The Unification Hierarchy is Undecidable

Werner Nutt

SEKI Report SR-89-06

SEKI Report SR-89-06, April 1989
FB Informatik, Universität Kaiserslautern, West Germany

The Unification Hierarchy is Undecidable

Werner Nutt

German Research Center for Artificial Intelligence (DFKI)
Postfach 2080, D-6750 Kaiserslautern, West Germany
e-mail: nutt@informatik.uni-kl.de

Abstract

In unification theory, equational theories can be classified according to the existence and cardinality of minimal complete solution sets for equation systems. For unitary, finitary, and infinitary theories minimal complete solution sets always exist and are singletons, finite, or possibly infinite sets, respectively. In nullary theories, minimal complete sets do not exist for some equation systems. These classes form the unification hierarchy.

We show that it is not possible to decide where a given equational theory resides in the unification hierarchy. Moreover, it is proved that for some classes this problem is not even recursively enumerable.

Keywords: Equational Theories, Matching, Unification.

Contents

1 Introduction

Unification theory is concerned with problems of the following kind: Given two terms built from function symbols and variables, do there exist terms that can be substituted for the variables such that the two terms thus obtained are equal? This operation, called *unification* of terms, is the fundamental operation in automated deduction. In his seminal paper that presented the resolution calculus for first order predicate logic, Robinson [1965] gave an algorithm to compute a unifying substitution of two terms and proved that this *unifier* is most general in the sense that every other unifier can be obtained from it by further instantiation of variables.

Plotkin [1972] suggested to generalize Robinson's syntactic unification to unification modulo equationally defined first order theories as a more efficient means for equational deduction. Since then, equational unification has been built into resolution theorem provers, logic programming languages, and completion procedures for rewriting systems. In his survey, Siekmann [1989] gives an overview of the different applications of unification.

In the presence of equalities, a single most general unifier representing all solutions need no longer exist. If for instance associative and commutative function symbols are involved, a finite number of unifiers is needed to represent all other unifiers. In the case of associativity alone, even infinitely many unifiers may be necessary. Therefore, one introduces the concept of a *complete set of unifiers* representing all solutions and, more specifically, a *minimal complete set* of unifiers.

Siekmann [1978] divided equational theories into four classes. For *unitary*, *finitary*, and *infinitary* theories minimal complete sets of unifiers always exist and are singletons, finite, or possibly infinite sets, respectively. In *nullary* theories, minimal complete sets do not exist for some equation systems. This classification is known as the unification hierarchy. Examples for the classes are the theory of boolean rings (unitary), the theory of associativity and commutativity (finitary) and associativity alone (infinitary). It is well known that unification of typed lambda terms is nullary, but for a long time it was an open problem whether there exist nullary first order theories until Fages and

Huet [1986] constructed an (artificial) example. A naturally occurring example was exhibited by Baader [1986] and Schmidt-Schauß [1986] who independently proved for unification under associativity and idempotence, that is unification in idempotent semigroups, that minimal complete sets need not exist.

The question whether the hierarchy can still be refined has to be answered negatively. Book and Siekmann [1986] showed that if for an equational theory there exists an equation system having a minimal complete set whose cardinality is at least two then there are systems having minimal complete sets of arbitrarily great cardinality.

From a computational point of view, theories with small minimal complete sets are what is needed whereas infinitary or nullary theories are of little practical interest. It would therefore be desirable to recognize from the presentation of a theory its unification type to exclude unfeasible cases from the very beginning.

We prove that this is impossible. To be more precise, we show that none of the unification types is decidable and that the classes of infinitary and nullary theories are not even semi-decidable, that is, recursively enumerable. Moreover, the same is still true if unification is replaced by the somewhat more special case of matching where substitution is only allowed for the variables on one side of the equations to be unified.

The undecidability of the unification and matching hierarchy has already been stated in [Bürckert et al. 1987], but the proof in that paper contains a serious error [Baader 1989].

The paper is organized as follows. In section 2 we briefly review the basic definitions of unification theory and fix our notation. Section 3 presents results from combinatorial group theory saying that there are groups for which it is undecidable whether a given element has order one, finite order greater one, or infinite order. In section 4, these problems are reduced to the decision problem whether a theory is of unification or matching type unitary, finitary or infinitary. The undecidability of type nullary is shown in section 5 by a reduction of the consistency problem for equational theories.

2 Basic Definitions and Notations

We briefly review the necessary notions and notation from unification and monoid theory. A collection of papers representing the state of the art in unification theory can be found in the special issue [Kirchner 1989].

2.1 Equational Theories

We assume that two disjoint denumerable sets of symbols are given, a set of function symbols (like a, b, f) and a set of variables (like x, y, z).

A *signature* Σ is a finite set of function symbols each of which is associated with a nonnegative integer, determining its arity. We define Σ-terms (like s, t) and Σ-substitutions (like $\lambda, \mu, \sigma, \tau$) as usual. The set of variables occurring in s is denoted as $\mathcal{V}(s)$. A substitution σ that is determined by its values on the variables $\{x_1, \ldots, x_n\}$ will be represented as $[x_1/\sigma x_1, \ldots, x_n/\sigma x_n]$. The identity substitution that maps every term to itself is written as $[\,]$.

An *equational theory* $\mathcal{E} = (\Sigma, E)$ is a pair consisting of a signature Σ and a finite set $E = \{s_1 \doteq t_1, \ldots, s_n \doteq t_n\}$ of equations between Σ-terms. The theory $\mathcal{E}$ induces a stable congruence $=_{\mathcal{E}}$ on the set of all Σ-terms. A theory is *monadic* if its signature contains only unary function symbols. Since we assume a fixed denumerable set of symbols, there are only denumerably many equational theories.

For a given set of variables V we extend $=_{\mathcal{E}}$ to substitutions by defining $\sigma =_{\mathcal{E},V} \sigma'$ if $\sigma x =_{\mathcal{E}} \sigma' x$ for all $x \in V$. In this case we say that σ and σ' are $\mathcal{E}$-equal on V. We define a quasi-ordering on substitutions by $\sigma \geq_{\mathcal{E},V} \sigma'$ if there exists a substitution λ such that $\sigma =_{\mathcal{E},V} \lambda\sigma'$. In this case we say that σ' is *more general on* V than σ and that σ is an *$\mathcal{E}$-instance on* V of σ'. We say that σ' is *strictly more general on* V than σ, and we write $\sigma >_{\mathcal{E},V} \sigma'$ if $\sigma \geq_{\mathcal{E},V} \sigma'$ and not $\sigma' \geq_{\mathcal{E},V} \sigma$. We say that σ' and σ are *independent on* V, if neither $\sigma' \geq_{\mathcal{E},V} \sigma$ nor $\sigma \geq_{\mathcal{E},V} \sigma'$.

A theory $\mathcal{E}$ is *inconsistent* if $x =_{\mathcal{E}} y$ holds for two distinct variables x, y, otherwise it is *consistent*. In the following, we require equational theories to be consistent.

2.2 Unification and Matching

A Σ-*equation system* is a finite sequence $\Gamma = \langle s_1 \doteq t_1, \ldots, s_n \doteq t_n \rangle$ of equations between Σ-terms. The set of variables occurring in Γ is denoted as $\mathcal{V}(\Gamma)$.

A unification problem is given by a theory $\mathcal{E} = (\Sigma, E)$ and a Σ-equation system Γ. An $\mathcal{E}$-*unifier* of Γ is a substitution σ such that $\sigma s_i =_{\mathcal{E}} \sigma t_i$ for $i = 1, \ldots, n$. We denote the set of all $\mathcal{E}$-unifiers of Γ as $U_{\mathcal{E}}(\Gamma)$. A subset $U \subseteq U_{\mathcal{E}}(\Gamma)$ is *complete* if for every $\sigma \in U_{\mathcal{E}}(\Gamma)$ there is a $\sigma' \in U$ such that $\sigma \geq_{\mathcal{E},\mathcal{V}(\Gamma)} \sigma'$. A complete set U represents $U_{\mathcal{E}}(\Gamma)$ in the sense that every unifier is an $\mathcal{E}$-instance on $\mathcal{V}(\Gamma)$ of some element of U.

The set of complete subsets of $U_{\mathcal{E}}(\Gamma)$ is ordered by set inclusion. A complete subset is *minimal* if it is minimal with respect to set inclusion. In general, minimal complete sets need not exist, but if they exist they have equal cardinality [Fages/Huet, 1986]. Furthermore, two minimal complete subsets U and U' are equivalent in the sense that for every $\sigma \in U$ there exists some $\sigma' \in U'$ such that $\sigma \geq_{\mathcal{E},\mathcal{V}(\Gamma)} \sigma'$ and $\sigma' \geq_{\mathcal{E},\mathcal{V}(\Gamma)} \sigma$. A complete subset U is minimal iff any two elements of U are independent on $\mathcal{V}(\Gamma)$.

Often one defines complete sets of minimal unifiers instead of minimal complete sets of unifiers. It is easy to show that both concepts are equivalent, but the latter allows for technically simpler proofs.

Siekmann [1978, 1989] introduced a classification of equational theories, which is known as the unification hierarchy. He divided equational theories into four classes, depending on the existence and cardinality of minimal sets of unifiers. Let $\mathcal{E}$ be a theory, then:

$\mathcal{E} \in \mathcal{U}_1$	iff	minimal sets of unifiers exist for all Γ and have at most one element ($\mathcal{E}$ is of type 1 or $\mathcal{E}$ is *unitary*)
$\mathcal{E} \in \mathcal{U}_\omega$	iff	finite minimal sets of unifiers exist for all Γ and $\mathcal{E} \notin \mathcal{U}_1$ ($\mathcal{E}$ is of type ω or $\mathcal{E}$ is *finitary*)
$\mathcal{E} \in \mathcal{U}_\infty$	iff	minimal sets of unifiers exist for all Γ and $\mathcal{E} \notin \mathcal{U}_1 \cup \mathcal{U}_\omega$ ($\mathcal{E}$ is of type ∞ or $\mathcal{E}$ is *infinitary*)
$\mathcal{E} \in \mathcal{U}_0$	iff	there is some Γ for which no minimal set of unifiers exists ($\mathcal{E}$ is of type 0 or $\mathcal{E}$ is *nullary*).

If we are only interested in substituting into the variables of one side of the equations, we call such a problem an *$\mathcal{E}$-matching problem.* We write $\langle s_1 \ll t_1, \ldots, s_n \ll t_n \rangle$ for the problem to find a substitution σ, satisfying $\sigma x = x$ for all $x \in \bigcup_{i=1}^{n} \mathcal{V}(t_i)$, with $\sigma s_i =_{\mathcal{E}} t_i$ for $i = 1, \ldots, n$. We call such a substitution an *$\mathcal{E}$-matcher* of $s_1, \ldots, s_n$ to $t_1, \ldots, t_n$. Notice that the restriction on σ implies that σ does not change the terms t_i, that is $\sigma t_i = t_i$, and hence every $\mathcal{E}$-matcher is also an $\mathcal{E}$-unifier of the terms. The set of all $\mathcal{E}$-matchers of $s_1, \ldots, s_n$ to $t_1, \ldots, t_n$ is denoted by $M_{\mathcal{E}}(s_1 \ll t_1, \ldots, s_n \ll t_n)$.

Let V be the set of variables occurring in the terms s_i and t_i. A subset $M \subseteq M_{\mathcal{E}}$ is *complete* if for every $\sigma \in M_{\mathcal{E}}$ there exists some $\sigma' \in M$ with $\sigma \geq_{\mathcal{E},V} \sigma'$. Again, a complete set of matchers is *minimal* if it is minimal with respect to set inclusion.

Analogously to the unification hierarchy, we define a matching hierarchy with classes $\mathcal{M}_1$, $\mathcal{M}_\omega$, $\mathcal{M}_\infty$, and $\mathcal{M}_0$ of equational theories depending on the existence and cardinality of minimal sets of matchers.

2.3 Words, Monoids, Groups

An *alphabet* Σ is a finite set of function symbols. We denote the set of words (like u, v, w) over Σ by Σ^* and the empty word by e.

A *monoid presentation* (or Thue system) is a pair $\mathcal{M} = (\Sigma, \Delta)$ consisting of an alphabet Σ and a finite set Δ of word equations over Σ. The equations introduce a congruence $=_{\mathcal{M}}$ on Σ^*, thus associating to every word $w \in \Sigma^*$ the $=_{\mathcal{M}}$-equivalence class $\overline{w}$. By abuse of notation we will identify the presentation $\mathcal{M}$ and the factor monoid $\Sigma^* / =_{\mathcal{M}}$, speaking of the *finitely presented monoid* $\mathcal{M}$.

We assume that for every alphabet Σ there exists a disjoint alphabet $\Sigma^{-1} = \{a^{-1} \mid a \in \Sigma\}$. An alphabet Σ' is a *group alphabet* if $\Sigma' \doteq \Sigma \cup \Sigma^{-1}$ for some alphabet Σ. The *inverse* of a word over Σ' is defined by $e^{-1} = e$, $(aw)^{-1} = w^{-1}a^{-1}$, and $(a^{-1}w)^{-1} = w^{-1}a$. For integers $n \in \mathbf{Z}$ the *n-th power* of w is defined by $w^0 = e$, $w^n = ww^{n-1}$ if $n > 0$, and $w^n = (w^{-1})^{-n}$ if $n < 0$.

A *group presentation* is a monoid presentation $\mathcal{G} = (\Sigma \cup \Sigma^{-1}, \Delta)$ such that for all $a \in \Sigma$ we have $aa^{-1} \doteq e \in \Delta$ and $a^{-1}a \doteq e \in \Delta$. The factor monoid

defined by $\mathcal{G}$ is a group with inverses $(\overline{w})^{-1} = \overline{w^{-1}}$.

For $\overline{w} \in \mathcal{G}$ the *subgroup generated by* $\overline{w}$ is the least subgroup of $\mathcal{G}$ containing $\overline{w}$. It consists of the elements $\overline{w^k}$ for $k \in \mathbf{Z}$, and is denoted as $\langle \overline{w} \rangle$.

The *word problem* for a finitely presented group $\mathcal{G}$ is to decide for an arbitrary word w whether $w =_{\mathcal{G}} e$. There exist finitely presented groups with an undecidable word problem.

An alphabet Σ can be transformed into a signature by considering each element as a unary function symbol. Given a variable x, every word $w = a_1 a_2 \ldots a_n \in \Sigma^*$ is then transformed into a term $a_1(a_2(\ldots(a_n(x))\ldots))$, abbreviated to wx. Conversely, for every Σ-term t there exists a word $w \in \Sigma^*$ with $t = wx$ for some variable x.

To every finitely presented monoid $\mathcal{M} = (\Sigma, \Delta)$ there corresponds a monadic theory $\mathcal{E} = (\Sigma, E)$ where E is obtained from Δ by transforming each word equation $u \doteq v \in \Delta$ into the term equation $ux \doteq vx$. Equality in $\mathcal{M}$ and equality with respect to $\mathcal{E}$ are related by the equivalence $u =_{\mathcal{M}} v \iff ux =_{\mathcal{E}} vx$ for all $u, v \in \Sigma^*$.

3 The Order Problem

In this section we review some undecidability results from group theory.

The cardinality of a set S is denoted as $|S|$, where $|S| = \infty$ if S is infinite. If $\mathcal{G} = (\Sigma, \Delta)$ is a finitely presented group and $w \in \Sigma^*$, then the *order* of w is defined as $ord(w) = |\langle \overline{w} \rangle|$, that is, $ord(w)$ is the cardinality of the subgroup generated by $\overline{w}$.

Proposition 3.1. *Let $\mathcal{G} = (\Sigma, \Delta)$ be a finitely presented group and $w \in \Sigma^*$. If $\langle \overline{w} \rangle$ is finite, then $ord(w)$ is the least nonnegative integer n such that $w^n =_{\mathcal{G}} e$. If $\langle \overline{w} \rangle$ is infinite, such an integer does not exist. In particular, $ord(w) = 1$ iff $w =_{\mathcal{G}} e$.*

We will show that there are finitely presented groups for which it is undecidable whether a word has order one, finite order greater one, or infinite order.

Since deciding whether a word has order one is equivalent to the word problem, part of our claim follows from the existence of a group with an undecidable word problem. To show that all three problems are undecidable, we need groups with additional properties.

Theorem 3.2. *There exists a finitely presented group $\mathcal{G} = (\Sigma, \Delta)$ with an undecidable word problem such that the only element of finite order is the identity.*

Proof. Actually, such a group was exhibited by Boone and Collins. We refer to the presentation of their construction in [Rotman 1973] and show that every nonidentity element of this group has infinite order . Since we are not interested in group theoretic details, we present our arguments in such a way that it is possible to verify their correctness using standard textbooks on the subject.

In [Rotman 1973], a finite sequence of finitely presented groups $\mathcal{G}_0$, $\mathcal{G}_1$, $\mathcal{G}_1'$, $\mathcal{G}_2$, $\mathcal{G}_3$, $\mathcal{G}$ is constructed. It is shown that $\mathcal{G}_0$ is a free group, and that each of the other groups is an *HNN* extension with basis its predecessor. The group $\mathcal{G}$ has an undecidable word problem.

To this construction the Torsion Theorem for *HNN* extensions [Lyndon/Schupp 1977] can be applied. It says that an *HNN* extension has elements of finite order n only if its basis has elements of order n. Since in a free group every nonidentity element has infinite order, it follows from the Torsion Theorem that none of the groups occurring in the sequence has elements of finite order $n > 1$. In particular, $\mathcal{G}$ is a group with an undecidable word problem such that the only element of finite order is the identity. □

Since in this group a word has either order one or inifinite order, we obtain the following corollary.

Corollary 3.3. *There exists a finitely presented group $\mathcal{G} = (\Sigma, \Delta)$ such that the following problems are undecidable:*
INSTANCE: *a word $w \in \Sigma^*$*

QUESTION 1: *is* $ord(w) = 1$ *?*
QUESTION 2: *is* $ord(w) = \infty$ *?*

Corollary 3.4. *There exists a finitely presented group* $\mathcal{G} = (\Sigma, \Delta)$ *such that the set* $\{w \in \Sigma^* \mid ord(w) = \infty\}$ *is not recursively enumerable.*

Proof. The group from Theorem 3.2 has the desired property. For this group, the set $\{w \in \Sigma^* \mid ord(w) = \infty\}$ is the complement of the set $\{w \in \Sigma^* \mid ord(w) = 1\}$, the latter being undecidable but recursively enumerable. □

To find a group where it is undecidable whether a word has finite order greater one, we have to modify the construction exhibited by the last theorem.

Corollary 3.5. *There exists a finitely presented group* $\mathcal{G}' = (\Sigma', \Delta')$ *such that the following problem is undecidable:*
INSTANCE: a word $w' \in \Sigma'^*$
QUESTION: *is* $1 < ord(w') < \infty$ *?*

Proof. By Theorem 3.2 there exists a finitely presented group $\mathcal{G} = (\Sigma, \Delta)$ with an undecidable word problem such that the only element of finite order is the identity. Let b be a symbol not occurring in Σ. Define

$$\mathcal{G}' := (\Sigma', \Delta')$$

where

$$\begin{aligned} \Sigma' &= \Sigma \cup \{b, b^{-1}\} \qquad \text{and} \\ \Delta' &= \Delta \cup \{ab \doteq ba \mid a \in \Sigma\} \\ &\quad \cup \{bb^{-1} \doteq e, b^{-1}b \doteq e\} \\ &\quad \cup \{bb \doteq e\}. \end{aligned}$$

That is, $\mathcal{G}'$ is the direct product of $\mathcal{G}$ with the cyclic group of order two.

Now, for $w' \in (\Sigma')^*$ we have $1 < ord(w') < \infty$ if and only if $w' =_{\mathcal{G}'} bw$ for some $w \in \Sigma^*$ satisfying $w =_{\mathcal{G}} e$. Thus determining whether a given element of

$\mathcal{G}'$ has strictly finite order is equivalent to solving the word problem in $\mathcal{G}$ which is undecidable. □

4 Undecidability of Types Unitary, Finitary, and Infinitary

The aim of this section is to reduce the problem of deciding the order of a group element to the problem of deciding the unification type of an equational theory.

Construction 4.1. Let $\mathcal{G} = (\Sigma, \Delta)$ be a finitely presented group. For every $w \in \Sigma^*$ we define a finitely presented monoid

$$\mathcal{G}_w := (\Sigma \cup \{f\}, \Delta \cup \{fw \doteq f\})$$

where f is a symbol not occurring in Σ. We denote the monadic theory corresponding to $\mathcal{G}_w$ as $\mathcal{E}_w$.

Next, we investigate $\mathcal{E}_w$-equality of terms. Given a word $w \in \Sigma^*$, we say that words $u, v \in \Sigma^*$ are *equal modulo* w if $u =_{\mathcal{G}} w^k v$ for some integer k, and we write $u \sim_w v$.

Proposition 4.2. *$\sim_w$ is an equivalence relation on Σ^*.*

In fact, $\sim_w$ is the right congruence defined by $\langle \overline{w} \rangle$.

Proposition 4.3. *Let $u, v \in \Sigma^*$. Then $fu =_{\mathcal{G}_w} fv$ if and only if $u \sim_w v$.*

Lemma 4.4. *Let $u = u_0 f u_1 f \ldots f u_m$ and $v = v_0 f v_1 f \ldots f v_n$ where $u_i, v_j \in \Sigma^*$. Then $u =_{\mathcal{G}_w} v$ if and only if*

1. $m = n$
2. $u_0 =_{\mathcal{G}} v_0$, *and*
3. $u_i \sim_w v_i$ *for* $i = 1, \ldots, m$.

Proof. The sufficiency of the conditions is an immediate consequence of Proposition 4.3.

To prove the necessity, suppose $u =_{\mathcal{G}_w} v$. Since no equation in $\mathcal{G}_w$ changes the number of fs, u and v contain the same number of fs. Thus condition (1) is necessary. A further inspection of the equations shows, that every proof of $u =_{\mathcal{G}_w} v$ contains proofs of $u_0 =_{\mathcal{G}_w} v_0$ and $fu_i =_{\mathcal{G}_w} fv_i$ for $i = 1, \ldots, m$. Since u_0, v_0 don't contain fs, the proof of $u_0 =_{\mathcal{G}_w} v_0$ is in fact a proof of $u_0 =_{\mathcal{G}} v_0$. Thus condition (2) is necessary. The necessity of condition (3) follows from Proposition 4.3. □

The idea in defining $\mathcal{E}_w$ is best illustrated by the following example. Consider the $\mathcal{E}_w$-unification problem $\langle fx \doteq fy \rangle$. Then the substitution $\sigma_0 = [x/y, y/y]$ is a unifier, and more generally, for every $k \in \mathbf{Z}$ the substitution $\sigma_k = [x/w^k y, y/y]$ is also a unifier.

If $ord(w) = 1$, then all these unifiers are $\mathcal{E}_w$-equal. If $ord(w) = n < \infty$, then $\sigma_0, \ldots, \sigma_{n-1}$ are pairwise $\mathcal{E}_w$-different on $\{x, y\}$, and $\sigma_k =_{\mathcal{E}_w, \{x,y\}} \sigma_{k+n}$ for $k \in \mathbf{Z}$. Finally, if $ord(w) = \infty$ then all σ_k are $\mathcal{E}_w$-different on $\{x, y\}$.

Next we show that every $\mathcal{E}_w$-unifier of our problem is an $\mathcal{E}_w$-instance of some σ_k on $\{x, y\}$. If τ is an arbitrary unifier, then τx and τy contain the same number of fs. Suppose the two terms do not contain any fs. Then we have $\tau x = uz$ and $\tau y = vz$ for some $u, v \in \Sigma^*$ and some variable z. Since $fuz = \tau(fx) =_{\mathcal{E}_w} \tau(fy) = fvz$, Lemma 4.4 implies $u \sim_w v$, hence $u =_{\mathcal{G}} w^k v$ for some $k \in \mathbf{Z}$. Thus, $\tau =_{\mathcal{E}_w, \{x,y\}} [x/w^k vz, y/vz] =_{\mathcal{E}_w, \{x,y\}} [y/vz][x/w^k y, y/y] = \lambda\sigma_k$, where $\lambda = [y/vz]$. This implies $\tau \geq_{\mathcal{E}_w, \{x,y\}} \sigma_k$. In case τx and τy contain some f, a similar argument shows that $\tau \geq_{\mathcal{E}_w, \{x,y\}} \sigma_k$ for some $k \in \mathbf{Z}$.

Finally, we examine which of the unifiers σ_k are independent. Suppose $\sigma_k =_{\mathcal{E}_w, \{x,y\}} \lambda\sigma_l$. We can assume that $\lambda = [y/vy]$ for some $v \in (\Sigma \cup \{f\})^*$. Then we have $y = \sigma_k y =_{\mathcal{E}_w} (\lambda\sigma_l)y = \lambda(\sigma_l y) = \lambda y = vy$, hence $y =_{\mathcal{E}_w} vy$. This yields $w^k y = \sigma_k x =_{\mathcal{E}_w} (\lambda\sigma_l)x = \lambda(\sigma_l x) = \lambda w^l y = w^l vy =_{\mathcal{E}_w} w^l y$. Hence $\sigma_k \geq_{\mathcal{E}_w, \{x,y\}} \sigma_l$ iff $w^k =_{\mathcal{G}_w} w^l$. Thus we have shown that for w of finite order σ_k and σ_l are independent on $\{x, y\}$ if $0 \leq k < l < ord(w)$, and that for w of infinite order, σ_k and σ_l are $\mathcal{E}_w$-independent on $\{x, y\}$ if $k \neq l$.

In summary, the $\mathcal{E}_w$-unification problem $\langle fx \doteq fy \rangle$ has a minimal complete set of unifiers of cardinality $ord(w)$.

The same kind of argument that we used in the discussion of the above example applies to arbitrary unification and matching problems consisting of a single equation. The next two propositions give a complete case analysis of such problems.

Proposition 4.5. (Unification) *Suppose* $u = u_0 f u_1 f \dots f u_m$ *and* $v = v_0 f v_1 f \dots f v_n$ *where* u_i, $v_j \in \Sigma^*$ *such that* $m \leq n$.

1. *The unification problem* $\langle ux \doteq vx \rangle$ *is solvable iff* $u =_{\mathcal{G}_w} v$. *In this case* $\{[]\}$ *is a minimal complete set of unifiers.*

2. *The unification problem* $\langle u_0 x \doteq vy \rangle$ *is solvable and* $\{[x/u_0^{-1}vy, y/y]\}$ *is a minimal complete set of unifiers.*

3. *For* $m > 0$ *the unification problem* $\langle ux \doteq vy \rangle$ *is solvable iff*

   - $u_o =_{\mathcal{G}} v_0$
   - $u_i \sim_w v_i$ *for* $i = 1, \dots, m-1$.

   In this case,

   $$\{ [x/u_m^{-1} w^k v_m f \dots f v_n y, y/y] \mid k \in \mathbf{Z} \}$$

   is a minimal complete set of unifiers if $ord(w) = \infty$, *and*

   $$\{ [x/u_m^{-1} w^k v_m f \dots f v_n y, y/y] \mid 0 \leq k < ord(w) \}$$

   is a minimal complete set of unifiers if $ord(w) < \infty$.

Proposition 4.6. (Matching) *Suppose* $u = u_0 f u_1 f \dots f u_m$ *and* $v = v_0 f v_1 f \dots f v_n$ *where* u_i,$v_j \in \Sigma^*$.

1. *The matching problem* $\langle ux \ll vx \rangle$ *is solvable iff* $u =_{\mathcal{G}_w} v$. *In this case* $\{[]\}$ *is a minimal complete set of matchers.*

2. *The matching problem* $\langle u_0 x \ll vy \rangle$ *is solvable and* $\{[x/u_0^{-1}vy, y/y]\}$ *is a minimal complete set of matchers.*

3. *For* $m > 0$ *the matching problem* $\langle ux \ll vy \rangle$ *is solvable iff*

   - $m \leq n$
   - $u_o =_{\mathcal{G}} v_0$
   - $u_i \sim_w v_i$ *for* $i = 1, \ldots, m-1$.

   In this case,

   $$\{ [x/u_m^{-1}w^k v_m f \ldots f v_n y, y/y] \mid k \in \mathbf{Z} \}$$

   is a minimal complete set of matchers if $ord(w) = \infty$, *and*

   $$\{ [x/u_m^{-1}w^k v_m f \ldots f v_n y, y/y] \mid 0 \leq k < ord(w) \}$$

   is a minimal complete set of matchers if $ord(w) < \infty$.

Bürckert et al. [1987] give an example of a theory of type 0 such that for every equation minimal complete sets of unifiers and matchers, respectively, exist. For this theory, systems that do not possess minimal sets consist of at least two equations. The example shows that in general we cannot locate a theory in the hierarchy by inspecting only single equations. On the other hand, we can do so provided the theory is not nullary [Bürckert et al. 1987].

Lemma 4.7. *$\mathcal{E}_w$ is not nullary.*

Proof. It suffices to prove that there is no infinite descending chain of substitutions $\sigma_1 >_{\mathcal{E}_w, V} \sigma_2 >_{\mathcal{E}_w, V} \ldots$ where V is a finite set of variables. Assume by contradiction that such an infinite chain exists.

Let $W_i := \bigcup_{x \in V} \mathcal{V}(\sigma_i x)$ be the set of variables introduced by σ_i via the variables in V. Since $\sigma_i >_{\mathcal{E}_w, V} \sigma_{i+1}$ and $\mathcal{E}_w$ is monadic, we have $|W_i| \leq |W_{i+1}|$. Furthermore, we have $|W_i| \leq |V|$, since $\mathcal{E}_w$ is monadic. Therefore we can assume without loss of generality that $W_i = W$ for some fixed finite set W.

For each $y \in W$ let $V_i^y := \{x \in V \mid \mathcal{V}(\sigma_i x) = \{y\}\}$. Every family $(V_i^y)_{y \in W}$ is a partition of V. Since V is finite, there exist only finitely many partitions of V. Therefore we can assume without loss of generality that $V_i^y = V^y$ for some fixed partition $(V^y)_{y \in W}$ of V. Thus for every $x \in V$ we have $\mathcal{V}(\sigma_i x) = \mathcal{V}(\sigma_{i+1} x)$.

Furthermore we can assume without loss of generality that for every $x \in V$ all terms $\sigma_i x$ contain the same number of fs.

Let λ_i be substitutions such that $\sigma_i =_{\mathcal{E}_w, V} \lambda_i \sigma_{i+1}$. To obtain a contradiction, it suffices to construct substitutions μ_i such that $\mu_i \sigma_i =_{\mathcal{E}_w, V} \sigma_{i+1}$.

Since for $x \in V$ the terms $\sigma_i x$ and $\sigma_{i+1} x$ contain the same number of fs, the substitution λ_i doesn't introduce any f. Hence, for $y \in W$ the term $\lambda_i y$ contains only symbols from the group alphabet. Now, define $\mu_i y := v^{-1} y$ where $vy = \lambda_i y$ for $y \in W$ and $\mu_i y := y$ otherwise.

We will show that $\mu_i \sigma_i =_{\mathcal{E}_w, V} \sigma_{i+1}$. Let $x \in V$. Then $x \in V^y$ for some $y \in W$. Let $\sigma_i x = u_i y$, $\sigma_{i+1} x = u_{i+1} y$, and $\lambda_i y = vy$. Then $u_i =_{\mathcal{G}_w} u_{i+1} v$ which implies $u_i v^{-1} =_{\mathcal{G}_w} u_{i+1}$. By definition of the μ_is it follows that $\mu_i \sigma_i x =_{\mathcal{E}_w} \sigma_{i+1} x$, which yields the claim. □

Propositions 4.5 and 4.6 say that for a single equation in $\mathcal{E}_w$ minimal complete sets of unifiers and matchers, respectively, have at most cardinality $ord(w)$ and that there exist such sets having exactly cardinality $ord(w)$. Since no theory $\mathcal{E}_w$ is nullary, the position of $\mathcal{E}_w$ in the hierarchy depends on the order of w.

Proposition 4.8.

- $\mathcal{E}_w \in \mathcal{M}_1 \iff \mathcal{E}_w \in \mathcal{U}_1 \iff ord(w) = 1$
- $\mathcal{E}_w \in \mathcal{M}_\omega \iff \mathcal{E}_w \in \mathcal{U}_\omega \iff 1 < ord(w) < \infty$
- $\mathcal{E}_w \in \mathcal{M}_\infty \iff \mathcal{E}_w \in \mathcal{U}_\infty \iff ord(w) = \infty$

Having established the correspondence between the order of group elements and the type of an equational theory, we can reduce the order problem for groups to the problem of locating a theory in the hierarchy.

Theorem 4.9.

1. *$\mathcal{U}_\infty$ and $\mathcal{M}_\infty$ are not recursively enumerable.*

2. *$\mathcal{U}_1, \mathcal{U}_\omega, \mathcal{U}_\infty$, $\mathcal{M}_1$, $\mathcal{M}_\omega$, and $\mathcal{M}_\infty$ are undecidable.*

Proof. 1. The claim is true, since by Proposition 3.4 there exists a finitely presented group $\mathcal{G} = (\Sigma, \Delta)$ such that the set $\{w \in \Sigma^* \mid ord(w) = \infty\}$ is not recursively enumerable.

2. The claim is true, since by Propositions 3.3 and 3.5 there exist finitely presented groups for which it is undecidable whether a word has order one, finite order greater one, or infinite order. □

5 Undecidability of Type Nullary

In this section we reduce the consistency problem for equational theories to the decision problem whether a theory is nullary. Since the disjoint combination of a consistent theory and a nullary theory is again nullary, by combination of an arbitrary theory $\mathcal{E}$ with a nullary theory we can construct a theory that is nullary if and only if $\mathcal{E}$ is consistent.

We start with a well-known result from equational logic, which has been proved by Perkins [1967]. Recall that a theory $\mathcal{E}$ is inconsistent iff $x =_\mathcal{E} y$ for two distinct variables x and y, and consistent otherwise.

Lemma 5.1. *The following problem is undecidable:*
INSTANCE: *an equational theory $\mathcal{E}$*
QUESTION: *is $\mathcal{E}$ consistent ?*

Corollary 5.2. *The set of equational theories $\{\mathcal{E} \mid \mathcal{E}$ is consistent$\}$ is not recursively enumerable.*

Proof. If for a theory $\mathcal{E}$ we have $x =_{\mathcal{E}} y$, then this fact can be derived by equational deduction. By a dovetailing argument, this implies that the set of inconsistent theories is recursively enumerable. Hence, the set of consistent theories is not recursively enumerable, since, by the preceding lemma, it is undecidable. □

Let $\mathcal{E}_1 = (\Sigma_1, E_1)$ and $\mathcal{E}_2 = (\Sigma_2, E_2)$ be equational theories such that the signatures Σ_1 and Σ_2 are disjoint. The *disjoint combination* of $\mathcal{E}_1$ and $\mathcal{E}_2$ is the theory $\mathcal{E}_1 \uplus \mathcal{E}_2 := (\Sigma_1 \cup \Sigma_2, E_1 \cup E_2)$. The following lemma which is due to Tidén [1986] and Schmidt-Schauß [1989] says that the disjoint combination of consistent theories does not influence the structure of pure unification problems.

Lemma 5.3. *Let $\mathcal{E}_1 = (\Sigma_1, E_1)$ and $\mathcal{E}_2 = (\Sigma_2, E_2)$ be consistent equational theories such that Σ_1 and Σ_2 are disjoint, and let $\mathcal{E} := \mathcal{E}_1 \uplus \mathcal{E}_2$ be their disjoint combination. If Γ is an $\mathcal{E}_1$-unification problem and U is a complete set of $\mathcal{E}_1$-unifiers of Γ, then*

1. *U is also a complete set of $\mathcal{E}$-unifiers of Γ*
2. *$\geq_{\mathcal{E}_1, \mathcal{V}(\Gamma)}$ and $\geq_{\mathcal{E}, \mathcal{V}(\Gamma)}$ agree on U.*

Theorem 5.4. *$\mathcal{U}_0$ and $\mathcal{M}_0$ are not recursively enumerable.*

Proof. Let $\mathcal{E}_0 = (\Sigma_0, E_0)$ be a nullary theory. Then there exist an $\mathcal{E}_0$-unification problem Γ and a complete set of unifiers U_0 of Γ such that U_0 has no minimal complete subset.

Suppose $\mathcal{E}$ is a consistent theory. By the preceding lemma, U_0 is also a complete set of unifiers of Γ for the combined theory $\mathcal{E}^+ := \mathcal{E}_0 \uplus \mathcal{E}$, and U_0 has no minimal complete subset if $\mathcal{E}$ is consistent. Hence, $\mathcal{E}^+$ is nullary if $\mathcal{E}$ is consistent. Conversely, the combined theory $\mathcal{E}^+$ is inconsistent if $\mathcal{E}$ is inconsistent. Thus we have proved that $\mathcal{E}^+$ is nullary if and only if $\mathcal{E}$ is consistent.

Were $\mathcal{U}_0$ recursively enumerable, then in particular the set of theories $\{\mathcal{E}^+ \mid \mathcal{E}^+ \text{ is nullary}\}$ would be recursively enumerable. Hence the set $\{\mathcal{E} \mid$

$\mathcal{E}$ is consistent} would be recursively enumerable, which is impossible by Corollary 5.2.

The proof that $\mathcal{M}_0$ is not recursively enumerable is completely analogous. □

Theorem 5.5. *$\mathcal{U}_0$ and $\mathcal{M}_0$ are not recursively enumerable.*

Proof. Let $\mathcal{E}_0 = (\Sigma_0, E_0)$ be a nullary theory. Then there exist an $\mathcal{E}_0$-unification problem Γ and a complete set of unifiers U_0 of Γ such that U_0 has no minimal complete subset.

Suppose $\mathcal{E} = (\Sigma, E)$ is a consistent theory such that Σ and Σ_0 are disjoint. By the preceding lemma, U_0 is also a complete set of unifiers of Γ for the combined theory $\mathcal{E}^+ := \mathcal{E}_0 \uplus \mathcal{E}$, and U_0 has no minimal complete subset if $\mathcal{E}$ is consistent. Hence, $\mathcal{E}^+$ is nullary if $\mathcal{E}$ is consistent. Conversely, the combined theory $\mathcal{E}^+$ is inconsistent if $\mathcal{E}$ is inconsistent. Thus we have proved that $\mathcal{E}^+$ is nullary if and only if $\mathcal{E}$ is consistent.

Were $\mathcal{U}_0$ recursively enumerable, then in particular the set of theories $\{\mathcal{E}_0 \uplus \mathcal{E} \mid \mathcal{E}_0$ and $\mathcal{E}$ have disjoint signatures, and $\mathcal{E}_0 \uplus \mathcal{E}$ is nullary$\}$ would be recursively enumerable. From this it would follow that the set $\{\mathcal{E} \mid \mathcal{E}_0$ and $\mathcal{E}$ have disjoint signatures, and $\mathcal{E}$ is consistent$\}$ is recursively enumerable, which is impossible by Corollary 5.2. □

Corollary 5.6. *$\mathcal{U}_0$ and $\mathcal{M}_0$ are not decidable.*

6 Conclusion

There is no algorithm to decide for an arbitrary equational theory where it resides in the unification or matching hierarchy. Moreover, our proofs show also that for the restricted case of a theory having only unary function symbols it is impossible to decide whether it is unitary, finitary or infinitary.

The undecidability proofs for the types ∞ and 0 admit the stronger result

that these types are not even recursively enumerable. It is an open problem whether the types 1 and ω are semi-decidable, and I conjecture they are not.

In the light of this paper's results, it seems more promising to investigate the hierarchy problem for special classes of theories. Since theories that are essentially equivalent can be presented with different signatures and different equations, a viable method can be to single out algebraic and model theoretic properties of a theory that determine its unification type. In general, these properties will not be decidable, but decidable sufficient criteria are to be expected.

Acknowledgments: I like to thank K. Madlener for his hints to the literature on undecidability results in group theory. H.-J. Bürckert and J. Siekmann read draft versions, and discussions with them contributed very much to the present form of the paper.

References

F. Baader, "The Theory of Idempotent Semigroups is of Unification Type Zero," *J. Automated Reasoning* **2**, 1986, 283–286.

F. Baader, personal communication, 1989.

R. Book and J. Siekmann, "On Unification: Equational Theories are not Bounded," *J. Symbolic Computation* **2**, 1986, 317–324.

H.-J. Bürckert, A. Herold, and M. Schmidt-Schauß, "On Equational Theories, Unification, and Decidability," *Proc. 2nd Conference on Rewriting Techniques and Applications, LNCS* **256**, Springer, 1987, 240–250. Also C. Kirchner (ed.), *J. Symbolic Computation, Special Issue on Unification*, 1989.

C. Kirchner (ed.), *J. Symbolic Computation, Special Issue on Unification*, 1989, to appear.

F. Fages and G. Huet, "Complete Sets of Unifiers and Matchers in Equational Theories," *Theoretical Computer Science* **43** (2,3), 1986, 189–200.

R. C. Lyndon and P. E. Schupp, *Combinatorial Group Theory*, Springer, 1977.

P. Perkins, "Unsolvable Problems for Equational Theories," *Notre Dame J. Formal Logic*, **8**, 1967, 175–185.

G. Plotkin, "Building in Equational Theories," *Machine Intelligence* **7**, 1972, 73–90.

J. A. Robinson, "A Machine-Oriented Logic Based on the Resolution Principle", *J. ACM* **12** (1), 1965, 23–41.

J. J. Rotman, *The Theory of Groups*, Allyn and Bacon, 1973.

M. Schmidt-Schauß, "Unification under Associativity and Idempotence is of Type Nullary," *J. Automated Reasoning* **2**, 1986, 277–281.

M. Schmidt-Schauß, "Unification in a Combination of Arbitrary Disjoint Equational Theories," in C. Kirchner (ed.), *J. Symbolic Computation, Special Issue on Unification*, 1989.

J. H. Siekmann, *Unification and Matching Problems*, PhD Thesis, University of Essex, 1978.

J. H. Siekmann, "Unification Theory. A Survey," in C. Kirchner (ed.), *J. Symbolic Computation, Special Issue on Unification*, 1989.

E. Tidén, "Unification in Combinations of Collapse-Free Theories with Disjoint Sets of Function Symbols," *Proc. 8th Conference on Automated Deduction, LNCS* **230**, Springer, 1986, 431–450.