Open access • Journal Article • DOI:10.1007/S10958-009-9397-Z

Complexity of the identity checking problem for finite semigroups — Source link

Jorge Almeida, Mikhail V. Volkov, Svetlana V. Goldberg

Institutions: University of Porto, Ural State University

Published on: 14 Apr 2009 - Journal of Mathematical Sciences (Springer US)

Topics: Bicyclic semigroup, Special classes of semigroups, Semigroup and Identity (philosophy)

Complexity of the Identity Checking Problem for Finite Semigroups

J. Almeida M. V. Volkov S. V. Goldberg*

Abstract

We prove that the identity checking problem in a finite semigroup S is co-NP-complete whenever S has a nonsolvable subgroup or S is the semigroup of all transformations on a 3-element set.

1 Motivation and Main Results

Many basic algorithmic questions in algebra whose decidability is well known and/or obvious give rise to fascinating and sometimes very hard problems if one looks for the *computational complexity* of corresponding algorithms[1]. As an example, we mention the following question VAR-MEMB: *given two finite algebras $\mathcal{A}$ and $\mathcal{B}$ of the same similarity type, does the algebra $\mathcal{A}$ satisfy all identities of the algebra $\mathcal{B}$?* (The notation VAR-MEMB comes from "variety membership" since in the language of variety theory the question is about the membership of the algebra $\mathcal{A}$ to the variety generated by the algebra $\mathcal{B}$.) Clearly, the problem VAR-MEMB is of importance for universal algebra in which equational classification of algebras is known to play a central role. At the same time the problem is of interest for computer science: see, for instance, [3, Section 1] for a discussion of its relationships to formal specification theory. The fact that the problem VAR-MEMB is decidable easily follows from Tarski's HSP-theorem and has been already mentioned in Kalicki's paper [12] more than 50 years ago. However an investigation of the computational complexity of this problem has started only recently and has brought rather unexpected results. First, Bergman and Slutzki [3] gave an upper bound by showing that the problem VAR-MEMB belongs to the class 2-EXPTIME (the class of problems solvable in double exponential time). For some time it appeared that this bound was very rough but then Szekely [30] showed that the problem is NP-hard, and Kozik [17, 18] proved that it is even EXPSPACE-hard. Finally, Kozik [19] has

*The first author acknowledges the support of the Centro de Matemática da Universidade do Porto, financed by FCT through the programmes POCTI and POSI, with Portuguese and European Community structural funds, as well as the support of the FCT project PTDC/MAT/65481/2006. The second and the third authors have been supported by the Russian Foundation for Basic Research, grant 05-01-00540.

[1] In this paper complexity is understood in the sense of the monographs [7, 21]; the reader can find there the definitions of the complexity classes NP, co-NP, EXPSPACE, etc that are mentioned below.

shown that the problem VAR-MEMB is 2-EXPTIME, thus confirming that the bound by Bergman and Slutzki is in fact tight.

The question which we deal with in the present paper is in a certain sense even more fundamental than the question VAR-MEMB. Indeed, when asking VAR-MEMB, one asks whether the algebra $\mathcal{A}$ satisfies each of the (infinitely many) identities holding in the algebra $\mathcal{B}$, while here we concentrate on a single act of satisfaction by asking, for any fixed finite algebra $\mathcal{A}$, if it satisfies a *single* given identity. We shall refer to the question as to *the identity checking problem in the algebra* $\mathcal{A}$ and denote it by CHECK-ID($\mathcal{A}$). More formally, CHECK-ID($\mathcal{A}$) is a combinatorial decision problem whose instance is an arbitrary pair (p, q) of terms in the type of the algebra $\mathcal{A}$. The answer to the instance (p, q) of CHECK-ID($\mathcal{A}$) is "YES" or "NO" depending on whether or not the identity $p \doteq q$ holds in $\mathcal{A}$. Clearly, the question is decidable: if the terms p and q together depend on m variables, one can simply substitute for the variables all possible m-tuples of elements in the algebra $\mathcal{A}$ and then check whether or not all substitutions yield equal values to the terms p and q. We observe, however, that the number of m-tuples subject to the evaluation is $|\mathcal{A}|^m$, whence the time consuming by such a straightforward algorithm in the worst case exponentially depends on the size of the input data. On the other hand, it is obvious that for any finite algebra $\mathcal{A}$ the problem CHECK-ID($\mathcal{A}$) belongs to the complexity class co-NP: if for some pair (p, q) of terms, the identity $p \doteq q$ fails in the algebra $\mathcal{A}$, then a nondeterministic polynomial algorithm can guess an m-tuple of elements in $\mathcal{A}$ witnessing the failure and then confirm the guess by computing the values of the terms p and q at this m-tuple.

Sapir has suggested to investigate the computational complexity of the problem CHECK-ID($\mathcal{A}$) (as well as of the problem VAR-MEMB), see Problems 2.4 and 2.5 in the well known survey [14]. As observed in [14, P. 402], if $\mathcal{A}$ is the 2-element Boolean algebra, then the problem CHECK-ID($\mathcal{A}$) is equivalent to the "negation" of the classic SATISFIABILITY problem. Since the latter is known to be NP-complete (cf. [7, 21]), this implies that checking identities in the 2-element Boolean algebra is co-NP-complete. What can be said about the complexity of CHECK-ID($\mathcal{A}$) provided the underlying finite algebra $\mathcal{A}$ has less expressive power in comparison with Boolean algebras, in particular, if $\mathbf{A}$ is a semigroup, a group, a ring? This question also was explicitly mentioned in [14]. So far a complete answer has been obtained for associative rings: Hunt and Stearns [10] have shown that the problem CHECK-ID($\mathcal{R}$) is decidable in polynomial time whenever the ring $\mathcal{R}$ is nilpotent, while Burris and Lawrence [4] have proved that the problem is co-NP-complete if $\mathcal{R}$ is not nilpotent. Groups with feasible identity checking still are not completely described but recently one has obtained considerable advances towards such a description. Namely, Burris and Lawrence [5] have proved that the problem CHECK-ID($\mathcal{G}$) is decidable in polynomial time whenever the group $\mathcal{G}$ is nilpotent or dihedral; the latter result has been obtained also by Horváth and Szabó [9] who have also established polynomial decidability of identity checking for some other types of metabelian groups. On the other hand, Horváth, Lawrence, Merai and Szabó [8] have discovered that for every nonsolvable finite group $\mathcal{G}$ the problem CHECK-ID($\mathcal{G}$) is co-NP-complete. For finite semigroups beyond the class of groups,

one has found so far only isolated examples in which identity checking is co-NP-complete, cf. [11, 15, 16, 23–25, 27, 28]. We notice that examples exhibited in [16, 24] demonstrate, in particular, that the class of semigroups with polynomial identity checking is not closed with respect to taking subsemigroups.

In Section 2 we establish the following reduction:

Theorem 1. *Let $\mathcal{S}$ be a finite semigroup, $\mathcal{G}$ the direct product of all its maximal subgroups. There exists a polynomial reduction of the problem* Check-Id($\mathcal{G}$) *to the problem* Check-Id($\mathcal{S}$).

This theorem and the aforementioned result from [8] about nonsolvable groups immediately imply

Corollary 1. *If a finite semigroup contains a nonsolvable subgroup, then identity checking in the semigroup is* co-NP*-complete.*

The converse of Corollary 1 is not true as there exist even semigroups with co-NP-complete identity checking and only trivial subgroups [11, 16, 24]. However, combining Corollary 1 with some known results, one can completely classify some important series of semigroups with respect to the complexity of identity checking. For instance, the following corollary gives an exhaustive answer for semigroup of matrices of a finite field.

Corollary 2. *Identity checking in the semigroup of all $n \times n$-matrices over a finite field is* co-NP*-complete for $n > 1$ and is decidable in polynomial time for $n = 1$.*

The same result has been independently obtained by Szábo and Vértesi [29] who used a different technique. Their proof relies on arithmetic properties of orders of finite matrix groups and involves, in particular, classic Zsigmondy's theorem about primitive divisors of the sequence of differences of powers of natural numbers with the same exponents. Our approach only uses the fact that "sufficiently large" semigroups of matrices over a finite field contain nonsolvable subgroups.

Yet another classic series of finite semigroups consists of the semigroups of all transformations on an n-element set, $n = 1, 2, \ldots$. In Section 3 we study the complexity of identity checking for these semigroups. For $n \geq 5$ one can also use Corollary 1, but the case $n \leq 4$ requires a different approach. We have succeeded in analyzing the case $n = 3$ that allows us to obtain the following "almost complete" result:

Theorem 2. *Identity checking in the semigroup of all transformations on an n-element set is* co-NP*-complete for $n = 3$ and $n \geq 5$ and is decidable in polynomial time for $n = 1, 2$.*

The question about the complexity of identity checking in the semigroup of all transformations on a set with 4 elements still remains open. We notice that the reduction from Theorem 1 is applicable to this case as well. Indeed, even though the group of all permutations of a 4-element set is solvable, it does not fall into any known class of groups with polynomial identity checking.

Theorem 1 is a joint result by the authors while Theorem 2 has been obtained by the third author. Some of the results of the present paper have been announced in [1].

2 Proof of Theorem 1

Theorem 1 has arisen as one of the applications of the theory of group generic sets in the free profinite semigroup developed in [2]. In order to make the present paper be understandable without acquaintance with [2], we give here a "finitized" version of the proof in which all profinite objects are substituted by their suitable finite approximations. The reader who knows the definition and some basic properties of the free profinite semigroups can easily "pass to the limit" and recover the natural generality of the constructions presented below.

We introduce some notions of semigroup theory that are necessary for the sequel and recall two elementary facts whose proofs can be found, for instance, in [22, Chapter 3], see there Proposition 1.4 and Corollary 1.7. Let, as usual, $\mathcal{S}^1$ be the least semigroup with the identity element containing the given semigroup $\mathcal{S}$ (that is, $\mathcal{S}^1 = \mathcal{S}$ if $\mathcal{S}$ has an identity element and otherwise $\mathcal{S}^1 = \mathcal{S} \cup \{1\}$ where the new symbol 1 behaves as a multiplicative identity element). On each semigroup $\mathcal{S}$ one can define 3 natural preorders $\leq_{\mathscr{L}}$, $\leq_{\mathscr{R}}$ and $\leq_{\mathscr{J}}$ which are the relations of left, right and bilateral divisibility respectively:

$$a \leq_{\mathscr{L}} b \Leftrightarrow a = sb \text{ for some } s \in \mathcal{S}^1;$$
$$a \leq_{\mathscr{R}} b \Leftrightarrow a = bs \text{ for some } s \in \mathcal{S}^1;$$
$$a \leq_{\mathscr{J}} b \Leftrightarrow a = sbt \text{ for some } s, t \in \mathcal{S}^1.$$

We denote by $\mathscr{L}$, $\mathscr{R}$ and $\mathscr{J}$ the equivalence relations corresponding to the preorders $\leq_{\mathscr{L}}$, $\leq_{\mathscr{R}}$ and $\leq_{\mathscr{J}}$ (that is, $a \mathscr{L} b$ if and only if $a \leq_{\mathscr{L}} b \leq_{\mathscr{L}} a$ etc). In addition, let $\mathscr{H} = \mathscr{L} \cap \mathscr{R}$.

Proposition 2.1. *Let $\mathcal{S}$ be a finite semigroup, $s, t \in \mathcal{S}$.*
1) If $s \leq_{\mathscr{L}} t$ and $s \mathscr{J} t$, then $s \mathscr{L} t$.
2) If $s \leq_{\mathscr{J}} s^2$, then the $\mathscr{H}$-class of the element s is a maximal subgroup of the semigroup $\mathcal{S}$.

Let $\Sigma = \{x_1, \ldots, x_m\}$ be a finite aplphabet, Σ^+ the free semigroup over Σ, that is the set of words composed from the letters $x_1, \ldots, x_m$ using concatenation. We say that a word $u \in \Sigma^+$ is

- a *factor* of a word $v \in \Sigma^+$ if $u \geq_{\mathscr{J}} v$;
- a *suffix* of a word $v \in \Sigma^+$ if $u \geq_{\mathscr{L}} v$;
- a *prefix* of a word $v \in \Sigma^+$ if $u \geq_{\mathscr{R}} v$.

If every letter $x_1, \ldots, x_m \in \Sigma$ appears as a factor in a word $w \in \Sigma^+$, we say that the word w has *full content*.

Every endomorphism φ of the semigroup Σ^+ is uniquely determined by m words $w_i = x_i\varphi$, $i = 1, \ldots, m$ which we refer to as the *components* of the

endomorphism. It is convenient to identify the endomorphism φ and the vector $[w_1, \dots, w_m]$ of its components. According to this convention an expression of the form $[w_1, \dots, w_m]^k$ denotes the k-th power (iteration) of the endomorphism $[w_1, \dots, w_m]$.

Lemma 2.2. *Suppose that the words $w_1, \dots, w_m$ over $\Sigma = \{x_1, \dots, x_m\}$ satisfy the following conditions:*

(a) *each of the words $w_1, \dots, w_m$ has full content;*

(b) *each of the words $w_1, \dots, w_m$ starts and ends with the letter x_1;*

(c) *the word x_1^2 appears as a factor in the word w_1.*

Let $\mathcal{S}$ be an arbitrary finite semigroup and ℓ the maximum length of an $\leq_{\mathscr{J}}$-chain without $\mathscr{J}$-equivalent elements in $\mathcal{S}$. Then for every homomorphism $\Sigma^+ \to \mathcal{S}$ there is a subgroup $\mathcal{H}$ in $\mathcal{S}$ such that the values of all components of the endomorphism $[w_1, \dots, w_m]^{2\ell}$ under this homomorphism belong to $\mathcal{H}$.

Proof. We fix a homomorphism $\Sigma^+ \to \mathcal{S}$ and denote the image of a word $w \in \Sigma^+$ under this homomorphism by $\overline{w}$. For each $k = 1, 2, \dots$, let

$$[w_1, \dots, w_m]^k = [w_{1,k}, \dots, w_{m,k}];$$

thus, the word $w_{i,k}$ is the i-th component of the k-th iteration of the endomorphism $\varphi = [w_1, \dots, w_m]$. We notice that

$$\begin{aligned} w_{i,k+1} = x_i\varphi^{k+1} = (x_i\varphi)\varphi^k = w_i(x_1, \dots, x_m)\varphi^k = \\ = w_i(x_1\varphi^k, \dots, x_m\varphi^k) = w_i(w_{1,k}, \dots, w_{m,k}). \quad (1) \end{aligned}$$

In view of the condition (a), the equalities (1) imply that the word $w_{i,k}$ is a factor of the word $w_{j,k+1}$ for all $k = 1, 2, \dots$ and for all $i, j = 1, \dots, m$. Since the divisibility relations are preserved under homomorphisms, the following inequalities hold in the semigroup $\mathcal{S}$:

$$\overline{w}_{1,1} \geq_{\mathscr{J}} \overline{w}_{1,2} \geq_{\mathscr{J}} \cdots \geq_{\mathscr{J}} \overline{w}_{1,2\ell+1}.$$

Due to the choice of the number ℓ, we deduce (using the pigeonhole principle), that this sequence contains 3 adjacent $\mathscr{J}$-equivalent elements. Let $k < 2\ell$ be such that $\overline{w}_{1,k} \mathscr{J} \overline{w}_{1,k+1} \mathscr{J} \overline{w}_{1,k+2}$. By the condition (c) and the equalities (1), the word $w_{1,k}^2$ appears as a factor in the word $w_{1,k+1}$. Hence in the semigroup $\mathcal{S}$ we have $\overline{w}_{1,k}^2 \geq_{\mathscr{J}} \overline{w}_{1,k+1} \mathscr{J} \overline{w}_{1,k}$. Using Proposition 2.1.2, we conclude that the $\mathscr{H}$-class $\mathcal{H}$ of the element $\overline{w}_{1,k}$ is a maximal subgroup of the semigroup $\mathcal{S}$. Furthermore, in view of the condition (b) and the equalities (1), the word $w_{1,k}$ appears as a prefix as well as a suffix of each of the words $w_{i,k+1}$, which, in turn, appear as factors in the word $w_{1,k+2}$ by (a). Hence all elements $\overline{w}_{i,k+1}$ lie in the same $\mathscr{J}$-class of the semigroup $\mathcal{S}$. Moreover, by Proposition 2.1.1 and its dual all these elements belong to the same $\mathscr{L}$-class and the same $\mathscr{R}$-class as the element $\overline{w}_{1,k}$. Thus, all elements $\overline{w}_{i,k+1}$ lie in the subgroup $\mathcal{H}$, whence the subgroup contains all elements $\overline{w}_{i,n}$ for all $n > k$. We see that the subgroup $\mathcal{H}$ indeed contains the values of all words $w_{1,2\ell}, \dots, w_{m,2\ell}$ under the homomorphism that we consider. $\square$

The free semigroup Σ^+ can be considered as a subsemigroup in the free group $\mathcal{FG}(\Sigma)$ over Σ.

Lemma 2.3. *Suppose that the words $w_1, \ldots, w_m \in \Sigma^+$ generate the free group $\mathcal{FG}(\Sigma)$. Then, for every finite group $\mathcal{H}$ and every m elements $h_1, \ldots, h_m \in \mathcal{H}$ there exists a homomorphism $\zeta : \Sigma^+ \to \mathcal{H}$ such that $w_i\zeta = h_i$ for all $i = 1, \ldots, m$.*

Proof. Since the words $w_1, \ldots, w_m$ generate $\mathcal{FG}(\Sigma)$, the extension ψ of the endomorphism $[w_1, \ldots, w_m]$ to $\mathcal{FG}(\Sigma)$ is surjective. It is well known (cf. [20, Proposition I.3.5]) that every surjective endomorphism of a finitely generated free group is an automorphism. Let $g_i = x_i\psi^{-1}$, $i = 1, \ldots, m$. Then

$$w_i(g_1, \ldots, g_m) = w_i(x_1\psi^{-1}, \ldots, x_m\psi^{-1}) = \\ = w_i(x_1, \ldots, x_m)\psi^{-1} = x_i\psi\psi^{-1} = x_i \quad (2)$$

for all $i = 1, \ldots, m$. Since the equalities (2) hold in the free m-generated group, they remain valid under any interpretation of the letters $x_1, \ldots, x_m$ by arbitrary m elements of an arbitrary group. Now we define a homomorphism $\zeta : \Sigma^+ \to \mathcal{H}$ letting

$$x_i\zeta = g_i(h_1, \ldots, h_m), \quad i = 1, \ldots, m.$$

Then in view of (2) we have

$$w_i(x_1, \ldots, x_m)\zeta = w_i(x_1\zeta, \ldots, x_m\zeta) = \\ = w_i\big(g_1(h_1, \ldots, h_m), \ldots, g_m(h_1, \ldots, h_m)\big) = h_i$$

for all $i = 1, \ldots, m$. □

For each positive integer m we consider the following collection of m words:

$$\begin{aligned} w_1 &= x_1^2 x_2 \cdots x_m x_1, \\ w_2 &= x_1 x_2^2 \cdots x_m x_1, \\ &\cdots\cdots\cdots\cdots \\ w_{m-1} &= x_1 x_2 \cdots x_{m-1}^2 x_m x_1, \\ w_m &= x_1 x_2 \cdots x_m x_1. \end{aligned} \quad (3)$$

Clearly, the words (3) satisfy the conditions (a)–(c) of Lemma 2.2. It is easy to check that they also satisfy the condition of Lemma 2.3. Indeed, the following equalities hold in the free group $\mathcal{FG}(\Sigma)$:

$$\begin{aligned} x_1 &= w_1 w_m^{-1}, \\ x_2 &= x_1^{-1} w_2 w_m^{-1} x_1, \\ x_3 &= (x_1 x_2)^{-1} w_3 w_m^{-1} x_1 x_2, \\ &\cdots\cdots\cdots\cdots \\ x_{m-1} &= (x_1 x_2 \cdots x_{m-2})^{-1} w_{m-1} w_m^{-1} x_1 x_2 \cdots x_{m-2}, \\ x_m &= (x_1 x_2 \cdots x_{m-1})^{-1} w_m x_1^{-1}, \end{aligned}$$

and this proves that the words (3) generate $\mathcal{FG}(\Sigma)$. We are now ready to prove Theorem 1.

Proof of Theorem 1. Let $\mathcal{S}$ be a finite semigroup, $\mathcal{G}$ the direct product of all its maximal subgroups. We aim to construct a polynomial time reduction from the problem Check-Id($\mathcal{G}$) to the problem Check-Id($\mathcal{S}$). Consider an arbitrary instance of Check-Id($\mathcal{G}$), i. e. an arbitrary pair of words $u, v \in \Sigma^+$ where $\Sigma = \{x_1, \ldots, x_m\}$ is an appropriate alphabet. We take the collection (3) corresponding to m and, as in the proof of Lemma 2.2, let

$$[w_1, \ldots, w_m]^k = [w_{1,k}, \ldots, w_{m,k}]$$

for every $k = 1, 2, \ldots$. Denote by ℓ the maximum length of a $\leq_{\mathscr{J}}$-chain without $\mathscr{J}$-equivalent elements in $\mathcal{S}$. We want to show that the identity

$$u(x_1, \ldots, x_m) \doteq v(x_1, \ldots, x_m). \tag{4}$$

holds in the group $\mathcal{G}$ if and only if the identity

$$u(w_{1,2\ell}, \ldots, w_{m,2\ell}) \doteq v(w_{1,2\ell}, \ldots, w_{m,2\ell}) \tag{5}$$

holds in the semigroup $\mathcal{S}$.

First suppose that the identity (4) holds in $\mathcal{G}$. Consider an arbitrary homomorphism $\zeta : \Sigma^+ \to \mathcal{S}$. As was noticed above, the words (3) satisfy the conditions of Lemma 2.2, whence the images of the words $w_{1,2\ell}, \ldots, w_{m,2\ell}$ under the homomorphism lie in a subgroup $\mathcal{H}$ of the semigroup $\mathcal{S}$. Since $\mathcal{H}$ is a subgroup of $\mathcal{G}$, the identity (4) holds in $\mathcal{H}$, and hence, substituting for $x_1, \ldots, x_m$ the images of the words $w_{1,2\ell}, \ldots, w_{m,2\ell}$ yield the equality

$$u(w_{1,2\ell}\zeta, \ldots, w_{m,2\ell}\zeta) = v(w_{1,2\ell}\zeta, \ldots, w_{m,2\ell}\zeta)$$

in $\mathcal{H}$. However,

$$\begin{aligned} u(w_{1,2\ell}\zeta, \ldots, w_{m,2\ell}\zeta) &= u(w_{1,2\ell}, \ldots, w_{m,2\ell})\zeta, \\ v(w_{1,2\ell}\zeta, \ldots, w_{m,2\ell}\zeta) &= v(w_{1,2\ell}, \ldots, w_{m,2\ell})\zeta; \end{aligned}$$

this means that the expressions $u(w_{1,2\ell}\zeta, \ldots, w_{m,2\ell}\zeta)$ and $v(w_{1,2\ell}\zeta, \ldots, w_{m,2\ell}\zeta)$ can be thought of as the images of the words $u(w_{1,2\ell}, \ldots, w_{m,2\ell})$ and respectively $v(w_{1,2\ell}, \ldots, w_{m,2\ell})$ under the homomorphism ζ. Since these images coincide under an arbitrary homomorphism $\zeta : \Sigma^+ \to \mathcal{S}$, the identity (5) holds in the semigroup $\mathcal{S}$.

Now suppose that the identity (5) holds in the semigroup $\mathcal{S}$. We want to show that the identity (4) holds in an arbitrary subgroup $\mathcal{H}$ of $\mathcal{S}$. Since the words (3) generate the free group $\mathcal{FG}(\Sigma)$, the extension ψ of the endomorphism $[w_1, \ldots, w_m]$ to $\mathcal{FG}(\Sigma)$ is surjective. Then any power of ψ, in particular, $\psi^{2\ell}$ is surjective. Hence the components of the endomorphism $[w_1, \ldots, w_m]^{2\ell}$, i. e. the words $w_{1,2\ell}, \ldots, w_{m,2\ell}$ also generate the free group $\mathcal{FG}(\Sigma)$. Therefore Lemma 2.3 applies to the words $w_{1,2\ell}, \ldots, w_{m,2\ell}$ and for every m-tuple of elements $h_1, \ldots, h_m \in \mathcal{H}$ there exists a homomorphism $\zeta : \Sigma^+ \to \mathcal{H}$ such that $w_{i,2\ell}\zeta = h_i$ for all $i = 1, \ldots, m$. Since the identity (5) holds in the semigroup $\mathcal{S}$, it holds also in the subgroup $\mathcal{H}$. Hence we have the equalities

$$u(h_1, \ldots, h_m) = u(w_{1,2\ell}\zeta, \ldots, w_{m,2\ell}\zeta) = v(w_{1,2\ell}\zeta, \ldots, w_{m,2\ell}\zeta) = v(h_1, \ldots, h_m),$$

which show that the words $u(x_1, \ldots, x_m)$ and $v(x_1, \ldots, x_m)$ have the same value under any interpretation of their letters by elements of $\mathcal{H}$. This means that the identity (4) holds in $\mathcal{H}$. Identities are inherited by direct products whence (4) holds in $\mathcal{G}$ as well.

Now we observe that the length of each of the words (3) does not exceed $m+2$, and therefore, the length of each of the words $w_{1,2\ell}, \ldots, w_{m,2\ell}$ does not exceed $(m+2)^{2\ell}$. Here the parameter ℓ is defined by the semigroup $\mathcal{S}$ only and does not depend on the size of the instance (u, v) (i. e. the sum of the lengths of the words u and v), and the parameter m does not exceed this size. Since the length of the word $u(w_{1,2\ell}, \ldots, w_{m,2\ell})$ (respectively, $v(w_{1,2\ell}, \ldots, w_{m,2\ell})$) does not exceed the product of the maximum length of the words $w_{i,2\ell}$ and the length of the word u (respectively, v), we see that checking the identity (4) in the group $\mathcal{G}$ reduces to checking that the semigroup $\mathcal{S}$ satisfies an identity whose size is bounded by a polynomial of the size of (4). Theorem 1 is thus proved. □

As was mentioned in Section 1, **Corollary 1** is an immediate consequence of Theorem 1 combined with the result of [8] that identity checking in each finite nonsolvable group is co-NP-complete.

Proof of Corollary 2. By the classic Jordan-Dickson theorem (see, e. g., [13, Section 4.2]) the group of all invertible $n \times n$-matrices over a finite field $\mathcal{K}$ is nonsolvable with two exceptions: $n = 2$, $|\mathcal{K}| = 2$ and $n = 2$, $|\mathcal{K}| = 3$. By Corollary 1 we conclude that identity checking in the semigroup of all $n \times n$-matrices over $\mathcal{K}$ is co-NP-complete whenever $n \geq 3$ or $|\mathcal{K}| \geq 4$. The two aforementioned exceptional cases were analyzed in respectively [27] and [28]. □

3 Proof of Theorem 2

We denote by $\mathcal{T}_n$ the semigroup of all transformations on an n-element set. We apply transformations on the right whence the product $\alpha\beta$ of two transformations $\alpha, \beta \in \mathcal{T}_n$ is the result of applying first α and then β. We notice that this convention does not affect the complexity of identity checking – the semigroup $\overleftarrow{\mathcal{T}_n}$ of all "left" transformations on an n-element set is anti-isomorphic to $\mathcal{T}_n$ and satisfies an identity if and only if $\mathcal{T}_n$ satisfies the mirror image of the identity.

Already Galois knew that for $n \geq 5$ the group $\mathcal{S}_n$ of all permutations on an n-element set is nonsolvable, and therefore, as was mentioned in Section 1, for $n \geq 5$ Theorem 2 immediately follows from Corollary 1. The semigroup $\mathcal{T}_1$ contains only one element whence identity checking in $\mathcal{T}_1$ is trivial: every identity holds in $\mathcal{T}_1$. The semigroup $\mathcal{T}_2$ has 4 elements and one can apply Klíma's result [16, Proposition 4] which claims that the problem Check-Id($\mathcal{S}$) is decidable in polynomial time for every monoid $\mathcal{S}$ with at most 5 elements. For the reader's convenience, taking into account that the paper [16] still remains unpublished, we describe here a polynomial algorithm for checking identities in $\mathcal{T}_2$ that depend on neither Klíma's general result nor results from Tesson's thesis [31] which Klíma has used.

Let Σ be an alphabet. The *multiplicity* of a letter $x \in \Sigma$ in a word $w \in \Sigma^+$ is the number of different occurrences of x as a factor of w, i. e. the number

of different factorizations of the form $w = uxv$, where u, v are possibly empty words. We denote by $\mathrm{suff}_x(w)$ the maximum suffix of the word w containing no occurrence of the letter x. Observe that $\mathrm{suff}_x(w) = w$ whenever x does not occur in w.

Proposition 3.1. *An identity $u \doteq v$ holds in the semigroup $\mathcal{T}_2$ if and only if for every two letters x and y the multiplicities of y in the words $\mathrm{suff}_x(u)$ and $\mathrm{suff}_x(v)$ have the same parity and are simultaneously equal to 0 or different from 0.*

Proof. **Necessity.** We assume that transformations from $\mathcal{T}_2$ act on the set $\{1, 2\}$ and denote by $\binom{12}{ij}$ the transformation sending 1 to i and 2 to j, where $i, j \in \{1, 2\}$. The identity permutation $\binom{12}{12}$ is denoted by ε.

First consider the case when the letter x does not occur in the words u and v. Suppose that the multiplicities of the letter y in the words $\mathrm{suff}_x(u) = u$ and $\mathrm{suff}_x(v) = v$ have different parities. Then under the substitution $y \mapsto \binom{12}{21}$, $z \mapsto \varepsilon$ for all $z \neq y$, the value of the word with the odd multiplicity of y is equal to $\binom{12}{21}$ while the value of the word with even multiplicity of y is ε. Thus, such an identity $u \doteq v$ fails in $\mathcal{T}_2$. Now suppose that the multiplicity of the letter y in one of the words under consideration, u, say, is different from 0 while the other word contains no occurrence of y. Then under the substitution $y \mapsto \binom{12}{11}$, $z \mapsto \varepsilon$ for all $z \neq y$, the value of the word u is equal to $\binom{12}{11}$ while the value of the word v is ε. Thus, in this case the identity $u \doteq v$ fails in $\mathcal{T}_2$ as well.

Now assume that x occurs in one of the words u or v. As shown in the previous paragraph, x appears also in the other word. Suppose that the multiplicities of the letter y in the words $\mathrm{suff}_x(u)$ and $\mathrm{suff}_x(v)$ have different parities. Consider the substitution $x \mapsto \binom{12}{11}$, $y \mapsto \binom{12}{21}$, $z \mapsto \varepsilon$ for all $z \neq y$. It is easy to see that under this substitution the value of the word with the odd multiplicity of y in the maximum suffix containing no occurrence of x is equal to $\binom{12}{22}$ while the value of the other word is equal to $\binom{12}{11}$. Again, we see that the identity $u \doteq v$ fails in $\mathcal{T}_2$. Finally, suppose that the letter y occurs only in one of the words $\mathrm{suff}_x(u)$ or $\mathrm{suff}_x(v)$, say, in the first one. Consider the substitution $x \mapsto \binom{12}{11}$, $y \mapsto \binom{12}{22}$, $z \mapsto \varepsilon$ for all $z \neq y$. The value of the word u under this evaluation is equal to $\binom{12}{22}$ while the value of the word v is $\binom{12}{11}$. Hence, in this case the identity $u \doteq v$ also fails in $\mathcal{T}_2$.

Sufficiency. Let Σ be the set of all letters that occur in either u or v. Consider an arbitrary homomorphism $\zeta : \Sigma^+ \to \mathcal{T}_2$. If the image of ζ is contained in the group $\mathcal{S}_2$, then the condition that the multiplicities of every letter in the words u and v have same parity ensures the equality $u\zeta = v\zeta$. Otherwise, let x be the "rightmost" letter in u such that $x\zeta \notin \mathcal{S}_2$, that is $y\zeta \in \mathcal{S}_2$ for any letter y which occurs $\mathrm{suff}_x(u)$. Then the equality $u\zeta = v\zeta$ follows from the condition that $\mathrm{suff}_x(u)$ and $\mathrm{suff}_x(v)$ contain the same letters and with the multiplicities of the same parity. □

It is clear that the condition of Proposition 3.1 can be verified in polynomial (in fact, even linear) time of the sum of the length of the words u and v. We notice that the necessity of the condition was basically shown by Edmunds [6,

Lemma 4.5]. (The monoid M_{31} considered by Edmunds in this lemma is nothing but the semigroup $\overleftarrow{\mathcal{T}_2}$ with 0 adjoined; this monoid and $\overleftarrow{\mathcal{T}_2}$ satisfy the same identities.) An earlier characterization of the identities of the semigroup $\overleftarrow{\mathcal{T}_2}$ found by Simel'gor [26] uses a recursion over the subsets of the alphabet, and therefore, does not immediately lead to a polynomial algorithm for the problem CHECK-ID($\overleftarrow{\mathcal{T}_2}$).

The rest of the section deals with the case $n = 3$. We notice that for the semigroup $\mathcal{T}_3$ one cannot use the reduction of Theorem 1 because all subgroups in $\mathcal{T}_3$ are isomorphically embedded into $\mathcal{S}_3$ and the latter subgroup is dihedral whence the problem CHECK-ID($\mathcal{S}_3$) is decidable in polynomial time [5]. Nevertheless, we shall prove that the problem CHECK-ID($\mathcal{T}_3$) is co-NP-complete; the proof relies on techniques suggested in [27].

We denote by $\mathcal{T}_3(m)$ the set of all transformations from $\mathcal{T}_3$ whose image consists of m elements. This defines a partition of the semigroup $\mathcal{T}_3$ into the sets $\mathcal{T}_3(3) = \mathcal{S}_3$, $\mathcal{T}_3(2)$ and $\mathcal{T}_3(1)$. We assume that all transformations under consideration act on the set $\{1, 2, 3\}$, and assign to each transformation $\varphi \in \mathcal{T}_3(2)$ its kernel $\ker\varphi$, i. e. the partition of the set $\{1, 2, 3\}$ into 2 classes such that $i, j \in \{1, 2, 3\}$ belong to the same class if and only if $i\varphi = j\varphi$, and its image $\operatorname{Im}\varphi$, i. e. the 2-element subset $\{1\varphi, 2\varphi, 3\varphi\}$ of the set $\{1, 2, 3\}$. If ξ is a partition of the set $\{1, 2, 3\}$ into 2 classes and A is a 2-element subset of $\{1, 2, 3\}$, we write $A \in \xi$ whenever A coincides with one of the ξ-classes. The following fact is quite obvious:

Lemma 3.2. *If $\varphi, \psi \in \mathcal{T}_3(2)$, then $\varphi\psi \in \mathcal{T}_3(1)$ if and only if $\operatorname{Im}\varphi \in \ker\psi$.*

We notice that permutations $\pi \in \mathcal{S}_3$ act in a natural way on the set of all 2-element subsets of $\{1, 2, 3\}$ as well as on the set of all partitions of $\{1, 2, 3\}$ into two classes. The following observation is obvious:

Lemma 3.3. *If $\varphi \in \mathcal{T}_3(2)$, $\pi \in \mathcal{S}_3$, then $\pi\varphi, \varphi\pi \in \mathcal{T}_3(2)$ and we have*

- $\ker(\pi\varphi) = (\ker\varphi)\,\pi^{-1}$, $\operatorname{Im}(\pi\varphi) = \operatorname{Im}\varphi$;
- $\ker(\varphi\pi) = \ker\varphi$, $\operatorname{Im}(\varphi\pi) = (\operatorname{Im}\varphi)\,\pi$.

Using a straightforward induction, one deduces from Lemmas 3.2 and 3.3 the following result:

Lemma 3.4. *Let $\varphi_1, \ldots, \varphi_n \in \mathcal{T}_3(2)$, $\pi_1, \ldots, \pi_{n+1} \in \mathcal{S}_3$. The product $\psi = \pi_1\varphi_1\pi_2\varphi_2\cdots\pi_n\varphi_n\pi_{n+1}$ belongs to $\mathcal{T}_3(1)$ if and only if there is an index $k \in \{1, \ldots, n-1\}$ such that $(\operatorname{Im}\varphi_k)\,\pi_{k+1} \in \ker\varphi_{k+1}$. Moreover, if $\psi \in \mathcal{T}_3(2)$, then $\ker\psi = (\ker\varphi_1)\,\pi_1^{-1}$, $\operatorname{Im}\psi = (\operatorname{Im}\varphi_n)\,\pi_{n+1}$.*

The next corollary of Lemmas 3.2 and 3.3 also will be useful in the sequel:

Lemma 3.5. *For each cyclic permutation $\pi \in \{(123), (132)\}$ and each transformation $\varphi \in \mathcal{T}_3(2)$, the product $\varphi\pi\varphi\pi^2\varphi^2$ belongs to $\mathcal{T}_3(1)$.*

Proof. Since $\operatorname{Im}\varphi$, $\operatorname{Im}(\varphi\pi)$ and $\operatorname{Im}(\varphi\pi^2)$ are different 2-element sets, one of them should constitute a class of the partition $\ker\varphi$. □

We register also the following elementary observation:

Lemma 3.6. *Every transformation $\varphi \in \mathcal{T}_3(2)$ verifies the equality $\varphi^2 = \varphi^4$, and if $\varphi^2 \in \mathcal{T}_3(2)$, then even the equality $\varphi = \varphi^3$ holds true.*

Proof. First assume that $\varphi^2 \in \mathcal{T}_3(2)$. Then $\operatorname{Im}\varphi = \operatorname{Im}(\varphi^2)$, i. e. φ acts on the 2-element set $\operatorname{Im}\varphi$ as a permutation. Thus, φ^2 acts on $\operatorname{Im}\varphi$ as the identity permutation, whence $\varphi = \varphi^3$.

If $\varphi^2 \in \mathcal{T}_3(1)$, then $\varphi^2 = \varphi^4$ because every constant transformation is idempotent. □

Proposition 3.7. *The problem* Check-Id($\mathcal{T}_3$) *is* co-NP*-complete.*

Proof. Consider the problem 6-Coloring whose instances are arbitrary simple graphs Γ (that is, graphs without loops and multiple edges). The answer to an instance Γ is "YES" if and only if the vertices of the graph Γ can be colored with 6 colors such that every two adjacent vertices have different colors. It is easy to see that the problem 6-Coloring belongs to the complexity class NP and that the classic NP-complete problem 3-Coloring polynomially reduces to 6-Coloring via the well known construction of graph composition, see, e. g., [7, Section 6.2]). Therefore the problem 6-Coloring also is NP-complete.

Now let $\Gamma = (V, E)$ be an arbitrary simple graph without isolated vertices. Given Γ, we shall construct an identity $p \doteq q$, whose size (that is, the sum of lengths of the words p and q) is bounded by a polynomial of the number of vertices in Γ, and shall show that the graph Γ has a 6-coloring if and only is the identity $p \doteq q$ fails in the semigroup $\mathcal{T}_3$. Since adding or removing isolated vertices to a graph does not affect its chromatic number, we thus shall get a polynomial reduction of the problem 6-Coloring to the negation of the problem Check-Id($\mathcal{T}_3$). This will imply that the problem Check-Id($\mathcal{T}_3$) is co-NP-complete.

We construct the desired identity over the alphabet $\Sigma = V \cup E \cup \{x\}$, where x is a "new" letter that occurs in neither V nor E. To each edge $e_i \in E$ we assign the word $w_i = e_i v_j v_k^5 e_i^5 v_k v_j^5$ where the vertices $v_j, v_k \in V$ are the two ends of the edge e_i. We order the edges and the pairs of different edges of the graph Γ and consider the products

$$P = \prod_{e_i \in E} (x w_i^4)^6, \quad Q = \prod_{e_i \in E} (x w_i^6)^6, \quad H = \prod_{e_i, e_j \in E} (w_i w_j w_i w_j^2 w_i^2)^6,$$

in which factors corresponding to edges or pairs of edges are listed in the chosen order. Let $p = PP^2PxH$, $q = PQ^2PxH$. Then $p \doteq q$ is the desired identity.

It is easy to calculate that the sum of the lengths of the words p and q is bounded by a quadratic polynomial of the number of edges of the graph Γ, and thus, by a polynomial of fourth degree of the number of vertices in Γ. It remains to verify that the identity $p \doteq q$ fails in the semigroup $\mathcal{T}_3$ if and only if the graph Γ admits a 6-coloring.

First assume that the vertices of Γ can be colored with 6 colors. Then there exists a mapping $\zeta : V \to \mathcal{S}_3$ such that $v_j\zeta \neq v_k\zeta$ for any two adjacent vertices

$v_j, v_k \in V$. Taking into account that the group $\mathcal{S}_3$ satisfies the identity $x^6 \doteq 1$ and extending ζ to the set V^+ of all words over V, we can rewrite the previous inequality as $\left(v_j v_k^5\right)\zeta \neq \varepsilon$, where ε stands for the identity permutation $\binom{123}{123}$. Since the center of the group $\mathcal{S}_3$ is trivial, there exists a permutation $\pi_{jk} \in \mathcal{S}_3$ that does not commute with the permutation $\left(v_j v_k^5\right)\zeta$. Now we extend the mapping ζ to the set $(V \cup E)^+$ by letting $e_i\zeta = \pi_{jk}$ where the indices j and k are determined by the condition that the vertices v_j and v_k are the ends of the edge e_i. Thus, $\left(e_i v_j v_k^5\right)\zeta \neq \left(v_j v_k^5 e_j\right)\zeta$, whence, using the identity $x^6 \doteq 1$ once again, we conclude that $w_i\zeta = \left(e_i v_j v_k^5 e_i^5 v_k v_j^5\right)\zeta \neq \varepsilon$. It is clear that $w_i\zeta$ is an even permutation, that is, $w_i\zeta$ is one of the cycles (123) or (132). In particular, $w_i^4\zeta = w_i\zeta$.

Finally, we extend ζ to a homomorphism $\Sigma^+ \to \mathcal{T}_3$ by putting $x\zeta = \varphi$, where $\varphi = \binom{123}{233}$. We observe that $\operatorname{Im}\varphi = \{2,3\} \in \ker\varphi = 1 \mid 23$ but if π is either of the cycles (123) or (132), then $\operatorname{Im}(\varphi\pi) \notin \ker\varphi$. Therefore Lemma 3.4 implies that $(PP^2Px)\zeta \in \mathcal{T}_3(2)$. Since $H\zeta = \varepsilon$, we conclude that $p\zeta \in \mathcal{T}_3(2)$. On the other hand, it is clear that $(xw_i^6)^6\zeta = \varphi^2 = \binom{123}{333}$ for each i, whence $q\zeta \in \mathcal{T}_3(1)$. Thus, $p\zeta \neq q\zeta$, and the identity $p \doteq q$ fails in the semigroup $\mathcal{T}_3$.

Conversely, suppose that the identity $p \doteq q$ fails in $\mathcal{T}_3$, that is, $p\zeta \neq q\zeta$ under some homomorphism $\zeta : \Sigma^+ \to \mathcal{T}_3$. First, we show that the image of the letter x under such a homomorphism must be a transformation from $\mathcal{T}_3(2)$, whose square belongs to $\mathcal{T}_3(1)$, while the image of each word w_i must be a non-identity permutation from $\mathcal{S}_3$. For this, we exclude all other a priori possible cases of how the elements $x\zeta$ and $w_i\zeta$ can be located within the semigroup $\mathcal{T}_3$.

First of all, we observe that the words p and q share the suffix PxH. If the image of PxH under the homomorphism ζ belongs to $\mathcal{T}_3(1)$, i. e. is a constant transformation, then $p\zeta = (PxH)\zeta = q\zeta$, a contradiction to the choice of the identity $p \doteq q$ and the homomorphism ζ. Hence, in particular, we have $x\zeta \notin \mathcal{T}_3(1)$ and $w_i\zeta \notin \mathcal{T}_3(1)$ for all i. Besides that, if $x^2\zeta \in \mathcal{T}_3(1)$, then $w_i\zeta \neq \varepsilon$ for all i. Indeed, otherwise the image of the factor xw_i^4x that occurs in the common suffix PxH is a constant transformation.

Now assume that $w_i\zeta \in \mathcal{T}_3(2)$ for some i. If there exists an index j such that $w_j\zeta \in \mathcal{S}_3\backslash\{\varepsilon\}$, then, taking into account that the permutation $w_j\zeta$ is even, we can apply Lemma 3.5 to the image of the factor $w_iw_jw_iw_j^2w_i^2$ of the word H. Again we see that the image of the common suffix PxH is a constant transformation, a contradiction. If $w_i\zeta \in \mathcal{T}_3(2) \cup \{\varepsilon\}$ for all i, then Lemma 3.6 implies that $w_i^2\zeta = w_i^4\zeta = w_i^6\zeta$, whence $P\zeta = Q\zeta$ and $p\zeta = q\zeta$, a contradiction.

We have proved that $w_i\zeta \in \mathcal{S}_3$ for all i. Assume that $x\zeta \in \mathcal{S}_3$. Then the identity $x^6 \doteq 1$ holding in $\mathcal{S}_3$ and the construction of the words P, Q and H imply the equalities $P\zeta = Q\zeta = H\zeta = \varepsilon$. Therefore $p\zeta = q\zeta = x\zeta$, a contradiction. Now suppose that $x^2\zeta \in \mathcal{T}_3(2)$. In this case $H\zeta = \varepsilon$ and $w_i^6\zeta = \varepsilon$. We denote $x\zeta$ by φ, $P\zeta$ by ψ. Lemma 3.6 yields the equalities

$$q\zeta = (PQ^2PxH)\zeta = \psi(\varphi^6 \cdots \varphi^6)^2\psi\varphi = \psi\varphi^2\psi\varphi \tag{6}$$

Now we observe that the word P begins with the letter x, whence $\psi = \varphi\chi$ for some χ and $\varphi^2\psi = \varphi^3\chi = \varphi\chi = \psi$ by Lemma 3.6. In view if this, the equality (6) means that $q\zeta = \psi^2\varphi$. On the other hand, we have $p\zeta = (PP^2Px)\zeta =$

$\psi^4\varphi$. Clearly, the transformation ψ belongs to either $\mathcal{T}_3(2)$ or $\mathcal{T}_3(1)$. Therefore $\psi^2 = \psi^4$ because in the former case Lemma 3.6 applies, while in the latter case ψ is a constant transformation whence $\psi = \psi^2$. Thus, $p\zeta = \psi^4\varphi = \psi^2\varphi = q\zeta$, a contradiction.

Summarizing, we see that the only possible configuration is the following: $x\zeta \in \mathcal{T}_3(2)$, $x^2\zeta \in \mathcal{T}_3(1)$ and $w_i\zeta \in \mathcal{S}_3\backslash\{\varepsilon\}$ for each i. Recall that $w_i = e_i v_j v_k^5 e_i^5 v_k v_j^5$ where the vertices $v_j, v_k \in V$ are the ends of the edge e_i. Since the identity $x^6 \doteq 1$ holds in $\mathcal{S}_3$, the inequality $w_i\zeta \neq \varepsilon$ is only possible provided that $v_j\zeta \neq v_k\zeta$. Hence the homomorphism ζ assigns to each pair of adjacent vertices of the graph Γ a pair of distinct elements of the group $\mathcal{S}_3$ and thus defines a 6-coloring of Γ.

Proposition 3.7 is thus proved, and this also completes the proof of Theorem 2. □

References

[1] *J. Almeida, S. V. Plescheva, M. V. Volkov*, An application of group generic implicit operators to the complexity of identity checking in finite semigroups, Internat. Algebraic Conference dedicated to the centinenial of P. G. Kontorovich and the 70th birthday of L. N. Shevrin, Abstracts, Ekterinburg: Ural State University, 2005, 16–17.

[2] *J. Almeida, M. V. Volkov*, Subword complexity of profinite words and subgroups of free profinite semigroups, Int. J. Algebra and Computation 16, no.2 (2006), 221–258.

[3] *C. Bergman, G. Slutzki*, Complexity of some problems concerning varieties and quasi-varieties of algebras, SIAM J. Comput., 30, no.2 (2000), 359–382.

[4] *S. Burris, J. Lawrence*, The equivalence problem for finite rings, J. Symbolic Computation, 15, no.1 (1993), 67–71.

[5] *S. Burris, J. Lawrence*, Results on the equivalence problem for finite groups, Algebra Universalis, 52, no.4 (2005), 495–500.

[6] *C. C. Edmunds*, On certain finitely based varieties of semigroups, Semigroup Forum, 15, no.1 (1977), 21–39.

[7] *M. R. Garey, D. S. Johnson*, Computers and Intractability: A Guide to the Theory of NP-completeness, Freeman, 1979.

[8] *G. Horváth, J. Lawrence, L. Mérai, Cs. Szabó*, The complexity of the equivalence problem for nonsolvable groups, Bull. London Math. Soc 39, no.3 (2007), 433–438.

[9] *G. Horváth, Cs. Szabó*, The complexity of checking identities over finite groups, Int. J. Algebra and Computation, 16, no.5 (2006), 931–939.

[10] *H. B. Hunt III, R. E. Stearns*, The complexity of equivalence for commutative rings, J. Symbolic Computation, 10, no.5 (1990), 411–436.

[11] *M. Jackson, R. McKenzie*, Interpreting graph colorability in finite semigroups, Int. J. Algebra and Computation, 16, no.1 (2006), 119–140.

[12] *J. Kalicki*, On comparison of finite algebras, Proc. Amer. Math. Soc., 3, no.1 (1952), 36–40.

[13] *M. I. Kargapolov, J. I. Merzljakov*, Fundamentals of the Theory of Groups, Springer, 1979.

[14] *O. G. Kharlampovich, M. V. Sapir*, Algorithmic problems in varieties, Int. J. Algebra and Computation, 5, no.4-5 (1995), 379–602.

[15] *A. Kisielewicz*, Complexity of semigroup identity checking, Int. J. Algebra and Computation, 14, no.4 (2004), 455–464.

[16] *O. Klíma*, Complexity issues of checking identities in finite monoids, Semigroup Forum, accepted.

[17] *M. Kozik*, On Some Complexity Problems in Finite Algebras, PhD Dissertation, Vanderbilt University, Nashville, 2004.

[18] *M. Kozik*, Computationally and algebraically complex finite algebra membership problems, Int. J. Algebra and Computation, 17, no.8 (2007), 1635-1666.

[19] *M. Kozik*, Varietal membership problem is 2EXPTIME complete, submitted.

[20] *R. C. Lyndon, P. E. Schupp*, Combinatorial Group Theory, Berlin–Heidelberg–N.y.: Springer-Verlag, 1977.

[21] *C. H. Papadimitriou*, Computational Complexity, Reading–Menlo Park–N.Y.: Addison-Wesley Publishing Company, 1994.

[22] *J-E. Pin*, Varieties of Formal Languages, Oxford: North Oxford Academic and N.Y.: Plenum, 1986.

[23] *S. V. Plescheva, V. Vértesi*, Complexity of the identity checking problem in a 0-simple semigroup, Proc. Ural. State Univ., no.43, Computer Science and Information Technology, no.1 (2006), 72–102 [in Russian].

[24] *S. Seif*, The Perkins semigroup has co-NP-complete term-equivalence problem, Int. J. Algebra and Computation, 15, no.2 (2005), 317–326.

[25] *S. Seif, Cs. Szabó*, Computational complexity of checking identities in 0-simple semigroups and matrix semigroups over finite fields, Semigroup Forum, 72, no.2 (2006), 207–222.

[26] *E. P. Simel'gor*, Identities in the finite symmetric semigroup, Contemporary Algebra, 1 (1974), 174–188 [in Russian].

[27] *Cs. Szabó, V. Vértesi*, The complexity of the word-problem for finite matrix rings, Proc. Amer. Math. Soc., 132, no.12 (2004), 3689–3695.

[28] *Cs. Szabó, V. Vértesi*, The complexity of checking identities for finite matrix rings, Algebra Universalis, 51, no.4 (2004), 439–445.

[29] *Cs. Szabó, V. Vértesi*, The identity checking problem in finite rings, submitted.

[30] *Z. Székely*, Computational complexity of the finite algebra membership problem for varieties, Int. J. Algebra and Computation, 12, no.6 (2002), 811–823.

[31] *P. Tesson*, Computational Complexity Questions Related to Finite Monoids and Semigroups, PhD Thesis, McGill University, Montréal, 2003.