Complexity Issues of Checking Identities in Finite Monoids

Ondřej Klíma[1]

Communicated by Mikhail Volkov

Abstract We study the computational complexity of checking identities in a fixed finite monoid. We find the smallest monoid for which this problem is coNP-complete and describe a significant class of finite monoids for which the problem is tractable.

Keywords checking identities, semigroups, complexity

1 Introduction

One of the fundamental questions in universal algebra is the verification of identities in algebras. In this paper we consider the problem of checking identities in a fixed finite monoid, which we refer to as the CHECK-ID problem. Another well known name of this problem is the Term Equivalence (TERM-EQ) problem, and we will consider also its natural generalization, namely the Polynomial Equivalence (POL-EQ) problem. A polynomial over a finite monoid M is a sequence of variables and elements of M and the POL-EQ problem asks to decide for a given pair of polynomials whether the products of the two sequences are equal under each assignment of variables.

Both these problems are in the complexity class coNP. Under the assumption coNP$\neq$P (which is assumed throughout the paper) one can ask for which monoids the problems are decidable in polynomial time (tractable) and for which monoids the problems are coNP-complete. For an introduction to the complexity theory see [9].

The Polynomial Equivalence problem was studied also in associative ring theory where a dichotomy theorem was proved by Hunt and Stearns [8] for finite commutative rings and later by Burris and Lawrence [2] for the general case: a ring has tractable Polynomial Equivalence problem whenever it is nilpotent, and has coNP-complete this problem otherwise. Weaker results are known in the case of groups: the POL-EQ problem is tractable for nilpotent groups [3, 4] and the POL-EQ problem is coNP-complete for non-solvable groups [7].

[1] O.Klíma
Department of Mathematics and Statistics, Masaryk University, Janáčkovo nám. 2a, 662 95 Brno, Czech Republic,
klima@math.muni.cz, `http://www.math.muni.cz/~klima`
The author was supported by the Ministry of Education of the Czech Republic under the project MSM 0021622409 and by the Grant no. 201/06/0936 of the Grant Agency of the Czech Republic.

In the case of semigroups and monoids there are some results concerning completely 0-simple semigroups and matrix semigroups over finite fields [10, 12, 13]. In [14] Szabó and Vértesi have proved hardness of the CHECK-ID problem for the monoid of 2×2 matrices over $\mathbb{Z}_2$ and have asked for a smaller example of such a semigroup. In this paper we describe the smallest monoid with this property, namely the six-element monoid which is called Brandt monoid in the literature. The fact that the Brandt monoid has coNP-complete CHECK-ID problem was independently observed by Seif [11].

2 Preliminaries

The free monoid over an arbitrary alphabet A is denoted A^*. The neutral element of every monoid is denoted 1.

Let M be a finite monoid and $\mathcal{X}$ be a countable set of variables. The elements from $\mathcal{X}^*$ and $(M \cup \mathcal{X})^*$ are called *terms* and *polynomials*, respectively. A *substitution* is an arbitrary mapping $\sigma : \mathcal{X} \to M$. For a given substitution σ we denote by the same symbol σ also the unique extension to the morphism $\sigma : (M \cup \mathcal{X})^* \to M$ which behaves as an identity on elements from M. We say that two terms (or polynomials) u, v are *equivalent* in M if $\sigma(u) = \sigma(v)$ for every substitution $\sigma : \mathcal{X} \to M$. An *identity* $u = v$ is a pair of terms, i.e. $u, v \in \mathcal{X}^*$, and we say that this identity is valid in the monoid M if the terms u and v are equivalent in M.

We are interested in the problem of checking the validity of identities in a fixed finite monoid M and in the generalization of this problem to the case of polynomials.

CHECK-ID(M)
Instance: An identity, i.e. a pair of terms, $u = v$, where $u, v \in \mathcal{X}^*$.
Question: Is the identity $u = v$ valid in M?

When we consider polynomials instead of terms, we obtain the following generalization.

POL-EQ(M)
Instance: A pair of polynomials $u, v \in (M \cup \mathcal{X})^*$.
Question: Are these polynomials equivalent in M?

We should point out that for every monoid M we have the individual problem CHECK-ID(M) and the individual problem POL-EQ(M). In other words, for different monoids we have different problems CHECK-ID (and POL-EQ respectively) for which we can obtain different results concerning their complexity. Further, the monoid M is not a part of an instance, i.e. its order $|M|$ can be used as a constant when we calculate time complexity of algorithms solving our problems. The time complexity function of a considered algorithm is a function which maps each natural number n to the maximum number of steps which the

algorithm makes on an input of size n. In our problems CHECK-ID(M) and POL-EQ(M) the size of an input, i.e. size of an instance, is simply the sum of the lengths of the given terms and polynomials, respectively.

Note also that each instance of the CHECK-ID(M) problem is an instance of the POL-EQ(M) problem. This means that there is a trivial polynomial-time reduction from CHECK-ID(M) to POL-EQ(M).

A basic idea for solving the POL-EQ(M) problem is to consider its complement, which is trivially in NP; therefore the POL-EQ(M) problem (and hence also the CHECK-ID(M) problem) is in the complexity class coNP. When dealing with the complement of the POL-EQ(M) problem, we are looking for a morphism which distinguishes the given pair of polynomials. So we can take all possible pairs of different elements of the monoid and ask whether there is a morphism which maps the given pair of polynomials to the pair of elements. This idea leads us to consider the problem of solving equations in the monoid M.

EQN(M)
Instance: A pair of polynomials $u, v \in (M \cup \mathcal{X})^*$.
Question: Does there exist a substitution $\sigma : \mathcal{X} \to M$ such that $\sigma(u) = \sigma(v)$?

2T-EQN(M)
Instance: A pair of polynomials $u, v \in (M \cup \mathcal{X})^*$ and a pair of elements $m, n \in M$.
Question: Does there exist a substitution $\sigma : \mathcal{X} \to M$ such that $\sigma(u) = m$ and $\sigma(v) = n$?

The previous observation can then be formulated in the following way.

Lemma 1. *Let M be a finite monoid such that the* 2T-EQN(M) *problem is decidable in polynomial time. Then the* POL-EQ(M) *and* EQN(M) *problems are also decidable in polynomial time.*

Proof. Let $\mathcal{A}$ be a polynomial algorithm solving the 2T-EQN(M) problem. Let u, v be an instance of the POL-EQ(M) problem. Then for every pair m, n of different elements of M we use the algorithm $\mathcal{A}$ to find whether there is a morphism σ such that $\sigma(u) = m$ and $n = \sigma(v)$. If there is such a morphism then $\sigma(u) \neq \sigma(v)$ and polynomials u, v are not equivalent. Conversely, if there is no such morphism for every choice of m and n then polynomials u, v are equivalent. Time complexity of our algorithm is bounded by $|M|^2$ times the complexity of the algorithm $\mathcal{A}$. Since $|M|$ is a constant, we have a polynomial algorithm for the POL-EQ(M) problem.

For the EQN(M) problem we just consider the instances of the 2T-EQN(M) problem of the form u, v, m, m, where m is an arbitrary element of M. □

We adopt some notation from combinatorics on words. We say that a polynomial $u \in (M \cup \mathcal{X})^*$ is a *factor* of a polynomial $v \in (M \cup \mathcal{X})^*$ if $v = sut$ for some polynomials $s, t \in (M \cup \mathcal{X})^*$. We speak about *prefix* when s is the empty word and *suffix* when t is the empty word. For an arbitrary polynomial $u \in (M \cup \mathcal{X})^*$

we denote by $\mathrm{c}(u)$ the *content* of u, i.e. the set of all variables from $\mathcal{X}$ which occur in u.

We denote by $E(M)$ the set of all idempotents of a monoid M, i.e. $E(M) = \{e \in M \mid e^2 = e\}$. We will use standard notions from semigroup theory like Green's relations $\mathcal{J}$, $\mathcal{R}$, $\mathcal{L}$ and $\mathcal{H}$ (see e.g. chapter 2 in [5]). As usually, for $a \in M$ we denote $\mathcal{J}_a$ the set of all elements $\mathcal{J}$-related to a, i.e. $\mathcal{J}_a = \{b \mid MbM = MaM\}$. We will also use the following lemma.

Lemma 2 ([5] Proposition 2.3.3). *Let M be a finite monoid. If $e, f \in E(M)$, $e \mathcal{L} f$ then $ef = e$.*

A central role in the paper is played by the following two monoids which are well-known from the literature. They are important because they are minimal ones outside some natural classes of monoids.

We define the Brandt monoid B_2^1 and the monoid A_2^1 by their presentations:

$$\mathrm{B}_2^1 = \langle a, b \mid a^2 = b^2 = 0, aba = a, bab = b \rangle \quad \text{and}$$

$$\mathrm{A}_2^1 = \langle a, b \mid a^2 = a, b^2 = 0, aba = a, bab = b \rangle.$$

Both B_2^1 and A_2^1 have six elements 1, a, b, ab, ba and 0 and they have the same Green's relations. The structure of the monoids can be viewed in Figure 1 where

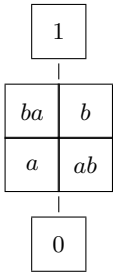

Fig. 1. The structure of the monoids B_2^1 and A_2^1.

we use egg-boxes to visualize relations between elements. (Each row represents an $\mathcal{R}$-class, each column an $\mathcal{L}$-class and each cell an $\mathcal{H}$-class. Each egg-box is a $\mathcal{J}$-class and egg-boxes are ordered by $\leq_{\mathcal{J}}$ in the usual way.) The property which distinguishes the monoids B_2^1 and A_2^1 is that the set of all idempotents in B_2^1, i.e. $E(\mathrm{B}_2^1) = \{0, ab, ba, 1\}$, forms a submonoid of B_2^1 but the set of all idempotents of A_2^1, i.e. $E(\mathrm{A}_2^1) = \{0, a, ab, ba, 1\}$, does not. On the other hand, a common property of B_2^1 and A_2^1 is that $s^3 = s^2$ for each element s, and hence s^2 is an idempotent for each s. Altogether, we can distinguish these two monoids by an identity $(x^2y^2)^2 = x^2y^2$ which is satisfied in B_2^1 but it is not satisfied in A_2^1.

Any set of identities naturally corresponds to the class of all monoids which satisfy these identities. We call these classes *varieties* and these are exactly the

classes of monoids closed under taking submonoids, morphic images and products. For a monoid M we denote by $\langle M \rangle$ the smallest variety which contains the monoid M. From this point of view, the CHECK-ID(M) problem is just the so-called identity problem for the variety $\langle M \rangle$.

Other natural classes of finite monoids, so-called *pseudovarieties*, are closed under taking submonoids, morphic images and finite products. In this paper we will work just with the pseudovariety $\mathbf{DO} \cap \overline{\mathbf{G_{NIL}}}$ which is given by the following property: $M \in \mathbf{DO} \cap \overline{\mathbf{G_{NIL}}}$ if and only if every subgroup of M is nilpotent and for every $e, f \in E(M)$ such that $e \mathcal{J} f$ we have $ef \in E(M) \cap \mathcal{J}_e$.

3 The Smallest Monoid with Hard CHECK-ID Problem

We modify the methods from [1] which were used for solving of equations. First of all, we improve the original proof of NP-hardness of the EQN(B_2^1) problem to the case of the CHECK-ID(B_2^1) problem.

Proposition 3. *The* CHECK-ID(B_2^1) *problem is coNP-complete.*

Proof. Recall that the set of all idempotents $\{0, ab, ba, 1\}$ forms a submonoid of B_2^1 and $s^3 = s^2$ is an idempotent for each element $s \in \mathrm{B}_2^1$.

We show a polynomial reduction from the NP-complete problem 1-in-3-SAT (called the *exactly-one-in-three satisfiability problem* in the literature — see [9]) into the coTERM-EQ(B_2^1) problem. An instance of the 1-in-3-SAT problem is a conjunction $\Phi = \Phi_1 \wedge \Phi_2 \wedge \cdots \wedge \Phi_k$ of clauses and each clause Φ_r, $1 \leq r \leq k$, is of the form $l_1 \vee l_2 \vee l_3$, where l_j, $1 \leq j \leq 3$, is a *literal* (i.e. l_j is a Boolean variable X from the set Var or its negation $\neg X$). A *valuation* is a mapping $\nu : Var \to \{\mathtt{true}, \mathtt{false}\}$. The question in the 1-in-3-SAT problem is whether there exists a valuation ν such that exactly one of $\nu(l_1)$, $\nu(l_2)$ and $\nu(l_3)$ is $\mathtt{true}$ for every clause $\Phi_r = l_1 \vee l_2 \vee l_3$. We say that Φ is 1-satisfiable if such a valuation ν exists.

Let $\Phi = \Phi_1 \wedge \Phi_2 \wedge \cdots \wedge \Phi_k$ be an instance of the 1-in-3-SAT problem. Let $\{X_1, X_2, \ldots, X_n\}$ be a set of all variables occurring in the formula Φ.

For each Boolean variable X_i, $1 \leq i \leq n$, we introduce variables x_i and $\overline{x_i}$. For a literal l we denote by $\widetilde{l}$ the corresponding variable: $\widetilde{l} = x_i$ if the literal l is the Boolean variable X_i and $\widetilde{l} = \overline{x}_i$ if the literal l is a negation of the Boolean variable X_i. We also introduce a new variable y and put $\Sigma = \{y, x_1, \overline{x_1}, \ldots, x_n, \overline{x_n}\} \subset \mathcal{X}$.

Now, for each Boolean variable X_i with the corresponding variable x_i we define the following term

$$w(X_i) = (yx_i\overline{x}_i y\overline{x}_i x_i)^2$$

and for each clause $\Phi_r = l_1 \vee l_2 \vee l_3$ we define the term

$$u(\Phi_r) = (y\widetilde{l_1}\widetilde{l_2}\widetilde{l_3})^2.$$

Finally, we define

$$t = w(X_1) \ldots w(X_n) u(\Phi_1) \ldots u(\Phi_k) y.$$

The result will follow from the next:
Claim: The instance Φ is 1-satisfiable if and only if there is a substitution $\sigma : \Sigma \to \mathrm{B}_2^1$ such that $\sigma(t)$ is not an idempotent, i.e. terms t^2 and t are not equivalent in the monoid B_2^1.
Proof of the claim: Let $\sigma : \Sigma \to \mathrm{B}_2^1$ be such that $\sigma(t)$ is not an idempotent, i.e. $\sigma(t) = a$ or $\sigma(t) = b$. We will discuss only the first case, the second one is obtained by interchanging a and b. It is easy to see that $\sigma(y) = a$, because w's and u's are squares, and thus $\sigma(w(X_i))$ and $\sigma(u(\Phi_r))$ are idempotents. Since $\sigma(y) = a$ and y is contained in each $w(X_i)$ and $u(\Phi_r)$, we see that $\sigma(w(X_i))$ and $\sigma(u(\Phi_r))$ cannot be equal to 1 and we can deduce that $\sigma(w(X_i)) = \sigma(u(\Phi_r)) = ab$. For every i we have $\sigma(x_i), \sigma(\overline{x}_i) \in \{1, b\}$ and $\sigma(x_i) \neq \sigma(\overline{x}_i)$ — otherwise $\sigma(w(X_i)) = 0$. So, we can define a valuation: $\nu(X_i) = \texttt{true}$ if $\sigma(x_i) = b$ (and $\sigma(\overline{x}_i) = 1$ at the same time) and $\nu(X_i) = \texttt{false}$ if $\sigma(x_i) = 1$ (and $\sigma(\overline{x}_i) = b$ at the same time). Now, for each clause $\Phi_r = l_1 \vee l_2 \vee l_3$ exactly one of $\nu(l_1)$, $\nu(l_2)$ and $\nu(l_3)$ is equal to `true`, because otherwise $\sigma(u(\Phi_r)) = 0$. Hence, the formula Φ is 1-satisfiable.

If we assume that there is a valuation ν which 1-satisfies the formula Φ, then we can define the substitution $\sigma : \Sigma \to \mathrm{B}_2^1$ in the following way. If $\nu(X_i) = \texttt{true}$ then we put $\sigma(x_i) = b$ and $\sigma(\overline{x}_i) = 1$; if $\nu(X_i) = \texttt{false}$ then we put $\sigma(x_i) = 1$ and $\sigma(\overline{x}_i) = b$; and finally we put $\sigma(y) = a$. So, for each Boolean variable X_i we have $\sigma(x_i\overline{x}_i) = \sigma(\overline{x}_i x_i) = b$, hence $\sigma(w(X_i)) = ab$. Analogically, $\sigma(u(\Phi_r)) = ab$, hence $\sigma(t) = a$ is not an idempotent. □

Remark 4. If we consider an equation $t = a$ instead of the identity $t = t^2$ in the previous proof, then we obtain the proof of NP-completeness of $\mathrm{EQN}(\mathrm{B}_2^1)$ similar to original proof from [1].

We use a result given by P. Tesson in his PhD Thesis [15] — the tractability of the Program Satisfiability problem for all monoids from the class $\mathbf{DO} \cap \overline{\mathbf{G_{NIL}}}$. We can deduce the following statement from his proofs, specially from the proofs of Lemmas 5.1. and 5.15.

Proposition 5 ([15]). *The* 2T-EQN(M) *problem is decidable in polynomial time for every monoid* $M \in \mathbf{DO} \cap \overline{\mathbf{G_{NIL}}}$.

We obtain the following statement as a direct consequence of Lemma 1.

Proposition 6. *The* POL-EQ(M) *problem is decidable in polynomial time for every monoid* $M \in \mathbf{DO} \cap \overline{\mathbf{G_{NIL}}}$.

Note that the class $\mathbf{DO} \cap \overline{\mathbf{G_{NIL}}}$ contains many important classes of monoids, e.g. all commutative monoids and all idempotent monoids. As a side result we can also obtain the observation that the monoid B_2^1 is the smallest one with the hard CHECK-ID problem, moreover it is the smallest among the monoids with the hard POL-EQ problem.

Proposition 7. *Let* M *be an arbitrary monoid with at most five elements. Then the* POL-EQ(M) *problem is decidable in polynomial time.*

Proof. We show that each monoid of this size is inside the class $\mathbf{DO} \cap \overline{\mathbf{G_{NIL}}}$ and hence the statement is a consequence of Proposition 6. Let a monoid M have at most five elements. Then M has only nilpotent subgroups because every non-nilpotent group has at least six elements. Assume for a moment that there are $\mathcal{J}$-related idempotents $e, f \in E(M)$ such that $ef \notin E(M) \cap \mathcal{J}_e$. Clearly, $1 \notin \mathcal{J}_e$ because the $\mathcal{J}$-class of 1 is a subgroup in every finite monoid. If $e \mathcal{L} f$ then by Lemma 2 we have $ef = e \in E(M) \cap \mathcal{J}_e$ a contradiction. So, e is not $\mathcal{L}$-related to f and dually $\mathcal{R}_e \neq \mathcal{R}_f$. Hence $\mathcal{J}_e$ contains at least two $\mathcal{L}$-classes and two $\mathcal{R}$-classes, i.e. $\mathcal{J}_e$ contains at least four elements. Since $1 \notin \mathcal{J}_e$ and M has at most five elements, we see that M consists of the element 1 and the four-element class $\mathcal{J}_e$. Hence $ef \in \mathcal{J}_e$ and $(ef)^2 \in \mathcal{J}_e$. Finally, $(ef)^2 \mathcal{L} (ef)$, $(ef)^2 \mathcal{R} (ef)$ and $(ef)^2 = ef$ follows. This is a contradiction with $ef \notin E(M) \cap \mathcal{J}_e$. □

Note that the proof of the previous proposition can be used to characterize all monoids outside $\mathbf{DO} \cap \overline{\mathbf{G_{NIL}}}$ which have six elements. Indeed, there is a unique six-element non-nilpotent group, namely S_3 (the permutation group over a three-element set). Further, if we consider a six-element monoid with idempotents e, f as in the proof, then there are exactly two possibilities: in the first case the class $\mathcal{J}_e$ contains only two idempotents (namely e, f) and then the monoid is isomorphic to B_2^1 and in the second case the class $\mathcal{J}_e$ contains three idempotents and then the monoid is isomorphic to A_2^1.

So, there are exactly three monoids outside the class $\mathbf{DO} \cap \overline{\mathbf{G_{NIL}}}$ which have at most six elements, namely B_2^1, A_2^1 and S_3. We show the tractability of the POL-EQ(A_2^1) problem in Lemma 8. Recently in [3, 6], it was proved that the POL-EQ(S_3) problem is decidable in polynomial time. Hence B_2^1 is the only monoid with at most six elements and hard CHECK-ID and POL-EQ problems.

Lemma 8. *The* POL-EQ(A_2^1) *problem is decidable in polynomial time.*

Proof. Let $u, v \in (\mathrm{A}_2^1 \cup \mathcal{X})^*$ be an instance of the POL-EQ(A_2^1) problem. We construct a certain set $T_{u,v}$ of test morphisms which proves or disproves the equivalence of the polynomials u and v. A test morphism

$$\tau_L : (\mathrm{A}_2^1 \cup \mathcal{X})^* \to \mathrm{A}_2^1$$

for any 5-tuple $L = (Y, x, y, c, d)$ where $Y \subset \mathcal{X}$, $x, y \in \mathcal{X} \setminus Y$, $c, d \in \mathrm{A}_2^1$ is defined in the following way:

$$\tau_L(z) = \begin{cases} 1, & z \in Y \\ c, & z = x \\ d, & z = y \\ a, & z \notin Y \cup \{x, y\}. \end{cases}$$

Of course, there are too many such morphisms. However, it is clear that for every τ_L we can compute the values $\tau_L(u)$ and $\tau_L(v)$ in polynomial time. In the rest of the proof we show how, given polynomials u and v, to select some test morphisms τ_L such that the set $T_{u,v}$ of the selected morphisms is of polynomial size with respect to the size of u and v and has the following property: there is

a morphism σ such that $\sigma(u) \neq \sigma(v)$ if and only if there is such a morphism in the set $T_{u,v}$. Clearly, this will imply that the problem POL-EQ(A_2^1) is solvable in polynomial time.

Assume that there is a morphism σ such that $\sigma(u) \neq \sigma(v)$. We consider several cases and for each of them we put polynomially many test morphisms into the set $T_{u,v}$.

1. Assume that $\sigma(u) = 1$ and $\sigma(v) \neq 1$. There are two possibilities: the polynomial v contains some of the elements $0, a, ab, ba, b$ or the polynomial v contains some variable x_v which does not occur in u and such that $\sigma(x_v) \neq 1$. In the first case we can consider the morphism τ_L where $L = (Y, x, y, c, d)$, $Y = \mathrm{c}(uv)$, $x, y \in \mathcal{X} \setminus Y$ arbitrary variables, $c = d = 0$. This means that τ_L maps all variables used in u and v to the element 1. Hence $\tau_L(u) = 1 \neq \tau_L(v)$. We put this morphism to $T_{u,v}$.

In the second case we can consider the morphism τ_L where $L = (Y, x, y, c, d)$, $Y = \mathrm{c}(uv) \setminus \{x_v\}$, $x = x_v$, and y an arbitrary variable, $c = d = 0$. Then $\tau_L(u) = 1 \neq \tau_L(v) = 0$. This means that we need to put one test morphism to $T_{u,v}$ for each choice of $x \in \mathrm{c}(v) \setminus \mathrm{c}(u)$. Surely, we need only polynomially many morphisms.

2. Assume that $\sigma(u), \sigma(v) \in \mathcal{J}_a$ but these elements are not $\mathcal{R}$-related (the case when they are not $\mathcal{L}$-related is dual[2]), i.e. we can assume $\sigma(u)\ \mathcal{R}\ a$ and $\sigma(v)\ \mathcal{R}\ b$. Let p be the longest prefix of u such that $\sigma(p) = 1$, i.e. $u = pku'$ where $p, u' \in (\mathrm{A}_2^1 \cup \mathcal{X})^*$, $k \in \{a, ab\} \cup \mathcal{X}$, $\sigma(p) = 1$, $\sigma(k) \in \{a, ab\}$), and let q be the longest prefix of v such that $\sigma(q) = 1$, i.e. $v = q\ell v'$ where $q, v' \in (\mathrm{A}_2^1 \cup \mathcal{X})^*$, $\ell \in \{b, ba\} \cup \mathcal{X}$, $\sigma(q) = 1$, $\sigma(\ell) \in \{b, ba\}$). If $k \in \{a, ab\}$ and $\ell \in \{b, ba\}$ then we consider the morphism τ_L where $L = (\mathrm{c}(pq), x, y, 0, 0)$, $x, y \notin \mathrm{c}(uv)$ arbitrary variables. Then $\tau_L(u)\ \mathcal{R}\ a$ and $\tau_L(v)\ \mathcal{R}\ b$. Analogically, if $k = x_u \in \mathcal{X}$, $\sigma(x_u) \in \{a, ab\}$ and $\ell \in \{b, ba\}$ then we consider the morphism τ_L where $L = (\mathrm{c}(pq), x_u, y, a, 0)$, $y \notin \mathrm{c}(uv)$ an arbitrary variable, and we have $\tau_L(u)\ \mathcal{R}\ a$ and $\tau_L(v)\ \mathcal{R}\ b$ again. The situations when $\ell \in \mathcal{X}$ are similar. This means that we need to put one test morphism to $T_{u,v}$ for each pair of prefixes p of u and q of v. We use polynomially many morphisms.

3. The last case which we have to discuss is that $\sigma(u)\ \mathcal{J}\ a$ but $\sigma(v) = 0$ (the case $\sigma(v)\ \mathcal{J}\ a$ but $\sigma(u) = 0$ is analogical). If $\sigma(x_v) = 0$ for some variable $x_v \in \mathrm{c}(v)$, then x_v does not occur in u and we can use the test morphism from case 1. We also use the test morphism from case 1 in the situation when v contains 0.

So, we assume that $\sigma(x) \neq 0$ for all variables and that u and v do not contain 0. Now, v has a factor $\alpha w \beta$ where $\alpha, \beta \in \mathrm{A}_2^1 \cup \mathcal{X}$, $w \in (\mathcal{X} \cup \{1\})^*$ and $\sigma(\alpha) \in \{b, ab\}$, $\sigma(w) = 1$, $\sigma(\beta) \in \{b, ba\}$. If $\alpha, \beta \in \mathcal{X}$ then we consider the morphism τ_L where $L = (\mathrm{c}(w), \alpha, \beta, \sigma(\alpha), \sigma(\beta))$; if $\alpha \in \mathcal{X}$ and $\beta \in \{b, ba\}$ then we consider τ_L where $L = (\mathrm{c}(w), \alpha, y, \sigma(\alpha), 0)$ and $y \in \mathcal{X} \setminus \mathrm{c}(uv)$; (and similarly if $\alpha \in \{b, ab\}, \beta \in \mathcal{X}$); and finally if $\alpha \in \{b, ab\}$ and $\beta \in \{b, ba\}$ then we use the test morphism from case 1. In all situations $\tau_L(u) \in \mathcal{J}_a$ and $\tau_L(v) = 0$. This means that we need to put one test morphism to $T_{u,v}$ for each factor w of v.

[2] We just switch from prefixes to suffixes in the following argument.

There are only polynomially many factors of v, hence we put polynomially many morphisms to $T_{u,v}$. □

Note that arguments similar to those used in the previous proof lead also to the observation that the 2T-EQN(A_2^1) problem is decidable in polynomial time, in particular the EQN(A_2^1) problem is decidable in polynomial time too. This result is contained in [1].

We also note that the tractability of the CHECK-ID(A_2^1) problem has been proved by Szabó and Seif [13] who used different techniques.

4 Final Remarks

We recall a well-known fact.

Lemma 9. $\mathrm{B}_2^1 \in \langle \mathrm{A}_2^1 \rangle$.

Proof. Let $\mathrm{A}_2^1 = \{1, c, d, cd, dc, 0\}$, where $c^2 = c$, $d^2 = 0$, $cdc = c$, $dcd = d$. We denote M the submonoid of the monoid $\mathrm{A}_2^1 \times \mathrm{A}_2^1$ generated by the elements $a = (c, d)$ and $b = (d, c)$. The monoid M contains the elements $1_{\mathrm{A}_2^1 \times \mathrm{A}_2^1} = (1, 1)$, a, b, $ab = (cd, dc)$, $ba = (dc, cd)$ and a certain subset I of elements with 0 on one of the coordinates. We also have $aba = a$, $bab = b$, and $a^2, b^2 \in I$. Moreover, the set I is an ideal of M. Now, one can check that the mapping $\varphi : M \to \mathrm{B}_2^1$ given by the images of generators $\varphi(a) = a$, $\varphi(b) = b$ is a surjective morphism, where $\varphi(x) = 0$ for each $x \in I$. In other words B_2^1 is the Rees quotient of M by the ideal I. □

This lemma has interesting consequences. First, it shows that the class of all finite monoids with the tractable identity checking problem is not a pseudovariety.

Although methods and results concerning the CHECK-ID problems and the POL-EQ problems are very close, the complexity of the problems is not always the same.

Proposition 10. *The* CHECK-ID($\mathrm{B}_2^1 \times \mathrm{A}_2^1$) *problem is decidable in polynomial time and the* POL-EQ($\mathrm{B}_2^1 \times \mathrm{A}_2^1$) *problem is coNP-complete.*

Proof. From Lemma 9 we have $\langle \mathrm{A}_2^1 \rangle = \langle \mathrm{B}_2^1 \times \mathrm{A}_2^1 \rangle$, hence the CHECK-ID($\mathrm{B}_2^1 \times \mathrm{A}_2^1$) problem is decidable in polynomial time by Lemma 8. On the other hand we show that the POL-EQ(B_2^1) problem can be reduced to the POL-EQ($\mathrm{B}_2^1 \times \mathrm{A}_2^1$) problem. Then the statement follows from Proposition 3.

First, we consider a morphism $\alpha : \mathrm{B}_2^1 \to \mathrm{B}_2^1 \times \mathrm{A}_2^1$ given by the rule $\alpha(m) = (m, 0)$ for every $m \in \mathrm{B}_2^1$. This morphism can be extended to the morphism $\alpha : (\mathrm{B}_2^1 \cup \mathcal{X})^* \to (\mathrm{B}_2^1 \times \mathrm{A}_2^1 \cup \mathcal{X})^*$. Now, if we have an instance of the POL-EQ(B_2^1) problem $u, v \in (\mathrm{B}_2^1 \cup \mathcal{X})^*$ then we consider the instance $s = \alpha(u) \cdot (1, 0)$, $t = \alpha(v) \cdot (1, 0)$ of the POL-EQ($\mathrm{B}_2^1 \times \mathrm{A}_2^1$) problem. It is easy to see that the polynomials s and t are equivalent in $\mathrm{B}_2^1 \times \mathrm{A}_2^1$ if and only if the polynomials u and v are equivalent in B_2^1. It is also clear that this is a polynomial reduction. □

Note that the EQN($B_2^1 \times A_2^1$) problem is NP-complete, because we can reduce the EQN(B_2^1) problem (see Remark 4) to the EQN($B_2^1 \times A_2^1$) problem using the same idea as in the previous proof.

The relationship between the problems CHECK-ID, POL-EQ and EQN could be a task for a future research on this field.

Historical remark

Before the paper was finished, its preliminary version had been available on the author's web page for a long time. For that reason some papers (e.g. [6]) refer to the preprint which had contained a few additional results, namely examples of monoids with different complexity of the studied problems.

Also a note in the paper [11] mentioned the preprint version.

Acknowledgments

I would like to thank: Pascal Tesson for sending me his excellent PhD thesis and for drawing my attention to his results concerning equations, Michal Kunc and Libor Polák for useful discussions, and the anonymous referee for corrections of my language errors and suggestions how to improve the presentation of the paper.

References

1. Barrington, D.M., McKenzie, P., Moore, C., Tesson, P., Thérien, D.: Equation satisfiability and program satisfiability for finite monoids. In Proceedings of MFCS'00, LNCS **1893**, 172–181 (2000)
2. Burris, S., Lawrence, J.: The equivalence problem for finite rings. J. of Symbolic Computation **15**, 67–71 (1993)
3. Burris, S., Lawrence, J.: Results on the equivalence problem for finite groups. Algebra Universalis **52**/4, 495–500 (2005)
4. Goldmann, M., Russell, A.: The complexity of solving equations over finite groups. Proc. IEEE Conference on Computational Complexity, 80–86 (1999)
5. Howie, J.M.: Fundamentals of Semigroup Theory. Oxford University Press (1995)
6. Horváth, G., Szabó, Cs.: The complexity of checking identities over finite groups. Int. J. Algebra and Computation **16**/5, 931–939 (2006)
7. Horváth, G., Lawrence, J., Mérai, L., Szabó, Cs.: The complexity of the equivalence problem for nonsolvable groups. Bull. London Math. Soc. **39**, 433–438 (2007)
8. Hunt, H., Stearns, R.: The complexity for equivalence for commutative rings. J. of Symbolic Computation **10**, 411–436 (1990)
9. Papadimitriou, C.H.: Computational Complexity. Addison-Wesley Publishing Company (1994)
10. Plescheva, S.V., Vértesi, V.: Complexity of the identity checking problem in a 0-simple semigroup. Proc. Ural. State Univ. **43**, Computer Science and Information Technology **1**, 72–102 (2006) (Russian)
11. Seif, S.: The Perkins semigroup has coNP-complete term-equivalence problem. Int. J. Algebra and Computation **15**/2, 317–326 (2005)

12. Seif, S., Szabó, Cs.: Algebra complexity problems involving graph homomorphism, semigroups and the constraint satisfaction problem. Journal of Complexity **19**/2, 153–160 (2003)
13. Seif S., Szabó, Cs.: The computational complexity of checking identities in simple semigroups and matrix semigroups over finite fields. Semigroup Forum **72**/2, 207–222 (2006)
14. Szabó, Cs., Vértesi, V.: The complexity of the word problem for finite matrix rings. Proc. Amer. Math. Soc. **132**/12, 439–445 (2004)
15. Tesson, P.: Computational Complexity Questions Related to Finite Monoids and Semigroups — Ph.D. Thesis. Available at `http://www.cs.mcgill.ca/~ptesso/`