NOVI SAD J. MATH.
VOL. 28, NO. 2, 1998, 109-117

UNDECIDABLE VARIETIES WITH SOLVABLE WORD PROBLEMS – III (A SEMIGROUP VARIETY)

Siniša Crvenković, Igor Dolinka
Institute of Mathematics,
University of Novi Sad
Trg D. Obradovića 4, 21000 Novi Sad,
Yugoslavia
e-mail: {*sima,dockie*}*@unsim.ns.ac.yu*

Abstract

The present note is a continuation of our work in [5], [6] and [7] on constructing varieties of small types given by reasonably simple recursive lists of equations, having solvable word problem, but undecidable equational theory (and thus uniformly unsolvable word problem). Here we give an example of a semigroup variety of such kind, inspired by some ideas of Wells [16]. This, in a certain sense, unifies our previous results in this field.

AMS Mathematics Subject Classification (1991): 08B99, 20M05, 20M07
Key words and phrases: varieties, decidability problems, semigroups

1. Introduction

Let $\mathcal{V}$ be a variety of algebras of a given type τ. The set of all equations of type τ holding on all members of $\mathcal{V}$, that is

$$Eq(\mathcal{V}) = \{p \approx q : \ \mathcal{V} \models p \approx q\},$$

is called *the equational theory of* $\mathcal{V}$. The equational theory of a variety $\mathcal{V}$ is said to be decidable, whenever $Eq(\mathcal{V})$ is a recursive set, otherwise it is

undecidable. Of course, one can consider other sets of formulæ, such as all first-order formulæ and quasi-identities, which are true on $\mathcal{V}$. In this way, we obtain respectively the elementary and the implicational theory of $\mathcal{V}$, and one can consider questions of their decidability as well. Of course, decidability of the elementary theory yields decidability of the implicational theory, and the latter yields decidabilty of the equational theory for any variety $\mathcal{V}$.

For example, varieties of Abelian groups and Boolean algebras have decidable elementary theory. Varieties of all groups and all lattices provide further examples of those having decidable equational theory. On the other hand, equational theories of varieties of modular lattices and relation algebras appear to be undecidable.

Another class of decidability problems in algebra are *word problems.* A *presentation of type* τ is a pair $\langle G, R\rangle$, where G is a nonempty set and R is a set of equations of type $\tau_G = \tau \cup G$ without variables (the elements of G are treated as new constant symbols adjoined to τ). In the case of semigroups, both sides of equations from R are just words over G. A presetation is *finite*, if such are both G and R. If Σ is a set of identities of type τ, *the word problem* for $\langle G, R\rangle$ over Σ asks if there is an algorithm to determine whether $\Sigma \cup R \vdash u \approx v$ for two terms u, v of type τ_G without variables.

However, it is more cusomary to speak about word problems for algebras and varieties instead of a rather logical settings of presentations and equations. Therefore, we say that an alegebra A (belonging to a variety $\mathcal{V}$ of type τ) is *presented* by $\langle G, R\rangle$, if $A \cong F_{\mathcal{V}}(G)/\theta_R$, where $F_{\mathcal{V}}(G)$ is the $\mathcal{V}$-free algebra freely generated by G and θ_R is the congruence on $F_{\mathcal{V}}(G)$ generated by $\{\langle u, v\rangle : (u \approx v) \in R\}$. In that case, we denote $A = P_{\mathcal{V}}(G, R)$ and call the word problem for $\langle G, R\rangle$ over $Eq(\mathcal{V})$ *the word problem for* A. Now the true meaning of the word problem is much more transparent: it looks for the existence of an algorithm which should answer whether two elements of the free algebra $F_{\mathcal{V}}(G)$ (in free semigroups these are literally words) *represent* the same element of A, by identification (in the sense of the above isomorphism) of elements of G with the appropriate generating elements of A.

The *word problem for the variety* $\mathcal{V}$ is said to be *solvable*, if it is so for each finitely presented algebra in $\mathcal{V}$. However, in several cases it turns out that the whole multitude of these word problems can be solved in a uniform way, or, to be more specific, that there exists a universal algorithm which, given a finite presentation $\langle G, R\rangle$ as input, works exactly as the algorithm solving the word problem for $P_{\mathcal{V}}(G, R)$. If so, we say that $\mathcal{V}$ has *uniformly*

solvable word problem.

The diversity just described raised the natural question whether varieties whose word problem is solvable, but *not* uniformly, exist at all. Mekler, Nelson and Shelah [14] constructed such an example by encoding computations of certain Turing machines by equations and utilizing the unsolvability of the Halting Problem. Of course, their example by far did not matched any natural class of algebras. Examples of such kind, obtained as a result of algebraization of different Turing machines, were known ever earlier, see Wells [15], who supplied examples of simpler types, but with enormous number of axioms. The varieties from latter examples met, in fact, the requirements of being *pseudorecursive* (see [15]), and such varieties are, for example, those having solvable word problem, but undecidable equational theory. This undecidability condition is stronger than the uniform unsolvability of the word problem, since the latter can be shown to be equivalent to the undecidability of the implicational theory.

However, in [15] and [16], Wells presented an another pattern for producing pseudorecursive varieties. This is a technique ha called *pleonastic variable rewriting* and it uses, in essence, the well-known *Craig's trick* from model theory. Of course, it is reasonable to require that the varieties in question are given by recursive sets of identities, i.e. that $Eq(\mathcal{V})$ is an axiomatic theory. Even though, the key for undecidability of $Eq(\mathcal{V})$ is still in the list of axioms for equations of $\mathcal{V}$. This direction was followed in examples presented by Crvenković and Delić [3], [4] and Crvenković and Dolinka [5], [6], [7].

In [7], the authors constructed a variety of groupoids with the desired properties. Unfortunately, introduction of associativity for the binary operation in that example would cause difficulties that could be overcome only by adding a unary operation symbol to the language, as it was done in [6]. Nevertheless, in what follows, we develop and idea from Wells [16] in order to obtain the missing pseudorecursive semigroup variety defined in Craig's fashion. In this way, our previous efforts in the topic are unified by the present paper.

For all undefined notions of universal algebra and semigroup theory, we refer to [1] and [10].

2. Preliminaries and the Main Theorem

Given any nonempty set X, we denote by X^+ the free semigroup over X. Throughout the paper, we are going to fix a countably infinite set of symbols $A = \{a_n : n \in \mathbb{N}\}$, as well as its subsets $A_n = \{a_1, \ldots, a_n\}$ for all $n \in \mathbb{N}$. Also, we choose a recursive function $\psi : \mathbb{N} \mapsto \mathbb{N}$ such that the set of its images

$$\Psi = \{\psi(n) : n \in \mathbb{N}\}$$

is *not* recursive (the existence of such function is well-known in the recursion theory).

Finally, consider the following identities:

$$(1) \quad (xy)z \approx x(yz),$$
$$(2) \quad x^3y \approx x^3,$$
$$(3) \quad yx^3 \approx x^3,$$
$$(4) \quad xyxzx \approx x^3,$$
$$(5) \quad x^2yx \approx x^3,$$
$$(6) \quad xyx^2 \approx x^3,$$
$$(7) \quad xy_1^2y_2^2 \ldots y_{\psi(n)}^2x \approx x^{n+3},\ n \in \mathbb{N}.$$

The semigroup variety determined by identities (1)–(6) we denote by $\mathcal{W}$, while its subvariety defined by the sequence of identities (7) will be in the sequel denoted by $\mathcal{V}$. The aim of the present paper is now to prove the following result.

Main Theorem. *The variety $\mathcal{V}$ has a solvable word problem and undecidable equational theory.*

Two remarks should be given at this point concerning the equations above. First, note that (2) and (3) say, in fact, that the cube of each element of any semigroup from $\mathcal{W}$ is the zero element of that semigroup. Since a semigroup can contain at most one zero, it is justified to write the symbol 0 instead of a cube of any variable (or term) in the identities we deal with. Thus (2)–(6) can be rephrased as follows:

$$0 \cdot y \approx y \cdot 0 \approx xyxzx \approx x^2yx \approx xyx^2 \approx 0,$$

while (7) is obviously equivalent to

$$xy_1^2y_2^2 \ldots y_{\psi(n)}^2x \approx 0,\ n \in \mathbb{N}.$$

Nevertheless, we shall not pursue this new notation for (7), despite its convinience. Namely, it takes only a short reflection to see that the set of these slightly modified equational axioms for $\mathcal{V}$ is *not* recursive. But the major feature of Craig's trick is that the original set of identities (1)–(7) *is* recursive, by virtue of the pleonastic use of x and its $(n+3)^{\text{th}}$ power. Of course, it is not hard to construct an algorithm which determines whether a given semigroup identity is of the form

$$xy_1^2y_2^2\dots y_k^2x \approx x^m$$

for some $m > 3$. Now the above equation belongs to the sequence (7) if and only if $k = \psi(m-3)$, which can easily be decided using the Turing machine which computes the recursive function ψ. Hence, the given system of identities is a recursive base for $\mathcal{V}$.

3. The proof of the Main Theorem

Let I_3 be the set of all words from A^+ which contain at least three occurences of some of the letters from A. The set of words $I_{3,n}$ is defined quite analogously within A_n^+.

Lemma 3.1. *I_3 is an ideal of A^+ and $I_{3,n}$ is an ideal of A_n^+ for all $n \in \mathbb{N}$.*

Proof. The assertion of the lemma follows easily from the fact that if u is any word and the word w contains at least three ocurences of a letter a_i, then the same holds for words uw and wu. □

Lemma 3.2. *The Rees quotient A^+/I_3 ($A_n^+/I_{3,n}$) is $\mathcal{W}$-free over A (over A_n, for all $n \in \mathbb{N}$).*

Proof. We present the proof for A^+/I_3, while the case of finitely generated Rees quotients is easily imitated.

First of all, recall that the elements of A^+/I_3 are 0 and all words not belonging to I_3, that is, all words containing each letter from A at most twice. The multiplication in this semigroup is defined such that $uv = 0$ if u and v together contain at least three occurences of the same letter, otherwise uv is just the concaternation of u and v. Now it is easy to verify that identities (2)–(6) are satisfied in A^+/I_3, because every interpretation of the variables yields on their left-hand sides either products in which 0 appears, or words with at least three occurences of some letter from A. In

both cases, the result of an interpretation of both sides of (2)–(6) is 0. Thus A^+/I_3 belongs to $\mathcal{W}$.

If X is a countably infinite set of variables, define

$$\theta_{\mathcal{W}} = \{\langle p, q\rangle \in X^+ \times X^+ : \ \mathcal{W} \models p \approx q\}.$$

Since it is known that $\theta_{\mathcal{W}}$ is a congruence of X^+ and that the $\mathcal{W}$-free semigroup over X is isomorphic to $X^+/\theta_{\mathcal{W}}$, our goal is to prove that the homomorphism $\varphi : X^+/\theta_{\mathcal{W}} \mapsto A^+/I_3$ which extends the mapping φ_0 given by $\varphi_0(x_n/\theta_{\mathcal{W}}) = a_n$ for all $n \in \mathbb{N}$ is, in fact, an isomorphism (of course, such homomorphism exists because of the conclusion of the previous paragraph). This follows almost immediately, because if

$$a_{i_1}a_{i_2}\dots a_{i_k} = a_{j_1}a_{j_2}\dots a_{j_m}$$

holds in A^+/I_3, then either $k = m$ and $i_r = j_r$ for all $1 \leq r \leq k$, or both sides of the above equality contain at least three occurences of some letter. But then in both cases it is a routine to show that the equation

$$x_{i_1}x_{i_2}\dots x_{i_k} \approx x_{j_1}x_{j_2}\dots x_{j_m}$$

is an equational consequence of (1)–(6) and thus it holds in $\mathcal{W}$. In other words,

$$x_{i_1}x_{i_2}\dots x_{i_k}/\theta_{\mathcal{W}} = x_{j_1}x_{j_2}\dots x_{j_m}/\theta_{\mathcal{W}},$$

which completes the proof of the lemma. □

Lemma 3.3. *The variety $\mathcal{V}$ is locally finite.*

Proof. By Lemma 3.2, the semigroup $A_n^+/I_{3,n}$ is $\mathcal{W}$-free over a set of n free generators. It has only finitely many elements – all words over A_n containing each letter at most twice and 0. The lemma now follows immediately. □

Denote by S the Rees quotient A^+/I_3 with the usual identification of its universe with the set of words $(A^+ \setminus I_3) \cup \{0\}$. Define J_ψ to be the set containing 0 and all words from S having subwords of the form $uw_1w_1w_2w_2\dots w_kw_ku$ for some $k \in \Psi$ and $u, w_1, w_2, \dots, w_k \in A^+$. By a similar argument as in Lemma 3.1, the following is obvious.

Lemma 3.4. *J_ψ is an ideal of S.* □

Denote by S_ψ the Rees quotient S/J_ψ defined over $(S \setminus J_\psi) \cup \{0\}$. Now we arrived to the key lemma in our proof.

Lemma 3.5. *$S_\psi \models xy_1^2y_2^2 \dots y_k^2x \approx x^3$ if and only if $k \in \Psi$.*

Proof. ($\Rightarrow$) Suppose $k \notin \Psi$. Then consider the interpretation of variables in S_ψ given by $x \to a_{k+1}$ and $y_i \to a_i$ for $1 \leq i \leq k$. Under this interpretation, x^3 has the value 0, and the value of the term $xy_1^2y_2^2 \dots y_k^2x$ in S is $a_{k+1}a_1a_1a_2a_2 \dots a_ka_ka_{k+1}$. By an easy inspection, one concludes that this word does not belong to J_ψ, because its only subwords with coinciding prefixes and suffixes are the whole word itself and the words a_ia_i for $1 \leq i \leq k$. Hence,

$$S_\psi \not\models xy_1^2y_2^2 \dots y_k^2x \approx x^3.$$

($\Leftarrow$) Let $k \in \Psi$. Any interpretation of the variables $x, y_1, y_2, \dots, y_k$ yields in S a word of the form $uw_1w_1w_2w_2 \dots w_kw_ku$ which is an element of J_ψ. So the identity $xy_1^2y_2^2 \dots y_k^2x \approx 0$ holds in S_ψ, as desired. □

It remains only to emphasize the conclusion of the above lemma.

Lemma 3.6. *$\mathcal{V} \models xy_1^2y_2^2 \dots y_k^2x \approx x^3$ if and only if $k \in \Psi$.*

Proof. First of all, the semigroup S_ψ belongs to $\mathcal{V}$, because it is is a homomorphic image of S (thereby satisfying (1)–(6)) and because it satisfies all identities of the form (7) by the previous lemma. The direct part of this lemma follows from this observation and the direct part of the previous lemma, while the converse implication is immediate, being an obvious consequence of the defining equations (7). □

Proof of the Main Theorem. By Lemma 3.3, $\mathcal{V}$ is locally finite, so all of its finitely presented members are finite algebras, having trivially solvable word problem. On the other hand, suppose $Eq(\mathcal{V})$ is decidable. Then it is quite easy to construct an algorithm which recognizes equations of the form

$$xy_1^2y_2^2 \dots y_k^2x \approx x^3,$$

whose validity in $\mathcal{V}$ can be, by assumption, algorithmically decided. But then, by Lemma 3.6, we have just obtained an algorithm for deciding whether $k \in \Psi$. Contradiction. □

References

[1] Burris, S., Sankappanavar, H.P., A Course in Universal Algebra, Springer-Verlag, 1981.

[2] Crvenković, S., Word problems for varieties of algebras – survey, Filomat (Niš) 9 (3) (1995) (Proc. Int. Conf. on Algebra, Logic & Discrete Math., Niš, 1995, eds. S. Bogdanović, M. Ćirić and Ž. Perović), 427–448.

[3] Crvenković, S., Delić, D., A variety with locally solvable, but globally unsolvable word problem, Algebra Universalis 35 (1996), 420–424.

[4] Crvenković, S., Delić, D., Different levels of word problems for some classes of varieties, Novi Sad J. Math. 26 (1) (1996), 93–102.

[5] Crvenković, S., Dolinka, I., Undecidable varieties with solvable word problems – I, Facta Universitatis (Niš), Ser. Math. Inform. 11 (1996), 1–8.

[6] Crvenković, S., Dolinka, I., Undecidable varieties with solvable word problems – II, Novi Sad J. Math. 26 (2) (1996), 21–30.

[7] Crvenković, S., Dolinka, I., A variety with undecidable equational theory and solvable word problem, Int. J. Algebra Comp., to appear.

[8] Delić, D., The Word Problem for Some Classes of Algebras (in Serbian), M. Sc. Thesis, University of Novi Sad, 1994, 80pp.

[9] Delić, D., From multisorted structures to pseudorecursive varieties, Trans. Amer. Math. Soc., to appear.

[10] Howie, J.M., An Introduction to Semigroup Theory, Academic Press, 1976.

[11] Kharalampovich, O.G., Sapir M.V., Algorithmic problems in varieties, Int. J. Algebra Comp. 5 (4-5) (1995), 379–602.

[12] Ruškuc, N., Semigroup Presentations, Ph. D. Thesis, University of St Andrews, 1995, xiii+256pp.

[13] McNulty, G., A field guide to equational logic, J. Symb. Comp. 14 (1992), 371–397.

[14] Mekler, A., Nelson, E., Shelah, S., A variety with solvable, but not uniformly solvable, word problem, Proc. London Math. Soc. 66 (1993), 225–256.

[15] Wells, B., Pseudorecursive Varieties and Their Implications for Word Problems, Ph.D. Thesis, University of California at Berkeley, 1982, 243pp.

[16] Wells, B., Pseudorecursive varieties of semigroups – I, Int. J. Algebra Comp. 6 (4) (1996), 457–510.

Received by the editors October 27, 1998.