UNDECIDABLE VARIETIES WITH SOLVABLE WORD PROBLEMS – I

Siniša Crvenković and Igor Dolinka

Abstract. The purpose of this paper is to present some new, simpler examples of recursively based undecidable varieties of finite type having solvable word problems.

1. Introduction

Given an algebraic language $\mathcal{L}$ and a set Σ of identities, different decision problems concerning Σ may arise. Generally, one can ask if the sets of all first–order, implicational or equational consequences of Σ are recursive. If so, we say that the elementary, implicational, equational theory based on Σ are decidable.

For example, Abelian groups and Boolean algebras appear to have decidable elementary theory. Obviously, decidability of elementary theory yields decidability of implicational theory, and that decidability of equational theory. Decidable equational theories include commutative semigroups, groups, lattices, etc. On the other hand, modular lattices and relation algebras have undecidable equational theories.

An another kind of decision problems in algebra are *word problems.* A *presentation* is a pair (G, R), where G is a set of new constant symbols, extending $\mathcal{L}$ to $\mathcal{L}_G = \mathcal{L} \cup G$, and R is a set of equations over $\mathcal{L}_G$ in which no variables appear. The presentation is finite, if G and R are both finite. The word problem for (G, R) over Σ is *solvable* iff the set of equational consequences of $\Sigma \cup R$ without variables is recursive, i.e. iff there is an algorithm to decide whether any two words in the language $\mathcal{L}_G$ having no variables are equal.

An algebra $\mathbf{A}$ is *presented* by (G, R), iff $\mathbf{A}$ is isomorphic to the $\mathcal{L}$-reduct of the 0-rank free algebra of the variety, generated by $\Sigma \cup R$, or equivalently iff it is isomorphic to $\mathbf{F}_{\mathcal{V}}(G)/\theta_R$, where $\mathcal{V}$ is the variety generated by Σ, and

$$\theta_R = \{(p, q) | \Sigma \cup R \vdash p \approx q\},$$

is a congruence on $\mathbf{F}_{\mathcal{V}}(G)$. Denote such $\mathbf{A}$ by $\mathbf{A} = \mathcal{P}_{\mathcal{V}}(G, R)$. Now, the word problem for $\mathbf{A}$ is the word problem for (G, R).

By investigating word problems for varieties of algebras, one is concerned with two questions:

1991 *Mathematics Subject Classification:* 0B899, 08A50

(1) is the word problem solvable for each finitely presented algebra $\mathbf{A} = \mathcal{P}_{\mathcal{V}}(G, R)$?

(2) is there a universal algorithm which, given a finite presentation (G, R), solves the word problem for $\mathbf{A} = \mathcal{P}_{\mathcal{V}}(G, R)$?

If the answer to (1) is positive, we say that $\mathcal{V}$ has *solvable local word problem* (the word *local* is usually omited). If (2) has a positive answer, we say that $\mathcal{V}$ has *solvable global* (or *uniformly solvable*) *word problem.*

One can prove that decidability of the implicational theory based on Σ and the global word problem for $\mathcal{V} = mod(\Sigma)$ are equivalent.

In this paper, we are going to present varieties of the types (2,1,0), (2,1), (2,0,0) and (2,0) with solvable word problems having undecidable equational theories (which implies the unsolvability of the global word problems).

Examples of varieties with this property were presented earlier in the papers of Wells [10],[11],[12], Mekler, Nelson and Shelah [8] and Crvenković and Delić [3],[4]. This paper is a contribution to the topic.

2. Example of a variety of the type (2,1,0)

In the sequel, φ will be a primitive recursive function, $X = \{\varphi(k) | k \in \mathbf{N}\}$ nonrecursive recursively enumerable set with $1 \notin X$, where $\mathbf{N} = \{1, 2, \ldots\}$.

Consider the algebraic language $\{\,\cdot\,, f, 0\}$ of the type (2,1,0) and the following identities in this language:

$$
\begin{array}{lrcl}
(1) & (xy)z & \approx & 0, \\
(2) & x(xy) & \approx & 0, \\
(3) & x(y(zu)) & \approx & x(z(yu)), \\
(4) & f(x)y & \approx & 0, \\
(5) & f(f(x)) & \approx & 0, \\
(6) & f(x_1(\ldots(x_n f(y))\ldots)) & \approx & 0,\ n \in \mathbf{N}, \\
(7) & f(x_1(x_2(\ldots(x_{\varphi(n)}x_1)\ldots))) & \approx & f^n(0),\ n \in \mathbf{N}.
\end{array}
$$

The listed set of identities is obviously recursive. Denote the variety defined by (1)–(7) by $\mathcal{V}$. We immediately have $f(0) \approx 0$, $x \cdot 0 \approx 0 \cdot x \approx 0$, as consequeces of the identities given above. Therefore, the constant 0 will be the zero of the algebras in $\mathcal{V}$. In the following, our goal will be to prove:

Theorem 2.1. *$\mathcal{V}$ has undecidable equational theory and solvable word problem.*

3. Word problem for $\mathcal{V}$

Let $\mathbf{F}^n_{\mathcal{V}}$ be the free algebra in $\mathcal{V}$ over the set of generators $\{g_1, \ldots, g_n\}$. We are going to prove that this algebra is finite. Clearly, this follows from the finitness of the algebra $\mathbf{F}^n_{\mathcal{V}_1}$, where $\mathcal{V}_1$ is the variety generated by the identities (1)–(6).

Assuming finitness of $\mathbf{F}^n_{\mathcal{V}}$, one easily deduces the solvability of the word problem for $\mathcal{V}$. Now, it remains to list the words of $\mathbf{F}^n_{\mathcal{V}_1}$.

Lemma 3.1. *Each word in $\mathbf{F}^n_{\mathcal{V}_1}$ is one of the following:*

$$\begin{array}{ll} (i) & 0, g_r, \\ (ii) & g_{k_1}(g_{k_2}(\ldots(g_{k_m}g_r)\ldots)), \\ (iii) & f(w), \\ (iv) & g_{k_1}(\ldots(g_{k_m}f(w))\ldots), \end{array}$$

where in (ii) and (iv) $i \neq j$ implies $k_i \neq k_j$, and in (iii) and (iv) w denotes a word of the type (ii).

Proof. By the induction on the complexity of the word (number of operation symbols) in $\mathbf{F}^n_{\mathcal{V}_1}$, we have:

1. The complexity of t is 0. We have either $t = 0$ or $t = g_r$.

2. The complexity of t is 1. Then t is one of the words

$$f(0), f(g_r).$$

But then the first one is equivalent to 0, while the second is of the type (iii).

3. Let k be the complexity of the word t, while all words of complexity $\leq k-1$ have one of the form (i) – (iv). We have two cases:

(a) $t = t_1t_2$.

Clearly, if $t_1 = uv$ then t is equivalent to 0, by (1). The same situation we have if $t_1 = f(u)$, because of (4). The only possibility remaining is $t_1 = g_l$. Now, the claim is obvious if the word t_2 has the form (i) or (iii). If t_2 is of the form (ii), we have:

$$t = g_l(g_{k_1}(g_{k_2}(\ldots(g_{k_m}g_r)\ldots))).$$

If $l = k_i$ for some $i, 1 \leq i \leq m$, we easily conclude, applying (3), that t is equivalent to

$$g_l(g_l(g_{k_1}(\ldots(g_{k_m}g_r)\ldots))),$$

i.e. to 0, by (2). In the opposite case, t is of the type (ii). Finally, if the word t_2 has the form (iv), the proof is similar.

(b) $t = f(t_1)$.

If t_1 belongs to (i), the case is trivial. If t_1 is of the type (ii), we obtain a word of the type (iii). Finally, if t_1 belongs to one of the classes (iii) or (iv), we have 0 as the result, according to the laws (5) and (6), respectively.

Define:

$$M = \sum_{k=0}^{n} \binom{n}{k} k!.$$

By elementary combinatorial calculation, we have:

$$|\mathbf{F}^n_{\mathcal{V}_1}| \leq 1 + n + 2nM + nM^2. \quad \square$$

4. Undecidability of the equational theory of $\mathcal{V}$

Let $\mathcal{K}_1$ be the variety of the type (2,0), generated by the identities (1)–(3) and $\mathbf{F}_{\mathcal{K}_1}$ its free algebra over the countable set of generators $G = \{g_0, g_1, g_2, \ldots\}$. Define an algebra $\mathbf{A} = (A, \cdot, \phi, 0)$ of the type (2,1,0) in the following way: let $A = F_{\mathcal{K}_1}$, and let us identify 0 with the constant, appearing in $\mathbf{F}_{\mathcal{K}_1}$. The multiplication in $\mathbf{A}$ is the same as in $\mathbf{F}_{\mathcal{K}_1}$. Finally, we put:

$$\phi(w) = \begin{cases} g_0 w & w = g_{k_1}(\ldots(g_{k_m} g_{k_1})\ldots), m \notin X, m \neq 1 \\ 0 & \text{otherwise} \end{cases}$$

Here we assumed $i \neq j \Rightarrow k_i \neq k_j$.

Lemma 4.1. *$\mathbf{A} \in \mathcal{V}$.*

Proof. Identities (1)–(3) are automatically true in $\mathbf{A}$. One easily verifies (4), since $(g_0 w)y = 0$. For (5) we have either $\phi(\phi(w)) = 0$ or $\phi(\phi(w)) = g_0(g_0 w) = 0$; moreover:

$$g_0(w_1(\ldots(w_n(g_0 w))\ldots)) = 0,$$

which is obvious from (2) and (3), so that we have (6). Finally, we see that the only possibility for the expression, standing as the argument of the unary operation simbol in (7), not to be 0 is for the valuation $x_i = g_{k_i}$ (k_i's are all different). But then we have:

$$\phi(g_{k_1}(\ldots(g_{k_m} g_{k_1})\ldots)) = 0,$$

because of $m \in X$, and because $g_{k_1}(\ldots(g_{k_m} g_{k_1})\ldots)$ cannot be reduced to a shorter word, since one easily proves that the polynomial

$$x_1(x_2(\ldots(x_k x_1)\ldots))$$

is esentially k-ary, for all $k \geq 2$ (see, for example, lemma 2.10 in [5]). $\square$

Lemma 4.2.

$$\mathcal{V} \models f(x_1(x_2(\ldots(x_{m-1}(x_m x_1))\ldots))) \approx 0 \textit{ iff } m \in X$$

Proof. Implication ($\Longleftarrow$) is trivial. For the reverse, consider the valuation in the previously described algebra $\mathbf{A}$: $x_i = g_i$, $1 \leq i \leq m$, and suppose $m \notin X$. We have:

$$g_0(g_1(g_2(\ldots(g_m g_1)\ldots))) = 0,$$

which is false in $\mathbf{A}$, i.e. in $\mathbf{F}_{\mathcal{K}_1}$. $\square$

The statement of the previous lemma obviously implies the undecidability of $Eq(\mathcal{V})$ and completes the proof of the theorem 2.1.

5. Variety of the type (2,1)

Since the constant 0 is zero in the variety $\mathcal{V}$, we can easily remove it from the language. Let us replace every occurence of the symbol 0 with, for example, $x(xx)$ in each of the identities (1)–(7). By imitation of the proof, given above, we have a variety of the type (2,1), having the desired properities, defined by the following identities:

$$\begin{aligned}
y(x(xx)) &\approx x(xx).\\
(xy)z &\approx u(uu),\\
x(xy) &\approx z(zz),\\
x(y(zu)) &\approx x(z(yu)),\\
f(x)y &\approx z(zz),\\
f(f(x)) &\approx y(yy),\\
f(x_1(\ldots(x_n f(y))\ldots)) &\approx x(xx),\ n\in\mathbf{N},\\
f(x_1(x_2(\ldots(x_{\varphi(n)}x_1)\ldots))) &\approx f^n(x(xx)),\ n\in\mathbf{N}.
\end{aligned}$$

6. Example of a variety of the type (2,0,0) and its word problem

Let us consider an algebraic language $\{\,\cdot\,,0,c\}$ of the type (2,0,0) and the following identities:

$$x(y_1(\ldots(y_n(xy_{n+1}))\ldots)) \approx 0,\ n\in\mathbf{N}, \tag{8}$$

$$c^2 \approx 0, \tag{9}$$

$$c(x_1(x_2(\ldots(x_{\varphi(n)}x_1)\ldots))) \approx \underbrace{c(c(\ldots(c(cc))\ldots))}_{n}, \tag{10}$$

where on the right-hand side of the last identity we have n occurences of the symbol c. Now, let $\mathcal{V}$ denotes the variety of the type (2,0,0), generated by the identities (1),(2),(8),(9),(10). Of course, this set of identities is also recursive. Here we shall assume $2\notin X$.

Theorem 6.1. *$\mathcal{V}$ has undecidable equational theory and solvable word problem.*

Lemma 6.1. *$\mathcal{V}$ has solvable word problem.*

Proof. Note that, estimating in lemma 3.1 the number of elements of $\mathbf{F}^n_{\mathcal{V}_1}$, we used, in fact, the scheme (8), which is equational consequence of (2) and (3) (the combination of laws (2) and (3) is stronger, since it allows us to put k_i's in strictly increasing order; so the estimation, given in the inequality in the secion 3 – denote it by L_n – can be even improved). Therefore, if $\mathcal{K}_2$ denotes the variety of the type (2,0), defined by (1),(2) and (8), and $\mathbf{F}^n_{\mathcal{V}}, \mathbf{F}^n_{\mathcal{K}_2}$ are the corresponding free algebras over a set of n generators, we have:

$$|\mathbf{F}^n_{\mathcal{V}}| \le |\mathbf{F}^{n+1}_{\mathcal{K}_2}| \le L_{n+1},$$

so the word problem for any finitely presented algebra in $\mathcal{V}$, which is a homomorphic image of $\mathbf{F}^n_{\mathcal{V}}$ for some $n \in \mathbf{N}$, immediately turns out to be solvable. $\square$

7. Undecidability of the equational theory of $\mathcal{V}$

We are going to define an algebra $\mathbf{A} = (A, \cdot, 0, c)$ of the type (2,0,0). Let $A = F_{\mathcal{K}_2} \cup \{c\}$, where $\mathbf{F}_{\mathcal{K}_2}$ denotes the free algebra in $\mathcal{K}_2$ over a countable set of generators. The binary operation and the constant 0 is identical in $\mathbf{F}_{\mathcal{K}_2}$ and $\mathbf{A}$. The only thing left to define is multiplication by the constant c. We put:

$$tc = 0, \text{ for all } t \in A,$$

$$ct = \begin{cases} g_0 t & t = g_{k_1}(\ldots(g_{k_m} g_{k_1})\ldots), m \notin X, m \neq 1 \\ 0 & \text{otherwise} \end{cases}$$

Again, we have $i \neq j \Rightarrow k_i \neq k_j$.

Lemma 7.1. $\mathbf{A} \in \mathcal{V}$.

Proof. It is obvious that the identities (1),(2) and (8) should be verified only for those valuations of the variables, for which some of them has the value c. Also, (9) is immediately clear.

In (1), the straightforward cases are $y = c$ and $z = c$ (recall that in $\mathcal{V}$ $x \cdot 0 \approx 0 \cdot x \approx 0$ holds). If $x = c$ and $cy = 0$, the identity is verified; in the opposite, $cy = g_0 y$, $(g_0 y)z = 0$

In (2), the case $y = c$ is obvious. Put $x = c$. The identity holds if $cy = 0$; in the opposite case we have either $c(cy) = 0$ or $c(cy) = g_0(g_0 y) = 0$.

Now we check (8). The identity is clear for $y_{n+1} = c$. Therefore, we have two cases:

1. $x = c$. We have two possibilities: $cy_{n+1} = 0$ and $cy_{n+1} = g_0 y_{n+1}$. In the second case we obtain either

$$c(y_1(\ldots(y_n(g_0 y_{n+1}))\ldots)) = 0$$

or

$$c(y_1(\ldots(y_n(g_0 y_{n+1}))\ldots)) = g_0(y_1(\ldots(y_n(g_0 y_{n+1}))\ldots)) = 0.$$

2. $y_i = c$, for some $i \leq n$, with $x \neq c$ and $y_{n+1} \neq c$. Again, we have one of the following two cases:

$$c(y_{i+1}(\ldots(y_n(xy_{n+1}))\ldots)) = 0,$$

$$c(y_{i+1}(\ldots(y_n(xy_{n+1}))\ldots)) = g_0(y_{i+1}(\ldots(y_n(xy_{n+1}))\ldots)).$$

In the second case, the identity holds, because the letter x occurs two times in the expression, corresponding to the left-hand side of the identity (8).

Finally, we have (10) to check. But here we have the same case as in lemma 4.1: the only nontrivial valuation is $x_i = g_{k_i}$ with all k_i's different, for which we have:

$$c(g_{k_1}(\ldots(g_{k_m} g_{k_1})\ldots)) = 0. \quad \square$$

Lemma 7.2.

$$\mathcal{V} \models c(x_1(x_2(\ldots(x_m x_1)\ldots))) \approx 0 \textit{ iff } m \in X.$$

Proof. The implication ($\Longleftarrow$) is trivial, since $1, 2 \notin X$ by earlier assumptions. To prove ($\Longrightarrow$), suppose that the identity, given above, holds for some $m \notin X$. But then consider the valuation in $\mathbf{A}$: $x_i = g_i$; it follows that

$$g_0(g_1(\ldots(g_m g_1)\ldots)) = 0.$$

Contradiction. $\square$

The proof of the theorem 6.1 is now complete.

8. Variety of the type (2,0)

Using the same technique, as in section 5, removing the zero-constant symbol, we have a variety of the type (2,0) having solvable word problem and undecidable equational theory, defined by the identities:

$$\begin{aligned}
c^2 x &\approx c^2, \\
x c^2 &\approx c^2, \\
(xy)z &\approx c^2, \\
x(xy) &\approx c^2, \\
x(y_1(\ldots(y_n(x y_{n+1}))\ldots)) &\approx c^2, \; n \in \mathbf{N}, \\
c(x_1(x_2(\ldots(x_{\varphi(n)} x_1)\ldots))) &\approx \underbrace{c(c(\ldots(c(cc))\ldots))}_{n}, \; n \in \mathbf{N}.
\end{aligned}$$

References

[1] S. Burris and H. P. Sankappanavar: *A course in universal algebra*, Springer–Verlag, New York, Berlin, Heidelberg, 1981.

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

[3] S. Crvenković and D. Delić: *A variety with locally solvable, but globally unsolvable word problem*, Algebra Universalis (to appear).

[4] S. Crvenković and D. Delić: *Different levels of word problems for some classes of varieties*, Novi Sad J. Math (to appear).

[5] S. Crvenković and J. Dudek: *Rectangular groupoids*, Czechoslovak Math. J. **35 (110)** (1985), 405–414.

[6] G. Grätzer: *Universal algebra*. Springer–Verlag, New York, Berlin, Heidelberg, 1979.

[7] G. McNulty: *An equational logic sampler*, (manuscript).

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

[9] E. Mendelson: *Introduction to mathematical logic*, Van Nostrand Publishing Co., Princeton, 1964.

[10] B. Wells: *A simple pseudorecursive variety of infinite type*, Abstracts Amer. Math. Soc., 1982.

[11] B. Wells: *Pseudorecursive varieties and their implications for word problems*, Ph.D. thesis, 243 pp., University of California, Berkeley, 1982.

[12] B. Wells: *Pseudorecursive varieties of semigroups – I*, Int. J. Algebra & Comp. (to appear).

University of Novi Sad
Faculty of Science
Institute of Mathematics
Trg Dositeja Obradovića 4
21000 Novi Sad, Yugoslavia