THE COMPLEXITY OF CHECKING IDENTITIES
OVER FINITE GROUPS

GÁBOR HORVÁTH* and CSABA SZABÓ†

Eötvös Loránd University, Department of Algebra and Number Theory
1117 Budapest, Pázmány Péter sétány 1/C, Hungary
*ghorvath@cs.elte.hu
†csaba@cs.elte.hu

Received 13 June 2005
Revised 31 August 2005

Communicated by R. McKenzie

We analyze the computational complexity of solving a single equation and checking identities over finite meta-abelian groups. Among others we answer a question of Goldmann and Russel from 1998: we prove that it is decidable in polynomial time whether or not an equation over the six-element group $S_3$ has a solution.

Keywords: Computational complexity; finite groups; identity checking; term equivalence; equation solvability.

1. Introduction

The computational complexity of the word problem in algebra is of greater and greater interest. In this paper we present results about the computational complexity of checking identities over finite groups. We use standard notations in computational complexity (see [3]).

In 1997, Ross Willard gave a talk at The Fields Institute where he presented several results and problems concerning algebraic complexity questions about rings. He defined two versions of the word problem. There are two kinds of words. A term on an algebra $A$ is an expression that can be obtained using (iterated) compositions of the basic operations and projections. Projections are trivial operations satisfying $p_i^n(x_1,\ldots,x_n) = x_i$. A polynomial on an algebra $A$ is an expression that can be obtained using (iterated) compositions of the basic operations, projections and nullary, constant operations. The two versions of the word problem are the term equivalence (TERM-EQ), and the polynomial equivalence (POL-EQ) problems.

Definition 1. Let $A$ be an algebra. Two terms (polynomials), $t_1$ and $t_2$, are called equivalent ($t_1(x_1,\ldots,x_n) \equiv t_2(x_1,\ldots,x_n)$ or shortly $t_1 \equiv t_2$) if the values of the
two terms (polynomials) are equal at every substitution from A. An instance of
the term (polynomial) equivalence problem TERM-EQ A (POL-EQ A) is a pair
of terms (polynomials), \( t_1 \) and \( t_2 \), with the question whether or not the two terms
(polynomials) are equivalent.

For finite structures there is an obvious algorithm to decide these problems.
Indeed, one can check every possible substitution, and if the two terms (polyno-
mials) agree at all of them then they are equivalent. On the other hand, if one
finds a tuple of elements NOT satisfying the equation, then it can be shown in
polynomial time that the two words are not equivalent. Hence for finite algebras
both equivalence problems are obviously in coNP. In what follows, all algebras will
be finite.

Thus two terms, \( t_1 \) and \( t_2 \), are equivalent if and only if \( t_1 = t_2 \) is an identity
over A. In case A is a group, this is equivalent to \( t_1 t_2^{-1} \equiv 1 \). Hence, we introduce
the following definition, often used in group theory.

**Definition 2.** A term over a group is called an identity if it is equivalent to 1, the
identity element of the group.

Willard in his talk discussed these two problems for rings. It was already known
[5] that for a commutative ring \( R \) the TERM-EQ problem is in \( P \) if \( R \) is nilpo-
tent and coNP-complete otherwise. Burris and Lawrence proved in [2] that the
same holds for rings in general. Following their proof it is easy to see that for
a nilpotent ring \( R \) the problem POL-EQ \( R \) is in \( P \) and it is a straightforward
consequence of their result that if the ring is not nilpotent, then POL-EQ \( R \) is
coNP-complete.

For groups the answer is far less complete. An unpublished result of Burris and
Lawrence (1994) is the following.

**Theorem 3.** Let \( G \) be a group. If \( G \) is nilpotent, then TERM-EQ \( G \) is in \( P \). If \( G \)
is not solvable, then TERM-EQ \( G \) is coNP-complete.

In this paper we would like to extend these results for a class of solvable non-
nilpotent groups. We prove that several kinds of semidirect products admit poly-
nomial time solvable TERM-EQ problem. For example, we prove that checking
identities is easy for the dihedral groups, for the alternating group \( A_4 \), for the
wreath product of two cyclic groups, etc.

The other problem to investigate is the complexity of solving equations and
systems of equations over finite algebras. These problems arise from unification
theory [6], formal languages [11] and, naturally, from universal algebra.

**Definition 4.** Let \( A \) be an algebra. The input of the polynomial satisfiability
problem (POL-SAT \( A \)) is a pair of polynomials \( s \) and \( t \) with the question whether
there is a substitution of the variables from \( A \) such that the values of the two
polynomials are the same.
Definition 5. Let $A$ be an algebra. The input of the polynomial system-satisfiability problem (POL-SYS $A$) are $2n$ polynomials $s_1, \ldots, s_n$ and $t_1, \ldots, t_n$ with the question whether there is a substitution of the variables from $A$ such that $s_i = t_i$ for all $i = 1, \ldots, n$.

The complexity POL-SYS is fully characterized for groups in [4, 8]:

Theorem 6. Let $A$ be a group. The problem $\text{POL-SYS } A$ is in $P$ if $A$ is Abelian and it is NP-complete otherwise.

The characterization of solving a single equation looks more complicated, though [4].

Theorem 7. Let $G$ be a group. If $G$ is nilpotent, then $\text{POL-SAT } G$ is in $P$. If $G$ is not solvable, then $\text{POL-SAT } G$ is coNP-complete.

The result tells nothing about non-nilpotent solvable groups. Goldmann and Russell explicitly ask in [4] to decide the complexity of solving an equation over $S_3$.

The POL-SAT problem was first examined for monoids and semigroups. Klíma [7] has analyzed the question for semigroups of size at most 6. He proved for almost all of these semigroups that solving an equation is either in $P$ or NP-complete. The only remaining case is the 6 element "monoid" $S_3$. He conjectures that the problem is in $P$.

In this paper we show the following: if $G \simeq A \rtimes B$, where $A \simeq \mathbb{Z}_p$ and $B \simeq \mathbb{Z}_q$ for some primes $p$ and $q$, then $\text{POL-SAT } G$ is in $P$. Thus, with $\mathbb{Z}_3 \simeq A$ and $\mathbb{Z}_2 \simeq B$ we answer the questions of both Goldmann and Russell, and Klíma.

The result suggests that the complexity of TERM-EQ and POL-SAT for a finite algebra $A$ is always the same. This is far from being true. Seif and Szabó present a 10-element semigroup (see [10]) for which the term-equivalence problem is decidable in polynomial time and the POL-SAT problem is coNP-complete. An even stronger result of Klíma is the following (see [7]):

Theorem 8. There is a semigroup $S$ of size 24 such that $\text{POL-SAT } S$ is NP-complete and $\text{POL-EQ } S$ is in $P$.

It may happen, though, that the complexity of the two problems coincide in the case of groups. At this point we do not even know the answer for $S_4$.

2. Semidirect Products

In this section we will prove for a class of non-nilpotent groups that the POL-EQ problem (so the TERM-EQ problem also) can be solved in polynomial time. The group operation will always be multiplication. The identity element of a group will be denoted by 1. The following method will play a crucial role in our investigation.
Collecting procedure: Let $G \simeq A \times B$ where $A$ is Abelian and let $t = x_1 x_2 \cdots x_k$ be a group polynomial over $G$. Without loss of generality we assume that the $x_i$ are constants or variables over $G$. Every element of $G$ can be uniquely written of the form $ba$ where $a \in A$ and $b \in B$. So we write $x_i$ of the form $b_i a_i$ where $a_i \in A$ and $b_i \in B$. Collecting the elements of $B$ to the left we obtain

$$t = (b_1 b_2 \cdots b_k) \cdot (a_1^{b_1} b_1 \cdots a_2^{b_2} b_2 \cdots a_k^{b_k} b_k).$$

This term is an identity if and only if both

$$b_1 b_2 \cdots b_k$$

and

$$(a_1^{b_1} b_1 \cdots a_2^{b_2} b_2 \cdots a_k^{b_k} b_k)$$

are identities (i.e. both are identically 1 for all substitutions over $G$). Let us examine the latter expression. Substitute $a_i = 1$ for all $i$, where $x_i$ is a variable, not constant. Then we get $t' = c_1^{w_1} c_2^{w_2} \cdots c_m^{w_m}$, where all $c_i$’s are constants from $A$ and $w_i$ is a word over $B$ (let us call $t'$ the constant part of (2)). Let us fix $j$. Substituting $a_i = 1$ for $i \neq j$ (where $a_i$ is not constant) we obtain an identity of the form $t'_j t''$ where $t'_j = a_j^{h_1} a_j^{h_2} \cdots a_j^{h_l}$ and $l$ is the number of the occurrences of $x_j$ in $t$ and $h_i$ is a semigroup polynomial over $B$ for every $1 \leq i \leq l$. Obviously, (2) is an identity if and only if $t'$ and $t'_j$ are identities for every $1 \leq j \leq k$. Hence we are looking for the complexity of checking whether or not $b_1 b_2 \cdots b_k$, $t$ and $t'_j$ are all identities.

Lemma 9. Let $F$ be a field of prime characteristic $p$ and $H \leq F^*$. For a polynomial $f(\bar{x}) \in F[x_1, x_2, \ldots, x_k]$ it can be checked in polynomial time whether or not it vanishes on $H$.

Proof. Let $a$ be a generator of $F^*$ and let $H = \langle a^l \rangle$. Putting $z_j = x_j^l$ we have $f(\bar{x})$ is identically 0 over $H$ if and only if $f(\bar{z})$ is identically 0 over $F^*$. A polynomial $g \in F[x_1, \ldots, x_k]$ admits this latter property if and only if $g = \sum x_i^{q-1} - 1 \cdot g_i(x)$ for some $g_i \in F[x_1, \ldots, x_k]$, where $|F| = q$. This condition can be checked in linear time since we only need to divide $g$ by $x_i^{q-1} - 1$ (i.e. substitute $x_i^{q-1} = 1$) for all $i \in \{1, \ldots, k\}$ and the remaining expression has to be 0.

Theorem 10. If $G \simeq A \times B$ where $A \simeq \mathbb{Z}_p$ for some prime $p$, and POL-EQ $B$ is in $P$ then POL-EQ $G$ is in $P$.

Proof. The subgroup $B$ acts on $A$. Now, Aut $(A) \simeq C_{p-1}$, the cyclic group of order $p-1$ and consists of the maps $a \rightarrow a^l$ for every $a \in A$ for some $1 \leq l \leq p-1$. Thus there is a homomorphism $\phi : B \rightarrow C_{p-1}$ such that $a^l = a^{\phi(b)}$ for every $a \in A$. Now, using the collecting procedure it is enough to check whether or not $b_1 b_2 \cdots b_k$, $a_j^{h_1} a_j^{h_2} \cdots a_j^{h_l}$ and $c_1^{w_1} c_2^{w_2} \cdots c_m^{w_m}$ are identities. The first condition can be checked in polynomial time by the assumption. For the second one we rewrite the expression $a_j^{h_1} a_j^{h_2} \cdots a_j^{h_l} = a_j^{\phi(h_1)} a_j^{\phi(h_2)} \cdots a_j^{\phi(h_l)} = a_j^{w_1 + w_2 + \cdots + w_l}$. Here $w_j$ denotes the image
of \( h_j \) at \( \phi \). Substituting \( \phi(h_j) = y_j \) we have \( w_j \) as a product of some of \( y_1, \ldots, y_k \) over \( \mathbb{Z}_p \), shortly a monomial, and \( f = w_1 + w_2 + \cdots + w_1 \) is a \( k \)-variable polynomial over \( \phi(B) \) where both the addition and the multiplication is understood in \( \mathbb{Z}_p \). The expression \( a_{1j}^{w_1}a_{2j}^{w_2}a_{k_j}^{w_k} \) is an identity if and only if \( f \) attains 0 every time when we substitute elements of \( \phi(B) \) for the variables. And this can be checked in polynomial time by Lemma 9. Finally, \( c_1^{w_1}c_2^{w_2} \cdots c_m^{w_m} \) can be written in the form \( c^{u_1}_1c^{u_2}_2 \cdots c^{u_m}_m \), where \( c \) is the generator of \( A \). Using the same idea, this is an identity if and only if \( w_1' + \cdots + w_m' \) attains 0 every time when we substitute elements of \( \phi(B) \) for the variables. Again, this can be checked in polynomial time by Lemma 9.

**Corollary 11.** If \( G \cong A \times B \), where \( \text{POL-EQ} B \) is in \( P \), and \( A \cong \mathbb{Z}_m \) where \( m \) is squarefree, then \( \text{POL-EQ} G \) is in \( P \).

**Proof.** Now, \( A \cong \oplus_{p|m} \mathbb{Z}_p \) and all summands are \( B \) invariant. Every constant can be uniquely decomposed into a product of elements from \( \mathbb{Z}_p \) for \( p|m \). For a polynomial \( p \) let \( t(p) \) denote the polynomial when we replace each constant by its \( p \) part. Obviously, a polynomial is an identity over \( \mathbb{G} \) if and only if \( t(p) \) is an identity over \( \mathbb{Z}_p \times B \) for every prime \( p \) dividing \( m \). This can be checked in polynomial time by Theorem 10.

Unfortunately the same idea does not work for a noncyclic normal subgroup, \( A \). The collecting procedure can be used in a few other cases, though.

**Theorem 12.** Let \( G \cong A \times B \) such that the following hold:

(a) \( A \) is Abelian and the exponent of \( A \) is squarefree;

(b) \( \text{POL-EQ} B \) is in \( P \);

(c) for ever prime \( p \) dividing the size of \( A \) and \( \mathfrak{P} \in \text{Syl}_p(A) \) the group \( B/C_B(B) \) is Abelian and \( p \nmid |B/C_B(B)| \), where \( C_B(B) \) denotes the centralizer of \( \mathfrak{P} \) in \( B \).

Then \( \text{POL-EQ} G \) is in \( P \).

**Proof.** After the collection procedure we see that it is enough to check identities over \( B \) and identities of the form (2)

\[
a^{x_{11}}_{1}a^{x_{12}}_{2}\cdots a^{x_{1n}}_{n}a^{x_{21}}_{1}a^{x_{22}}_{2}\cdots a^{x_{2n}}_{n}\cdots a^{x_{k1}}_{1}a^{x_{k2}}_{2}\cdots a^{x_{kn}}_{n},
\]

and \( c_1^{w_1}c_2^{w_2} \cdots c_m^{w_m} \) for the constants. The Sylow subgroups of \( A \) are \( B \) invariant, hence it is enough to check the identity for the Sylows of \( A \). Thus we may assume that \( A \) is an elementary Abelian \( p \)-group. Let \( A \cong \mathbb{Z}_p^m \) and let \( \varphi : B \rightarrow \text{Aut} \mathbb{Z}_p^m \cong GL_m(\mathbb{Z}_p) \) be the action of \( B \) on \( A \), \( \varphi(B) = H \). With these notations we need to check identity (2) for \( G \cong \mathbb{Z}_p^m \times H \), where \( H \) is an Abelian matrix group acting faithfully on \( \mathbb{Z}_p^m \) (note that \( H \cong \mathbb{Z}_p/B/C_B(B) \)). Let \( S \) denote the subring of the ring.
of $m$ by $m$ matrices generated by $H$. Now (3) can be rewritten as:
\begin{equation}
a^{k_{11}x_{1}^{1}x_{2}^{1}k_{12}x_{2}^{1}k_{12}x_{2}^{2}k_{21}x_{n}^{1}k_{22}x_{n}^{2}k_{22}x_{n}^{n} + \cdots + k_{21}x_{n}^{1}x_{2}^{1}x_{2}^{2}k_{22}x_{n}^{1}x_{n}^{n}}
\end{equation}
and it is enough to check whether or not the exponent
\begin{equation}
x_{1}^{k_{11}x_{1}^{1}x_{2}^{1}k_{12}x_{2}^{1}k_{12}x_{2}^{2}k_{21}x_{n}^{1}k_{22}x_{n}^{2}k_{22}x_{n}^{n} + \cdots + k_{21}x_{n}^{1}x_{2}^{1}x_{2}^{2}k_{22}x_{n}^{1}x_{n}^{n}}
\end{equation}
is identically 0 in $S$ when substituting the elements of $H$. The ring $S$ acts semisimply on $\mathbb{Z}_p^m$, because $p \nmid |H|$. By Maschke’s theorem $S$ is a direct sum of matrix-rings. As $H$ is commutative, $S$ is commutative as well, hence $S$ is a direct sum of fields: $S = \bigoplus_{i=1}^{\lambda} F_{q_i}$. Let $H_i$ denote the projection of $H$ to its $i$th coordinate. Expression (5) is identically 0 over $S$ if and only if it is 0 at every substitution from $H_i$ for every $i \leq s$. By Lemma 9, this can be checked in polynomial time, and so POL-EQG is in $P$.

Finally, consider the identity $c_1^{w_1}c_2^{w_2} \cdots c_\lambda^{w_\lambda} = 1$. Here we can write every $c_j$ as a linear combination of some fixed basis, \{\$v_i$\}, of $A$. Let $c_j = \prod_{\lambda} v_{i_1}^{\lambda_{1,i}}$. Thus, it is enough to check, whether $v_{i_1}^{\lambda_{1,i_1}}v_{i_2}^{\lambda_{2,i_2}} \cdots v_{i_\lambda}^{\lambda_{\lambda,i_\lambda}} = 1$ is an identity for all $1 \leq i \leq s$. The exponent has to be identically 0 over $H_i$, and this can be checked in polynomial time by Lemma 9.

**Corollary 13.** Let $G \simeq A \times B$, where $A$ and $B$ are Abelian groups, such that the exponent of $A$ is squarefree and $(|A|, |B|) = 1$ then, POL-EQG is in $P$.

**Proof.** The conditions of Theorem 12 trivially hold.

Now, we investigate the case when neither the size nor the exponent of the normal subgroup is squarefree. The modification of Lemma 9 remains valid for cyclic groups.

**Lemma 14.** Let $f(x_1, \ldots, x_k) = w_1 + \cdots + w_\lambda$ be a sum of monomials in $k$ variables over $\mathbb{Z}_p^\omega$ ($p > 2$) and let $H$ be the $p - 1$ element subgroup of $\mathbb{Z}_p^\omega$. Then, for any $M \leq H$ it can be checked in polynomial time whether or not $f$ vanishes on $M$.

**Proof.** Let $a$ be a generator of $H$ and let $M = \langle a^{\lambda} \rangle$. Putting $z_j = x_j^\lambda$ we have $f(\bar{x})$ is identically 0 over $M$ if and only if $f(\bar{x})$ is identically 0 over $H$. We claim that a polynomial $f \in \mathbb{Z}_p[x_1, \ldots, x_k]$ admits this latter property if and only if $f = \sum(x_i^{p^\lambda - 1} - 1)g_i(\bar{x})$ for some $g_i \in \mathbb{Z}_p[x_1, \ldots, x_k]$. This condition can be checked in linear time. Since the exponent of $H$ is $p - 1$, if $f$ is of the required form, it vanishes over $H$. On the other hand, as the elements of $H$ are pairwise incongruent mod $p$ (not only mod $p^\lambda$), the polynomial has to vanish over $\mathbb{Z}_p^\omega$, as well. By Lemma 9, this happens if and only if $f = \sum(x_i^{p^\lambda - 1} - 1)g_{i_1}(\bar{x}) \mod p$ and so $f = \sum(x_i^{p^\lambda - 1} - 1)g_{i_1}(\bar{x}) + pf_{i_1} \mod p^\lambda$. Hence $f_{i_1}$ is vanishing mod $p^\lambda$. By the previous arguments $f_{i_1} = \sum(x_i^{p^\lambda - 1} - 1)g_{i_2}(\bar{x}) \mod p$. Continuing in the same fashion we obtain that $f = \sum(x_i^{p^\lambda - 1} - 1)g_{i_1}(\bar{x})$. 

\[\square\]
The following theorem is a generalization of Theorem 10:

**Theorem 15.** Let $G \simeq A \rtimes B$ such that the following hold:

(a) $A$ is cyclic;
(b) $\text{POL-EQ } B$ is in $P$;
(c) for every prime $p$ dividing the size of $A$ and $P \in \text{Syl}_p(A)$ we have $p \nmid |B/C_B(P)|$.

Then $\text{POL-EQ } G$ is in $P$.

**Proof.** Going along the lines of Theorem 12, we may assume that $A \simeq \mathbb{Z}_{p^m}$. Moreover, after the collection procedure, it is enough to check identities over $B$ and identities of the form $f = w_1 + w_2 + \cdots + w_l = 0$ over $B/C_B(P)$ (Note that this works for the constant part as well, since we can write every constant as a power of the generator of $A$.) As $B/C_B(P) \leq \text{Aut}(\mathbb{Z}_{p^m})$, condition (c) implies that $B/C_B(P) \leq H$, where $H$ denotes the $p-1$ element subgroup of $\text{Aut}(\mathbb{Z}_{p^m})$. If $p = 2$, then $H = 1$, if $p > 2$, then identities can be checked in polynomial time over $B$ and $H$, by condition (b), and by Lemma 14, respectively. 

3. Satisfiability

A modification of the collecting procedure and Lemma 9 will also help us to find out the complexity of the POL-SAT problem for some metacyclic groups, including $S_3$.

**Theorem 16.** For any group $G$ of order $pq$ where $p$ and $q$ are primes $\text{POL-SAT } G$ is in $P$.

**Proof.** Consider the case when $G \simeq A \rtimes B$ where $A \simeq \mathbb{Z}_p$ and $B \simeq \mathbb{Z}_q$. We may assume that $G$ is not abelian, and so $p \neq q$.

Let $\{t, s\}$ be an instance of POL-SAT $G$. We would like to know whether or not $t = s$ has a solution. Multiplying by $s^{-1}$ and writing $t$ for $ts^{-1}$, we have to solve $t = 1$. After the collecting procedure we obtain the following equation:

$$t(g_1 \cdots g_k) = (b_1 b_2 \cdots b_k) \cdot (a_1 b_2 b_3 \cdots b_k a_2 b_3 \cdots b_k \cdots a_k b_k a_{k-1} a_k) = 1.$$ 

As $p$ and $q$ are coprime, both

$$b_1 b_2 \cdots b_k = 1$$

and

$$a_1 b_2 b_3 \cdots b_k a_2 b_3 \cdots b_k \cdots a_k b_k a_{k-1} a_k = 1$$

must hold. Since $B$ is cyclic, we can solve $b_1 \cdots b_k = 1$ as a congruence mod $q$, and we can express one of the variables (say, $b_1$) using the other variables and constants: $b_1 = c \prod b_i^{k+d}$, this is what a solution looks like mod $q$. Substituting this expression for $b_1$ in $t_1 t_2' \cdots t_k t'$, we only need to check the complexity of the satisfiability
of this latter equation under the constraint for $b_1$. By a similar argument as in the proof of Theorem 10 we arrive at the solubility of
\[ a x_1^{k_{11}} x_2^{k_{12}} \cdots x_n^{k_{1n}} + x_1^{k_{21}} x_2^{k_{22}} \cdots x_n^{k_{2n}} + \cdots + x_1^{k_{n1}} x_2^{k_{n2}} \cdots x_n^{k_{nn}} = 1, \]
where $a$ is a generator of $A$. Now, it is enough to check whether or not the exponent attains 0, that is whether or not
\[ x_1^{k_{11}} x_2^{k_{12}} \cdots x_n^{k_{1n}} + x_1^{k_{21}} x_2^{k_{22}} \cdots x_n^{k_{2n}} + \cdots + x_1^{k_{n1}} x_2^{k_{n2}} \cdots x_n^{k_{nn}} = 0 \]
has a solution over $\mathbb{Z}_p$. As $p$ is a prime, this equation has no solution if and only if
\[ (x_1^{k_{11}} x_2^{k_{12}} \cdots x_n^{k_{1n}} + x_1^{k_{21}} x_2^{k_{22}} \cdots x_n^{k_{2n}} + \cdots + x_1^{k_{n1}} x_2^{k_{n2}} \cdots x_n^{k_{nn}})^{p-1} = 1 \]
is an identity. This can be checked in polynomial time by Lemma 9, hence POL-SAT $G$ is in $P$.

4. Problems

Klíma’s example mentioned in the introduction suggests the following question:

**Problem 1.** Is there an algebra $A$ such that POL-EQ $A$ is hard and POL-SAT $A$ is in $P$?

If there is an example, it will not be a group. Indeed, for a group $G$ every instance $f_1 \equiv f_2$ of POL-EQ $G$ can be rewritten in the form $f_1 f_2^{-1} \equiv 1$. If you can check the solubility of $p = a$ in polynomial time, then the only thing to do is to check the solubility of $f_1 f_2^{-1} = g$ for every $g \neq 1$. The two polynomials are equivalent if and only if none of these equations have a solution.

The smallest group not discussed in this paper is $S_4$. This group can be considered as a semidirect product of $\mathbb{Z}_2^2$ and $S_3$. Here, the exponent of the first group is squarefree, TERM-EQ $S_3$ is in $P$, but the action of $S_3$ is not Abelian. If we attack this problem using our technics, then after the collecting procedure, going along the lines of the proof of Theorem 12 or Theorem 15, we should discuss terms over $M_2(\mathbb{Z}_2)$ evaluated on the invertible elements.

**Problem 2.** Find the complexity of TERM-EQ $S_4$ and POL-SAT $S_4$.

References


[7] O. Klíma, Complexity issues of checking identities in finite monoids, manuscript.


