INFORMATION AND COMPUTATION 87, 129–195 (1990)

Rigid E-Unification: NP-Completeness and Applications to Equational Matings*

JEAN GALLIER

Department of Computer and Information Science, University of Pennsylvania, Philadelphia, Pennsylvania 19104

PALIATH NARENDRAN†

Department of Computer Science, University of Calgary, 2500 University Avenue Northwest, Calgary Alberta T2N 1N4, Canada

DAVID PLAISTED

Department of Computer Science, New West Hall 035-A, University of North Carolina at Chapel Hill, Chapel Hill, North Carolina 27514

AND

WAYNE SNYDER

Computer Science Department, Room 280, Boston University, 111 Cummington Street, Boston, Massachusetts 02215

Rigid E-unification is a restricted kind of unification modulo equational theories, or E-unification, that arises naturally in extending Andrews' theorem proving method of matings to first-order languages with equality. This extension was first presented by J. H. Gallier, S. Raatz, and W. Snyder, who conjectured that rigid E-unification is decidable. In this paper, it is shown that rigid E-unification is NP-complete and that finite complete sets of rigid E-unifiers always exist. As a consequence, deciding whether a family of mated sets is an equational mating is an NP-complete problem. Some implications of this result regarding the complexity of theorem proving in first-order logic with equality are also discussed.

* This research was partially supported by the National Science Foundation under Grants DCR-85-16243 and DCR-86-07156, and by the Office of Naval Research under Grant N00014-88-K-0593.

† Present address: Department of Computer Science, State University of New York at Albany, Albany, New York 12222.

0890-5401/90 $3.00

1. INTRODUCTION

Rigid E-unification is a restricted kind of unification modulo equational theories, or E-unification, that arises naturally in extending Andrews' theorem proving method of matings to first-order languages with equality [1]. This extension was first presented by Gallier, Raatz, and Snyder [10], who conjectured that rigid E-unification is decidable. In this paper, it is shown that rigid E-unification is NP-complete and that finite complete sets of rigid E-unifiers always exist. These results were announced (without complete proofs) at LICS'88 [12].

We now explain why this result is significant for theorem proving in first-order languages with equality. At first glance, a generalization of the method of matings to first-order languages with equality where equality is built-in in the sense of Plotkin [26] (thus, it is not the naive method where explicit equality axioms are added, which is rejected for well-known inefficiency reasons) requires general E-unification. Hence, there are two factors contributing to the undecidability of the method of matings for first-order languages with equality: (1) the fact that one cannot predict how many disjuncts will occur in a Herbrand expansion (which also holds for first-order languages without equality); (2) the undecidability of the kind of unification required (E-unification). However, we have shown in [10, 13] that the completeness of the method of equational matings is preserved if unrestricted E-unification is replaced by rigid E-unification. Since we prove in this paper that rigid E-unification is decidable, the second undecidability factor is eliminated. This is the main reason why our result is significant.

The NP-completeness of rigid E-unification also shows clearly how the presence of equality influences the complexity of theorem proving methods. For languages without equality, one can use standard unification whose time complexity is polynomial, and in fact $O(n)$. For languages with equality, the type of unification required is NP-complete.

Before launching into rigid E-unification, let us recall how it arises naturally in generalizing the method of matings to first-order languages with equality. For details, the reader is referred to Gallier, Raatz, and Snyder [10], and Gallier, Narendran, Raatz, and Snyder [13]. The crucial observation due to Andrews is that a quantifier-free formula without equality is unsatisfiable iff certain sets of literals occurring in A (called *vertical paths*) are unsatisfiable. Matings come up as a convenient method for checking that vertical paths are unsatisfiable. Roughly speaking, a *mating* is a set of pairs of literals of opposite signs (*mated pairs*) such that all these (unsigned) pairs are globally unified by some substitution. The importance of matings stems from the fact that a quantifier-free formula A has a mating iff there is a substitution θ such that $\theta(A)$ is unsatisfiable. For languages without equality, this can be checked using standard unification.

In the case of languages with equality, one needs to extend matings to *equational matings*, which is nontrivial and requires proving a generalization of Andrews' version of the Skolem–Herbrand–Gödel theorem [1, 2]. An equational mating is now a set of sets of literals (*mated sets*), where a mated set consists of several positive equations and a single negated equation (rather than pairs of literals as in Andrews' case). Checking that a family of mated sets is unsatisfiable, i.e., an equational mating, is equivalent to the following problem.

PROBLEM 1. Given $E = \{E_i \mid 1 \leqslant i \leqslant n\}$ a family of n finite sets of equations and $S = \{\langle u_i, v_i \rangle \mid 1 \leqslant i \leqslant n\}$ a set of n pairs of terms, is there a substitution θ such that, treating each set $\theta(E_i)$ as a set of *ground* equations (i.e., holding the variables in $\theta(E_i)$ "rigid"), $\theta(u_i)$ and $\theta(v_i)$ are provably equal from $\theta(E_i)$ for $i = 1, ..., n$?

Equivalently, is there a substitution θ such that $\theta(u_i)$ and $\theta(v_i)$ can be shown congruent from $\theta(E_i)$ by the congruence closure method for $i = 1, ..., n$ (Kozen [19, 20], Nelson and Oppen [24], Downey, Sethi, and Tarjan [8])?

A substitution θ solving problem 1 is called a *rigid E-unifier of S*, and a pair $\langle E, S \rangle$ such that S has some rigid E-unifier is called an *equational premating*. It is shown in Section 10 that deciding whether a pair $\langle E, S \rangle$ is an equational premating is an NP-complete problem. Since the problem of deciding whether a family of mated sets forms an equational mating is equivalent to the problem of finding whether a pair $\langle E, S \rangle$ is an equational premating, the former problem is also NP-complete.[1] Actually, this result is an easy extension of a simpler problem, and we now focus on this problem.

PROBLEM 2. Given a finite set $E = \{u_1 \doteq v_1, ..., u_n \doteq v_n\}$ of equations and a pair $\langle u, v \rangle$ of terms, is there a substitution θ such that, treating $\theta(E)$ as a set of ground equations, $\theta(u) \overset{*}{\cong}_{\theta(E)} \theta(v)$, that is, $\theta(u)$ and $\theta(v)$ are congruent modulo $\theta(E)$ (by congruence closure)?

The substitution θ is called a *rigid E-unifier of u and v*.

EXAMPLE 1.1. Let $E = \{fa \doteq a,\ ggx \doteq fa\}$, and $\langle u, v \rangle = \langle gggx, x \rangle$. Then, the substitution $\theta = [ga/x]$ is a rigid E-unifier of u and v. Indeed, $\theta(E) = \{fa \doteq a,\ ggga \doteq fa\}$, and $\theta(gggx)$ and $\theta(x)$ are congruent modulo $\theta(E)$, since

$$\theta(gggx) = gggga \to gfa \qquad \text{using} \quad ggga \doteq fa$$
$$\to ga = \theta(x) \qquad \text{using} \quad fa \doteq a.$$

[1] We chose the terminology *equational premating* because an equational mating is an equational premating satisfying some extra properties; see [10] or [13].

Note that θ is not the only rigid E-unifier of u and v. For example, $[gfa/x]$ or more generally $[gf^n a/x]$ is a rigid E-unifier of u and v. However, θ is more general than all of these rigid E-unifiers (in a sense to be made precise later). It is shown in Section 8 that there is always a finite set of most general rigid E-unifiers called a complete set of rigid E-unifiers.

It is interesting to observe that the notion of rigid E-unification arises by *bounding* the resources, in this case, the number of available instances of equations in E. To be precise, only a single instance of each equation in E can be used, and in fact, these instances $\theta(u_1 \doteq v_1), \ldots, \theta(u_n \doteq v_n)$ must arise from the *same* substitution θ. Also, once these instances have been created, the remaining variables (if any) are considered rigid, that is, treated as constants, so that it is not possible to instantiate these instances. Thus, rigid E-unification and Girard's linear logic [14] share the same spirit. Since the resources are bounded, it is not too surprising that rigid E-unification is decidable, but it is not obvious at all that the problem is in NP. The special case of rigid E-unification where E is a set of ground equations has been investigated by Kozen [19, 20], who has shown that this problem is NP-complete. Thus, rigid E-unification is NP-hard, and we will show that it is also in NP, hence NP-complete.

Suppose we want to find a rigid E-unifier θ of u and v. Roughly, the idea is to use a form of unfailing completion procedure (Knuth and Bendix [18], Huet [16], Bachmair [3], Bachmair, Dershowitz, and Plaisted [4], Bachmair, Dershowitz, and Hsiang [5]). In order to clarify the differences between our method and unfailing completion, especially for readers unfamiliar with this method, we briefly describe the use of unfailing completion as a refutation procedure. For more details, the reader is referred to Bachmair [3].

Let E be a set of equations, and $\succ$ a reduction ordering total on ground terms. The central concept is that E is *ground Church–Rosser w.r.t.* $\succ$. The crucial observation is that every ground instance $\sigma(l) \doteq \sigma(r)$ of an equation $l \doteq r \in E$ is orientable w.r.t. $\succ$, since $\succ$ is total on ground terms. Let $E^{\succ}$ be the set of all instances $\sigma(l) \doteq \sigma(r)$ of equations $l \doteq r \in E \cup E^{-1}$ with $\sigma(l) \succ \sigma(r)$ (the set of *orientable instances*). We say that E is *ground Church–Rosser w.r.t.* $\succ$ iff for every two ground terms u, v, if $u \overset{*}{\leftrightarrow}_E v$, then there is some ground term w such that $u \overset{*}{\rightarrow}_{E^{\succ}} w$ and $w \overset{*}{\leftarrow}_{E^{\succ}} v$. Such a proof is called a *rewrite proof*.

An unfailing completion procedure attempts to produce a set E^{∞} equivalent to E and such that E^{∞} is ground Church–Rosser w.r.t. $\succ$. In other words, every ground equation provable from E has a rewrite proof in E^{∞}. The main mechanism involved in the computation of critical pairs. Given two equations $l_1 \doteq r_1$ and $l_2 \doteq r_2$ where l_2 is unifiable with a subterm l_1/β of l_1 which is not a variable, the pair $\langle \sigma(l_1[\beta \rightarrow r_2]), \sigma(r_1) \rangle$ where σ is a mgu of l_1/β and l_2 is a *critical pair*.

If we wish to use an unfailing completion procedure as a refutation procedure, we add two new constants T and F and a new binary function symbol eq to our language. In order to prove that $E \vdash u \doteq v$ for a ground equation $u \doteq v$, we apply the unfailing completion procedure to the set $E \cup \{eq(u, v) \doteq F,\ eq(z, z) \doteq T\}$, where z is a new variable. It can be shown that $E \vdash u \doteq v$ iff the unfailing completion procedure generates the equation $F \doteq T$. Basically, given any proof of $F \doteq T$, the unfailing completion procedure extends E until a rewrite proof is obtained. It can be shown that unfailing completion is a complete refutation procedure, but of course, it is not a decision procedure. It should also be noted that when unfailing completion is used as a refutation procedure, E^{∞} is actually never generated. It is generated "by need," until $F \doteq T$ turns up.

We now come back to our situation. Without loss of generality, it can be assumed that we have a rigid E-unifier θ of T and F such that $\theta(E)$ is ground. In this case, equations in $\theta(E)$ are orientable instances. The crucial new idea is that in trying to obtain a rewrite proof of $F \doteq T$, we still compute critical pairs, but we *never rename variables.* If l_2 is equal to l_1/β, then we get a critical pair essentially by simplification. Otherwise, some variable in l_1 or in l_2 becomes bound to a term *not* containing this variable. Thus the total number of variables in E keeps decreasing. Therefore, after a polynomial number of steps (in fact, the number of variables in E) we must stop or fail. So we get membership in NP. Oversimplifying a bit, we can say that our method is a form of lazy unfailing completion with no renaming of variables.

However, there are some significant departures from traditional Knuth–Bendix completion proceddures, and this is for two reasons. The first reason is that we must ensure termination of the method. The second is that we want to show that the problem is in NP, and this forces us to be much more concerned about efficiency.

Our method can be described in terms of a single transformation on triples of the form $\langle \mathscr{S}, \mathscr{E}, \mathscr{O} \rangle$, where $\mathscr{S}$ is a unifiable set of pairs, $\mathscr{E}$ is a set of equations, and $\mathscr{O}$ is something that will be needed for technical reasons and can be ignored for the present. Starting with an initial triple $\langle \mathscr{S}_0, \mathscr{E}_0, \mathscr{O}_0 \rangle$ initialized using E and u, v (except for $\mathscr{O}_0$ that must be guessed), if the number of variables in E is m, one considers sequences of transformations

$$\langle \mathscr{S}_0, \mathscr{E}_0, \mathscr{O}_0 \rangle \Rightarrow^{+} \langle \mathscr{S}_k, \mathscr{E}_k, \mathscr{O}_k \rangle,$$

consisting of at most $k \leqslant m$ steps. It will be shown that u and v have some rigid E-unifier iff there is some sequence of steps as above such that the special equation $F \doteq T$ is in $\mathscr{E}_k$ and $\mathscr{S}_k$ is unifiable. Then, the most general unifier of $\mathscr{S}_k$ is a rigid E-unifier of u and v.

Roughly speaking, $\mathscr{E}_{k+1}$ is obtained by overlapping equations in $\mathscr{E}_k$ (forming critical pairs), as in unfailing Knuth–Bendix completion procedures, except that no renaming of variables takes place. In order to show that the number of steps can be bounded by m, it is necessary to show that some measure decreases every time an overlap occurs, and there are two difficulties. First, the overlap of two equations may involve the identity substitution when some equation simplifies another one. In this case, the number of variables does not decrease, and no other obvious measure decreases. Second, it is more difficult to handle overlap at variable occurrences than it is in the traditional case, because we are not allowed to form new instances of equations.[2]

The first difficulty can be handled by using a special procedure for reducing a set of (ground) equations. Such a procedure is presented by Gallier *et al.* [11] and runs in polynomial time. Actually, one also needs a total simplification ordering $\prec$ on ground terms, and a way of orienting equations containing variables, which is the purpose of the mysterious component $\mathscr{O}$. The second difficulty is overcome by noting that one needs only consider ground substitutions, that the ordering $\prec$ (on ground terms) can be extended to ground substitutions, and that given any rigid E-unifier θ of u and v, there is always a least rigid E-unifier σ (w.r.t $\prec$) that is equivalent to θ (in a sense to be made precise).

Other complications arise in proving that the method is in NP; in particular, we found it necessary to represent most general unifiers (mgu's) by their triangular form (see Definition 3.3), as in Martelli and Montanari [22].

We now give an outline of the paper. Section 2 contains background material consisting of a summary of definitions and results needed in this paper. In Section 3, the representation of mgu's in triangular form is reviewed. In Section 4, some preorders on substitutions and complete sets of rigid E-unifiers are defined. The existence of minimal rigid E-unifiers is shown in Section 5. The procedure for reducing a set of (ground) equations and the notion of order assignment (the $\mathscr{O}$'s) are given in Section 6. The method for finding complete sets of rigid E-unifiers and two examples are given in Section 7. The soundness, completeeness, and decidability of the method are shown in Section 8. The NP-completeness of rigid E-unification is shown in Section 9. In Section 10, the decision procedure for rigid E-unification is extended to equational prematings. It is shown that finding prematings is NP-complete. Section 11 is the conclusion, and further work is briefly discussed.

[2] We realize that only readers intimately familiar with completion procedures will understand this problem. Other readers should move on. We hope that this point will become clear during reading of the proof of Theorem 8.2.

2. PRELIMINARIES

In order that this paper be self-contained, a summary of the basic definitions and results used is given in this section. These are basically consistent with [17, 9]. We begin with the basic algebraic notions of trees and substitutions.

DEFINITION 2.1. Let $\mathbf{N}$ be the set of natural numbers. A *ranked alphabet* is a set Σ with an associated function *arity*: $\Sigma \to \mathbf{N}$ assigning a *rank* or *arity* n to each symbol f in Σ. We denote the set of symbols of arity n by Σ_n. (For example, the set of constants is just Σ_0.)

DEFINITION 2.2. Let $\mathbf{N}_+$ denote the set of positive natural numbers. A *tree domain* D is a nonempty subset of strings in $\mathbf{N}_+^*$ satisfying the conditions:

(i) For all $\alpha, \beta \in \mathbf{N}_+^*$, if $\alpha\beta \in D$ then $\alpha \in D$.

(ii) For all $\alpha \in \mathbf{N}_+^*$, for every $i \in \mathbf{N}_+$, if $\alpha i \in D$ then, for every j, $1 \leqslant j \leqslant i$, $\alpha j \in D$.

DEFINITION 2.3. Given a ranked alphabet Σ, a *Σ-tree* (or *term*) is any function $t: D \to \Sigma$, where D is a tree domain denoted by $\mathrm{Dom}(t)$ and if $\alpha \in \mathrm{Dom}(t)$ and $\{i \mid \alpha i \in \mathrm{Dom}(t)\} = \{1, ..., n\}$, then $\mathrm{arity}(t(\alpha)) = n$. We shall denote the symbol $t(\varepsilon)$ by $\mathrm{Root}(t)$. Given a tree t and some tree address $\alpha \in \mathrm{Dom}(t)$, the *subtree of t rooted at α* is the tree, denoted t/α, whose domain is the set $\{\beta \mid \alpha\beta \in \mathrm{Dom}(t)\}$ and such that $t/\alpha(\beta) = t(\alpha\beta)$ for all $\beta \in \mathrm{Dom}(t/\alpha)$. Given two trees t_1 and t_2 and a tree address α in t_1 the *result of replacing t_2 at α* in t_1, denoted by $t_1[\alpha \leftarrow t_2]$, is the function whose graph is the set of pairs $\{(\beta, t_1(\beta)) \mid \beta \in \mathrm{Dom}(t_1), \alpha \text{ is not a prefix of } \beta\} \cup \{(\alpha\beta, t_2(\beta)) \mid \beta \in \mathrm{Dom}(t_2)\}$.

The set of all finite trees is denoted by T_Σ. Given a countably infinite set of variables $X = \{x_0, x_1, ...\}$, we can form the set of trees $T_\Sigma(X)$ by adjoining the set X to the set Σ_0. Thus, $T_\Sigma(X)$ is the set of all terms formed from the constant and function symbols in Σ and the variables in X.

We shall denote the *depth* of a term t, i.e., the length of the longest path in t (or, equivalently, the length of the longest string in $\mathrm{Dom}(t)$), by $|t|$. For example, $|f(a)| = 1$ and $|c| = 0$. The *size* of a term t is the number of addresses in $\mathrm{Dom}(t)$, and it is denoted by $\mathrm{size}(t)$. The set of variables occurring in a term t is the set

$$\mathrm{Var}(t) = \{x \in X \mid t(\alpha) = x \text{ for some } \alpha \in \mathrm{Dom}(t)\}.$$

Any term t for which $\mathrm{Var}(t) = \varnothing$ is called a *ground term*.

In the rest of this paper, we use the letters a, b, c, and d to denote constants; f, g, and h to denote functions;, l, r, s, t, u, v, and to denote terms; and α, β, and γ to denote tree addresses.

In order that $T_\Sigma(X)$ be nonempty, we assume that $\Sigma_0 \cup X \neq \varnothing$. Thus $T_\Sigma(X)$ is the free Σ-algebra generated by X. This property allows us to define substitutions.

DEFINITION 2.4. A *substitution* is any function $\theta: X \to T_\Sigma(X)$ such that $\theta(x) \neq x$ for only finitely many $x \in X$. Since $T_\Sigma(X)$ is freely generated by X, every substitution $\theta: X \to T_\Sigma(X)$ has a unique homomorphic extension $\hat{\theta}: T_\Sigma(X) \to T_\Sigma(X)$. In the sequel, we will identify θ and its homomorphic extension $\hat{\theta}$.

DEFINITION 2.5. Given a substitution σ, the *support* (or *domain*) of σ is the set of variables $D(\sigma) = \{x \mid \sigma(x) \neq x\}$. A substitution whose support is empty is termed the *identity substitution*, and is denoted by *Id*. The set of variables *introduced by* σ is $I(\sigma) = \bigcup_{x \in D(\sigma)} \mathrm{Var}(\sigma(x))$. Given a substitution σ, if its support is the set $\{x_1, ..., x_n\}$, and if $t_i = \sigma(x_i)$ for $1 \leqslant i \leqslant n$, then σ is also denoted by $[t_1/x_1, ..., t_n/x_n]$. Given a term r, we also denote $\sigma(r)$ as $r[t_1/x_1, ..., t_n/x_n]$. The *restriction* of a substitution θ to some V, denoted $\theta|_V$, is the substitution θ' such that

$$\theta'(x) = \begin{cases} \theta(x), & \text{if } x \in V; \\ x, & \text{otherwise.} \end{cases}$$

DEFINITION 2.6. The *composition* of σ and θ is the substitution denoted by $\sigma; \theta$ such that for every variable x we have $\sigma; \theta(x) = \hat{\theta}(\sigma(x))$. Given a set V of variables, we say that two substitutions σ and θ are *equal over* V, denoted $\sigma = \theta[V]$ iff $\forall x \in V$, $\sigma(x) = \theta(x)$. We say that σ is *more general than* θ *over* V, denoted by $\sigma \leqslant \theta[V]$, iff there exists a substitution η such that $\theta = \sigma; \eta[V]$. When $V = X$ (where X is the set of variables), we will drop the notation $[V]$. A substitution σ is *idempotent* if $\sigma; \sigma = \sigma$. It is easily seen that σ is idempotent iff $D(\sigma) \cap I(\sigma) = \varnothing$. Given two disjoint sets of variables $\{x_1, ..., x_n\}$ and $\{y_1, ..., y_n\}$, the substitution $[y_1/x_1, ..., y_n/x_n]$ is called a *renaming*.

We now proceed to review the basic notions of relations, orderings, and equational rewriting.

DEFINITION 2.7. Let $\Rightarrow$ be a binary relation $\Rightarrow \subseteq A \times A$ on a set A. The transitive closure of $\Rightarrow$ is denoted by $\Rightarrow^+$ and the reflexive and transitive closure of $\Rightarrow$ by $\Rightarrow^*$. The *converse* (or *inverse*) of the relation $\Rightarrow$ is the relation denoted as $\Rightarrow^{-1}$ or $\Leftarrow$, defined such that $u \Leftarrow v$ iff $v \Rightarrow u$. The symmetric closure of $\Rightarrow$, denoted by $\Leftrightarrow$, is the relation $\Rightarrow \cup \Leftarrow$.

DEFINITION 2.8. A relation $\succ$ on a set A is *Noetherian* or *well founded* iff there are no infinite sequences $\langle a_0, ..., a_n, a_{n+1}, ... \rangle$ of elements in A such that $a_n \succ a_{n+1}$ for all $n \geqslant 0$.[3]

DEFINITION 2.9. A *preorder* $\preccurlyeq$ on a set A is a binary relation $\preccurlyeq \subseteq A \times A$ that is reflexive and transitive. A *partial order* $\preccurlyeq$ on a set A is a preorder that is also antisymmetric. The converse of a preorder (or partial order) $\preccurlyeq$ is denoted as $\succcurlyeq$. A *strict ordering* (or *strict order*) $\prec$ on a set A is a transitive and irreflexive relation. Given a preorder (or partial order) $\preccurlyeq$ on a set A, the strict ordering $\prec$ associated with $\preccurlyeq$ is defined such that $s \prec t$ iff $s \preccurlyeq t$ and $t \not\preccurlyeq s$. Conversely, given a strict ordering $\prec$, the partial ordering $\prec$ associated with $\prec$ is defined such that $s \preccurlyeq t$ iff $s \prec t$ or $s = t$. The converse of a strict ordering $\prec$ is denoted as $\succ$. Given a preorder (or parrtial order) $\preccurlyeq$, we say that $\preccurlyeq$ is well founded iff $\succ$ is well founded.[4]

DEFINITION 2.10. Let $\rightarrow$ be a binary relation $\rightarrow \subseteq T_\Sigma(X) \times T_\Sigma(X)$ on terms. The relation $\rightarrow$ is *monotonic* iff for every two terms s, t and every function symbol f, if $s \rightarrow t$ then $f(..., s, ...) \rightarrow f(..., t, ...)$. The relation $\rightarrow$ is *stable* (under substitution) if $s \rightarrow t$ implies $\sigma(s) \rightarrow \sigma(t)$ for every substitution σ.

DEFINITION 2.11. A strict ordering $\prec$ has the *subterm property* iff $s \prec f(..., s, ...)$ for every term $f(..., s, ...)$ (since we are considering symbols having a fixed rank, the deletion property is superfluous, as noted by Dershowitz [7]). A *simplification ordering* $\prec$ is a strict ordering that is monotonic and has the subterm property. A *reduction ordering* $\preccurlyeq$ is a strict ordering that is monotonic, stable, and such that $\succ$ is well founded. With a slight abuse of language, we will also say that the converse $\succ$ of a strict ordering $\prec$ is a simplification ordering (or a reduction ordering). It is shown by Dershowitz [7] that there are simplification orderings that are total on ground terms.

[3] We warn the readers that this is not the usual way of defining a well-founded relation in set theory, as, for example, in Levy [21]. In set theory, the condition is stated in the form $a_{n+1} \prec a_n$ for all $n \geqslant 0$, where $\prec = \succ^{-1}$. It is the dual of the condition we have used, but since $\prec = \succ^{-1}$, the two definitions are equivalent. When using well-founded relations in the context of rewriting systems, we are usually interested in the reduction relation $\Rightarrow$ and the fact that there are no infinite sequences $\langle a_0, ..., a_n, a_{n+1}, ... \rangle$ such that $a_n \Rightarrow a_{n+1}$ for all $n \geqslant 0$. Thus, following other authors, including Dershowitz, we adopt the dual of the standard set-theoretic definition.

[4] Again, we caution our readers that in standard set theory it is $\prec$ that is well founded! However, our definition is equivalent to the standard set-theoretic definition of a well-founded partial ordering.

DEFINITION 2.12. Let $E \subseteq T_\Sigma(X) \times T_\Sigma(X)$ be a binary relation on terms. We define the relation $\leftrightarrow_E$ over $T_\Sigma(X)$ as the smallest symmetric, stable, and monotonic relation that contains E. This relation is defined explicitly as follows: Given any two terms $t_1, t_2 \in T_\Sigma(X)$, then $t_1 \leftrightarrow_E t_2$ iff there is some variant[5] (s, t) of a pair in $E \cup E^{-1}$, some tree address α in t_1, and some substitution σ, such that

$$t_1/\alpha = \sigma(s) \qquad \text{and} \qquad t_2 = t_1[\alpha \leftarrow \sigma(t)].$$

(In this case, we say that σ is a *matching substitution* of s onto t_1/α. The term t_1/α is called a *redex*.) Note that the pair (s, t) is used as a two-way rewrite rule (that is, nonoriented). In such a case, we denote the pair (s, t) as $s \doteq t$ and call it an *equation*. When $t_1 \leftrightarrow_E t_2$, we say that we have an *equality step*. It is well known that the reflexive and transitive closure $\overset{*}{\leftrightarrow}_E$ of $\leftrightarrow_E$ is the smallest stable congruence on $T_\Sigma(X)$ containing E. When we want to fully specify an equality step, we use the notation

$$t_1 \leftrightarrow_{[\alpha, s \doteq t, \sigma]} t_2$$

(where some of the arguments may be omitted). A sequence of equality steps

$$u = u_0 \leftrightarrow_E u_1 \leftrightarrow_E \cdots \leftrightarrow_E u_{n-1} \leftrightarrow_E u_n = v$$

is called a *proof* of $u \overset{*}{\leftrightarrow}_E v$.

DEFINITION 2.13. Given a finite set E of equations (ground or not), we say that E *is treated as a set of ground equations* iff for every pair of terms u, v (ground or not), for every proof of $u \overset{*}{\leftrightarrow}_E v$, then for every equality step $s \leftrightarrow_{[\alpha, l \doteq r, \sigma]} t$ in this proof, σ is the identity substitution and $l \doteq r \in E \cup E^{-1}$ (no renaming of the equations in $E \cup E^{-1}$ is performed). This means that variables are treated as constants. We use the notation $u \overset{*}{\cong}_E v$ to express the fact that $u \overset{*}{\leftrightarrow}_E v$, treating E as a set of ground equations. Equivalently, $u \overset{*}{\cong}_E v$ iff u and v can be shown congruent from E by *congruence closure* (Kozen [19, 20], Nelson and Oppen [24], Downey, Sethi, and Tarjan [8]) again, treating all variables as constants—they are considered *rigid*.

DEFINITION 2.14. When a pair $(s, t) \in E$ is used as an oriented equation (from left to right), we call it a *rule* and denote it as $s \to t$. The *reduction relation* $\to_E$ is the smallest stable and monotonic relation that contains E. We can define $t_1 \to_E t_2$ explicitly as in Definition 2.12, the only difference

[5] A pair (s, t) is a *variant* of a pair $(u, v) \in E$ iff there is some renaming ρ with domain $\mathrm{Var}(u) \cup \mathrm{Var}(v)$ such that $s = \rho(u)$ and $t = \rho(v)$.

being that (s, t) is a variant of a pair in E (and not in $E \cup E^{-1}$). When $t_1 \to_E t_2$, we say that t_1 *rewrites* to t_2, or that we have a *rewrite step*. When we want to fully specify a rewrite step, we use the notation

$$t_1 \to_{[\alpha, s \to t, \sigma]} t_2$$

(where some of the arguments may be omitted).

When $\mathrm{Var}(r) \subseteq \mathrm{Var}(l)$, then a rule $l \to r$ is called a *rewrite rule*; a set of such rules is called a *rewrite system*. A *degenerate equation* is an equation of the form $x \doteq t$, where x is a variable and $x \notin \mathrm{Var}(t)$, and a *nondegenerate equation* is an equation that is not degenerate.

DEFINITION 2.15. *Let* $\to \subseteq T_\Sigma(X) \times T_\Sigma(X)$ be a binary relation on $T_\Sigma(X)$. We say that $\to$ is *Church–Rosser* iff for all $t_1, t_2 \in T_\Sigma(X)$, if $t_1 \overset{*}{\leftrightarrow} t_2$, then there is some $t_3 \in T_\Sigma(X)$ such that $t_1 \overset{*}{\to} t_3$ and $t_2 \overset{*}{\to} t_3$. We say that $\to$ is *confluent* iff for all $t, t_1, t_2 \in T_\Sigma(X)$, if $t \overset{*}{\to} t_1$ and $t \overset{*}{\to} t_2$, then there is some $t_3 \in T_\Sigma(X)$ such that $t_1 \overset{*}{\to} t_3$ and $t_2 \overset{*}{\to} t_3$. A term s is *irreducible* w.r.t. $\to$ iff there is no term t such that $s \to t$.

Given a set R of rewrite rules, we say that R *is reduced* iff

(1) no left-hand side of any rewrite rule $l \to r \in R$ is reducible by any rewrite rule in $R - \{l \to r\}$;

(2) no right-hand side of any rewrite rule $l \to r \in R$ is reducible by any rewrite rule in R.

Given two sets R and R' of rewrite rules, we say that R and R' are *equivalent* iff for every two terms u and v, $u \overset{*}{\leftrightarrow}_R v$ iff $u \overset{*}{\leftrightarrow}_{R'} v$.

It is well known that a relation is confluent iff it is Church–Rosser [16]. We say that a rewrite system R is Noetherian, Church–Rosser, or confluent, iff the relation $\to_R$ associated with R given in Definition 2.14 has the corresponding property. We say that R is *canonical* iff it is Noetherian and confluent.

3. Most General Unifiers in Triangular Form

We now review the fundamental notion of a unifier and some of its basic properties. It is convenient to discuss unification in the framework of term systems, as in Martelli and Montanari [22], and already anticipated by Herbrand in his thesis [15].

DEFINITION 3.1. A *term pair* (or *pair*) is just a pair of two terms, denoted by $\langle s, t \rangle$, and a substitution θ is called a *unifier* of a pair $\langle s, t \rangle$

if $\theta(s) = \theta(t)$. A *term system* (or *system*) is a set of such pairs, and a substitution θ is a unifier of a system if it unifies each pair.

DEFINITION 3.2. A substitution σ is an (*idempotent*) *most general unifier*, or *mgu*, of a system S iff

(i) $D(\sigma) \subseteq \mathrm{Var}(S)$ and $D(\sigma) \cap I(\sigma) = \varnothing$ (σ is idempotent);

(ii) σ is a unifier of S;

(iii) for every unifier θ of S, $\sigma \leqslant \theta$ (that is, $\theta = \sigma; \eta$ for some η).

In order to show that our decision procedure is in NP, we will need the fact that if two terms u and v are unifiable, a mgu of u and v can be represented concisely in triangular form (the size of this system is linear in the number of symbols in u and v). This result can be obtained from the fast method using multiequations of Martelli and Montanari [22] or the fast method using the graph unification closure of Paterson and Wegman [25].

DEFINITION 3.3. Given an idempotent substitution σ (i.e., $D(\sigma) \cap I(\sigma) = \varnothing$) with domain $D(\sigma) = \{x_1, ..., x_k\}$, a *triangular form for* σ is a finite set T of pairs $\langle x, t \rangle$, where $x \in D(\sigma)$ and t is a term, such that this set T can be sorted (possibly in more than one way) into a sequence $\langle \langle x_1, t_1 \rangle, ..., \langle x_k, t_k \rangle \rangle$ satisfying the following properties: for every i, $1 \leqslant i \leqslant k$,

(1) $\{x_1, ..., x_i\} \cap \mathrm{Var}(t_i) = \varnothing$, and

(2) $\sigma = [t_1/x_1]; ...; [t_k/x_k]$.

The set of variables $\{x_1, ..., x_k\}$ is called the *domain* of T. Note, in particular, that $x_i \notin \mathrm{Var}(t_i)$ for every i, $1 \leqslant i \leqslant k$, but variables in the set $\{x_{i+1}, ..., x_k\}$ may occur in $t_1, ..., t_i$.

By successively eliminating the variables $x_2, x_3, ..., x_k$, it is easily seen that σ is an (idempotent) mgu of the term system T. As a consequence, if σ is an idempotent mgu of a system S, and T is a triangular form for σ, the systems S and T have exactly the same set of unifiers (because σ is a mgu of both S and T).

EXAMPLE 3.4. Consider the substitution $\sigma = [f(f(x_3, x_3), f(x_3, x_3))/x_1, f(x_3, x_3)/x_2]$. The system $T = \{\langle x_1, f(x_2, x_2)\rangle, \langle x_2, f(x_3, x_3)\rangle\}$ is a triangular form of σ since it can be ordered as $\langle \langle x_1, f(x_2, x_2)\rangle, \langle x_2, f(x_3, x_3)\rangle \rangle$ and $\sigma = [f(x_2, x_2)/x_1]; [f(x_3, x_3)/x_2]$.

The triangular form $T = \{\langle x_1, t_1 \rangle, ..., \langle x_k, t_k \rangle\}$ of a substitution σ also defines a substitution, namely $\sigma_T = [t_1/x_1, ..., t_k/x_k]$. This substitution is

usually different from σ and not idempotent as can be seen from Example 3.4. However, the substitution plays a crucial role in our decision procedure because of the following property.

LEMMA 3.5. *Given a triangular form* $T = \{\langle x_1, t_1\rangle, ..., \langle x_k, t_k\rangle\}$ *for a substitution* σ *and the associated substitution* $\sigma_T = [t_1/x_1, ..., t_k/x_k]$, *for every unifier* θ *of* T, $\theta = \sigma_T; \theta$.

Proof. Since θ is a unifier of T, we have $\theta(x_i) = \theta(t_i) = \theta(\sigma_T(x_i))$ for every i, $1 \leqslant i \leqslant k$. Since $\sigma_T(y) = y$ for all $y \notin \{x_1, ..., x_k\}$, $\theta = \sigma_T; \theta$ holds. ∎

Another important observation about σ_T is that even though it is usually not idempotent, at least one variable in $\{x_1, ..., x_k\}$ does not belong to $I(\sigma_T)$ (otherwise, condition (1) of the triangular form fails). We will assume that a procedure TU is available, which, given any unifiable term system S, returns a triangular form for an idempotent mgu of S, denoted by $TU(S)$. When S consists of a single pair $\langle u, v\rangle$, $TU(S)$ is also denoted by $TYU(u, v)$.

4. COMPLETE SETS OF RIGID E-UNIFIERS

We begin with the definition of a rigid E-unifier.

DEFINITION 4.1. Let $E = \{(s_1 \doteq t_1), ..., (s_m \doteq t_m)\}$ be a finite set of equations, and let $\mathrm{Var}(E) = \bigcup_{(s \doteq t) \in E} \mathrm{Var}(s \doteq t)$ denote the set of variables occurring in E.[6] Given a substitution θ, we let $\theta(E) = \{\theta(s_i \doteq t_i) \mid s_i \doteq t_i \in E,\ \theta(s_i) \neq \theta(t_i)\}$. Given any two terms u and v,[7] a substitution θ is a *rigid unifier of* u *and* v *modulo* E (for short, a *rigid* E*-unifier of* u *and* v) iff

> $\theta(u) \overset{*}{\cong}_{\theta(E)} \theta(v)$, that is, $\theta(u)$ and $\theta(v)$ are congruent modulo the set $\theta(E)$ considered as a set of *ground* equations.

Note that a rigid E-unifier is an E-unifier, but the converse is not true. We will also need some definitions regarding complete sets of rigid E-unifiers. First, we need to define some preorders on substitutions.

DEFINITION 4.2. Let E be a (finite) set of equations, and W a (finite) set of variables. For any two substitutions σ and θ $\sigma =_E \theta[W]$ iff $\sigma(x) \overset{*}{\cong}_E \theta(x)$ for every $x \in W$. The relation $\sqsubseteq_E$ is defined as follows. For any two substitutions σ and θ, $\sigma \sqsubseteq_E \theta[W]$ iff $\sigma =_{\theta(E)} \theta[W]$. The set W is omitted when

[6] It is possible that equations have variables in common.

[7] It is possible that u and v have variables in common with the equations in E.

$W = X$ (where X is the set of variables), and similarly E is omitted when $E = \varnothing$.

Intuitively speaking, $\sigma \sqsubseteq_E \theta$ iff σ can be generated from θ using the equations in $\theta(E)$. Clearly, $\sqsubseteq_E$ is reflexive. However, it is not symmetric, as shown by the following example.

EXAMPLE 4.3. *Let* $E = \{fx \doteq x\}$, $\sigma = [fa/x]$, and $\theta = [a/x]$. Then $\theta(E) = \{fa \doteq a\}$ and $\sigma(x) = fa \overset{*}{\cong}_{\theta(E)} a = \theta(x)$, and so $\sigma \sqsubseteq_E \theta$. On the other hand $\sigma(E) = \{ffa \doteq fa\}$, but a and fa are not congruent from $\{ffa \doteq fa\}$. Thus $\theta \sqsubseteq_E \sigma$ *does not* hold.

Some positive facts about the relation $\sqsubseteq_E$ are shown in the following lemma, transitivity in particular.

LEMMA 4.4. (i) *For any two substitutions* σ, θ, *if* $\sigma =_{\theta(E)} \theta$, *then* $\sigma(u) \overset{*}{\cong}_{\theta(E)} \theta(u)$ *for any term* u. (ii) *If* $\sigma =_{\theta(E)} \theta$, *then for all terms* u, v, *if* $u \overset{*}{\cong}_{\sigma(E)} v$ then $u \overset{*}{\cong}_{\theta(E)} v$. (iii) $\sqsubseteq_E$ *is transitive.* (iv) *For any two terms* u, v, *and any substitution* θ, *if* $u \overset{*}{\cong}_E v$ *then* $\theta(u) \overset{*}{\cong}_{\theta(E)} \theta(u)$.

Proof. An easy induction on terms yields (i). To show (ii), it is sufficient to show that $\sigma(l) \overset{*}{\cong}_{\theta(E)} \sigma(r)$ for every $l \doteq r \in E$. By (i), since $\sigma =_{\theta(E)} \theta$, we have $\sigma(l) \overset{*}{\cong}_{\theta(E)} \theta(l)$ and $\sigma(r) \overset{*}{\cong}_{\theta(E)} \theta(r)$. Since $l \doteq r \in E$, we have $\sigma(l) \overset{*}{\cong}_{\theta(E)} \sigma(r)$, proving (ii). Assume that, $\theta_1 =_{\theta_2(E)} \theta_2$ and $\theta_2 =_{\theta_3(E)} \theta_3$. Since $\theta_2 =_{\theta_3(E)} \theta_3$ and $\theta_1(x) \overset{*}{\cong}_{\theta_2(E)} \theta_2(x)$ for every variable x, by (ii), we have $\theta_1(x) \overset{*}{\cong}_{\theta_3(E)} \theta_2(x)$. Since we also have $\theta_2(x) \overset{*}{\cong}_{\theta_3(E)} \theta_3(x)$, by transitivity we have $\theta_1(x) \overset{*}{\cong}_{\theta_3(E)} \theta_3(x)$. Thus, $\theta_1 =_{\theta_3(E)} \theta_3$, establishing the transitivity of $\sqsubseteq_E$. Part (iv) is verified easily. ∎

Thus, by (iii), $\sqsubseteq_E$ is a preorder. By (i) and (ii), it is immediately verified that if σ is a rigid E-unifier of u and v and $\sigma \sqsubseteq_E \theta$, then θ is a rigid E-unifier of u and v. The converse is false, as shown by the following example.

EXAMPLE 4.5. Let $E = \{fx \doteq x\}$, $\sigma = [fa/x]$, $\theta = [a/x]$, and $\langle u, v \rangle = \langle a, fa \rangle$. Since $\theta(E) = \{fa \doteq a\}$, it is clear that θ is a rigid E-unifier of a and fa. But $\sigma(E) = \{ffa \doteq fa\}$ and a and fa are not congruent from $\{ffa \doteq fa\}$. Hence, σ is not a rigid E-unifier of a and fa.

We also need an extension of $\sqsubseteq_E$ defined as follows.

DEFINITION 4.6. Let E be a (finite) set of equations, and W a (finite) set of variables. The relation $\leqslant_E$ is defined as follows: for any two substitutions σ and θ, $\sigma \leqslant_E \theta[W]$ iff $\sigma; \eta \sqsubseteq_E \theta[W]$ for some substitution η (that is, $\sigma; \eta =_{\theta(E)} \theta[W]$ for some η). The conventions for omitting $[W]$ and E are those of Definition 4.2.

Intuitively speaking, $\sigma \leqslant_E \theta$ iff σ is more general than some substitution

that can be generated from θ using $\theta(E)$. Clearly, $\leqslant_E$ is reflexive. The transitivity of $\leqslant_E$ is shown in the next lemma.

LEMMA 4.7. *The relation $\leqslant_E$ is transitive.*

Proof. Assume that $\theta_1 \leqslant_E \theta_2$ and $\theta_2 \leqslant_E \theta_3$. By the definition of $\leqslant_E$, we have some η_1 and η_2 such that $\theta_1; \eta_1 =_{\theta_2(E)} \theta_2$ and $\theta_2; \eta_2 =_{\theta_3(E)} \theta_3$. By part (iv) of Lemma 4.4, $\theta_1; \eta_1 =_{\theta_2(E)} \theta_2$ implies $\theta_1; \eta_1; \eta_2 =_{\eta_2(\theta_2(E))} \theta_2; \eta_2$. Thus, we have $\theta_1; \eta_1; \eta_2 \sqsubseteq_E \theta_2; \eta_2$, and since $\theta_2; \eta_2 \sqsubseteq_E \theta_3$, by transitivity of $\sqsubseteq_E$, we have $\theta_1; \eta_1; \eta_2 \sqsubseteq_E \theta_3$, that is, $\theta_1 \leqslant_E \theta_3$. ∎

Thus, $\leqslant_E$ is a preorder, and it is clear that it extends $\sqsubseteq_E$. When $\sigma \leqslant_E \theta[W]$, we say that σ *is (rigid) more general than* θ *over* W. By the remark following the proof of Lemma 4.4 and part (iv) of Lemma 4.4, it is immediately verified that if σ is a rigid E-unifier of u and v and $\sigma \leqslant_E \theta$, then θ is a rigid E-unifier of u and v. From Example 4.5, the converse is false.

In the next definition, the concept of a most general unifier is generalized to rigid E-unifiers. Unlike standard unification, it is necessary to consider a set of substitutions.

DEFINITION 4.8. Given a (finite) set E of equations, for any two terms u and v, letting $V = \mathrm{Var}(u) \cup \mathrm{Var}(v) \cup \mathrm{Var}(E)$, a set U of substitutions is a *complete set of rigid E-unifiers for u and v* iff: For every $\sigma \in U$,

(i) $D(\sigma) \subseteq V$ and $D(\sigma) \cap I(\sigma) = \varnothing$ (idempotence);

(ii) σ is a rigid E-unifier of u and v;

(iii) for every rigid E-unifier θ of u and v, there is some $\sigma \in U$ such that $\sigma \leqslant_E \theta[V]$.

Condition (i) is the *purity condition*, condition (ii) the *consistency condition*, and condition (iii) the *completeness condition.*

By the remark following the proof of Lemma 4.7, if U is a complete set of rigid E-unifiers for u and v, $\sigma \in U$, and $\sigma \leqslant_E \theta$, then θ is a rigid E-unifier of u and v.

It is very useful to observe that if a procedure P for finding sets of rigid E-unifiers satisfies the property stated in Definition 4.9, given next, then in order to show that this procedure yields complete sets, there is no loss of generality in showing completeness with respect to *ground* rigid E-unifiers whose domains contain V (that is, in clause (iii) of Definition 4.8, $\theta(x)$ is a ground term for every $x \in D(\theta)$, and $V \subseteq D(\theta)$).

DEFINITION 4.9. A procedure P for finding sets of rigid E-unifiers is *pure* iff the following condition holds: For every ranked alphabet Σ, every

finite set E of equations over $T_\Sigma(X)$ and every u, $v \in T_\Sigma(X)$, if $U = P(E, u, v)$ is the set of rigid E-unifiers for u and v given by procedure P, then for every $\sigma \in U$, for every $x \in D(\sigma)$, every constant or function symbol occurring in $\sigma(x)$ occurs either in some equation in E or in u or in v.

In other words, $P(E, u, v)$ does not contain constant or function symbols that do not already occur in the input (E, u, v). To prove our claim, we proceed as follows. We add countably infinitely many new (distinct) constants c_x to Σ, each constant c_x being associated with the variable x. The resulting alphabet is denoted by Σ_{SK}. If θ is not ground, we create the Skolemized version of θ, that is, the substitution $\hat{\theta}$ obtained by replacing the variables in the terms $\theta(x)$ by new (distinct) constants.[8]

LEMMA 4.10. *Given a rigid E-unification procedure P satisfying the property of Definition* 4.9, *assume that for every ranked alphabet* Σ, *every finite set E of equations over* $T_\Sigma(X)$ *and every* u, $v \in T_\Sigma(X)$, *the set* $U = P(E, u, v)$ *of rigid E-unifiers of u and v given by P satisfies conditions* (i) *and* (ii) *of Definition* 4.8, *and the new condition* (iii'): *for every rigid E-unifier* θ *of u and v such that* $V \subseteq D(\theta)$ *and* $\theta(x) \in T_\Sigma$ *for every* $x \in D(\theta)$, *there is some* $\sigma \in U$ *such that* $\sigma \leqslant_E \theta[V]$ (*where* $V = \mathrm{Var}(E) \cup \mathrm{Var}(u, v)$). *Then every set* $U = P(E, u, v)$ *is a complete set of rigid E-unifiers for u and v.*

Proof. Let θ be any rigid E-unifier of u and v over $T_\Sigma(X)$. If $D(\theta)$ does not contain V, extend θ such that $\theta(y) = c_y$ for every $y \in V - D(\theta)$, and let $\hat{\theta}$ be the Skolemized version of this extension of θ. We are now considering the extended alphabet Σ_{SK}. It is immediately verified that $\hat{\theta}$ is also a rigid E-unifier of u and v such that $V \subseteq D(\hat{\theta})$ and $\hat{\theta}(x) \in T_{\Sigma_{\mathrm{SK}}}$ for all $x \in D(\hat{\theta})$. Then, there is some $\sigma \in U$ such that $\sigma \leqslant_E \hat{\theta}[V]$, which means that there is some substitution η (over $T_{\Sigma_{\mathrm{SK}}}(X)$) such that $\sigma; \eta \overset{*}{\cong}_{\hat{\theta}(E)} \hat{\theta}[V]$. Note that by the property of Definition 4.9, since E, u, and v do not contain Skolem constants, σ does not contain Skolem constants. Let η' be obtained from η by changing each Skolem constant back to the corresponding variable. Since σ does not contain Skolem constants, it is immediately verified that $\sigma; \eta' \overset{*}{\cong}_{\theta(E)} \theta[V]$. Thus, the set U is a complete set of rigid E-unifiers for u and v over $T_\Sigma(X)$. ∎

5. MINIMAL RIGID E-UNIFIERS

Given a finite or countably infinite ranked alphabet Σ, it is always possible to define a total simplification ordering $\preccurlyeq$ on T_Σ (the set of

[8] That is, $\hat{\theta}$ is obtained from θ by replacing every variable y in each term $\theta(x)$ by the corresponding Skolem constant c_y, for each $x \in D(\theta)$.

all ground terms). For instance, we can choose some total well-founded ordering $\preccurlyeq$ on Σ and extend $\preccurlyeq$ to T_Σ as follows: $s \prec t$ iff either

(1) $\text{size}(s) < \text{size}(t)$, or

(2) $\text{size}(s) = \text{size}(t)$ and $\text{Root}(s) \prec \text{Root}(t)$, or

(3) $\text{size}(s) = \text{size}(t)$, $\text{Root}(s) = \text{Root}(t)$, and letting $s = fs_1 \cdots s_n$ and $t = ft_1 \cdots t_n$, $\langle s_1, ..., s_n \rangle \prec_{\text{lex}} \langle t_1, ..., t_n \rangle$, where $\prec_{\text{lex}}$ is the lexicographic ordering induced by $\prec$.

In the rest of this paper, we assume that $\preccurlyeq$ is a fixed simplification ordering which is total on T_Σ. We shall use the total simplification ordering $\prec$ on T_Σ to define a well-founded partial order $\lessdot$ on ground substitutions. For this, it is assumed that the set of variables X is totally ordered as $X = \langle x_1, x_2, ..., x_n, ... \rangle$.

DEFINITION 5.1. The partial order $\lessdot$ is defined on ground substitutions as follows. Given any two ground substitutions σ and θ such that $D(\sigma) = D(\theta)$, letting $\langle y_1, ..., y_n \rangle$ be the sequence obtained by ordering the variables in $D(\sigma)$ according to their order in X, then $\sigma \lessdot \theta$ iff

$$\langle \sigma(y_1), ..., \sigma(y_n) \rangle \preccurlyeq_{\text{lex}} \langle \theta(y_1), ..., \theta(y_n) \rangle,$$

where $\preccurlyeq_{\text{lex}}$ is the lexicographic ordering on tuples induced by $\preccurlyeq$.

Since $\preccurlyeq$ is well founded and $\preccurlyeq$ is induced by the lexicographic ordering $\preccurlyeq_{\text{lex}}$ which is well founded, $\lessdot$ is also well founded. In fact, given any finite set V of variables, note that $\lessdot$ is a total well-founded ordering for the set of ground substitutions with domain V.

Given a set E of equations and a total simplification ordering $\preccurlyeq$ on ground terms, for any ground substitution θ, we let $\theta(E)$ denote the set $\{\theta(l) \doteq \theta(r) \mid \theta(l) \succ \theta(r), l \doteq r \in E \cup E^{-1}\}$ of oriented instances of E. Thus, we can also view $\theta(E)$ as a set of rewrite rules.

The reason for considering the well-founded order $\lessdot$ on ground substitutions is that minimal rigid E-unifiers exist. This is one of the reasons for the decidability of rigid E-unification. The example below gives some motivation for the next definition and lemma.

EXAMPLE 5.2. Let $E = \{fa \doteq a, ggx \doteq fa\}$, and $\langle u, v \rangle = \langle gggx, x \rangle$. It is obvious that there is a simplification ordering total on ground terms such that $a \prec f \prec g$. The main point of this example is the fact that some rigid E-unifiers of $gggx$ and x are redundant, in the sense that they are subsumed by rigid E-unifiers that are smaller w.r.t. $\leqslant_E$. For instance, $\theta = [gf^{10}a/x]$ is a rigid E-unifier of $gggx$ and x, but so is $\sigma = [ga/x]$, and $\sigma \sqsubseteq_E \theta$.

An illustration of the redundancy of θ is the fact that $\theta(x) = gf^{10}a$ is reducible by the rule $fa \to a$. The fact that some term $\theta(x)$ may be reducible by some oriented instance $\theta(l) \to \theta(r)$ of an equation $l \doteq r \in E \cup E^{-1}$ turns out to be a problem for the completeness of the method. In order to avoid such redundancies, for every rigid E-unifier θ of u and v, we consider the set $S_{E,u,v,\theta}$ of all ground rigid E-unifiers ρ of u and v such that $\rho \sqsubseteq_E \theta$ and $D(\rho) = D(\theta)$. The crucial fact is that the set $S_{E,u,v,\theta}$ has a smallest element σ under the ordering $\lll$, and that this least substitution is nicely reduced w.r.t. $\sigma(E)$. Intuitively speaking, we find the least ground rigid E-unifier σ of u and v constructible from θ and $\theta(E)$ (least w.r.t. $\lll$). Referring back to $\theta = [gf^{10}a/x]$, the substitution $\sigma = [ga/x]$ is the smallest element of $S_{E,u,v,\theta}$. In general, it is not sufficient simply to consider all ground substitutions ρ such that $\rho \sqsubseteq_E \theta$, because some of them may not be rigid E-unifiers of u and v. For instance, for $E = \{fa \doteq a,\ x \doteq fa\}$, and $\langle u, v\rangle = \langle gx, x\rangle$, $\theta = [ga/x]$ is a rigid E-unifier of gx and x, we have $\rho \sqsubseteq_E \theta$ for $\rho = [a/x]$, but ρ is not a rigid E-unifier of ga and a since $\rho(E) = \{fa \doteq a\}$. Thus, we have to consider rigid E-unifiers of u and v such that $\rho \sqsubseteq_E \theta$.

The least element σ of the set $S_{E,u,v,\theta}$ enjoys some nice reduction properties w.r.t. $\sigma(E)$. These properties, stated in the forthcoming lemma, will be used in the proof that the method is complete.

DEFINITION 5.3. Let E be a set of equations (over $T_\Sigma(X)$) and u, $v \in T_\Sigma(X)$ any two terms. For any ground rigid E-unifier θ of u and v, let

$$S_{E,u,v,\theta} = \{\rho \mid D(\rho) = D(\theta),\ \rho(u) \overset{*}{\cong}_{\rho(E)} \rho(v),\ \rho \sqsubseteq_E \theta, \text{ and } \rho \text{ ground}\}.$$

Obviously, $\theta \in S_{E,u,v,\theta}$, so $S_{E,u,v,\theta}$ is not empty. Since $\lll$ is total and well founded on ground substitutions with domain $D(\theta)$, the set $S_{E,u,v,\theta}$ contains some least element σ (w.r.t. $\lll$).

We shall now prove the following crucial result. For this, recall that a *degenerate equation* is of the form $x \doteq t$, where x is a variable and $x \notin \mathrm{Var}(t)$, and that a *nondegenerate equation* is not a degenerate equation.

LEMMA 5.4. *Let E be a set of equations (over $T_\Sigma(X)$) and u, $v \in T_\Sigma(X)$ any two terms. For any ground rigid E-unifier θ of u and v, if σ is the least element of the set $S_{E,u,v,\theta}$ of Definition 5.3, then the following properties hold:*

(1) *Every term of the form $\sigma(x)$ is irreducible by every oriented instance $\sigma(l) \to \sigma(r)$ of a nondegenerate equation $l \doteq r \in E \cup E^{-1}$, and*

(2) *every proper subterm of a term of the form $\sigma(x)$ is irreducible by every oriented instance $\sigma(l) \to \sigma(r)$ of a degenerate equation $l \doteq r \in E \cup E^{-1}$.*

Proof. To prove that σ has the desired properties, we proceed by contradiction. Assume that some subterm of a term of the form $\sigma(x)$ is reducible by some oriented instance $\sigma(l) \to \sigma(r)$ of an equation $l \doteq r \in E \cup E^{-1}$. Hence, $\sigma(x)/\beta = \sigma(l)$ for some address β in $\sigma(x)$ and $\sigma(l) \succ \sigma(r)$. In order to prove that $x \notin \mathrm{Var}(l, r)$ if either $l \doteq r$ is nondegenerate or $l \doteq r$ is degenerate and $\beta \neq \varepsilon$, we prove the following claim.

Claim. (i) $\sigma(y) \prec \sigma(x)$ for every $y \in \mathrm{Var}(r)$. (ii) $\sigma(y) \prec \sigma(x)$ for every $y \in \mathrm{Var}(l)$ if $l \doteq r$ is nondegenerate. (iii) $\sigma(l) \prec \sigma(x)$ if $\beta \neq \varepsilon$ and $l \doteq r$ is degenerate.

Proof of Claim. Since $\prec$ is a simplification ordering, by the subterm property, $\sigma(y) \preccurlyeq \sigma(r)$ for each $y \in \mathrm{Var}(r)$, and since $\sigma(l) \succ \sigma(r)$, we have $\sigma(y) \prec \sigma(l)$ for each $y \in \mathrm{Var}(r)$. Since $\sigma(l)$ is a subterm of $\sigma(x)$, $\sigma(l) \preccurlyeq \sigma(x)$, and we also have $\sigma(y) \prec \sigma(x)$ for each $y \in \mathrm{Var}(r)$. This proves (i). Next, we show that if $l \doteq r$ is nondegenerate, then l cannot be a variable. For the sake of contradiction, assume that $l = z$ for some variable z. If $z \in \mathrm{Var}(r)$, then $\sigma(r) \succ \sigma(z)$ by the subterm property, contradicting the assumption that $\sigma(z) \succ \sigma(r)$. But then $z \doteq r$ is degenerate, a contradiction. Now if $l \doteq r$ is nondegenerate, since l is not a variable, by the subterm property, we have $\sigma(y) \prec \sigma(l)$ for each $y \in \mathrm{Var}(l)$, and since $\sigma(l)$ is a subterm of $\sigma(x)$, $\sigma(l) \preccurlyeq \sigma(x)$, which implies $\sigma(y) \prec \sigma(x)$ for each $y \in \mathrm{Var}(l)$, showing (ii). If $l \doteq r$ is degenerate, and $\beta \neq \varepsilon$, then $l = y$ for some variable y and $\sigma(y)$ is a proper subterm of $\sigma(x)$, and so $\sigma(y) \prec \sigma(x)$, proving (iii). This concludes the proof of the claim. ∎

It is clear that the claim implies that $x \notin \mathrm{Var}(l, r)$ if either $l \doteq r$ is nondegenerate or $l \doteq r$ is degenerate and $\beta \neq \varepsilon$. We now form a new substitution σ' that will contradict the minimality of σ. We define σ' such that

$$\sigma'(y) = \begin{cases} \sigma(y), & \text{if } y \in D(\sigma) - \{x\}; \\ \sigma(x)[\beta \leftarrow \sigma(r)], & \text{if } y = x. \end{cases}$$

Since $\sigma(l) \succ \sigma(r)$ and $\sigma(x)/\beta = \sigma(l)$, by monotonicity of $\prec$, we have $\sigma'(x) \prec \sigma(x)$ and

$$\sigma(x) \to_{[\beta, \sigma(l) \to \sigma(r)]} \sigma'(x). \qquad (*)$$

By the definition of σ' and since $\sigma'(x) \prec \sigma(x)$, we have $\sigma' \ll \sigma$. Since by the hypothesis $\sigma =_{\theta(E)} \theta$, by Lemma 4.4, $\sigma(l) \overset{*}{\cong}_{\theta(E)} \theta(l)$ and $\sigma(r) \overset{*}{\cong}_{\theta(E)} \theta(r)$, and by $(*)$ and the fact that $l \doteq r \in E \cup E^{-1}$, we have $\sigma'(x) \overset{*}{\cong}_{\theta(E)} \sigma(x)$. Since $\sigma(y) \overset{*}{\cong}_{\theta(E)} \theta(y)$ and $\sigma'(y) = \sigma(y)$ for all $y \in D(\theta) - \{x\}$, we have $\sigma' =_{\theta(E)} \theta$. Since $x \notin \mathrm{Var}(l, r)$, $\sigma'(l) = \sigma(l)$, $\sigma'(r) = \sigma(r)$, and it is easy to see that $\sigma'(u)$ and $\sigma'(v)$ are congruent modulo the set of ground equations $\sigma'(E)$. (The equation $\sigma'(l) \doteq \sigma'(r)$, which is identical to $\sigma(l) \doteq \sigma(r)$ since $\sigma'(l) = \sigma(l)$

and $\sigma'(r) = \sigma(r)$, can be used to go from $\sigma'(x)$ to $\sigma(x)$ and conversely whenever necessary.) Hence, $\sigma' =_{\theta(E)} \theta$, $\sigma' \ll \sigma$, and σ' is a rigid E-unifier of u and v, which contradicts the minimality of σ. This concludes the proof. ∎

In view of Lemma 5.4, it is convenient to introduce the following definition.

DEFINITION 5.5. Given a set E of equations, a total simplification ordering $\preccurlyeq$ on ground terms, and any two terms u, v, a ground rigid E-unifier θ of u and v is *reduced w.r.t.* $\theta(E)$ iff

(1) every term of the form $\theta(x)$ is irreducible by every oriented instance $\theta(l) \to \theta(r)$ of a nondegenerate equation $l \doteq r \in E \cup E^{-1}$, and

(2) every proper subterm of a term of the form $\theta(x)$ is irreducible by every oriented instance $\theta(l) \to \theta(r)$ of a degenerate equation $l \doteq r \in E \cup E^{-1}$.

Thus, Lemma 5.4 asserts that two terms u, v have a rigid E-unifier if they have a rigid minimal (w.r.t. $\ll$) E-unifier θ that is reduced w.r.t. $\theta(E)$. Consequently it is sufficient to search for such rigid E-unifiers.

6. THE REDUCTION PROCEDURE

One of the major components of the decision procedure for rigid E-unification is a procedure for creating a reduced set of rewrite rules equivalent to a given (finite) set of ground equations. This procedure, first presented by Gallier *et al.* [11], runs in polynomial time. However, due to the possibility that variables may occur in the equations, we have to make some changes to this procedure. Roughly speaking, given a "guess" $\mathcal{O}$ (which we call an *order assignment*) of the ordering among all subterms of the terms in a set of equations E, we can run the reduction procedure R on E and $\mathcal{O}$ to produce a reduced rewrite system $R(E, \mathcal{O})$ equivalent to E, and whose orientation is dictated by the ordering $\mathcal{O}$. First, we need a few definitions.

DEFINITION 6.1. Given a set R of rewrite rules, we say that R is *rigid reduced* iff

(1) no left-hand side of any rewrite rule $l \to r \in R$ is reducible by any rewrite rule in $R - \{l \to r\}$ treated as a ground rule;

(2) no right-hand side of any rewrite rule $l \to r \in R$ is reducible by any rewrite rule in R treated as a ground rule.

DEFINITION 6.2. Given two sets E and E' of equations, we say that E and E' are *rigid equivalent* iff for every two terms u and b, $u \overset{*}{\cong}_E v$ iff $u \overset{*}{\cong}_{E'} v$ (treating E and E' as sets of ground equations).

It is clear that if E and E' are rigid equivalent, then for every substitution θ, $\theta(E)$ and $\theta(E')$ are rigid equivalent.

For technical reasons, it will be convenient to view the problem of rigid E-unification as the problem of deciding whether two fixed constants are rigid E-unifiable. This can be achieved as follows (the idea is borrowed from Dershowitz). Let eq be a new binary function symbol not occurring in Σ, and T and F two new constants not occurring in Σ. The following simple but useful lemma holds.

LEMMA 6.3. *Given a set E of equations and any two terms u and v, a substitution θ over $T_\Sigma(X)$ is a rigid E-unifier of u and v iff there is some substitution θ' over $T_\Sigma(X)$ such that $\theta = \theta'|_{D(\theta')-\{z\}}$ and $T \overset{*}{\cong}_{\theta'(E_{u,v})} F$, where $E_{u,v} = E \cup \{eq(u,v) \doteq F,\ eq(z,z) \doteq T\}$, and z is a new variable not in* $\mathrm{Var}(E) \cup \mathrm{Var}(u, v)$.

Proof. If a substitution θ over $T_\Sigma(X)$ is a rigid E-unifier of u and v, then $\theta(u) \overset{*}{\cong}_{\theta(E)} \theta(v)$, and extending θ' such that $\theta'(z) = \theta(u)$, since $\theta(eq(u, v)) \overset{*}{\cong}_{\theta(E)} eq(\theta(u), \theta(u))$, clearly

$$\begin{aligned} F &\overset{*}{\cong}_{\theta'(E_{u,v})} \theta'(eq(u, v)) \\ &\overset{*}{\cong}_{\theta'(E_{u,v})} \theta'(eq(z, z)) \\ &\overset{*}{\cong}_{\theta'(E_{u,v})} T. \end{aligned}$$

Conversely, if there is some substitution θ' over $T_\Sigma(X)$ such that $T \overset{*}{\cong}_{\theta'(E_{u,v})} F$, because eq, T, F are not in Σ, from the way congruence closure works, it must be the case that $\theta'(eq(z, z)) \overset{*}{\cong}_{\theta'(E_{u,v})} \theta'(eq(u, v))$. Letting $\theta = \theta'|_{D(\theta')-\{z\}}$, since θ' is over $T_\Sigma(X)$ and eq, T, F are not in Σ, we must also have $\theta'(z) \overset{*}{\cong}_{\theta(E)} \theta(u)$ and $\theta'(z) \overset{*}{\cong}_{\theta(E)} \theta(v)$. Thus $\theta(u) \overset{*}{\cong}_{\theta(E)} \theta(v)$, showing that θ is a rigid E-unifier of u and v. ∎

We also need to extend the total simplification ordering $\preccurlyeq$ so that T, F, and terms involving eq can be compared. Actually, it is not necessary to consider arbitrary terms containing eq, and we extend $\prec$ to the set $T_\Sigma \cup \{T, F\} \cup \{eq(u, v) \mid u, v \in T_\Sigma\}$ as follows:

For any terms s, t, u, $v \in T_\Sigma$,

(a) $T \prec F \prec u \prec eq(s, t)$; and

(b) $eq(s, t) \prec eq(u, v)$ iff $\{s, t\} \prec_{\mathrm{lex}} \{u, v\}$, where $\prec_{\mathrm{lex}}$ is the lexicographic extension of $\prec$ to pairs.

It is clear that we have defined a total simplification ordering on the set $T_\Sigma \cup \{T, F\} \cup \{eq(u, v) \mid u, v \in T_\Sigma\}$.

We will need to show that in searching for rigid E-unifiers, it is always possible to deal with sets of equations that are rigid reduced. The proof of this fact uses the result, shown elsewhere, that every finite set E of ground equations is equivalent to a reduced set $R(E)$ of rewrite rules. We now review the procedure first presented by Gallier *et al.* [11], which, given a total simplification ordering $\prec$ on ground terms and a finite set E of ground equations, returns a reduced rewrite system $R(E)$ equivalent to E.

DEFINITION 6.4 (Basic reduction procedure). Let E be a finite set of ground equations, and $\prec$ a simplification ordering total on ground terms. The basic reduction procedure generates a finite sequence of triples $\langle \mathscr{E}_i, \Pi_i, \mathscr{R}_i \rangle$, where $\mathscr{E}_i$ is a finite set of ground equations, Π_i is a partition (associated with $\mathscr{E}_i$), and $\mathscr{R}_i$ is a set of ground rewrite rules. Given a triple $\langle \mathscr{E}_i, \Pi_i, \mathscr{R}_i \rangle$, we let $\mathscr{T}_i$ be the set of all subterms of terms occurring in equations in $\mathscr{E}_i$ or in rewrite rules in $\mathscr{R}_i$. The procedure makes use of the *congruence closure* of a finite set of ground equations (Kozen [19, 20], Nelson and Oppen [24], Downey, Sethi, and Tarjan [8]). Congruence closures are represented by their associated partition Π. Given an equivalence relation represented by its partition Π, the equivalence class of t is denoted by $[t]_\Pi$, or $[t]$. Recall that s, t are in the same equivalence class of Π iff s and t are subterms of the terms occurring in E and $s \overset{*}{\leftrightarrow}_E t$ (for details, see Gallier [9]). The congruence closure algorithm will only be run once on E to obtain Π_0, but the partition Π_i may change due to further steps (simplification steps).

begin algorithm

Initially, we set $\mathscr{E}_0 = E$, $\mathscr{R}_0 = \varnothing$, and run a congruence closure algorithm on the ground set E to obtain Π_0. $i := 0$;

while Π_i has some nontrivial equivalence class[9] **do** {Simplification steps}

Let ρ_{i+1} be the smallest element[10] of the set

$$\bigcup_{C \in \Pi_i,\ |C| \geq 2} C$$

of terms belonging to nontrivial classes in Π_i.[11] Let C_{i+1} be the nontrivial class that contains ρ_{i+1}, and write $C_{i+1} =$

[9] That is, a class containing at least two elements, in which case $\mathscr{E}_i$ has at least one nontrivial equation.

[10] in the ordering $\prec$.

[11] where $|C|$ denotes the cardinality of the set C.

$\{\rho_{i+1}, \lambda_{i+1}^1, ..., \lambda_{i+1}^{k_{i+1}}\}$, where $k_{i+1} \geqslant 1$, since C_{i+1} is nontrivial. Let $\mathscr{S}_{i+1} = \{\lambda_{i+1}^1 \to \rho_{i+1}, ..., \lambda_{i+1}^{k_{i+1}} \to \rho_{i+1}\}$.

{Next, we use the rewrite rules in $\mathscr{S}_{i+1}$ to simplify the rewrite rules in $\mathscr{R}_i \cup \mathscr{S}_{i+1}$, the partition Π_i, and the equations in $\mathscr{E}_i$.}

To get $\mathscr{R}_{i+1}$, first, we get a canonical system equivalent to $\mathscr{S}_{i+1}$. For this, for every left-hand side λ of a rule in $\mathscr{S}_{i+1}$, replace every maximal redex of λ of the form λ^j by ρ. where $\lambda^j \to \rho \in \mathscr{S}_{i+1} - \{\lambda \to \rho\}$.[12] Let $\mathscr{S}'_{i+1}$ be the set of simplified rules. Also, let $\mathscr{R}'_{i+1}$ be the set obtained by simplifying the left-hand sides of rules in $\mathscr{R}_i$ using $\mathscr{S}_{i+1}$ (reducing maximal redexes only), and let

$$\mathscr{R}_{i+1} = \mathscr{R}'_{i+1} \cup \mathscr{S}'_{i+1}.$$

Finally, use $\mathscr{S}_{i+1}$ to simplify all terms in Π_i and $\mathscr{E}_i$, using the simplification process described earlier, to obtain Π_{i+1} and $\mathscr{E}_{i+1}$.

$i = i + 1$

endwhile

{All classes of Π_i are trivial, and the set $\mathscr{R}_i$ is a canonical system equivalent to E.}

end algorithm

It is shown in [11] that the above procedure always terminates with a system $\mathscr{R}_m$ equivalent to E that is reduced (and hence canonical).

However, in order to show later that our decision method is in NP, it turns out that we need a sharpening of the above result. We need to show that given a set E of ground equations, the term DAG associated with any equivalent reduced system R is of size no greater than the size of the term DAG associated with E itself, and that the number of rules in R is no greater than the number of equations in E. This is not at all obvious for our algorithm, but fortunately true. To be more specific, the *term DAG* associated with a finite set S of terms is the labeled directed graph whose set of noddes is the set of all subterms occurring in terms in S, where every constant symbol c or variable x is a terminal node labeled with c or x, and where every node $f(t_1, ..., t_k)$ is labeled with f and has exactly the k nodes $t_1, ..., t_k$ as immediate successors. In the case of a set of equations (or rewrite rules), the set of terms under consideration is the set of subterms occurring in left-hand or right-hand sides of equations (or rules). If a term DAG has m edges and n nodes, we define its size as (m, n).

[12] By a maximal redex of λ, we mean a redex of λ that is not a proper subterm of any other redex of λ. The simplified term is irreducible w.r.t. $\mathscr{S}_{i+1}$, so these replacements are done only once, and they can be done in parallel because they apply to independent subterms of λ.

The quickest way to prove this sharper result is to appeal to two facts: The first one is due to Metivier [23] (in fact, a direct proof is quite short).

LEMMA 6.5. *If R and R' are two equivalent reduced rewriting systems contained in some reduction ordering $\succ$, then $R = R'$.*

The second fact is that given a set E of p ground equations with term DAG of size (m, n), a reduced equivalent system R of p' rules with term DAG of size (m', n') such that $m' \leqslant m$, $n' \leqslant n$, and $p' \leqslant p$, is produced by a reduction process which is essentially just a Knuth–Bendix procedure restricted to ground terms.

DEFINITION 6.6. Let $\succ$ be a reduction ordering total on ground terms. Let R be a multiset of oriented pairs (s, t) which we may denote by $s \to t$ if $s \succ t$ and $s \leftarrow t$ if $s \prec t$. Finally, let $\to_R$ denote the rewriting relation induced by the nontrivial pairs. The first transformation simply removes trivial pairs from R:

$$\{(u, u)\} \cup R \Rightarrow R. \tag{1}$$

The second orients rules:

$$\{s \leftarrow t\} \cup R \Rightarrow \{t \to s\} \cup R. \tag{2}$$

Next, if $r \to r'$, then

$$\{l \to r\} \cup R \Rightarrow \{l \to r'\} \cup R, \tag{3}$$

and finally, if $l \to_R l'$, then

$$\{l \to r\} \cup R \Rightarrow \{(l', r)\} \cup R. \tag{4}$$

It should be noted that $\bigcup$ denotes multiset union, which implies that when a transformation is applied, the occurrence of the rule to which it is applied on the left-hand side (for instance, $s \leftarrow t$ in (2)) no longer exists on the right-hand side.

We now show that our reduction method always produces reduced systems whose associated term DAG is no greater than the term DAG associated with the input.

THEOREM 6.7. *Let $\succ$ be a simplification ordering total on ground terms. If E is a set of p ground equations, R is an equivalent reduced set of p' ground rewrite rules contained in $\succ$, and (m, n) and (m', n') are the sizes of*

the term DAGs associated with E and R respectively, then $m' \leqslant m$, $n' \leqslant n$, and $p' \leqslant p$.

Proof. We prove this by showing that every sequence of transformations issuing from E must eventually terminate with the set R, and that the size inequality stated above holds. Let

$$E = R_0 \Rightarrow R_1 \Rightarrow R_2 \Rightarrow \cdots$$

be any sequence of transformations starting with E and using the given ordering $\succ$. It is tedious but not hard to show that the transformations produce equivalent sets of rules, and we leave this to the reader. Similarly, it is not hard to show that any set which can not be transformed must be a reduced set of rules contained in $\succ$, since otherwise some transformation would apply. Now, by Lemma 6.5, if such a terminal set exists, it must be unique, and so it will be identical with R. Thus, we next show that the relation $\Rightarrow$ is Noetherian.

For any R, let $\mu(R) = \langle M, k \rangle$, where M is the multiset of all terms occurring in pairs in R and k is the number of pairs of the form $s \leftarrow t$. Let the ordering associated with this measure use the multiset extension of $\succ$ for the first component and the standard ordering on the natural numbers for the second. Clearly this ordering is wellfounded, since $\succ$ is. But then, each transformation reduces the measure of the set of pairs, since (1), (3), and (4) reduce M, and (2) reduces k without changing M. Thus any sequence of transformations must eventually terminate in the set R.

Finally, for any transformation $R_i \Rightarrow R_{i+1}$, note that the size of the current term DAG cannot increase, since (1) deletes nodes and possibly edges, (2) does not change the size, and (3) and (4) possibly decrease the number of nodes and preserve the number of edges. As a matter of fact, these transformations can be implemented by moving pointers. It is also obvious that each transformation either preserves or decreases the total number of rules. Thus, the claim follows by induction on the length of the transformation sequence. ∎

Another useful fact, needed later, is that the time complexity of the reduction procedure is in fact bounded by $O((m+n+p)^3)$, where (m, n) is the size of the term DAG associated with the input E, and p is the number of equations in E.

Unfortunately, given a *nonground* set E of equations, the reduction procedure just presented may not be applicable since some of the equivalence classes may contain terms involving variables and the ordering $\prec$ may no longer be total on such a partition. We need to guess how terms containing variables compare to other terms in the partition in order to reduce the equations. However, it is useful to observe that the reduction algorithm

applies, as long as at every stage of the algorithm, it is possible to determine the least element of each nontrivial equivalence class and to sort these least elements. This observation shows that in extending a simplification ordering $\prec$ total on ground terms to terms containing variables, it is sufficient to require this extension to have a least element in each nontrivial equivalence class and to be total on the set of least elements of these classes. Definition 6.12, below, makes use of this fact.

The key to extending ground orderings is that if some ground rigid E-unifier θ exists, since the ordering $\prec$ is total on ground terms, θ induces a preorder on the terms occurring in the congruence closure Π of E. For example, if $E = \{fa \doteq a, fa \doteq x\}$, $u = gx$, $v = x$, and $\theta = [ga/x]$, then Π has a single nontrivial class $\{fa, a, x\}$, and assuming that $a \prec f \prec g$, we have $a \prec fa \prec ga = \theta(x)$. Hence, we can extend $\prec$ so that $fa \prec x$. This way, the equations can be oriented as $fa \to a$, $x \to fa$.

We shall define the concept of an order assignment in order to formalize the above intuition. First, we define some relations induced by a ground substitution on a finite set of terms.

DEFINITION 6.8. Given a finite set S of terms, let $\mathrm{ST}(S)$ be the set of all subterms of terms in S (including the terms in S). Let $\preccurlyeq$ be a total simplification ordering on ground terms, and θ a ground substitution such that $\mathrm{Var}(S) \subseteq D(\theta)$. The relations $\equiv_{\theta, S}$ and $\preccurlyeq_{\theta, S}$ on $\mathrm{ST}(S)$ are defined as follows: For every $u, v \in \mathrm{ST}(S)$,

$$u \preccurlyeq_{\theta, S} v \qquad \text{iff} \quad \theta(u) \preccurlyeq \theta(v),$$

and

$$u \equiv_{\theta, S} v \qquad \text{iff} \quad \theta(u) = \theta(v).$$

When we have a partition Π induced by the congruence closure of a finite set E of equations treated as ground, S consists of the left-hand sides and right-hand sides of equations in E, and we denote $\preccurlyeq_{\theta, S}$ as $\preccurlyeq_{\theta, \Pi}$ and $\equiv_{\theta, S}$ as $\equiv_{\theta, \Pi}$. As the next example shows, the equivalence relation $\equiv_{\theta, \Pi}$ may be nontrivial.

EXAMPLE 6.9. *Let* $E = \{fx \doteq fgy, fgy \doteq gy, hgz \doteq gz\}$, $u = k(fx, gb)$, $b = k(ga, hgb)$, and $\theta = [ga/x, a/y, b/z]$. The nontrivial equivalence classes of the congruence closure Π of E are $\{fx, fgy, gy\}$, and $\{hgz, gz\}$. Then, since $\theta(x) = \theta(gy) = ga$, we have $x \equiv_{\theta, \Pi} gy$ and $fx \equiv_{\theta, \Pi} fgy$. Thus, $\equiv_{\theta, \Pi}$ has two nontrivial equivalence classes $\{x, gy\}$ and $\{fx, fgy\}$. Assuming that we have a total simplification ordering on ground terms such that $a \prec b \prec f \prec g \prec h$, we also have

$$y \preccurlyeq_{\theta, \Pi} z \preccurlyeq_{\theta, \Pi} x \preccurlyeq_{\theta, \Pi} gy \preccurlyeq_{\theta, \Pi} gz \preccurlyeq_{\theta, \Pi} fx \preccurlyeq_{\theta, \Pi} fgy \preccurlyeq_{\theta, \Pi} hgz.$$

The other pairs in $\preccurlyeq_{\theta,\Pi}$ are obtained by reflexivity and transitivity from $\equiv_{\theta,\Pi}$ and the above pairs.

This time, it is not obvious how to orient the equation $fx \doteq fgy$. This is because $\theta(fx) = \theta(fgy)$. One might think that this is a problem, but it can be overcome. Observe that since the ground equation $\theta(fx) \doteq \theta(fgy)$ is trivial, it does not help in any way in proving that $\theta(u)$ and $\theta(v)$ are congruent modulo $\theta(E)$. Also, observe that θ is a common unifier of every equivalence class modulo $\equiv_{\theta,\Pi}$. The solution is to factor out the preorder $\preccurlyeq_{\theta,\Pi}$ by the equivalence relation $\equiv_{\theta,\Pi}$. This can be achieved by choosing representatives into the classes modulo $\equiv_{\theta,\Pi}$ and replacing every term in $E \cup \{u, v\}$, by the representative in its class modulo $\equiv_{\theta,\Pi}$. In order to keep track of this equivalence, we also form the triangular form of the common mgu of these classes. Referring to Example 6.9, the mgu of the nontrivial classes $\{x, gy\}$ and $\{fx, fgy\}$ of $\equiv_{\theta,\Pi}$ is $[gy/x]$, represented by the triangular form $\langle x, gy\rangle$. If fgy is chosen as the representative in $\{fx, fgy\}$, the set of equations becomes $E' = \{fgy \doteq gy,\ hgz \doteq gz\}$, and we have $u' = k(fgy, gb)$ and $v' = k(ga, hgb)$. The nontrivial classes of the congruence closure of E' are $\{fgy, gy\}$, and $\{hgz, gz\}$. Now, the order is forced by θ: $gy \prec fgy$, $gy \prec gz$, and $gz \prec hgz$. Note that $\theta = [ga/x, a/y, b/z]$ is a unifier of $\langle x, gy\rangle$ and a rigid E'-unifier of $u' = k(fgy, gb)$ and $v' = k(ga, hgb)$.

The partition Π induces an equivalence relation on the set of equivalence classes modulo $\equiv_{\theta,\Pi}$ defined as follows.

DEFINITION 6.10. Given a set S and two equivalence relations Π and $\equiv$ on S, let $\Pi \sqcup \equiv = (\Pi \cup \equiv)^+$, the least equivalence relation containing Π and $\equiv$. The relation $\equiv/\Pi$ on the set of equivalence classes of $\equiv$ is defined as follows: for any two classes $[u]_{\equiv}$ and $[v]_{\equiv}$ of $\equiv$, $([u]_{\equiv}, [v]_{\equiv}) \in \equiv/\Pi$ iff $(u, v) \in \Pi \sqcup \equiv$.

Note that the sets of the form $\bigcup_{K \in \hat{C}} K$, where $\hat{C}$ is a class of $\equiv/\Pi$, are the equivalence classes of $\Pi \sqcup \equiv$. We will denote the set $\bigcup_{K \in \hat{C}} K$ (where $\hat{C}$ is a class of $\equiv/\Pi$) as $\bigcup \hat{C}$. Actually, every class of $\Pi \sqcup \equiv$ is both the union of some classes of Π and the union of some classes of $\equiv$.

EXAMPLE 6.11. Let $E = \{fx \doteq fgx,\ fy \doteq hy,\ kz \doteq fz\}$, and $\theta = [a/x, ga/y, b/z]$. The nontrivial classes of the congruence closure Π of E are $\{fx, fgx\}$, $\{fy, hy\}$, and $\{kz, fz\}$, and the equivalence relation $\equiv_{\theta,\Pi}$ has two nontrivial equivalence classes $\{y, gx\}$ and $\{fy, fgx\}$ since $\theta(y) = \theta(gx) = ga$. The nontrivial equivalence classes of $\equiv_{\theta,\Pi}/\Pi$ are $\{\{fx\}, \{fgx, fy\}, \{hy\}\}$ and $\{\{kz\}, \{fz\}\}$. If $\hat{C} = \{\{fx\}, \{fgx, fy\}, \{hy\}\}$, then $\bigcup \hat{C} = \{fx, fgx, fy, hy\}$.

The above discussion leads to the following definition, which makes use of the fact noted before Definition 6.8.

DEFINITION 6.12. Let $\preccurlyeq$ be a total simplification ordering on ground terms. Given a finite set S of terms and a partition Π on $\mathrm{ST}(S)$, given a preorder $\mathcal{O}$ on $\mathrm{ST}(S)$ also denoted as $\preccurlyeq_{\mathcal{O}}$, let $\equiv_{\mathcal{O}}$ be the equivalence relation associated with $\preccurlyeq_{\mathcal{O}}$ defined such that

$$\equiv_{\mathcal{O}} = \{(u, v) \mid u, v \in \mathrm{ST}(S),\ u \preccurlyeq_{\mathcal{O}} v \text{ and } v \preccurlyeq_{\mathcal{O}} u\},$$

and let $\mathrm{ST}(S)/\equiv_{\mathcal{O}}$ denote the set of equivalence classes of $\equiv_{\mathcal{O}}$. The partial ordering induced by $\preccurlyeq_{\mathcal{O}}$ on the set $\mathrm{ST}(S)/\equiv_{\mathcal{O}}$ is defined such that $[u] \preccurlyeq_{\mathcal{O}} [v]$ iff $u \preccurlyeq_{\mathcal{O}} v$ for every $[u]$, $[v] \in \mathrm{ST}(S)/\equiv_{\mathcal{O}}$. We say that the preorder $\mathcal{O}$ on $\mathrm{ST}(S)$ is an *order assignment for* Π iff the following properties hold:

(1) $\preccurlyeq_{\mathcal{O}}$ has the subterm property and is monotonic on $\mathrm{ST}(S)$, that is, for all $u_1, \ldots, u_n$, $v_1, \ldots, v_n \in \mathrm{ST}(S)$, if $u_i \preccurlyeq_{\mathcal{O}} v_i$ for $i = 1, \ldots, n$ and $f(u_1, \ldots, u_n)$ and $f(v_1, \ldots, v_n) \in \mathrm{ST}(S)$, then $f(u_1, \ldots, u_n) \preccurlyeq_{\mathcal{O}} f(v_1, \ldots, v_n)$;

(2) The restriction of $\preccurlyeq_{\mathcal{O}}$ to ground terms agrees with $\preccurlyeq$ (on $\mathrm{ST}(S)$), and the partial ordering $\preccurlyeq_{\mathcal{O}}$ on $\mathrm{ST}(S)/\equiv_{\mathcal{O}}$ is such that every nontrivial equivalence class $\hat{C}$ of $\equiv_{\mathcal{O}}/\Pi$ has a least element, and $\preccurlyeq_{\mathcal{O}}$ is total on this set of least elements.

(3) There is some joint unifier of all equivalence classes modulo $\equiv_{\mathcal{O}}$. By this, we mean that there is some θ such that for every class K of $\equiv_{\mathcal{O}}$, for every pair of terms $u, v \in K$, $\theta(u) = \theta(v)$.

Note that condition (3) implies that each class of the equivalence relation $\equiv_{\mathcal{O}}$ contains at most one ground term. Condition (1) implies that the partial ordering induced by $\preccurlyeq_{\mathcal{O}}$ on the set $\mathrm{ST}(S)/\equiv_{\mathcal{O}}$ in monotonic.

Given a finite set E of equations, if Π is the partition associated with the congruence closure of E, by an *order assignment for* E we mean an order assignment for Π.

Remarks. We can add the following condition to the definition of an order assignment:

(4) $\equiv_{\mathcal{O}}$ is a unification closure, that is, for all $f(u_1, \ldots, u_n)$ and $f(v_1, \ldots, v_n) \in \mathrm{ST}(S)$, if $f(u_1, \ldots, u_n) \equiv_{\mathcal{O}} f(v_1, \ldots, v_n)$, then $u_i \equiv_{\mathcal{O}} v_i$ for $i = 1, \ldots, n$.

One of the benefits of adding condition (4) is that there are fewer order assignments on a partition satisfying condition (4).

The following lemma gives a useful method for obtaining order assignments.

LEMMA 6.13. *Given a finite set S of terms and a partition Π on* $\mathrm{ST}(S)$, *given any ground substitution θ such that* $\mathrm{Var}(\Pi) \subseteq D(\theta)$: (i) *the preorder $\preccurlyeq_{\theta,\Pi}$ is an order assignment for Π satisfying condition* (4); (ii) *there exists an order assignment $\preccurlyeq_{\mathscr{C}}$ for Π such that $\preccurlyeq_{\mathscr{C}} \subseteq \preccurlyeq_{\theta,\Pi}$ and $\preccurlyeq_{\mathscr{C}}$ is a total ordering.*

Proof. (i) The verification is straightforward and left as an exercise. (ii) For every nontrivial equivalence class C modulo $\equiv_{\theta,\Pi}$, we extend the simplification ordering $\prec$ as follows. Whenever such a class contains some variable, say $C = \{x_1, ..., x_k, t_1, ..., t_m\}$ where $x_1, ..., x_k$ are variables, we extend $\prec$ to a relation $\prec'$ such that $x_i \prec' x_2 \prec' \cdots \prec' x_k$ and $x_i \prec' t_j$, for all i, j, $1 \leqslant i \leqslant k$, $1 \leqslant j \leqslant m$. It is clear that $\preccurlyeq'$ is a partial ordering contained in $\preccurlyeq_{\theta,\Pi}$. Now, we define $\prec_{\mathscr{C}}$ recursively as follows: $u \prec_{\mathscr{C}} v$ iff either

(1) $\theta(u) \prec \theta(v)$, or

(2) $\theta(u) = \theta(v)$, and either

(2a) u is a variable and $u \prec' v$, or

(2b) $u = f(u_1, ..., u_n)$, $v = f(v_1, ..., v_n)$, and $\langle u_1, ..., u_n \rangle \prec_{\mathscr{C}}^{\mathrm{lex}} \langle v_1, ..., v_n \rangle$,

where $\prec_{\mathscr{C}}^{\mathrm{lex}}$ is the lexicographic extension of $\prec_{\mathscr{C}}$.

We define $\preccurlyeq_{\mathscr{C}}$ as the reflexive closure of $\prec_{\mathscr{C}}$, and we claim that $\prec_{\mathscr{C}}$ is a total ordering which is an order assignment contained in $\preccurlyeq_{\theta,\Pi}$. The only problem is in showing that $\prec_{\mathscr{C}}$ is a total ordering, as the other conditions are then easily verified. To prove that $\prec_{\mathscr{C}}$ is a total ordering, due to clause (1) of the definition of $\prec_{\mathscr{C}}$, it is enough to show that for any two distinct elements u, v in some nontrivial class $\mathscr{C}$ modulo $\equiv_{\theta,\Pi}$, either $u \prec_{\mathscr{C}} v$ or $v \prec_{\mathscr{C}} u$, but not both. Note that the set of classes modulo $\equiv_{\theta,\Pi}$ is totally ordered: $C \ll C'$ iff $\theta(C) \prec \theta(C')$, where $\theta(C)$ denotes the common value of all terms $\theta(t)$, where $t \in C$. We proceed by induction on this well-ordering of the classes. Clearly, the least class contains some variable and at most one constant. But then, it is already totally ordered by $\prec'$. Given any other nontrivial class C, if u and v are both variables, we already know by (2a) that either $u \prec' v$ or $v \prec' u$, but not both. If u is a variable and v is not, by (2a) we can have only $u \prec' v$. If both u and v are not variables, then they must be of the form $u = f(u_1, ..., u_n)$ and $b = f(v_1, ..., v_n)$, since C is unified by θ. Since $u \neq v$, there is a least i such that $u_i \neq v_i$, and since θ unifies u and v, θ unifies u_i and v_i. But then, because $\prec$ has the subterm property, u_i, v_i belong to some class C_i such that $C_i \ll C$. Therefore, either $u_i \prec_{\mathscr{C}} v_i$ or $v_i \prec_{\mathscr{C}} u_i$, but not both, and thus by (2b), either $u \prec_{\mathscr{C}} v$ or $v \prec_{\mathscr{C}} u$, but not both. ∎

In view of Lemma 6.13, the following definition is justified.

DEFINITION 6.14. Given a finite set of terms S, an order assignment $\prec_{\mathcal{C}}$ for a partition Π on $\mathrm{ST}(S)$ is *realized* by a ground substitution θ such that $\mathrm{Var}(\Pi) \subseteq D(\theta)$ iff $\prec_{\mathcal{C}} \subseteq \preccurlyeq_{\theta, \Pi}$.

By condition (3) of Definition 6.12, the equivalence classes of $\equiv_{\mathcal{C}}$ have some common unifier. We now show how a triangular form of a joint mgu of these classes can be obtained.

DEFINITION 6.15. Given an order assignment $\prec_{\mathcal{C}}$ for a partition Π on $\mathrm{ST}(S)$, for every nontrivial equivalence class C of $\equiv_{\mathcal{C}}$, let $S_C = \{\langle t_2, t_1\rangle, \langle t_3, t_1\rangle, ..., \langle t_n, t_1\rangle\}$, where t_1 is any chosen representative in C and $C = \{t_1, ..., t_n\}$, and let $S_{\mathcal{C}} = \bigcup_{C \in \equiv_{\mathcal{C}}} S_C$ be the union of these systems. From the way the term system $S_{\mathcal{C}}$ is constructed, a substitution unifies $S_{\mathcal{C}}$ iff it unifies every class of $\equiv_{\mathcal{C}}$. Thus, we let $TU_{\mathcal{C}}$ denote the triangular form of the mgu of $S_{\mathcal{C}}$. We also denote by $\sigma_{\mathcal{C}}$ the substitution $[s_1/x_1, ..., s_k/x_k]$ defined by the triangular form $TU_{\mathcal{C}} = \{\langle x_1, s_1\rangle, ..., \langle x_k, s_k\rangle\}$, as explained after Definition 3.3.

Given two order assignments $\mathcal{C}$ on a partition Π for $\mathrm{ST}(S)$ and $\mathcal{C}'$ on a partition Π' for $\mathrm{ST}(S')$, we say that $\mathcal{C}$ and $\mathcal{C}'$ are *compatible* iff they coincide on $\mathrm{ST}(S) \cap \mathrm{ST}(S')$.

EXAMPLE 6.16. Let $E = \{fx \doteq fgy, fgy \doteq gy, hgz \doteq gz\}$, as in Example 6.9. The nontrivial equivalence classes of the congruence closure Π of E are $\{fx, fgy, gy\}$, and $\{hgz, gz\}$. The preorder $\mathcal{C}_1$ on $\{x, y, z, fx, gy, gz, fgy, hgz\}$ of example 6.9 whose only nontrivial equivalence classes are $\{x, gy\}$ and $\{fx, fgy\}$, and such that

$$y \preccurlyeq_{\theta, \Pi} z \preccurlyeq_{\theta, \Pi} x \preccurlyeq_{\theta, \Pi} gy \preccurlyeq_{\theta, \Pi} gz \preccurlyeq_{\theta, \Pi} fx \preccurlyeq_{\theta, \Pi} fgy \preccurlyeq_{\theta, \Pi} hgz$$

is an order assignment realized by $\theta = [ga/x, a/y, b/z]$.

Let $\mathcal{C}_2$ be the preorder on $\{x, y, z, fx, gy, gz, fgy, hgz\}$ whose equivalence relation is the identity relation, and such that $gy \preccurlyeq_{\mathcal{C}_2} gz$, $gy \preccurlyeq_{\mathcal{C}_2} fgy, fgy \preccurlyeq_{\mathcal{C}_2} fx$, and $gz \preccurlyeq_{\mathcal{C}_2} hgz$ (other pairs in $\preccurlyeq_{\mathcal{C}_2}$ are obtained by transitivity and reflexivity). It is immediately verified that $\mathcal{C}_2$ is an order assignment realized by $\theta = [ga/x, a/y, b/z]$, since $\preccurlyeq_{\mathcal{C}_2} \subseteq \preccurlyeq_{\theta, \Pi}$.

Let $\mathcal{C}_3$ be the preorder on $\{x, y, z, fx, gy, gz, fgy, hgz\}$ whose equivalence relation is the identity relation, and such that $fx \preccurlyeq_{\mathcal{C}_3} gz$, $fx \preccurlyeq_{\mathcal{C}_3} gy$, $gy \preccurlyeq_{\mathcal{C}_3} fgy$, and $gz \preccurlyeq_{\mathcal{C}_3} hgz$ (other pairs in $\preccurlyeq_{\mathcal{C}_3}$ are obtained by transitivity and reflexiviy). It is immediately verified that $\mathcal{C}_3$ is an order assignment, and that it is not realized by $\theta = [ga/x, a/y, b/z]$. This time, it is not true that $\preccurlyeq_{\mathcal{C}_3} \subseteq \preccurlyeq_{\theta, \Pi}$ since $\theta(fx) = fga$, $\theta(gy) = ga$, but $fga \not\prec ga$.

The next example arises from the problem of proving that every monoid such that $x \cdot x = 1$ (for all x) is commutative.

EXAMPLE 6.17. *Let* $\mathscr{E}$ be the set of equations

$$\begin{aligned}
\mathscr{E} = \{u_1 \cdot 1 &\doteq u_1\\
w_1 \cdot w_1 &\doteq 1\\
x_1 \cdot (y_1 \cdot z_1) &\doteq (x_1 \cdot y_1) \cdot z_1\\
x_2 \cdot (y_2 \cdot z_2) &\doteq (x_2 \cdot y_2) \cdot z_2\\
w_2 \cdot w_2 &\doteq 1\\
1 \cdot v_1 &\doteq v_1\\
x_3 \cdot (y_3 \cdot z_3) &\doteq (x_3 \cdot y_3) \cdot z_3\\
x_4 \cdot (y_4 \cdot z_4) &\doteq (x_4 \cdot y_4) \cdot z_4\\
w_3 \cdot w_3 &\doteq 1\\
eq(a \cdot b, b \cdot a) &\doteq F\\
eq(z, z) &\doteq T\}.
\end{aligned}$$

The nontrivial equivalence classes of the congruence closure Π of $\mathscr{E}$ are

$$\begin{aligned}
&\{T, eq(z, z)\},\\
&\{F, eq(a \cdot b, b \cdot a)\},\\
&\{1, w_2 \cdot w_2, w_3 \cdot w_3, w_1 \cdot w_1\},\\
&\{u_1, u_1 \cdot 1\},\\
&\{v_1, 1 \cdot v_1\},\\
&\{x_2 \cdot (y_2 \cdot z_2), (x_2 \cdot y_2) \cdot z_2\},\\
&\{x_4 \cdot (y_4 \cdot z_4), (x_4 \cdot y_4) \cdot z_4\},\\
&\{x_3 \cdot (y_3 \cdot z_3), (x_3 \cdot y_3) \cdot z_3\},\\
&\{x_1 \cdot (y_1 \cdot z_1), (x_1 \cdot y_1) \cdot z_1\}.
\end{aligned}$$

We define the order assignment $\mathscr{O}$ on Π whose equivalence relation is the identity and such that the ordering $\preccurlyeq_{\mathscr{O}}$ is defined by the order in which the elements in each class of Π are listed, and for the least elements in these classes, the order in which the classes are listed. All other pairs in $\prec_{\mathscr{O}}$ are determined by reflexivity and transitivity. It is easily seen that there is a total simplification ordering on ground terms such that $1 \prec a \prec b \prec \cdot$, and one can verify that $\prec_{\mathscr{O}}$ is an order assignment.

Another order assignment $\preccurlyeq_{\mathcal{O}'}$ is defined as the preorder extending $\preccurlyeq_{\mathcal{O}}$ and whose nontrivial equivalence classes of $\equiv_{\mathcal{O}'}$ are

$$\{a, u_1, x_1, x_2, y_2, w_2, x_4\},$$
$$\{b, z_2, v_1, x_3, z_3, y_4, z_4, w_3\},$$
$$\{w_2 \cdot w_2, x_2 \cdot y_2\},$$
$$\{a \cdot b, w_1, y_1, z_1, y_3, z, y_2 \cdot z_2, x_4 \cdot y_4\},$$
$$\{w_3 \cdot w_3, y_4 \cdot z_4\})$$
$$\{w_1 \cdot w_1, y_1 \cdot z_1\},$$

these classes being ordered as listed (since $a \prec b$). It is easy to verify that $\preccurlyeq_{\mathcal{O}'}$ is realized by the substitution

$$\theta = [a/u_1, a/x_1, a/x_2, a/y_2, a/w_2, a/x_4,$$
$$b/z_2, b/v_1, b/x_3, b/z_3, b/y_4, b/z_4, b/w_3,$$
$$a \cdot b/w_1, a \cdot b/y_1, a \cdot b/z_1, a \cdot b/y_3, a \cdot b/z].$$

Note that $\equiv_{\mathcal{O}'}$ causes the merging of some equivalence classes of Π, even some trivial ones.

One more issue that we would like to address before presenting a revised version of the procedure of Definition 6.4 is the simplification of equations using the equivalence relation $\equiv_{\mathcal{O}}$. This is primarily for efficiency reasons. The problem is illustrated by the order assignment $\preccurlyeq_{\mathcal{O}'}$ of Example 6.17.

EXAMPLE 6.18. Recall that the nontrivial equivalence classes of $\equiv_{\mathcal{O}'}$ (from Example 6.17) are

(1) $\{a, u_1, x_1, x_2, y_2, w_2, x_4\}$,
(2) $\{b, z_2, v_1, x_3, z_3, y_4, z_4, w_3\}$,
(3) $\{w_2 \cdot w_2, x_2 \cdot y_2\}$,
(4) $\{a \cdot b, w_1, y_1, z_1, y_3, z, y_2 \cdot z_2, x_4 \cdot y_4\}$,
(5) $\{w_3 \cdot w_3, y_4 \cdot z_4\}$,
(6) $\{w_1 \cdot w_1, y_1 \cdot z_1\}$.

The problem is to simplify the equations by replacing subterms by equivalent terms modulo $\equiv_{\mathcal{O}'}$, in such a way that $\preccurlyeq_{\mathcal{O}'}$ is a partial order on the new partition associated with the set of simplified equations. Clearly, this is a problem of choice of representatives. For example, how do we simplify

$x_1 \cdot (y_1 \cdot z_1) \doteq (x_1 \cdot y_1) \cdot z_1$? If we choose the first element of each class as a representative, then the above equation simplifies to $a \cdot (w_1 \cdot w_1) \doteq (a \cdot (a \cdot b)) \cdot (a \cdot b)$, if we replace maximal subterms (in the subterm ordering) by their representatives. But it is preferable to replace each variable by its representative in the class, since we obtain the ground equation $a \cdot ((a \cdot b) \cdot (a \cdot b)) \doteq (a \cdot (a \cdot b)) \cdot (a \cdot b)$. So, how do we proceed? A key observation is that the subterm ordering induces a strict order on the classes modulo $\equiv_{\mathcal{O}'}$. A class C precedes a class C', denoted as $C \ll C'$, iff C contains some term that is a proper subterm of some term in C'. Thus, $(1) \ll (3)$, $(1) \ll (4)$, $(2) \ll (4)$, $(2) \ll (5)$, $(4) \ll (6)$, and the other relations are obtained by transitivity and reflexivity. We propose to assign representatives from the bottom up, starting with the minimal classes (w.r.t. $\ll$) and proceeding up using the ordering $\ll$ on the classes. Furthermore, whenever possible, we pick ground representatives. For example, we would pick a in (1), b in (2), and then $a \cdot a$ in (3), $a \cdot b$ in (4), $b \cdot b$ in (5), and $(a \cdot b) \cdot (a \cdot b)$ in (6).

Before we proceed with rigorous definitions, let us observe that if $\mathcal{O}$ is an order assignment on a partition Π, since the classes modulo $\equiv_{\mathcal{O}}$ have some joint unifier, every nontrivial class contains at most one ground term, and all compound terms in a nontrivial class have the same root symbol. With a slight abuse of notation, we let $\equiv_{\mathcal{O}}$ denote the set of equivalence classes of the equivalence relation $\equiv_{\mathcal{O}}$.

DEFINITION 6.19. Let $\mathcal{O}$ be an order assignment on a partition Π. The relation $\ll$ is defined on the set of classes modulo $\equiv_{\mathcal{O}}$ as follows: given any two classes $K, K' \in \equiv_{\mathcal{O}}$, $K \ll K'$ iff there are terms $t \in K$ and $t' \in K'$ such that t is a proper subterm of t'.

LEMMA 6.20. *The relation $\ll$ given in Definition* 6.19 *is a strict order on the set of classes modulo $\equiv_{\mathcal{O}}$, and if $K \ll K'$ then $K \prec_{\mathcal{O}} K'$.*

Proof. It is clear that $\ll$ is transitive, and we need only show that it is irreflexive. As noted earlier, the classes modulo $\equiv_{\mathcal{O}}$ have some joint unifier, say θ. Then, for every class K of $\equiv_{\mathcal{O}}$, there is some term s such that $\theta(u) = s$ for all $u \in K$. With a slight abuse of notation, we use the notation $\theta(K)$ for this term s. Recall that $K \ll K'$ iff there are terms $t \in K$ and $t' \in K'$ such that t is a proper subterm of t'. Consequently, if $K \ll K'$ then $\theta(K) = \theta(t)$ is a proper subterm of $\theta(K') = \theta(t')$. Thus $K \ll K$ does not hold, since otherwise $\theta(K)$ would be a proper subterm of itself. Since $K \ll K'$ implies that $K \preccurlyeq_{\mathcal{O}} K'$, by the irreflexivity of $\ll$ we have $K \prec_{\mathcal{O}} K'$. ∎

We now use the strict order $\ll$ on the classes modulo $\equiv_{\mathcal{O}}$ to assign representatives inductively.

DEFINITION 6.21. Let $\mathcal{O}$ be an order assignment on a partition $\prod$ on ST(S). A function ρ: $\equiv_{\mathcal{O}} \to T_\Sigma(X)$ assigning a term $\rho(K)$ to every equivalence class K modulo $\equiv_{\mathcal{O}}$ is a *representative selector* iff for every minimal class K w.r.t. $\lessdot$, $\rho(K)$ is the unique ground term in K if it exists, or else any chosen element of K, and for every nonminimal class K, if

$$\hat{K} = \{f(t_1^1, ..., t_m^1), ..., f(t_1^n, ..., t_m^n)\}$$

is the subset of compound elements in K, then $\rho(K)$ is the unique ground term in

$$\rho(\hat{K}) = \{f(\rho([t_1^1]_{\equiv_{\mathcal{O}}}), ..., \rho([t_m^1]_{\equiv_{\mathcal{O}}})), ..., f(\rho([t_1^n]_{\equiv_{\mathcal{O}}}), ..., \rho([t_m^n]_{\equiv_{\mathcal{O}}}))\}$$

if it exists, or else any chosen element in $\rho(\hat{K})$, where $[u]_{\equiv_{\mathcal{O}}}$ denotes the equivalence class of u modulo $\equiv_{\mathcal{O}}$.

The *reduced partition* $\rho(\Pi)$ is the partition whose classes are the sets of the form $\{\rho(K) \mid K \in \hat{C}, K \text{ is a class modulo } \equiv_{\mathcal{O}}, \hat{C} \in \equiv_{\mathcal{O}}/\Pi\}$, and if Π is the congruence closure associated with a set E of equations, the *reduced set of equations* $\rho(E)$ is the set of equations $\{\rho([l]_{\equiv_{\mathcal{O}}}) \doteq \rho([r]_{\equiv_{\mathcal{O}}}) \mid l \doteq r \in E\}$. We also define the preorder $\rho(\preccurlyeq_{\mathcal{O}})$ on $\rho(\Pi)$ such that $\rho(K)\, \rho(\preccurlyeq_{\mathcal{O}})\, \rho(K')$ iff $u \preccurlyeq_{\mathcal{O}} v$ for some $u \in K$, $v \in K'$. It is obvious that $\rho(\preccurlyeq_{\mathcal{O}})$ is a partial order on $\rho(\Pi)$ since K, K' are classes modulo $\equiv_{\mathcal{O}}$.

Note that $\rho(K) \in K$ if K is a minimal class (w.r.t. $\lessdot$), but it is possible that $\rho(K) \notin K$ if K is not minimal. However, as shown in the next lemma, ρ is injective and even though $\rho(K)$ may not be in K, this does not matter for our purposes as shown below.

LEMMA 6.22. *Let $\mathcal{O}$ be an order assignment on a partition Π on* ST(S), *and θ any joint unifier of the classes modulo $\equiv_{\mathcal{O}}$.* (i) *For every class K modulo $\equiv_{\mathcal{O}}$, $\theta(K) = \theta(\rho(K))$ (with the slight abuse of notation where $\theta(K)$ denotes the term s such that $\theta(u) = s$ for all $u \in K$).* (ii) *Every representative selector is injective.*

Proof. First, note that since the set of classes modulo $\equiv_{\mathcal{O}}$ is finite, the strict order $\lessdot$ is well founded. We prove (i) by induction on the well-founded ordering $\lessdot$. For a minimal class K, since $\rho(K) = u$ for some element $u \in K$ and $\theta(K) = \theta(u)$, it is clear that $\theta(K) = \theta(u) = \theta(\rho(K))$. For a nonminimal class K, if

$$\hat{K} = \{f(t_1^1, ..., t_m^1), ..., f(t_1^n, ..., t_m^n)\}$$

is the subset of compound elements in K, then $\rho(K)$ is the unique ground term in

$$\rho(\hat{K}) = \{f([t_1^1]_{\equiv_{\mathcal{O}}}), ..., \rho([t_m^1]_{\equiv_{\mathcal{O}}})), ..., f(\rho([t_1^n]_{\equiv_{\mathcal{O}}}), ..., \rho([t_m^n]_{\equiv_{\mathcal{O}}}))\}$$

if it exists, or else any chosen element in $\rho(\hat{K})$. Assume that $f(\rho([t_1^1]_{\equiv_\mathscr{E}}), ..., \rho([t_m^1]_{\equiv_\mathscr{E}}))$ was picked. Since t_i^1 is a proper subterm of $f(t_1^1, ..., t_m^1)$, by the definition of $\ll$ we have $[t_i^1]_{\equiv_\mathscr{E}} \ll K$ for all i, $1 \leqslant i \leqslant m$. Thus, by the induction hypothesis

$$\theta(\rho([t_i^1]_{\equiv_\mathscr{E}})) = \theta([t_i^1]_{\equiv_\mathscr{E}}) = \theta(t_i^1)$$

for all i, $1 \leqslant i \leqslant m$, and since θ is a homomorphism,

$$\begin{aligned}\theta(\rho(K)) &= \theta(f(\rho([t_1^1]_{\equiv_\mathscr{E}}), ..., \rho([t_m^1]_{\equiv_\mathscr{E}}))) \\ &= f(\theta(\rho([t_1^1]_{\equiv_\mathscr{E}})), ..., \theta(\rho([t_m^1]_{\equiv_\mathscr{E}}))) \\ &= f(\theta(t_1^1), ..., \theta(t_m^1)) \\ &= \theta(f(t_1^1, ..., t_m^1)) \\ &= \theta(K).\end{aligned}$$

This concludes the induction step and the proof of (i).

To prove (ii), we proceed by induction on the well-founded ordering $\ll_2$ defined on pairs of classes modulo $\equiv_\mathscr{E}$ such that $\langle K_1, K_2 \rangle \ll_2 \langle K_1', K_2' \rangle$ iff $K_1 \ll K_1'$ and $K_2 \ll K_2'$. Assume that $\rho(K) = \rho(K')$. There are three cases.

If both K and K' are minimal w.r.t. $\ll$, since in this case $\rho(K) \in K$ and $\rho(K') \in K'$, we have $K = K'$.

If K is minimal but K' is not (the case where K' is minimal being symmetric), then $\rho(K')$ is some compound term but $\rho(K)$ is either a constant or a variable since K is minimal, and this is a contradiction.

If both K and K' are not minimal, then both $\rho(K)$ and $\rho(K')$ are compound terms and we have

$$\rho(K) = f(\rho([s_1]_{\equiv_\mathscr{E}}), ..., \rho([s_m]_{\equiv_\mathscr{E}}))$$

and

$$\rho(K') = f(\rho([t_1]_{\equiv_\mathscr{E}}), ..., \rho([t_m]_{\equiv_\mathscr{E}}))$$

for some terms $f(s_1, ..., s_m) \in K$ and $f(t_1, ..., t_m) \in K'$. From the definition of $\ll$ and $\ll_2$, it is clear that

$$\langle [s_i]_{\equiv_\mathscr{E}}, [t_i]_{\equiv_\mathscr{E}} \rangle \ll_2 \langle K, K' \rangle.$$

Since $\rho(K) = \rho(K')$, we have $\rho([s_i]_{\equiv_\mathscr{E}}) = \rho([t_i]_{\equiv_\mathscr{E}})$ for all i, $1 \leqslant i \leqslant m$. By the induction hypothesis, this yields $[s_i]_{\equiv_\mathscr{E}} = [t_i]_{\equiv_\mathscr{E}}$, that is, $s_i \equiv_\mathscr{E} t_i$ for all i, $1 \leqslant i \leqslant m$. Since $\equiv_\mathscr{E}$ is congruential, the above implies that $f(s_1, ..., s_m) \equiv_\mathscr{E} f(t_1, ..., t_m)$, and so $K = K'$. This concludes the induction step and proves that ρ is injective. ∎

The following lemma shows that representative selectors always exist.

LEMMA 6.23 (Construction of representative selectors). *Let $\mathcal{O}$ be an order assignment on a partition Π on* ST(S). *There is an algorithm to construct representative selectors* ρ: $\equiv_{\mathcal{O}} \to T_\Sigma(X)$.

Proof. It is easy to design an algorithm that proceeds bottom up in the acyclic graph corresponding to the strict order $\ll$, say performing a topological sort, and assigns representatives according to the rules given in Definition 6.21. The details are straightforward and left to the reader. ∎

LEMMA 6.24. *Let $\mathcal{O}$ be an order assignment on a partition Π on* ST(S). *The strict order $\rho(\preccurlyeq_{\mathcal{O}})$ on $\rho(\Pi)$ is a simplification ordering such that every nontrivial class of $\rho(\Pi)$ has a least element, and it is total on this set of least elements. If Π is the congruence closure associated with a set E of equations, then $\rho(\Pi)$ is the congruence closure associated with $\rho(E)$.*

Proof. To show that it is a simplification ordering, we proceed by induction on the well-founded ordering $\ll$. The other properties are immediate because $\preccurlyeq_{\mathcal{O}}$ is an order assignment. ∎

We can now modify the procedure of Definition 6.4 in order to accommodate variables.

DEFINITION 6.25 (Reduction procedure R). Let $\prec$ be a total simplification ordering on ground terms. Let $\mathcal{E} = \mathcal{E}_\Sigma \cup \{eq(u, v) \doteq F,\ eq(z, z) \doteq T\}$ be a finite set of equations, where $\mathcal{E}_\Sigma$ is a set of equations over $T_\Sigma(X)$, and $u, v \in T_\Sigma(X)$. Given any order assignment $\mathcal{O}$ on $\mathcal{E}$, the procedure R returns a rigid reduced rewrite system $R(\mathcal{E}, \mathcal{O})$. To form the system $R(\mathcal{E}, \mathcal{O})$, first, we use the algorithm of Lemma 6.23 to get a representative selector ρ for $\equiv_{\mathcal{O}}$ (if is not the identity), and we let $\mathcal{E}'$ be the reduced set $\rho(\mathcal{E})$. Trivial equations are discarded. Let Π' be the congruence closure associated with $\mathcal{E}'$. By Lemma 6.24, $\rho(\preccurlyeq_{\mathcal{O}})$ is a simplification ordering such that every nontrivial equivalence class of Π' has a least element and it is total on this set of least elements. From this point on, we apply to $\mathcal{E}'$ and Π' the procedure described in Definition 6.4, except that at the end of every round, it may be necessary to extend $\mathcal{O}$ and modify the representative selector ρ, since new terms may arise due to simplification. If at every round an extension of $\mathcal{O}$ can be found so that the next step can be performed, R succeeds and returns a rigid reduced rewrite system denoted as $R(\mathcal{E}, \mathcal{O})$. Otherwise, R returns failure.

It is useful to remark that since the reduction procedure deals with sets of equations of the form $\mathcal{E} = \mathcal{E}_\Sigma \cup \{eq(u, v) \doteq F,\ eq(z, z) \doteq T\}$, in the congruence closure Π of $\mathcal{E}$, the classes of T and F are always $\{eq(u, v), F\}$ and $\{eq(z, z), T\}$. From the way we have extended $\preccurlyeq$ to take care of T, F, and terms involving eq, it will be shown as a corollary of Theorem 8.2 that

there is no loss of generality in choosing order assignments such that $T \preccurlyeq_{\mathcal{O}} F \preccurlyeq_{\mathcal{O}} s \preccurlyeq_{\mathcal{O}} eq(u, v)$ for all $s, u, v \in T_\Sigma(X)$. Using Lemma 6.13, we can show the following crucial result.

LEMMA 6.26. *Let $\mathcal{E} = \mathcal{E}_\Sigma \cup \{eq(u, v) \doteq F, eq(z, z) \doteq T\}$ be a finite set of equations, where $\mathcal{E}_\Sigma$ is a set of equations over $T_\Sigma(X)$, $u, v \in T_\Sigma(X)$, and $\prec$ a total simplification ordering on ground terms.*

(i) *Given an order assignment $\mathcal{O}$ on $\mathcal{E}$, if a substitution θ (not necessarily ground) unifies $TU_{\mathcal{O}}$ and R does not fail, then $\theta(R(\mathcal{E}, \mathcal{O}))$ is rigid equivalent to $\theta(\mathcal{E})$.*

(ii) *Given an order assignment $\mathcal{O}$ on $\mathcal{E}$, if some ground substitution θ realizes $\mathcal{O}$ and R does not fail, then $\theta(R(\mathcal{E}, \mathcal{O}))$ is rigid equivalent to $\theta(\mathcal{E})$.*

Proof. First, we prove (i). Let Π be the congruence closure of $\mathcal{E}$, and let $TU_{\mathcal{O}}$ be the triangular form associated with $\equiv_{\mathcal{O}}$. Since θ unifies $TU_{\mathcal{O}}$, θ unifies every class modulo $\equiv_{\mathcal{O}}$. If ρ is the representative selector given by the algorithm of Lemma 6.23, by Lemma 6.22, we have $\theta(K) = \theta(\rho(K))$ for every class K modulo $\equiv_{\mathcal{O}}$. Then, for every equation $l \doteq r \in \mathcal{E}$, we have $\theta(\rho([l]_{\equiv_{\mathcal{O}}}) \doteq \rho([r]_{\equiv_{\mathcal{O}}})) = \theta(l \doteq r)$, and this shows that $\theta(\mathcal{E})$ and $\theta(\mathcal{E}') = \theta(\rho(\mathcal{E}))$ are rigid equivalent. Since the result of applying the reduction procedure of Definition 6.4 to $\mathcal{E}' = \rho(\mathcal{E})$ yields a system $R(\mathcal{E}, \mathcal{O})$ that is rigid equivalent to $\mathcal{E}'$ when R does not fail, the systems $\theta(R(\mathcal{E}, \mathcal{O}))$ and $\theta(\mathcal{E}')$ are also rigid equivalent, and so $\theta(R(\mathcal{E}, \mathcal{O}))$ and $\theta(\mathcal{E})$ are rigid equivalent.

The proof of (ii) follows from the fact that since θ realizes $\mathcal{O}$, then θ unifies $TU_{\mathcal{O}}$, and by using (i). ∎

It is important to note that part (i) of Lemma 6.26 holds even if θ is not ground. This fact will be used in the proof that the method is sound. We are now ready to define a procedure for finding rigid E-unifiers.

7. A METHOD FOR FINDING COMPLETE SETS OF RIGID E-UNIFIERS

This method uses the reduction procedure of Section 6 and a single transformation on certain systems defined next. First, the following definition is needed.

DEFINITION 7.1. Given a set E of equations and some equation $l \doteq r$, the set of equations obtained from E by deleting $l \doteq r$ and $r \doteq l$ from E is denoted by $(E - \{l \doteq r\})^\dagger$. Formally, we let $(E - \{l \doteq r\})^\dagger = (u \doteq v \mid u \doteq v \in E, u \doteq v \neq l \doteq r, \text{ and } u \doteq v \neq r \doteq l\}$.

DEFINITION 7.2. Let $\prec$ be a total simplification ordering on ground terms. We shall be considering finite sets of equations of the form $\mathscr{E} = \mathscr{E}_\Sigma \cup \{eq(u, v) \doteq F, eq(z, z) \doteq T\}$, where $\mathscr{E}_\Sigma$ is a set of equations over $T_\Sigma(X)$, and $u, v \in T_\Sigma(X)$. We define a transformation on systems of the form $\langle \mathscr{S}, \mathscr{E}, \mathscr{O} \rangle$, where $\mathscr{S}$ is a term system, $\mathscr{E}$ a set of equations as above, and $\mathscr{O}$ an order assignment:

$$\langle \mathscr{S}_0, \mathscr{E}_0, \mathscr{O}_0 \rangle \Rightarrow \langle \mathscr{S}_1, \mathscr{E}_1, \mathscr{O}_1 \rangle,$$

where $l_1 \doteq r_1, l_2 \doteq r_2 \in \mathscr{E}_0 \cup \mathscr{E}_0^{-1}$, either l_1/β is *not* a variable or $l_2 \doteq r_2$ is degenerate, $l_1/\beta \neq l_2$, $TU(l_1/\beta, l_2)$ represents a mgu of l_1/β and l_2 in triangular form,[13] $\sigma = [t_1/x_1, ..., t_p/x_p]$ where $TU(l_1/\beta, l_2) = \{\langle x_1, t_1 \rangle, ..., \langle x_p, t_p \rangle\}$,

$$\mathscr{E}'_1 = \sigma((\mathscr{E}_0 - \{l_1 \doteq r_1\})^+ \cup \{l_1[\beta \leftarrow r_2] \doteq r_1\}),$$

$\mathscr{O}_1$ is an order assignment on $\mathscr{E}'_1$ compatible with $\mathscr{O}_0$, $\mathscr{S}_1 = \mathscr{S}_0 \cup TU(l_1/\beta, l_2) \cup TU_{\mathscr{O}_1}$, and $\mathscr{E} = R(\mathscr{E}'_1, \mathscr{O}_1)$.

Observe that $\sigma(l_1[\beta \leftarrow r_2] \doteq r_1)$ looks like a critical pair of equations in $\mathscr{E}_0 \cup \mathscr{E}_0^{-1}$, but it is not. This is because a critical pair is formed by applying the mgu of l_1/β and l_2 to $l_1[\beta \leftarrow r_2] \doteq r_1$, but $[t_1/x_1, ..., t_p/x_p]$ is usually not a mgu of l_1/β and l_2. It is the composition $[t_1/x_1]; ...; [t_p/x_p]$ that is a mgu of l_1/β and l_2. The reason for not applying the mgu is that by repeated applications of this step, exponential size terms could be formed, and it would not be clear that the decision procedure is in NP. We have chosen an approach of "lazy" (or delayed) unification. Also note that we use the rigid reduced system $R(\mathscr{E}'_1, \mathscr{O}_1)$ rather than $\mathscr{E}_1$, and so, a transformation step is defined only if R does not fail. The method then is the following.

DEFINITION 7.3 (Method). Let $E_{u,v} = E \cup \{eq(u, v) \doteq F, eq(z, z) \doteq T\}$, $\mathscr{O}_0$ an order assignment of $E_{u,v}$, $\mathscr{S}_0 = TU_{\mathscr{O}_0}$, $\mathscr{E}_0 = R(E_{u,v}, \mathscr{O}_0)$, m the total number of variables in $\mathscr{E}_0$, and $V = \mathrm{Var}(E) \cup \mathrm{Var}(u, v)$. For any sequence

$$\langle \mathscr{S}_0, \mathscr{E}_0, \mathscr{O}_0 \rangle \Rightarrow^+ \langle \mathscr{S}_k, \mathscr{E}_k, \mathscr{O}_k \rangle$$

consisting of at most m transformation steps, if $\mathscr{S}_k$ is unifiable and $k \leqslant m$ is the first integer in the sequence such that $F \doteq T \in \mathscr{E}_k$, return the substitution $\theta_{\mathscr{S}_k} | V$, where $\theta_{\mathscr{S}_k}$ is the mgu of $\mathscr{S}_k$ (over $T_\Sigma(X)$).

We shall prove that the finite set of all substitutions returned by the method of Definition 7.3 forms a complete set of rigid E-unifiers of u and v. In particular, the method provides a decision procedure that is in NP. But first, we illustrate the method by means of two examples.

[13] Note that we are requiring that l_1/β and l_2 have a *nontrivial* unifier. The triangular form of mgus' is important for the NP-completeness of this method.

EXAMPLE 7.4. Let E be the set of equations $E = \{fa \doteq a,\ ggx \doteq fa\}$, and $\langle u, v\rangle = \langle gggx, x\rangle$. We have

$$E_{u,v} = \{fa \doteq a,\ ggx \doteq fa,\ eq(qqx, x) \doteq F,\ eq(z, z) \doteq T\}.$$

The congruence closure Π of $E_{u,v}$ has three nontrivial classes $\{a, fa, ggx\}$, $\{eq(gggx, x), F\}$, and $\{eq(z, z), T\}$. Let $\mathcal{O}_0$ be the order assignment on $E_{u,v}$ where every equivalence class is trivial and such that

$$T \prec_{\mathcal{O}_0} eq(gggx, x),$$
$$F \prec_{\mathcal{O}_0} eq(z, z),$$
$$a \prec_{\mathcal{O}_0} fa \prec_{\mathcal{O}_0} ggx,$$

the least elements of classes being ordered in the order of listing of the classes. We have $\mathcal{S}_0 = \varnothing$, and the reduced system $\mathcal{E}_0 = R(E_{u,v}, \mathcal{O}_0)$ is

$$\mathcal{E}_0 = \{fa \doteq a,\ ggx \doteq a,\ eq(ga, x) \doteq F,\ eq(z, z) \doteq T\}.$$

Note that there is an overlap between $eq(ga, x) \doteq F$ and $eq(z, z) \doteq T$ at address ε in $eq(ga, x)$, and we obtain the triangular system $\{\langle x, ga\rangle, \langle z, ga\rangle\}$ and the new equation $F \doteq T$. Thus, we have

$$\langle \mathcal{S}_0, \mathcal{E}_0, \mathcal{O}_0\rangle \Rightarrow \langle \mathcal{S}_1, \mathcal{E}_1, \mathcal{O}_1\rangle,$$

where $\mathcal{S}_1 = \{\langle x, ga\rangle, \langle z, ga\rangle\}$

$$\mathcal{E}'_1 = \{fa \doteq a,\ ggga \doteq a,\ eq(ga, ga) \doteq F,\ F \doteq T\},$$

and $\mathcal{O}_1$ is the restriction of $\mathcal{O}_0$ to the subterms in $\mathcal{E}'_1$. After reducing $\mathcal{E}'_1$, we have

$$\mathcal{E} = \{fa \doteq a,\ ggga \doteq a,\ eq(ga, ga) \doteq T,\ F \doteq T\}.$$

Since $F \doteq T \in \mathcal{E}_1$ and $\mathcal{S}_1$ is unifiable, the restriction $[ga/x]$ of the mgu $[ga/x, ga/z]$ of $\mathcal{S}_1$ to $\mathrm{Var}(E) \cup \mathrm{Var}(u, v) = \{x\}$ is a rigid E-unifier of $gggx$ and x.

EXAMPLE 7.5. Let E be the set of equations of Example 6.17 and $\langle u, v\rangle = \langle a \cdot b, b \cdot a\rangle$, so that

$$E_{u,v} = \{u_1 \cdot 1 \doteq u_1$$
$$w_1 \cdot w_1 \doteq 1$$
$$(x_1 \cdot y_1) \cdot z_1 \doteq x_1 \cdot (y_1 \cdot z_1)$$
$$(x_2 \cdot y_2 \cdot z_2 \doteq x_2 \cdot (y_2 \cdot z_2)$$

$$
\begin{aligned}
w_2 \cdot w_2 &\doteq 1\\
1 \cdot v_1 &\doteq v_1\\
(x_3 \cdot y_3) \cdot z_3 &\doteq x_3 \cdot (y_3 \cdot z_3)\\
(x_4 \cdot y_4) \cdot z_4 &\doteq x_4 \cdot (y_4 \cdot z_4)\\
w_3 \cdot w_3 &\doteq 1\\
eq(a \cdot b, b \cdot a) &\doteq F\\
eq(z, z) &\doteq T\}.
\end{aligned}
$$

In working out this example, the following useful fact will be used, Given an order assignment $\mathcal{O}$ on a partition Π associated with a set E of equations, if the rewrite system R obtained by orienting E using $\preccurlyeq_{\mathcal{O}}$ is already reduced, then there is no need to sort the least elements of the nontrivial classes.

Let $\mathcal{O}_0$ be the order assignment of Example 6.17. The set $E_{u,v}$ is already reduced, and so $\mathcal{E}_0 = R(E_{u,v}, \mathcal{O}_0) = E_{u,v}$.

There is an overlap between $(x_2 \cdot y_2) \cdot z_2 \doteq x_2 \cdot (y_2 \cdot z_2)$ and $w_2 \cdot w_2 \doteq 1$, due to the unification of the pair $\langle x_2 \cdot y_2, w_2 \cdot w_2 \rangle$. Thus we obtain the system

$$\mathcal{S}_1 = \{\langle x_2, w_2 \rangle, \langle y_2, w_2 \rangle\}$$

and the new equation

$$1 \cdot z_2 \doteq w_2 \cdot (w_2 \cdot z_2).$$

The nontrivial equivalence classes of the congruence closure Π_1 of $\mathcal{E}_1'$ are

$$
\begin{aligned}
&\{T, eq(z, z)\},\\
&\{F, eq(a \cdot b, b \cdot a)\},\\
&\{1, w_2 \cdot w_2, w_3 \cdot w_3, w_1 \cdot w_1\},\\
&\{u_1, u_1 \cdot 1\},\\
&\{v_1, 1 \cdot v_1\},\\
&\{1 \cdot z_2, w_2 \cdot (w_2 \cdot z_2)\},\\
&\{x_4 \cdot (y_4 \cdot z_4), (x_4 \cdot y_4) \cdot z_4\},\\
&\{x_3 \cdot (y_3 \cdot z_3), (x_3 \cdot y_3) \cdot z_3\},\\
&\{x_1 \cdot (y_1 \cdot z_1), (x_1 \cdot y_1) \cdot z_1\}.
\end{aligned}
$$

We define the order assignment $\mathcal{O}_1$ on Π_1 whose equivalence relation is the identity and such that the ordering $\preccurlyeq_{\mathcal{O}_1}$ is defined by the order in which the elements in each class of Π_1 are listed, and for the least elements in these classes, the order in which the classes are listed. It is easy to see that

$$\begin{aligned}
\mathscr{E}_1 = \{ & u_1 \cdot 1 \doteq u_1 \\
& w_1 \cdot w_1 \doteq 1 \\
& (x_1 \cdot y_1) \cdot z_1 \doteq x_1 \cdot (y_1 \cdot z_1) \\
& w_2 \cdot (w_2 \cdot z_2) \doteq 1 \cdot z_2 \\
& w_2 \cdot w_2 \doteq 1 \\
& 1 \cdot v_1 \doteq v_1 \\
& (x_3 \cdot y_3) \cdot z_3 \doteq x_3 \cdot (y_3 \cdot z_3) \\
& (x_4 \cdot y_4) \cdot z_4 \doteq x_4 \cdot (y_4 \cdot z_4) \\
& w_3 \cdot w_3 \doteq 1 \\
& eq(a \cdot b, b \cdot a) \doteq F \\
& eq(z, z) \doteq T \}.
\end{aligned}$$

There is an overlap between $1 \cdot z_2 \doteq w_2 \cdot (w_2 \cdot z_2)$ and $1 \cdot v_1 \doteq v_1$, due to the unification of the pair $\langle 1 \cdot z_2, 1 \cdot v_1 \rangle$. Thus we obtain the system

$$\mathscr{S}_2 = \{ \langle x_2, w_2 \rangle, \langle y_2, w_2 \rangle, \langle z_2, v_1 \rangle \}$$

and the new equation

$$v_1 \doteq w_2 \cdot (w_2 \cdot v_1).$$

The nontrivial equivalence classes of the congruence closure Π_2 of $\mathscr{E}_2'$ are

$$\begin{aligned}
& \{T, eq(z, z)\}, \\
& \{F, eq(a \cdot b, b \cdot a)\}, \\
& \{1, w_2 \cdot w_2, w_3 \cdot w_3, w_1 \cdot w_1\}, \\
& \{u_1, u_1 \cdot 1\}, \\
& \{v_1, 1 \cdot v_1, w_2 \cdot (w_2 \cdot v_1)\}, \\
& \{x_4 \cdot (y_4 \cdot z_4), (x_4 \cdot y_4) \cdot z_4\}, \\
& \{x_3 \cdot (y_3 \cdot z_3), (x_3 \cdot y_3) \cdot z_3\}, \\
& \{x_1 \cdot (y_1 \cdot z_1), (x_1 \cdot y_1) \cdot z_1\}.
\end{aligned}$$

We define the order assignment $\mathcal{O}_2$ on Π_2 whose equivalence relation is the identity and such that the ordering $\preccurlyeq_{\mathcal{O}_2}$ is defined by the order in which the elements in each class of Π_2 are listed, and for the least elements in these classes, the order in which the classes are listed. It is easy to see that

$$\begin{aligned}
\mathcal{E}_2 = \{ u_1 \cdot 1 &\doteq u_1 \\
w_1 \cdot w_1 &\doteq 1 \\
(x_1 \cdot y_1) \cdot z_1 &\doteq x_1 \cdot (y_1 \cdot z_1) \\
w_2 \cdot (w_2 \cdot v_1) &\doteq v_1 \\
w_2 \cdot w_2 &\doteq 1 \\
1 \cdot v_1 &\doteq v_1 \\
(x_3 \cdot y_3) \cdot z_3 &\doteq x_3 \cdot (y_3 \cdot z_3) \\
(x_4 \cdot y_4) \cdot z_4 &\doteq x_4 \cdot (y_4 \cdot z_4) \\
w_3 \cdot w_3 &\doteq 1 \\
eq(a \cdot b, b \cdot a) &\doteq F \\
eq(z, z) &\doteq T \}.
\end{aligned}$$

The next two steps are similar to the previous two. Due to the similarities, we omit some details.

There is an overlap between $x_4 \cdot (y_4 \cdot z_4) \doteq (x_4 \cdot y_4) \cdot z_4$ and $w_3 \cdot w_3 \doteq 1$, due to the unification of the pair $\langle y_4 \cdot z_4, w_3 \cdot w_3 \rangle$. We obtain the system

$$\begin{aligned}
\mathcal{S}_3 = \{ &\langle x_2, w_2 \rangle, \langle y_2, w_2 \rangle, \langle z_2, v_1 \rangle, \\
&\langle y_4, w_3 \rangle, \langle z_4, w_3 \rangle \}
\end{aligned}$$

and the new equation

$$x_4 \cdot 1 \doteq (x_4 \cdot w_3) \cdot w_3.$$

The order assignment $\mathcal{O}_3$ is easily determined, and we have

$$\begin{aligned}
\mathcal{E}_3 = \{ u_1 \cdot 1 &\doteq u_1 \\
w_1 \cdot w_1 &\doteq 1 \\
(x_1 \cdot y_1) \cdot z_1 &\doteq x_1 \cdot (y_1 \cdot z_1) \\
w_2 \cdot (w_2 \cdot v_1) &\doteq v_1
\end{aligned}$$

$$w_2 \cdot w_2 \doteq 1$$
$$1 \cdot v_1 \doteq v_1$$
$$(x_3 \cdot y_3)\, z_3 \doteq x_3 \cdot (y_3 \cdot z_3)$$
$$(x_4 \cdot w_3) \cdot w_3 \doteq x_4 \cdot 1$$
$$w_3 \cdot w_3 \doteq 1$$
$$eq(a \cdot b, b \cdot a) \doteq F$$
$$eq(z, z) \doteq T\}.$$

The next overlap is between $x_4 \cdot 1 \doteq (x_4 \cdot w_3) \cdot w_3$ and $u_1 \cdot 1 \doteq u_1$, due to the unification of the pair $\langle x_4 \cdot 1, u_1 \cdot 1 \rangle$. We obain the system

$$\mathscr{S}_4 = \{\langle x_2, w_2 \rangle, \langle y_2, w_2 \rangle, \langle z_2, v_1 \rangle,$$
$$\langle y_4, w_3 \rangle, \langle z_4, w_3 \rangle, \langle x_4, u_1 \rangle\}$$

and the new equation

$$(u_1 \cdot w_3) \cdot w_3 \doteq u_1.$$

The order assignment $\mathscr{O}_4$ is easily determined, and we have

$$\mathscr{E}_4 = \{u_1 \cdot 1 \doteq u_1$$
$$w_1 \cdot w_1 \doteq 1$$
$$(x_1 \cdot y_1) \cdot z_1 \doteq x_1 \cdot (y_1 \cdot z_1)$$
$$w_2 \cdot (w_2 \cdot v_1) \doteq v_1$$
$$w_2 \cdot w_2 \doteq 1$$
$$1 \cdot v_1 \doteq v_1$$
$$(x_3 \cdot y_3) \cdot z_3 \doteq x_3 \cdot (y_3 \cdot z_3)$$
$$(u_1 \cdot w_3) \cdot w_3 \doteq u_1$$
$$w_3 \cdot w_3 \doteq 1$$
$$eq(a \cdot b, b \cdot a) \doteq F$$
$$eq(z, z) \doteq T\}.$$

The next overlap is between $x_1(y_1 \cdot z_1) \doteq (x_1 \cdot y_1) \cdot z_1$ and $w_1 \cdot w_1 \doteq 1$, due to the unification of the pair $\langle y_1 \cdot z_1, w_1 \cdot w_1 \rangle$. We obtain the system

$$\mathscr{S}_5\{\langle x_2, w_2 \rangle, \langle y_2, w_2 \rangle, \langle z_2, v_1 \rangle,$$
$$\langle y_4, w_3 \rangle, \langle z_4, w_3 \rangle, \langle x_4, u_1 \rangle,$$
$$\langle y_1, w_1 \rangle, \langle z_1, w_1 \rangle\}$$

and the new equation

$$x_1 \cdot 1 \doteq (x_1 \cdot w_1) \cdot w_1.$$

The order assignement $\mathcal{O}_5$ is easily determined, and we have

$$\begin{aligned}
\mathcal{E}_5 = \{ & u_1 \cdot 1 \doteq u_1 \\
& w_1 \cdot w_1 \doteq 1 \\
& (x_1 \cdot w_1) \cdot w_1 \doteq x_1 \cdot 1 \\
& w_2 \cdot (w_2 \cdot v_1) \doteq v_1 \\
& w_2 \cdot w_2 \doteq 1 \\
& 1 \cdot v_1 \doteq v_1 \\
& (x_3 \cdot y_3) \cdot z_3 \doteq x_3 \cdot (y_3 \cdot z_3) \\
& (u_1 \cdot w_3) \cdot w_3 \doteq u_1 \\
& w_3 \cdot w_3 \doteq 1 \\
& eq(a \cdot b, b \cdot a) \doteq F \\
& eq(z, z) \doteq T \}.
\end{aligned}$$

The next overlap is between $x_1 \cdot 1 \doteq (x_1 \cdot w_1) \cdot w_1$ and $u_1 \cdot 1 \doteq u_1$, due to the unification of the pair $\langle x_1 \cdot 1, u_1 \cdot 1 \rangle$. We obtain the system

$$\begin{aligned}
\mathcal{S}_6 = \{ & \langle x_2, w_2 \rangle, \langle y_2, w_2 \rangle, \langle z_2, v_1 \rangle, \\
& \langle y_4, w_3 \rangle, \langle z_4, w_3 \rangle, \langle x_4, u_1 \rangle, \\
& \langle y_1, w_1 \rangle, \langle z_1, w_1 \rangle, (u_1, x_1 \rangle \}
\end{aligned}$$

and the new equation

$$x_1 \doteq (x_1 \cdot w_1) \cdot w_1.$$

The nontrivial equivalence classes of the congruence closure Π_6 of $\mathcal{E}'_6$ are

$$\begin{aligned}
& \{T, eq(z, z)\}, \\
& \{F, eq(a \cdot b, b \cdot a)\}, \\
& \{1, w_2 \cdot w_2, w_3 \cdot w_3, w_1 \cdot w_1\}, \\
& \{x_1, x_1 \cdot 1, (x_1 \cdot w_3) \cdot w_3, (x_1 \cdot w_1) \cdot w_1\}, \\
& \{v_1, 1 \cdot v_1, w_2 \cdot (w_2 \cdot v_1)\}, \\
& \{x_3 \cdot (y_3 \cdot z_3), (x_3 \cdot y_3) \cdot z_3\}.
\end{aligned}$$

We define the order assignment $\mathcal{O}_6$ on Π_6 whose equivalence relation is the identity and such that the ordering $\preccurlyeq_{\mathcal{O}_6}$ is defined by the order in which the elements in each class of Π_6 are listed, and for the least elements in these classes, the order in which the classes are listed. It is easy to see that

$$\begin{aligned}
\mathscr{E}_6 = \{ & x_1 \cdot 1 \doteq x_1 \\
& w_1 \cdot w_1 \doteq 1 \\
& (x_1 \cdot w_1) \cdot w_1 \doteq x_1 \\
& w_2(w_2 \cdot v_1) \doteq v_1 \\
& w_2 \cdot w_2 \doteq 1 \\
& 1 \cdot v_1 \doteq v_1 \\
& (x_3 \cdot y_3) \cdot z_3 \doteq x_3 \cdot (y_3 \cdot z_3) \\
& (x_1 \cdot w_3) \cdot w_3 \doteq x_1 \\
& w_3 \cdot w_3 \doteq 1 \\
& eq(a \cdot b, b \cdot a) \doteq F \\
& eq(z, z) \doteq T \}.
\end{aligned}$$

The next overlap is between $(x_1 \cdot w_1) \cdot w_1 \doteq x_1$ and $w_2 \cdot (w_2 \cdot v_1) \doteq v_1$, due to the unification of the pair $\langle x_1 \cdot w_1, w_2 \cdot (w_2 \cdot v_1) \rangle$. We obtain the system

$$\begin{aligned}
\mathscr{S}_7 = \{ & \langle x_2, w_2 \rangle, \langle y_2, w_2 \rangle, \langle z_2, v_1 \rangle, \\
& \langle y_4, w_3 \rangle, \langle z_4, w_3 \rangle, \langle x_4, u_1 \rangle, \\
& \langle y_1, w_1 \rangle, \langle z_1, w_1 \rangle, \langle u_1, x_1 \rangle, \\
& \langle x_1, w_2 \rangle, \langle w_1, w_2 \cdot v_1 \rangle \}
\end{aligned}$$

and the new equation

$$v_1 \cdot (w_2 \cdot v_1) \doteq w_2.$$

The order assignment $\mathcal{O}_7$ is easily determined, and we have

$$\begin{aligned}
\mathscr{E}_7 = \{ & w_2 \cdot 1 \doteq w_2 \\
& (w_2 \cdot v_1) \cdot (w_2 \cdot v_1) \doteq 1 \\
& v_1 \cdot (w_2 \cdot v_1) \doteq w_2 \\
& w_2 \cdot (w_2 \cdot v_1) \doteq v_1
\end{aligned}$$

$$w_2 \cdot w_2 \doteq 1$$
$$1 \cdot v_1 \doteq v_1$$
$$(x_3 \cdot y_3) \cdot z_3 \doteq x_3 \cdot (y_3 \cdot z_3)$$
$$(w_2 \cdot w_3) \cdot w_3 \doteq w_2$$
$$w_3 \cdot w_3 \doteq 1$$
$$eq(a \cdot b, b \cdot a) \doteq F$$
$$eq(z, z) \doteq T\}.$$

The next overlap is between $x_3 \cdot (y_3 \cdot z_3) \doteq (x_3 \cdot y_3) \cdot z_3$ and $(w_2 \cdot w_3) \cdot w_3 \doteq w_2$, due to the unification of the pair $\langle y_3 \cdot z_3, (w_2 \cdot w_3) \cdot w_3 \rangle$. We obtain the system

$$\begin{aligned}\mathcal{S}_8 = \{&\langle x_2, w_2\rangle, \langle y_2, w_2\rangle, \langle z_2, v_1\rangle,\\ &\langle y_4, w_3\rangle, \langle z_4, w_3\rangle, \langle x_4, u_1\rangle,\\ &\langle y_1, w_1\rangle, \langle z_1, w_1\rangle, \langle u_1, x_1\rangle,\\ &\langle x_1, w_2\rangle, \langle w_1, w_2 \cdot v_1\rangle, \langle y_3, w_2 \cdot w_3\rangle,\\ &\langle z_3, w_3\rangle\}\end{aligned}$$

and the new equation

$$x_3 \cdot w_2 \doteq (x_3 \cdot (w_2 \cdot w_3)) \cdot w_3.$$

The order assignment $\mathcal{O}_8$ is easily determined, and we have

$$\begin{aligned}\mathcal{E}_0 = \{&w_2 \cdot 1 \doteq w_2\\ &(w_2 \cdot v_1) \cdot (w_2 \cdot v_1) \doteq 1\\ &v_1 \cdot (w_2 \cdot v_1) \doteq w_2\\ &w_2 \cdot (w_2 \cdot v_1) \doteq v_1\\ &w_2 \cdot w_2 \doteq 1\\ &1 \cdot v_1 \doteq v_1\\ &(x_3 \cdot (w_2 \cdot w_3)) \cdot w_3 \doteq x_3 \cdot x_2\\ &(w_2 \cdot w_3) \cdot w_3 \doteq w_2\\ &w_3 \cdot w_3 \doteq 1\\ &eq(a \cdot b, b \cdot a) \doteq F\\ &eq(z, z) \doteq T\}.\end{aligned}$$

The next overlap is between $(x_3 \cdot (w_2 \cdot w_3)) \cdot w_3 \doteq x_3 \cdot w_2$ and $v_1 \cdot (w_2 \cdot v_1) \doteq w_2$, due to the unification of the pair $\langle x_3 \cdot (w_2 \cdot w_3), v_1 \cdot (w_2 \cdot v_1) \rangle$. We obtain the system

$$\begin{aligned}\mathscr{S}_9 = \{&\langle x_2, w_2\rangle, \langle y_2, w_2\rangle, \langle z_2, v_1\rangle,\\ &\langle y_4, w_3\rangle, \langle z_4, w_3\rangle, \langle x_4, u_1\rangle,\\ &\langle y_1, w_1\rangle, \langle z_1, w_1\rangle, \langle u_1, x_1\rangle,\\ &\langle x_1, w_2\rangle, \langle w_1, w_2 \cdot v_1\rangle, \langle y_3, w_2 \cdot w_3\rangle,\\ &\langle z_3, w_3\rangle, \langle x_3, v_1\rangle, \langle w_3, v_1\rangle\}\end{aligned}$$

and the new equation

$$w_2 \cdot v_1 \doteq v_1 \cdot w_2.$$

The order assignment $\mathscr{O}_9$ is easily determined, and we have

$$\begin{aligned}\mathscr{E}_9 = \{&w_2 \cdot 1 \doteq w_2\\ &(w_2 \cdot v_1) \cdot (w_2 \cdot v_1) \doteq 1\\ &v_1 \cdot (w_2 \cdot v_1) \doteq w_2\\ &w_2 \cdot (w_2 \cdot v_1) \doteq v_1\\ &w_2 \cdot w_2 \doteq 1\\ &1 \cdot v_1 \doteq v_1\\ &v_1 \cdot w_2 \doteq w_2 \cdot v_1\\ &(w_2 \cdot v_1) \cdot v_1 \doteq w_2\\ &v_1 \cdot v_1 \doteq 1\\ &eq(a \cdot b, b \cdot a) \doteq F\\ &eq(z, z) \doteq T\}.\end{aligned}$$

The next overlap is between $eq(a \cdot b, b \cdot a) \doteq F$ and $v_1 \cdot w_2 \doteq w_2 \cdot v_1$, due to the unification of the pair $\langle b \cdot a, v_1 \cdot w_2\rangle$. We obtain the system

$$\begin{aligned}\mathscr{S}_{10} = \{&\langle x_2, w_2\rangle, \langle y_2, w_2\rangle, \langle z_2, v_1\rangle,\\ &\langle y_4, w_3\rangle, \langle z_4, w_3\rangle, \langle x_4, u_1\rangle,\\ &\langle y_1, w_1\rangle, \langle z_1, w_1\rangle, \langle u_1, x_1\rangle,\\ &\langle x_1, w_2\rangle, \langle w_1, w_2 \cdot v_1\rangle, \langle y_3, w_2 \cdot w_3\rangle,\\ &\langle z_3, w_3\rangle, \langle x_3, v_1\rangle, \langle w_3, v_1\rangle,\\ &\langle v_1, b\rangle, \langle w_2, a\rangle\}\end{aligned}$$

and the new equation

$$eq(a \cdot b, a \cdot b) \doteq F.$$

The order assignment $\mathcal{O}_{10}$ is obvious, and we have

$$\begin{aligned}
\mathcal{E}_{10} = \{ & a \cdot 1 \doteq a \\
& (a \cdot b) \cdot (a \cdot b) \doteq 1 \\
& b \cdot (a \cdot b) \doteq a \\
& a \cdot (a \cdot b) \doteq b \\
& a \cdot a \doteq 1 \\
& 1 \cdot b \doteq b \\
& b \cdot a \doteq a \cdot b \\
& (a \cdot b) \cdot b \doteq a \\
& b \cdot b \doteq 1 \\
& eq(a \cdot b, a \cdot b) \doteq F \\
& eq(z, z) \doteq T \}.
\end{aligned}$$

The last overlap is between $eq(z, z) \doteq T$ and $eq(a \cdot b, a \cdot b) \doteq F$. We obtain the system

$$\begin{aligned}
\mathcal{S}_{11} = \{ & \langle x_2, w_2 \rangle, \langle y_2, w_2 \rangle, \langle z_2, v_1 \rangle, \\
& \langle y_4, w_3 \rangle, \langle z_4, w_3 \rangle, \langle x_4, u_1 \rangle, \\
& \langle y_1, w_1 \rangle, \langle z_1, w_1 \rangle, \langle u_1, x_1 \rangle, \\
& \langle x_1, w_2 \rangle, \langle w_1, w_2 \cdot v_1 \rangle, \langle y_3, w_2 \cdot w_3 \rangle, \\
& \langle z_3, w_3 \rangle, \langle x_3, v_1 \rangle, \langle w_3, v_1 \rangle, \\
& \langle v_1, b \rangle, \langle w_2, a \rangle, \langle z, a \cdot b \rangle \}
\end{aligned}$$

and the new equation

$$F \doteq T.$$

After reducing $\mathcal{E}'_{11}$, we obtain

$$\begin{aligned}
\mathscr{E}_{11} = \{ a \cdot 1 &\doteq a \\
(a \cdot b) \cdot (a \cdot b) &\doteq 1 \\
b \cdot (a \cdot b) &\doteq a \\
a \cdot (a \cdot b) &\doteq b \\
a \cdot a &\doteq 1 \\
1 \cdot b &\doteq b \\
b \cdot a &\doteq a \cdot b \\
(a \cdot b) \cdot b &\doteq a \\
b \cdot b &\doteq 1 \\
eq(a \cdot b, a \cdot b) &\doteq T \\
F &\doteq T \}.
\end{aligned}$$

Since $F \doteq T \in \mathscr{E}_{11}$ and $\mathscr{S}_{11}$ is unifiable, the restriction of the mgu of $\mathscr{S}_{11}$ to $\mathrm{Var}(E)$ is a rigid E-unifier of $a \cdot b$ and $b \cdot a$, and it is easy to verify that this substitution is

$$\begin{aligned}
\theta = [& a/u_1, a/x_1, a/x_2, a/y_2, a/w_2, a/x_4, \\
& b/z_2, b/v_1, b/x_3, v/z_3, b/y_4, b/z_4, b/w_3, \\
& a \cdot b/w_1, a \cdot b/y_1, a \cdot b/z_1, a \cdot b/y_3].
\end{aligned}$$

Hence, we have shown that every monoid such that $x \cdot x = 1$ for all x is commutative.

It is interesting to note that most of the guessing in Example 7.5 has to do with guessing overlaps among equations, because the ordering of the terms is never really problematic. This is because we can use the subterm property, the fact that consants are always smaller than compound terms, and some depth considerations. By contrast, we shall redo Example 7.5 using the order assignment $\mathscr{O}'$ of Example 6.17. This time, it will not even be necessary to form critical pairs, but this is because $\mathscr{O}'$ is already a guess of a solution! Note that this guess represents one partition among a very large number of partitions. We will come back to this point after the example.

EXAMPLE 7.6. Recall that the nontrivial equivalence classes of $\equiv_{\mathscr{O}'}$ are

$$\{a, u_1, x_1, x_2, y_2, w_2, x_4\},$$
$$\{b, z_2, v_1, x_3, z_3, y_4, z_4, w_3\},$$

$$\{w_2 \cdot w_2, x_2 \cdot y_2\},$$
$$\{a \cdot b, w_1, y_1, z_1, y_3, z, y_2 \cdot z_2, x_4 \cdot y_4\},$$
$$\{w_3 \cdot w_3, y_4 \cdot z_4\},$$
$$\{w_1 \cdot w_1, y_1 \cdot z_1\}.$$

Using the method of Definition 6.21 for choosing a representative selector and forming a reduced set of equations, it is easy to see that $E_{u,v}$ yields the set of ground equations

$$\begin{aligned}
\mathscr{E}' = \{a \cdot 1 &\doteq a \\
(a \cdot b) \cdot (a \cdot b) &\doteq 1 \\
(a \cdot (a \cdot b)) \cdot (a \cdot b) &\doteq a \cdot ((a \cdot b) \cdot (a \cdot b)) \\
(a \cdot a) \cdot b &\doteq a \cdot (a \cdot b) \\
a \cdot a &\doteq 1 \\
1 \cdot b &\doteq b \\
(b \cdot (a \cdot b)) \cdot b &\doteq b \cdot ((a \cdot b) \cdot b) \\
(a \cdot b) \cdot b &\doteq a \cdot (b \cdot b) \\
b \cdot b &\doteq 1 \\
eq(a \cdot b, b \cdot a) &\doteq F \\
eq(a \cdot b, a \cdot b) &\doteq T\}.
\end{aligned}$$

With a little bit of work, one can verify that F and T are congruent from $\mathscr{E}'$. Thus, we have found a solution, and it easy to see that the joint mgu of the classes of $\equiv_{\mathscr{O}'}$ is the substitution θ of Example 7.5.

It is particularly appropriate at this point to comment on the computational complexity of guessing an order assignment $\mathscr{O}$. Note that this involves guessing an equivalence relation $\equiv_{\mathscr{O}}$, that is, a partition. The number of partitions on a set of n elements is given by the "Bell exponential number" B_n (Berge [6]). The Bell numbers have the remarkable property that

$$\sum_{n=0}^{\infty} \frac{B_n}{n!} t^n = e^{e^t - 1}.$$

From this, we have the formula

$$B_{n+1} = \frac{1}{e}\left(1 + \frac{2^n}{1!} + \frac{3^n}{2!} + \frac{4^n}{3!} + \cdots + \frac{m^n}{(m-1)!} + \cdots\right)$$

attributed to G. Dobinski (Berge [6]), which shows clearly that B_{n+1} grows exponentially fast. In the case of Example 7.6, there are 18 variables, and B_{17} is already a respectable number! It is therefore highly desirable to find criteria for weeding out partitions that will lead to failure of the method. It is also desirable to favor the formation of critical pairs, since this is much more deterministic than guessing partitions.

8. Soundness, Completeness, and Decidability of the Method

First, we show the soundness of the method.

THEOREM 8.1 (Soundness). *Let E be a set of equations over $T_\Sigma(X)$, u, v two terms in $T_\Sigma(X)$, $E_{u,v} = E \cup \langle eq(z,z) \doteq T, eq(u,v) \doteq F\}$, $\mathcal{C}_0$ an order assignment on $E_{u,v}$, $\mathcal{S}_0 = TU_{\mathcal{C}_0}$, $\mathcal{E}_0 = R(E_{u,v}, \mathcal{C}_0)$, m the total number of variables in $\mathcal{E}_0$, and $V = \mathrm{Var}(E) \cup \mathrm{Var}(u,v)$. If*

$$\langle \mathcal{S}_0, \mathcal{E}_0, \mathcal{C}_0 \rangle \Rightarrow^+ \langle \mathcal{S}_k, \mathcal{E}_k, \mathcal{C}_k \rangle,$$

where $\mathcal{S}_k$ is unifiable, $F \doteq T \in \mathcal{E}_k$ and $F \doteq T \notin \mathcal{E}_i$ for all i, $0 \leqslant i < k \leqslant m$, then $\theta_{\mathcal{S}_k}|_V$ is a rigid E-unifier of u and v, where $\theta_{\mathcal{S}_k}$ is the mgu of $\mathcal{S}_k$ (over $T_\Sigma(X)$).

Proof. We shall prove the following claim by induction on k.

Claim. Given any set $\mathcal{E} = \mathcal{E}_\Sigma \cup \{eq(u,v) \doteq F, \mathrm{eq}(z,z) \doteq T\}$, with $\mathcal{E}_\Sigma$ a set of equations over $T_\Sigma(X)$ and $u, v \in T_\Sigma(X)$, for any triple $\langle \mathcal{S}_0, \mathcal{E}_0, \mathcal{C}_0 \rangle$, where $\mathcal{C}_0$ is an order assignment on $\mathcal{E}$, $\mathcal{S}_0$ is any triangular form containing $TU_{\mathcal{C}_0}$, and $\mathcal{E}_0 = R(\mathcal{E}, \mathcal{C}_0)$, if

$$\langle \mathcal{S}_0, \mathcal{E}_0, \mathcal{C}_0 \rangle \Rightarrow^+ \langle \mathcal{S}_k, \mathcal{E}_k, \mathcal{C}_k \rangle,$$

where $\mathcal{S}_k$ is unifiable, $F \doteq T \in \mathcal{E}_k$, and $F \doteq T \notin \mathcal{E}_i$ for all i, $0 \leqslant i < k \leqslant m$, then $\theta_{\mathcal{S}_k}$ is a rigid $\mathcal{E}$-unifier of T and F, where $\theta_{\mathcal{S}_k}$ is the mgu of $\mathcal{S}_k$ (over $T_\Sigma(X)$).

Proof of Claim. In the base case, we must have $k = 1$ because $F \doteq T \notin \mathcal{E}_0 \cup \mathcal{E}_0^{-1}$. In order that $F \doteq T$ be in $\mathcal{E}_1$, the transformation step must be

$$\langle \mathcal{S}_0, \mathcal{E}_0, \mathcal{C}_0 \rangle \Rightarrow \langle \mathcal{S}_0 \cup TU(eq(z,z), eq(u,v)) \cup TU_{\mathcal{C}_1}, R(\mathcal{E}_1', \mathcal{C}_1), \mathcal{C}_1 \rangle,$$

where $\mathcal{E}_1' = \sigma((\mathcal{E}_0 - \{eq(z,z) \doteq T\}) \cup \{F \doteq T\})$, $TU(eq(z,z), eq(u,v))$ is the triangular form of a mgu of $eq(z,z)$ and $eq(u,v)$(over $T_\Sigma(X)$), and

$\theta' = \theta_{\mathscr{S}_1}$ is the mgu of $\mathscr{S}_1$. Since $TU(eq(z, z), eq(u, v))$ is a triangular form of the mgu of $eq(z, z)$ and $eq(u, v)$ and θ' is the mgu of $\mathscr{S}_1 = \mathscr{S}_0 \cup TU(eq(z, z), eq(u, v)) \cup TU_{\mathscr{C}_1}$, we have $\theta'(eq(u, v)) = \theta'(eq(z, z))$. Since $eq(u, v) \doteq F$ and $eq(z, z) \doteq T$ are in $\mathscr{E}_0$, we have $T \overset{*}{\cong}_{\theta'(\mathscr{E}_0)} F$, and θ' is a rigid $\mathscr{E}_0$-unifier of T and F (over $T_\Sigma(X)$). Recall that $TU_{\mathscr{C}_0} \subseteq \mathscr{S}_0$. Since $\mathscr{S}_0 \subseteq \mathscr{S}_1$ and θ' is a mgu of $\mathscr{S}_1$, θ' unifies $TU_{\mathscr{C}_0}$. Thus, by Lemma 6.26(i), $\theta'(\mathscr{E})$ and $\theta'(\mathscr{E}_0) = \theta'(R(\mathscr{E}, \mathscr{C}_0))$ are rigid equivalent. Therefore, θ' is a rigid $\mathscr{E}$-unifier of T and F.

For the induction step, assume that

$$\langle \mathscr{S}_0, \mathscr{E}_0, \mathscr{C}_0 \rangle \Rightarrow \langle \mathscr{S}_1, \mathscr{E}_1, \mathscr{C}_1 \rangle \Rightarrow^+ \langle \mathscr{S}_k, \mathscr{E}_k, \mathscr{C}_k \rangle,$$

where $\mathscr{S}_1 = \mathscr{S}_0 \cup TU(l_1/\beta, l_2) \cup TU_{\mathscr{C}_1}$, $\mathscr{E}_1 = R(\mathscr{E}'_1, \mathscr{C}_1)$ with

$$\mathscr{E}'_1 = \sigma((\mathscr{E}_0 - \{l_1 \doteq r_1\})^\dagger \cup \{l_1[\beta \leftarrow r_2] \doteq r_1\}),$$

$\mathscr{S}_k$ is unifiable, $F \doteq T \in \mathscr{E}_k$, $F \doteq T \notin \mathscr{E}_i$ for all i, $0 \leqslant i < k \leqslant m$, $TU(l_1/\beta, l_2)$ represents a mgu of l_1/β and l_2 in triangular form, $\sigma = [t_1/x_1, ..., t_p/x_p]$, where $TU(l_1/\beta, l_2) = \{\langle x_1, t_1 \rangle, ..., \langle x_p, t_p \rangle\}$, and $\theta' = \theta_{\mathscr{S}_k}$ is the mgu of $\mathscr{S}_k$ over $T_\Sigma(X)$. Note that $TU_{\mathscr{C}_1} \subseteq \mathscr{S}_1 \subseteq \mathscr{S}_k$ and $l_1[\beta \leftarrow r_2] \doteq r_1$ cannot be $F \doteq T$. Thus the induction hypothesis applies to $\langle \mathscr{S}_1, \mathscr{E}_1, \mathscr{C}_1 \rangle$, and the mgu θ' of $\mathscr{S}_k$ is a rigid $\mathscr{E}_1$-unifier of T and F (over $T_\Sigma(X)$). Since θ' is a mgu of $\mathscr{S}_k$, $TU(l_1/\beta, l_2) \subseteq \mathscr{S}_k$, and $TU(l_1/\beta, l_2)$ represents a mgu of l_1/β and l_2 in triangular form, we have $\theta'(l_1/\beta) = \theta'(l_2)$. Because $TU(l_1/\beta, l_2)$ represents a mgu of l_1/β and l_2 in triangular form, σ is the substitution associated with $TU(l_1/\beta, l_2)$, and θ' is a unifier of $TU(l_1/\beta, l_2)$, by Lemma 3.5, we have $\sigma; \theta' = \theta'$. Consequently

$$\begin{aligned} \theta'(\mathscr{E}'_1) &= \theta'(\sigma((\mathscr{E}_0 - \{l_1 \doteq r_1\})^\dagger \cup \{l_1[\beta \leftarrow r_2] \doteq r_1\})) \\ &= \theta'((\mathscr{E}_0 - \{l_1 \doteq r_1\})^\dagger \cup \{l_1[\beta \leftarrow r_2] \doteq r_1\}). \end{aligned} \tag{1}$$

From $\theta'(l_1/\beta) = \theta'(l_2)$, we have

$$\theta'(l_1) = \theta'(l_1)[\beta \leftarrow \theta'(l_1/\beta)] = \theta'(l_1)[\beta \leftarrow \theta'(l_2)]. \tag{2}$$

Then we have

$$\begin{aligned} \theta'(l_1[\beta \leftarrow r_2]) &= \theta'(l_1)[\beta \leftarrow \theta'(r_2)] \\ &\rightarrow_{\theta'(r_2 \doteq l_2)} \theta'(l_1)[\beta \leftarrow \theta'(l_2)] \\ &= \theta'(l_1) \qquad \text{by (2)}, \\ &\rightarrow_{\theta'(l_1 \doteq r_1)} \theta'(r_1) \end{aligned}$$

and

$$\begin{aligned}\theta'(l_1) &= \theta'(l_1)[\beta \leftarrow \theta'(l_2)] \qquad \text{by (2)}\\ &\to_{\theta'(l_2 \doteq r_2)} \theta'(l_1)[\beta \leftarrow \theta'(r_2)]\\ &= \theta'(l_1[\beta \leftarrow r_2])\\ &\to_{\theta'(l_1[\beta \leftarrow r_2] \doteq r_1)} \theta'(r_1)\end{aligned}$$

Thus, $\theta'(l_1[\beta \leftarrow r_2] \doteq r_1)$ is provable from $\{\theta'(l_1 \doteq r_1), \theta'(l_2 \doteq r_2)\}$ and $\theta'(l_1 \doteq r_1)$ is provable from $\{\theta'(l_1(\beta \leftarrow r_2] \doteq r_1), \theta'(l_2 \doteq r_2)\}$. Since $l_1 \doteq r_1, l_2 \doteq r_2 \in \mathscr{E}_0 \cup \mathscr{E}_0^{-1}$, then $\theta'(\mathscr{E}_0)$ and $\theta'((\mathscr{E}_0 - \{l_1 \doteq r_1\})^{\dagger} \cup \{l_1[\beta \leftarrow r_2] \doteq r_1\})$ are rigid equivalent and by (1), $\theta'(\mathscr{E}_1')$ and $\theta'(\mathscr{E}_0)$ are rigid equivalent. Since $TU_{\mathscr{C}_1} \subseteq \mathscr{S}_1 \subseteq \mathscr{S}_k$ and θ' is the mgu of $\mathscr{S}_k$, θ' unifies $TU_{\mathscr{C}_1}$, and, by Lemma 6.26(i), $\theta'(\mathscr{E}_1) = \theta'(R(\mathscr{E}_1', \mathscr{C}_1))$ is rigid equivalent to $\theta'(\mathscr{E}_1')$. Since we just showed that $\theta'(\mathscr{E}_1')$ and $\theta'(\mathscr{E}_0)$ are rigid equivalent, then $\theta'(\mathscr{E}_1)$ is rigid equivalent to $\theta'(\mathscr{E}_0)$. Hence, since by the induction hypothesis $T \overset{*}{\cong}_{\theta'(\mathscr{E}_1)} F$, we have $T \overset{*}{\cong}_{\theta'(\mathscr{E}_0)} F$, and θ' is a rigid $\mathscr{E}_0$-unifier of T and F (over $T_\Sigma(X)$). Since $TU_{\mathscr{C}_0} \subseteq \mathscr{S}_0 \subseteq \mathscr{S}_k$ and θ' is a mgu of $\mathscr{S}_k$, θ' unifies $TU_{\mathscr{C}_0}$. Thus, by Lemma 6.26(i), $\theta'(\mathscr{E})$ and $\theta'(\mathscr{E}_0) = \theta'(R(\mathscr{E}, \mathscr{C}_0))$ are rigid equivalent. Therefore, θ' is a rigid $\mathscr{E}$-unifier of T and F. This concludes the induction step and the proof of the claim. ▮

Applying the claim to $\mathscr{C}_0 = TU_{\mathscr{C}_0}$, and $\mathscr{E}_0 = R(E_{u,v}, \mathscr{C}_0)$, we have that θ' is a rigid $E_{u,v}$-unifier of T and F, where $\theta' = \theta_{\mathscr{S}_k}$ is the mgu of $\mathscr{S}_k$(over $T_\Sigma(X)$), and by Lemma 6.3, $\theta_{\mathscr{S}_k}|_V$ is a rigid E-unifier of u and v. ▮

The reader may have noticed that the proof of Theorem 8.1 does not use the fact that the systems $R(\mathscr{E}_i, \mathscr{C}_i)$ are rigid reduced, but only the fact that $\theta'(\mathscr{E}_i)$ and $\theta'(R(\mathscr{E}_i', \mathscr{C}_i))$ are rigid equivalent provided that θ' unifies $TU_{\mathscr{C}_i}$. However, the fact that the systems $R(\mathscr{E}_i', \mathscr{C}_i)$ are rigid reduced plays a crucial role in the proof of the completeness theorem. The careful reader may also have noticed that if θ' is the mgu of $\mathscr{S}_k$, its Skolemized form $\hat{\theta}'$ may not realize any of the order assignments $\mathscr{C}_i$! However, this does not matter for soundness. The important fact for soundness of that $\theta'(\mathscr{E}_i)$ and $\theta'(R(\mathscr{E}_i', \mathscr{C}_i))$ are rigid equivalent provided that θ' unifies $TU_{\mathscr{C}_i}$. The $\mathscr{C}_i$'s are needed only for the completeness of the method, and to make sure that the reduction procedure terminates. This will be clarified by the proof of the completeness theorem. What is true is that for any mgu θ' obtained in the soundness theorem, there is another ground substitution θ_1 such that $\theta_1 \sqsubseteq_E \hat{\theta}'$, and there is another sequence of steps as in the soundness theorem such that θ_1 is a unifier of $\mathscr{S}_k$ (the last triangular system in the second sequence) and realizes all the $\mathscr{C}_i$'s of the second sequence.

We now turn to the completeness part. The main technique is roughly

the removal of peaks by the use of critical pairs (Bachmair [3], Bachmair, Dershowitz, and Plasted [4], Bachmair, Dershowitz, and Hsiang [5]).

THEOREM 8.2 (Completeness). *Let E be a set of equations over $T_\Sigma(X)$ and u, v two terms in $T_\Sigma(X)$. If θ is any rigid E-unifier of u and v, then there is an order assignment $\mathcal{O}_0$ on $E_{u,v}$, and letting $\mathcal{S}_0 = TU_{\mathcal{O}_0}$, $\mathcal{E}_0 = R(E_{u,v}, \mathcal{O}_0)$, m the number of variables in $R(E_{u,v}, \mathcal{O}_0)$, and $V = \mathrm{Var}(E) \cup \mathrm{Var}(u, v)$, there is a sequence of transformations*

$$\langle \mathcal{S}_0, \mathcal{E}_0, \mathcal{O}_0 \rangle \Rightarrow^+ \langle \mathcal{S}_k, \mathcal{E}_k, \mathcal{O}_k \rangle,$$

where $k \leqslant m$, $\mathcal{S}_k$ is unifiable, $F \doteq T \in \mathcal{E}_k$, $F \doteq T \notin \mathcal{E}_i$ for all i, $0 \leqslant i < k$, and $\theta_{\mathcal{S}_k}|_V \leqslant_E \theta[V]$, where $\theta_{\mathcal{S}_k}$ is the mgu of $\mathcal{S}_k$ over $T_\Sigma(X)$. Furthermore, $\theta_{\mathcal{S}_k}|_V$ is a rigid E-unifier of u and v.

Proof. First, since it is clear that the method satisfies the condition of Definition 4.9. by Lemma 4.10, it can be assumed that θ is a ground substitution and that $V \subseteq D(\theta)$. By lemma 6.3, θ can be extended to a substitution θ' such that $\theta = \theta'|_{D(\theta') - \{z\}}$ and θ' is a rigid $E_{u,v}$-unifier of T and F, where $E_{u,v} = E \cup \{eq(u, v) \doteq F,\ eq(z, z) \doteq T\}$ and z is a new variable not in V. By Lemma 5.4, there is a minimal ground substitution θ_1 such that $\theta_1 \sqsubseteq_{E_{u,v}} \theta'$, θ_1 is a rigid $E_{u,v}$-unifier of T and F, θ_1 is reduced w.r.t. $\theta_1(E_{u,v})$, and since $D(\theta) = D(\theta_1)$ and $V \subseteq D(\theta)$, we also have $V \subseteq D(\theta_1)$. Let $\mathcal{O}_0 \subseteq \preccurlyeq_{\theta_1, E_{u,v}}$ be some order assignment garanteed to exist by Lemma 6.13. Since θ_1 realizes $\mathcal{O}_0$, by Lemma 6.26(ii), $\theta_1(\mathcal{E}_0) = \theta_1(R(E_{u,v}, \mathcal{O}_0))$ and $\theta_1(E_{u,v})$ are rigid equivalent. It is also true that θ_1 unifies $TU_{\mathcal{O}_0}$. We claim that θ_1 must be reduced w.r.t. $\theta_1(\mathcal{E}_0)$. Otherwise, as in the proof of Lemma 5.4, we would be able to form a substitution $\theta_1' \ll \theta_1$ such that $\theta_1' \sqsubseteq_{\mathcal{E}_0} \theta_1$. Since $\theta_1(E_{u,v})$ and $\theta_1(\mathcal{E}_0)$ are rigid equivalent, we would have $\theta_1' \sqsubseteq_{E_{u,v}} \theta_1$, and with $\theta_1 \sqsubseteq_{E_{u,v}} \theta'$, using the transitivity of $\sqsubseteq_{E_{u,v}}$ shown in Lemma 4.4, we would have $\theta_1' \sqsubseteq_{E_{u,v}} \theta'$, and so $\theta_1' \in S_{E_{u,v}, R, F, \theta'}$, contradicting the minimality of θ_1. We shall prove the following claim.

Claim. Given a ground substitution θ_1 such that $V \subseteq D(\theta_1)$, letting $\mathcal{O}_0 \subseteq \preccurlyeq_{\theta_1, \mathcal{E}}$, be some order assignment garanteed to exist by lemma 6.13, $\mathcal{E}_0 = R(\mathcal{E}, \mathcal{O}_0)$ where $\mathcal{E} = \mathcal{E}_\Sigma \cup \{eq(u, v) \doteq F,\ eq(z, z) \doteq T\}$, with $\mathcal{E}_\Sigma$ a set of equations over $T_\Sigma(X)$ and $u, v \in T_\Sigma(X)$, and $\mathcal{S}_0$ a triangular form containing $TU_{\mathcal{O}_0}$ if θ_1 is reduced w.r.t. $\theta_1(\mathcal{E}_0)$, a unifier of $\mathcal{S}_0$, and a $\mathcal{E}_0$-unifier of T and F, then there is a sequence of transformations

$$\langle \mathcal{S}_0, \mathcal{E}_0, \mathcal{O}_0 \rangle \Rightarrow^+ \langle \mathcal{S}_k, \mathcal{E}_k, \mathcal{O}_k \rangle,$$

where $k \leqslant m$, $\mathcal{S}_k$ is unifiable, $F \doteq T \in \mathcal{E}$, $F \doteq T \notin \mathcal{E}_i$ for all i, $0 \leqslant i < k$, and θ_1 unifies $\mathcal{S}_k$ (over $T_\Sigma(X)$). Furthermore, θ_1 realizes all $\mathcal{O}_i$, $0 \leqslant i \leqslant k$.

Proof of Claim. Let

$$T = u_0 \leftrightarrow_{\theta_1(\mathscr{E}_0)} u_1 \leftrightarrow_{\theta_1(\mathscr{E}_0)} \cdots \leftrightarrow_{\theta_1(\mathscr{E}_0)} u_{n-1} \leftrightarrow_{\theta_1(\mathscr{E}_0)} u_n = F$$

be a proof that $T \overset{*}{\cong} \theta_{1(\mathscr{E}_0)} F$. We proceed by induction on the pair $\langle m, \{u_0, ..., u_n\}\rangle$, where m is the number of variables in $\mathscr{E}_0$ and $\{u_0, ..., u_n\}$ is the multiset of terms occurring in the proof. We use the well-founded ordering on pairs where the ordering on the first component is the ordering on the natural numbers, and the ordering on the second component is the multiset ordering $\prec_m$ extending $\prec$. First, observe that since $T \prec F \prec r \prec eq(s, t)$ for all $r, s, t \in T_\Sigma$, the above proof must have some peak because oriented instances of the equations $eq(u, v) \doteq F$ and $eq(z, z) \doteq T$ are of the form $eq(s, t) \to F$ and $eq(s, s) \to T$. Thus, in the base case, we have $m = 1$, $n = 2$, and $u_1 = \theta_1(eq(u, v)) = \theta_1(eq(z, z))$. Hence, θ_1 is a unifier of $eq(z, z)$ and $eq(u, v)$. Since θ_1 is also a unifier of $\mathscr{S}_0$, it is obvious that θ_1 is a unifier of $\mathscr{S}_0 \cup TU(eq(z, z), eq(u, v))$. Let $\mathscr{E}'_1 = \sigma((\mathscr{E}_0 - \{eq(z, z) \doteq T\}) \cup \{F \doteq T\})$ and $\mathscr{O}_1 \subseteq \preccurlyeq_{\theta_1, \mathscr{E}'_1}$ be some order assignment guaranteed to exist by Lemma 6.13, where σ is associated with $TU(eq(z, z), eq(u, v))$. Clearly, θ_1 is a unifier of $TU_{\mathscr{O}_1}$. Hence, θ_1 unifies $\mathscr{S}_0 \cup TU(eq(z, z), eq(u, v)) \cup TU_{\mathscr{O}_1}$, and we have

$$\langle \mathscr{S}_0, \mathscr{E}_0, \mathscr{O}_0 \rangle \Rightarrow \langle \mathscr{S}_1, \mathscr{E}_1, \mathscr{O}_1 \rangle,$$

with $\mathscr{S}_1 = \mathscr{S}_0 \cup TU(eq(z, z), eq(u, v)) \cup TU_{\mathscr{O}_1}$ and $\mathscr{E}_1 = R(\mathscr{E}'_1, \mathscr{O}_1)$. Note that $R(\mathscr{E}'_1, \mathscr{O}_1)$ does not fail because for every round of the reduction procedure, we can choose some order assignment $\mathscr{O}_1 \subseteq \preccurlyeq_{\theta_1, \mathscr{E}'}$ induced by θ_1 on the current set of equations $\mathscr{E}'$. Since θ_1 also realizes $\mathscr{O}_1 \subseteq \preccurlyeq_{\theta_1, \mathscr{E}'_1}$ (and $\mathscr{O}_0$), the claim holds.

For the induction step, consider a peak $u_{i-1} \leftarrow_{\theta_1(\mathscr{E}_0)} u_i \to_{\theta_1(\mathscr{E}_0)} u_{i+1}$. Note that $u_i \succ u_{i-1}$ and $u_i \succ u_{i+1}$. Assume that

$$u_i \to_{[\beta_1, \theta_1(l_1 \doteq r_1)]} u_{i-1}$$

and

$$u_i \to_{[\beta_2, \theta_1(l_2 \doteq r_2)]} u_{i+1},$$

where $l_1 \doteq r_1$, $l_2 \doteq r_2 \in \mathscr{E}_0 \cup \mathscr{E}_0^{-1}$ and β_1 and β_2 are addresses in u_i. We need to examine overlaps carefully. There are three cases.

Case 1. β_1 and β_2 are independent. Then, letting $v = u_i[\beta_1 \leftarrow \theta_1(r_1), \beta_2 \leftarrow \theta_1(r_2)]$, we have $u_{i-1} \to_{\theta_1(\mathscr{E}_0)} v \leftarrow_{\theta_1(\mathscr{E}_0)} u_{i+1}$, and $u_i \succ v$. We obtain a proof with associated sequence $\langle u_0, ..., u_{i-1}, v, u_{i+1}, ..., u_n \rangle$. Since $u_i \succ v$,

$$\{u_0, ..., u_n\} \succ_m \{u_0, ..., u_{i-1}, v, u_{i+1}, ..., u_n\},$$

and we conclude by applying the induction hypothesis.

Case 2. β_1 is an ancestor of β_2 (the case where β_2 is an ancestor of β_1 is similar), and letting $\beta_2 = \beta_1\beta$, $\theta_1(l_1)/\beta = \theta_1(l_2)$, and β occurs in some subterm of the form $\theta_1(x)$ in $\theta_1(l_1)$, where x is a variable in l_1.[14] Because θ_1 is rigid reduced w.r.t. $\theta_1(\mathscr{E}_0)$, by Lemma 5.4, $\theta_1(l_1)/\beta$ cannot be a proper subterm of $\theta_1(x)$. Thus, the only possibility is that $\theta_1(l_1)/\beta = \theta_1(x)$. By Lemma 5.4, $l_2 \doteq r_2$ must be a degenerate equation, and we have $l_2 = y$ for some variable y. The case $y = x$ is impossible because $\mathscr{E}_0$ is rigid reduced. Thus $y \neq x$, and since $\theta_1(l_1)/\beta = \theta_1(x) = \theta_1(l_2)$, θ_1 is a unifier of $\langle x, y \rangle$. The rest of this case proceeds as in Case 3, below.

Case 3. β_1 is an ancestor of β_2 (the case where β_2 is an ancestor of β_1 is similar), and letting $\beta_2 = \beta_1\beta$, $\theta_1(l_1/\beta) = \theta_1(l_2)$, and either l_1/β is not a variable, or $l_1/\beta = x$ and $l_2 \doteq r_2$ is a degenerate equation $y \doteq r_2$ with $y \neq x$. In either case, θ_1 unifies l_1/β and l_2. Since $\mathscr{E}_0$ is rigid reduced, we must have $l_1/\beta \neq l_2$. Let $TU(l_1/\beta, l_2)$ be a triangular representation of the mgu of l_1/β and l_2, and $\sigma = [t_1/x_1, ..., t_p/x_p]$, with $TU(l_1/\beta, l_2) = \{\langle x_1, t_1 \rangle, ..., \langle x_p, t_p \rangle\}$. Since θ_1 unifies $TU(l_1/\beta, l_2)$, by Lemma 3.5, σ; $\theta_1 = \theta_1$. Since σ; $\theta_1 = \theta_1$, and θ_1 unifies l_1/β and l_2, as in the proof of Theorem 8.1, we can show that $\theta_1(\mathscr{E}'_1)$ and $\theta_1(\mathscr{E}_0)$ are rigid equivalent, where

$$\mathscr{E}'_1 = \sigma((\mathscr{E}_0 - \{l_1 \doteq r_1\})^{\dagger} \cup \{l_1[\beta \leftarrow r_2] \doteq r_1\}).$$

Since $\theta_1(\mathscr{E}_0)$ and $\theta_1(\mathscr{E}'_1)$ are rigid equivalent and θ_1 is minimal in $S_{E_{\mathscr{U}}, V, T, F, \theta'}$, as shown just before the claim, θ_1 is also reduced w.r.t. $\theta_1(\mathscr{E}'_1)$. Since θ_1 unifies $\mathscr{S}_0$ and $TU(l_1/\beta, l_2)$, it unifies $\mathscr{S}_0 \cup TU(l_1/\beta, l_2)$.

Let $\mathscr{O}_1 \subseteq \preccurlyeq_{\theta_1, \mathscr{E}'_1}$ be some order assignment guaranteed to exist by Lemma 6.13. Clearly, θ_1 unifies $TU_{\mathscr{O}_1}$, and so θ_1 unifies $\mathscr{S}_0 \cup TU(l_1/\beta, l_2) \cup TU_{\mathscr{O}_1}$. We have

$$\langle \mathscr{S}_0, \mathscr{E}_0, \mathscr{O}_0 \rangle \Rightarrow \langle \mathscr{S}_1, \mathscr{E}_1, \mathscr{O}_1 \rangle,$$

where $\mathscr{S}_0 \cup TU(l_1/\beta, l_2) \cup TU_{\mathscr{O}_1}$ and $\mathscr{E}_1 = R(\mathscr{E}'_1, \mathscr{O}_1)$. The reason why $R(\mathscr{E}'_1, \mathscr{O}_1)$ does not fail is that for every round of the reduction procedure, we can choose some order assignment $\mathscr{O}'_1 \subseteq \preccurlyeq_{\theta_1, \mathscr{E}'}$ induced by θ_1 on the current set of equations $\mathscr{E}'$. Since θ_1 unifies $TU_{\mathscr{O}_1}$, by Lemma 6.26(i),

[14] Readers familiar with this kind of argument might wonder why we are not elminating the peak by finding a v such that $u_{i-1} \overset{*}{\rightarrow}_{\mathscr{E}_0} v \overset{*}{\leftarrow}_{\mathscr{E}_0} u_{i+1}$, as in the nonrigid case (Knuth and Bendix [18], Huet [16], Bachmair [3], Bachmair, Dershowitz, and Plaisted [4]). This is because the above rewrite proof uses a new instance $\eta(l_1 \doteq r_1)$ of the equation $l_1 \doteq r_1 \in \mathscr{E}_0 \cup \mathscr{E}_0^{-1}$ with a matching substitution η that has been obtained from θ_1 by reducing $\theta_1(x)$ by the instance $\theta_1(l_2 \doteq r_2)$. However, in the rigid case, $\eta(l_1 \doteq r_1)$ may *not* be in $\theta_1(\mathscr{E}_0)$. This is the reason why we need Lemma 5.4, and fortunately, degenerate equations do not cause trouble because the total number of variables is reduced as shown in case (3).

$\theta_1(\mathscr{E}_1) = \theta_1(R(\mathscr{E}'_1, \mathscr{C}_1))$ and $\theta_1(\mathscr{E}'_1)$ are rigid equivalent. Since $\theta_1(\mathscr{E}_0)$ and $\theta_1(\mathscr{E}'_1)$ are rigid equivalent, then $\theta_1(\mathscr{E}_0)$ and $\theta_1(\mathscr{E}_1)$ are rigid equivalent. Since θ_1 is a rigid $\mathscr{E}_0$-unifier of T and F, θ_1 is also a rigid $\mathscr{E}_1$-unifier of T and F. Since θ_1 is minimal in $S_{E_{u,v}, T, F, \theta'}$, $\theta_1(E_{u,v})$, $\theta_1(\mathscr{E}_0)$, and $\theta_1(\mathscr{E}_1)$ are rigid equivalent, and $\theta_1 \sqsubseteq_{E_{u,v}} \theta'$, as argued previously, θ_1 is also reduced w.r.t. $\theta_1(\mathscr{E}_1)$. Also note that at least one variable in the set $\{x_1, ..., x_p\}$ does not occur in $I(\sigma)$ (as noted after Lemma 3.5). Thus, this variable does not occur in $\mathscr{E}_1$, and $m' < m$, where m' is the number of variables in $\mathscr{E}_1$. Therefore, we can apply the induction hypothesis to θ_1, $\mathscr{S}_1$, $\mathscr{E}_1$, and $\mathscr{C}_1$ and obtain a sequence

$$\langle \mathscr{S}_1, \mathscr{E}_1, \mathscr{C}_1 \rangle \Rightarrow^+ \langle \mathscr{S}_k, \mathscr{E}_k, \mathscr{C}_k \rangle,$$

where $k \leqslant m'$, $\mathscr{S}_k$ is unifiable, $F \doteq T \in \mathscr{E}_k$, $F \doteq T \notin \mathscr{E}_i$ for all i, $0 \leqslant i < k$, and θ_1 is a unifier of $\mathscr{S}_k$. The induction hypothesis also tells us that θ_1 realizes all $\mathscr{C}_i$ for $1 \leqslant i \leqslant k$, and since θ_1 also realizes $\mathscr{C}_0$ (by its definition), this concludes the induction step and the proof of the claim. ∎

From the claim applied to $\mathscr{S}_0 = TU_{\mathscr{C}_0}$ and $\mathscr{E}_0 = R(E_{u,v}, \mathscr{C}_0)$, there is a sequence of at most m transformations as stated in the theorem, and θ_1 is a unifier of $\mathscr{S}_k$. Since $\theta_{\mathscr{S}_k} \leqslant \theta_1[V]$ where $\theta_{\mathscr{S}_k}$ is the mgu of $\mathscr{S}_k$ and we know that $\theta_1 \sqsubseteq_{E_{u,v}} \theta'$, we have $\theta_{\mathscr{S}_k} \leqslant E_{u,v} \theta'[V]$. Therefore, $\theta_{\mathscr{S}_k}|_V \leqslant_E \theta[V]$. Finally, by Theorem 8.1, we see that $\theta_{\mathscr{S}_k}|_V$ is a rigid E-unifier of u and v. ∎

We are now in a position to prove the claim made just after the proof of the soundness theorem and justify the remark about order assignments made just before stating Lemma 6.26.

COROLLARY 8.3. *If θ' is the mgu produced by a sequence of steps as in the soundness theorem, there is a ground substitution θ_1 such that $V \subseteq D(\theta_1)$ and a sequence of steps*

$$\langle \mathscr{S}_0, \mathscr{E}_0, \mathscr{C}_0 \rangle \Rightarrow^+ \langle \mathscr{S}_k, \mathscr{E}_k, \mathscr{C}_k, \rangle$$

such that $\theta_1 \sqsubseteq_E \hat{\theta}'$, θ_1 is a unifier of $\mathscr{S}_k$, and θ_1 realizes all the $\mathscr{C}_i$'s in the above sequence. In particular, the method is still complete if we restrict ourselves to order assignments $\mathscr{O}$ such that $T \leqslant_{\mathscr{O}} F \leqslant_{\mathscr{O}} s \leqslant_{\mathscr{O}} eq(u, v)$ for all s, u, $v \in T_\Sigma(X)$. In view of part (ii) *of* Lemma 6.13, *the method is also complete if we restrict ourselves to order assignments $\mathscr{O}$ that are partial orderings (that is, when $\equiv_{\mathscr{O}}$ is the identity relation).*

Theorem 8.2 also shows that rigid E-unification is decidable.

COROLLARY 8.4. *Rigid E-unification is decidable.*

Proof. By Theorem 8.2, a (ground) rigid E-unifier θ of u and v exists iff there is some sequence of transformations

$$\langle \mathscr{S}_0, \mathscr{E}_0, \mathscr{O}_0 \rangle \Rightarrow^+ \langle \mathscr{S}_k, \mathscr{E}_k, \mathscr{O}_k \rangle$$

of at most $k \leqslant m$ steps, where m is the number of variables in $\mathscr{E}_0$, and such that $\mathscr{S}_k$ is unifiable (over $T_\Sigma(X)$), $F \doteq T \in \mathscr{E}_k$ and $F \doteq T \notin \mathscr{E}_i$ for all i, $0 \leqslant i < k$. Clearly, all these conditions are finitary and can be tested. Thus, rigid E-unification is decidable. ▮

Combining the results of Theorems 8.1 and 8.2 we also obtain the fact that for any E, u, v, there is always a finite complete set of rigid E-unifiers.

THEOREM 8.5. *Let E be a set of equations over $T_\Sigma(X)$, u, v two terms in $T_\Sigma(X)$, m the number of variables in $E \cup \{u, v\}$, and $V = \mathrm{Var}(E) \cup Var(u, v)$. There is a finite complete set of rigid E-unifiers for u and v given by the set*

$$\{\theta_{\mathscr{S}_k} | _V \mid \langle \mathscr{S}_0, \mathscr{E}_0, \mathscr{O}_0 \rangle \Rightarrow^+ \langle \mathscr{S}_k, \mathscr{E}_k, \mathscr{O}_k \rangle, k \leqslant m\},$$

for any order assignment $\mathscr{O}_0$ on $E_{u,v}$, with $\mathscr{S}_0 = TU_{\mathscr{O}_0}$, $\mathscr{E}_0 = R(E_{u,v}, \mathscr{O}_0)$, and where $\mathscr{S}_k$ is unifiable, $F \doteq T \in \mathscr{E}_k$, $F \doteq T \notin \mathscr{E}_i$ for all i, $0 \leqslant i < k$, and $\theta_{\mathscr{S}_k}$ is the mgu of $\mathscr{S}_k$ over $T_\Sigma(X)$.

Proof. Follows immediately from Theorems 8.1 and 8.2 and the fact that m is an upper bound on the length of such sequences. ▮

Theorem 8.2 shows that rigid E-unification is not only decidable but also in NP.

9. NP-Completeness of Rigid E-Unification

First, recall that rigid E-unification is NP-hard. This holds even for ground sets of equations, as shown by Kozen [19, 20]. Indeed, it is easy to reduce the satisfiability problem to rigid E-unification modulo a set E of ground equations.

THEOREM 9.1. *Rigid E-unification is NP-complete.*

Proof. We already know that rigid E-unification is NP-hard. By Corollary 8.4, the problem is decidable. It remains to show that it is in NP. From Corollary 8.4, u and v have some rigid E-unifier iff there is some sequence of transformations

$$\langle \mathscr{S}_0, \mathscr{E}_0, \mathscr{O}_0 \rangle \Rightarrow^+ \langle \mathscr{S}_k, \mathscr{E}_k, \mathscr{O}_k \rangle$$

of at most $k \leqslant m$ steps, where m is the number of variables in $\mathscr{E}_0$, and such that $\mathscr{S}_k$ is unifiable (over $T_\Sigma(X)$), $F \doteq T \in \mathscr{E}_k$ and $F \doteq T \notin \mathscr{E}_i$ for all i, $0 \leqslant i < k$. We need to verify that it is possible to check these conditions in polynomial time. First, observe that a triangular form can be computed in polynomial time, applying the substitutions associated with triangular forms can also be done in polynomial time, and checking that a preorder is an order assignment can be done in polynomial time. Finally, we need to show that the total cost of producing reduced systems is polynomial. This is a crucial point that had been overlooked in a previous version of this paper, and we thank Leo Bachmair for pointing out this subtlety to us. We use two facts that have to do with implementing the steps of the algorithms using term DAGs.

(1) We have already noted (see Theorem 6.7) that the size of the term DAG associated with a reduced system equivalent to an input set of equations is no greater than the size of the input term DAG, the number of rules no greater that the number of input equations, and that the reduction procedure runs in $O((m+n+p)^3)$, where (m, n) is the size of the input term DAG and p the number of equations in E.

(2) The term DAG associated with the system $\mathscr{E}'_{i+1}$ obtained from $\mathscr{E}_i$ by a transformation step can be obtained from the term DAG associated with $\mathscr{E}_i$ by moving pointers, and if (m', n') and (m, n) are the sizes of the term DAGs of the systems $\mathscr{E}'_{i+1}$ and $\mathscr{E}_i$, respectively, and p' and p the numbers of equations in these systems, then $m' \leqslant m$, $n' \leqslant n$, and $p' \leqslant p$.

The reason why (2) holds is that the terms occurring in the triangular form of the substitution σ associated with the transformation step all belong to the term DAG associated with $\mathscr{E}_i$. For instance, this is easily seen if one uses Paterson and Wegman's method [25]. Now, forming $l_1[\beta \leftarrow r_2]$ involves only pointer redirection, and so does the application of σ. Thus, the size of the resulting term DAG cannot increase. By the definition of the transformations, it is also obvious that $p' \leqslant p$.

Because the number of steps is at most the number of variables in $\mathscr{E}_0$, the total cost of producing reduced systems is indeed polynomial in the size of the input.

It is interesting to note the analogy of this part of our proof with Kozen's proof that his method is in NP [20]. Both use the term DAG representation in a crucial way. In this way, we avoid the potential exponential explosion that can take place during reductions if identical subterms are not shared. ▮

If E is a set of ground equations, the $\mathscr{O}_i$'s are useless and the reduction procedure R need only be applied once at the beginning to E. Thus, we obtain the following corollary of Theorem 9.1 which provides another

proof of a result first established by Kozen [19, 20]. Actually, in view of Theorem 8.5, we have shown a result stronger than Kozen's.

COROLLARY 9.2. *Given a finite set E of ground equations and any two terms u and v, rigid E-unification is NP-complete. Furthermore, the procedure of Definition 7.3 yields a finite complete set of rigid E-unifiers of u and v, the reduction procedure R need only be applied once to E, and the $\mathcal{C}_i$'s are unnecessary.*

10. APPLICATIONS OF RIGID E-UNIFICATION TO EQUATIONAL MATINGS

Rigid E-unification came up naturally in the process of generalizing Andrews' method of matings to first-order languages with equality (Gallier, Raatz, and Snyder [10], Gallier, Narendran, Raatz, and Snyder [13]). Actually, what is needed is a generalization of rigid E-unification involving several sets of equations and pairs of terms. In this section, it is shown that the method developed for one set of equations and one pair can be easily generalized to tackle the more general problem. In fact, we shall give an algorithm to decide whether a family of mated sets is an equational (pre)mating that is in NP.

DEFINITION 10.1. Let $E = \{E_i \mid 1 \leqslant i \leqslant n\}$ be a family of n sets of equations (over $T_\Sigma(X)$) and $S = \{\langle u_i, v_i \rangle \mid 1 \leqslant i \leqslant n\}$ a set of n pairs of terms (over $T_\Sigma(X)$). A substitution θ (over $T_\Sigma(X)$) is a *rigid E-unifier of S* iff

$$\theta(u_i) \stackrel{*}{=}_{\theta(E_i)} \theta(v_i)$$

for every i, $1 \leqslant i \leqslant n$. A pair $\langle E, S \rangle$ such that S has some rigid E-unifier is called an *equational premating*.[15]

The suitable generalization of the preorder $\leqslant_E$ to a family $E = \{E_i \mid 1 \leqslant i \leqslant n\}$ of n sets of equations turns out to be the following.

DEFINITION 10.2. Given a family $E = \{E_i \mid 1 \leqslant i \leqslant n\}$ of n sets of equations, for any (finite) set of variables V, for any two substitutions σ and θ, $\sigma \leqslant_E \theta$ iff there is some η such that $\sigma; \eta \sqsubseteq_{E_i} \theta[V]$ for every i, $1 \leqslant i \leqslant n$.

Note that this condition is stronger than the condition $\sigma \leqslant_{E_i} \theta[V]$ for every i, $1 \leqslant i \leqslant n$, because with this second condition we know only that there are substitutions $\eta_1, \ldots, \eta_n$ such that $\sigma; \eta_i \sqsubseteq E_i \theta[V]$ for every i,

[15] We chose the terminology *equational premating* because an equational mating is an equational premating satisfying some extra properties; see Gallier, Raatz, and Snyder [10], or Gallier, Narendran, Raatz, and Snyder [13].

$1 \leqslant i \leqslant n$. In Definition 10.2, it is required that $\eta_1 = \cdots = \eta_n$. The generalization of Theorem 8.2 goes through with the stronger definition 10.2, which is obviously preferable.

Complete sets of rigid E-unifiers for S are defined as follows.

DEFINITION 10.3. *Let* $E = \{E_i \mid 1 \leqslant i \leqslant n\}$ and $S = \{\langle u_i, v_i \rangle \mid 1 \leqslant i \leqslant n\}$ as in Definition 10.1, and let $V = \mathrm{Var}(E) \cup \mathrm{Var}(S)$. A set U of substitutions is a *complete set of rigid E-unifiers for* S iff: For every $\sigma \in U$,

(i) $D(\sigma) \subseteq V$ and $D(\sigma) \cap I(\sigma) = \varnothing$ (idempotence);

(ii) σ is a rigid E-unifier of S;

(iii) for every rigid E-unifier θ of S, there is some $\sigma \in U$ such that $\sigma \leqslant_E \theta[V]$.

Minimal rigid E-unifiers also exist and are defined as follows.

DEFINITION 10.4. Let E be a set of sets of equations and S a term system as in Definition 10.1. For any ground rigid E-unifier θ of S, let

$$S_{E,S,\theta} = \{\rho \mid D(\rho) = D(\theta),\ \rho(u_i) \stackrel{*}{\cong}_{\rho(E_i)} \rho(v_i),\ \rho \sqsubseteq_{E_i} \theta,\ 1 \leqslant i \leqslant n, \text{ and } \rho \text{ ground}\}.$$

Since $\lessdot\!\lessdot$ is total and well-founded on ground substitutions with domain $D(\theta)$, the set $S_{E,S,\theta}$ contains some least element σ (w.r.t. $\lessdot\!\lessdot$).

It is easy to see that Lemma 5.4 can be generalized as follows.

LEMMA 10.5 *Let E be a set of sets of equations and S a term system as in Definition* 10.1. *For any ground rigid E-unifier θ of S, if σ is the least element of the set $S_{E,S,\theta}$ of Definition* 10.4, *then the following properties hold*:

(1) $\sigma \sqsubseteq_{E_i} \theta$ *for every* i, $1 \leqslant i \leqslant n$,

(2) *every term of the form $\sigma(x)$ is irreducible by every oriented instance $\sigma(l) \to \sigma(r)$ of a nondegenerate equation $l \doteq r \in E \cup E^{-1}$, and*

(3) *every proper subterm of a term of the form $\sigma(x)$ is irreducible by every oriented instance $\sigma(l) \to \sigma(r)$ of a degenerate equation $l \doteq r \in E \cup E^{-1}$.*

Lemma 6.3 is easily generalized as follows. We let $eq_1, \ldots, eq_n$ be n new distinct binary function symbols not in Σ (and distinct from T and F).

LEMMA 10.6. *Let E be a set of sets equations and S a term system as in Definition* 10.1. *A substitution θ over $T_\Sigma(X)$ is a rigid E-unifier of S iff there is some substitution θ' over $T_\Sigma(X)$ such that $\theta = \theta'|_{D(\theta') - \{z_1, \ldots, z_n\}}$ and $T \stackrel{*}{\cong}_{\theta'(E^i)} F$ for every i, $1 \leqslant i \leqslant n$, where $E^i = E_i \cup \{eq_i(u_i, v_i) \doteq F$,*

$eq_i(z_i, z_i) \doteq T\}$, *and* $\{z_1, ..., z_n\}$ *is a set of new variables not in* $\mathrm{Var}(E) \cup \mathrm{Var}(S)$.

The total simplification ordering $\prec$ is extended to the set

$$T_\Sigma \cup \{T, F\} \cup \bigcup_{i=1}^{i=n} \{eq_i(u, v) \mid u, v \in T_\Sigma\}$$

as follows:

For any terms s, t, u, $v \in T_\Sigma$,

(a) $T \prec F \prec u \prec eq_i(s, t)$;

(b) $eq_i(s, t) \prec eq_i(u, v)$ iff $\{s, t\} \prec_{\mathrm{lex}} \{u, v\}$, where $\prec_{\mathrm{lex}}$ is the lexicographic extension of $\prec$ to pairs;

(c) $eq_i(s, t) \prec eq_j(u, v)$ iff $1 \leqslant i < j \leqslant n$.

Clearly, this extension of $\prec$ is a total simplification ordering. We define a transformation on systems as follows.

DEFINITION 10.7. *Let* $\prec$ be a total simplification ordering on ground terms. We shall be considering n-tuples $\mathscr{E} = \langle \mathscr{E}^1, ..., \mathscr{E}^n \rangle$ of finite sets of equations of the form $\mathscr{E}^i = \mathscr{E}^i_\Sigma \cup \{eq_i(u, v) \doteq F, eq_i(z_i, z_i) \doteq T\}$, where $\mathscr{E}^i_\Sigma$ is a set of equations over $T_\Sigma(X)$ and $u, v \in T_\Sigma(X)$. We define a transformation on systems of the form $\langle \mathscr{S}, \mathscr{E}, \mathscr{O} \rangle$, where $\mathscr{S}$ is a term system, $\mathscr{E}$ an n-tuple of sets of equations as above, and $\mathscr{O}$ an order assignment:

$$\langle \mathscr{S}_0, \mathscr{E}_0, \mathscr{O}_0 \rangle \Rightarrow \langle \mathscr{S}_1, \mathscr{E}_1, \mathscr{O}_1 \rangle,$$

where $l_1 \doteq r_1$, $l_2 \doteq r_2 \in \mathscr{E}^i_0 \cup (\mathscr{E}^i_0)^{-1}$ for some i, $1 \leqslant i \leqslant n$, either l_1/β is *not* a variable or $l_2 \doteq r_2$ is degenerate, $l_1/\beta \neq l_2$, $TU(l_1/\beta, l_2)$ represents a mgu of l_1/β and l_2 in triangular form, $\sigma = [t_1/x_1, ..., t_p/x_p]$, where $TU(l_1/\beta, l_2) = \{\langle x_1, t_1 \rangle, ..., \langle x_p, t_p \rangle\}$,

$$\mathscr{E}'^i_1 = \sigma((\mathscr{E}^i_0 - \{l_1 \doteq r_1\})^+ \cup \{l_1[\beta \leftarrow r_2] \doteq r_1\})$$

$$\text{and} \qquad \mathscr{E}'^j_1 = \sigma(\mathscr{E}^j_0) \qquad \text{for every} \quad j \neq i,$$

$\mathscr{O}_1$ is an order assignment on $\mathscr{E}'_1$ compatible with $\mathscr{O}_0$, $\mathscr{S}_1 = \mathscr{S}_0 \cup TU(l_1/\beta, l_2) \cup TU_{\mathscr{O}_1}$, and $\mathscr{E}_1 = \langle \mathscr{E}^1_1, ..., \mathscr{E}^n_1 \rangle$, where $\mathscr{E}^j_1 = R(\mathscr{E}'^j_1, \mathscr{O}_1)$ for all j, $1 \leqslant j \leqslant n$.

The method for finding rigid E-unifiers of S is the following.

DEFINITION 10.8 (Method). Let $E = \{E_i \mid 1 \leqslant i \leqslant n\}$ and $S = \{\langle u_i, v_i \rangle \mid 1 \leqslant i \leqslant n\}$ as in Definition 10.1, let $E^i = E_i \cup \{eq_i(u_i, v_i) \doteq F, eq_i(z_i, z_i) \doteq T\}$ for every i, $1 \leqslant i \leqslant n$, $\mathscr{O}_0$ an order assignment on $\langle E^1, ..., E^n \rangle$, $\mathscr{S}_0 = TU_{\mathscr{O}_0}$,

$\mathscr{E}^i_0 = R(E^i, \mathscr{O}_0)$ for every i, $1 \leqslant i \leqslant n$, $\mathscr{E}_0 = \langle \mathscr{E}^1_0, ..., \mathscr{E}^n_0 \rangle$, m the total number of variables in $\mathscr{E}_0$, and $V = \mathrm{Var}(E) \cup \mathrm{Var}(S)$. For any sequence

$$\langle \mathscr{S}_0, \mathscr{E}_0, \mathscr{O}_0 \rangle \Rightarrow^+ \langle \mathscr{S}_k, \mathscr{E}_k, \mathscr{O}_k \rangle$$

consisting of at most m transformation steps, if $\mathscr{S}_k$ is unifiable and $k \leqslant m$ is the first integer in the sequence such that $F \doteq T \in \mathscr{E}^i_k$ for every i, $1 \leqslant i \leqslant n$, return the substitution $\theta_{\mathscr{S}_k}|_V$, where $\theta_{\mathscr{S}_k}$ is the mgu of $\mathscr{S}_k$ (over $T_\Sigma(X)$).

The proofs of Theorems 8.1 and 8.2 can be easily adapted to prove that the finite set of all substitutions returned by the method of Definition 10.8 forms a complete set of rigid E-unifiers for S. In particular, the method provides a decision procedure for deciding whether a family of mated sets is an equational premating that is in NP.

THEOREM 10.9 (Soundness). *Let* $E = \{E_i \mid 1 \leqslant i \leqslant n\}$ *and* $S = \{\langle u_i, v_i \rangle \mid 1 \leqslant i \leqslant n\}$ *as in Definition* 10.1, *let* $E^i = E_i \cup \{eq_i(u_i, v_i) \doteq F,\ eq_i(z_i, z_i) \doteq T\}$ *for every* i, $1 \leqslant i \leqslant n$, $\mathscr{O}_0$ *an order assignment on* $\langle E^1, ..., E^n \rangle$, $\mathscr{S}_0 = TU_{\mathscr{O}_0}$, $\mathscr{E}^i_0 = R(E^i, \mathscr{O}_0)$ *for every* i, $1 \leqslant i \leqslant n$, $\mathscr{E}_0 = \langle \mathscr{E}^1_0, ..., \mathscr{E}^n_0 \rangle$, m *the total number of variables in* $\mathscr{E}_0$, *and* $V = \mathrm{Var}(E) \cup \mathrm{Var}(S)$. *If*

$$\langle \mathscr{S}_0, \mathscr{E}_0, \mathscr{O}_0 \rangle \Rightarrow^+ \langle \mathscr{S}_k, \mathscr{E}_k, \mathscr{O}_k \rangle,$$

where $\mathscr{S}_k$ *is unifiable,* $F \doteq T \in \mathscr{E}^j_k$ *and* $F \doteq T \notin \mathscr{E}^j_i$ *for all* i *and* j, $0 \leqslant i < k \leqslant m$, $1 \leqslant j \leqslant n$, *then* $\theta_{\mathscr{S}_k}|_V$ *is a rigid* E*-unifier of* S, *where* $\theta_{\mathscr{S}_k}$ *is the mgu of* $\mathscr{S}_k$ (*over* $T_\Sigma(X)$).

Proof. It is essentially the same as the proof of Theorem 8.1, except that Lemma 10.6 is used instead of Lemma 6.3. ∎

THEOREM 10.10 (Completeness). *Let* $E = \{E_i \mid 1 \leqslant i \leqslant n\}$ *and* $S = \{\langle u_i, v_i \rangle \mid 1 \leqslant i \leqslant n\}$ *as in Definition* 10.1, *and let* $E^i = E_i \cup \{eq_i(u_i, v_i) \doteq F,\ eq_i(z_i, z_i) \doteq T\}$ *for every* i, $1 \leqslant i \leqslant n$. *If* θ *is any rigid* E*-unifier of* S, *then there is an order assignment* $\mathscr{O}_0$ *on* $\langle E^1, ..., E^n \rangle$, *and letting* $\mathscr{S}_0 = TU_{\mathscr{O}_0}$, $\mathscr{E}^i_0 = R(E^i, \mathscr{O}_0)$ *for every* i, $1 \leqslant i \leqslant n$, $\mathscr{E}_0 = \langle \mathscr{E}^1_0, ..., \mathscr{E}^n_0 \rangle$, m *the total number of variables in* $\mathscr{E}_0$, *and* $V = \mathrm{Var}(E) \cup \mathrm{Var}(S)$, *there is a sequence of transformations*

$$\langle \mathscr{S}_0, \mathscr{E}_0, \mathscr{O}_0 \rangle \Rightarrow^+ \langle \mathscr{S}_k, \mathscr{E}_k, \mathscr{O}_k \rangle,$$

where $k \leqslant m$, $\mathscr{S}_k$ *is unifiable,* $F \doteq T \in \mathscr{E}^j_k$, $F \doteq T \notin \mathscr{E}^j_i$ *for all* i *and* j, $0 \leqslant i < k$, $1 \leqslant j \leqslant n$, *and* $\theta_{\mathscr{S}_k}|_V \leqslant_E \theta[V]$, *where* $\theta_{\mathscr{S}_k}$ *is the mgu of* $\mathscr{S}_k$ *over* $T_\Sigma(X)$. *Furthermore,* $\theta_{\mathscr{S}_k}|_V$ *is a rigid* E*-unifier of* S.

Proof. It is a simple generalization of the proof of Theorem 8.2.

Lemma 10.5 is used instead of Lemma 5.4. In the proof of the claim, we also need to consider the n-tuple of proofs

$$T = u_0^i \leftrightarrow_{\theta_1(\mathscr{E}_0^i)} u_1^i \leftrightarrow_{\theta_1(\mathscr{E}_0^i)} \cdots \leftrightarrow_{\theta_1(\mathscr{E}_0^i)} u_{n_i-1}^i \leftrightarrow_{\theta_1(\mathscr{E}_0^i)} u_{n_i}^i = F,$$

showing that $T \overset{*}{\cong}_{\theta_1(\mathscr{E}_0^i)} F$ for all i, $1 \leqslant i \leqslant n$. We proceed by induction on the pair $\langle m, M \rangle$, where m is the number of variables in $\mathscr{E}_0$ and

$$M = \bigcup_{i=1}^{i=n} \{u_0^i, \ldots, u_{n_i}^i\},$$

is the union of the multisets $\{u_0^i, \ldots, u_{n_i}^i\}$ of terms occurring in the ith proof. The details are straightforward. ▮

Actually, Theorem 10.10 can be sharpened. Examination of the induction proof reveals that for any rigid E-unifier θ of S, a rigid E-unifier more general than θ can be found, even if the transformations are applied in a certain order.

DEFINITION 10.11. We say that a derivation

$$\langle \mathscr{S}_0, \mathscr{E}_0, \mathscr{C}_0 \rangle \Rightarrow^+ \langle \mathscr{S}_m, \mathscr{E}_m, \mathscr{C}_m \rangle$$

is an *lr-derivation* iff for every subderivation

$$\langle \mathscr{S}_0, \mathscr{E}_0, \mathscr{C}_0 \rangle \Rightarrow^* \langle \mathscr{S}_i, \mathscr{E}_i, \mathscr{C}_i \rangle \Rightarrow \langle \mathscr{S}_{i+1}, \mathscr{E}_{i+1}, \mathscr{C}_{i+1} \rangle,$$

in the step from i to $i+1$ $(0 \leqslant i < m)$, the equations $l_1 \doteq r_1$ and $l_2 \doteq r_2$ are chosen in the set $\mathscr{E}_i^j$ such that $j \geqslant 1$ is the least index such that $F \doteq T \in \mathscr{E}_i^l$ for every $l < j$ and $F \doteq T \notin \mathscr{E}_i^j$.

In some sense, such derivations compute rigid E-unifiers incrementally from left to right.

THEOREM 10.12 (Incremental Completeness). *Theorem* 10.10 *holds with lr-derivations instead of arbitrary derivations.*

This sharpening of Theorem 10.10 is very useful in practice, because it yields an incremental way of finding rigid E-unifiers. From Theorem 10.10, it is obvious that Theorem 8.5 also holds for a set of sets of equations E and a term system S.

THEOREM 10.13. *Let* $E = \{E_i \mid 1 \leqslant i \leqslant n\}$ *and* $S = \{\langle u_i, v_i \rangle \mid 1 \leqslant i \leqslant n\}$ *as in Definition* 10.1, $E^i = E_i \cup \{eq_i(u_i, v_i) \doteq F, eq_i(z_i, z_i) \doteq T\}$ *for every* i, $1 \leqslant i \leqslant n$, m *the number of variables in* $E \cup S$, *and* $V = \mathrm{Var}(E) \cup \mathrm{Var}(S)$.

There is a finite complete set of rigid E-unifiers for S given by the set

$$\{\theta_{\mathscr{S}_k} | \nu | \langle \mathscr{S}_0, \mathscr{E}_0, \mathscr{O}_0 \rangle \Rightarrow^+ \langle \mathscr{S}_k, \mathscr{E}_k, \mathscr{O}_k \rangle, k \leqslant m\},$$

for any order assignment $\mathscr{O}_0$ *on* $\langle E^1, ..., E^n \rangle$, *with* $\mathscr{S}_0 = TU_{\mathscr{O}_0}$, $\mathscr{E}^i_0 = R(E^i, \mathscr{O}_0)$ *for every i,* $1 \leqslant i \leqslant n$, $\mathscr{E}_0 = \langle \mathscr{E}^1_0, ..., \mathscr{E}^n_0 \rangle$, *and where* $\mathscr{S}_k$ *is unifiable,* $F \doteq T \in \mathscr{E}^j_k$, $F \doteq T \notin \mathscr{E}^j_i$ *for all i and j,* $0 \leqslant i < k$, $1 \leqslant j \leqslant n$, *and* $\theta_{\mathscr{S}_k}$ *is the mgu of* $\mathscr{S}_k$ *over* $T_\Sigma(X)$.

Finally, it is obvious that Theorem 10.10 yields a generalization of Theorem 9.1 to equational prematings.

THEOREM 10.14. *Finding whether a pair* $\langle E, S \rangle$ (*as in definition* 10.1) *is an equational premating is NP-complete.*

As a consequence, since the problem of deciding whether a family of mated sets forms an equational mating is precisely the problem of finding whether a pair $\langle E, S \rangle$ (as in Definition 10.1) is an equational premating,[16] the former problem is also NP-complete.

11. CONCLUSION AND FURTHER WORK

We have shown that both rigid E-unification and finding whether a pair $\langle E, S \rangle$ is an equational premating are NP-complete problems. We also have shown that finite complete sets of rigid E-unifiers always exist. Theorem 10.14 has important implications regarding the computational complexity of theorem proving for first-order languages with equality using the method of matings. It shows that there is an algorithm for finding equational matings, but not only is the problem of deciding whether an equational mating is p-acceptable co-NP-complete; the problem of deciding that a family of mated sets is an equational mating is also NP-complete. For languages without equality, the first problem is still co-NP-complete, but the second can be solved in polynomial time using standard unification, and in fact in linear time.

In view of Example 7.6, it is essential to find ways of trimming the search space of order assignments. When a reduction ordering $\prec$ is available and all subterms in $\mathscr{E}'_i$ are ordered by $\prec$, $\mathscr{O}_i$ is completely determined. It would be interesting to investigate subcases where order assignments can be found quickly. An actual implementation of the algorithm would also be interesting. In a different direction, it is clear that a rigid E-unification algorithm can be used for general E-unification. One simply runs the rigid E-unification algorithm incrementally, fixing the number of instances of equations

[16] See Gallier, Raatz, and Snyder [10], or Gallier, Narendran, Raatz, and Snyder [13].

allowed at the beginning, and increasing this number gradually until enough E-unifiers are found (or running forever). There is however a problem of redundancy: a member of a complete set found at some stage can be subsumed by a rigid E-unifier produced at a later stage. It would be interesting to investigate this problem and see how this method compares with other E-unification procedures. The above questions are left for further research.

ACKNOWLEDGMENTS

We thank Leo Bachmair, Jin Choi, Jean Yves Girard, Tomas Isakowitz, Frank Pfenning, Stan Raatz, and Rick Statman for insightful comments.

RECEIVED November 30, 1988; FINAL MANUSCRIPT RECEIVED August 15, 1989

REFERENCES

1. ANDREWS, P. (1981), Theorem proving via general matings, *J. Assoc. Comput. Mach.* **28**, No. 2, 193–214.
2. ANDREWS, P. (1986), "An Introduction to Mathematical Logic and Type Theory: To Truth through Proof," Academic Press, New York.
3. BACHMAIR, L. (1989), "Canonical Equational Proofs, Research Notes in Theoretical Computer Science," Wiley, New York.
4. BACHMAIR, L., DERSHOWITZ, N., AND PLAISTED, D. (1987), Completion without failure, *in* "Proceedings, CREAS, Lakeway, TX, May"; also submitted for publication.
5. BACHMAIR, L., DERSHOWITZ, N., AND HSIANG, J. (1986), Orderings for equational proofs, *in* "Proceedings, LICS'86, Cambridge, MA, June 16–18," pp. 346–357.
6. BERGE, C. (1971), "Principles of Combinatorics," Academic Press, New York.
7. DERSHOWITZ, N. (1987), Termination of rewriting, *J. Symbolic Comput.* **3**, 69–116.
8. DOWNEY, P. J., SEETHI, R., AND TARJAN, E. R. (1980), Variations on the common subexpressions problem, *J. Assoc. Comput. Mach.* **27**, No. 4, 758–771.
9. GALLIER, J. H. (1986), "Logic for Computer Science: Foundations of Automatic Theorem Proving," Harper & Row, New York.
10. GALLIER, J. H., RAATZ, S., AND SNYDER, W. (1987), Theorem proving using rigid E-unification: Equational matings, *in* "Proceedings, LICS'87, Ithaca, NY, June 22–25," pp. 338–346.
11. GALLIER, J. H., NARENDRAN, P., PLAISTED, D., RAATZ, S., AND SNYDER, W. (1987), Finding canonical rewriting systems equivalent to a finite set of ground equations in polynomial time, submitted for publication.
12. GALLIER, J. H., NARENDRAN, P., PLAISTED, D., AND SNYDER, (1988), Rigid E-unification is NP-complete, *in* "Proceedings, LICS'88, Edinburgh, Scotland, July 5–8," pp. 218–227.
13. GALLIER, J. H., NARENDRAN, P., RAATZ, S., AND SNYDER, W. (1988), Theorem proving using equational matings and rigid E-unification, submitted for publication.
14. GIRARD, J. Y. (1987), Linear logic, *Theoret. Comput. Sci.* **50**, No. 1, 1–102.
15. HERBRAND, J. (1971), Sur la théorie de la démonstration, *in* "Logical Writings" (W. Goldfarb, Ed.), Harvard Univ Press, Cambridge MA.

16. HUET, G. (1980), Confluent reductions: Abstract properties and applications to term rewriting systems, *J. Assoc. Comput Mach.* **27**, No. 4, 797–821.
17. HUET, G., AND OPPEN, D. C. (1982), Equations and rewrite rules: A survey, *in* "Formal Languages: Perspectives and Open Problems" (R. V. Book, Ed.), Academic Press, New York.
18. KNUTH, D. E., AND BENDIX, P. B. (1970), Simple word problems in univeral algebras, *in* "Computational Problems in Abstract Algebra" (J. Leech, Ed.), Pergamon, Elmsford, N.Y.
19. KOZEN, D. (1976), "Complexity of Finitely Presented Algebras," Technical Report TR 76–294, Department of Computer Science, Cornell University, Ithaca, NY.
20. KOZEN, D. (1981), Positive first-order logic is NP-complete, *IBM J. Res. Develop.* **25**, No. 4, 327–332.
21. LEVY, A. (1979), "Basic Set Theory," Springer-Verlag, New York.
22. MARTELLI, A., AND MONTANARI, U. (1982), An efficient unification algorithm, *ACM Trans. Programming Languages Systems* **4**, No. 2, 258–282.
23. METIVIER, Y. (1983), About the rewriting systems produced by the Knuth–Bendix completion algorithm, *Inform. Process. Lett.* **16**, 31–34.
24. NELSON G., AND OPPEN, D. (1980), Fast decision procedures based on congruence closure, *J. Assoc. Comput. Mach.* **27**, No. 2, 356–364.
25. PATERSON, M. S., AND WEGMAN, M. N. (1978), Linear unification, *J. Comput. System Sci.* **16**, 158–167.
26. PLOTKIN, G. (1972), Building in equational theories, *Machine Intelligence* **7**, 73–90.