Any ground associative-commutative theory has a finite canonical system

Paliath Narendran
Inst. of Prog. and Logics
SUNY at Albany
Albany, New York 12222
USA
dran@cs.albany.edu

Michaël Rusinowitch
INRIA & CRIN
BP 239
54506 Vandoeuvre-les-Nancy
France
rusi@loria.fr

Abstract

We show that theories presented by a set of ground equations with several associative-commutative (AC) symbols always admit a finite canonical system. This result is obtained through the construction of a reduction ordering which is AC-compatible and total on the set of congruence classes generated by the associativity and commutativity axioms. As far as we know, this is the first ordering with such properties, when several AC function symbols and free function symbols are allowed. Such an ordering is also a fundamental tool for deriving complete theorem proving strategies with built-in associative commutative unification.

1 Introduction

In this paper, we show that there is an algorithm which, given any finite set E of ground equations which contains associative commutative operation symbols, produces a reduced canonical rewriting system R equivalent to E. The method we use follows the general approach of Knuth and Bendix [KB70] of generating word problem decision algorithms for abstract algebras. It has been known for a long time that this method always succeeds with *purely ground* equations, partly due to the existence of reduction orderings which are total on ground terms. In order to deal with non-orientable axioms, like the commutativity one for instance, the completion technique of Knuth and Bendix has been extended to equivalence class term rewriting systems by [Hue80, LB77, PS81, JK86]. In this framework, Ballantyne and Lankford [BL81] designed a completion algorithm for finitely presented commutative semigroups. This is the case of one binary associative-commutative function and a finite number of constants. Termination of the algorithm was obtained using Dickson's lemma. Our result can be viewed as a generalization

of Ballantyne and Lankford's when there are several binary commutative-associative functions and also non-constant function symbols. To prove that completion always succeeds we first need to build a reduction ordering which is total on the set of classes of terms with respect to the congruence generated by the associative commutative axioms. This construction, which generalizes polynomial orderings, is outlined in Section 3. Then, in Section 4, we define a completion procedure and show that it always stops with a finite canonical system. Here, as in the semigroup case, Dickson's lemma is the decisive argument.

2 Preliminaries and notations

Here, we suppose that we are given a signature F which contains a subset F_{AC} of associative commutative operations. Our notations will be adapted to this framework. For a detailed survey on term rewriting the reader may consult [DJ90].

Let $T(F)$ be the set of terms on F (all terms to be considered in the sequel do not have variables). The congruence on $T(F)$ generated by the associative commutative equations satisfied by the symbols in F_{AC} will be written: $=_{F_{AC}}$ or $=_{AC}$ when there is no ambiguity. The extension of this relation to multisets of terms is $==_{AC}$. The root symbol of a term t is denoted by $root(t)$. We write $s[t]_p$ to indicate that a term s contains t as a subterm at position p. Positions are classically coded by sequences of integers. For instance, $t_{|p}$ indicates the subterm of t which occurs at position p.

A *rewrite rule* on $T(F)$ is an ordered pair (l, r) of terms also denoted by $l \to r$. A *rewrite system* is any set R of rewrite rules. The rewriting relation generated by a rewrite system R is the binary relation $\to_R$ defined on terms by: $s \to_R t$ iff $s =_{AC} u[l]_p$ and $t =_{AC} u[r]_p$ for some context u, position p and rule $l \to r$ in R. The inverse of $\to_R$ is denoted by $\leftarrow_R$. The transitive reflexive closure of $\to_R$ (resp. $\leftarrow_R$) is denoted by $\to_R^*$ (resp. $\leftarrow_R^*$). A term t is *irreducible* in R if there is no u such that $t \to_R u$. An irreducible term s is called a *normal form* of t in R if $t \to_R^* s$. The congruence relation generated by R and the AC axioms is denoted by: $\overset{R}{\longleftrightarrow}$. The rewrite system R is *confluent* if $s \leftarrow_R^* u \to_R^* t$ implies that there exist v, w such that $s \to_R^* v =_{AC} w \leftarrow_R^* t$. The rewrite system R is *locally confluent* if $s \leftarrow_R u \to_R t$ implies that there exist v, w such that $s \to_R^* v =_{AC} w \leftarrow_R^* t$. A rewrite system R *terminates* if $\to_R$ is noetherian. A set R of rules is *reduced* if for every rule $l \to r$ in R, l is irreducible under $\to_{R-\{l \to r\}}$ and r is irreducible under $\to_R$. A rewrite system is *canonical* if it is terminating, confluent and reduced. In a canonical system terms have unique normal forms. As a consequence the word problem is decidable in every theory which admits a canonical system.

3 A compatible ordering for AC theories

The design of orderings for proving termination of rewrite systems modulo AC has been considered a hard task. In fact, to our knowledge, very few constructions are available in the literature. Perhaps the best known among them is the *associative path ordering* scheme [BP85],

which extends the *recursive path ordering* (see also [BD86]). However, this ordering puts serious limitations on the precedence of AC-symbols. In fact two AC-symbols cannot be compared in the precedence unless they are related by a distributivity law. That explains why there is no hope to get a total ordering from the *associative path ordering*. An extension of Knuth-Bendix ordering has also been proposed by [Ste90]. However, it suffers the same kind of restriction. Recently a very interesting method has been proposed for proving termination of AC rewrite-systems in [KSZ90]. However, it seems difficult to adapt it to derive a total ordering on ground terms.

Another construction uses polynomial interpretations. We are going to elaborate on this method in order to obtain an ordering with the required properties for our purpose. Hence, let us first recall the interpretation technique. Each n-ary function symbol f is interpreted as an integer polynomial P^f with n indeterminates. The interpretation $I(t)$ of a term t is recursively defined by the rule:

$$I(f(t_1, ..., t_n)) = P^f(I(t_1), ..., I(t_n))$$

A set of rules terminates if we can choose polynomial interpretations such that for every rule $l \to r$ in the set we have $I(l) > I(r)$. Some other properties, to be detailed in this section, are also required.

For proving termination of rewrite systems modulo AC axioms, the ordering should possess the *AC-compatibility* property:

Definition 1 *An ordering $>$ on $T(F)$ is AC-compatible iff whenever we have $s > t$, $s =_{AC} s'$ and $t =_{AC} t'$ we also have $s' > t'$.*

The easiest way to ensure AC-compatibility with polynomial interpretations is to use polynomials which interpret identically the terms of the same AC-class. BenCherifa and Lescanne have pointed out the following necessary and sufficient condition for such a property:

Each polynomial $P^f(x, y)$ interpreting an AC symbol f must be of the form $axy + b(x + y) + c$ where the coefficients satisfy $b^2 = b + ac$.

In order to get an ordering which is also monotonic and total, here, we shall use another construction which may be interesting on its own. Instead of taking numerical values for the coefficients a,b and c, we shall take integer polynomials for them. We now describe the construction precisely.

Our interpretation domain will be the free commutative ring on $\{X_f; f \in F\}$, which is isomorphic to $Z[X_1, ..., X_m]$, where m is the cardinal of F. This algebra will be denoted by ZT. Hence, to each function symbol $f \in F$, is associated an indeterminate X_f.

The subset of elements of ZT whose coefficients are non-negative integers is denoted by NT. Let us define an ordering on NT. We suppose a given total precedence on the indeterminates and we suppose that the indeterminates of every monomial are sorted decreasingly

according to this order. Two monomials are compared first by their degree, and second, when these degrees are equal, by lexicographic order.

We define $>_N$ to be the multiset extension of this ordering and we shall use it to compare polynomials, by treating them as multisets of monomials. The main property of $>_N$ is that it is *well-founded.*

The set NT is the target of the interpretation I that we are going to introduce now. For every term $f(t_1, ..., t_n)$ in $T(F)$,

$$I(f(t_1, ..., t_n)) = (X_f+1)((X_f^2+2X_f)I(t_1)I(t_2)\cdots I(t_n)+(X_f+1)(I(t_1)+I(t_2)+\cdots+I(t_n))+1)$$

and for any constant a, $I(a) = X_a + 1$.

The following lemma is straightforward:

Lemma 1 *If $s =_{AC} t$ then $I(s) = I(t)$.*

Let $root(t)$ denote the root symbol of a term t. When the arity of $root(t)$ is k, the k-tuple $(t_{|1}, ..., t_{|k})$ of immediate subterms of t is denoted by $im(t)$. We also introduce for each AC-symbol f a function ρ_f which maps every term to a multiset of terms and which is defined recursively as:

$$\rho_f(g(s_1, ..., s_n)) = \begin{cases} \bigcup_{i=1}^{i=n} \rho_f(s_i) & \text{if } g = f \\ \{g(s_1, ..., s_n)\} & otherwise \end{cases}$$

The next lemma tells that we can recover the root symbol of s from its interpretation $I(s)$.

Lemma 2 *Given terms s and t, if $I(s) = I(t)$ then $root(s) = root(t)$.*

Proof: Suppose that $s = f(s_1, ..., s_n)$ and $t = g(t_1, ..., t_m)$, where f and g represent two different function symbols. Then

$$I(s) = (X_f + 1)((X_f^2 + 2X_f)(I(s_1)\cdots I(s_n)) + (X_f + 1)(I(s_1) + \cdots + I(s_n)) + 1) \quad (1)$$
$$I(t) = (X_g + 1)((X_g^2 + 2X_g)(I(t_1)\cdots I(t_m)) + (X_g + 1)(I(t_1) + \cdots + I(t_m)) + 1) \quad (2)$$

If $I(s) = I(t)$ then $(X_f + 1)$ divides $I(t)$ in ZT. However, since ZT is a factorial ring and $(X_f + 1)$ does not divide $(X_g + 1)$, we have:

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

Let $g_1, ..., g_m$ be the root symbols of $t_1, ..., t_m$ respectively. Applying the substitution $\sigma = \{X_g \leftarrow X_f, X_{g_1} \leftarrow X_f, ..., X_{g_m} \leftarrow X_f\}$ to the previous expression, we get:

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

This is equivalent to have:

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

However, since every $I(t_i)$ admits some $X_{g_k} + 1$ as a factor, we can notice that $X_f + 1$ divides $\sigma(I(t_1) \cdots I(t_m))$. This causes a contradiction.

Lemma 3 *Given terms s and t, if $I(s) = I(t)$ then every function symbol has the same number of occurrences in s and t.*

Proof: Notice that the maximal monomial in $I(s)$ is $\prod_{f \in S} X_f^3 \cdot \prod_{f \in C} X_f$ where S (resp. C) is the multiset of symbols in s whose arity is > 0 (resp. 0).

We are now in position to define the relation on $T(F)$ that we want to use as an ordering for proving termination.

Definition 2 *Let $s = f(s_1, ..., s_n)$ and $t = g(t_1, ..., t_m)$. Then $s \succ t$ iff*

- *$I(s) >_N I(t)$ or*
- *$I(s) = I(t)$ and*
  - *if $f \in AC$ then $\rho_f(s) \gg\!\!\succ \rho_f(t)$*
  - *if $f \notin AC$ then $im(s) \succ_{lex} im(t)$*

  where $\gg\!\!\succ$ is defined by: $X = \{a_1, ..., a_n\} \gg\!\!\succ Y = \{b_1, ..., b_m\}$ iff
  - *$X \neq \emptyset$ and $Y = \emptyset$ or*
  - *for some i,j: $a_i =_{AC} b_j$ and $X - \{a_i\} \gg\!\!\succ Y - \{b_j\}$ or*
  - *for some $i,j_1,...,j_k$: $a_i \succ b_{j_1}, ..., b_{j_k}$ $X - \{a_i\} \gg\!\!\succ Y - \{b_{j_1}, ..., b_{j_k}\}$.*
  - *for some $i,j_1,...,j_k$: $a_i \succ b_{j_1}, ..., b_{j_k}$ $X - \{a_i\} ==_{AC} Y - \{b_{j_1}, ..., b_{j_k}\}$.*

  and where $\succ_{lex}$ is defined by: $(a_1, ..., a_n) \succ_{lex} (b_1, ..., b_m)$ iff $\exists i, \forall j < i$ $a_j =_{AC} b_j$ and $a_i \succ b_i$.

The important properties of this relation are quoted in the next proposition:

Proposition 1 *The relation $\succ$ is*

1. *irreflexive and transitive*
2. *well-founded (there is no infinite descending chain $t_1 \succ t_2 \succ ....$)*

3. *monotonic (for any function f and terms s, t, $s_1, ..., s_n$, $s \succ t$ implies $s' = f(s_1, ..., s_{i-1}, s, s_{i+1}, ..., s_n) \succ f(s_1, ..., s_{i-1}, t, s_{i+1}, ..., s_n) = t'$).*

4. *total on the set of AC-classes (for all s,t we have either $s \succ t$ or $t \succ s$ or $s =_{AC} t$)*

5. *AC-compatible.*

Proof of 1: Irreflexivity is obtained easily by induction on the size of terms. Suppose now that $t \succ s$ and $s \succ u$. If $I(t) >_N I(s)$ and $I(s) >_N I(u)$ then $I(t) >_N I(u)$ and therefore $t \succ u$. We can draw the same conclusion if $I(t) = I(s)$ and $I(s) >_N I(u)$ or if $I(t) >_N I(s)$ and $I(s) = I(u)$. Now, if $I(t) = I(s) = I(u)$ then, due to lemma 2, s, t, and u have the same root symbol f. Suppose f is AC then $\rho_f(t) \succ\!\!\succ \rho_f(s)$ and $\rho_f(s) \succ\!\!\succ \rho_f(u)$. By induction on the sizes of terms we have $\rho_f(t) \succ\!\!\succ \rho_f(u)$ and then $t \succ u$. When f is not AC, we apply the same reasoning to $\succ_{lex}$.

Proof of 2: Suppose that there is an infinite antichain: $t_1 \succ t_2 \succ \cdots$. Since $>_N$ is well-founded, there exists k such that for all $j \geq k$, we have $I(t_j) = I(t_k)$. Hence, by lemma 3, the terms t_j for $j \geq k$ have the same number of occurrences of any function symbol. But from a finite multiset of symbols we can build only finitely many ground terms. Therefore, by the pigeon-hole principle, there exist two indices l,m ($l > m$) such that $t_l = t_m$. But, by transitivity, $t_l \succ t_m$. However, this is not compatible with irreflexivity.

Proof of 3: If $I(s) >_N I(t)$ then $I(f(..s..)) >_N I(f(..t..))$ and $f(..s..) \succ f(..t..)$ follows. Suppose now that $I(s) = I(t)$. If f is not an AC symbol, $im(s') \succ_{lex} im(t')$. If f is an AC symbol then we notice that $\rho_f(s') \succ\!\!\succ \rho_f(t')$.

Proof of 4: We use induction on the size of terms. Suppose that 4 is true for all terms of size $< k$. Then n-uples (resp. multisets) of terms each of size less than k can be ordered with $\succ_{lex}$ (resp. $\succ\!\!\succ$). Let s, t be such that (at least) one of them has size k. Suppose that neither $s \succ t$ nor $t \succ s$. Then $I(s) = I(t)$. But, if $f = root(s)$ is AC, then by the induction hypothesis, $\rho_f(s) \succ\!\!\succ \rho_f(t)$ or $\rho_f(t) \succ\!\!\succ \rho_f(s)$ or $im(s) =\!=_{AC} im(t)$. The first two cases contradict the hypothesis. Hence there only remains the third from which we derive $s =_{AC} t$. When $root(s)$ is not AC, the proof is similar.

Proof of 5: Suppose that $s' =_{AC} s = f(s_1, ..., s_n) \succ t = g(t_1, ..., t_n) =_{AC} t'$. If $I(s) >_N I(t)$, by lemma 1, we also have $I(s') >_N I(t')$. If $I(s) = I(t)$ and f is not an AC function, the corresponding components of $im(s)$ and $im(s')$ are AC-equal. Since $g = f$, the same is true for $im(t)$ and $im(t')$. Therefore, $im(s') \succ_{lex} im(t')$. If f is AC, notice that $\rho_f(s) =\!=_{AC} \rho_f(s')$ and $\rho_f(t) =\!=_{AC} \rho_f(t')$. From $\rho_f(s) =\!=_{AC} \rho_f(t)$, we derive also $\rho_f(s') =\!=_{AC} \rho_f(t')$.

4 Completion of ground systems with associative-commutative symbols

Solving the word problem by completion in theories presented by sets of ground equations is known to be always possible, even efficiently [GNP*88, Sny89]. When the signature is built solely from constants and one associative commutative operation, we get finitely presented commutative semigroups. In such structures, the word problem can still be solved by completion [BL81]. We are going to show in the following that this method generalizes to signatures which contain free function symbols and several associative commutative operations.

For convenience, we shall use the flattened representation for terms which contain AC symbols. For instance, if $f \in F_{AC}$, a flattened representation of $f(a, f(b, c))$ is $f(a, b, c)$. When $f(t_1, ..., t_n)$ is a flattened representation of t and $f \in AC$, then for all i the root of t_i differs from f. In that case, we say that the t_i are the *fundamental subterms* of t and we write $fs(t) = \{t_1, ..., t_n\}$. Note also that $\rho_f(t) = fs(t)$ when the root of t is $f \in F_{AC}$.

In the completion approach to word problems, the main operation is the generation of critical pairs, which can be used to test the confluence property of the rewriting relation. Hence, we give the suitable definition of critical pairs for our framework:

Definition 3 *Assume that $l \to r$ and $g \to d$ are two rules in R such that $l =_{AC} f(t_1, ..., t_n)$, $g =_{AC} f(s_1, ..., s_m)$, $f \in F_{AC}$ and there exist i and j such that $t_i =_{AC} s_j$. Let S be a maximal multiset of terms such that there exist $\{k_1, ..., k_v\} \subseteq \{1, ..., n\}$ and $\{l_1, ..., l_u\} \subseteq \{1, ..., n\}$ with:*

$$S \cup \{t_k; k \in \{k_1, ..., k_v\}\} =_{=AC} \{t_k; k = 1, .., n\}$$

and

$$S \cup \{s_l; l \in \{l_1, ..., l_u\}\} =_{=AC} \{s_l; l = 1, .., m\}.$$

The pair of terms $(f(s_{l_1}, ..., s_{l_u}, r), f(t_{k_1}, ..., t_{k_v}, d))$ is called a critical pair.

A critical pair (r, s) of R is *trivial* if there is a term t such that $r \to_R^* t$ and $s \to_R^* t$. The main property of reduced systems of rules is stated in the proposition:

Proposition 2 *Given a reduced system R, the relation $\to_R$ is locally confluent if and only if every critical pair (r, s) of R is trivial.*

Remark: If we compare with the general AC-completion procedure, the critical pairs we need here are between a rule and an extended rule. There are no critical pairs between rules since the left-hand side are kept reduced. Critical pairs between extended rules are covered by the other ones.

We introduce now a completion procedure which, given a ground AC theory, always yields a canonical system. We assume that the equations are oriented according to an ordering

$>$ which is well-founded, monotonic, AC-compatible and total on the set of AC congruence classes. Due to our construction of Section 3, we know that such orderings exist. We extend $>$ to rewrite rules by comparing their left-hand sides and right-hand sides in a lexicographic way. This ordering on rules is noetherian too. Our completion procedure when applied to an initial set L_0 of rules produces a sequence of sets of rules $L_0, R_0, ..., L_i, R_i, L_{i+1}, R_{i+1}, ...$ which is defined as follows:

- Given L_i, generate a reduced set R_i:
  - While possible do:
    - Choose $(r,s) \in R_i$ and simplify every rule of $R_i - \{(r,s)\}$ which is *not smaller* than (r,s) by (r,s).
    - For any simplified rule (u,v) do
      If $u =_{AC} v$ then delete (u,v) else if $v > u$ then replace (u,v) by (v,u).
  - EndWhile
- Given R_i, compute its set of non-trivial critical pairs CP_i.
- If $CP_i = \emptyset$ then halt else let $L_{i+1} = R_i \cup \{(r,s); (r,s)$ or $(s,r) \in CP_i$ and $r > s\}$.

Given a set of rules R, and an AC symbol f, we define its *set of generators* $G_f(R)$ to be the set of congruence classes modulo R of the elements of the following set:

$$\bigcup_{(l,r)\in R_f} (\rho_f(l) \cup \rho_f(r))$$

where R_f is the set of rules in R such that at least one of their sides has f as root symbol. We also define $N(R)$ to be the set of sides of rules of R whose root symbol is not AC. For instance, consider the following system R:

$$\begin{aligned} a + b &\rightarrow a * b \\ a * c &\rightarrow g(e) \\ e &\rightarrow f \end{aligned}$$

where $+$ and $*$ are AC. Then $G_+(R) = \{a, b, a * b\}$, $G_*(R) = \{a, b, c, a + b, g(e)\}$ and $N(R) = \{e, f, g(e)\}$. The elements of $G_+(R)$ and $G_*(R)$ have to be considered as *representatives* of their congruence classes modulo R.

The important fact about the set of generators is that it cannot *increase* during the completion procedure. Let us be more specific. The relation $>$ is extended to sets of terms in the following way: $A > B$ if B is obtained either by replacing some element a of A by b such that $a > b$ or by removing some element from A. The relation $>$ is still well-founded on sets. Due to the structure of our completion procedure which simplifies all occurrences of a reducible term in the same step, we notice that $N(R)$ cannot get larger with respect to $>$.

Lemma 4 *For all $i \geq 0$, $G_f(R_i) \subseteq G_f(L_i)$ and $N(R_i) \leq N(L_i)$. If (r,s) is a critical pair of R with $r > s$, then $G_f(R \cup \{(r,s)\}) = G_f(R)$ and $N(R) = N(R \cup \{(r,s)\})$.*

Theorem 1 *When applied to any finite set of rules R, the completion procedure halts with a canonical system.*

Proof: The procedure never fails to orient a new pair of terms since we are provided with an ordering which can always compare two terms which are not congruent modulo AC. Consider now the smallest rule r_1 in $\bigcup_{i\geq 0} R_i$. It belongs to some set R_{i_1}. Notice that r_1 also belongs to any R_j with $j \geq i_1$. Otherwise it would be reducible by some other rule in $\bigcup_{i\geq 0} R_i$. But this possibility is ruled out by the fact that r_1 is minimal and a rule is never reduced by a bigger rule. Consider now the rule r_2 which is minimal in $(\bigcup_{i\geq i_1} R_i) - \{r_{i_1}\}$. It belongs to some set R_{i_2}. Note that r_2 also belongs to any R_j with $j \geq i_2$. The reason is that if it were reducible, that could only be possible by r_1. However, since R_{i_2} is reduced this case is excluded. Hence, by induction, we can build a sequence $r_{i_1}, ..., r_{i_k}, ...$ such that r_{i_k} is minimal in $(\bigcup_{i\geq i_{k-1}} R_i) - \{r_{i_1}, ..., r_{i_{k-1}}\}$. The fact that R_{i_k} is reduced shows that r_{i_k} cannot be reduced later on. Consider now the set $S = \{r_{i_1}, ..., r_{i_k}, ...\}$. We have the following result:

Lemma 5 *The set of rules S is canonical.*

Sketch of proof: It is not difficult to see that S is reduced. Suppose that there is a non-trivial critical pair (u,v) between two rules of S, say r_l and r_m. Consider a minimal proof of (u,v) in $\bigcup_{i\geq 0} R_i$ with respect to the proof ordering defined in [BDH86]. If one step uses a rule which is not in S, this rule will be reduced at some stage of the algorithm. Therefore, we can build a smaller proof. Hence, we can assume that every step in the minimal proof of (u,v) is justified by a rule in S. If this proof is not a rewrite proof, then the computation of a new critical pair allows again to derive a smaller proof.

We prove now that S is finite. Assume that S is infinite. Notice that for any AC symbol f, $G_f(S) \subseteq G_f(R)$. Hence, $G_f(S)$ is finite. Also by lemma 4 we can prove that $N(S)$ is finite. Since S is infinite there are infinitely many rules $(l_i \to r_i)_{i\geq 0}$ whose left-hand sides have the same root symbol f. From the finiteness of $N(S)$ we deduce that f is necessarily AC. Since S is reduced, all the proper subterms of the left-hand sides of S are in normal form. As a consequence, we have:

Lemma 6 *If $s \in fs(l_i)$, $t \in fs(l_j)$ and $s \overset{R}{\longleftrightarrow} t$ then $s =_{AC} t$.*

We introduce the notation K_i for the multiset of congruence classes modulo $\overset{R}{\longleftrightarrow}$ of the elements of $fs(l_i)$. Since $G_f(S)$ is finite (let M be its cardinality) and since every element of K_i is also an element of $G_f(S)$ then we can associate to each K_i a vector of integers $(h_1, h_2, \ldots, h_M)$ where h_g is the number of times that the element of rank g in $G_f(S)$ occurs in K_i. We apply Dickson's lemma [Dic13] to this set of vectors. Let us recall this result:

Lemma 7 *(Dickson's Lemma) Given $n \in N$, every infinite sequence of n-dimensional vectors with nonnegative integer components must contain an infinite subsequence that is nondecreasing with respect to $\leq$ where $W \leq V$ if there exists a vector U with nonnegative components such that $V = W + U$.*

From this lemma we deduce that there exist two rules $l_k \rightarrow r_k$ and $l_j \rightarrow r_j$ such that K_k is a submultiset of K_j. By the previous lemma, this ensures the existence of a submultiset A of $fs(l_j)$ such that $A =_{=AC} fs(l_k)$. This implies that l_j can be simplified by $l_k \rightarrow r_k$, contradicting the fact that S is reduced.

We can now achieve the proof of theorem 1. Since S is finite, let m be the smallest index such that $S \subseteq R_m$. One easily sees that $S = R_j$ for all $j \geq m$. In particular $R_{m+1} = R_m$, which means that the completion procedure stops at step m. □

5 Related problems, further works and conclusion

In the previous section, it was shown that in ground associative commutative theories the word problem can always be solved by construction of a canonical system. A natural generalization of the word problem is the unifiability problem. We have investigated this problem by coding it as a reachability problem in Petri nets [PM90]. Then, from the decidability of reachability in Petri nets [May81], the decidability of unifiability in ground AC theories should follow. This idea comes from the observation that the elements of finitely presented commutative semigroups can be represented as vectors of integers. In the general case of several associative commutative symbols, the problem must be coded as a conjunction of reachability problems, each of them being related to one of the AC symbols.

For proving that we can always orient ground AC systems we have developed a generalization of the polynomial ordering. Instead of using polynomials with numerical range we rather use polynomials whose range are polynomial rings. To our knowledge, this is the first occurrence of a reduction ordering which is total on the set of congruence classes modulo AC and which is AC-compatible (for a signature which contains any number of AC symbols). Orderings with such properties are fundamental to derive refutationally complete theorem-proving strategies with built-in associative commutative unification [AH90].

Another interesting issue would be to see what happens when we replace the associativity and commutativity axioms by another well-behaved theory E. Does every ground presentation admit a canonical rewrite system modulo E? An interesting result along these lines is the construction in [KN85] of a Thue system which has a decidable word problem but which has no canonical system. Whether it is possible to extend fast ground completion techniques of [GNP*88, Sny89] to the ground AC case is also an open problem.

Acknowledgements: We thank Eric Domenjoud for reading the manuscript and Uwe Waldmann for correcting a definition.

References

[AH90] S. Anantharaman and J. Hsiang. An automated proof of the moufong identities in alternative rings. *J. Automated Reasoning*, 6:79–109, 1990.

[BD86] L. Bachmair and N. Dershowitz. Commutation, transformation and termination. In J. Siekmann, editor, *Proceedings 8th Conf. on Automated Deduction*, pages 5–20, Springer-Verlag, 1986. Lecture Notes in Computer Science, volume 230.

[BDH86] L. Bachmair, N. Dershowitz, and J. Hsiang. Orderings for equational proofs. In *Proceedings Symp. Logic in Computer Science*, pages 346–357, Boston (Massachusetts USA), 1986.

[BL81] A.M. Ballantyne and D. Lankford. New decision algorithms for finitely presented commutative semigroups. *Comp. & Maths. with Appl.*, 7:159–165, 1981.

[BL87] A. BenCherifa and P. Lescanne. Termination of rewriting systems by polynomial interpretations and its implementation. *Science of Computer Programming*, 9(2):137–160, October 1987.

[BP85] L. Bachmair and D.A. Plaisted. Termination orderings for associative-commutative rewriting systems. *Journal of Symbolic Computation*, 1:329–349, 1985.

[D87] N. Dershowitz. Termination of Rewriting. *Journal of Symbolic Computation*, 1 & 2:69-116, 1987.

[DJ90] N. Dershowitz and J.-P. Jouannaud. Rewrite systems. In Van Leuven, editor, *Handbook of Theoretical Computer Science*, North Holland, 1990.

[Dic13] L. Dickson. Finiteness of the odd perfect and primitive abundant numbers with n distinct prime factors. *Amer. J. Math.*, XXXV:413–422, 1913.

[GNP*88] J. Gallier, P. Narendran, D. Plaisted, S. Raatz, and W. Snyder. Finding canonical rewriting systems equivalent to a finite set of ground equations in polynomial time. In E. Lusk and R. Overbeek, editors, *Proceedings 9th Int. Conf. on Automated Deduction*, pages 182–196, Springer-Verlag, Lecture Notes in Computer Science, 1988.

[HsRus86] J. Hsiang, and M. Rusinowitch. A new method for establishing refutational completeness in theorem proving. Proceedings of the 8th Conference on Automated Deduction, LNCS 230 (1986) 141-152.

[Hue80] G. Huet. Confluent reductions : abstract properties and applications to term rewriting systems. *Journal of the Association for Computing Machinery*, 27(4):797–821, October 1980.

[JK86] J.-P. Jouannaud and H. Kirchner. Completion of a set of rules modulo a set of equations. *SIAM Journal of Computing*, 15(4):1155–1194, 1986.

[KN86b] D. Kapur and P. Narendran. NP-completeness of the associative-commutative unification and related problems. Unpublished Manuscript, Computer Science Branch, General Electric Corporate Research and Development, Schenectady, NY, Dec. 1986.

[KN85] D. Kapur and P. Narendran. A finite Thue system with decidable word problem and without equivalent finite canonical system. *Theoretical Computer Science*, 35:337–344, 1985.

[KSZ90] D. Kapur, G. Sivakumar, and H. Zhang. A New Method for Proving Termination of AC-Rewrite Systems. To be presented at the Conference on the *Foundations of Software Technology and Theoretical Computer Science,* New Delhi, India, December 1990.

[KB70] 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, Oxford, 1970.

[Lan79] D.S. Lankford. *On Proving Term Rewriting Systems are Noetherian.* Technical Report, Louisiana Tech. University, Mathematics Dept., Ruston LA, 1979.

[LB77] D.S. Lankford and A. Ballantyne. *Decision procedures for simple equational theories with permutative axioms: complete sets of permutative reductions.* Technical Report, Univ. of Texas at Austin, Dept. of Mathematics and Computer Science, 1977.

[May81] E. W. Mayr. An algorithm for the general petri net reachability problem. In *Proceedings of STOC*, 1981.

[PM90] P. Narendran and M. Rusinowitch. Unifiability in ground AC theories. 1990. In preparation.

[PS81] G. Peterson and M. Stickel. Complete sets of reductions for some equational theories. *Journal of the Association for Computing Machinery*, 28:233–264, 1981.

[Sny89] W. Snyder. Efficient completion: an $O(nlogn)$ algorithm for generating reduced sets of ground rewrite rules equivalent to a set of ground equations E. In N. Dershowitz, editor, *Proceedings 3rd Conf. on Rewriting Techniques and Applications*, pages –, Springer-Verlag, Lecture Notes in Computer Science, 1989.

[Ste90] Steinbach, J. AC-termination of rewrite systems - A modified Knuth-Bendix ordering. Proceedings 2nd International Conference on Algebraic and Logic Programming, Nancy (France), Lecture Notes in Computer Science 463, 372-386, (1990).