On word problems in equational theories

Michaël Rusinowitch, Jieh Hsiang

INRIA

UNITÉ DE RECHERCHE
INRIA-LORRAINE

Institut National
de Recherche
en Informatique
et en Automatique

Domaine de Voluceau
Rocquencourt
B.P. 105
78153 Le Chesnay Cedex
France
Tél. (1) 39 63 55 11

Rapports de Recherche

N° 678

ON WORD PROBLEMS IN EQUATIONAL THEORIES

Michael RUSINOWITCH
Jieh HSIANG

JUIN 1987

ON WORD PROBLEMS IN EQUATIONAL THEORIES

PROBLEMES DE MOTS DANS LES THEORIES EQUATIONNELLES

PAR

MICHAEL RUSINOWITCH

ET

JIEH HSIANG

Résumé : Nous montrons comment utiliser l'algrorithme de Knuth et Bendix comme une procédure de semi-décision pour les problèmes de mots, même en présence d'équations non orientables.

Abstract : The Knuth-Bendix procedure for word problems in universal algebra is known to be very effective when it is applicable. However, the procedure will fail if it generates equations which cannot be oriented into rules (i.e, the system is not noetherian), or if it generates infinitely many rules (i.e, the system is not confluent). In 1980 Huet showed that even if the system is not confluent, the Knuth-Bendix procedure still yiels a demi-decision procedure for word problems, provided that every equation can be oriented. In this paper we show that even if there are non-orientable equations, the Knuth-Bendix procedure can still be modified into a reasonably efficient semi-decision procedure for word problems in equational theories. Thus, we have lifted the noetherian requirement in the Knuth-Bendix procedure. Several confluence results are also given in the paper together with some experiments. Our method can also be extended to more general theories. Comparison with related works is also given.

The proof of completeness, which is an interesting subject by itself, employs a new proof technique which utilizes a notion of transfinite semantic trees which is designed for proving refutational completeness of theorem proving methods in general.

On Word Problems in Equational Theories[1]

Jieh Hsiang
Department of Computer Science
SUNY at Stony Brook
Stony Brook, NY 11794
U.S.A.

Michael Rusinowitch
CRIN
B.P. 239
54506 Vandoeuvre-les-Nancy
France

First draft: November 1985
Revised: August 1986

Abstract

The Knuth-Bendix procedure for word problems in universal algebra is known to be very effective when it is applicable. However, the procedure will fail if it generates equations which cannot be oriented into rules (i.e., the system is not *noetherian*), or if it generates infinitely many rules (i.e., the system is not *confluent*). In 1980 Huet showed that even if the system is not confluent, the Knuth-Bendix procedure still yields a semi-decision procedure for word problems, provided that every equation can be oriented. In this paper we show that even if there are non-orientable equations, the Knuth-Bendix procedure can still be modified into a reasonably efficient semi-decision procedure for word problems in equational theories. Thus, we have lifted the noetherian requirement in the Knuth-Bendix procedure. Several confluence results are also given in the paper, together with some experiments. Our method can also be extended to more general theories. Comparison with related works is also given.

The proof of completeness, which is an interesting subject by itself, employs a new proof technique which utilizes a notion of transfinite semantic trees which is designed for proving refutational completeness of theorem proving methods in general.

1. Introduction

Given an equational theory E, a *term rewriting system for* E is a finite set of rewrite rules $R=\{l_i \rightarrow r_i\}_{i=1}^{n}$ such that $\{l_i = r_i\}_{i=1}^{n}$ and E are equivalent (i.e., $s=t$ is true in $\{l_i = r_i\}_{i=1}^{n}$ if and only if $s=t$ in E). A term t is *reduced* using rule $l \rightarrow r$ if a subterm s of t, which is an instance of the left hand side l, is replaced by the corresponding instance of the right hand side r. A term s is **reachable** from t if t

[1]Research supported in part by the NSF grant DCS-8401624, and the Greco de Programmation of France.

can be reduced to s after a finite number of reductions. A term is *irreducible* if no rule can be applied to it. We use t^* to denote an irreducible form of t. We call a term rewriting system **noetherian** if there is no infinite sequence of reductions from any term, and **confluent** if for any distinct terms t, r, and s, if r and s are both reachable from t, then there is another term u which is reachable from both r and s. A rewriting system satisfying these two properties is called a **canonical term rewriting system**. It is easy to see that if R is a canonical term rewriting system, then every term has a unique irreducible form with respect to R. Thus, to check if an equation $s =_E t$ is valid, all that needs be done is to reduce both s and t to their irreducible forms and see if they are identical.

Knuth and Bendix ([KnB70]) gave a necessary and sufficient condition for a noetherian term rewriting system to be confluent (and therefore canonical). They also presented a completion procedure for extending a non-canonical system to a canonical one without changing the original theory (although the method does not always terminate successfully). The most basic construct in the Knuth-Bendix procedure is the **superposition process**:

> Given two rules $g[u] \rightarrow d$ and $l \rightarrow r$, if there is a most general unifier σ such that $u\sigma = l$, then $< g[r]\sigma, d\sigma >$ is called a **critical pair** of the two rules.

A critical pair $< s, t >$ is *divergent* if the irreducible terms of s and t are not identical. The Knuth-Bendix completion procedure consists of finding divergent critical pairs and orienting them into rules, and in the meantime keep terms fully reduced with respect to the current set of rules. From now on we shall call the Knuth-Bendix completion procedure the **KB procedure**.

However, this procedure fails when it

- generates an incomparable (unorientable) critical pair, or it
- generates infinitely many rules.

The first problem is in general undecidable ([HuL78]). That is, there is no decision procedure for deciding whether there is a well-founded reduction ordering for any given set of equations. Some special cases of non-orientable equations, such as the commutative axioms, have been studied individually ([LaB77, PeS81]) by incorporating special unification algorithms into the completion procedure. This approach of incorporating special unification algorithms for non-orientable equations has been taken more systematically in [JoK84], where an extension called E-term rewriting is proposed.

A "semi-solution" for the second problem was given in [Hue81]. While proving the correctness of the Knuth-Bendix procedure, Huet showed that even if the procedure generates infinitely many rules, it still provides a semi-decision procedure for the word

problem. To be more precise, assuming that all critical pairs generated are orientable (under the same reduction ordering), and the superposition process is *fair* (no equation is left un-considered), then $s =_E t$ if and only if the KB procedure eventually generates enough rules to reduce both to the same term. Thus, Huet showed that even if infinitely many rules are generated, the KB-procedure still provides a *semi-decision* procedure for the word problem of an equational theory. This observation improves the functionality of the original KB-procedure considerably, since it demonstrates the use of a rewriting system even if it is not confluent. However, once again, Huet's algorithm does not work when a critical pair is non-orientable.

2. A Knuth-Bendix Type Procedure that Does Not Fail

In this paper we present an extension of the Knuth-Bendix procedure which removes the noetherian requirement. We show that even if there are non-orientable equations, we still have a reasonably efficient semi-decision procedure for the word problem of equational theories.

Our method is motivated from the following refutational formulation of Huet's result: Given an equational theory E and an equation $s = t$. Let $\hat{s} \neq \hat{t}$ be the skolemized inequality resulting from the negation of $s = t$. Since all variables in all equations are universally quantified, all variables in s and t are replaced by skolem constants in $\hat{s} \neq \hat{t}$ (thus, $\hat{s}$ and $\hat{t}$ are ground terms). From now on we use $\hat{s}$ for the skolemized term of s. Huet's result can be stated refutationally as follows: Given E and $s = t$. Assume the noetherian and fairness properties as stated before, then $s = t$ is a theorem of E if and only if the Knuth-Bendix procedure will eventually generate enough rules to reduce $\hat{s} \neq \hat{t}$ to some $\hat{r} \neq \hat{r}$. To paraphrase it in theorem proving terms, $E \cup \{\hat{s} \neq \hat{t}, x = x\}$ is E-unsatisfiable if and only if the Knuth-Bendix procedure will eventually generate enough rules to reduce $\hat{s} \neq \hat{t}$ to some $\hat{r} \neq \hat{r}$ which, with $x = x$, generates a contradiction.

2.1. Strong Simplification Ordering

We start with the following definition.

Let F be a (finite) set of operators, and T be the set of terms generated from F and a countably infinite set of variables. A **strong simplification ordering** $>$ on T is an ordering which satisfies the following properties:

(i) $c[t] > t$, where c and t are in T. (*subterm* property)

(ii) $s > t$ implies $c[s] > c[t]$, where s, t, and c are in T. (*monotonicity* property)

(iii) $s > t$ implies $s\sigma > t\sigma$, where s and t are in T, and σ is a substitution. (*substitution* property)

(iv) $>$ is total on the set of ground terms (the Herbrand universe).

Conditions (i) through (iii) form what is usually called simplification orderings ([Der82]), which also includes condition (iv) in [Pla78].

Theorem (Dershowitz) A strong simplification ordering is well-founded on T.

We remark that most of the commonly used orderings (e.g., the recursive path ordering [Der82], recursive decomposition ordering [JLR82], path of subterm ordering [Pla78]) are either strong simplification orderings or can be modified easily into one.

From now on, we assume that $>$ is a strong simplification ordering on the term algebra. Note that such an ordering always exists. The problem usually encountered in term rewriting is to find one which can orient all equations into rules.[2]

2.2. Extended Critical Pairs and Reductions

The basic ingredient in our method is the following:

Definition Given two equations $g[u]=d$, $l=r$, where u is a nonvariable subterm of g. if there is an mgu σ such that

(i) $u\sigma = l\sigma$,

(ii) $r\sigma \not\geq l\sigma$, and

(iii) $d\sigma \not\geq g\sigma$,

then $\langle d\sigma, g[r]\sigma \rangle$ is an **extended critical pair.**

We call the process of generating an extended critical pair the **extended superposition process.** Note that if $l=r$ and $g=d$ are orientable, then (ii) and (iii) become

[2] It is also known that there are noetherian term rewriting systems which cannot be oriented by simplification orderings ([Der82]).

(ii') $l\sigma > r\sigma$, and

(iii') $g\sigma > d\sigma$,

and the above procedure is equivalent to the superposition and critical pair definitions in the original KB-procedure.

The definition of reduction is modified accordingly:

Definition A term $s[u]$ is **reducible** by an equation $l=r$ if there is a substitution σ such that

(i) $l\sigma = u$, and

(ii) $l\sigma > r\sigma$.

We also say that $s[u]$ is **reduced** to $s[r\sigma]$ using $l=r$.

Since the ordering $>$ is well-founded, no term can be reduced indefinitely. For example, given a ground term $a*b$ and an equation $x*y=y*x$. Assume that the ordering orders $a*b > b*a$, then $a*b$ can be reduced to $b*a$ using the equation, but not from $b*a$ to $a*b$. On the other hand, this equation cannot be used to reduce the (non-ground) term $w*z$, since $w*z \not> z*w$. This modification of reductions is important, without which we cannot obtain the confluence results to be given later.

The notions of extended superposition and reduction form the foundation of our inference rules.

2.3. Inference Rules for the Unfailing KB Procedure

Before giving our procedure and the inference rules, we give an informal description of the procedure. Suppose we start from a set of equations E, a (skolemized) $\hat{s} \neq \hat{t}$, and a strong simplification ordering $>$. The goal is to prove that $E \cup \{\hat{s} \neq \hat{t}\}$ is E-unsatisfiable or, equivalently, $s=t$ is a theorem of E. Our strategy is very similar to the KB-procedure. It generates divergent extended critical pairs from two equations, orients the critical pairs into rules if possible, and tries to use this new equation to reduce the inequality. If either no divergent critical pair can be generated, or the inequality has been reduced to some $\hat{r} \neq \hat{r}$, the procedure stops. If $\hat{r} \neq \hat{r}$ is generated, then this inequality and $x=x$ generates the contradiction. Otherwise $\hat{s} \neq \hat{t}$ is consistent with E.

The above description can be separated into the following three inference rules:

Equation Generation

Find an extended critical pair $<u, v>$, reduce it using the existing equations as much as possible. If the resulting pair still diverges, orient it into a rule if possible.

Target Reduction

Reduce $\hat{s} \neq \hat{t}$ using the new equation if possible, and replace $\hat{s} \neq \hat{t}$ by the new inequality.

Final Refutation

When some $\hat{r} \neq \hat{r}$ is generated, use $\hat{r} \neq \hat{r}$ and $x = x$ to produce the contradiction.

We assume that the procedure is fair, in other words, all pairs of equations will be considered for equation generation eventually. We call this method the **unfailing Knuth-Bendix procedure** or **UKB-procedure** in short. Note that there is only one inequality in the current set at all time.

The UKB-procedure is complete for word problems in equational theories. In other words,

> **Theorem 1:** *Given E and $s = t$, then $s = t$ is a theorem of E iff the above procedure, when applied to $E \cup \{\hat{s} = \hat{t}\}$, produces* $1 = 0$.

This implies that, if $s = t$ is a theorem of E, this fact can be established by *reducing* $\hat{s} \neq \hat{t}$ using equations and rules generated from E. The proof of the theorem uses a refutational proof technique, based on transfinite semantic trees, introduced in [HsR85]. It is given in a later section of the paper.

Similar to the original Knuth-Bendix procedure, our procedure yields a canonical system when it terminates. However, if the system contains equations which cannot be oriented, then only the canonicity of the ground terms is guaranteed.

> **Theorem 2:** *If no more divergent critical pair is found, and all rules are orientable, then the resulting rewrite system is canonical. That is, all provably equal terms have the same normal form.*

> **Theorem 3:** *If no more divergent critical pair is found, then the resulting system is canonical on ground terms.*

Both theorems are easy consequences of Theorem 1. Theorem 3 means that, if no divergent critical pair can be found, and if some of the equations in the resulting set (call it R) cannot be oriented, then R only yields a unique normal form for every ground term, but not terms with variables. That is, all provably equal ground terms have the same normal form. We call such a system a **ground canonical system**. As a typical example of a ground canonical system, consider a set R with only one equation $x*y = y*x$. Clearly R has no critical pair while the term $x*y$ has no unique normal form. On the other hand, the ground term $a*b$ does have a unique normal form, which is either $a*b$ or $b*a$, depending on which term is smaller in the ordering. Also notice that we do not require the equivalent classes imposed by the non-orientable equations to be finite (such restrictions are usually imposed in term rewriting methods with special

unification algorithms, e.g. [LaB77], [JoK84]).

Although a ground canonical system does not guarantee a unique normal form for every term, it still provides a *linear* decision procedure for the word problem of the general terms via reduction. The procedure is this: Given an equation $s = t$, we take its negation, skolemize it, and obtain an inequality $\hat{s} \neq \hat{t}$ with all the variables in s and t replaced by new skolem constants. In order to maintain the well-foundedness and normal forms of the original system, we may extend the ordering by choosing the skolem constants to be larger than the existing ones. Since there is no more critical pair in R, the only applicable inference is to reduce $\hat{s} \neq \hat{t}$ to its normal form. By Theorem 1, $\hat{s}$ and $\hat{t}$ can be reduced to the same term if and only if $s = t$ in the original theory. Moreover, there is practically no search space in the reduction process since only one inequality is kept in the data base at all time. Thus, we have

> **Theorem 4:** *If no more divergent critical pair is found, then the resulting rewriting system provides a (linear) decision procedure for deciding the word problem of the given theory.*

2.4. Discussions

Before proceed further, we discuss a few features of our method and some differences between our procedure and the Knuth-Bendix-Huet procedure and its other extensions.

(1) There is no noetherian requirement in our method. That is, even if equations are not orientable, our procedure does not fail. Thus, our method provides a fully general semi-decision procedure for equational theory without any "side-effects". Similar to the Huet's version of the KB-procedure, we also do not require the system to be confluent.

(2) We require the ordering used for ordering terms to be a simplification ordering and to be total on ground terms. The KB-procedure allows any well-founded reduction ordering and is more general.

(3) When no divergent critical pair can be found and all equations can be oriented into rules (as in Theorem 2), the resulting canonical system is only guaranteed to be *left-reduced* (all left hand sides of rules are not reducible by any other rule), but may not be *inter-reduced* (i.e., all terms appeared in rules are not reducible by any other rule). For example, given two equations $\{a = b, b = c\}$, our procedure may produce a system $\{a \rightarrow b, b \rightarrow c\}$, but not $\{a \rightarrow c, b \rightarrow c\}$. This is due to the inference rules which we choose. However, this is not a serious problem, because every left-reduced, critical pair free canonical system can be transformed into an inter-reduced one without too much difficulty.

(4) One of the most important recent advances in term rewriting is the notion of E-term rewriting ([JoK84]), which utilizes special unification algorithms and has a weaker Church-Rosser property. Our procedure is different in that it does not require any special unification algorithm. One advantage with the E-term rewriting approach is that, if such an E-unification algorithm exists, sometimes the corresponding E-completion procedure (which employs the E-unification algorithm) terminates and returns a canonical system (with respect to E). Unfortunately such specialized unification algorithms are rare and difficult to find. Our method, on the other hand, is completely general since it does not reply on the existence of any special unification algorithm. As we shall see later in an example involving a permutative axiom (which cannot be oriented), our method eventually generates a ground canonical system while E-completion fails since there is no known unification algorithm for this particular axiom. A disadvantage of our method, however, is that for certain axioms our process may continue indefinitely while E-completion will terminate if special unification algorithms are used. An typical example is the AC-theory ([PeS81], [LaB77]). We believe that our method can be combined with E-term rewriting, although we have not worked out the details completely. Also, we emphasize that the major purpose of our method is to achieve a failure-proof semi-decision procedure, not for generating decision procedures.

(5) Some historical remarks: In [Lan75], Lankford described a procedure which is similar to the unfailing KB given here, although no proof was given in that paper. Similar results were also discovered by Plaisted [Pla85]. Interestingly enough, all these results, including ours, have the same restriction on orderings (simplification ordering which is total on ground terms). A weaker version (which requires a simplification ordering which is order isomorphic to ω on ground terms) was mentioned in [Pet83]. Our paper is different from the others in several ways. First of all, we give a completeness proof, which was not given in any of these papers. More importantly, the notion of extended reduction does not seem to exist in the other methods. Consequently, they could not derive the confluence results. The most important aspect is that our notion of extended critical pairs is closer to the original notion in the Knuth-Bendix method. In the other papers such as [Pet83], critical pairs may be generated from the right hand side of a rule. This would certainly increase the search space during the completion process considerably. (Peterson's method can only impose the ordering restriction on one of the two equations used in superposition, not both of them. It does not seem obvious to modify his proof to have stronger restrictions such as ours.) Recently, using another proof technique, a method similar to ours was also derived in [BDH85].

3. Extending to More General Theories

The UKB-procedure can be extended to a more general theory, which allows inequalities with free variables.

We call a theory an **extended equational theory** if it contains a (finite) set of equalities and inequalities, with all variables (implicitly) universally quantified. The differences between equational theories and extended equational theories are that the latter (1) allows more than one inequality, and (2) allows inequalities with variables. The UKB-procedure can be modified to become a semi-decision procedure by adding the following inference rule:

Extended Narrowing

Given an equality $l=r$ and an inequality $g[u]\neq d$, if there is an mgu σ such that

(i) $u\sigma=l\sigma$, and

(ii) $r\sigma \not\geq l\sigma$,

then $(g[r]\neq d)\sigma$ is **narrowed** from $g[u]\neq d$ using $l=r$.

Note that the target reduction inference rule is a special case of extended narrowing. They are identical if the inequality is ground. The **final refutation** inference rule also needs be modified to cope with variables:

Reflexive Refutation

Given an inequality $g\neq d$. If there is a unifier σ such that $g\sigma=d\sigma$, then we achieve the contradiction *NIL*.

The complete strategy for extended equational theory includes the *equation generation, reflexive refutation,* and the *extended narrowing* inference rules. We also assume that the application of inference rules to equalities and inequalities is fair. We call this strategy the **S-strategy**.

> **Theorem 5:** *The S-strategy is complete for extended equational theories. That is, given an extended equational theory T, T is E-unsatisfiable if and only if contradiction can be generated from $T\cup\{x=x\}$ using the S-strategy.*

4. Proof of Completeness

We now prove the completeness of the S-strategy. The completeness of UKB follows as a corollary.

4.1. A Completeness Proof Method based on Transfinite Semantic Trees

In this subsection we describe a proof method based on transfinite semantic trees which we use to prove the completeness of the given strategies. Since the domain we

are dealing here has only equality and its negation but not other logical connectives, we shall only introduce the concepts in the proof method which are directly related. For a more general description of the proof method, see [HsR85].

An *inference rule* is a rule for deducing a consequence from a set of formulas. A *(theorem proving) strategy* is a set of inference rules. Let *Inf* be a theorem proving strategy and S a set of clauses, $Inf(S)$ denotes the set of clauses obtained by adding to S all clauses generated by applying some rule in *Inf* to S. Let $Inf^{n+1}(S)=Inf(Inf^n(S))$ and $Inf^*(S)$ be the limit of $Inf^n(S)$ when n approaches infinity. When there is no ambiguity about *Inf*, we simply use S^* for $Inf^*(S)$.

A strategy *Inf* is *(refutationally) complete* if, given any unsatisfiable set of clauses S, *Inf* can deduce *NIL*, the empty clause. The following trivial result will serve as the basis of our development.

> **Proposition:** *Inf is (refutationally) complete if for every unsatisfiable set of clauses S, NIL (the empty clause) belongs to* S^*.

The equality predicate cannot be treated as any other predicate because it assumes the axioms of a congruence relation:

$\forall x\,(x=x)$
$\forall x,y\,(x=y)\supset(y=x)$
$\forall x,y,z\,(x=y)\wedge(y=z)\supset(x=z)$
Given any f, $(x=y)\supset f(\cdots,x,\cdots)\supset f(\cdots,y,\cdots)$,

These axioms can be satisfied in a special class of interpretations called the *E-interpretations*. Let *TERM* (resp. *GT*) be the set of terms (resp. ground terms), *ATOM* (resp. *GA*) the set of atomic formulas (resp. ground atomic formulas). An *E-interpretation* is a function I with domain $D(I)$ included in *GA* and range $\{true, false\}$ satisfying :

$a=a$ in $D(I)$ implies $I(a=a)=true$,
$a=b$, $B[a]$, $B[b]$ in $D(I)$ and $I(a=b)=T$ implies $I(B[a])=I(B[b])$.

Note that we consider $a=b$ and $b=a$ as the same atom.

We have the following well-known result (see, e.g., [ChL73]):

> **Theorem:** *Call the set of equational axioms K, and let S be a set of clauses. Then* $S\cup K$ *is unsatisfiable (we say that S is E-unsatisfiable) iff S is not valid in any E-interpretation on GA.*

This motivates us to build semantic trees which capture the E-interpretations. For this purpose, we need *GA* to be well-ordered in such a way that every ground atom occurs before any atom it can reduce. For example, given two atoms $g(a)=a$ and

$f(g(a))=a$, if an E-interpretation evaluates $g(a)=a$ as *true*, then it can be considered as $g(a)\rightarrow a$ which can reduce $f(g(a))=a$ to $f(a)=a$. Therefore the value of $f(g(a))=a$ should be determined *after* both $f(a)=a$ and $g(a)=a$ are evaluated, since the value of the former may depend on those of the other two. The strong simplification orderings introduced before satisfy our requirement. Under such an ordering, let $s=t$ be a ground atom and assuming that $s>t$, then any atom containing s as a proper subterm will appear later in the ordering. Also, since the ordering is total on ground atoms, any two ground atoms are comparable.

4.1.1. Transfinite E-Semantic Trees

Let $>$ be a strong simplification ordering. We build an *E-semantic tree* which contains the set of E-interpretations and nothing else. This E-semantic tree is *unique* with respect to the ordering $<$ on the set GA.

Let I be an E-interpretation I and B a ground atom in GA, a *partial E-interpretation of I at B* is a partial interpretation of I which is defined on all the members of GA which are smaller than B (not including B). Given two partial E-interpretations I and J, one at B_1 and one at B_2, we say that J is an *extension* of I if $B_1<B_2$ and I is a partial interpretation of J at B_1 (i.e. I and J are identical when they are both defined).

The *E-semantic tree* (denoted ET) is a (downward) tree whose nodes at level B (where B is an element in GA) are all the partial E-interpretations at B. To paraphrase it in a more formal way, the E-semantic tree (with respect to an ordering $<$) can be defined inductively as follows:

- the root is the empty interpretation
- the successors of a node I at level B are the extensions of I where, according to the definition of E-interpretations, can be one of the following cases:

  Case 1: If $B=(a=a)$ then I has only one successor J and J satisfies $J(a=a)=true$.

  Case 2: If $B=B[s]$, $s=t<B$, $B[t]<B$, and $I(s=t)=true$, then I has one successor J which satisfies $J(B)=I(B[t])$.

  Case 3: Otherwise, I has two successors L and R with: $L(B)=true$ and $R(B)=false$.

Case 2, where the major difference between this definition of E-semantic tree and the other definitions occurs, is explained as follows. If $s>t$, then by the monotonicity of the ordering which ensures that $B[s]>B[t]$, the atom $B[t]$ must have appeared before $B[s]$. By the way the E-semantic tree is defined, $I(B[t])$ must have already been assigned a value. If $I(s=t)=true$, then by the definition of E-interpretations, $I(B[s])$

must have the same value as $I(B[t])$. Therefore there is only one consistent extension of I to the atom B, not two. Case 2 also hints the use of reduction in paramodulation: if $s=t$ is true and $s>t$, then $B[s]$ can be *reduced* to $B[t]$ by using $s\rightarrow t$, and the two atoms ($B[s]$ and $B[t]$) must have the same truth value.

This definition of E-semantic tree is similar to the one in [Pet83]. However, by the way we define the orderings, the semantic trees so constructed are in general transfinite. We emphasize that it is not easy to extend Peterson's proof method to transfinite semantics trees, because his method is based on induction which does not work on transfinite trees.

The *closed E-semantic tree* of a set of clauses S, denoted by $ET(S)$, is the maximal subtree of ET such that for every node I in $ET(S)$, every clause C in S, and every ground substitution θ such that the atoms of $C\theta$ are in the domain of I, we do not have $I(C\theta)=false$ ($I(C\theta)\neq false$). In other words, if I is the last node of a **maximal path** in a closed semantic tree, then any extension of I will refute some ground instance of some clause C in S. If I refutes some $C\theta$, that is, $I(C\theta)=false$, then we call I a **failure node**. The most significant difference between our definition of semantic trees and others (e.g. [KoH69], [ChL73], [Pet83]) is that the closed semantic tree we defined *may not* be finite. It is because our trees are transfinite in general. Therefore, Herbrand's Theorem (cf. Theorem 4.3, page 61, [ChL73]) is not needed in our framework. All we need is the following (trivially true) theorem

> **Theorem** *If S is an E-unsatisfiable set then every maximal path in $ET(S)$ has an extension (thus, can be extended to a failure node).*

Two other crucial properties of the closed semantic trees are that (1) they are topologically closed, and (2) the closed E-semantic tree is *unique* with respect to the ordering $>$ and S.

> **Closure Lemma:** *The limit of an increasing sequence of nodes of $ET(S)$ belongs to $ET(S)$.*

The relationship between the E-semantic trees and the completeness of *inf* is captured by the following Fundamental Theorem. First we define the ***closed E-semantic tree** of S to be $ET(S*)$. (Recall that $S*$ with respect to a set of inference rules *Inf* includes all the consequences which can be deduced from S using the inference rules.) It is clear that a set contains the empty clause *NIL* if and only if its closed E-semantic tree is empty. Therefore we have:

> **Fundamental Theorem:** *Inf is complete if and only if $ET(S*)$ is empty whenever S is E-unsatisfiable.*

Now we outline the proof method. Suppose *inf* is not complete. By the *Fundamental Theorem*, there is an E-unsatisfiable set of clauses S (including the clause $x=x$) whose *closed E-semantic tree is not empty. If we can show that, no matter what the closed tree is, it can always be "shrunk" into a smaller closed tree for $S*$, then by the uniqueness (and the maximality) of the E-closed semantic tree, we have a contradiction. Consequently, *inf* is complete.

4.2. Completeness of the Strategies

In what follows, we give the proof of completeness of the S-strategy based on the method given above. The completeness of UKB is an easy corollary. We first prove the completeness for the ground case, the non-ground case follows from a lifting lemma to be given later.

Assume that the S-strategy is not complete, then by the Fundamental Theorem there is an E-unsatisfiable set of (ground) clauses S such that $ET(S*)$ is not empty. We define a maximal path of nodes in $ET(S*)$ by transfinite induction as follows:

The first element of the path is the root of $ET(S*)$.

Suppose I is the last element of the sequence which we have defined so far. I can be viewed as a partial E-interpretation defined up to some ground equality say $a=b$ where $a \geq b$. The path is extended (or stops) according to the following rules:

(1) if I has no successor in $ET(S*)$ then the path is completed.

(2) if I has one successor J in $ET(S*)$ then the next element of the path will be J.

(3) if I has two successors L and R in $ET(S*)$ with $L(a=b)=true$ and $R(a=b)=false$ then

  (3.1) if there is $a=c$, $a>c$ [3], in $S*$ such that $I(c=b)=true$, the next element will be L.

  (3.2) otherwise the next element is R.

This path of nodes is not empty since $ET(S*)$ is not empty. Let K be the limit node of the path. By the Closure Lemma, K has an extension labeled by some $s=t$. (without loss of generality, we assume that $s \geq t$.) K may have one or two successors. However, by the definition of the path, any immediate successor of K must be a failure node. We now show that in every possible case some inference rule in *inf* can be applied to force either K or one of its ancestor node to be a failure node, thus, reaches a contradiction. As a remark, Condition 3.1 is needed to exclude the possibility of

[3] It is obvious that $c \geq b$.

superimposing into the right hand side of a rule (see Case 2.2 in the proof).

The following enumerates all possibilities.

Case 0

$s=t$ is K-irreducible.

Case 0.1: (See Figure 1)

$s=t$ is a ground equality $a=a$. Since K has no successor in $ET(S*)$, $a\neq a$ must be a member of $S*$. Then by *reflexive refutation* (between $a\neq a$ and $x=x$), the empty clause also belongs to $S*$. This contradicts to the assumption that $ET(S*)$ is not empty.

Case 0.2: (See Figure 2)

Otherwise, K has two successors in ET. Then both $s=t$ and $s\neq t$ must be members of $S*$. By *extended narrowing* on $s\neq t$ using $s=t$ (noting that $s\rightarrow t$ since $s>t$), we produce $t\neq t$ which is also in $S*$. Since $t=t$ is a smaller atom than $s=t$, $t=t$ must have appeared in the partial interpretation K. By the definition of E-interpretations, $K(t=t)=true$. Therefore K must falsify $t=t$, contradicting to the assumption that K does not falsify anything in $S*$.

Case 1: (See Figure 3)

$s=t$ is K-reducible to some equality g such that $K(g)=true$. Then by the definition of E-semantic trees and K, $s\neq t$ belongs to $S*$. We denote $s\neq t$ by the expression e. Let $l=r$ be the smallest equality such that $l>r$, l is a subterm of e, and $K(l=r)=true$. It is easy to see that $l=r$ is K-irreducible (otherwise it will not be the smallest such element as chosen). Let J be the node of the path at $l=r$. By the definition of the chosen path, the right child of J must lead to an equality $l=u$ such that $l>u$, $l=u$ belongs to $S*$, and $J(u=r)=K(u=r)=true$. Since l is a subterm of e, $e[u]$ is an *extended narrowing* of $l=u$ on e. Therefore, $e[u]$ belongs to $S*$. Once again, since both $e[r]$ and $e[u]$ are smaller atoms than $e[l]$, they must have been defined in K. By the definition of E-interpretations, But $K(e[u])=K(e[r])=false$. Thus, K will falsify $e[u]$, contradicting the assumption that K is in $ET(S*)$.

Case 2:

$s=t$ is K-reducible to some equality g such that $K(g)=false$. Then $s=t$ belongs to $S*$, since K is the last node of the chosen path.

Case 2.1: (See Figure 4)

There is an equality $l=r$ (with $l\geq r$) such that $K(l=r)=true$ and l is a subterm of s. We can assume that $l=r$ is the smallest (w.r.t. $>$) such atom. This implies that $l=r$ is K-irreducible. Let J be the node of the path at $l=r$. As in Case 1 there is $l=u$ in $S*$ such that $J(u=r)=K(u=r)=true$. By

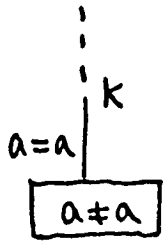

Figure 1

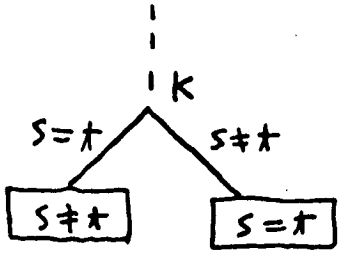

Figure 2

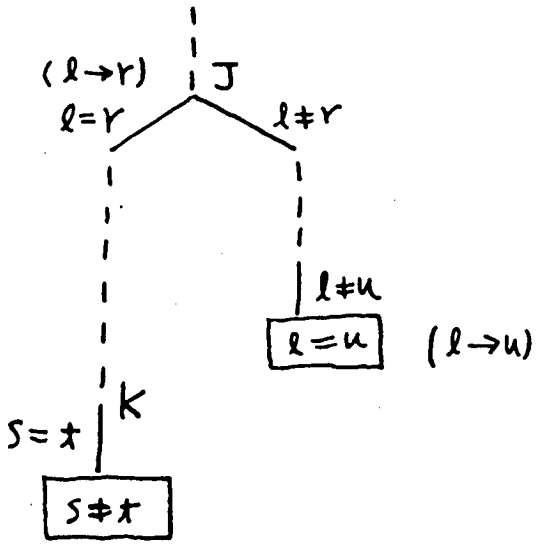

Figure 3

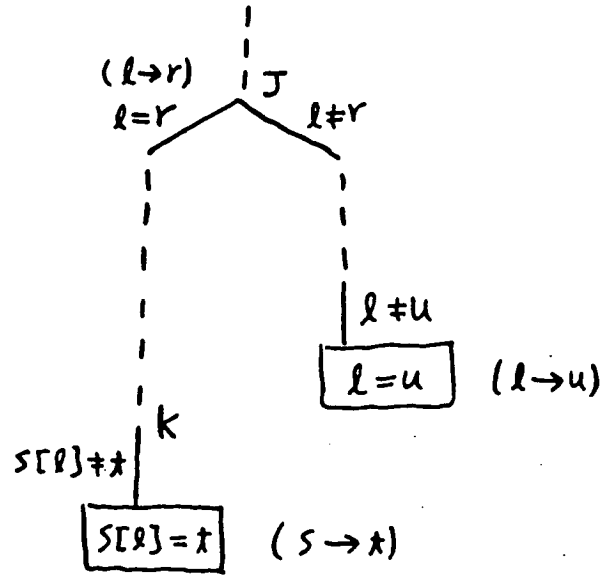

Figure 4

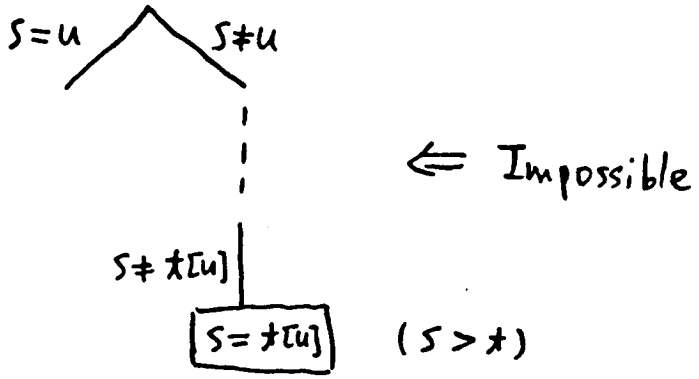

Figure 5

extended superposition of $l=u$ and $s=t$, we obtain $s[u]=t$. Note that it is a legitimate inference since $l>u$ and $s>t$. Thus, $s[u]=t$ belongs to $S*$. However, since $s=t$ can be K-reduced to $s[r]=t$, $K(s[u]=t)=K(s[r]=t)=false$. Therefore K falsifies $s[u]=t$, contradiction.

Case 2.2: (See Figure 5)

There is *no* equality $l=r$ (with $l \geq r$) such that $K(l=r)=true$ and l is a subterm of s. In other words, t is K-reducible and s is not. Let u be the smallest term such that $K(t=u)=true$ and $t>u$. It is clear that $s=u$ is K-irreducible. Let J be the node of the path at $s=u$. Since $s=t$ is K-reducible to $s=u$, we have $K(s=u)=false$. Therefore the node following J in the path is its *right* child. This contradicts (3.1) of the construction of the path which forces the path to choose the *left* child at J since $s=u$ is J-irreducible, $s=t$ is in $S*$, $t>u$, and $J(t=u)=K(t=u)=true$.

4.2.1. The Lifting Arguments

To lift the above proof from ground to non-ground, we need the following:

> **Paramodulation Lifting Lemma** *Let C_1 and C_2 be two clauses and θ be a ground substitution. Also let r be a proper (i.e. nonvariable) subterm of C_2 and C' be an oriented paramodulant from paramodulating $C_1\theta$ into $C[r]_2\theta$ at $r\theta$. Then there is a paramodulant of C_1 into $C_2[r]$ at r.*

In order to use the paramodulation lifting lemma, we need to ensure that whenever extended superposition or extended narrowing is applied to a ground clause (say $C[s]$) in the above proof, s has a corresponding nonvariable subterm in the original clause. This can be ensured by the following lemma:

> **Lemma** *Suppose θ is a ground substitution and $C\theta$ is a clause such that $I(C\theta)=false$. Then there exists an I-irreducible ground substitution σ such that $I(C\sigma)=false$.*

With this lemma, we can choose $C[s]$ so that the substitutions corresponding to its non-ground clause (call it D) are I-irreducible. Thus, the extended superposition/narrowing which is performed on $C[s]$ has to be on a subterm corresponding to a nonvariable subterm of D.

Both lemmas above are proved in [Pet83]. Consequently,

> **Theorem** *The S-strategy is complete for the extended equational theories.*

The difference between the problem domains of the S-strategy and UKB is that one can have arbitrary inequalities while the other only have those that are ground.

Consequently, Extended Narrowing instead of Target Reduction and Reflexive Refutation instead of Final Refutation must be employed in the S-strategy. However, it is easy to see that Target Reduction and Final Refutation are merely instances of the other two inference rules (e.g. reduction is narrowing without instantiating any variables). Therefore, by replacing Extended Narrowing and Reflexive Refutation in the proof of completeness of the S-strategy by the corresponding inference rules in the UKB, we have:

> **Corollary** *UKB is complete for equational theories. That is, UKB is a semi-decision procedure for deciding the word problem of equational theories.*

5. An Implementation and Some Examples

In this section we describe an implementation of UKB and the S-strategy and show some examples. Our implementation (called *Sbreve*) is based on modified version of the term rewriting laboratory *Reve* 2.4 [For84] and is written by J. Mzali on a Sun3/75 in the language CLU. In addition to the inference rules and strategies given above, we have also implemented a *subsumption check*, which detects and eliminates critical pairs which are instances of the already existing equations. This check is needed to prevent UKB from generating the same (non-orientable) critical pair indefinitely. Note that such a mechanism is not needed in the original KB-procedure since the KB-procedure assumes that every critical pair can be oriented.

In order to handle the situation of an equation with different variables on the two sides, Knuth-Bendix introduced a simple technique of *splitting*. Assume that an equation $l=r$ has common variables $x_1, \cdots, x_n$, l has some other variables which are not in r and vice versa, then a new function $f(x_1, \ldots, x_n)$ is created, along with two rules $l \rightarrow f(x_1, \cdots, x_n)$ and $r \rightarrow f(x_1, \cdots, x_n)$. This feature is also implemented in *Reve* and has been used in [Hsi85]. Because splitting was designed mainly for resolving non-orientable critical pairs, it is not a necessity in UKB. However, splitting is still a convenient feature since it can reduce the complexity of terms (by eliminating non-essential variables). Another feature incorporated in *Sbreve* is a simple device for detecting inconsistent theories, that is, theories with only models of one element.

In what follows we give a couple of examples. The first one is from [Ped85].

An *entropic groupoid* is an algebraic structure with two axioms:

$(xy)(zw)=(xz)(yw)$
$(xy)x=x$.

Note that the first axiom is a *permutative* axiom and cannot be oriented. Thus, the KB-completion procedure fails for this problem (so does E-term rewriting). With our

method, the axioms are arranged as

$(xy)(zw)=(xz)(yw)$ e1
$(uv)u \rightarrow u$ r2

By unifying u in r2 with (zw) of the left hand side of e1, we produce a critical pair

$$((zw)z)(yw)=(zw),$$

which becomes a rule

$$z(yw)\rightarrow zw. \qquad \text{r3}$$

R3 simplifies e1 into

$$(xy)w=(xz)w. \qquad \text{e4}$$

Eventually, the following canonical system is generated:

$(xy)x \rightarrow x$ r2
$x(yz)\rightarrow xz$ r3
$(xy)z=(xw)z$ e4
$((xy)z)w \rightarrow xw$ r5

By Theorem 3, this system is a ground canonical system which reduces every ground term to a unique normal form. It took *Sbreve* 6 cpu-seconds on a Sun3/75 to complete this example.

The next example is for the S-strategy. This problem is given by Overbeek in [85], and is due to Smullyan according to Overbeek. Given the following extended theory

$S(x,S(y,z))=S(f(x,y),z)$ e1
$S(m,x)=S(x,x)$ e2
$S(a,x)\neq x$ e3

If the ordering is first by size, then lexicographically from left to right, then the first equation can be ordered as

$$S(f(x,y),z)\rightarrow S(x,S(y,z)). \qquad \text{r1}$$

Note that the *only* extended critical pair between r1 and e2 that can be obtained by superposing the left hand side of r1 and $S(x,x)$ is:

$$S(x,S(y,f(x,y)))\rightarrow S(m,f(x,y)). \qquad \text{r4}$$

It should be obvious why it can indeed be oriented. Rule r4 and e3, using extended narrowing, derives

$$S(m, f(x, y)) \neq S(y, f(x, y)) \qquad \text{e5}$$

Now e5, using reflexive refutation by unifying y and m, deduces $S(m, f(x, m)) \neq S(m, f(x, m))$, which leads to the contradiction.

If e1 is ordered the other way (by right-to-left lexicographic ordering), then the search space is larger since there are more extended superpositions. However the proof can still be obtained after generating about 6 equations (among them only 2 are useful).

The proof is found by *Sbreve* in 4 cpu-seconds.

6. References

[BDH85] L. Bachmair, N. Dershowitz and J. Hsiang, *Orderings for Equational Proofs*, Conference on Logic in Computer Science, June 1985.

[ChL73] C. L. Chang and C. T. Lee, *Symbolic Logic and Mechanical Theorem Proving*, Academic Press, 1973.

[Der82] N. Dershowitz, "Orderings for Term Rewriting Systems", *J.TCS*, **17**, 3 (1982), 279-301.

[For84] R. Forgaard, "A Program for Generating and Analyzing Term Rewriting Systems", Master's Thesis, MIT Lab. for Computer Science, 1984.

[Hsi85] J. Hsiang, "Two Results in Term Rewriting Theorem Proving", *Proc. of 1st International Conference in Rewrite Techniques and Applications*, May, 1985.

[HsR85] J. Hsiang and M. Rusinowitch, "A New Method for Establishing Refutational Completeness in Theorem Proving", Tech. Rep. 85/24,, SUNY at Stony Brook, Nov. 1985.

[HuL78] G. Huet and D. S. Lankford, "On the Uniform Halting Problem for Term Rewriting Systems", Report 283, INRIA, 1978.

[Hue81] G. Huet, "A Complete Proof of Correctness of Knuth-Bendix Completion Algorithm", *J. Computer and System Sciences*, **23**, (1981), 11-21.

[JLR82] J. P. Jouannaud, P. Lescanne and F. Reinig, "Recursive Decomposition Ordering", *Conf. on Formal Description of Programming Concepts II*, 1982, 331-346.

[JoK84] J. Jouannaud and H. Kirchner, "Completion of a Set of Rules Modulo a Set of Equations", *11th Symposium on Principles of Programming Languages*, Salt Lake City, Utah, January, 1984.

[KnB70] D. E. Knuth and P. B. Bendix, "Simple Word Problems in Universal Algebras", in *Computational Algebra*, J. Leach, (ed.), Pergamon Press, 1970,

263-297.

[KoH69] R. A. Kowalski and P. Hayes, "Semantic Trees in Automatic Theorem Proving", in *Machine Intelligence*, vol. 5, B. Meltzer and D. Michie, (eds.), American Elsevier, 1969, 181-201.

[Lan75] D. S. Lankford, "Canonical Inference", Report ATP-32, Univ. of Texas at Austin, 1975.

[LaB77] D. S. Lankford and A. M. Ballantyne, "Decision Procedure for Simple Equational Theories with Commutative-Associative Axioms", Report ATP-39, Univ. of TExas at Austin, 1977.

[Ped85] J. Pedersen, "Obtaining Complete Sets of Reductions and Equations without using Special Unification Algorithms", Unpublished manuscript, 1985.

[PeS81] G. E. Peterson and M. E. Stickel, "Complete Sets of Reductions for Some Equational Theories", *J. ACM*, **28**, (1981), 233-264.

[Pet83] G. E. Peterson, "A Technique for Establishing Completeness Results in Theorem Proving with Equality", *SIAM J. of Computing*, **12**, 1 (1983), 82-100.

[Pla78] D. A. Plaisted, "A Recursively Defined Ordering for Proving Termination of Term Rewriting Systems", UIUCDCS-R-78-943, Univ. of Illinois, Urbana, IL, 1978.

[Pla85] D. Plaisted, "Private Communication", , 1985.

[85] "Assoc. of Automated Reasoning Newsletter", , 1985.

Imprimé en France
par
l'Institut National de Recherche en Informatique et en Automatique