Complexity Issues of Checking Identities in Finite Monoids

Ondřej Klíma *

Dept. of Mathematics, Masaryk University, Janáčkovo nám. 2a, 662 95 Brno, Czech Republic, klima@math.muni.cz, http://www.math.muni.cz/~klima
fax: 420 541 210 337

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. We also compare the complexities of this problem and the problem of solving equations in the same monoid.
Keywords: checking identities, semigroups, complexity
MSC 2000: 68Q25, 20M05

1 Introduction

The fundamental question 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 Term Equivalence problem, and its generalization the Polynomial Equivalence (POL-EQ) problem. A polynomial for 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 product of the sequences is equal under any assignment of variables.

The Polynomial Equivalence problem was studied also in ring theory where a dichotomy theorem was proved by Hunt and Stearns [4] for finite commutative rings and later by Burris and Lawrence [2] in the general case — a ring has tractable Polynomial Equivalence problem if and only if it is nilpotent. Burris and Lawrence used the same idea to obtain a result (unpublished) in the case of groups — the POL-EQ problem is tractable for nilpotent groups and is coNP-complete for non-solvable groups.

In the case of semigroups and monoids there are some results concerning completely 0-simple semigroups and matrix semigroups over finite fields [5, 6]. In [7] the authors prove the hardness of the Term Equivalence problem for the monoid of 2×2 matrices over $\mathbb{Z}_2$ and ask for the smallest example of such a semigroup. In this paper we describe the smallest monoid with this property.

There is a natural connection between the Polynomial Equivalence problem and the problem of solving equations. We modify the results and methods from

* The author was supported by the Grant Agency of the Czech Republic, grant No. 201/01/0323.

the paper [1] where the Equation Satisfiability problem and the Target Equation Satisfiability problem were discussed.

2 Preliminaries

2.1 Structure of finite monoids

We recall the basic facts from semigroup theory, which we will use in this paper.

Let $(M, \cdot, 1)$ be a monoid, i.e. a set M with an associative operation $\cdot$ and a neutral element 1. We will denote it shortly M. An element $e \in M$ is called an *idempotent* if $e^2 = e$ and the set of all idempotents of the monoid M is denoted by $E(M)$. It is folklore that for any finite monoid M there is a natural number t such that m^t is an idempotent for any element $m \in M$ and this idempotent is a unique one in the subsemigroup $\{m^s \mid s \in \mathbb{N}\}$ of M generated by the element m. Recall that in the case when M is a group this t can be chosen as the order of M, i.e. the number of elements of M.

The left (right) ideal generated by an element $m \in M$ is the set Mm (resp. mM), and its two-sided ideal is the set MmM. The following equivalence relations on M, called *Green's relations*, describe which elements generate the same ideals. For $m, m' \in M$ we put

$m\mathcal{J}m'$ iff $MmM = Mm'M$,

$m\mathcal{L}m'$ iff $Mm = Mm'$,

$m\mathcal{R}m'$ iff $mM = m'M$,

$m\mathcal{H}m'$ iff both $m\mathcal{L}m'$ and $m\mathcal{R}m'$.

We denote the $\mathcal{J}$-class ($\mathcal{L}$-class, $\mathcal{R}$-class, $\mathcal{H}$-class) of an element m by $\mathcal{J}_m$ (resp. $\mathcal{L}_m$, $\mathcal{R}_m$, $\mathcal{H}_m$). If we instead ask whether element's ideals are contained in one another, we can define natural pre-orders $\leq_{\mathcal{J}}$, $\leq_{\mathcal{L}}$, $\leq_{\mathcal{R}}$ on M with e.g. $m \leq_{\mathcal{J}} m'$ iff $MmM \subseteq Mm'M$. These pre-orders give partial orders on the partitions $M/\mathcal{J}$, $M/\mathcal{L}$ and $M/\mathcal{R}$ respectively. We say that a $\mathcal{J}$-class ($\mathcal{L}$-class, $\mathcal{R}$-class, $\mathcal{H}$-class) is *regular* if it contains some idempotent.

We explain these definitions in the following example, where we show a pair of monoids with identical Green's relations.

Example 1. We define the monoids B_2 and U by presentations: $\mathrm{B}_2 = \langle a, b \mid a^2 = b^2 = 0, aba = a, bab = b\rangle$ and $\mathrm{U} = \langle a, b \mid a^2 = a, b^2 = 0, aba = a, bab = b\rangle$. Both B_2 and U have six elements 1, a, b, ab, ba and 0 and the same Green's relations, namely three $\mathcal{J}$-classes $\{1\}$, $\{a, ab, ba, b\}$ and $\{0\}$, four $\mathcal{L}$-classes $\{1\}$, $\{a, ba\}$, $\{ab, b\}$ and $\{0\}$, four $\mathcal{R}$-classes $\{1\}$, $\{a, ab\}$, $\{ba, b\}$ and $\{0\}$, and six one-element $\mathcal{H}$-classes. The structure of the monoids can be viewed in Figure 1 where we use so-called 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 and U is that the set of all idempotents in B_2, i.e. $E(\mathrm{B}_2) = \{0, ab, ba, 1\}$, forms a submonoid of B_2 but the set of all idempotents of U, i.e. $E(\mathrm{U}) = \{0, a, ab, ba, 1\}$ does not. On the other hand, a common property of B_2 and U is that $s^3 = s^2$ for any element s and hence s^2

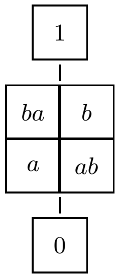

Fig. 1. The structure of the monoids B_2 and U.

is an idempotent for any s. Altogether, we can distinguish these two monoids by an identity $(x^2y^2)^2 = x^2y^2$ which is satisfied in B_2 but is not satisfied in U. (Another such identity is for example $x^2y^2 = y^2x^2$.)

We summarize basic results about Green's relations in the following lemma, which will be used through the whole paper and which can be found in any monograph on semigroup theory, e.g. in [3].

Lemma 1. *Let M be a finite monoid.*

i) *The relations $\mathcal{L}$ and $\mathcal{R}$ commute, i.e. the relation $\mathcal{R} \circ \mathcal{L} = \mathcal{L} \circ \mathcal{R}$ is their supremum $\mathcal{L} \vee \mathcal{R}$ in the lattice of all equivalence relations on M.*
ii) *$\mathcal{L} \vee \mathcal{R} = \mathcal{J}$.*
iii) *If $m\mathcal{J}n$ then the classes $\mathcal{H}_m$ and $\mathcal{H}_n$ have the same number of elements.*
iv) *If $m\mathcal{J}n$ and $m \leq_{\mathcal{L}} n$ (resp. $m \leq_{\mathcal{R}} n$) then $m\mathcal{L}n$ (resp. $m\mathcal{R}n$).*
v) *The maximal subsets of M which form groups are exactly the classes $\mathcal{H}_e$, where $e \in E(M)$. Moreover $\mathcal{J}_1 = \mathcal{H}_1$.*
vi) *Any $\mathcal{L}$-class (and $\mathcal{R}$-class) contained in a regular $\mathcal{J}$-class is regular itself.*
vii) *If $e, f \in E(M)$, $e\mathcal{L}f$ then $ef = e$.*

2.2 Free monoids and morphisms

The free monoid over an arbitrary alphabet A is denoted A^*.

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. We say that two polynomials (or terms) u, v are *equivalent* in M if and only if $\sigma(u) = \sigma(v)$ for any morphism $\sigma : (M \cup \mathcal{X})^* \to M$ which behaves as an identity on elements from M. Note that any such morphism is fully established by a mapping $\sigma|_{\mathcal{X}} : \mathcal{X} \to M$.

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 $s, t \in (M \cup \mathcal{X})^*$. 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.

2.3 Varieties and pseudovarieties

The problem which we are interested in is a checking the validity of identities in a fixed finite monoid — a formal definition and its slight generalization are introduced in the next section. From the algebraic point of view any set of identities naturally corresponds to the class of all monoids which satisfy these identities. These classes are called *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. So, the problem of checking identities for the monoid M is just the identity problem for the variety $\langle M \rangle$.

For finite monoids there are another natural classes, so-called *pseudovarieties*, which are closed under taking submonoids, morphic images and finite products. We define pseudovarieties of semigroups and groups in the same way. In fact, not every pseudovariety of monoids is the class of finite members of some variety; for example the class of all finite groups forms a pseudovariety (we denote it $\mathbf{G}$), although the class of all groups does not form a variety. Some natural subclasses of $\mathbf{G}$ (nilpotent groups $\mathbf{G_{NIL}}$ for example) form also pseudovarieties.

There are certain natural operators on the pseudovarieties of monoids, semigroups and groups. For an arbitrary pseudovariety of groups $\mathbf{H}$ we denote by $\overline{\mathbf{H}}$ the class of all monoids whose all regular $\mathcal{H}$-classes are groups from the class $\mathbf{H}$. For any pseudovariety of semigroups $\mathbf{V}$ we denote by $\mathbf{DV}$ the pseudovariety of all monoids whose regular $\mathcal{J}$-classes lie in $\mathbf{V}$. For example, if $\mathbf{O}$ denotes the class of orthodox semigroups (a semigroup S is *orthodox* iff $E(S)$ is a subsemigroup), then a monoid M belongs to the class $\mathbf{DO}$ if and only if any regular $\mathcal{J}$-class of M is closed under products and any product of two idempotents is an idempotent. Equivalently, $M \in \mathbf{DO}$ if and only if for any $e, f \in E(M)$, $e \mathcal{J} f \implies ef \mathcal{R} e$. Another important example is the class $\mathbf{DA}$ of all finite monoids whose regular $\mathcal{J}$-classes are aperiodic subsemigroups (a semigroup is *aperiodic* if it contains only trivial subgroups).

For a pair of monoids M and N we write $N \prec M$ if and only if the monoid N is a morphic image of some submonoid of the monoid M, we say that the monoid N *divides* the monoid M in this case.

3 Term and polynomial equivalence problems

Definition 1. *Let M be a finite monoid. Given a pair of polynomials as an instance of the* POL-EQ(M) *problem, the task is to decide whether these polynomials are equivalent in M. The* TERM-EQ(M) *problem is the restriction of the* POL-EQ(M) *problem where only terms are considered.*

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 TERM-EQ(M) problem) is in 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 polynomials to these elements. This idea leads to consideration of the problem of solving equations in the monoid M.

Definition 2. *Let M be a finite monoid. Given a pair of polynomials u, v as an instance of the* EQN(M) *problem, the task is to decide whether there is a morphism $\sigma : (M \cup \mathcal{X})^* \to M$ which behaves as an identity on elements from M such that $\sigma(u) = \sigma(v)$. Given a pair of polynomials u, v and a pair of elements $m, n \in M$, the* 2T-EQN(M) *problem is to determine whether there is a morphism $\sigma : (M \cup \mathcal{X})^* \to M$ which behaves as an identity on elements from M such that $\sigma(u) = m$ and $\sigma(v) = n$.*

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

Lemma 2. *For any finite monoid M there are reductions of the* EQN(M) *and co* POL-EQ(M) *problems to the* 2T-EQN(M) *problem.* □

4 The Smallest Monoid with Hard TERM-EQ 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) problem to the case of the TERM-EQ problem.

Proposition 1. *The* TERM-EQ(B_2) *problem is coNP-complete.*

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

We reduce the problem 1-in-3-SAT into coTERM-EQ(B_2). Let $\Phi = C_1 \wedge C_2 \wedge \cdots \wedge C_k$ be an instance of the problem 1-in-3-SAT, where each clause C_r, $1 \leq r \leq k$, is of the form $l_1 \vee l_2 \vee l_3$ and any literal l_j, $1 \leq j \leq 3$, is a Boolean variable X or its negation $\neg X$. Recall that the question in the problem 1-in-3-SAT is whether there exists a valuation of Boolean variables such that for every clause $C_r = l_1 \vee l_2 \vee l_3$ of the formula Φ exactly one of the literals l_1, l_2 and l_3 is valuated by true. Let $\{X_1, X_2, \ldots, X_n\}$ be the set of all variables occurring in the formula Φ.

For any 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 a Boolean variable X_i and $\widetilde{l} = \overline{x}_i$ if the literal l is a negation of a Boolean variable X_i. We also introduce a variable y and put $\Sigma = \{y, x_1, \overline{x_1}, \ldots, x_n, \overline{x_n}\} \subset \mathcal{X}$.

Now, for any Boolean variable X_i with the corresponding variable x_i we define a term $w(X_i) = (yx_i\overline{x}_iy\overline{x}_ix_i)^2$ and for any clause $C_r = l_1 \vee l_2 \vee l_3$ we define a term $u(C_r) = (y\widetilde{l_1}\widetilde{l_2}\widetilde{l_3})^2$. Finally, we define $v = w(X_1) \ldots w(X_n)u(C_1) \ldots u(C_k)y$.
Claim: The instance Φ is satisfiable (in the sense of 1-in-3-SAT) if and only if there is a substitution $\sigma : \Sigma \to \mathrm{B}_2$ such that $\sigma(v)$ is not an idempotent, i.e. terms v^2 and v are not equivalent in the monoid B_2.

Proof of the claim: Let $\sigma : \Sigma \to B_2$ be such that $\sigma(v)$ is not an idempotent, i.e. $\sigma(v) = a$ or $\sigma(v) = b$. 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, i.e. $\sigma(w(X_i))$ and $\sigma(u(C_r))$ are idempotents. Because $\sigma(y) = a$ and y is contained in all $w(X_i)$ and $u(C_r)$, we see that $\sigma(w(X_i))$ and $\sigma(u(C_r))$ cannot be equal to 1 and we can deduce that $\sigma(w(X_i)) = \sigma(u(C_r)) = ab$. For any 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: X_i is true if $\sigma(x_i) = b$ (and $\sigma(\overline{x}_i) = 1$ at the same time) and X_i is false if $\sigma(x_i) = 1$ (and $\sigma(\overline{x}_i) = b$ at the same time). Now, for any clause $C_r = l_1 \vee l_2 \vee l_3$ exactly one of l_1, l_2 and l_3 is valuated by true, because otherwise $\sigma(u(C_r)) = 0$. Hence, the formula Φ is satisfiable.

If we assume that the formula Φ is satisfiable, then we can define the substitution $\sigma : \Sigma \to B_2$ in the following way. If X_i is true then we put $\sigma(x_i) = b$ and $\sigma(\overline{x}_i) = 1$; if X_i is false then we put $\sigma(x_i) = 1$ and $\sigma(\overline{x}_i) = b$; and finally we put $\sigma(y) = a$. So, for any 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, $\sigma(u(C_r)) = ab$, hence $\sigma(v) = a$ is not an idempotent. $\square$

If we look at the polynomial algorithm for the EQN problem for monoids from the class **DA** in the paper [1] we can see that its slight modification leads to the tractability of the POL-EQ(M) problem for any monoid $M \in \mathbf{DA}$. But we can also use a more general result given by P. Tesson in his PhD Thesis — 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 2 ([8]). *The* 2T-EQN(M) *problem is decidable in polynomial time for any monoid* $M \in \mathbf{DO} \cap \overline{\mathbf{G_{NIL}}}$.

We obtain the following statement as a direct consequence of Lemma 2.

Proposition 3. *The* POL-EQ(M) *problem is decidable in polynomial time for any 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. commutative monoids, idempotent monoids. As a side result we can also obtain the observation that the monoid B_2 is the smallest one with the hard TERM-EQ problem.

Proposition 4. *Let M be a monoid with at most five elements. Then the* POL-EQ(M) *problem is decidable in polynomial time.*

Proof. We show that any monoid of this size is inside the class $\mathbf{DO} \cap \overline{\mathbf{G_{NIL}}}$ and hence the statement is a consequence of Proposition 3. Let a monoid M have at most five elements. Then $M \in \overline{\mathbf{G_{NIL}}}$ because any non-nilpotent group has at least six elements. Assume that M is outside the class **DO**. Then there are $e, f \in E(M)$, $e\mathcal{J}f$ such that $ef \notin \mathcal{J}_e$ by Lemma 1-iv). We can see $\mathcal{L}_e \neq \mathcal{L}_f$ and $\mathcal{R}_e \neq \mathcal{R}_f$ by Lemma 1-vii). Hence $\mathcal{J}_e$ contains at least four elements and this is a contradiction with the number of elements of the monoid M, because $ef, 1 \notin \mathcal{J}_e$. $\square$

Note that any monoid outside $\mathbf{DO}$ is divided by B_2 or U. 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, U and S_3 (the permutation group over a three-element set). We show the tractability of the POL-EQ(U) problem in Lemma 3. The complexity of POL-EQ(S_3) has not been described yet. There is a quasipolynomial algorithm for a more general Program Satisfiability problem in [1] (see also [8]), but we believe we would be able to prove that the POL-EQ(S_3) problem is tractable. Hence B_2 should be the only monoid with at most six elements and hard TERM-EQ and POL-EQ problems.

Lemma 3. *The* POL-EQ(U) *problem is decidable in polynomial time.*

Proof. We construct a certain set $T_{u,v}$ of test morphisms which proves or disproves the equivalence of given polynomials u and v. More precisely, we prove that if there is a morphism σ such that $\sigma(u) \neq \sigma(v)$ then there is such a morphism in the set $T_{u,v}$. Note that the set $T_{u,v}$ depends on polynomials u and v, but always has a polynomial size.

Let $u, v \in (\mathrm{U} \cup \mathcal{X})^*$ be a pair of polynomials. Assume that there is a morphism σ such that $\sigma(u) \neq \sigma(v)$. We distinguish between several cases and for each of them we put certain test morphisms into the set $T_{u,v}$.

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 which does not occur in u and $\sigma(x) \neq 1$. In the first case we can consider the morphism τ which maps any variable to the element 1. In the second case we can consider the morphism σ_x mapping any variable to the element a except for x which is mapped to 0. In both cases we see that the images of u and v are different. We put the morphism τ and all the morphisms σ_x into the set $T_{u,v}$. The case when $\sigma(u) \neq 1$, $\sigma(v) = 1$ is also covered by these morphisms.

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), 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. $u = pku'$ or $u = pxu'$ where $k \in \{a, ab\}$, $x \in \mathcal{X}$, $u' \in (\mathrm{U} \cup \mathcal{X})^*$ and let q be the longest prefix of v such that $\sigma(q) = 1$, i.e. $v = qlv'$ or $v = qyv'$ where $l \in \{b, ba\}$, $y \in \mathcal{X}$, $v' \in (\mathrm{U} \cup \mathcal{X})^*$. Now we define a morphism $\sigma_{p,q}$ in the following way: $\sigma_{p,q}(x) = 1$ for all $x \in \mathrm{c}(p) \cup \mathrm{c}(q)$, $\sigma_{p,q}(y) = ba$ and $\sigma_{p,q}(z) = a$ otherwise. It is easy to see that $\sigma_{p,q}(u)\mathcal{R}\sigma(u)$ and $\sigma_{p,q}(v)\mathcal{R}\sigma(v)$, i.e. $\sigma_{p,q}(u) \neq \sigma_{p,q}(v)$. So, we put the morphism $\sigma_{p,q}$ into the set $T_{u,v}$ for any possible pair of prefixes of u and v.

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 $\sigma(x) = 0$ for some variable x, then x does not occur in u and we see that $\sigma_x(u)\mathcal{J}a$ but $\sigma_x(v) = 0$. So, we can 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 $\alpha, \beta \in \mathrm{U} \cup \mathcal{X}$, $w \in \mathcal{X}^*$ and $\sigma(\alpha) \in \{b, ab\}$, $\sigma(w) = 1$, $\sigma(\beta) \in \{b, ba\}$. We define a morphism $\sigma_{\alpha w \beta}$ in the following way $\sigma_{\alpha w \beta}(x) = 1$ for all $x \in \mathrm{c}(w)$, $\sigma_{\alpha w \beta}(\alpha) = ab$ if $\alpha \in \mathcal{X}$, $\sigma_{\alpha w \beta}(\beta) = ba$ if $\beta \in \mathcal{X}$ and $\sigma_{\alpha w \beta}(z) = a$ otherwise. We can see that $\sigma_{\alpha w \beta}(u)\mathcal{J}a$ but $\sigma_{\alpha w \beta}(v) = 0$ and put $\sigma_{w,x,y}$ into the set $T_{u,v}$. Because there is only polynomially many factors of u and v we have to put only polynomially many morphisms into $T_{u,v}$. $\square$

5 Reductions Between Problems

We have described certain monoids with tractable POL-EQ problem and an example of a monoid with hard TERM-EQ problem. In all these cases the complexity of the TERM-EQ and POL-EQ problems was the same. So, there is a natural question whether there exists a monoid M for which the TERM-EQ(M) problem is decidable in polynomial time but the POL-EQ(M) problem is coNP-complete. (Such a question makes sense only if $P \neq NP$. For that reason we assume $P \neq NP$ in the whole section.) The answer is "yes" and the example follows. The idea is to use the coNP-hardness of the POL-EQ(B_2) problem and extend the monoid B_2 to a monoid with tractable TERM-EQ problem but still with hard POL-EQ problem.

Proposition 5. *There is a monoid M such that the* TERM-EQ(M) *problem is decidable in polynomial time and the* POL-EQ(M) *problem is coNP-complete.*

Proof. We define a ten-element monoid

$$\begin{aligned}\mathrm{BU} = \langle a, b, c, d \mid\ & ac = ca = ad = da = bc = cb = bd = db = 0,\\ & a^2 = b^2 = d^2 = 0, c^2 = c, aba = a, bab = b, cdc = c, dcd = d\rangle.\end{aligned}$$

The monoid BU has a pair of submonoids isomorphic to B_2 and U, namely $S_B = \{1, a, b, ab, ba, 0\}$ and $S_U = \{1, c, d, cd, dc, 0\}$ and any product of an element from S_B and an element from S_U is 0 with the exception of the products where the neutral element 1 occurs. The crucial property of the monoid BU is that it generates the same variety of monoids as the monoid U does.

Lemma 4. $\langle \mathrm{U} \rangle = \langle \mathrm{BU} \rangle$.

Proof. It is easy to see that $\langle \mathrm{U} \rangle \subseteq \langle \mathrm{BU} \rangle$, because U is isomorphic to a submonoid of BU.

We prove the converse inclusion in two steps, namely we prove $\mathrm{B}_2 \prec \mathrm{U} \times \mathrm{U}$ and $\mathrm{BU} \prec \mathrm{B}_2 \times \mathrm{U}$.

Let $\mathrm{U} = \{1, c, d, cd, dc, 0\}$, where $c^2 = c$, $d^2 = 0$. We denote M the submonoid of the monoid $\mathrm{U} \times \mathrm{U}$ generated by the elements $a = (c, d)$ and $b = (d, c)$. The monoid M contains the elements $1_{\mathrm{U} \times \mathrm{U}} = (1, 1)$, a, b, $ab = (cd, dc)$, $ba = (dc, cd)$ and a certain subset I of elements with 0 on one of the coordinates, which is an ideal of M. Now, one can check that the mapping $\varphi : M \to \mathrm{B}_2$ given by the images of generators $\varphi(a) = a$, $\varphi(b) = b$ is a surjective morphism, i.e. B_2 is the Rees quotient of M by the ideal I. So, $\mathrm{B}_2 \prec \mathrm{U} \times \mathrm{U}$.

Analogically, we consider the ideal J of the monoid $\mathrm{B}_2 \times \mathrm{U}$ consisting of the elements which do not have any coordinate equal to 1 and of the elements $(0, 1)$ and $(1, 0)$. The monoid BU is the Rees quotient of $\mathrm{B}_2 \times \mathrm{U}$ by J, hence $\mathrm{BU} \prec \mathrm{B}_2 \times \mathrm{U}$. $\square$

Because $\langle \mathrm{BU} \rangle = \langle \mathrm{U} \rangle$, the TERM-EQ(BU) problem is equivalent to the TERM-EQ(U) problem, which is decidable in polynomial time as we have shown in Lemma 3.

For the second part of the statement we modify the proof of Proposition 1 — this modification is almost the original proof from [1]. Intuitively, we put to the definitions of terms (now polynomials) the element a instead of the variable y. In fact, the definitions are simpler overall, because we can not use powers. We can redefine $w(X) = ax\overline{x}a\overline{x}x$, $u(C_r) = a\widetilde{l_1}\widetilde{l_2}\widetilde{l_3}$, $v = w(X_1)\dots w(X_n)u(C_1)\dots u(C_k)a$ and consider the pair of polynomials v and 0 as the instance of the problem. $\square$

We have considered certain problems where we ask for existence of a substitution which distinguishes or identifies given polynomials. There is a natural question whether one of these problems can be reduced to another. In Lemma 2 we saw that the 2T-EQN(M) problem is more general than the EQN(M) and coPOL-EQ(M) problems. In what follows we discuss other possible reductions. We start with the case of groups.

Lemma 5. *Let M be a group. Then the co*POL-EQ(M) *problem can be reduced to the* EQN(M) *problem.*

Proof. Let M be a group of order r. We can rewrite any instance u, v of the coPOL-EQ(M) problem to the instance uv^{r-1}, 1 of the same problem. And there is a solution of this problem if and only if the equation $uv^{r-1} = a$ has a solution for some $a \neq 1$. $\square$

One can think that the tractability of the EQN(M) and POL-EQ(M) problems implies the tractability of the 2T-EQN(M) problem, but this is not true.

Proposition 6. *There is a monoid M such that both* EQN(M) *and* POL-EQ(M) *problems are decidable in polynomial time but the* 2T-EQN(M) *problem is NP-complete.*

Proof. The proof is not included due to space limitation. The example of such a monoid M_6 is given in Figure 2. The monoid M_6 is constructed in such a way that the subset $\{1, a_i, a_ib, ba_i, ba_ib, 0\}$ is a submonoid isomorphic to B_2 for $i = 1, 2$ and the subsets $\{1, a_i, a_ic_i, c_ia_i, c_i, 0\}$ and $\{1, c_i, c_ib, bc_i, bc_ib = ba_ib, 0\}$ are submonoids isomorphic to U for $i = 1, 2$ (particularly $a_i^2 = b^2 = 0, c_i^2 = c_i$). Then one can consider a pair of equations $w(X_1)\dots w(X_n)u(C_1)\dots u(C_k)a = a$ from the proof of Proposition 5 for both a_1, a_2 which has solution iff corresponding formula is satisfiable. $\square$

We complete this discussions with an example of a monoid having hard EQN problem but tractable POL-EQ problem.

Proposition 7. *There is a monoid M such that the* POL-EQ(M) *problem is decidable in polynomial time but the* EQN(M) *problem is NP-complete.*

Proof. Again, the proof is not included and the example can be viewed in Figure 2. Here, submonoid $\{1, a, b, ab, ba, 0\}$ of the monoid M_7 is B_2 which implies NP-completeness of the EQN(M_7) problem and elements $c_i^2 = c_i$ in submonoids isomorphic to U play the role of the element a in U. $\square$

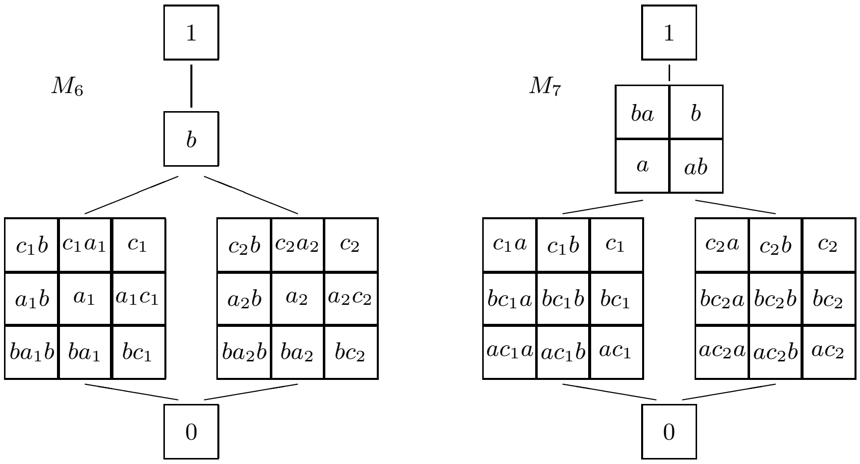

Fig. 2. The structure of the monoids M_6 and M_7.

6 Conclusion and Future Work

We have studied the problem of checking identities in finite monoids. Some results, methods and open questions for this problem are similar to those for the problem of solving equations. From this point of view it is important to compare these problems. We have given several examples which show that the complexities of these problems are independent. Our examples are quite complicated, so we may ask for simpler ones. We did not touch the special case of groups although we expect that the problem of checking identities is tractable at least for the six-element symmetric group.

I would like to thank Pascal Tesson for sending me his excellent PhD thesis and drawing my attention to his results concerning equations, and Michal Kunc for useful discussions.

References

[1] D. M. Barrington, P. McKenzie, C. Moore, P. Tesson and D. Thérien. Equation Satisfiability and Program Satisfiability for Finite Monoids. In Proceedings of MFCS'00, Vol. 1893 of LNCS (2000), 172–181.

[2] S. Burris and J. Lawrence. The equivalence problem for finite rings. J. of Symbolic Computation **15** (1993), 67–71.

[3] J. M. Howie. Fundamentals of Semigroup Theory, Oxford University Press, (1995).

[4] H. Hunt and R. Stearns. The complexity for equivalence for commutative rings. J. of Symbolic Computation **10** (1990), 411–436.

[5] S. Seif and C. Szabó. Algebra complexity problems involving graph homomorphism, semigroups and the constraint satisfaction problem. Journal of Complexity **19**/2 (2003), 153–160.

[6] S. Seif and C. Szabó. The computational complexity of checking identities in simple semigroups and matrix semigroups over finite fields. (submitted)

[7] C. Szabó and V. Vértesi. The Complexity of the Word Problem for finite matrix rings. (submitted)

[8] P. Tesson. Computational Complexity Questions Related to Finite Monoids and Semigroups. Ph.D. Thesis available at `http://www.cs.mcgill.ca/~ptesso/`.