Complexity of Checking Identities in Monoids of Partial Transformations [1]

Ondřej Klíma[2]

History of the paper In 2007 I have started to write this paper and then I realized that Almeida,Volkov and Goldberg wrote the article [1]. Since results from [1] cover some of my results, I stoped improving of the paper and I moved my attantion to the missing case $\mathbb{T}_4$. Consequently, I prepared paper [10]. Since the intersection of what follows with [1] is not large, still the paper contains many original results. Hopefully, one day I return to the paper and prepare a final version of it. Or maybe, the material contained in this paper would distribute to another papers on the topic.

One can recognize that some of the proving techniques used here are those from [10].

Abstract We study the computational complexity of checking identities in a fixed finite monoid. In this paper we concentrate on the case of monoids of transformations. We prove that the problem of checking identities in the monoid of all transformations of a two-element set is decidable in polynomial time, but the same problem is coNP-complete for the monoid of all transformations of three-element set, five-element set and any larger set. Similar results are established for monoids of all partial transformations and monoids of injective partial transformations.

Keywords Checking identities, Finite semigroups, Complexity

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 (TERM-EQ) 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(()M) problem asks to decide for a given pair of polynomials whether the product of the sequences is equal in M under any assignment of variables. Easily the problems are in the complexity class coNP, therefore the

[1] The author was supported by the Ministry of Education of the Czech Republic under the project MSM 0021622409 and by the Grant no. 201/09/1313 of the Grant Agency of the Czech Republic.

[2] O.Klíma
Department of Mathematics and Statistics, Masaryk University, Kotlářská 2, 611 37 Brno, Czech Republic,
klima@math.muni.cz, http://www.math.muni.cz/~klima

goal of the study is an observation for which monoids the problems are decidable in polynomial time and for which when they are coNP-complete. Of course, these questions are interesting only under the assumption that coNP≠P (and NP≠P) which we will assume throughout the paper. (See [13] for an introduction to complexity theory.)

The Polynomial Equivalence problem was studied also in ring theory where a dichotomy theorem was proved by Hunt and Stearns [8] for finite commutative rings and later by Burris and Lawrence [3] in the general case: a ring has tractable Polynomial Equivalence problem if it is nilpotent and this problem is hard otherwise. 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 it is coNP-complete for non-solvable groups. Probably other researchers stated these observations but upto our knowledge it is contained only in the recent paper [5].

An interesting case which can be studied is the case of the group of all permutations of an n-element set, denoted by $\mathbb{S}_n$. The Polynomial Equivalence problem is tractable for $\mathbb{S}_2$ trivially and the tractability was also proved for $\mathbb{S}_3$ [6]. On the other side, $\mathbb{S}_n$ is a non-solvable group for $n \geq 5$ and hence the Term Equivalence problem is coNP-complete for these groups. Finally, the complexity of the identity checking problem for $\mathbb{S}_4$ is an interesting open problem. Description of the complexity of the TERM-EQ($\mathbb{S}_4$) problem could help to better understanding of checking identities in solvable non-nilpotent groups.

In the case of semigroups and monoids the study of the identity checking problem were started by Popov and Volkov [14]. From a variety of papers touching this topic we can mentioned for example papers concerning completely 0-simple semigroups and matrix semigroups over finite fields [16, 17]. In [18] Szabó and Vértesi 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 [9] the author mentioned a significant class of finite monoids for which the problem is tractable and found the smallest monoid for which this problem is coNP-complete, namely the six-element Brandt monoid. The letter observation was independently made by Seif [15]. The natural representation of the Brandt monoid, which was applied in [9], used partial transformations of a two-element set. More precisely, the Brandt monoid consists of all partial transformations of a two-element set having one-element domain, together with the empty transformation and the identity transformation.

In this paper we continue the study of the Term and Polynomial Equivalence problems for small monoids. As natural extensions of the techniques used in [9], we try to describe the complexity of the problems for monoids of transformations. For example, if we add to the Brandt monoid one element corresponding to the non-identical permutation of the two-element set, then we obtain a seven-element monoid with a tractable Polynomial Equivalence problem. This monoid is, in fact, the monoid of all injective partial transformations of a two-element set. But if we consider the monoid of all partial transformations of a two-element set, then the Term Equivalence problem is coNP-complete again.

These results are parts of the present paper. If we denote by $\mathbb{T}_n$ the monoid of all transformations of an n-element set X_n, $\mathbb{PT}_n$ the monoid of all partial transformations of X_n and $\mathbb{I}_n$ the monoid of all injective transformations of X_n then the results of the paper are following. The Polynomial Equivalence problem is decidable in polynomial time for monoids $\mathbb{T}_2$ and $\mathbb{I}_2$ and is coNP-complete for monoids $\mathbb{T}_n$ and $\mathbb{I}_n$ for $n \geq 3$. Analogically, the Polynomial Equivalence problem is coNP-complete for all monoids $\mathbb{PT}_n$ for $n \geq 2$. We prove the same result for the Term Equivalence problem with the exception $n = 4$. We strongly believe that our method of the proof for the case $n = 3$ can be modified for the missing case $n = 4$, but such modification would be probably too technical.

Note that the monoids of transformations play the important role in theory of representation of semigroups. It is well-known that for any finite group there is an injective morphism from this group to some group $\mathbb{S}_n$. The same is true in the case of semigroups for the monoids $\mathbb{T}_n$. The monoids $\mathbb{I}_n$ play the same role in the class of inverse semigroups.

In the paper we will also study one problem which is really close to the identity checking problem, namely the problem of solving of single equation. Usually the techniques which can be used for solving of single equations can help also in the case of identities and also the hardness results can be obtained for both problems in a similar way. For example in paper [2] it was shown that the problem of solving one equation in the Brandt monoid is NP-hard. By the modification of the proof of this result the author obtained the coNP-hardness for the identity checking problem.

We should mentioned that for the problem of solving system there are more complete results. A dichotomy theorem was proved in the case of systems of equations over finite groups [4]: a group has tractable problem of solving systems of equations if it is commutative and this problem is NP-hard otherwise. The case of monoids and semigroups was studied in [12] and [11] where some dichotomy theorems were established and also an interesting connections to constrain satisfaction problem were studied.

Some of these mentioned results will be used in this paper to help prove our results. Note that we are really far from establishing an analogical dichotomy theorem in the case of one equation or the identity checking problem.

The structure of the paper is the following. In the second preliminary section we fix notation and recall known results. In Section 3 we concentrate to the case of monoids of transformation on two elements set. Then, in Section 4, we interrupt the results concerning concrete monoids and we establish few general reductions between studied problems in the case of an arbitrary n-elements set. In Section 5 we present hardness results concerning three elements set. Finally, in the last section we summerize the results and we discuss few questions which could be solve in the future research.

2 Preliminaries

2.1 Definition of the problems

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 $\mathtt{var}(u)$ the set of all variables from $\mathcal{X}$ which occur in u and $\mathtt{con}(u)$ the set of all constants from M which occur in u.

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.*

The TERM-EQ(M) problem is also called the identity checking problem for M, because the instance of the problem is an identity and the question is whether this identity is satisfied in 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 TERM-EQ(M) problem) is in coNP.

It is natural to consider an analog of the POL-EQ(M) problem namely problem of solving equations. The reasons are basically two; there are reductions between mentioned problems on one side and the proving techniques are usually same on the other side.

Definition 2. *Let M be a finite monoid. Given a finite set of pairs of polynomials $\{(u_i, v_i) \mid u_i, v_i \in (M \cup \mathcal{X})^*, i = 1, 2 \ldots, m\}$ as an instance of the* S-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 $\sigma(u_i) = \sigma(v_i)$ for all $i = 1, 2 \ldots, m$. The* EQN(M) *problem is the restriction of the* S-EQN(M) *problem where just one equation is considered, i.e $m = 1$.*

Again, the defined problems are trivially in NP. The following observation is easy exercise.

Lemma 1 ([9]). *Let M be a group. Then the co*POL-EQ(M) *problem can be reduced to the* EQN(M) *problem.*

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. The EQN(M) problem can be solved in the same way but the considered pairs are not different. This idea leads to consideration of the following problem.

Definition 3. *Let M be a finite monoid. 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.

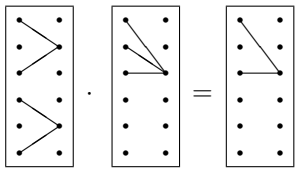
Lemma 2. *For any finite monoid M there are polynomial reductions of the* EQN(M) *and co*POL-EQ(M) *problems to the* 2T-EQN(M) *problem.* □

2.2 Monoids of transformations

In this paper we will study complexity issues of the defined problems for monoids of transformations. For an arbitrary finite set A, the monoid of all transformations of A is denoted by $\mathbb{T}_A$, the monoid of all partial transformations of A is denoted by $\mathbb{PT}_A$, the monoid of all injective partial transformations of A is denoted by $\mathbb{I}_A$ and the group of all permutations of A is denoted by $\mathbb{S}_A$. For a natural number n we denote the set $X_n = \{1, 2, \ldots, n\}$ and write $\mathbb{T}_n$ instead of $\mathbb{T}_{X_n}$ and so on.

For any $n \in \mathbb{N}$ the inclusions $\mathbb{S}_n \subseteq \mathbb{T}_n \subseteq \mathbb{PT}_n$ and $\mathbb{S}_n \subseteq \mathbb{I}_n \subseteq \mathbb{PT}_n$ are clear and we have also $\mathbb{S}_n = \mathbb{T}_n \cap \mathbb{I}_n$. Because $X_n \subseteq X_{n+1}$ we also have the inclusions $\mathbb{PT}_n \subseteq \mathbb{PT}_{n+1}$ and $\mathbb{I}_n \subseteq \mathbb{I}_{n+1}$. For $A \subseteq X_n$ we also

We represent an element of the set $\mathbb{PT}_n$, i.e. a partial mapping from the set X_n into itself, as a sequence of the values of the single elements of the set X_n. For example $\langle 13 - 2 \rangle$ represents a partial mapping $f \in \mathbb{PT}_4$ with domain $\{1, 2, 4\}$ such that $f(1) = 1$, $f(2) = 3$ and $f(4) = 2$. We will denote the operation composition of transformations by the symbol $\cdot$ which we will usually omitted. We will compose transformations from left to right, which means that for $a, b \in \mathbb{PT}_n$ and $x \in X_n$ we define $(a \cdot b)(x)$ by the rule $(a \cdot b)(x) = b(a(x))$. For example we have $\langle 2 - 25 - 5 \rangle \cdot \langle 333 - -- \rangle = \langle 3 - 3 - -- \rangle$ in $\mathbb{PT}_6$. The reason is that we will use a graphic presentation of transformations where points are mapped from left to right. E.g. the previous equality will be drown in the following way.



Sometimes we will also use the standard notation of domains and images of transformations, i.e. for $f \in \mathbb{PT}_n$ we denote $\mathrm{Dom}(f) = \{x \in X_n \mid f(x) \text{ is defined } \}$ and $\mathrm{Im}(f) = \{f(x) \mid x \in X_n\}$. For a set A we denote by $|A|$ the number of elements of A.

2.3 Known results

We recall useful known results.

Proposition 1 ([4]). *If G is a finite group the* S-EQN(G) *problem is computable in polynomial time if G is commutative and is NP-complete otherwise.*

Notice that for a moniod M the S-EQN(M) problem is computable in polynomial time if M is commutative and is the union of its subgroups and is NP-complete otherwise (see [12, 11]).

The case of a single equation or identity is less complete.

Proposition 2 ([4]). *Let G be a finite group. If G is nilpotent then the* EQN(G) *problem is decidable in polynomial time. If G is non-solvable then* EQN(G) *is coNP-complete.*

The analogical result for term equivalence problem is mentioned many times in literature and the result is attributed to Lawrence. The part of decidability for nilpotent groups follows from Proposition 2 and Lemma 1. Up to our knowledge the complete proof of coNP-hardness for non-solvable groups is written only in the paper [5].

Proposition 3 ([5]). *If G is a finite, non-solvable group, then the* TERM-EQ(G) *problem is coNP-complete.*

Small monoids are inside the significant class of monoids for which a polynomial algorithm for the 2T-EQN(M) problem is known.[3] This result is contained implicitly in [19].

Proposition 4 ([9, 19]). *Let M be a finite monoid with at most five elements. Then the* 2T-EQN(M) *problem is decidable in polynomial time. In particular, the* EQN(M), TERM-EQ(M) *and* POL-EQ(M) *problems are decidable in polynomial time.*

3 The case of transformations of two-element set

For the two-element group $\mathbb{S}_2$ all the problems are tractable, because $\mathbb{S}_2$ is a commutative group for which we have Proposition 1. The monoid $\mathbb{T}_2$ has four elements and the tractability follows from Proposition 4. Both these observations are simple and they can also be proved directly. The case of $\mathbb{I}_2$ and $\mathbb{PT}_2$ is more complicated. We start with injective partial transformations.

[3] This class is $\mathbf{DO} \cap \overline{\mathbf{G_{Nil}}}$.

3.1 The case of the monoid $\mathbb{I}_2$

Lemma 3. *The* 2T-EQN($\mathbb{I}_2$) *problem is decidable in polynomial time.*

Proof. The monoid $\mathbb{I}_2$ has seven elements:

$$\mathbb{I}_2 = \{\langle --\rangle, \langle 1-\rangle, \langle 2-\rangle, \langle -1\rangle, \langle -2\rangle, \langle 12\rangle, \langle 21\rangle\}.$$

The commutative group $\mathbb{S}_2 = \{\langle 12\rangle, \langle 21\rangle\}$ is a submonoid of the monoid $\mathbb{I}_2$. We denote $I = \{\langle 1-\rangle, \langle 2-\rangle, \langle -1\rangle, \langle -2\rangle\}$ and $I_0 = I \cup \{\langle --\rangle\}$. The set I_0 is an ideal of the monoid $\mathbb{I}_2$, i.e. for any $s \in \mathbb{I}_2, t \in I_0$ we have $st, ts \in I_0$. The empty transformation $\langle --\rangle$ is a zero element of the monoid $\mathbb{I}_2$, i.e. for any $s \in \mathbb{I}_2$ we have $\langle --\rangle \cdot s = s \cdot \langle --\rangle = \langle --\rangle$.

We consider the natural ordering on the set $\mathbb{I}_2$, namely ordering by the inclusion $\subseteq$ if we interpret transformations as relations, i.e. subsets of the set $X_2 \times X_2$. Moreover, $(\mathbb{I}_2, \cdot, \subseteq)$ is an ordered monoid; this means that the following condition is satisfied:

$$\forall a, b, c \in \mathbb{I}_2 : \quad a \subseteq b \implies ac \subseteq bc, ca \subseteq cb.$$

The basic idea of the algorithm is that we are looking for solutions which are maximal with respect to the ordering $\subseteq$. Such solutions will map almost all variables into $\mathbb{S}_2$. Recall that we are able to solve the S-EQN($\mathbb{S}_2$) problem in polynomial time.

Let $u, v \in (\mathcal{X} \cup \mathbb{I}_2)^*$ and $m, n \in \mathbb{I}_2$ form an instance of the 2T-EQN($\mathbb{I}_2$) problem. We distinguish certain cases depending on m and n. In any of them we show that there is a solution of the instance if and only if there is a solution of a special form which can be computed in polynomial time.

Case 1: $m = n = \langle --\rangle$.

The system is not solvable if and only if u or v is an element from $\mathbb{I}_2$ different from the element $\langle --\rangle$. This can be easily check.

Case 2: $m, n \in \mathbb{S}_2$.

Then for any solution σ of the instance we have $\sigma(x) \in \mathbb{S}_2$ for any variable $x \in \mathtt{var}(u) \cup \mathtt{var}(v)$ and $\mathtt{con}(u) \cup \mathtt{con}(v) \subseteq \mathbb{S}_2$. So, we can find this solution as a solution of the system of two equations over $\mathbb{S}_2$.

Case 3: $m \in I, n \in \mathbb{S}_2$.

Assume that $\sigma : \mathcal{X} \to \mathbb{I}_2$ is a solution of the instance. Then there is a variable $x \in \mathtt{var}(u)$ such that $\sigma(x) \in I$ or there is a constant $k \in \mathtt{con}(u)$ such that $k \in I$. We will discuss these two cases separately. Moreover, in the first case we consider separately all possibilities, i.e pairs consisting from a variable $x \in \mathtt{con}(u)$ and a value $\sigma(x) = k \in I$. For any such possibility we substitute k for all occurrences of x in u and denote the resulting polynomial $\overline{u}$. Altogether we discuss separately polynomialy many cases and in each of them we solve a pair of equations $\{(\overline{u}, m), (v, n)\}$ where $m \in I, n \in \mathbb{S}_2$ and $\mathtt{con}(\overline{u}) \cap I \neq \emptyset$.

Let we have such instance and still assume that σ is a solution. If we consider all occurrences of the constants from the set I in the polynomial $\overline{u}$ we obtain the following factorization of the polynomial $\overline{u}$:

$$\overline{u} = u_1 k_1 u_2 k_2 \dots k_p u_{p+1}, \quad \text{where } u_i \in (\mathcal{X} - \{x\} \cup \mathbb{S}_2)^*, k_i \in I.$$

Claim: there is a substitution $\sigma' : \mathcal{X} \to \mathbb{S}_2$ such that $\sigma'(\overline{u}) = \sigma(\overline{u})$ and $\sigma'(v) = \sigma(v)$.

It is easy to see that $\sigma(y) \neq \langle -- \rangle$ for any $y \in \mathtt{var}(\overline{u})$. Now if $\sigma(y) \in \mathbb{S}_2$ then we put $\sigma'(y) = \sigma(y)$; if $\sigma(y) = \langle 1- \rangle$ or $\sigma(y) = \langle -2 \rangle$ then we put $\sigma'(y) = \langle 12 \rangle$; and if $\sigma(y) = \langle 2- \rangle$ or $\sigma(y) = \langle -1 \rangle$ then we put $\sigma'(y) = \langle 21 \rangle$. This means that $\sigma(y) \subseteq \sigma'(y)$ for any $y \in \mathtt{var}(\overline{u})$ and hence $\sigma(u_i) \subseteq \sigma'(u_i)$. It follows that $\sigma(\overline{u}) \subseteq \sigma'(\overline{u})$. Because $\sigma'(\overline{u}) \in I_0$ we have $\sigma(\overline{u}) = \sigma'(\overline{u})$. The second observation $\sigma'(v) = \sigma(v)$ is trivial and we have proved the claim.

If we look on the factorization of $\overline{u}$ we see that elements $k_i \in I$ have a one-element domain and also a one-element image. Hence the values $m_i = \sigma'(u_i) \in \mathbb{S}_2$ are determined by $\overline{u}$. More precisely $m_i \in \mathbb{S}_2$ is determined by $k_{i-1} \in I$ and $k_i \in I$ for $i = 2, \dots p$; m_1 is determined by $\mathrm{Dom}(m)$ and k_1 and finally m_{p+1} is determined by k_p and $\mathrm{Im}(m)$. This means that we are looking for a substitution $\sigma' : \mathcal{X} \to \mathbb{S}_2$ which is a solution of the system $\{(u_i, m_i) \mid i = 1, 2, \dots, p+1\} \cup \{(v, n)\}$.

So, we reduce the case $m \in I, n \in \mathbb{S}_2$ to solving linearly many systems of equations over $\mathbb{S}_2$.

Case 4: $m = \langle -- \rangle$, $n \in \mathbb{S}_2$.

At first if there is a variable $x \in \mathtt{var}(u)$ such that $x \notin \mathtt{var}(v)$ then the instance is solvable if and only if the equation (v, n) is solvable in $\mathbb{S}_2$. The same is true if $\langle -- \rangle \in \mathtt{con}(u)$.

So, assume that $\langle -- \rangle \notin \mathtt{con}(u)$ and let $\sigma : \mathcal{X} \to I \cup \mathbb{S}_2$ be a solution of the instance.

We denote some factor w of the polynomial u which is the shortest factor of u with respect to the property $\sigma(w) = \langle -- \rangle$. This means that for any proper factor w' of the polynomial w we have $\sigma(w') \neq \langle -- \rangle$.

Claim: If $w = w_1 w_2 \dots w_p$, where $w_i \in \mathcal{X} \cup I \cup \mathbb{S}_2$, then $\sigma(w_1), \sigma(w_p) \in I$ and $\sigma(w_i) \in \mathbb{S}_2$ for any $i = 2, \dots, p-1$.

Indeed, we have assumed $\langle -- \rangle \notin \mathtt{con}(u)$ and $\sigma(x) \neq \langle -- \rangle$ for all $x \in \mathtt{var}(u)$. Now, because $\sigma(w_1 w_2 \dots w_{p-1}) \neq \langle -- \rangle$ and $\sigma(w_1 w_2 \dots w_p) = \langle -- \rangle$ we can see that $\sigma(w_p) \in I$. Analogically $\sigma(w_1) \in I$. We denote $s = \sigma(w_2 \dots w_{p-1})$ and we show that $\mathrm{Im}(s) = X_2$. Let $a \in \mathrm{Dom}(\sigma(w_p))$ then $a \in \mathrm{Im}(s)$ otherwise $s \cdot \sigma(w_p) = \langle -- \rangle$. Analogically if $b \in \mathrm{Im}(\sigma(w_1))$ then $b \in \mathrm{Dom}(s)$. But $s(b) \neq a$ because $\sigma(w_1) \cdot s \cdot \sigma(w_p) = \langle -- \rangle$. Hence $\mathrm{Im}(s) = X_2$, which means $s \in \mathbb{S}_2$ and this implies the property $\sigma(w_i) \in \mathbb{S}_2$ for any $i = 2, \dots, p-1$. So, the claim is proved.

This means that for any factor $w = w_1 w_2 \dots w_p$ of u we consider all possible values $a \in I$, $b \in \mathbb{S}_2$, $c \in I$, such that $abc = \langle -- \rangle$ and put $\sigma(w_1) = a$, $\sigma(w_n) = c$ and then we solve the system of the two equations $\{(w_2 \dots w_{n-1}, b), (v, n)\}$ in the group $\mathbb{S}_2$. Clearly, there are polynomialy many factors of u, i.e. we have to discuss only polynomialy many cases.

Case 5: $m = \langle -- \rangle$, $n \in I$.

We have to combine methods from cases 3 and 4. We distinguish polynomialy many cases for both equations and in any of them we obtain the pair of systems

of equations over $\mathbb{S}_2$. At the end we simply put these systems together and solve in $\mathbb{S}_2$.

Case 6: $m, n \in I$.

We use method from case 3 for both equations.

Conclusion

We distinguish polynomial many cases and in any of them we check easy condition (case 1) or solve certain system of equations in $\mathbb{S}_2$. □

The previous lemma has the following consequence if we apply Lemma 2.

Proposition 5. *The* POL-EQ($\mathbb{I}_2$) *problem, the* TERM-EQ($\mathbb{I}_2$) *problem and the* EQN($\mathbb{I}_2$) *problem are decidable in polynomial time.*

3.2 The case of the monoid $\mathbb{PT}_2$

We prove that all considered problems are hard in the case of monoid $\mathbb{PT}_2$.

Proposition 6. *The* EQN($\mathbb{PT}_2$) *problem is NP-complete and the* TERM-EQ($\mathbb{PT}_2$) *problem (and hence also the* POL-EQ($\mathbb{PT}_2$) *problem) is coNP-complete.*

Proof. First of all, we recall the structure of the monoid $\mathbb{PT}_2$. The monoid $\mathbb{PT}_2$ has nine elements: $\mathbb{PT}_2 = \mathbb{I}_2 \cup \{\langle 11\rangle, \langle 22\rangle\}$. The commutative group $\mathbb{S}_2 = \{\langle 12\rangle, \langle 21\rangle\}$ is a submonoid of the monoid $\mathbb{PT}_2$.

We will show the polynomial reduction from the well-known NP-complete problem 3-SAT to the coTERM-EQ($\mathbb{T}_2$) problem. As we will see the reduction from the 3-SAT problem to the EQN($\mathbb{PT}_2$) problem can be made in the same way. At first we recall the definition of the 3-SAT problem (see [13] for more details).

An instance of the 3-SAT problem is a conjunction $\Phi \equiv \Phi_1 \wedge \Phi_2 \wedge \ldots \wedge \Phi_p$ of clauses and each clause Φ_i, $1 \leq i \leq p$, 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 *variable* from the set *Var*, possibly negated — we call it *positive* resp. *negative* literal). A *valuation* is a mapping $\nu : Var \to \{T, F\}$. Every valuation extends naturally to Φ and we say that Φ is *satisfiable* if and only if there exists a valuation ν such that $\nu(\Phi) = T$. The question of the 3-SAT problem is whether a given formula Φ is satisfiable.

Let Φ be an instance of the 3-SAT problem. We construct a pair of terms $L, R \in \mathcal{X}^*$ which are equivalent if and only if the formula Φ is not satisfiable, in other words the formula Φ will be satisfiable if and only if there is a substitution $\sigma : \mathcal{X} \to \mathbb{PT}_2$ such that $\sigma(L) \neq \sigma(R)$.

Assume that $Var = \{x_1, \ldots, x_r\}$ is a set of all boolean variables occurring in the formula Φ and for any $i = 1, \ldots, r$ introduce four variables $x_i, \overline{x}_i, y_i, \overline{y}_i \in \mathcal{X}$. We take two other variables $a, b \in \mathcal{X}$ and we will assume that all these variables are pairwise different. For a positive literal $l = x$ we define $\widetilde{l} = x$ and for a negative literal $l = \neg x$ we define $\widetilde{l} = \overline{x}$.

Now, for a boolean variable $x \in Var$ we define the following terms

$$v_1^x = b(ax^2)^2b(a\overline{x}^2)^2b, \quad v_2^x = by\overline{y}ab\overline{y}yabay\overline{y}ba\overline{y}yb, \quad v_3^x = bax^2\overline{x}^2b,$$

$$v_4^x = byx^2\overline{y}ab\overline{yx}^2yab \quad \text{and} \quad v^x = v_1^x v_2^x v_3^x v_4^x.$$

For each clause $\Phi_i \equiv l_1 \vee l_2 \vee l_3$, $1 \leq i \leq p$, we define term

$$u_i = ba \cdot \widetilde{l_1}^2\widetilde{l_2}^2\widetilde{l_3}^2 \cdot b.$$

Finally, we denote

$$A = a^3b^2a^3b^2, \quad B = a^2b^2a^2b^2, \quad V = v^{x_1}v^{x_2}\dots v^{x_r} \cdot u_1u_2\dots u_p \ ,$$

and

$$L = VA, \quad R = VB.$$

In the rest of the proof we show that the formula Φ is satisfiable if and only if there is a substitution $\sigma : \mathcal{X} \to \mathbb{PT}_2$ such that $\sigma(L) \neq \sigma(R)$.

Let $\nu : Var \to \{T, F\}$ be a valuation such that $\nu(\Phi) = T$. We define $\sigma(a) = \langle 21\rangle$, $\sigma(b) = \langle 1-\rangle$. Then we can compute $\sigma(A) = \langle --\rangle$ and $\sigma(B) = \langle 1-\rangle$. Further, for any boolean variable $x \in Var$ such that $\nu(x) = T$ we define $\sigma(x) = \langle 11\rangle$, $\sigma(\overline{x}) = \langle 12\rangle$, $\sigma(y) = \langle 12\rangle$ and $\sigma(\overline{y}) = \langle 21\rangle$. Then for such $x \in Var$ we can see that $\sigma(v_1^x) = \langle 1-\rangle$, $\sigma(v_2^x) = \langle 1-\rangle$, $\sigma(v_3^x) = \langle 1-\rangle$, $\sigma(v_4^x) = \langle 1-\rangle$ and hence $\sigma(v^x) = \langle 1-\rangle$. For any $x \in Var$ such that $\nu(x) = F$ we define $\sigma(x) = \langle 12\rangle$, $\sigma(\overline{x}) = \langle 11\rangle$, $\sigma(y) = \langle 21\rangle$ and $\sigma(\overline{y}) = \langle 12\rangle$. Then we can analogically compute $\sigma(v_1^x) = \langle 1-\rangle$, $\sigma(v_2^x) = \langle 1-\rangle$, $\sigma(v_3^x) = \langle 1-\rangle$, $\sigma(v_4^x) = \langle 1-\rangle$ and hence $\sigma(v^x) = \langle 1-\rangle$ again. Now, we have to compute values $\sigma(u_i)$. Because for any clause $\Phi_i \equiv l_1 \vee l_2 \vee l_3$ we have $\sigma(\widetilde{l_1}), \sigma(\widetilde{l_2}), \sigma(\widetilde{l_3}) \in \{\langle 11\rangle, \langle 12\rangle\}$ and because at least one of the literals l_1, l_2, l_3 is valuated by T we know, that at least one of the values $\sigma(\widetilde{l_1}), \sigma(\widetilde{l_2}), \sigma(\widetilde{l_3})$ is equal to $\langle 11\rangle$ hence $\sigma(\widetilde{l_1}^2\widetilde{l_2}^2\widetilde{l_3}^2) = \langle 11\rangle$. From that reason $\sigma(u_i) = \langle 1-\rangle$ for any $i = 1, \dots, p$. So, we can finish our computations with conclusion that $\sigma(V) = \langle 1-\rangle$ and hence $\sigma(L) = \langle --\rangle \neq \langle 1-\rangle = \sigma(R)$.

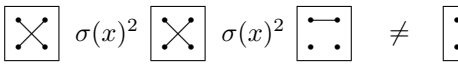
Let us suppose that $\sigma : \mathcal{X} \to \mathbb{PT}_2$ is an arbitrary substitution which disprove the equivalence of the terms L, R, i.e. $\sigma(L) \neq \sigma(R)$. We find a valuation ν which satisfies Φ.

At first, $\sigma(L) \neq \sigma(R)$ implies $\sigma(A) \neq \sigma(B)$ and consequently $\sigma(a)^3 \neq \sigma(a)^2$. If we check all the elements in the monoid $\mathbb{PT}_2$ we observe that there is a unique element $e \in \mathbb{PT}_2$ with the property $e^3 \neq e^2$, namely $e = \langle 21\rangle$. Hence $\sigma(a) = \langle 21\rangle$ and we have

 $\sigma(b)^2$  $\sigma(b)^2 \quad \neq \quad \sigma(b)^2 \quad \sigma(b)^2$.

One can check that this implies $\sigma(b) \in \{\langle 1-\rangle, \langle -2\rangle\}$. We will assume that $\sigma(b) = \langle 1-\rangle$ because if $\sigma(b) = \langle -2\rangle$ then the following discussion can be done dually.

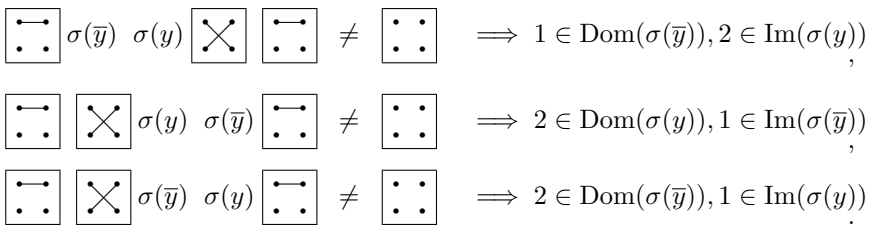
So, we suppose that $\sigma(a) = \langle 21\rangle$, $\sigma(b) = \langle 1-\rangle$ and $\sigma(V) \neq \langle --\rangle$. Let x be a boolean variable. Then we have $\sigma(v^x) \neq \langle --\rangle$. Because $\sigma(v_1^x) \neq \langle --\rangle$ and $(ax^2)^2 b$ is a factor of v_1^x we see



One can check that $\{e^2 \mid e \in \mathbb{PT}_2\} = \{\langle 12\rangle, \langle 1-\rangle, \langle 11\rangle, \langle -2\rangle, \langle 22\rangle, \langle --\rangle\}$ and from previous inequality we have $\sigma(x)^2 \in \{\langle 12\rangle, \langle 11\rangle\}$. The same can be proved for $\overline{x}$, i.e $\sigma(\overline{x})^2 \in \{\langle 12\rangle, \langle 11\rangle\}$.

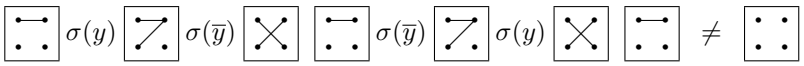
Now, we look at the inequality $\sigma(v_2^x) \neq \langle --\rangle$. For a prefix of $\sigma(v_2^x)$ we obtain the inequality

It follows that $1 \in \mathrm{Dom}(\sigma(y))$ and $2 \in \mathrm{Im}(\sigma(\overline{y}))$. Analogically, from other factors of $\sigma(v_2^x)$ we obtain



Altogether, we deduce $\mathrm{Dom}(\sigma(y)) = \mathrm{Dom}(\sigma(\overline{y})) = \mathrm{Im}(\sigma(y)) = \mathrm{Im}(\sigma(\overline{y})) = X_2$ and we can conclude $\sigma(y), \sigma(\overline{y}) \in \mathbb{S}_2$. Moreover, from any mentioned inequality we see that $\sigma(y)\sigma(\overline{y}) = \langle 21\rangle$, hence $\{\sigma(y), \sigma(\overline{y})\} = \mathbb{S}_2$, particularly $\sigma(y) \neq \sigma(\overline{y})$.

Now, we show $\sigma(x)^2 \neq \sigma(\overline{x})^2$. We have already seen that both $\sigma(x)^2$ and $\sigma(\overline{x})^2$ belong to the set $\{\langle 12\rangle, \langle 11\rangle\}$. If $\sigma(x)^2 = \sigma(\overline{x})^2 = \langle 12\rangle$ then $\sigma(v_3^x) = \langle --\rangle$ which is a contradiction. Assume for a moment that $\sigma(x)^2 = \sigma(\overline{x})^2 = \langle 11\rangle$. Then from $\sigma(v_4^x) \neq \langle --\rangle$ we have



and this implies that both $\sigma(y)$ and $\sigma(\overline{y})$ are equal to $\langle 21\rangle$ which is a contradiction with the previous paragraph. We have proved that $\{\sigma(x)^2, \sigma(\overline{x})^2\} = \{\langle 12\rangle, \langle 11\rangle\}$.

This means that we can define consistent valuation $\nu : Var \to \{T, F\}$ in the following way. If $\sigma(x)^2 = \langle 11\rangle$ (and $\sigma(\overline{x})^2 = \langle 12\rangle$) at the same time, then we define $\nu(x) = T$ and if $\sigma(x)^2 = \langle 12\rangle$ (and $\sigma(\overline{x})^2 = \langle 11\rangle$) then we put $\nu(x) = F$.

Now, if we take clause $\Phi_i \equiv l_1 \vee l_2 \vee l_3$ then from the fact $\sigma(u_i) \neq \langle --\rangle$ we can deduce that at least one of the values $\sigma(\widetilde{l_1})^2, \sigma(\widetilde{l_2})^2, \sigma(\widetilde{l_3})^2$ is equal to $\langle 11\rangle$. This implies that at least one of the values $\nu(l_1), \nu(l_2), \nu(l_3)$ is T. Altogether, our valuation ν satisfies the formula Φ.

We have reduced the 3-SAT problem to the TERM-EQ($\mathbb{PT}_2$) problem and it is easy to see that the terms L and R can be construct from the formula Φ in the

polynomial time and hence our reduction is polynomial. We can conclude that the TERM-EQ($\mathbb{PT}_2$) problem (and also the POL-EQ($\mathbb{PT}_2$) problem) is coNP-complete. The proof of NP-completeness of the EQN($\mathbb{PT}_2$) problem is simpler because for an instance Φ of the 3-SAT problem we construct equation $(V', \langle 1- \rangle)$ where V' is obtained form V by replacing of all occurrences of the variable a by the element $\langle 21 \rangle$ and all occurrences of the variable b by the element $\langle 1- \rangle$.

□

4 Reductions between problems

In this section we show few reductions between our problems. At first for the equation problem and the polynomial equivalence problem we show reductions from our monoids of transformations of n-element set to monoids of transformations of large set. We use standard notation from complexity theory: we write $P \leq_P Q$ if there is a polynomial reduction from the problem P to the problem Q.

4.1 Reductions for POL-EQ and EQN

Proposition 7. *For any $n \in \mathbb{N}$ we have:*

1. POL-EQ($\mathbb{PT}_n$) $\leq_P$ POL-EQ($\mathbb{PT}_{n+1}$),
2. POL-EQ($\mathbb{I}_n$) $\leq_P$ POL-EQ($\mathbb{I}_{n+1}$),
3. POL-EQ($\mathbb{T}_n$) $\leq_P$ POL-EQ($\mathbb{T}_{n+1}$),
4. EQN($\mathbb{PT}_n$) $\leq_P$ EQN($\mathbb{PT}_{n+1}$),
5. EQN($\mathbb{I}_n$) $\leq_P$ EQN($\mathbb{I}_{n+1}$),
6. EQN($\mathbb{T}_n$) $\leq_P$ EQN($\mathbb{T}_{n+1}$).

Proof. We prove the first statement in detail. Let L, R be polynomials over $\mathbb{PT}_n$, i.e. $L, R \in (\mathbb{PT}_n \cup \mathcal{X})^*$. We consider the element $s = \langle 12 \dots n- \rangle \in \mathbb{PT}_{n+1}$. This means, that $s(i) = i$ for all $i \in X_n$ and $n+1 \notin \mathrm{Dom}(s)$.

We replace any variable x in L and R, by sxs, and we denote the resulting expression $\overline{L}$ and $\overline{R}$ respectively. Because any element of $\mathbb{PT}_n$ is also an element of $\mathbb{PT}_{n+1}$, the expressions $\overline{L}$ and $\overline{R}$ are polynomials over $\mathbb{PT}_{n+1}$.

Now we show that the polynomials L and R are equivalent over $\mathbb{PT}_n$ if and only if the polynomials $\overline{L}$ and $\overline{R}$ are equivalent over $\mathbb{PT}_{n+1}$.

Let L and R are not equivalent over $\mathbb{PT}_n$. Then there is a substitution $\sigma : \mathcal{X} \to \mathbb{PT}_n$ such that $\sigma(L) \neq \sigma(R)$. Because $\sigma(x) \in \mathbb{PT}_n \subseteq \mathbb{PT}_{n+1}$ for any $x \in \mathcal{X}$, the mapping σ is also a substitution $\sigma : \mathcal{X} \to \mathbb{PT}_{n+1}$. We have $\sigma(sxs) = \sigma(x)$, hence $\sigma(\overline{L}) = \sigma(L) \neq \sigma(R) = \sigma(\overline{R})$ and $\overline{L}$ and $\overline{R}$ are not equivalent over $\mathbb{PT}_{n+1}$.

Let assume that $\overline{L}$ and $\overline{R}$ are not equivalent over $\mathbb{PT}_{n+1}$, i.e. there exists $\alpha : \mathcal{X} \to \mathbb{PT}_{n+1}$ such that $\alpha(\overline{L}) \neq \alpha(\overline{R})$. We define substitution $\sigma : \mathcal{X} \to \mathbb{PT}_{n+1}$ in the following way: $\sigma(x) = \alpha(sxs) = s\alpha(x)s$. Because $n+1 \notin \mathrm{Dom}(s)$ and $n+1 \notin \mathrm{Im}(s)$ the element $\sigma(x)$ belongs to $\mathbb{PT}_n$. So, we have defined $\sigma : \mathcal{X} \to \mathbb{PT}_n$ and it is easy to see that $\sigma(L) = \alpha(\overline{L}) \neq \alpha(\overline{R}) = \sigma(R)$.

The same construction is also possible for equations, so fourth part of the statement is clear.

Also the same construction work in the case of the monoids $\mathbb{I}_n$, hence second and fifth statements follow.

The case of full transformations is similar. We can do the same construction, where the element $s \in \mathbb{T}_{n+1}$ is define in the following way: $s(i) = i$ for all $i \in X_n$ and $s(n+1) = n$. Second difference is such that we replace any element $t \in \mathbb{T}_n$ from the instance of the problem by the element $t' \in \mathbb{T}_{n+1}$ where $t'(i) = t(i)$ for all $i \in X_n$ and $t'(n+1) = t(n)$. In this way one can establish the rest of the statement. □

Note that the similar results can be also state for systems of equations and pairs of equations. On the other side this technique can not be used for the term equivalence problem.

If we apply the proposition to Proposition 6 we obtain the following.

Corollary 1. *For $n \geq 2$, the* POL-EQ($\mathbb{PT}_n$) *problem is coNP-complete and the* EQN($\mathbb{PT}_n$) *problem is NP-complete.*

The similar result will be obtain for monoids $\mathbb{I}_n$ and $\mathbb{T}_n$, $n \geq 3$, in the next section.

4.2 Reductions for TERM-EQ

We use completely different reduction to show hardness results for term equivalence problems. We start with some technical lemmas.

For $m \in \mathbb{N}$ we fix $\mathcal{X}_m = \{x_1, x_2 \ldots, x_m\} \subset \mathcal{X}$ and then $\mathcal{X}_m^* = \{x_1, x_2 \ldots, x_m\}^* \subseteq \mathcal{X}^*$ is the set of all terms in variables $x_1, x_2 \ldots, x_m$.

Lemma 4. *Let M be a finite monoid which has k elements and let $m \in \mathbb{N}$. Then there exists a term $w \in \mathcal{X}_m^*$ of the polynomial length with respect to m which satisfies the following condition: for any morphism $\varphi : \mathcal{X}_m^* \to M$ we have:*

1. *$\varphi(w)$ is an idempotent,*
2. *$(\forall u \in \mathcal{X}_m^*)\ (\exists v_0, v_1 \in \mathcal{X}_m^*)\ \varphi(v_0 u v_1) = \varphi(w)$.*

Proof. We consider all possible words over the set of variables $\mathcal{X}_m$ of length k and we define w_0 as the product of all of them (in one fix order). Note that the length of w_0 is km^k. We define $w = w_0^{k!}$ which has a polynomial length with respect to m and we prove the statement for this word.

Let $\varphi : \mathcal{X}_m^* \to M$ be an arbitrary morphism.

1. It is well known fact that for any $a \in M$ the element $a^{k!}$, where $k = |M|$, is an idempotent. Hence $\varphi(w) = \varphi(w_0^{k!}) = \varphi(w_0)^{k!}$ is an idempotent.

2. Let $u \in \mathcal{X}_m^*$. We prove the property with respect to the length of the word u. If $|u| \leq k$ then u is a factor of w and the statement is trivial. If $|u| = l > k$ and $u = x_{i_1} \ldots x_{i_l}$. Then $\varphi(u) = \varphi(x_{i_1}) \ldots \varphi(x_{i_l})$ and we consider the following sequence of l elements from M

$$\varphi(x_{i_1}),\ \varphi(x_{i_1})\varphi(x_{i_2}),\ \varphi(x_{i_1})\varphi(x_{i_2})\varphi(x_{i_3}),\ \ldots,\ \varphi(x_{i_1}) \ldots \varphi(x_{i_l}).$$

Because $l > k$ (recall that k is a number of elements of M) there exist indexes $p < q$ such that $\varphi(x_{i_1}) \dots \varphi(x_{i_p}) = \varphi(x_{i_1}) \dots \varphi(x_{i_q})$. Hence

$$\varphi(u) = \varphi(x_{i_1}) \dots \varphi(x_{i_p})\varphi(x_{i_{q+1}}) \dots \varphi(x_{i_l}) = \varphi(x_{i_1} \dots x_{i_p} x_{i_{q+1}} \dots x_{i_l}).$$

But the word $u' = x_{i_1} \dots x_{i_p} x_{i_{q+1}} \dots x_{i_l}$ is shorter then the word u and by induction assumption there are words v_0, v_1 such that $\varphi(w) = \varphi(v_0 u' v_1) = \varphi(v_0)\varphi(u')\varphi(v_1) = \varphi(v_0)\varphi(u)\varphi(v_1) = \varphi(v_0 u v_1)$. □

For the reader which is familiar with Green relations, we can note that the previous lemma says that $\varphi(w)$ is $\mathcal{J}$-minimal in the subsemigroup generated by the image of the morphism φ. Hence the $\mathcal{H}$-class of the element $\varphi(w)$ is a group and in the case of the monoid $\mathbb{PT}_n$ this group is isomorphic to the subgroup of $\mathbb{S}_n$.

For the reader which is not familiar with Green relations, we present direct proof of this statement without using the machinery of structural semigroup theory.

Lemma 5. *Put $M = \mathbb{PT}_n$ and let $m \in \mathbb{N}$. Let w be a term which satisfy the conditions from the previous lemma and let $\varphi : \mathcal{X}_m^* \to M$ be an arbitrary morphism. Then for any variable $x \in \mathcal{X}_m$ the restriction of the transformation $\varphi(wxw) \in \mathbb{PT}_n$ to the set $\mathrm{Im}(\varphi(w))$ is a permutation of this set.*

Proof. We prove the statement for an arbitrary term $u \in \mathcal{X}_m^*$.

At first, we know that $\varphi(w) = \varphi(w) \cdot \varphi(w) = \varphi(ww)$ from the first statement of the previous lemma. We denote $A = \mathrm{Im}(\varphi(w))$. Because $\varphi(w)$ is idempotent, we see that $\varphi(w)|_A = id_A$.

Now we consider an element of the form $\varphi(wuw)$ where $u \in \mathcal{X}_m^*$. Because $\mathrm{Im}(\varphi(wuw)) \subseteq \mathrm{Im}(\varphi(w)) = A$ we can see that $\varphi(wuw)|_A$ is a partial transformation of the set A.

By the second part of the previous lemma we know that there exist $v_0, v_1 \in \mathcal{X}_m^*$ such that $\varphi(v_0 wuw v_1) = \varphi(w)$. If we use the equality $\varphi(w) = \varphi(ww)$ we deduce that $\varphi(wv_0w)\varphi(wuw)\varphi(wv_1w) = \varphi(w)$. Because $\mathrm{Im}(\varphi(wuw)) \subseteq A$ we deduce $\varphi(wv_0w)|_A \cdot \varphi(wuw)|_A \cdot \varphi(wv_1w)|_A = \varphi(w)|_A = id_A$.

If we denote $P_A^\varphi = \{\varphi(wuw)|_A \mid u \in \mathcal{X}_m^*\} \subseteq \mathbb{PT}_A$ then the previous paragraph has the following interpretation. For any element $s \in P_A^\phi$ there exist elements $t_0, t_1 \in P_A^\phi$ such that $t_0 s t_1 = id_A$. Consequently, s is a permutation of the set A, which we wanted to prove. □

Proposition 8. *For any $n \in \mathbb{N}$ we have:*

1. TERM-EQ($\mathbb{S}_n$) $\leq_P$ TERM-EQ($\mathbb{PT}_n$),
2. TERM-EQ($\mathbb{S}_n$) $\leq_P$ TERM-EQ($\mathbb{I}_n$),
3. TERM-EQ($\mathbb{S}_n$) $\leq_P$ TERM-EQ($\mathbb{T}_n$),

Proof. We prove the first statement in detail.

Let (u, v) be an instance of the TERM-EQ($\mathbb{S}_n$) problem. We can assume that $m \in \mathbb{N}$ is a such that $\mathtt{var}(uv) = \mathcal{X}_m$. Let w be a term satisfying conditions from Lemma 4 and Lemma 5.

We consider the mapping $\alpha : \mathcal{X}_m \to \mathcal{X}_m$ given by the rule $\alpha(x) = wxw$ for any $x \in \mathcal{X}_m$. We denote $\overline{u} = \alpha(u)$, $\overline{v} = \alpha(v)$. We will show that $\mathbb{S}_n$ satisfies the identity $u = v$ if and only if $\mathbb{PT}_n$ satisfies the identity $\overline{u} = \overline{v}$. This gives a polynomial reduction of the TERM-EQ($\mathbb{S}_n$) problem to the TERM-EQ($\mathbb{PT}_n$) problem because terms $\overline{u}$ and $\overline{v}$ have the polynomial size with respect to terms u and v.

In fact, we will prove that $\mathbb{S}_n$ does not satisfy the identity $u = v$ if and only if $\mathbb{PT}_n$ does not satisfy the identity $\overline{u} = \overline{v}$.

So, let $\varphi : \mathcal{X}_m \to \mathbb{S}_n$ be such that $\varphi(u) \neq \varphi(v)$. The morphism φ can be also seen as a morphism to $\mathbb{PT}_n$. For the term w the lemmas are valid, hence $\varphi(w) \in \mathbb{S}_n$ is an idempotent, i.e. $\varphi(w) = 1$. This implies $\varphi(\alpha(s)) = \varphi(s)$ for any term $s \in \mathcal{X}_m^*$. Because $\varphi(\overline{u}) = \varphi(u) \neq \varphi(v) = \varphi(\overline{v})$, the morphism $\varphi : \mathcal{X}_m \to \mathbb{PT}_n$ disproves the identity $\overline{u} = \overline{v}$ in $\mathbb{PT}_n$.

Now let $\varphi : \mathcal{X}_m \to \mathbb{PT}_n$ be such that $\varphi(\overline{u}) \neq \varphi(\overline{v})$. We denote $A = \mathrm{Im}(\varphi(w))$ and we define a mapping $\psi : \mathcal{X}_m \to \mathbb{S}_A$ by the rule $\psi(x) = \varphi(wxw)|_A$ for any $x \in \mathcal{X}_m$. This definition is correct by Lemma 5. The same lemma implies the equality $\psi(s) = \varphi(\alpha(s))|_A$ for any $s \in \mathcal{X}_m^*$. Now from the inequality

$$\varphi(w)\varphi(\overline{u}) = \varphi(\overline{u}) \neq \varphi(\overline{v}) = \varphi(w)\varphi(\overline{v})$$

we can see that $\varphi(\overline{u})|_A \neq \varphi(\overline{v})|_A$. Finally, we can deduce that $\psi(u) = \varphi(\overline{u})|_A \neq \varphi(\overline{v})|_A = \psi(v)$ and we see that the morphism ψ disproves the identity $u = v$ in $\mathbb{S}_A$. Because $A \subseteq X_n$, the group $\mathbb{S}_A$ is isomorphism to the subgroup of $\mathbb{S}_n$. This implies that the identity $u = v$ is not satisfied in $\mathbb{S}_n$.

It is easy to see that the proof works in the same way also in the case of the monoids $\mathbb{I}_n$ and $\mathbb{T}_n$. □

The TERM-EQ($\mathbb{S}_n$) problem is coNP-complete for $n \geq 5$ by Proposition 3.

Corollary 2. *The* TERM-EQ(M) *problem is coNP-complete for any* $M = \mathbb{PT}_n$, *for any* $M = \mathbb{I}_n$ *and for any* $M = \mathbb{T}_n$ *for* $n \geq 5$.

5 The case of transformations of three-element set

The main goal of this section is to prove coNP-completeness of the TERM-EQ($\mathbb{PT}_3$) problem and of the TERM-EQ($\mathbb{T}_3$) and TERM-EQ($\mathbb{I}_3$) problems as well. Note that the proof is uselessly complicated becasue we do all three proofs in the same manner. The idea is make a reduction of the S-EQN($\mathbb{S}_3$) problem to the coTERM-EQ($\mathbb{PT}_3$) problem. Basically, we encode a system of equations over $\mathbb{S}_3$ to certain identity over $\mathbb{PT}_3$ in such a way that solutions of the system correspond to morphisms disproving the identity. The first step is an elimination of constants from the input system over $\mathbb{S}_3$. We explain it in the technical lemmas bellow. Before these lemmas we recall the inner automorphisms of the group $\mathbb{S}_3$ which play an useful role in our construction.

Lemma 6. *For an arbitrary element* $g \in \mathbb{S}_3$ *the mapping* $\omega_g : \mathbb{PT}_3 \to \mathbb{PT}_3$ *defined by the rule* $\omega_g(x) = gxg^5$ *is an automorphism of the monoid* $\mathbb{PT}_3$. *If we*

consider the restriction of ω_g to the set $\mathbb{S}_3$, which we denote ω'_g, then it is an (inner) automorphism of the group $\mathbb{S}_3$. Moreover, for different elements of $\mathbb{S}_3$ these automorphisms are different, i.e $g \neq h \implies \omega'_g \neq \omega'_h$. In particular, if a, b are different cycles of the length 2 then there is a unique element $g \in \mathbb{S}_3$ such that $\omega_g(a) = \langle 213 \rangle$ and $\omega_g(b) = \langle 132 \rangle$.

Proof. The fact that ω_g and ω'_g are automorphisms is easy to see. Indeed, g^6 is the identity permutation, i.e. $g^5 = g^{-1}$ and ω_1 is the identity automorphism, from which the equalities $\omega_g(xy) = \omega_g(x)\omega_g(y)$, $\omega_g(1) = 1$, $\omega_g \circ \omega_{g^{-1}} = \omega_{g^{-1}} \circ \omega_g = \omega_1$ follow. First two ensured that ω_g is a morphism from $\mathbb{PT}_3$ to itself and the third one says that ω_g is a bijection. Remark that ω'_g is an automorphism of $\mathbb{S}_3$ is trivial.

If for two elements $g, h \in \mathbb{S}_3$ we have $\omega'_g = \omega'_h$ then for any element $x \in \mathbb{S}_3$ we have $gxg^{-1} = hxh^{-1}$, i.e. $xg^{-1}h = g^{-1}hx$. In other words the element $g^{-1}h$ commutes with all elements from $\mathbb{S}_3$. This implies that $g^{-1}h$ is the identity permutation and consequently $g = h$. Hence there are six different inner automorphisms of $\mathbb{S}_3$. If we take an arbitrary pair of different cycles of the length 2, then they form a pair of generators of the group $\mathbb{S}_3$. From that reason this pair is mapped under different inner automorphisms to different pairs of different cycles of length 2. So, we obtain six different pairs of images. Because there are exactly six such pairs we see that the pair $\langle 213 \rangle, \langle 132 \rangle$ is one of them and possible g is uniquely determined. □

Remark 1. The image of an element $s \in \mathbb{PT}_3$ in a given inner automorphism ω_g can be seen in such a way, that we just renamed the elements in X_3 using the permutation g^{-1}. For example, if we take $s = \langle 12- \rangle$ then $\omega_g(s)$ is one of the transformations $\langle 12- \rangle$, $\langle 1-3 \rangle$ or $\langle -23 \rangle$ depending on the permutation g.

Now we describe some useful property concerning to the monoid $\mathbb{PT}_3$.

Lemma 7. *For any element $s \in \mathbb{PT}_3$ at least one of the following conditions is satisfied.*

1. $s^4 = \langle --- \rangle$,
2. $s^4 = s^2$,
3. $s \in \mathbb{S}_3$ *is a cycle of the length* 3.

Note that two conditions in the previous lemma can be true at the same time, e.g. the element $s = \langle --- \rangle$ satisfies the first two conditions.

Proof. If $|\operatorname{Im}(s)| = 3$ then $s \in \mathbb{S}_3$ and the second or the third condition is satisfied.

If $|\operatorname{Im}(s)| = 1$ then there are two possibilities $s^2 = \langle --- \rangle$ or $s^2 = s$. Hence the statement is true for such elements and moreover if we apply this observation to s^2 we obtain the statement for s satisfying $|\operatorname{Im}(s^2)| = 1$.

So, the last case which we have to discuss is $|\operatorname{Im}(s)| = 2$ and $|\operatorname{Im}(s^2)| = 2$. Then s maps the two-element set $\operatorname{Im}(s)$ to itself. Hence restriction of s^2 to the set $\operatorname{Im}(s)$ is an identity and the equality $s^4 = s^2$ follows. □

As a consequence of the previous lemma we obtain the following easy observation.

Lemma 8. *For any element $s \in \mathbb{PT}_3$ the element s^6 is an idempotent.*

From Lemma 7 we also derive the following statement.

Lemma 9. *Let elements $a, b, c \in \mathbb{PT}_3$ be such that*

$$(a^3b^3)^2c^6(a^3b^3)^4c^6 \neq (a^3b^3)^4c^6(a^3b^3)^2c^6.$$

Then $a, b \in \mathbb{S}_3$ are different cycles of length 2, $c \notin \mathbb{S}_3$ and $c^6 \neq \langle - - - \rangle$.

Proof. Let $a, b, c \in \mathbb{PT}_3$ satisfy the inequality. The statement $c^6 \neq \langle - - - \rangle$ is trivial. It is easy to see that $c \in \mathbb{S}_3$ implies $c^6 = 1$ and in this case the inequality is not possible.

If we denote $s = a^3b^3$ then we see that the first and the second case from Lemma 7 are not possible for s. Hence $s \in \mathbb{S}_3$ is a cycle of the length 3. This implies $a, b \in \mathbb{S}_3$ and we see that both elements a^3 and b^3 are equal to the identity permutation or to cycles of the length 2. Because $s = a^3b^3$ is a cycle of the length 3 we see that both a^3 and b^3 are different cycles of the length 2. □

The usage of the previous lemma in our reduction is straightforward. An instance of the TERM-EQ($\mathbb{PT}_3$) problem will have the form

$$u(x_a^3x_b^3)^2x_c^6(x_a^3x_b^3)^4x_c^6v = u(x_a^3x_b^3)^4x_c^6(x_a^3x_b^3)^2x_c^6v$$

where x_a, x_b will be variables corresponding to two different cycles a, b of the length 2 which generate the group $\mathbb{S}_3$ and x_c will be special variable. The previous lemma ensures that if this identity is not satisfied in $\mathbb{PT}_3$ then variables x_a and x_b take values a and b respectively. The given system over $\mathbb{S}_3$ will be encode in a term v in such a way that all constants from the system will be replaced by terms in variables x_a, x_b corresponding to expressions of these constants by generators a, b.

We will need more technical lemmas concerning terms from which the identity will be built. We denote the term

$$v(y, z_1, z_2, z_3, z_4, z_5) = y^6(z_1y^6z_1^5)y^6(z_2y^6z_2^5)y^6 \dots y^6(z_5y^6z_5^5)y^6.$$

Lemma 10. *Let $\varphi : \{y, z_1, z_2, z_3, z_4, z_5\} \to \mathbb{PT}_3$ be a mapping which satisfies $\varphi(\{z_1, z_2, z_3, z_4, z_5\}) = \mathbb{S}_3 \setminus \{1\}$. Then for the term $v = v(y, z_1, z_2, z_3, z_4, z_5)$ defined above the following is true.*

1. *If $\varphi(y) \notin \mathbb{T}_3$ then $\varphi(v) = \langle - - - \rangle$.*
2. *If $\varphi(y) \in \mathbb{T}_3 \setminus \mathbb{S}_3$ then $\varphi(v) \in \{\langle 111 \rangle, \langle 222 \rangle, \langle 333 \rangle\}$.*
3. *If $\varphi(y) \in \mathbb{S}_3$ then $\varphi(v) = 1$.*

Proof. Recall that $\varphi(y^6) = \varphi(y)^6$ is always an idempotent.

At first, if $\varphi(y) \in \mathbb{S}_3$ then $\varphi(y^6) = \langle 123 \rangle$ is the identity permutation hence $\varphi(v) = \varphi(z_1^6z_2^6 \dots z_5^6) = \langle 123 \rangle$ is also the identity permutation.

If $\varphi(y) \notin \mathbb{S}_3$ then $|\operatorname{Im}(\varphi(y))| \leq 2$.

Assume that $\varphi(y) \notin \mathbb{T}_3$. If $|\operatorname{Im}(\varphi(y^6))| = 0$ then the statement is true. If $|\operatorname{Im}(\varphi(y^6))| = 1$ then for $p \in \operatorname{Im}(\varphi(y^6))$ and $q \notin \operatorname{Dom}(\varphi(y^6))$ there is a permutation $s \in \mathbb{S}_3 \setminus \{1\}$ such that $s(p) = q$. Hence $\varphi(y^6)\varphi(z_i)\varphi(y^6) = \langle - - - \rangle$ for certain $i \in \{1, \ldots, 5\}$. If $|\operatorname{Im}(\varphi(y^6))| = 2$ then $\varphi(y^6) \in \{\langle 12- \rangle, \langle 1-3 \rangle, \langle -23 \rangle\}$. From remark 1 we know that $\varphi(z_i y^6 z_i^5) = \omega_{\varphi(z_i)}(\varphi(y^6))$ belongs to the same set and moreover we have $\{\varphi(z_i y^6 z_i^5) \mid i = 1, \ldots, 5\} = \{\langle 12- \rangle, \langle 1-3 \rangle, \langle -23 \rangle\}$. The equality $\varphi(v) = \langle - - - \rangle$ follows.

Now we will discuss the case $\varphi(y) \in \mathbb{T}_3 \setminus \mathbb{S}_3$. If $|\operatorname{Im}(\varphi(y^6))| = 1$ then the statement is clear. If $|\operatorname{Im}(\varphi(y^6))| = 2$ then we denote p, q, r such that $\{p, q, r\} = X_3$ and $\varphi(y^6)$ maps p to p, q to p and r to r. Then there is a (non-identical) permutation which maps the subset $\{p, r\}$ to $\{p, q\}$ hence $\varphi(y^6 z_i y^6)$ is a constant transformation for some $i \in \{1, \ldots, 5\}$. And because $\operatorname{Im}(\varphi) \subseteq \mathbb{T}_3$ we see that also $\varphi(v) \in \mathbb{T}_3$ is a constant transformation. □

We construct one more similar term which will be used in our reduction. Put

$$u(y, z, z_1, z_2) = y^6\ z\ y^6\ z_1 z z_1\ y^6\ z_2 z z_2\ y^6\ z_1 z_2 z_1 z z_1 z_2 z_1\ y^6.$$

Lemma 11. *Let $\varphi : \{y, z, z_1, z_2\} \to \mathbb{PT}_3$ be such that $\varphi(z_1), \varphi(z_2) \in \mathbb{S}_3$ are different cycles of the length 2 and $\varphi(y) \in \mathbb{T}_3 \setminus \mathbb{S}_3$. Then for the term $u = u(y, z, z_1, z_2)$ defined above the following is true.*

1. *If $\varphi(z) = 1$ then $\varphi(u) = \varphi(y)^6$.*
2. *If $\varphi(z) \in \mathbb{S}_3 \setminus \{1\}$ then $\varphi(u) \in \{\langle 111 \rangle, \langle 222 \rangle, \langle 333 \rangle\}$.*

Proof. Let all assumptions be true. As we know $\varphi(y^6) \in \mathbb{T}_3 \setminus \mathbb{S}_3$ is an idempotent. If $\varphi(y^6) \in \{\langle 111 \rangle, \langle 222 \rangle, \langle 333 \rangle\}$ then the both statements are valid. If $\varphi(z) = 1$ then $\varphi(z_1 z z_1) = \varphi(z_1^2) = 1$ and similarly $\varphi(z_2 z z_2) = \varphi(z_1 z_2 z_1 z z_1 z_2 z_1) = 1$ hence the second statement is also valid.

So, assume that $|\operatorname{Im}(\varphi(y^6))| = 2$ and $\varphi(z) \in \mathbb{S}_3 \setminus \{1\}$. Now $\varphi(z_1)$, $\varphi(z_2)$ and $\varphi(z_1 z_2 z_1)$ are three different cycles of the length 2. Recall that by Remark 1 the elements of the form $\omega_g(\varphi(z))$ can be viewed as the elements $\varphi(z)$ with renaming set X_3 by permutation g^{-1}. Hence, if $\varphi(z)$ is a cycle of the length 2 then the set

$$V = \{\varphi(z), \varphi(z_1 z z_1), \varphi(z_2 z z_2), \varphi(z_1 z_2 z_1 z z_1 z_2 z_1)\}$$

consists of all cycles of the length 2. If $\varphi(z)$ is a cycle of the length 3 then the set V consists of all cycles of the length 3.

We denote p, q, r such that $\{p, q, r\} = X_3$ and $\varphi(y^6)$ maps p to p, q to p and r to r. Now there is an element s in the set V (the set V is equal to $\{\langle 213 \rangle, \langle 321 \rangle, \langle 132 \rangle\}$ or to $\{\langle 231 \rangle, \langle 312 \rangle\}$) such that s maps q to r, i.e. subset $\{p, r\}$ to the subset $\{p, q\}$. Hence $\varphi(y^6) s \varphi(y^6) = \langle ppp \rangle$ tor some $s \in V$. This implies that $\varphi(u)$ is a constant transformation. □

Now we are ready to prove the main result of this section.

Proposition 9. S-EQN($\mathbb{S}_3$) $\leq_P$ *co* TERM-EQ($\mathbb{PT}_3$).

Proof. First of all we note that the instance of the S-EQN($\mathbb{S}_3$) problem can be written in a special form $\{L_1 = 1, L_2 = 1, \dots, L_k = 1\}$ because $\mathbb{S}_3$ is a group of order 6 and any equality $s = t$ is equivalent to the equality $st^5 = 1$.

So, let $\{L_1 = 1, L_2 = 1, \dots, L_k = 1\}$ be an instance of the S-EQN($\mathbb{S}_3$) problem which contains variables $\mathcal{X}_m = \{x_1, \dots, x_m\}$. We will consider three new variables x_a, x_b, x_c.

If we denote $a = \langle 213\rangle$, $b = \langle 132\rangle$ then an arbitrary element of $\mathbb{S}_3$ can be written in one of the following way: $1, a, b, ab, ba, aba$. For any polynomial $s \in (\mathcal{X}_m \cup \mathbb{S}_3)^*$ we denote by $\overline{s}$ the term which we obtain from s by replacing any occurrence of a constant $1, a, b, ab, ba, aba$ by the term $1, x_a, x_b, x_ax_b, x_bx_a, x_ax_bx_a$ respectively. This means that $\overline{u} \in (\mathcal{X}_m \cup \{x_a, x_b\})^*$.

We will use terms v and u defined above. We consider the following term:

$$v_c = v(x_c, x_a, x_b, x_ax_b, x_bx_a, x_ax_bx_a),$$

and for $i \in \{1, \dots, k\}$ we consider terms

$$u_{L_i} = u(x_c, \overline{L_i}, x_a, x_b) \quad \text{and} \quad v_{L_i} = v(\overline{L_i}, x_a, x_b, x_ax_b, x_bx_a, x_ax_bx_a).$$

Futher

$$w_1 = (x_a^3x_b^3)^2x_c^6(x_a^3x_b^3)^4x_c^6, \quad w_2 = (x_a^3x_b^3)^4x_c^6(x_a^3x_b^3)^2x_c^6.$$

Finally, we consider the following pair of terms

$$L = v_cw_1u_{L_1}v_{L_1}\dots u_{L_k}v_{L_k}, \quad R = v_cw_2u_{L_1}v_{L_1}\dots u_{L_k}v_{L_k}$$

which will form an instance of the TERM-EQ($\mathbb{PT}_3$) problem.

We prove that the original system $\{L_1 = 1, L_2 = 1, \dots, L_k = 1\}$ has a solution in $\mathbb{S}_3$ if and only if the identity $L = R$ does not hold in $\mathbb{PT}_3$.

Let assume that $\varphi : \mathcal{X}_m \to \mathbb{S}_3$ is a solution of the system $\{L_1 = 1, L_2 = 1, \dots, L_k = 1\}$. We extend the definition of φ to the set of variables $\mathcal{X}_m \cup \{x_a, x_b, x_c\}$ by the rules $\varphi(x_a) = a = \langle 213\rangle$, $\varphi(x_b) = b = \langle 132\rangle$ and $\varphi(x_c) = \langle 223\rangle$.

From the definition of the terms $\overline{L_i}$ follows that $\varphi(\overline{L_i}) = \varphi(L_i) = 1$. Hence $\varphi(v_{L_i}) = 1$ and $\varphi(u_{L_i}) = \varphi(x_c)^6 = \langle 223\rangle$. From this we can see $\varphi(u_{L_1}v_{L_1}\dots u_{L_k}v_{L_k}) = \varphi(x_c)^6$ which is an idempotent. Now we can compute $\varphi(x_a^3x_b^3) = \langle 213\rangle\langle 132\rangle = \langle 312\rangle$, $\varphi(x_a^3x_b^3)^2 = \langle 231\rangle$, $\varphi(x_a^3x_b^3)^4 = \langle 312\rangle$. Hence $\varphi(w_1) = \langle 231\rangle\langle 223\rangle\langle 312\rangle\langle 223\rangle = \langle 222\rangle$ and $\varphi(w_2) = \langle 312\rangle\langle 223\rangle\langle 231\rangle\langle 223\rangle = \langle 233\rangle$. The exact computation of $\varphi(v_c)$ is not needed, because by Lemma 10 we see $\varphi(v_c) \in \{\langle 111\rangle, \langle 222\rangle, \langle 333\rangle\}$ and because the suffix of the term v_c is x_c^6 we deduce $\varphi(v_c) \in \{\langle 222\rangle, \langle 333\rangle\}$. Hence $\varphi(v_cw_1x_c^6) = \langle 222\rangle \neq \langle 333\rangle = \varphi(v_cw_2x_c^6)$ and this conclude that φ disprove the constructed identity in $\mathbb{PT}_3$.

Now we assume that the identity $L = R$ is not satisfied in $\mathbb{PT}_3$, i.e we assume that there is a morphism $\varphi_0 : (\mathcal{X}_m \cup \{x_a, x_b, x_c\})^* \to \mathbb{PT}_3$ such that $\varphi_0(L) \neq \varphi_0(R)$. Note that if we take an arbitrary automorphism ω of the monoid $\mathbb{PT}_3$ then the composition of the morphisms φ_0 and ω also disproves the identity.

We use Lemma 9 to the inequality $\varphi_0(L) \neq \varphi_0(R)$. We obtain that $\varphi_0(x_a)$ and $\varphi_0(x_b)$ are different cycles of the length 2. Now we apply Lemma 6 and we

see that there is an morphism ($\varphi_0\omega_g$ for certain g) which disproves the identity and which maps the variable x_a to the element $a = \langle 213\rangle$ and the variable x_b to $b = \langle 132\rangle$. We denote this morphism φ and we will work with them from this moment. Our goal is to prove $\varphi(\overline{L_i}) = 1$ for any $i = 1, \ldots, k$.

From Lemma 9 we know that $\varphi(x_c^6)$ is an idempotent outside $\mathbb{S}_3$. Because $\varphi(v_c) \neq \langle - - -\rangle$ Lemma 10 implies $\varphi(x_c^6) \in \mathbb{T}_3 \setminus \mathbb{S}_3$. Futher $\varphi(v_{L_i}) \neq \langle - - -\rangle$ implies that $\varphi(\overline{L_i}) \in \mathbb{T}_3$ and consequenty $\varphi : \mathcal{X}_m \cup \{x_a, x_b, x_c\}^* \to \mathbb{T}_3$. Now if $\varphi(\overline{L_i}) \notin \mathbb{S}_3$ then by Lemma 10 we have $\varphi(v_{L_i}) \in \{\langle 111\rangle, \langle 222\rangle, \langle 333\rangle\}$. If $\varphi(\overline{L_i}) \in \mathbb{S}_3 \setminus \{1\}$ then by Lemma 11 we have $\varphi(u_{L_i}) \in \{\langle 111\rangle, \langle 222\rangle, \langle 333\rangle\}$. So altogether $\varphi(\overline{L_i}) \neq 1$ implies $\varphi(v_{L_i})\varphi(v_{L_i})$ is a constant transformation. Because $\varphi : \mathcal{X}_m \cup \{x_a, x_b, x_c\}^* \to \mathbb{T}_3$ we see that this is a contradiction as both sides of $\varphi(L) \neq \varphi(R)$ are equal to the transformation $\varphi(u_{L_1} v_{L_1} \ldots u_{L_k} v_{L_k}) \in \{\langle 111\rangle, \langle 222\rangle, \langle 333\rangle\}$.

So, we proved that $\varphi(\overline{L_i}) = 1$ for all $i \in \{1, \ldots, k\}$ and because $\varphi(x_a) = a = \langle 213\rangle$ and $\varphi(x_b) = b = \langle 132\rangle$ we see that the restriction of the morphism φ to the set $\mathcal{X}_m^*$ is a solution of the given system over $\mathbb{S}_3$. □

If we check the proof carefully we can see that the reduction is, in fact, also the reduction of the S-EQN($\mathbb{S}_3$) problem to the coTERM-EQ($\mathbb{T}_3$) problem.

Corollary 3. *The* TERM-EQ($\mathbb{PT}_3$) *problem and the* TERM-EQ($\mathbb{T}_3$) *problem are coNP-complete.*

Also the same construction can be simplified to prove NP-hardnes of the EQN($\mathbb{T}_3$) problem. If we use Proposition 7 we obtain the following.

Corollary 4. *For any $n \geq 3$ the* EQN($\mathbb{T}_n$) *problem is NP-complete and the* POL-EQ($\mathbb{T}_n$) *problem is coNP-complete.*

To prove the same result for $\mathbb{I}_3$ we have to slightly modified the previous reduction. In fact, the reduction is easier as we can not discuss so much cases. We improve Lemmas 9 and 11 for the case when we consider elements from $\mathbb{I}_3$ only.

Lemma 12. *Let $\varphi : \{y, z_1, z_2, z_3, z_4, z_5\} \to \mathbb{I}_3$ be a mapping which satisfies $\varphi(\{z_1, z_2, z_3, z_4, z_5\}) = \mathbb{S}_3 \setminus \{1\}$. Then for the term $v = v(y, z_1, z_2, z_3, z_4, z_5)$ the following is true.*

1. *If $\varphi(y) \notin \mathbb{S}_3$ then $\varphi(v) = \langle - - -\rangle$.*
2. *If $\varphi(y) \in \mathbb{S}_3$ then $\varphi(v) = 1$.*

Proof. It is just a direct consequence of Lemma 10. □

In the case of Lemma 11 we redefine the term u to make the proof easier. Put

$$u'(y, z, z_1, z_2) = (y^6\ z)^6(y^6\ z_1 z z_1)^6(y^6\ z_2 z z_2)^6(y^6\ z_1 z_2 z_1 z z_1 z_2 z_1)^6 y^6.$$

Lemma 13. *Let $\varphi : \{y, z, z_1, z_2\} \to \mathbb{I}_3$ be such that $\varphi(z_1), \varphi(z_2) \in \mathbb{S}_3$ are different cycles of the length 2 and $\varphi(y) \in \mathbb{I}_3 \backslash \mathbb{S}_3$. Then for the term $u' = u'(y, z, z_1, z_2)$ defined above the following is true.*

1. *If $\varphi(z) = 1$ then $\varphi(u') = \varphi(y)^6$.*
2. *If $\varphi(z) \in \mathbb{S}_3 \setminus \{1\}$ then $\varphi(u') = \langle - - - \rangle$.*

Proof. The first case is the same as in the proof of Lemma 11. Now let $\varphi(z) \in \mathbb{S}_3 \backslash \{1\}$. We have an idempotent $\varphi(y^6) \in \mathbb{I}_3 \backslash \mathbb{S}_3$. An element in $\mathbb{I}_3$ is an idempotent iff maps its domain identically. Denote $p \in X_3$ such that $p \notin \mathrm{Dom}(\varphi(y^6))$ and q, r the rest elements from X_3.

Once again

$$V = \{\varphi(z), \varphi(z_1 z z_1), \varphi(z_2 z z_2), \varphi(z_1 z_2 z_1 z z_1 z_2 z_1)\}$$

consists of all cycles of the length 2 or of both cycles of the length 3. In the first case if we multiply these elements by $\varphi(y^6)$ from left and then consider the sixth power we obtain the set of three elements which maps identically the sets $\{q, r\}$, $\{q\}$ and $\{r\}$ respectively. Their product is $\langle - - - \rangle$. In the second case if we multiply cycle of length 3 by $\varphi(y^6)$ from left and then consider the sixth power we obtain $\langle - - - \rangle$ directly. □

Now we repeat the reduction of the problem. In the prove we will discus only the changes.

Proposition 10. S-EQN($\mathbb{S}_3$) $\leq_P$ *co* TERM-EQ($\mathbb{I}_3$).

Proof. Let $\{L_1 = 1, L_2 = 1, \ldots, L_k = 1\}$ be an instance of the S-EQN($\mathbb{S}_3$) problem. Variables $\mathcal{X}_m = \{x_1, \ldots, x_m\} \cup \{x_a, x_b, x_c\}$ and elements a, b are the same. Also the construction of the terms $\overline{L_i}$ and the terms v_{L_i}. The term v_c is not needed any more and $u'_{L_i} = u'(x_c, \overline{L_i}, x_a, x_b)$ is changed a bit. Finally, we consider the following instance of the TERM-EQ($\mathbb{PT}_3$) problem:

$$w_1 u'_{L_1} v_{L_1} \ldots u'_{L_k} v_{L_k} = w_2 u'_{L_1} v_{L_1} \ldots u'_{L_k} v_{L_k}$$

where w_1 and w_2 are the same as in the proof of Proposition 9. We prove that the original system $\{L_1 = 1, L_2 = 1, \ldots, L_k = 1\}$ has a solution in $\mathbb{S}_3$ if and only if this identity does not hold in $\mathbb{I}_3$.

For a solution $\varphi : \mathcal{X}_m \to \mathbb{S}_3$ of the system $\{L_1 = 1, L_2 = 1, \ldots, L_k = 1\}$ we define once again $\varphi(x_a) = a$, $\varphi(x_b) = b$ and we update $\varphi(x_c) = \langle 12 - \rangle$.

From the definition of the terms $\overline{L_i}$ follows that $\varphi(\overline{L_i}) = \varphi(L_i) = 1$. Hence $\varphi(v_{L_i}) = 1$ and $\varphi(u'_{L_i}) = \varphi(x_c)^6$. From this we can see $\varphi(u_{L_1} v_{L_1} \ldots u_{L_k} v_{L_k}) = \varphi(x_c)^6 = \langle 12 - \rangle$. Now we have $\varphi(x_a^3 x_b^3)^2 = \langle 231 \rangle$, $\varphi(x_a^3 x_b^3)^4 = \langle 312 \rangle$ again. Hence $\varphi(w_1) = \langle 231 \rangle \langle 12 - \rangle \langle 312 \rangle \langle 12 - \rangle = \langle 1 - - \rangle$ and $\varphi(w_2) = \langle 312 \rangle \langle 12 - \rangle \langle 231 \rangle \langle 12 - \rangle = \langle -2 - \rangle$. Hence $\varphi(w_1 x_c^6) = \langle 1 - - \rangle \neq \langle -2 - \rangle = \varphi(w_2 x_c^6)$ and this conclude that φ disprove the constructed identity in $\mathbb{I}_3$.

Now we assume that the identity is not satisfied in $\mathbb{I}_3$. As before we consider φ disproving identity and satisfying $\varphi(x_a) = a$, $\varphi(x_b) = b$.

From Lemma 9 we know that $\varphi(x_c^6)$ is an idempotent different from 1. From Lemma 12 we know that $\varphi(\overline{L_i})$ belongs to $\mathbb{S}_3$ and from Lemma 13 we see that $\varphi(\overline{L_i}) = 1$. These imply that the restriction of the morphism φ to the set $\mathcal{X}_m^*$ is a solution of the given system over $\mathbb{S}_3$. □

Corollary 5. *The* TERM-EQ($\mathbb{I}_3$) *problem is coNP-complete.*

Again, our construction can be simplified to prove NP-hardnes of the EQN($\mathbb{I}_3$) problem and Proposition 7 give the following.

Corollary 6. *For any* $n \geq 3$ *the* EQN($\mathbb{I}_n$) *problem is NP-complete and the* POL-EQ($\mathbb{I}_n$) *problem is coNP-complete.*

6 Conclusion and Future Work

We summarize the results contained in Proposition 5 and Corollaries 1— 6.

Theorem 1. *Let* $n \in \mathbb{N}$, $n \geq 2$. *Then*
(i) for $n = 2$*:* EQN($\mathbb{T}_2$), TERM-EQ($\mathbb{T}_2$), POL-EQ($\mathbb{T}_2$) *are in P,*
(ii) for $n \geq 3$, EQN($\mathbb{T}_n$) *is NP-complete,*
(iii) for $n \geq 3$, POL-EQ($\mathbb{T}_n$) *is coNP-complete,*
(iv) for $n = 3$ *and* $n \geq 5$, TERM-EQ($\mathbb{T}_n$) *is coNP-complete,*
(v) for $n = 2$*:* EQN($\mathbb{I}_2$), TERM-EQ($\mathbb{I}_2$), POL-EQ($\mathbb{I}_2$) *are in P,*
(vi) for $n \geq 3$, EQN($\mathbb{I}_n$) *is NP-complete,*
(vii) for $n \geq 3$, POL-EQ($\mathbb{I}_n$) *is coNP-complete,*
(viii) for $n = 3$ *and* $n \geq 5$, TERM-EQ($\mathbb{I}_n$) *is coNP-complete,*
(ix) EQN($\mathbb{PT}_n$) *is NP-complete,*
(x) POL-EQ($\mathbb{PT}_n$) *is coNP-complete,*
(xi) for $n \neq 4$, TERM-EQ($\mathbb{PT}_n$) *is coNP-complete.*

We strongly believe that for the missing cases, namely TERM-EQ($\mathbb{T}_4$), TERM-EQ($\mathbb{I}_4$) and TERM-EQ($\mathbb{PT}_4$), one can use an analogical method to one from the previous section.

Conjecture 1. The problems TERM-EQ($\mathbb{T}_4$), TERM-EQ($\mathbb{I}_4$) and TERM-EQ($\mathbb{PT}_4$) are coNP-complete.

In the topic there are really interesting open questions. First goal should be describtion of the complexity of the problems in the case of groups. The complexity of the TERM-EQ($\mathbb{S}_4$) problem is first which sould be characterize.

Other direction is to discuss wheter the problems POL-EQ(M) and EQN(M) are of the same complexity. Some partial results are known (see [9]).

For more open problems see [5, 6].

Acknowledgments

Supported by the Ministry of Education of the Czech Republic under the project MSM0021622409.

References

[1] Almeida J., Volkov M.V., Goldberg S. V.: Complexity of the identity checking problem for finite semigroups. J. Math. Sci. **158**(5), 605–614 (2009)

[2] 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.

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

[4] M. Goldmann and A. Russel. The complexity of solving equations over finite groups. Proc. IEEE Conference on Computational Complexity (1999), 80–86.

[5] G. Horváth, L. Mérai and C. Szabó. The complexity of the word problem over finite non-solvable groups. (preprint)

[6] G. Horváth and C. Szabó. The complexity of checking identities over finite groups. (preprint)

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

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

[9] O. Klíma. Complexity issues of checking identities in finite monoids. (preprint) - 2009 - Semigroup Forum

[10] O. Klíma. Identity Checking Problem for Monoids of Transformations, submitted

[11] O. Klíma., P. Tesson and D. Thérien. Dichotomies in the complexity of solving systems of equations over finite semigroup. Theory of Computing Systems, Vol 40, Num. 3 (2007).

[12] C. Moore, P. Tesson and D. Theérien. Satisfiability of systems of equations over finite monoids. In MFCS'01 Vol.?? of LNCS (2001), 537–547.

[13] Papadimitriou C. H.: Computational Complexity (1994), Addison-Wesley Publishing Company.

[14] V.Y.Popov and M.V.Volkov. Complexity of checking identities and quasi-identities in finite semigroups. Journal of Symbolic logic ....

[15] S. Seif. .... Int. J. of Algebra and Computation **15**/2 (2005), 317–326.

[16] 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.

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

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

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