mul} \{s_1, \ldots, s_{i-1}, t_1, \ldots, t_k, s_{i+1}, \ldots, s_n\}$ if $k \in \mathbb{N}$ and $\forall j \in$

$\{1,\ldots,k\}$, $s_i \to t_j$. A fundamental property is the following due to Dershowitz and Manna in 1979 [12]: if $\to$ is Noetherian, then $\to_{mul}$ is Noetherian.

A *quasi-ordering* $\succeq$ is a reflexive ($x \succeq x$ for all x) and transitive ($x \succeq y$ and $y \succeq z$ implies $x \succeq z$) relation. If it is antisymmetric ($x \succeq y$ and $y \succeq x$ implies $x = y$), it is an ordering. A strict ordering is an irreflexive (not $x \succeq x$, for all x), antisymmetric and transitive relation. If $\succeq$ is a quasi ordering, the relation $\succ$ given by $s \succ t$ if $s \succeq t$ and not $t \succeq s$, is a strict ordering called strict ordering associated to $\succeq$. The relation $\simeq$ given by $s \simeq t$ if $s \succeq t$ and $t \succeq s$, is an equivalence relation called equivalence relation associated to $\succeq$.

Reciprocally, if $\succ$ is a strict ordering and $\simeq$ an equivalence relation compatible with $\succ$ ($s \simeq s' \succ t' \simeq t$ implies $s \succ t$), then $\simeq \cup \succ$ is a quasi ordering. Because of this condition, in the following of the paper we always define directly $\succeq$ (unlike what is done usually in the literature).

A quasi-ordering is *total* if for all x and y, either $x \succeq y$ or $y \succeq x$. A quasi-ordering is said *well-founded* if its associated strict ordering is Noetherian.

Lexicographic extension is a way of building new orderings from old ones: if $\mathcal{E}$ is equipped with quasi orderings $\succeq_1, \ldots, \succeq_n$ then we define the *lexicographic extension* $\succeq = (\succeq_1, \ldots, \succeq_n)_{lex}$ by $s \succeq t$ if and only if there exists $k \in \{1,\ldots,n\}$ such that $\forall i < k,\ s \succeq_i t$ and $s \succ_k t$, or $\forall i,\ s \simeq_i t$. If $\succeq_1, \ldots, \succeq_n$ are well-founded then $(\succeq_1, \ldots, \succeq_n)_{lex}$ is well-founded.

If $\mathcal{E}$ is equipped with a quasi-ordering $\succeq$ then the multiset extension of this relation is a quasi-ordering called *multiset ordering* on $\mathcal{M}(\mathcal{E})$ and denoted by $\succeq_{mul}$.

We call *interpretation domain* a set D equipped with a well-founded quasi-ordering.

2.2 Generalities about term algebras

We recall briefly the basic definitions about term algebras and rewriting. Our notations and definitions are consistent with those given in the survey of Dershowitz and Jouannaud [11].

We denote $\mathcal{T}(\mathcal{F},\mathcal{X})$, or $\mathcal{T}$ for short, the set of terms over a signature $\mathcal{F}$ and variables $\mathcal{X}$. We denote the arity of a symbol f by $\mathrm{arit}(f)$. The subterm of a term s at position p is denoted by $s|_p$, and $s[t]_p$ is the term obtained by putting t at position p in s. We denote substitutions by Greek letters, $s\sigma$ is the application of σ on s.

As we will see below, it is sometimes useful to allow AC operators to have more than two arguments, in that case we say they are *varyadic*. We denote $\mathcal{TV}(\mathcal{F},\mathcal{FV},\mathcal{X})$ the set of terms on fixed arity symbols $\mathcal{F}$ and varyadic symbols $\mathcal{FV}$. The operation of *flattening* transforms a term in $\mathcal{T}$ into a varyadic term by normalizing w.r.t. the rules $f(x_1,\ldots,x_i,f(y_1,\ldots,y_n),x_{i+1},\ldots,x_m) \to f(x_1,\ldots,x_i,y_1,\ldots,y_n,x_{i+1},\ldots,x_m)$ for each varyadic symbol f. We denote the flat form of a term s by $\overline{s}$.

A relation $\to$ on $\mathcal{TV}(\mathcal{F},\mathcal{FV},\mathcal{X})$ is said *monotonic* if $s \to t$ implies $f(...,s,...) \to f(...,t,...)$; and *stable by instantiation* if $s \to t$ implies $s\sigma \to t\sigma$. If both properties are true, it is said a *congruence*.

An *equation* is a pair of terms, denoted $s = t$. An equation is *valid* in an $\mathcal{F}$-algebra A if for any $\mathcal{F}$-morphism $g : \mathcal{T} \to A$ we have $g(s) = g(t)$. An equation $s = t$ is a consequence of a set of equations E if $s = t$ is valid in every algebra that validates E. The set of consequences of E, denoted $\mathcal{T}h(E)$ is the *equational theory* of E.

The *equality modulo* E, generated by a set of equations E, is the smallest congruence containing E, denoted $=_E$. Because of Birkhoff's theorem: $s = t$ is a consequence of E if and only if $s =_E t$, we may usually confuse E, $\mathcal{T}h(E)$ and $=_E$.

The main example we are concerned with is the associative-commutative theory, denoted by AC. Over a signature $\mathcal{F}$ which contains a subset $\mathcal{F}_{\mathrm{AC}}$ of binary symbols, AC is the set $\{f(x,y) = f(y,x), f(f(x,y),z) = f(x,f(y,z)) \mid f \in \mathcal{F}_{\mathrm{AC}}\}$. Usually AC operators are used in infix notation ($+$, $*$, etc.). As said before, we may use flat terms to represent AC equivalent terms by working with varyadic terms $\mathcal{TV}(\mathcal{F}, \mathcal{F}_{\mathrm{AC}}, \mathcal{X})$.

2.3 Reduction and simplification orderings

A quasi-ordering $\succeq$ on $\mathcal{TV}(\mathcal{F}, \mathcal{FV}, \mathcal{X})$ is a *reduction ordering* if $\simeq$ is a congruence, $\succ$ is a congruence, and $\succeq$ is well-founded. The following proposition is trivial, but remark we need both congruence properties of the strict ordering and the associated equivalence.

Proposition 2.1 *Lexicographic composition of reduction orderings is a reduction ordering.*

Notice that a reduction ordering can never be total on terms with variables, since making two distinct variables comparable contradicts automatically stability with instantiation and well-foundedness. For this reason, we will say that a reduction ordering is *total* whenever it is *total on ground terms*.

Classically, we consider particular reduction orderings: simplification orderings. A quasi-ordering $\succeq$ on $\mathcal{TV}(\mathcal{F}, \mathcal{FV}, \mathcal{X})$ is a *simplification ordering* if $\simeq$ is a congruence, $\succ$ is a congruence, and $\succeq$ has the subterm property: if t is a subterm of s then $s \succeq t$ (at least if s and t are ground terms). Notice that the subterm property above defined on varyadic terms is equivalent to the subterm property $f(\ldots, s, \ldots) \succeq s$ and the deletion property $f(\ldots, s, \ldots) \succeq f(\ldots, \ldots)$ of Dershowitz [10]. The main result is the following, a consequence of Kruskal's theorem:

Theorem 2.2 (Dershowitz 82) *On a finite signature, every simplification ordering is well-founded, hence is a reduction ordering.*

2.4 Compatibility of orderings with equational theories

In order to work with a built-in theory E, we need orderings to be compatible with E.

Definition 2.3 *A quasi-ordering $\succeq$ on terms is* compatible with a theory E *(or is E-*compatible*) if for all s, s', t and t' such that $s =_E s'$ and $t =_E t'$, $s \succeq t$ implies $s' \succeq t'$ and $s \succ t$ implies $s' \succ t'$. This is equivalent to say $=_E \subseteq \simeq$.*

Unfortunately, in general there are no simplification orderings compatible with a theory E (except $=_E$ itself). For example, if E contains ACI$(+) = \{x + x \to x\}$ (idempotency) and $\succeq$ is ACI-compatible, then for all terms s and t such that $s \succ t$, we have:

$$s =_{\mathrm{ACI}} s + s \succ s + t =_{\mathrm{ACI}} s + s + t \succ \cdots$$

which contradicts the well-foundedness. The same phenomenon arises when E contains $AG(+, 0, -)$ (Abelian group theory), because

$$s =_{\mathrm{AG}} s + s + (-s) \succ s + t + (-s) \cdots$$

This phenomenon originates the motivation below.

If E is not trivial, an E-compatible quasi-ordering can never be a true ordering (antisymmetry is always false), hence it is more interesting to have a weaker condition that we call *E-antisymmetry*, that is $s \succeq t$ and $t \succeq s$ implies $s =_E t$. In that case we call $\succeq$ an *E-ordering*. Hence we will call a *total E-ordering* an E-ordering total on ground terms: for every ground terms s and t, either $s \succ t$, $t \succ s$, or $s =_E t$.

2.5 The main motivation

For the rest of the paper, we introduce a fundamental example which has guided this work. This example arose in the study of decidability of the word problem in some classes of equational theories [22]: the *E-ground theories* for a fixed E, that is the class of all equational theories which can be presented by a set of rules of the form $E \cup C$ where C is a set of ground rules. The two cases we are going to consider in this paper are first when E is the Abelian group theory (AG), and second when E is the commutative rings theory (CR) (several other cases are considered in [22]). The goal was to provide a decision procedure for the word problem in such a class of theories by a completion technique, that is building a convergent set of rules equivalent to the theory. For that, we need a total E-ordering to insure that all ground equations which may appear in the completion process can be oriented as a rewrite rule. Unfortunately, as we have seen above, no such ordering exist if E contains the Abelian group theory.

The idea was to introduce a variant of the E-completion algorithm in the case when E possesses an AC-convergent system R, which needs an ordering compatible only with AC, but has to make decrease the rules of R. In the case E = AG, we will see this is rather easy (Theorem 4.8). In the case E = CR, this is much harder (Theorem 5.9) because of the distributivity law: neither Narendran and Rusinowitch ordering, nor Nieuwenhuis and Rubio ordering, orient distributivity in the right way. We will need to combine carefully two recent definitions of AC orderings: the *modified associative path ordering* of Delor and Puel [7], and any total AC-ordering defined by our generic definition (Definition 5.2).

Notice the importance of the case E = CR, because it corresponds to the computation of Gröbner bases of polynomial ideals [5], where polynomials are considered as terms over the signature $\{+, *, 0, 1, -, X_1, \ldots, X_n\}$ where $+$ and $*$ are AC.

3 Two important families of simplification orderings

There are several classes of simplification orderings known in the literature: Knuth-Bendix orderings [16, 23, 30], decomposition orderings [27], interpretations by elementary functions, etc. For our purpose, we need only the two families which are certainly the most well-known: *polynomial interpretations* and *path orderings*.

3.1 Orderings generated by polynomial interpretations

Polynomial interpretations have been first introduced by Lankford [17] for the termination of rewrite systems (they were already in the work of Manna and Ness [19] in a slightly different context). Originally, they interpret terms into the set of natural numbers. In the following we need more general interpretation domains: polynomials in integer coefficients. For using polynomial interpretation we have to restrict ourselves to non-varyadic terms.

We use as interpretation domain a set of polynomials $D = \mathbb{N}[X_j, j \in J]$ in integer coefficients, where $(X_j)_{j \in J}$ is a finite family of indeterminates, equipped with an ordering *compatible with polynomial substitution*, that is if $P > Q$ then for all $(R_j)_{j\in J}$, $P\{X_j \mapsto R_j\} > Q\{X_j \mapsto R_j\}$. The main examples of such orderings that are used in practise are built by comparing polynomials as considered as multisets of monomials, where monomials can be compared in various ways: given a precedence on indeterminates $X_1 > \cdots > X_k$, we can compare monomials for example by their exponents (lexicographically), or by their total degree before, of course many variants are possible.

In order to define orderings on terms with variables, we interpret terms as *polynomial functions* over D. We need to define an ordering on such functions that will be stable by instantiation. The simplest way is product ordering: $P > Q$ if for each monomial of Q there is a monomial of P (each time a different one) which is greater for the product ordering of the exponents and the coefficient. This ordering is stable by instantiation on the condition that interpretation goes into $D - \{0, 1\}$ (implying $x > 1$ for every variable x), a condition we will always assume.

Definition 3.1 *A* polynomial interpretation *is a family of polynomial functions ϕ_f with n variables : $D^n \to D$, for each $f \in \mathcal{F}$ of arity n, such that in each variable the degree of ϕ_f is at least one.*

A polynomial interpretation generates an interpretation I of terms as follows:

$$\begin{cases} I(f(s_1, \dots, s_n)) = \phi_f(I(s_1), \dots, I(s_n)) \\ I(x) = x \end{cases}$$

The polynomial ordering *generated by I is the relation $\succeq_I$ on $\mathcal{T}(\mathcal{F}, \mathcal{X})$ given by $s \succeq_I t$ if and only if $I(s) \geq I(t)$.*

The main result is the following proposition.

Proposition 3.2 *For all I, $\succeq_I$ is a simplification ordering.*

Proof. Let us verify each required properties:

- context-stability: if $s \succ_I t$ then for all f of arity n and for all terms $u_1, \dots, u_{i-1}$, $u_{i+1}, \dots, u_n$ we have

  $$I(f(u_1, \dots, u_{i-1}, s, u_{i+1}, \dots, u_n)) = \phi_f(I(u_1), \dots, I(u_{i-1}), I(s), I(u_{i+1}), \dots, I(u_n))$$

  and the same for t. Since ϕ_f is of degree 1 in each variable, it is increasing hence

  $$f(u_1, \dots, u_{i-1}, s, u_{i+1}, \dots, u_n) \succ_I f(u_1, \dots, u_{i-1}, t, u_{i+1}, \dots, u_n).$$

  The same holds for the quasi-ordering $\succeq_I$.

- stability by instantiation: if $s \succ_I t$ and σ is a substitution, then $I(s\sigma) = I(s)\overline{\sigma}$ considering $\overline{\sigma}$ a polynomial substitution, hence $I(s\sigma) \succ_I I(t\sigma)$. The same holds for $\succeq_I$.

- subterm property: trivial. □

Example 3.3 *Let us show termination of the following rewrite system (associativity and distributivity) [17]:*

$$\begin{cases} (x+y)+z \to x+(y+z) \\ x*(y+z) \to (x*y)+(x*z) \\ (x+y)*z \to (x*z)+(y*z) \end{cases}$$

We use the interpretation on $D = \mathbb{N}$

$$\begin{cases} \phi_+(x,y) = 2x+y+1 \\ \phi_*(x,y) = xy \end{cases}$$

For associativity rule we have

$$\begin{cases} I((x+y)+z) = 4x+2y+z+3 \\ I(x+(y+z)) = 2x+2y+z+2 \end{cases}$$

The first polynomial is greater than the second for product ordering ($4x > 2x$ et $3 > 2$). For the other rules:

$$\begin{cases} I(x*(y+z)) = 2xy+xz+x \\ I((x*y)+(x*z)) = 2xy+xz+1 \end{cases}$$

and again the first polynomial is greater than the second ($x > 1$)

3.2 Path orderings

The notion of path ordering has been introduced simultaneously by Plaisted [26] and Dershowitz [8,12] in 1978, these versions use multiset orderings. Then, the so-called lexicographic path ordering has been introduced by Kamin and Lévy in 1980 [14], and finally Dershowitz has given a more general definition in 1982 [9]: recursive path ordering with status (see also [18]). We give here a variant of this last version adapted to varyadic terms.

Definition 3.4 *A* precedence *is a quasi-ordering on $\mathcal{F} \cup \mathcal{FV}$. A* status *is an element of* $\{\text{MUL}, \text{LEX}\}$*,* MUL *being the multiset status and* LEX *the lexicographic one. A map* stat *from $\mathcal{F} \cup \mathcal{FV}$ on* $\{\text{MUL}, \text{LEX}\}$ *is admissible for a precedence $\succeq$ if:*

1. *for all f in $\mathcal{FV}$,* $\text{stat}(f) = \text{MUL}$*;*
2. *for all f and g of $\mathcal{F} \cup \mathcal{FV}$, $f \simeq g$ implies*
   (a) $\text{stat}(f) = \text{stat}(g)$
   (b) *if* $\text{stat}(f) = \text{LEX}$ *(hence $f \notin \mathcal{FV}$ by (1)), then* $\text{arit}(f) = \text{arit}(g)$*.*

Remark: we can give an even more general definition by assigning to each operator of LEX status of arity n a permutation of $\{1, \ldots, n\}$. In particular, operators with the identity permutation have the left-right lexicographic status, and operators with the "mirror" permutation $1 \to n, 2 \to n-1, \ldots, n \to 1$ have the right-left lexicographic status.

Definition 3.5 *Let $\succeq$ be a precedence on $\mathcal{F}$ and* stat *an admissible status function. We call* recursive path ordering *the relation $\succeq_{rpo}$ on $\mathcal{TV}(\mathcal{F}, \mathcal{FV}, \mathcal{X})$ defined recursively by $s \succeq_{rpo} t$ if and only if*

- $s = x \in \mathcal{X}$ *and* $t = x$ *or*
- $s = f(s_1, \ldots, s_n)$ *for an* $f \in \mathcal{F} \cup \mathcal{FV}$ *and*
  - $\exists i,\ s_i \succeq_{rpo} t$ *or*
  - $t = g(t_1, \ldots, t_m)$ *and*
    - $f \succ g$ *and* $\forall j,\ s \succ_{rpo} t_j$ *or*
    - $f \simeq g$ *(hence* $\mathrm{stat}(f) = \mathrm{stat}(g)$ *by (2a)) and*
      - $\mathrm{stat}(f) = \textsc{mul}$ *and* $\{s_1, \ldots, s_n\}(\succeq_{rpo})_{mul}\{t_1, \ldots, t_m\}$ *or*
      - $\mathrm{stat}(f) = \textsc{lex}$ *(hence* $n = m$ *by (2b)),* $\forall j,\ s \succ_{rpo} t_j$*, and* $(s_1, \ldots, s_n)(\succeq_{rpo})_{lex}(t_1, \ldots, t_n)$

Remark: in the general case where to each operator f with LEX status is associated a permutation π_f, one has to replace the last line by

$$(s_{\pi_f(1)}, \ldots, s_{\pi_f(n)})(\succeq_{rpo})_{lex}(t_{\pi_g(1)}, \ldots, t_{\pi_g(n)}).$$

Proposition 3.6 (Dershowitz 1982) *If the precedence is well-founded (in particular if the signature is finite),* $\succeq_{rpo}$ *is a simplification ordering. If the precedence is total then* $\succeq_{rpo}$ *is total.*

4 AC-compatible orderings

4.1 AC orderings generated by polynomial interpretations

A first class of AC-compatible orderings can be defined by polynomial interpretations using polynomials of the appropriate form. Since polynomial interpretations are only defined on non-varyadic terms, it is not possible to flatten terms before comparing them. We work then on non-flat terms, and we have a condition on the form of polynomial to insure the AC-compatibility.

Definition 4.1 *Let* $+$ *be an AC symbol. We say that* ϕ_+ *is an AC polynomial if* $\phi_+(\phi_+(x, y), z) = \phi_+(x, \phi_+(y, z))$ *and* $\phi_+(x, y) = \phi_+(y, x)$*.*

Proposition 4.2 *If* ϕ_f *is an AC polynomial for all AC symbols* f*, then the generated polynomial ordering is AC-compatible.*

The following characterization is due to Ben Cherifa and Lescanne [4].

Proposition 4.3 *A polynomial* ϕ_+ *is AC if and only if it is of the form* $\phi_+(x, y) = axy + b(x + y) + c$ *such that* $b^2 = b + ac$*.*

Proof. If $P(X, Y) = \phi_+(X, Y)$ is AC compatible, the condition of commutativity implies that it is symmetric in X and Y, hence $P(X, Y) = Q(XY, X + Y)$. The associativity condition implies the relation on degrees $d^\circ_X(P(P(X, Y), Z)) = d^\circ_X(P(X, P(Y, Z)))$ hence $d^\circ_X(P)^2 = d^\circ_X(P)$ hence P is at most of degree 1 in X; and the same holds for Y because it is symmetric.

P is then of the form $P(X,Y) = aXY + b(X+Y) + c$. Let's write again the associativity condition:

$$\begin{aligned} a\,[aXY + b(X+Y) + c]\,Z + b\,[aXY + b(X+Y) + c + Z] + c &= \\ aX\,[aYZ + b(Y+Z) + c] + b\,[X + aYZ + b(Y+Z) + c] + c & \end{aligned}$$

hence

$$\begin{aligned} a^2XYZ + abXZ + abYZ + baXY + b^2X + b^2Y + (ac+b)Z + bc + c &= \\ a^2XYZ + abXY + abXZ + baYZ + (ac+b)X + b^2Y + b^2Z + bc + c & \end{aligned}$$

hence by identification of coefficients $b^2 = b + ac$. The reciprocal is trivial. □

Example 4.4 *Let's show termination of the classical rewrite system on natural numbers:*

$$\begin{cases} AC(+) \\ x + 0 \rightarrow x \\ x + s(y) \rightarrow s(x+y) \end{cases}$$

We use the interpretations:

$$\begin{cases} \phi_0 = 2 \\ \phi_s(X) = X + 1 \\ \phi_+(X,Y) = XY \end{cases} .$$

The polynomial ϕ_+ satisfies the condition $b^2 = b + ac$ and we have:

$$\begin{cases} I(x+0) = 2x > x = I(x) \\ I(x + s(y)) = xy + y > xy + 1 = I(s(x+y)) \end{cases}$$

hence the system terminates modulo AC.

Example 4.5 *For the canonical system of commutative rings theory: + and $*$ AC,*

$$\begin{cases} x + 0 \rightarrow x & x * 1 \rightarrow x & x * (y+z) \rightarrow (x*y) + (x*z) \\ x + (-x) \rightarrow 0 & -(-x) \rightarrow x & x * (-y) \rightarrow -(x*y) \\ -0 \rightarrow 0 & x * 0 \rightarrow 0 & -(x+y) \rightarrow (-x) + (-y) \end{cases}$$

we use the interpretation $\phi_0 = \phi_1 = 2$, $\phi_+(x,y) = x + y + 4$, $\phi_*(x,y) = xy + 2(x+y) + 2$ and $\phi_-(x) = 2x + 3$.

As one can see on this last example, finding a suitable polynomial interpretation requires some expertise.

4.2 AC orderings based on recursive path ordering

A natural idea is to use recursive path ordering on flat terms with a multiset status for AC symbols. Unfortunately, such an ordering is no more monotonic because of flattening. A classical example is the following:

Example 4.6 *Assume you have two AC symbols* $+$ *and* $*$ *with* $* > +$. *Then for an arbitrary constant* a *we have* $a * a \succ_{rpo} a + a$, *hence by monotonicity we should have* $a * (a * a) \succ_{rpo} a*(a+a)$ *but when comparing these two terms we compare the multisets* $\{a, a, a\}$ *and* $\{a, a+a\}$, *and the second is greater!*

In fact, we have the following result:

Proposition 4.7 *If all AC symbols are minimal in the precedence, then* $\succeq_{rpo}$ *is an AC-compatible simplification ordering on flat terms.*

By Proposition 3.6, if we want a total ordering, we could not have more than one AC symbol.

Proposition 4.8 *If the signature contains only one AC symbol* $+$, *if the precedence is total such that* $+$ *is the minimal operator, then* $\succeq_{rpo}$ *is a total AC-compatible simplification ordering on flat terms. If all operators have lexicographic status except* $+$ *which has multiset status, then* $\succeq_{rpo}$ *is AC-antisymmetric, hence is a total AC-ordering.*

Let us go back to our fundamental example. The AC-convergent system for Abelian groups theory is: $+$ AC and

$$\left\{ \begin{array}{lll} x + 0 \rightarrow x & -0 \rightarrow 0 & -(x+y) \rightarrow (-x) + (-y) \\ x + (-x) \rightarrow 0 & -(-x) \rightarrow x & \end{array} \right.$$

One can easily verify that rules are decreasing w.r.t. *rpo* with precedence $- > 0 > +$. As a consequence we have obtained a solution for the first part of our main motivation.

Associative path ordering

The *associative path ordering* is an AC-compatible simplification ordering which accepts several AC symbols. The original version of this ordering has been given by Bachmair and Plaisted [3], a modified version has been given then by Bachmair and Dershowitz [1, 2] and a more elaborate version has been described by Delor and Puel [7]. We recall here this last version because only this one can be used for our fundamental example on commutative rings.

For arbitrary non constant symbols f and g, let us denote by $D_i(f, g)$ the i-th distributivity rule of f over g:

$$\begin{array}{l} f(x_1, \ldots, x_{i-1}, g(y_1, \ldots, y_k), x_{i+1}, \ldots, x_n) \rightarrow \\ \quad g(f(x_1, \ldots, x_{i-1}, y_1, x_{i+1}, \ldots, x_n), \ldots, f(x_1, \ldots, x_{i-1}, y_k, x_{i+1}, \ldots, x_n)) \end{array}$$

Let us denote $D(f, g)$ the set of rules $(D_i(f, g))_{1 \leq i \leq \mathrm{arit}(f)}$.

Let us assume given a precedence $>$ and let us denote $\mathcal{D}_>$ the set of distributivity rules $D(f, g)$ for all non constant symbols f and g such that $f > g$, and f is AC or less than an AC symbol. The definition of the associative path ordering needs the convergence of this system, which is true only under some conditions. Delor and Puel described several admissible conditions, we recall here the one we are interested in.

Lemma 4.9 (Delor & Puel 1992) *If the precedence is of the form* $\cdots > * > u_k > \cdots > u_1 > + > a$ *where* $*$ *and* $+$ *are AC,* u_i *are unary symbols and* a *is a constant, then* $\mathcal{D}_>$ *is AC-convergent.*

Proof. We give the proof here because it needs the introduction of a particular ordering which will be used again later: for proving termination of $\mathcal{D}_>$, one does only have to check that the rules decrease w.r.t. the polynomial ordering generated by the interpretation $I_{\mathcal{D}}$ given by $\phi_*(x,y) = xy$, $\phi_+(x,y) = x + y + 2$ and $\phi_{u_i}(x) = (i+1)x + 1$. □

We assume in the following that the condition above is satisfied. Let us denote $s\downarrow_>$ the normal form of a term s for system $\mathcal{D}_>$. The *modified associative path ordering* is defined by comparison of normal forms:

Definition 4.10 *$s \succeq_{mapo} t$ if and only if $\overline{s\downarrow_>} \succeq_{rpo} \overline{t\downarrow_>}$.*

Theorem 4.11 (Delor & Puel 1992) *$\succeq_{mapo}$ is an AC-simplification ordering [7].*

This ordering as defined above considers as equivalent both sides of a distributivity rule, hence can not be used as is for proving termination of the AC-convergent for rings for example. This have already been remarked for the first version of the ordering, and the solution is to compose lexicographically this ordering with another one. There have been several choices proposed for this second ordering, one being to compare the size of terms in increasing order: this is well-founded because classes of ACD-equivalent terms are finite.

In fact, we propose here a new very simple solution, avoiding this comparison of sizes in this unnatural way: one can use the ordering defined by the interpretation $I_{\mathcal{D}}$ extended to all other symbols by $\phi_a = 2$ for all constant a and $\phi_f(x_1, \ldots, x_n) = 1 + x_1 + \cdots + x_n$ for non constant symbols f.

Example 4.12 *For the termination of the AC-convergent system for commutative rings (Example 4.5), we choose precedence $* > - > + > 0$, which satisfies the condition.*

Remark again that the use of precedence-based orderings is much more easier than polynomial interpretations. Finally, remark that this ordering is total if precedence is total, but is not AC-antisymmetric: for example, $a * (b + c) + d * c$ and $a * b + (a + d) * c$ have the same distributive normal form and same interpretation w.r.t. $I_{\mathcal{D}}$.

5 Total AC-orderings

The existence of a total AC-ordering when the signature contains more than one AC symbol has been an open problem until 1991, when Narendran and Rusinowitch [24] have found a first solution, based on polynomial interpretation. Then Nieuwenhuis and Rubio in 1993 [25] have given another solution by a more simple technique because based on a recursive path ordering. What we want to show now is that the reason why both definitions induce a total AC-ordering is the same, even if they are very different definitions: these definitions are based on a *head-preserving interpretation.*

5.1 Quasi-ordering generated by a head-preserving interpretation

Definition 5.1 *A* head-preserving interpretation *is a map I from $\mathcal{T}(\mathcal{F}, \mathcal{X})$ into an interpretation domain $(D, \geq)$, such that for all terms s and t, $I(s) = I(t)$ implies $\mathcal{H}\mathrm{ead}(s) = \mathcal{H}\mathrm{ead}(t)$.*

From such an interpretation, we can build a quasi-ordering in the following way.

Definition 5.2 *The quasi-ordering generated by I is the relation $\succeq_I$ on $\mathcal{T}$ given by $s \succeq_I t$ if and only if either*

- $I(s) > I(t)$ *or*
- $I(s) = I(t)$*, let f be the common head symbol of s and t, then*
  - $f \notin \mathcal{F}_{\mathrm{AC}}$ *and* $(s_1, \ldots, s_n)(\succeq_I)_{lex}(t_1, \ldots, t_n)$ *where* $s = f(s_1, \ldots, s_n)$ *and* $t = f(t_1, \ldots, t_n)$
  - $f \in \mathcal{F}_{\mathrm{AC}}$ *and* $\{s'_1, \ldots, s'_n\}(\succeq_I)_{mul}\{t'_1, \ldots, t'_m\}$ *where* $f(s'_1, \ldots, s'_n)$ *(resp.* $f(t'_1, \ldots, t'_m)$*) is the result of flattening s (resp. t) at top.*

Proposition 5.3 *The relation $\succeq_I$ is an AC-ordering*

Proof. Reflexivity is trivial, for transitivity we prove the property

$$\text{for all } s, t \text{ and } u \text{ such that } \begin{cases} |s| \leq k \\ |t| \leq k \\ |u| \leq k \end{cases}, \begin{cases} s \succeq_I t \\ t \succeq_I u \end{cases} \Longrightarrow s \succeq_I u$$

by induction on k. The case $k = 1$ is trivial. Let us assume the property true for all $j < k$ and let us prove it for k: the only non-trivial case is the one when $I(s) = I(t) = I(u)$. By the head-preservation property, we know that s, t and u have the same head symbol f, let's say $s = f(s_1, \ldots, s_n)$, $t = f(t_1, \ldots, t_n)$ and $u = f(u_1, \ldots, u_n)$. If $f \notin \mathcal{F}_{\mathrm{AC}}$ then $(s_1, \ldots, s_n)(\succeq_I)_{lex}(t_1, \ldots, t_n)$ and $(t_1, \ldots, t_n)(\succeq_I)_{lex}(u_1, \ldots, u_n)$, hence by induction $(s_1, \ldots, s_n)(\succeq_I)_{lex}(u_1, \ldots, u_n)$. The case $f \in \mathcal{F}_{\mathrm{AC}}$ is similar with the multiset functional instead of lexicographic one. AC-antisymmetry is immediate: if both $s \succeq_I t$ and $t \succeq_I s$, then necessarily $I(s) = I(t)$, hence they have the same head, and we conclude by induction. □

Now, if we want a reduction ordering, we have to insure more properties on the interpretation I.

Proposition 5.4 *If $\geq$ is total on D, then $\succeq_I$ is total. If I is AC-compatible, that is*

$$s =_{\mathrm{AC}} t \Longrightarrow I(s) = I(t) \tag{1}$$

then $\succeq_I$ is AC-compatible. If I has the subterm property, that is

$$t \text{ strict subterm of } s \Longrightarrow I(s) > I(t) \tag{2}$$

then $\succeq_I$ has the subterm property.

Proof. Trivial. □

Proposition 5.5 *If I is monotonic, that is*

$$I(s) = I(t) \quad \Longrightarrow \quad I(f(\ldots, s, \ldots)) = I(f(\ldots, t, \ldots)) \tag{3}$$

$$I(s) > I(t) \quad \Longrightarrow \quad I(f(\ldots, s, \ldots)) > I(f(\ldots, t, \ldots)) \tag{4}$$

then $\succeq_I$ is monotonic.

Proof. Assume $s \succeq_I t$. If $I(s) > I(t)$ then we conclude easily by (4). If $I(s) = I(t)$ then by (3) $I(f(\ldots,s,\ldots)) = I(f(\ldots,t,\ldots))$, we have two cases:

- if $f \notin \mathcal{F}_{\mathrm{AC}}$, clearly we have $(\ldots,s,\ldots)(\succeq_I)_{lex}(\ldots,t,\ldots)$;
- if $f \in \mathcal{F}_{\mathrm{AC}}$, we have to take care of flattening, that is if we call g the common head symbol of s and t (the same by head-preservation property): if $f \neq g$ we conclude as in the first case, and if $f = g$ then we conclude by the property $\overline{f(\ldots,s,\ldots)} = f(\ldots,s_1,\ldots,s_n,\ldots)$. □

Proposition 5.6 *If I is stable by instantiation, that is*

$$I(s) = I(t) \implies I(s\sigma) = I(t\sigma) \tag{5}$$
$$I(s) > I(t) \implies I(s\sigma) > I(t\sigma) \tag{6}$$

then $\succeq_I$ is stable by instantiation.

Proof. We proof $s \succeq_I t \implies s\sigma \succeq_I t\sigma$ by induction on the sizes of s and t: if $s \succ_I t$ then if $I(t) > I(s)$ we conclude by (5), and if $I(s) = I(t)$ we apply induction hypothesis on subterms of s and t. The only non trivial case is when the common head symbol f of s and t is AC, and s have a variable x at depth 1 which is instantiated by a term whose head is also f. In that case, we know that $\{x,s_1,\ldots,s_n\}(\succ_I)_{mul}\{t_1,\ldots,t_m\}$ and the key argument is that by definition of multiset ordering, either $\{s_1,\ldots,s_n\}(\succeq_I)_{mul}\{t_1,\ldots,t_m\}$ or there is a t_j equal to x and $\{s_1,\ldots,s_n\}(\succ_I)_{mul}\{t_1,\ldots,t_{j-1},t_{j+1},\ldots,t_m\}$. In both cases we can conclude easily. □

5.2 Examples of AC interpretations

The first ones are polynomial interpretations: The first, introduced by Narendran and Rusinowitch in 1991, interprets terms in a ring of multivariate polynomials with integer coefficients. the second interprets terms in the set $\mathbb{N}$ of natural numbers. The third is the one of Nieuwenhuis and Rubio and interprets in multisets of terms by computation of normal forms with respect to a particular rewrite system.

5.2.1 Interpretation of Narendran and Rusinowitch

We associate to each symbol f an indeterminate X_f and we interpret on the domain of polynomials $D = \mathbb{N}[X_f, f \in \mathcal{F}]$. I is given by

- if a is a constant, then $\phi_a = X_a + 1$;
- if f is not a constant:

$$\phi_f(X_1,\ldots,X_n) = (X_f+1)\left((X_f^2+2X_f)X_1\cdots X_n + (X_f+1)(X_1+\cdots+X_n)+1\right);$$

- if x is a variable, $I(x) = x$.

The head-preservation property is of course the main result of Narendran and Rusinowitch, and uses an argument of divisibility of polynomials [24]:

Proof. Suppose that $I(s) = I(t)$ where $s = f(s_1,\ldots,s_n)$ and $t = g(t_1,\ldots,t_n)$. The cases where f or g is a constant are immediate. Let us reason by contradiction and assume $f \neq g$, then we have:

$$\begin{cases} I(s) = (X_f+1)\Big((X_f^2+2X_f)I(s_1)\cdots I(s_n) + (X_f+1)(I(s_1)+\cdots+I(s_n))+1\Big) \\ I(t) = (X_g+1)\Big((X_g^2+2X_g)I(t_1)\cdots I(t_m) + (X_g+1)(I(t_1)+\cdots+I(t_m))+1\Big) \end{cases}$$

and since $I(s) = I(t)$, X_f+1 divides $I(t)$. Since X_f+1 and X_g+1 are relatively prime, we can apply Gauss' lemma in the factorial ring $\mathbb{Z}[X_f, f \in \mathcal{F}]$ and we obtain

$$X_f+1 \mid (X_g^2+2X_g)I(t_1)\cdots I(t_m) + (X_g+1)(I(t_1)+\cdots+I(t_m))+1$$

This property will remain true if we apply a polynomial substitution. Let us apply the substitution $\sigma = \{X_g \mapsto X_f, g \in \mathcal{F} - \{f\}\}$. We obtain

$$X_f+1 \mid ((X_f^2+1)^2-1)\sigma(I(t_1)\cdots I(t_m)) + (X_f+1)\sigma((I(t_1)+\cdots+I(t_m)))+1$$

and then

$$X_f+1 \mid\ -\sigma(I(t_1))\cdots\sigma(I(t_m))+1$$

but every $\sigma(I(t_i))$ possesses a factor X_f+1 hence

$$X_f+1 \mid 1$$

which is a contradiction. □

Property (1) is true because polynomials satisfy the formula $b^2 = b + ac$, and (2), (3), (4), (5) and (6) are true because they are always true for polynomial interpretations (Proposition 3.2).

Example 5.7 *Let us compare the members of the distributivity rule $x*(y+z)$ and $(x*y)+(x*z)$. We have the leading monomials:*

$$\begin{cases} I(x*(y+z)) = (X_*+1)(X_*^2+2X_*)(X_++1)(X_+^2+2X_+)xyz+\cdots \\ I((x*y)+(x*z)) = (X_*+1)^2(X_*^2+2X_*)^2(X_++1)(X_+^2+2X_+)x^2yz+\cdots \end{cases}$$

hence this ordering does not orient distributivity in the natural way.

Notice that the whole expressions of the interpretations above are very large, and one can imagine that an implementation of this ordering could be very expensive.

5.2.2 Interpretations in natural numbers

Narendran and Rusinowitch have asked the question whether it was possible to use an interpretation over integers. Thanks to the genericity of our definition, we only have to search for an interpretation I satisfying the required property. We choose then $D = \mathbb{N}$, and we try to use a polynomial interpretation of the form

$$\phi_f(x_1,\ldots,x_n) = ax_1\cdots x_n + b(x_1+\cdots+x_n)+c$$

where $b^2 = b + ac$, with the constraint of head-preservation property. The first idea we had is to index the set of operators $\mathcal{F} = \{f_1, \ldots, f_N\}$, and choose corresponding coefficient a_i, b_i and c_i such that $I(f_i(\ldots)) \equiv i \pmod{N}$. This can be satisfied by choosing $c_i \equiv i \pmod{N}$ and $a_i \equiv b_i \equiv 0 \pmod{N}$, which leads to:

$$\begin{cases} a_i = N(N(i + Nd_i) - 1) \\ b_i = N(i + Nd_i) \\ c_i = i + Nd_i \end{cases}$$

where each d_i can be chosen arbitrarily.

This interpretation supposes finite and known *a priori* the number of operators. In practise, this can cause some problems if one wants to build the ordering incrementally. Moreover, one may want to have infinitely many different operators. To avoid this problem, we can choose another method: let $\mathcal{F} = \{f_1, f_2, \ldots\}$, and let us try to have $I(f_i(\ldots)) = 2^i n$ where n is odd. This leads to the following solution:

$$\begin{cases} a_i = 2^{i+1}(2^{2i+1} - 1) \\ b_i = 2^{2i+1} \\ c_i = 2^i \end{cases} .$$

Of course, there are certainly many other solutions. About the orientation of distributivity, these orderings can not be convenient, and in fact it is easy to see that if I is any polynomial interpretation, it can not orient distributivity in the right way.

5.2.3 Interpretation of Nieuwenhuis and Rubio

Nieuwenhuis and Rubio have introduced in 1993 [25] an interpretation based on a precedence like *rpo*, instead of using polynomial interpretations. We choose $D = \mathcal{M}(\mathcal{TV}(\mathcal{F} \cup \{\perp\}, \mathcal{F}_{\mathrm{AC}}, \mathcal{X}))$, where $\perp$ is a new constant, equipped with the multiset extension of an *rpo* for a given total arbitrary precedence on the condition that $\perp$ is minimal, with LEX status for non AC symbols and MUL status for AC symbols. $I(s)$ is the multiset of normal forms of $\overline{s}$ w.r.t. the following rewrite system:

$$\begin{cases} f(u_1, \ldots, u_p, g(s_1, \ldots, s_k), v_1, \ldots, v_q) \to f(u_1, \ldots, u_p, s_i, v_1, \ldots, v_q) \\ f(u_1, \ldots, u_p, a, v_1, \ldots, v_q) \to f(u_1, \ldots, u_p, \perp, v_1, \ldots, v_q) \end{cases}$$

for each AC symbol f, each symbol g which is not a constant and such that $f > g$, $1 \leq i \leq \mathrm{arit}(g)$, and for each constant a such that $f > a$.

The head-preservation property is trivially satisfied since the rewrite system above keeps the top symbol the same. Property (1) is true thanks to flattening. Unfortunately, the other properties are not satisfied:

- if $+ > f$ where $\mathrm{arit}(f) = 1$, then for any constant a, $I(f(a)) = \{f(a)\} \succ \{a\} = I(a)$, but $I(a + f(a)) = \{a + a\} = I(a + a)$ hence (4) is not satisfied;
- it is not a simplification ordering on terms with variables: if $* > +$, then $I(y + z) = \{y + z\}$ and $I(x * (y + z)) = \{x * y, x * z\}$ are not comparable, hence the subterm property (2) is not satisfied. Equivalently, if the precedence is not total, the ordering is no more a simplification ordering (same example where x, y and z are uncomparable constants).

In their paper, Nieuwenhuis and Rubio showed first less restrictive properties, like $I(s) > I(t)$ implies $I(f(\ldots,s,\ldots)) > I(f(\ldots,t,\ldots))$ if $\mathcal{H}\mathrm{ead}(s) \geq f$, are satisfied and then showed it suffices to have a total AC-compatible simplification ordering on ground terms, and then showed that $I(s) > I(t)$ implies $I(s\sigma) > I(t\sigma)$ if σ is ground which is enough for proving termination of rewrite systems (even on terms with variables). But as noticed above, their ordering is *not* a simplification ordering on terms with variables.

Example 5.8 *Let us compare for this ordering the members of the distributivity rule $x*(y+z)$ and $(x*y)+(x*z)$, with the natural precedence $* > +$: $I(x*(y+z)) = \{x*y, x*z\}$ is less than $I((x*y)+(x*z)) = \{(x*y)+(x*z)\}$, hence this ordering does not orient distributivity in the natural way. Notice that if we choose the unnatural precedence $+ > *$, we obtain $I(x*(y+z)) = \{x*(y+z)\}$ and $I((x*y)+(x*z)) = \{x+x, y+x, x+z, y+z\}$ hence the two terms are uncomparable.*

5.3 Comparison of the definitions

Here is a very simple example which shows how simpler it is to use precedence-based ordering than polynomial interpretation: assume one wants to have a total AC ordering with which he wants to orient the rule of a rewrite system which contains the rule $x + x \to 0$.

With the precedence-based ordering of Nieuwenhuis and Rubio, you only have to choose a precedence satisfying $+ > 0$.

With our first interpretation we don't know what to do if we do not know the total number of symbols. With the second we have to use

$$\left\{ \begin{array}{l} I(x+y) = 2(18xy + 4(x+y) + 1) \\ I(0) = 3 \end{array} \right.$$

and with the ordering of Narendran and Rusinowitch, we have the interpretation

$$\left\{ \begin{array}{l} I(x+y) = (X_+ + 1)((X_+^2 + 2X_+)xy + (X_+ + 1)(x+y) + 1) \\ I(0) = X_0 + 1 \end{array} \right.$$

and it is enough to choose $X_+ > X_0$.

5.4 Definition of total AC reduction ordering which orients distributivity in the right way

We get back now to our fundamental example, where we need a total AC-ordering which orients the convergent rewrite system of commutative rings in the right way. We have seen that none of the total AC-orderings above orients the distributivity in the right way, and conversely we have an AC-ordering (Example 4.12) which orients right these rules but is not total.

To solve the problem, the idea is now quite simple: we build a lexicographic extension of these orderings.

Theorem 5.9 *Let us assume we have a signature containing exactly two AC symbols $+$ and $*$, and arbitrary many non-AC symbols with at least a unary symbol $-$ and a constant 0. Let us assume we have a total precedence $>$ such that $* > - > + > 0$ and $f > *$ for each other* *symbol f, and let $\succeq_{tot}$ be any total AC-ordering. Then the relation $(\succeq_{mapo}, \succeq_D, \succeq_{tot})$ is a total AC-ordering which orients all rules of the usual convergent system for commutative rings in the right way.*

Proof. This ordering is trivially an AC-compatible quasi-ordering since we compose lexicographically AC-compatible quasi-orderings (Proposition 2.1). It is total on ground terms because the precedence is total, and finally if two terms are equivalent with respect to this quasi-ordering, they are equivalent with respect to the last component, which is AC-antisymmetric hence these terms are AC-equal. The fact that it orients right the rules of commutative rings has been verified in Example 4.12. □

6 Conclusion

We have unified the two already known definitions of total AC-orderings, by showing that the idea of head-preserving interpretations was crucial. We have shown how to combine such ordering with associative path ordering to get an ordering orienting distributivity in the right way. These results have important consequences since they allow a uniform decision algorithm for large classes of equational theories [22].

Nevertheless, they are still some unsatisfactory points. First of all, we would like to have a head-preserving interpretation based on a precedence like the one of Nieuwenhuis and Rubio, but which satisfies all the additional properties (1) to (2), hence being truely a simplification ordering on terms with variables. We should like also to have a definition allowing partial precedences.

Second point: these orderings lead to heavy implementations: computation of interpretations for $\succeq_{apo}$ and for $\succeq_{tot}$ are computationally expensive, and can lead to large expressions to be compared then with a path ordering, which is still expensive (see Example 5.7).

Third, it appears that for the fundamental example we have introduced, it is not really necessary to have an ordering defined on all terms: it could be enough to have an ordering defined only on terms *in normal form* with respect to commutative rings' theory. As a consequence, it is not necessary to use the *mapo* anymore, since every term to be compared is already in distributive normal form! This remark lead to an interesting problem for the future: E-compatible orderings do not exist in general, but in the case when every E-congruence classes possesses a normal form, is it possible to define an ordering on the set of those normal forms, with suitable properties for use in theorem provers which build in the equational theory E?

References

[1] L. Bachmair. Associative-commutative reduction orderings. *Info Proc. Letters*, 1992.

[2] L. Bachmair and N. Dershowitz. Commutation, transformation, and termination. In J. H. Siekmann, editor, *Proc. 8th Int. Conf. on Automated Deduction, Oxford, England, LNCS 230*, pages 5–20, July 1986.

[3] L. Bachmair and D. A. Plaisted. Termination orderings for associative-commutative rewriting systems. *Journal of Symbolic Computation*, 1(4):329–349, Dec. 1985.

[4] A. Ben Cherifa and P. Lescanne. An actual implementation of a procedure that mechanically proves termination of rewriting systems based on inequalities between polynomial interpretations.

In *Proc. 8th Int. Conf. on Automated Deduction, Oxford, England, LNCS 230*, pages 42–51. Springer-Verlag, July 1986.

[5] B. Buchberger. History and basic features of the critical pair / completion procedure. *Journal of Symbolic Computation*, 3(1), Feb. 1987.

[6] H. Comon and R. Treinen. Ordering constraints on trees. In S. Tison, editor, *Proc. CAAP 94, LNCS*, Edinburgh, Apr. 1994. Springer Verlag. (Invited Lecture).

[7] C. Delor and L. Puel. Extension of the associative path ordering to a chain of associative-commutative symbols. In *Proc. 5th Rewriting Techniques and Applications, Montréal, LNCS 690*, 1993.

[8] N. Dershowitz. A note on simplification orderings. *Information Processing Letters*, 9(5):212–215, Nov. 1979.

[9] N. Dershowitz. Orderings for term rewriting systems. *Theoretical Computer Science*, 17(3):279–301, Mar. 1982.

[10] N. Dershowitz. Termination of rewriting. *Journal of Symbolic Computation*, 3(1):69–115, Feb. 1987.

[11] N. Dershowitz and J.-P. Jouannaud. Rewrite systems. In J. van Leeuwen, editor, *Handbook of Theoretical Computer Science*, volume B, pages 243–309. North-Holland, 1990.

[12] N. Dershowitz and Z. Manna. Proving termination with multiset orderings. *Commun. ACM*, 22(8):465–476, Aug. 1979.

[13] J.-P. Jouannaud and M. Okada. Satisfiability of systems of ordinal notations with the subterm property is decidable. In *Proc. 18th Int. Coll. on Automata, Languages and Programming, Madrid, LNCS 510*, 1991.

[14] S. Kamin and J.-J. Lévy. Two generalizations of the recursive path ordering. Available as a report of the department of computer science, University of Illinois at Urbana-Champaign, 1980.

[15] C. Kirchner, editor. *Proceedings Rewriting Techniques and Applications'93*, Lecture Notes in Computer Science 690, Montreal, Canada, 1993. Springer-Verlag.

[16] D. E. Knuth and P. B. Bendix. Simple word problems in universal algebras. In J. Leech, editor, *Computational Problems in Abstract Algebra*, pages 263–297. Pergamon Press, 1970.

[17] D. S. Lankford. On proving term rewriting systems are Noetherian. Technical Report MTP-3, Mathematics Department, Louisiana Tech. Univ., 1979.

[18] P. Lescanne. Uniform termination of term rewriting systems with status. In *Proc. 9th CAAP*, Cambridge, 1984. Cambridge University Press.

[19] Z. Manna and S. Ness. On the termination of markov algorithms. In *Proc. third Hawaii International Conference on Systems Sciences*, pages 789–792, Honolulu, HI, 1970.

[20] C. Marché. On ground AC-completion. In R. V. Book, editor, *Proc. 4th Rewriting Techniques and Applications, LNCS 488*, Como, Italy, Apr. 1991. Springer-Verlag.

[21] C. Marché. Réécriture modulo une théorie présentée par un système convergent et décidabilité des problèmes du mot dans certains classes de théories équationnelles. Thèse de Doctorat, Université de Paris-Sud, France, 1993.

[22] C. Marché. Normalised rewriting and normalised completion. In *Proc. 9th IEEE Symp. Logic in Computer Science*, Paris, France, July 1994.

[23] U. Martin. How to choose the weights in the Knuth-Bendix ordering. In *Proc. 2nd Rewriting Techniques and Applications, Bordeaux, LNCS 256*. Springer-Verlag, May 1987.

[24] P. Narendran and M. Rusinowitch. Any ground associative-commutative theory has a finite canonical system. In R. V. Book, editor, *Proc. 4th Rewriting Techniques and Applications, LNCS 488*, Como, Italy, Apr. 1991. Springer-Verlag.

[25] R. Nieuwenhuis and A. Rubio. A precedence-based total AC-compatible ordering. In C. Kirchner, editor, *Proc. 5th Rewriting Techniques and Applications, Montréal, LNCS 690*. Springer-Verlag, June 1993.

[26] D. A. Plaisted. A recursively defined ordering for proving termination of term rewriting systems. Unpublished report R-78-943, University of Illinois, Urbana, IL, 1978.

[27] M. Rusinowitch. Path of subterms ordering and recursive decomposition ordering revisited. *Journal of Symbolic Computation*, 3(1), 1987.

[28] M. Rusinowitch and L. Vigneron. Automated deduction with associative-commutative operators. In *Fundamentals of Artificial Intelligence, P. Jorrand Editor, LNCS 535*. Springer-Verlag, 1991.

[29] M. Rusinowitch and L. Vigneron. Associative commutative deduction. Rapport de Recherche 91-R-201, Centre de Recherche en Informatique de Nancy, 1992.

[30] J. Steinbach. AC-termination of rewrite systems: a modified Knuth-Bendix ordering. In H. Kirchner and W. Wechler, editors, *Proc. 2nd Int. Conf. on Algebraic and Logic Programming, LNCS 463*, pages 372–386, Oct. 1990.