Unification in Commutative Semigroups

Andrzej Kisielewicz*

Institute of Mathematics, University of Wroclaw, Wroclaw, Poland

Communicated by Walter Feit
Received January 27, 1997

Unification is one of the basic concepts of automated theorem proving. It concerns such questions as finding solutions of finite sets of equations, determining if every solution comes from a most general solution, and if so, determining how many most general solutions are needed to generate all solutions. These solutions given in terms of substitutions are called, more formally, unifiers. The unification type of a variety (equational class) of algebras is defined according to the cardinality or existence of minimal complete sets of most general unifiers. Of particular interest, from a computational point of view, are varieties of groups and semigroups. So far the problem has been considered mainly for particular varieties. In this paper we determine unification types for all varieties of commutative semigroups. In particular, we prove that for commutative semigroups the unification problem is solvable in the very strong sense that there is an algorithm which for any two finite sets $\Sigma_1$ and $\Sigma_2$ of semigroup equations produces the minimal complete set of the most general unifiers of $\Sigma_1$ over the variety of commutative semigroups generated by $\Sigma_2$. It seems that this is the first so general decidability result in the area.

1. INTRODUCTION

The process of solving equations is central to much of algebra. The unification problem in the context of varieties of algebras was first considered by G. D. Plotkin [24]. Much work on unification has been done in last decade. In one, computational, direction unification algorithms were developed for particular varieties of algebras. In another, mathematical, direction some undecidability results were obtained and unification types were established for most important varieties. We have made an attempt to list the most recent references. For earlier results and wide applications

* Supported by KBN Grant 2 P 301 027 07.
E-mail address: kisiel@math.uni.wroc.pl.
We shall use the following general terminology. Let $V$ be a variety (equational class) of algebras and $X$ a fixed infinite set of variables. Terms in the language of the equational theory of $V$ are called $V$-terms. Substitutions are functions assigning $V$-terms to variables. If $\sigma$ is a substitution and $p$ a $V$-term, then by $\sigma(p)$ we denote the term resulting from substituting for every variable $v$ in $p$ the corresponding term $\sigma(v)$.

We shall consider only substitutions restricted to a finite number of variables. Assuming that variables in question form an ordered $n$-tuple, e.g., $(v_1, \ldots, v_n)$, a substitution $\sigma$ will be identified with an $n$-tuple of $V$-terms $t_1, \ldots, t_n$, meaning that $\sigma(v_i) = t_i$ for all $i$. The product $\sigma_1 \sigma_2$ of two substitutions is defined by $(\sigma_1 \sigma_2)(v_i) = \sigma_2(\sigma_1(v_i))$, where the right hand side is interpreted, of course, as the image of the term $\sigma_1(v_i)$ under the substitution $\sigma_2$.

For a finite set of equations $S$ over $V$ in the variables $x_1, \ldots, x_n$ and a substitution $\sigma$ of $V$-terms for these variables we say that $\sigma$ is a unifier of $S$ (or unifies $S$), if the equation $\sigma(p) = \sigma(q)$ holds in $V$ for each equation $p = q \in S$.

Let $U(S, V)$ denote the set of all unifiers of $S$ in $V$. For $\sigma_1, \sigma_2 \in U(S, V)$ we say that $\sigma_1$ is more general than $\sigma_2$, and write $\sigma_1 \leq \sigma_2$, if there is a substitution $\tau$ such that $\sigma_2 = \tau \sigma_1$.

Let $\sim$ be the equivalence relation $\leq \cap \geq$. Minimal elements (modulo $\sim$) of $U(S, V)$ are called the most general unifiers of $S$. A set $\mathcal{B}$ of most general unifiers is called complete, if for every $\sigma \in U(S, V)$ there is $\tau \in \mathcal{B}$ such that $\tau \leq \sigma$, and it is called minimal, if no element can be removed from $\mathcal{B}$ without violating this property.

Now, if every $U(S, V)$ is of the form $\{\sigma : \sigma \geq \sigma_0\}$ for some most general unifier $\sigma_0$, then variety $V$ is said to have unitary unification type. If the unification type of $V$ is not unitary, but every $U(S, V)$ is of the form $\{\sigma : \sigma \geq \sigma_1 \text{ or } \ldots \text{ or } \sigma \geq \sigma_n\}$ for some most general unifiers $\sigma_1, \ldots, \sigma_n$, then unification type of $V$ is finitary. If not, but still every $U(S, V)$ is of the form $\{\sigma : \sigma \geq \sigma_i \text{ for } i < \omega\}$, then the unification type of $V$ is infinitary. Otherwise, $V$ is said to have nullary unification type.

We should note that some authors prefer more precise terminology in terms of free objects and homomorphisms (which is usually connected with using semantical arguments rather than syntactical). Some other authors prefer to speak about first order theories and languages rather than about varieties (and make a clear distinction between variables and their names). We prefer a little informality in order to present our arguments in reasonably short form. What is more important, the reader should note that in some papers variants of unification problems are considered in computer science see [16, 29, 31]. For background on varieties and equations see [22].
admitting constants (and even additional function symbols) in the language of groups or semigroups, which often changes situation completely.

In this paper we consider the standard language of semigroups without constants. Note however, that admitting constants without any relations (as it is usually done for the variety of all semigroups or all commutative semigroups) does not change the situation very much and our proofs can be modified easily to include this case.

2. EXAM P L E S

We start from three simple examples we are going to refer to later in our proof.

Example 1. Denote by $\Sigma$ the set consisting of two equations $xyzt = yz^2$ and $xy^2z = xyt^3$. We wish to find all solutions

$$(x, y, z, t) = (v_1^{\alpha_1} \cdots v_n^{\alpha_n}, v_1^{\beta_1} \cdots v_n^{\beta_n}, v_1^{\gamma_1} \cdots v_n^{\gamma_n}, v_1^{\delta_1} \cdots v_n^{\delta_n})$$

of $\Sigma$ in the variety VCS of all commutative semigroups. First, we note, that since in VCS two terms are equal if and only if they have the same exponents, we may reduce $\Sigma$ to the system $xt \approx z$ and $yz \approx t^3$. Then, substituting a possible solution (1) to the reduced equations leads (for every $i \leq n$) to a system of homogenous linear equations

$$\alpha_i - \gamma_i + \delta_i = 0$$
$$\beta_i + \gamma_i - 3\delta_i = 0$$

with integral coefficients. Of course, we are interested only in solutions in non-negative integers of this system. There are well-known algorithms to solve systems of linear Diophantine equations. Here, it is not difficult to see that such solutions are generated by four-tuples

$$(\alpha_i, \beta_i, \gamma_i, \delta_i) = (0, 2, 1, 1), (1, 1, 2, 1), (2, 0, 3, 1).$$

The combinations of these yield seven ($= 2^3 - 1$) solutions of $\Sigma$ in the variety of all commutative monoids (i.e., semigroups with the unit) containing all most general solutions. Some of them, however, are not solutions in VCS, since they involve the unit (e.g., $(x, y, z, t) = (1, v^2, v, v)$). Yet, it is already not difficult to determine the most general solutions $(x, y, z, t)$ of $\Sigma$ generating all solutions of $\Sigma$ in VCS. These are

$$(v, v, v^2, v), (v, vu^2, v^2u, vu), (vu^2, v, v^2u^3, vu), (vu^2, w^2v, wv^2u^3, wvu).$$
UNIFICATION IN COMMUTATIVE SEMIGROUPS

It is the idea contained in this example that can be generalized to obtain the result that the unification type of VCS is finitary (cf. Lemma 4.1).

Example 2. Let NULL be the variety of null-semigroups, i.e., of those satisfying \( xy = z^2 \). We denote 0 = xy. Here, every equation is equivalent either to equation \( 0 = xy \) (if terms on both sides are composite) or to \( x = 0 \) or \( x = y \). In the first case the equation always holds, so the most general unifier is given in terms of single variables. In the second case the most general unifier has 0 at the place corresponding to the variable \( x \). In the third case the most general unifier is just \( \sigma = (v, v) \) (which is more general than \((0,0)\)). It follows easily that NULL has unitary unification type.

Example 3. Let \( A_r \) be the variety of commutative semigroups satisfying \( x^r y = y \) \((r > 1)\). This is equivalent to the variety of abelian groups of exponent \( r \). We denote \( 1 = x^r \). Here every equation is equivalent to

\[ x_{a_1}^{f_1} \cdots x_{a_n}^{f_n} = 1 \]

with \( 0 < a_1, \ldots, a_n \leq r \) and every unifier can be written in the form

\[ \sigma = (v_1^{a_1}, v_1^{a_2}, \ldots, v_1^{a_s}, \ldots, v_s^{a_s}) \]

where the right hand side is understood to be an \( n \)-tuple with \( 0 < a_i, \beta_i, \ldots, \xi_i \leq r \) for all \( i \leq s \). Note that \( \sigma \) unifies Eq. (2) if and only if \( \sigma_i = (v_i^{a_i}, v_i^{a_2}, \ldots, v_i^{a_s}) \) unifies (2) for all \( i \leq s \). Hence, looking for unifiers of a set of equations \( \Sigma \) we need only to look for unifiers of the form \( \sigma_i \) above. Since \( 0 < a_i, \beta_i, \ldots, \xi_i \leq r \), there is only a finite number of different unifiers of \( \Sigma \) of this form, say, \( \sigma_1, \sigma_2, \ldots, \sigma_s \). Then, \( \sigma \) given in (3) is also the unifier of \( \Sigma \), and obviously, it is more general than any other unifier of \( \Sigma \). Hence, the unification type of \( A_r \) is unitary.

3. VARIETIES OF COMMUTATIVE SEMIGROUPS

Most of the results on unification in groups and semigroups concern particular varieties rather than families of varieties (such as all subvarieties of a given variety). This is due to the fact that there is relatively little knowledge on varieties of groups and semigroups. Well-known families of varieties, like the varieties of abelian groups, for example, tend to lead to simple generalizations provided the original problem is solved for a representative of the family.

The varieties of commutative semigroups are not like that. Our proof is based on the description of varieties of commutative semigroups given in
ANDRZEJ KISIELEWICZ

[17], which is, not quite simple and easy, but as we shall see, useful. For the convenience of the reader we recall here briefly the terminology of this description and the results we apply.

Let $\Gamma$ denote the set of all finite sequences $(\alpha_1, \ldots, \alpha_n)$ of non-negative integers such that at least one $\alpha_j \neq 0$. We define

\[ (\alpha_1, \ldots, \alpha_n) \leq (\beta_1, \ldots, \beta_m) \]

if and only if there is a partition $\pi$ of the set $\{1, \ldots, n\}$ and a one-to-one mapping $\psi$ from the set $B_{\pi}$ of the blocks of $\pi$ into the set $\{1, \ldots, m\}$ such that for every $B \in B_{\pi}, \sum_{i \in B} \alpha_i \leq b_{\psi(B)}$. Then, $(\Gamma, \leq)$ is a well-quasi-ordered set; in particular, every (order) filter $J$ in $\Gamma$ is finitely generated.

Note that two sequences are equivalent (the relation $\leq$ holds in both directions) if and only if they differ at most in the arrangement of elements and the number of zeros. Thus, in every equivalence class there is a nondecreasing sequence of positive integers, and it is unique. Every filter is generated by a finite set of such sequences. The least set among these is an antichain of minimal elements, and it is called the fundamental antichain of the filter. By $d(J)$ we denote the maximal length of the sequences in the fundamental antichain.

Note that if $n < m$ and $\beta_1 \geq \cdots \geq \beta_n$, the relation (4) does not depend on $\beta_{m+1} \geq \cdots \geq \beta_m$. We will need later the following simple consequence of this fact.

**Lemma 3.1.** Let $(\alpha_1, \ldots, \alpha_n) \in \Gamma$ with $\alpha_1 \geq \cdots \geq \alpha_n$ and $J$ be a filter in $(\Gamma, \leq)$. If $n > d = d(J)$, then $(\alpha_1, \ldots, \alpha_n) \in J$ if and only if $(\alpha_1, \ldots, \alpha_n) \in J$

We shall use the fact, that in particular, if $\alpha_i \leq \beta_i$ for all $i \leq n \leq m$, then the relation (4) holds. Also, for $k = \sum \alpha_i$ the one-element sequence $(k) \geq (\alpha_1, \ldots, \alpha_n)$. Consequently, in every (nonempty) filter $J$ there is a sequence of the length one. The least $k$ such that $(k) \in J$ is denoted by $k(J)$.

For integers $k \geq m \geq 0$, $r > 0$, and the sequences $(\alpha_1, \ldots, \alpha_n)$, $(\beta_1, \ldots, \beta_n)$ in $\Gamma$ we consider the following four conditions.

(N1) If $\sum \alpha_i \neq \sum \beta_i$, then both $\sum \alpha_i, \sum \beta_i \geq k$.

(N2) If $\sum \alpha_i = \sum \beta_i$, then for every $j$ such that $\alpha_j \neq \beta_j$, both $(\alpha_j + \sum \alpha_i), (\beta_j + \sum \beta_i) \geq k$.

(N3) For every $i$, $\alpha_i \equiv \beta_i \pmod{r}$.

(N4) For every $i$, if $\alpha_i \neq \beta_i$, then both $\alpha_i, \beta_i \geq m$. 
We say that an equation of the form

\[ x_1^{\alpha_1} \cdots x_n^{\alpha_n} = x_1^{\beta_1} \cdots x_n^{\beta_n} \]  

(5)

satisfies the conditions (N1)–(N4), if the sequences of the exponents do so.

Let \( m \geq 0, r > 0 \) be integers and \( J \), a nonempty filter contained in the (principal) filter \([m]\) generated by the one-element sequence \((m)\) (for \( m = 0 \), we define \([0]\) = \( \Gamma \)). Let \( \pi \) be an equivalence relation on the set \( \Gamma \setminus J \) of those finite sequences of positive integers that are not in \( J \). Then \( \pi \) is called a remainder of type \((m,r,J)\) if for all pairs \((\alpha_1, \ldots, \alpha_n), (\beta_1, \ldots, \beta_n) \) \( \in \pi \) the following conditions are satisfied.

\( (\pi 0) \quad n = t. \)

\( (\pi 1) \) The conditions (N1)–(N4) hold, for \( k = k(J) \).

\( (\pi 2) \) For every permutation \( \sigma \) of the set \( \{1, 2, \ldots, n\} \),

\[ ((\alpha_{1\sigma}, \ldots, \alpha_{n\sigma}), (\beta_{1\sigma}, \ldots, \beta_{n\sigma})) \in \pi. \]

\( (\pi 3) \) For every \( i \) with \( \alpha_i \neq \beta_i \) and \( \mu_i = \min(\alpha_i, \beta_i) \),

\[ (\alpha_1, \ldots, \alpha_n, \mu_i) \in J. \]

\( (\pi 4) \) Either \((\alpha_1, \ldots, \alpha_n, 1), (\beta_1, \ldots, \beta_n, 1) \) \( \in \pi \) or both \((\alpha_1, \ldots, \alpha_n, 1), (\beta_1, \ldots, \beta_n, 1) \) \( \in J \).

\( (\pi 5) \) For every \( i \leq j \leq n \), if \((\alpha_1, \ldots, \alpha_i + \alpha_j, \ldots, \alpha_n) \) is the sequence obtained from \((\alpha_1, \ldots, \alpha_n) \) by replacing \( \alpha_i \) by \( \alpha_i + \alpha_j \) and deleting \( \alpha_i \), then either \((\alpha_1, \ldots, \alpha_i + \alpha_j, \ldots, \alpha_n), (\beta_1, \ldots, \beta_i + \beta_j, \ldots, \beta_n) \) \( \in \pi \) or both \((\alpha_1, \ldots, \alpha_i + \alpha_j, \ldots, \alpha_n), (\beta_1, \ldots, \beta_i + \beta_j, \ldots, \beta_n) \) \( \in J \).

In [17] it has been shown that every remainder can be explicitly described by listing a finite number of elements. Namely, to put it briefly, if \( Id(\pi) \) is the set of the equations of the form (5) corresponding to the elements of \( \pi \), then for every remainder \( \pi \) there exists a finite set \( F(\pi) \) of equations, such that an equation \( e \in Id(\pi) \) if and only if it is of the form \( wt = ut \) for some word \( t \) (possibly empty) and \((w = u) \in F(\pi) \). A minimal finite set with this property is called a base of the remainder \( \pi \). By \( d(\pi) \) we denote the minimal number of variables necessary to write this set down.

Now, given integers \( m \geq 0, r > 0 \), a nonempty filter \( J \subseteq [m] \), and a remainder \( \pi \) of type \((m,r,J)\), we define \( \mathcal{F}(m,r,J,\pi) \) to be the class of all commutative semigroups \( S \) such that an Eq. (5) (with \( \alpha_i + \beta_i > 0 \)) holds in \( S \) if and only if either both \((\alpha_1, \ldots, \alpha_n), (\beta_1, \ldots, \beta_n) \) \( \in J \) and satisfy the condition (N3) and (N4), or both \((\alpha_1, \ldots, \alpha_n), (\beta_1, \ldots, \beta_n) \notin J \) and \((\alpha_1, \ldots, \alpha_n), (\beta_1, \ldots, \beta_n) \) \( \in \pi \).
By $\text{VCS}$ we denote the variety of all commutative semigroups. Then, our main result in [17, Theorem 4.8] can be stated as follows.

**Theorem 3.2.** Every class $\mathcal{V}(m, r, J, \pi)$ defined above is a variety, and every variety of commutative semigroups, other than $\text{VCS}$, is of this form.

The least remainder $\theta$ of type $(m, r, J)$ is the identity relation on the set $\Gamma_\theta \setminus J$. We write $\mathcal{V}(m, r, J)$ for $\mathcal{V}(m, r, J, \theta)$, and by $B(m, r, J)$ we denote the normal equational basis for $\mathcal{V}(m, r, J)$. The basis consists of the equations

$$x_1^{a_1} \cdots x_n^{a_n} = x_1^{a_1 + \epsilon} x_2^{a_2} \cdots x_n^{a_n},$$

for all sequences $(a_1, \ldots, a_n)$ in the fundamental antichain $A$ of $J$, and in addition, the equation $x^m y^k = x^m y^k$, $k = k(J)$, whenever $\alpha_i > m$ for all sequences in $A$ (that is, whenever it is not a consequence of the equations (6) themselves). The normal equational basis for $\mathcal{V}(m, r, J, \pi)$ is the union of $B(m, r, J)$ and a base for remainder $\pi$. The minimal number of variables necessary to write down such a basis is $\max(d(J), d(\pi))$ (unless $d(J) = 1$ and $m < k$; then this number may equal 2).

In [17] there is also an algorithm that for a given set of commutative semigroup equations $\Sigma$ outputs the $\mathcal{V}(m, r, J, \pi)$-form of the variety axiomatized by $\Sigma$ [17, Algorithm 5.5, p. 295]. We will make use of the fact of existence of such an algorithm only.

### 4. Unification Results

Let $V = \mathcal{V}(m, r, J, \pi)$ or $V = \text{VCS}$ be a variety of commutative semigroups, and $\Sigma$ a finite set of commutative semigroup equations in the variables $x_1, \ldots, x_n$. Then every $\sigma \in U(\Sigma, V)$ is of the form

$$\sigma = (v_1^{a_1} \cdots v_i^{a_i} \cdots v_s^{a_s}),$$

for some $s > 0$, where the right hand side is understood to be an $n$-tuple with $a_i, b_i, \ldots, e_i \geq 0$ for all $i \leq s$. Variables $v_1, \ldots, v_s$ will be referred to as variables of the unifier $\sigma$, and the numbers $a_i, b_i, \ldots, e_i$ will be called exponents of (the variable $v_i$ in) $\sigma$. We admit exponents equal to zero meaning that the corresponding variable is absent assuming, at the same time, that $\Sigma a_i, \Sigma b_i, \ldots, \Sigma e_i > 0$.

We introduce one more technical notion to apply in our proofs. If $\sigma'$ is a unifier more general than $\sigma$ and for each variable $u$ occurring in $\sigma'$ there is a variable $v_i$ in $\sigma$ such that exponents of $u$ in $\sigma'$ are not larger than the corresponding exponents of $v_i$ in $\sigma$ than we say that $\sigma'$ is strongly more general than $\sigma$. 
We start from the lemma that makes possible to include the special case of $V = VCS$ of Theorem 3.2 into our general proof.

**Lemma 4.1.** For every $V$ and $\Sigma$ as above, there exists a positive integer $M$ such that for every unifier $\sigma \in U(\Sigma, V)$ there is a strongly more general unifier with exponents not exceeding $M$.

**Proof.** First consider the case of $V = VCS$. Let $\sigma$ of the form (7) be a unifier of $\Sigma$. Then, in case of $VCS$, $\tau = (\xi_1, \xi_2, \ldots, \xi_f)$ is a unifier of $\Sigma$ for every $i \leq s$, provided a unit is adjoined to our theory and variables with the exponent 0 are treated as the unit. (In other words, $\tau$ is a solution of $\Sigma$ in the variety of all commutative monoids.)

To describe all the unifiers of $\Sigma$ it is enough to describe those of the form of $\tau$ above. This leads in an obvious way to a system $H$ of homogeneous linear equations in $\alpha_i, \beta_i, \ldots, \xi_i$ as in Example 1. Generalizing the observation made in Example 1, one sees that all we need is to show that there is $M$ such that each solution $(\alpha_i, \beta_i, \ldots, \xi_i)$ of $H$ in non-negative integers is a linear combination with non-negative integral coefficients of solutions with values not exceeding $M$.

To this end, let $S$ be a set of solutions $(\alpha_i, \beta_i, \ldots, \xi_i)$ of $H$ in non-negative integers such that neither majorizes other term by term. It is not difficult to observe that such a set must be finite (cf. [19] or [17, p. 279]), and therefore we may assume, in addition, that $S$ is maximal with this property. Choose $M$ to be the maximal integer value occurring in elements of $S$ and extend $S$ to the set of all solutions with values not exceeding $M$.

We claim that every solution of $H$ is a linear combination with non-negative integral coefficients of elements of $S$. Indeed, assume to the contrary, that there is a solution $s \in S$ that does not have this property and that $s$ is chosen to have the least possible sum $\alpha_i + \beta_i + \cdots + \xi_i$. By assumption there is $s' \in S$ such that $s$ majorizes $s'$ term by term. To get a desired contradiction it is enough to note that $s - s'$ is also a solution of $H$ belonging to $S$ and $s = s' + (s - s')$.

In case of $V = \mathcal{F}(m, r, J, \pi)$ the lemma is an immediate consequence of the fact that, according to Theorem 3.2, the equation $x^{k(1) + r} \approx x^{k(1)}$ holds in $V$. $\blacksquare$

Now we prove the following

**Lemma 4.2.** Let $V$ and $\Sigma$ be as above. Then, there exists a positive integer $N$ such that for every unifier $\sigma \in U(\Sigma, V)$ there is a strongly more general unifier in less than $N$ variables.

**Proof.** Suppose that $\sigma$ is of form (7). By virtue of Lemma 4.1 we may assume that $0 \leq \alpha_i, \beta_i, \ldots, \xi_i \leq M$ for all $i$. Call $n$-tuple $(\alpha_i, \beta_i, \ldots, \xi_i)$ the class of the variable $v_i$ occurring in $\sigma$. Then, there is a finite number $c$ of
the classes of variables whose components do not exceed \( M \). Let \( d \) be the minimal number of variables in the normal equational basis of \( V \), that is, \( d = \max(d(J), d(\pi)) \) or \( d = 2 \) (see Section 2). If \( V = VCS \), then we put \( d = 1 \). Now, if for the number \( s \) of variables in \( \sigma \), we have \( s > N = c \cdot d \), then there are at least \( d + 1 \) variables of the same class in \( \sigma \). Deleting one of these variables from \( \sigma \) we obtain a substitution \( \sigma' \), which is obviously strongly more general than \( \sigma \). All that remains is to prove that \( \sigma' \) is also a unifier of \( \Sigma \) in \( V \).

If \( V = VCS \), then this fact is clear from observations made in the proof of Lemma 4.1. Hence, assume that \( V = \mathcal{V}(m, r, J, \pi) \) and let \( p \equiv q \in \Sigma \). Then, since \( \sigma \) unifies \( \Phi \), \( \sigma(p) \equiv \sigma(q) \) holds in \( V \). Assuming that it is \( v_1, \ldots, v_{d+1} \) that are the variables of the same class in \( \sigma \), \( \sigma(p) \equiv \sigma(q) \) is of the form

\[
v_1^a \cdots v_{d}^a v_{d+1}^s = v_1^b \cdots v_{d}^b v_{d+1}^t,
\]

where \( s \) and \( t \) are \( V \)-terms having no occurrence of variables \( v_1, \ldots, v_{d+1} \).

If \( V \subseteq VCS \), then this fact is clear from observations made in the proof of Lemma 4.1. Hence, assume that \( V \subseteq VV \), \( r \), \( J \), \( p \), and let \( \alpha_s, \beta_s \) be the corresponding sequences of exponents of Eq. (9). Note that \( \alpha' \) and \( \beta' \) are obtained from \( \alpha \) and \( \beta \), respectively, just by removing the first element and that the number of \( \alpha \)'s in \( \alpha \) (\( \beta \)'s in \( \beta \)) is greater than \( d \geq \max(d(J), d(\pi)) \).

Suppose first that both \( \alpha, \beta \in J \). Then, by definition, \( \alpha \) and \( \beta \) satisfy conditions (N3) and (N4). It follows that also \( \alpha' \) and \( \beta' \) satisfy conditions (N3) and (N4). In turn, by Lemma 3.1, \( \alpha', \beta' \in J \), as well. Using the definition of \( \mathcal{V}(m, r, J, \pi) \) again we infer that (9) holds in \( V \).

The second possibility is that \( \alpha, \beta \notin J \) and (8) is of the form \( wt = ut \) with \( w = u \) \( \in F(\pi) \) (cf. Section 2). Since \( d \geq d(\pi) \), it follows that there is a variable \( v_j \) with \( j \leq d + 1 \) not occurring in \( w = u \), and hence, occurring in term \( t \). Consequently, \( \alpha = \beta \) and therefore (8) is of the form \( wt' = ut' \) for some term \( t' \). Obviously, \( \alpha, \beta \notin J \). Hence, by definition, (9) holds in \( V \) also in this case, thus completing the proof.

Combining Lemma 4.1 and Lemma 4.2 yields that every variety of commutative semigroups has either finitary or unitary unification type.

We show that except for the varieties given in Example 2 and 3 the first case holds.
**Theorem 4.3.** Every nontrivial variety $V$ of commutative semigroups has finitary unification type, unless $V$ is the variety of abelian groups of exponent $r > 1$ or the variety of null-semigroups, in which cases the unification type is unitary.

**Proof.** Assume, from now on, that $V$ is a nontrivial variety other than that of null-semigroups. Suppose also that $V$ has unitary unification type. We show that $V$ is the variety of abelian groups.

To this end, let $\sigma = (q, r, s, t)$, where $q, r, s, t$ are terms, be the most general unifier of equation $xy = zw$.

First, suppose to the contrary that no equation of the form $x^a = x$ ($a > 1$) holds in $V$. Then, since $\sigma_0 = (v, u, v, u)$ unifies $xy = zw$, and $\sigma$ is more general than $\sigma_0$, the terms $q, r, s$, and $t$ in $\sigma$ must be just single variables. Moreover, we have also $q \neq r$, since otherwise, the equation $v = u$ would have to hold in $V$. By the same reason, $q \neq t$. To prove, in turn, that also $q \neq s$, it is enough to observe that $\sigma_1 = (v, u, u, v)$ also unifies $xy = zw$ and use an analogous argument. Continuing in this way, we obtain that $q, r, s, t$ are pairwise distinct variables. Whence, equation $xy = zw$ holds in $V$, which means that $V$ is the variety of null-semigroups.

This contradiction proves that equation $x^a = x$ holds in $V$ for some $a > 1$.

Now assume, again to the contrary, that $V$ is regular, i.e., in every equation holding in $V$ the same variables occur on both sides. As $\sigma$ is more general than $\sigma_0$ defined above, there is a substitution $\tau$ such that $\tau(q) = v$ holds in $V$. Since this equation is regular (by assumption), $\tau$ has to substitute just $v$ for every variable in $q$. Similarly, $\tau(t) = u$ holds in $V$, and consequently, $\tau$ substitutes $u$ for every variable in $t$. It follows that terms $q$ and $t$ have no variables in common. Applying the same argument to substitution $\sigma_1$ rather than $\sigma_0$, one can infer that terms $q$ and $s$ have no variables in common, either. Since $\sigma$ unifies $xy = zw$, it follows that an irregular equation holds in $V$.

From the latter it is easy to deduce that there are positive integers $b, c, d$ such that equation $x^by^c = y^d$ holds in $V$. Now, combining this with the fact that $x^a = x$ holds in $V$, as well, it is not difficult to infer that $x^ay = y$. (In fact, this can be obtained immediately using Algorithm 5.5 given in [17].) This proves that $V$ is the variety of abelian groups of exponent dividing $a$, thus completing the proof.

Our proofs partially show that for varieties of commutative semigroups all typical questions concerning unification are decidable. In fact, we have the following general result.

**Theorem 4.4.** There is an algorithm which for any two finite sets $\Sigma_1$ and $\Sigma_2$ of semigroup equations produces the minimal complete set $U$ of the most general unifiers of $\Sigma_1$ over the variety $V$ of commutative semigroups generated
by \( \Sigma_1 \). Moreover, if \( \Sigma_2 \) contains a nontrivial equation, then the set \( U \) is always nonempty; otherwise \( (V = VCS) \) it may happen to be empty, meaning that no unifier of \( \Sigma_1 \) in \( V \) exists.

Proof. If \( \Sigma_2 \) is empty (or consists of only trivial equations), then \( V = VCS \) and the fact stated in the theorem is well known (see, e.g., [31]). Hence, we may suppose that \( V \neq VCS \), and consequently, that an equation \( x^{k+r} = x^k \) holds in \( V \) for some \( k, r > 0 \).

First, note that in this case substitution \( v = x^c \) for every variable \( v \) in \( \Sigma_1 \) is a unifier of \( \Sigma_1 \) in \( V \), provided \( c \) is sufficiently large. Indeed, equation \( x^{k+r} = x^k \) can be used to reduce the exponent of \( x \) on both sides of the equation to the same value. This proves the second statement.

Now, the proof of Lemma 4.2 shows, in fact, how the minimal set of most general unifiers can be found. First, observe that due to Algorithm 5.5 in [17] number \( D \) in this proof, and hence, number \( N \) can be effectively computed \( (M = k + r \) here). Therefore, by Lemma 4.2, there is a complete set of most general unifiers of \( \Sigma_1 \) contained in the set of unifiers in less than \( N \) variables with exponents not exceeding \( M = k + r \). The latter is obviously finite. So, it is enough to show that there is an algorithm for given two unifiers \( \sigma_1 \) and \( \sigma_2 \) that decides whether \( \sigma_1 \) is more general than \( \sigma_2 \).

To check this, we may restrict ourselves to only those substitutions in which variables in \( \sigma_1 \) are replaced by terms using only variables of \( \sigma_2 \), and with exponents not exceeding \( M = k + r \). Again, they are finite in number. Recalling that the result of substitution can be compared with \( \sigma_2 \) using Algorithm 5.5 in [17], completes the proof.

REFERENCES


