SOME DECIDABLE CONGRUENCES OF FREE MONOIDS

Jaroslav Ježek

Abstract. Let W be the free monoid over a finite alphabet A. We prove that a congruence of W generated by a finite number of pairs $\langle au, u\rangle$, where $a \in A$ and $u \in W$, is always decidable.

0. Introduction

Consider an equational theory E (of an arbitrary signature) based on a finite set of equations of the form $F(t_1, \ldots, t_n) \approx t_1$. It was proved in [2] and [3] that E has a unique perfect base P; this perfect base is a convergent term rewrite system for E. If P turns out to be finite, or at least recursive, it follows that the equational theory E is decidable. In many cases P is infinite, and we do not know if it is always recursive. For this reason, the question whether E is always decidable was formulated as an open problem in [3]. In this paper we will show that the answer is yes in the special case of equational theories (of the above form) of algebras with unary operations.

For a given unary signature τ, the terms over a single variable stand in a natural one-to-one correspondence with words over the alphabet A consisting of the operation symbols in τ. This natural correspondence can be extended to a correspondence between regular equations (equations having the same variables at the left and the right sides) and ordered pairs of words. Due to this correspondence, there is a natural isomorphism between the lattice of regular equational theories of signature τ and congruences of the free monoid over A. So, we are not going to work with equational theories; congruences of the free monoid will take their place.

A congruence r of the free monoid W over a finite alphabet A is called decidable if there is an algorithm deciding which ordered pairs of words belong to r. The aim of this paper is to prove that every congruence generated by a finite number of ordered pairs of the form $\langle au, u\rangle$, where $a \in A$ and $u \in W$, is decidable. The equivalent formulation, in terms of equational theories of unary algebras, is a corollary. The techniques used are those of term rewriting (see [1] for a survey) and perfect bases [3].

1. Congruences of free monoids

Let A be a finite alphabet and W be the free monoid over A. The elements of W are called words. A word u is said to be a subword of a word v if $v = puq$ for some words p and q. We write $u \subseteq v$ if u is a subword of v. If $u \subseteq v$ and $u \neq v$,

The work on this paper was partially supported by grant 201/96/0312, Grant Agency of the Czech Republic.

we say that u is a proper subword of v and write $u \subset v$. Two words are called incomparable if neither is a subword of the other. We say that u is a beginning (or an end) of v if $v = up$ (or $v = pu$, respectively) for some word p. The length of a word u is denoted by $\lambda(u)$.

Let S be a set of nonempty words. We denote by B_S the set of the ordered pairs $\langle au, u\rangle$ such that $au \in S$ and $a \in A$, and by α_S the congruence of W generated by B_S. Our aim is to study this congruence and to determine under what conditions it is decidable.

Given three words u, v and ar (where $a \in A$), we write $u \to_{ar} v$ if v can be obtained from u by replacing a subword ar with r. We write $u \to_S v$ if $u \to_{ar} v$ for some $ar \in S$. We say that u can be rewritten to v with respect to S if there exists a finite sequence $u_0, u_1, \dots, u_k$ ($k \geq 1$) such that $u_0 = u$, $u_k = v$ and $u_i \to_S u_{i+1}$ for all i.

We denote by $Q(S)$ the least set of words containing S and satisfying the following two conditions:

(1) if $au \in Q(S)$ and $u \to_{bw} v$ for some $bw \in Q(S)$ (where $a, b \in A$), then $av \in Q(S)$;
(2) if $aubv \in Q(S)$ and $bvw \in Q(S)$ (where $a, b \in A$), then $auvw \in S$.

By a derivation from S we mean a finite nonempty sequence $u_0, \dots, u_n$ of words such that for every $i \in \{0, \dots, n\}$ we have either $u_i \in S$ or there exist two (not necessarily distinct) indexes $j, k < i$ such that either $u_j = au$, $u_k = bw$, $u \to_{bw} v$ and $u_i = av$, or else $u_j = aubv$, $u_k = bvw$ and $u_i = auvw$ (where $a, b \in A$). We also say that $u_0, \dots, u_n$ is a derivation of u_n from S. Clearly, a word u belongs to $Q(S)$ if and only if there exists a derivation of u from S.

1.1. Lemma. *Let S be a set of nonempty words. Then $\alpha_{Q(S)} = \alpha_S$.*

Proof. Since $S \subseteq Q(S)$, we have $\alpha_S \subseteq \alpha_{Q(S)}$. Let $a_0u_0, \dots, a_nu_n$ be a derivation from S and let us prove by induction on i that $\langle a_iu_i, u_i\rangle \in \alpha_S$. The only case deserving attention is the case $a_ju_j = aubv$, $a_ku_k = bvw$, $a_iu_i = auvw$. By induction, $aubv\ \alpha_S\ ubv$ and $bvw\ \alpha_S\ vw$. We have $auvw\ \alpha_S\ aubvw\ \alpha_S\ ubvw\ \alpha_S\ uvw$. □

For any set S of words we denote by $R(S)$ the subset of S consisting of the words $u \in S$ that have no subword belonging to S.

1.2. Lemma. *Let S be a set of nonempty words. Then $\alpha_{RQ(S)} = \alpha_S$.*

Proof. By 1.1, $\alpha_{Q(S)} = \alpha_S$. Since $RQ(S) \subseteq Q(S)$, we have $\alpha_{RQ(S)} \subseteq \alpha_S$. It remains to prove $\langle au, u\rangle \in \alpha_{RQ(S)}$ by induction on the length of a word $au \in Q(S)$. If $au \in RQ(S)$, it is clear. Now let au have a proper subword belonging to S.

If the subword is a beginning of au, then we can write $u = u_1u_2$ where u_2 is nonempty and $au_1 \in Q(S)$. By induction, $au_1\ \alpha_{RQ(S)}\ u_1$; but then $au_1u_2\ \alpha_{RQ(S)}\ u_1u_2$, i.e., $au\ \alpha_{RQ(S)}\ u$.

In the other case we have $au = au_1bvu_2$ where $b \in A$ and $bv \in Q(S)$. By induction, $bv\ \alpha_{RQ(S)}\ v$. We have $au_1vu_2 \in Q(S)$, so by induction $au_1vu_2\ \alpha_{RQ(S)}\ u_1vu_2$. But $au\ \alpha_{RQ(S)}\ au_1vu_2$ and $u_1vu_2\ \alpha_{RQ(S)}\ u$, so $au\ \alpha_{RQ(S)}\ u$. □

By a perfect set of words we mean a set S satisfying the following two conditions:

(1) S is a set of nonempty, pairwise incomparable words;

(2) if $aubv \in S$ and $bvw \in S$ (where $a \in A$ and $b \in A$), then there is a word t such that uvw can be rewritten to t with respect to S and the word at has a beginning belonging to S.

By a perfect modification of a set S of nonempty words we mean a perfect set S' such that $\alpha_S = \alpha_{S'}$.

1.3. Theorem. *Let S be a perfect set of words. Then for any word u there exists a unique word u' such that u can be rewritten to u' and u' has no subword belonging to S. For any two words u, v we have $u\ \alpha_S\ v$ if and only if $u' = v'$.*

Proof. In the terminology of term rewriting, it is sufficient to prove that the set B_S has confluent critical pairs. Applied to our case, this means to prove that if $aubv \in S$ and $bvw \in S$, then $ubvw$ and $auvw$ can be rewritten to the same word with respect to S. Now $ubvw$ can be rewritten to uvw, and the rest follows from (2). □

1.4. Theorem. *Every set S of nonempty words has precisely one perfect modification. $RQ(S)$ is the perfect modification of S.*

Proof. By Lemma 1.2, $\alpha_S = \alpha_{QR(S)}$. Clearly, $QR(S)$ has the property (1); it is easy to see that it also has the property (2).

Let S_1 and S_2 be two perfect sets such that $\alpha_{S_1} = \alpha_{S_2}$; denote this congruence by α. We are going to prove $S_1 = S_2$. Let $au \in S_1$. Since $au\ \alpha\ u$, it follows from Theorem 1.3 applied to S_2 that au contains a subword $bv \in S_2$. Now $bv\ \alpha\ v$, so Theorem 1.3 applied to S_1 yields the existence of a subword $cw \in S_1$ in bv. But au contains no subword from S_1 other than itself, so $cw = bv = au$. We get $au \in S_2$ and thus $S_1 \subseteq S_2$. Similarly one can prove $S_2 \subseteq S_1$. □

For any set S of nonempty words denote by H_S the set of the words that contain no subword belonging to S. This set is always nonempty: at least it contains the empty word. For any word t we define a word $\nu_S(t) \in H_S$ by induction on the length of t as follows: if t is empty, then $\nu_S(t) = t$; if $t = aw$ where $a \in A$, then

$$\nu_S(aw) = \begin{cases} a\nu_S(w) & \text{if } a\nu_S(w) \in H_S, \\ \nu_S(w) & \text{otherwise.} \end{cases}$$

Equivalently,

$$\nu_S(aw) = \begin{cases} a\nu_S(w) & \text{if no beginning of } a\nu_S(w) \text{ belongs to } S, \\ \nu_S(w) & \text{otherwise.} \end{cases}$$

Clearly, ν_S is a mapping of W onto H_S and is the identity on H_S. It is easy to see that $\langle t, \nu_S(t)\rangle \in \alpha_S$ for any word t. If S is recursive, then ν_S is a computable mapping.

Let U be a set of words. For any word t and any $u \in U$ we define a word $t *_U u \in U$ by induction on the length of t as follows: if t is empty, then $t *_U u = u$; if $t = aw$ where $a \in A$, then

$$aw *_U u = \begin{cases} a(w *_U u) & \text{if } a(w *_U u) \in U, \\ w *_U u & \text{otherwise.} \end{cases}$$

Clearly, $aw *_U u = a *_U (w *_U u)$. So, if $t = a_1 \dots a_k$, where $a_i \in A$, then $t *_U u = a_1 *_U (a_2 *_U \dots (a_k *_U u))$. We get $t_1 t_2 *_U u = t_1 *_U (t_2 *_U u)$ for any words t_1, t_2 and $u \in U$.

U is called a model of S if $av *_U u = v *_U u$ for all $av \in S$ and all $u \in U$.

1.5. Lemma. *Let $\alpha_{S_1} = \alpha_{S_2}$. Then S_1 and S_2 have the same models.*

Proof. Let U be a model of S_1. Define a binary relation r on W by $\langle p, q\rangle \in r$ if and only if $p *_U u = q *_U u$ for all $u \in U$. It is easy to check that r is a congruence of W containing B_{S_1}, so r contains $\alpha_{S_1} = \alpha_{S_2} \supseteq B_{S_2}$ and U is a model of S_2. □

1.6. Lemma. *Let S be a set of nonempty words and P be the perfect modification of S. Let n be a positive integer. The set of the words of length at most n that belong to H_P is a model of S.*

Proof. Put $U = \{u \in H_P : \lambda(u) \leq n\}$. It is easy to prove by induction for any word t that if $u \in U$, then either $t *_U u\ \alpha_S\ tu$ or $\lambda(t *_U u) = n$. From this we get: either $t *_U u = \nu_P(tu)$ or $\lambda(t*_U) = n$. Let $av \in S$ and $u \in U$. We are going to prove $av*_U u = v*_U u$. Of course, $av*_U u = a*_U(v*_U u)$. If $\lambda(v*_U u) = n$, then $a(v*_U u) \notin U$ and so $a *_U (v *_U u) = v *_U u$. Let $\lambda(v *_U u) < n$. Then $a *_U (v *_U u) = a *_U \nu_P(vu)$; this word is either $a\nu_P(vu) = \nu_P(avu) = \nu_P(vu) = v *_U u$, or $\nu_P(vu) = v *_U u$, so in both cases $a *_U (v *_U u) = v *_U u$. □

1.7. Lemma. *Let S be a set of nonempty words and P be the perfect modification of S. Let U be a nonempty set of words. If U is closed with respect to subwords and contains a word not belonging to H_P, then it is not a model of S.*

Proof. Let w be a shortest word from $U - H_P$. Since w does not belong to H_P, it contains a subword belonging to P; this subword belongs to $U - H_P$, so by the minimality of w we get $w \in P$. We have $w = au$ for some $a \in A$ and some word u. The empty word o belongs to U. Evidently $au *_U o = au$ and $u *_U o = u$, so $au *_U o \neq u *_U o$ and U is not a model of P. By Lemma 1.5, U is not a model of S. □

1.8. Theorem. *Let S be a finite set of nonempty words. The perfect modification of S is a recursive set, and the congruence α_S is decidable.*

Proof. Let n be a positive integer. Suppose that we can decide for any word of length less than n whether it belongs to the perfect modification P of S. We shall show how to decide the same for any word of length n.

Let us consider all sets U of words with the following three properties:

(1) every word in U is of length at most n;
(2) a word of length less than n belongs to U if and only if it belongs to H_P;
(3) U is a model of S.

Clearly, every set with these properties is finite, there are finitely many of them, and we are able to find them effectively. Now, according to 1.6 and 1.7, the largest among these sets is precisely the intersection of H_P with the set of words of length at most n.

So, the set H_P is recursive. Consequently, the set P is recursive: a word u belongs to P if and only if it does not belong to H_P, but every proper subword of u belongs to H_P. Also, the mapping ν_P is computable. We have $\langle u, v\rangle \in \alpha_S$ if and only if $\nu_P(u) = \nu_P(v)$, so we are able to decide which pairs of words belong to α_S. □

1.9. Example. One would be tempted to speed up the algorithm in 1.8 a little by saying that a word u belongs to H_P iff the set $U = \{u\} \cup \{v \in H_P : \lambda(v) < \lambda(u)\}$ is a model of S. But this is not true. Let, for example, $S = \{aba\}$, so that

$P = \{ab^i a : i \geq 1\}$, and let $u = aa$. Then u belongs to H_P, although U is not a model of S: we have $aba *_U o = aa \neq a = ba *_U o$, where o is the empty word.

2. Equational theories of unary algebras

2.1. Theorem. *Let E be an equational theory of a finite unary signature, based on a finite number of equations of the form $F_0F_1 \dots F_k(x) \approx F_1 \dots F_k(x)$. Then E is decidable.*

Proof. This is a reformulation of Theorem 1.8. □

References

1. N. Dershowitz and J.-P. Jouannaud, *Rewrite systems*, Chapter 6, 243–320 in J. van Leeuwen, ed., Handbook of Theoretical Computer Science, B: Formal Methods and Semantics. North Holland, Amsterdam 1990.
2. J. Ježek, *Free groupoids in varieties determined by a short equation*, Acta Univ. Carolinae **23** (1982), 3–24.
3. J. Ježek and G.F. McNulty, *Perfect bases for equational theories*, to appear in J. Symbolic Computation.

Charles University, Sokolovská 83, 186 00 Praha 8, Czech Republic