Equivalence and equation solvability problems for the alternating group $\mathbf{A}_4$

Gábor Horváth*

Institute of Mathematics, University of Debrecen, Pf. 12, Debrecen, 4010, Hungary

Csaba Szabó

Eötvös Loránd University, Department of Algebra and Number Theory, 1117 Budapest, Pázmány Péter sétány 1/c, Hungary

Abstract

It is observed in this paper that the complexities of the equivalence and the equation solvability problems are not determined by the clone of the algebra. In particular, we prove that for the alternating group on four elements these problems have complexity in P; if we extend the group by the commutator as an extra operation, then the equivalence problem is coNP-complete and the equation solvability problem is NP-complete.

Keywords: complexity, equivalence, equation solvability

1. Introduction

A group $\mathbf{G} = (G, \cdot, ^{-1})$ is a set G with a multiplication operation $\cdot$ and an inverse operation $^{-1}$. *Terms* for groups are finite words over the alphabet $\{ x_1, \dots, x_n, \dots \} \cup \{ x_1^{-1}, \dots, x_n^{-1}, \dots \}$, and *polynomials* over $\mathbf{G}$ are finite words over $\{ x_1, \dots, x_n, \dots \} \cup \{ x_1^{-1}, \dots, x_n^{-1}, \dots \} \cup \{ g \mid g \in G \}$. To each term or polynomial $t(x_1, \dots, x_n)$ and each group $\mathbf{G}$ one has a naturally associated *term or polynomial function* $t^{\mathbf{G}} \colon G^n \to G$. A group $\mathbf{G}$ *satisfies* an equation $s(\bar{x}) \approx t(\bar{x})$ or $\mathbf{G} \models s \approx t$ if the corresponding functions $s^{\mathbf{G}}$ and $t^{\mathbf{G}}$ are the same.

*Corresponding author. Phone: +36 52 512900/22798. Fax: +36 52 536914.

Email addresses: ghorvath@science.unideb.hu (Gábor Horváth), csaba@cs.elte.hu (Csaba Szabó)

The *(term or polynomial) equivalence problem* for a group $\mathbf{G}$ asks whether or not for two (term or polynomial) expressions s and t the group $\mathbf{G}$ satisfies $\mathbf{G} \models s \approx t$. Or equivalently, if s and t determine the same function over $\mathbf{G}$. The *equation solvability problem for* $\mathbf{G}$ asks whether or not $s = t$ for some substitution over $\mathbf{G}$.

The first results about the equivalence problem for various finite algebraic structures were carried out by Hunt and Stearns (see [1]). They considered finite commutative rings and finite lattices. It was shown that the equivalence problem for a finite commutative ring has polynomial time complexity if the ring is nilpotent, or is coNP-complete if the ring is not nilpotent. Later, Burris and Lawrence proved in [2] that the same holds for finite rings in general. Several results are published about the equivalence problem for finite monoids, e.g. [3], [4], [5], [6], [7], [8], [9], [10], [11].

The equivalence problem for finite groups has proved to be far more challenging. In 2004, Burris and Lawrence [12] proved that if $\mathbf{G}$ is nilpotent or $\mathbf{G} \simeq \mathbf{D_n}$, the dihedral group for odd n, then the equivalence problem for $\mathbf{G}$ has polynomial complexity. Horváth and Szabó [13] generalized this result and showed that if $\mathbf{G} \simeq \mathbf{A} \rtimes \mathbf{B}$, where $\mathbf{A}$ and $\mathbf{B}$ are abelian groups, such that the exponent of $\mathbf{A}$ is squarefree and $(|\mathbf{A}|, |\mathbf{B}|) = 1$, then the equivalence problem for $\mathbf{G}$ has polynomial complexity. Horváth, Lawrence, Mérai and Szabó [14] showed that if $\mathbf{G}$ is nonsolvable, then the equivalence problem is coNP-complete. The smallest group for which the computational complexity of the equivalence problem is not known is $\mathbf{S}_4$.

Goldmann and Russel [15] proved that if $\mathbf{G}$ is nilpotent then the equation solvability problem over $\mathbf{G}$ is in P, while if $\mathbf{G}$ is not solvable, then the equation solvability problem is NP-complete. Little is known for solvable, nonnilpotent groups. In [15] Goldmann and Russel explicitly ask for the complexity of the equation solvability problem for $\mathbf{S}_3$. In [13] it is proved that this problem is in P.

In Section 3 we extend the results of the paper [13] and prove that both the equation solvability and the equivalence problem has polynomial time complexity for the alternating group $\mathbf{A}_4$ (Theorems 6 and 7). Then in Section 4 we add the commutator as a new basic operation to the group $\mathbf{A}_4$, and consider the algebra $\mathbf{A}_4^{[,]} = (A_4, \cdot, [,])$. We prove that the equivalence problem over $\mathbf{A}_4^{[,]}$ is coNP-complete (Theorem 13) and the equation solvability problem over $\mathbf{A}_4^{[,]}$ is NP-complete (Theorem 14). These results show that the complexity of the equivalence and equation solvability problems may change

by changing the representation of the clone of the algebra. For two element algebras this cannot happen. Gorazd and Krzaczkowski [16] showed that for two element algebras the complexity of the equation solvability problem depends only on the clone and not on the presentation.

2. Preliminaries

We start with some notations and definitions.

Definition 1. Let $\mathbf{G}$ be a finite group.

1. The *equivalence problem for* $\mathbf{G}$ asks whether or not for two input term expressions s and t the corresponding functions are the same, i.e. does $\mathbf{G} \models s \approx t$ hold?
2. The *polynomial equivalence problem for* $\mathbf{G}$ asks whether or not for two input polynomial expressions p and q (possibly containing constants from G) the corresponding functions are the same, i.e. does $\mathbf{G} \models p \approx q$ hold?
3. The *equation solvability problem for* $\mathbf{G}$ asks whether or not two input polynomial expressions p and q (possibly containing constants from $\mathbf{G}$) attain the same value for at least one substitution from $\mathbf{G}$, i.e. does the equation $p = q$ have a solution over $\mathbf{G}$?

One might ask as item (4) the complexity of the term solvability problem. This problem is trivial, because substituting the identity element to every variable always gives a solution.

These questions are investigated from the computational perspective. For that, we need to define the '*length*' of a polynomial or term. The length of a polynomial p over $\mathbf{G}$ is the number of variable and constant symbols occurring in p. Let us denote the length of p by $\|p\|$.

Let $\mathbf{G}$ be a finite group, and N denote its number of elements. Let $p(x_1, \ldots, x_n)$ be a polynomial over $\mathbf{G}$. Replace every occurrence of x_i^{-1} in p by x_i^{N-1}. Denote the resulting polynomial by p'. Now, $\|p'\| \leq (N-1) \cdot \|p\|$, and $\mathbf{G} \models p \approx p'$. Thus, we may assume that the instances of the equivalence or equation solvability problems are inverse-free. Therefore, throughout the paper we consider the equivalence and equation solvability problems over the semigroup $\mathbf{G} = (G, \cdot)$.

For a group $\mathbf{G}$ let $\mathbf{G}^{[,]} = (G, \cdot, [,])$ be the algebra with underlying set G and with the group multiplication $\cdot$, and the commutator operation $[,]$, where

$[x, y] = x^{-1} \cdot y^{-1} \cdot x \cdot y$. The equivalence and equation solvability problems can be rephrased for $\mathbf{G}^{[,]}$ by allowing the expressions containing the commutator operation $[,]$:

Definition 2. Let $\mathbf{G} = (G, \cdot, ^{-1})$ be a given finite group.

1. The *equivalence problem for* $\mathbf{G}^{[,]} = (G, \cdot, [,])$ asks whether or not for two input term expressions s and t (possibly containing the commutator $[,]$) the corresponding functions are the same, i.e. does $\mathbf{G} \models s \approx t$ hold?
2. The *polynomial equivalence problem for* $\mathbf{G}^{[,]} = (G, \cdot, [,])$ asks whether or not for two input polynomial expressions p and q (possibly containing constants from G and the commutator $[,]$) the corresponding functions are the same, i.e. does $\mathbf{G} \models p \approx q$ hold?
3. The *equation solvability problem for* $\mathbf{G}^{[,]} = (G, \cdot, [,])$ asks whether or not two input polynomial expressions p and q (possibly containing constants from G and the commutator $[,]$) attain the same value for at least one substitution from $\mathbf{G}$, i.e. does the equation $p = q$ have a solution over $\mathbf{G}$?

Again, the length of a polynomial over $\mathbf{G}^{[,]}$ is defined as the number of variable and constant symbols occurring in p. An immediate consequence of the definition is the following lemma:

Lemma 3. *For polynomial expressions $p, q_1, \ldots, q_n$ we have*

$$\|p\,(q_1, \ldots, q_n)\| \leq \|p\| \cdot \max\{\, \|q_i\| : i = 1, \ldots, n \,\}.$$

For a group $\mathbf{G}$ with N elements we have $\mathbf{G} \models t \approx s$ if and only if $\mathbf{G} \models ts^{N-1} \approx 1$. Thus for groups we can restrict ourselves to checking identities of the form $t \approx 1$. Similarly, for the equation solvability: over $\mathbf{G}$ the equation $t = s$ can be solved if and only if the equation $ts^{N-1} = 1$ can be solved. These alterations to the identities/equations do not change the answer, and increase the length by a constant factor only. Thus the complexity does not change. Another easy but important observation is the following:

Proposition 4. *Let $\mathbf{G}$ be a finite group.*

1. *If the equivalence problem for $\mathbf{G}$ is coNP-complete, then the polynomial equivalence problem for $\mathbf{G}$ is coNP-complete, as well.*

2. *If the polynomial equivalence problem for* $\mathbf{G}$ *is in P, then the equivalence problem for* $\mathbf{G}$ *is in P, as well.*
3. *If the equation solvability problem for* $\mathbf{G}$ *is in P, then the (polynomial) equivalence problem for* $\mathbf{G}$ *is in P, as well.*

Proof. Items 1 and 2 are trivial, as every expression is a polynomial. For proving item 3 let the elements of $\mathbf{G}$ be $1 = g_1, \ldots, g_N$. If we need to decide for an expression t, whether or not $\mathbf{G} \models t \approx 1$, we decide for every $2 \leq i \leq N$ whether or not the equation $t = g_i$ has a solution over $\mathbf{G}$. If for an i (where $2 \leq i \leq N$) the equation $t = g_i$ is solvable, then clearly $\mathbf{G} \not\models t \approx 1$. If for every $2 \leq i \leq N$ the equation $t = g_i$ is not solvable, then $\mathbf{G} \models t \approx 1$. □

3. Equivalence and solvability for $\mathbf{A}_4$

We prove in this Section that the equation solvability problem for $\mathbf{A}_4$ is in P. In conjunction with Proposition 4 it follows that the (polynomial) equivalence problem for $\mathbf{A}_4$ is in P, as well.

The method called 'collecting procedure' was introduced in [13] to determine the complexity of the equivalence problem for some meta-Abelian groups. Now, we use it to determine the complexity of the equation solvability for $\mathbf{A}_4$. Let

$$\mathbf{A} = \left\{ \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right\}, \tag{1}$$

$$\mathbf{B} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\}, \tag{2}$$

where the group multiplication in $\mathbf{A}$ is the vector space addition, the group multiplication in $\mathbf{B}$ is the matrix multiplication and the action is defined by $v^M = M^{-1}vM = M(v)$. Here $M(v)$ denotes the usual matrix product. Note that $M(v) \neq Mv$, but this will cause no confusion in the paper. Now, $\mathbf{A} \simeq \mathbf{Z}_2^2$, $\mathbf{B} \simeq \mathbf{Z}_3$ and $\mathbf{A}_4$ is isomorphic to the semidirect product $\mathbf{A} \rtimes \mathbf{B}$. Every element $g \in \mathbf{A}_4$ can be uniquely written in the form $g = ba$, where $b \in \mathbf{B}$ and $a \in \mathbf{A}$. We refer to a and b as the $\mathbf{A}$-part and the $\mathbf{B}$-part of g, respectively. We shall usually refer to the elements of $\mathbf{A}$ by v (as vector) and refer to the elements of $\mathbf{B}$ by M (as matrix).

Let $t(x_1, \ldots, x_n)$ be a polynomial over $\mathbf{A}_4$, i.e. a product of variables and constants. We rewrite t by the steps of the **collecting procedure** from [13]:

Step 1. We introduce two n-tuples of new variables, $Y = \{ y_1, \ldots, y_n \}$ and $Z = \{ z_1, \ldots, z_n \}$ and write $z_j y_j$ for every occurrence of the variable x_j. We think of z_j and y_j as the **B**-parts and **A**-parts of x_j. Then every constant g occurring in t is replaced by ba, where b is the **B**-part and a is the **A**-part of g. This way we obtain a $2n$-ary polynomial, $t_2(y_1, \ldots, y_n, z_1, \ldots, z_n)$, where every odd element is over **B** and every even element is over **A**. There is a natural correspondence between evaluations of t over $\mathbf{A}_4$ and evaluations of t_2 where the values of elements of Z are from **B** and the values of elements of Y are from **A**. Clearly, $t(g_1, g_2 \ldots, g_n) = t_2(v_1, \ldots, v_n, M_1, \ldots, M_n)$, where v_i and M_i are the **A**-parts and **B**-parts of g_i.

Step 2. Now, using $ab = ba^b$ for every $a \in \mathbf{A}$ and $b \in \mathbf{B}$ we rewrite t_2 pulling all **B**-parts to the front. We obtain

$$t_2 = (b_1 b_2 \ldots b_k) \cdot \left(a_1^{b_2 b_3 \ldots b_k} a_2^{b_3 \ldots b_k} \ldots a_{k-1}^{b_k} a_k \right),$$

where b_i is either a variable z_i or the **B**-part of a constant occurring in t and similarly, a_i is either from Y or from **A**.

Step 3. As the groups **A** and **B** are abelian, we can regroup the elements with the same **A**-part and write the **B**-parts in a closed form. From the matrix representation of **B** and **A** we have $a^{b_1} a^{b_2} = a^{b_1 + b_2}$, hence we obtain

$$t_2 = M \cdot z_1^{\alpha_1} z_2^{\alpha_2} \ldots z_n^{\alpha_n} \cdot \prod a_i^{f_i(b_1, b_2 \ldots, b_k)},$$

where M is an element of **B**, $f_i(b_1, b_2 \ldots, b_k)$ is the sum of the monomials occurring as exponents of a_i in t_2. Let $v = [0, 1]^T \in \mathbf{A}$. Every constant a_i can be written as v^{M_i} for some $M_i \in \mathbf{B}$. Collecting the constants to the front we obtain

$$t_2 = M \cdot z_1^{\alpha_1} z_2^{\alpha_2} \ldots z_n^{\alpha_n} \cdot v^{f_0(b_1, b_2, \ldots, b_n)} \prod y_i^{f_i(b_1, b_2 \ldots, b_k)}.$$

Note that the whole procedure takes $O\left(\|t\|^3 \right)$ time.

Lemma 5. *Let $t\,(x_1, \ldots, x_n)$ be a group polynomial over $\mathbf{A}_4$, and let*

$$t_2 = M \cdot z_1^{\alpha_1} z_2^{\alpha_2} \ldots z_n^{\alpha_n} \cdot v^{f_0(b_1, b_2, \ldots, b_n)} \prod y_i^{f_i(b_1, b_2 \ldots, b_k)}$$

be the polynomial obtained from the collecting procedure. Assume that either $M = 1$ or there exists an i such that $3 \nmid \alpha_i$.

If there is an i such that $3 \nmid \alpha_i$, then let m be minimal such that $\alpha_m \not\equiv 0 \pmod 3$. Let us replace z_m by $\left(M \prod_{i \neq m} z_i^{\alpha_i} \right)^{-\alpha_m}$ in f_i for every $i =$

$0, 1, \ldots, n$ *and denote these polynomials by* g_i*. If* $M = 1$ *and* $3 \mid \alpha_i$ *for every* i*, then let* $g_i = f_i$*. Then the equation* $t = 1$ *cannot be solved if and only if*

1. *the polynomial* $g_0^3 - 1$ *is identically 0 for substitutions over* $\mathbf{B}$*, and*
2. *the polynomials* $g_1, \ldots, g_n$ *are identically 0 for substitutions over* $\mathbf{B}$*.*

Proof. Assume first that $g_0^3 - 1$ is not identically 0. As g_0 is a polynomial of matrices from $\mathbf{B}$, it attains either 0 or a value from $\mathbf{B}$. Since the exponent of $\mathbf{B}$ is 3, g_0 attains 0 for some $M_1, M_2, \ldots M_n$. Substituting $y_i = 1$ and $z_i = M_i$ we obtain $t = 1$.

Now, assume that $g_0^3 - 1$ is identically 0 and there is a g_j for some $1 \leq j \leq n$ such that g_j is not identically 0. Let $g_j(M_1, M_2, \ldots, M_n) \neq 0$. Substituting $z_i = M_i$, $y_j = v^{-g_0(M_1,\ldots,M_n)g_j(M_1,\ldots M_n)^{-1}}$ and $y_i = 1$, otherwise, we obtain $t = 1$.

For the other direction assume that $g_0^3 - 1$ and g_j are all identically 0. Then $g_0^3 = 1$ and g_0 attains a nonzero element b from $\mathbf{B}$ for any substitution. Thus $t = v^b \neq 1$ for any substitution. □

We are ready to prove the main result of this Section:

Theorem 6. *The equation solvability problem for* $\mathbf{A}_4$ *is in P.*

Proof. Let $\{p, q\}$ be an instance of the equation solvability problem for $\mathbf{A}_4$ and $t = pq^5$. The equation $p = q$ is solvable if and only if $t = 1$ has a solution. After the collecting procedure we obtain

$$t_2 = M \cdot z_1^{\alpha_1} z_2^{\alpha_2} \ldots z_n^{\alpha_n} \cdot v^{f_0(b_1,b_2,\ldots,b_n)} \prod y_i^{f_i(b_1,b_2\ldots,b_k)},$$

and $t = 1$ is solvable if and only if $t_2 = 1$ is solvable, where the variables z_i attain values form $\mathbf{B}$ and the variables y_i attain values from $\mathbf{A}$. Hence $t_2 = 1$ if and only if $M \cdot z_1^{\alpha_1} z_2^{\alpha_2} \ldots z_n^{\alpha_n} = 1$ and $v^{f_0(b_1,b_2,\ldots,b_n)} \prod y_i^{f_i(b_1,b_2\ldots,b_k)} = 1$ have a solution in common.

If $M \neq 1$ and $3 \mid \alpha_i$ for every i, then $M \cdot z_1^{\alpha_1} z_2^{\alpha_2} \ldots z_n^{\alpha_n} = M$ for every substitution and thus $t = 1$ has no solution. If $M = 1$ or not all α_i are divisible by 3, then by Lemma 5 we have to decide whether or not some polynomials are identically 0 over $\mathbf{B}$. The matrices of $\mathbf{B}$ generate a subring of $\mathbf{M_2(Z_2)}$ isomorphic to the four element field. We need to evaluate the polynomials only over the nonzero elements, and decide if they are identically 0 over these substitutions. By Lemma 9 in [13] this can be done in polynomial

time. Each of the above steps can be done in polynomial time in $\|t\|$, hence the equation solvability problem for $\mathbf{A}_4$ is in P . □

An immediate corollary of Proposition 4 and Theorem 6 is the following:

Theorem 7. *The (polynomial) equivalence problem for* $\mathbf{A}_4$ *is in P.*

4. Equivalence and solvability for $\mathbf{A}_4^{[,]}$

In this Section we consider the equivalence and satisfiability problems for the algebra $\mathbf{A}_4^{[,]}$. Over $\mathbf{A}_4^{[,]}$ every expression can be obtained using the group multiplication and the group commutator. We reduce the graph 3-colorability problem to the equivalence problem and to the solvability problem. For every graph Γ we construct an expression t_Γ over $\mathbf{A}_4^{[,]}$ and an element $a \in \mathbf{A}_4$ such that Γ is 3-colorable if and only if t_Γ is not an identity, if and only if the equation $t_\Gamma = a$ can be solved.

Let $\Gamma = (V, E)$ be an arbitrary simple graph with no loops or multiple edges, $V = \{ v_1, \ldots, v_n \}$ and $E = \{ e_1, \ldots, e_m \}$. We call a coloring of the vertices *proper* if the colors of adjacent vertices are distinct. The graph 3-colorability problem asks whether or not the vertices of an input graph Γ have a proper coloring by 3 colors. This problem is well-known to be NP-complete, see e.g. [17].

Let $\mathbf{V}$ denote the commutator subgroup of $\mathbf{A}_4$ and $\mathbf{1}$ denote the trivial subgroup of $\mathbf{A}_4$:

$$\mathbf{V} = \mathbf{A}_4' = \{(12)(34), (13)(24), (14)(23), id\}, \text{ and } \mathbf{1} = \{id\}.$$

We shall need the following observations about $\mathbf{A}_4$.

Lemma 8. *Let* $a \in \mathbf{V} \setminus \mathbf{1}$. *Then*

$$[a, \mathbf{V}] = [\mathbf{V}, a] = \begin{cases} \mathbf{V} & \text{if } a \notin \mathbf{V} \\ \mathbf{1} & \text{if } a \in \mathbf{V} \end{cases}$$

Proof. The statement can be checked by easy calculations. □

Definition 9. Let $x_1, x_2, z_1, z_2, \ldots z_m$ be distinct variables, and let

$$s_m(x_1, x_2, z_1, z_2, \ldots, z_m) = [[\ldots[[[x_1, x_2], z_1], z_2], \ldots, z_{m-1}], z_m]$$

be the left associated commutator of the $m + 2$ variables.

Proposition 10. *Let $g_1, \ldots, g_m \in \mathbf{A}_4$. Then*

$$s_m\left(\mathbf{A}_4, \mathbf{A}_4, g_1, \ldots, g_m\right) = \begin{cases} \mathbf{1} & \text{if } g_i \in \mathbf{V} \text{ for some } i, \\ \mathbf{V} & \text{if } g_i \notin \mathbf{V} \text{ for every } i. \end{cases}$$

Proof. We prove the Proposition by induction on m. As $s_1\left(\mathbf{A}_4, \mathbf{A}_4, g_1\right) = \left[\left[\mathbf{A}_4, \mathbf{A}_4\right], g_1\right]$ and $\left[\mathbf{A}_4, \mathbf{A}_4\right] = \mathbf{V}$, by Lemma 8 the statement holds. Now, observe that

$$s_{i+1}\left(\mathbf{A}_4, \mathbf{A}_4, g_1, \ldots, g_{i+1}\right) = \left[s_i\left(\mathbf{A}_4, \mathbf{A}_4, g_1, \ldots, g_i\right), g_{i+1}\right].$$

Hence, $s_i = \mathbf{1}$ implies $s_{i+1} = \mathbf{1}$. If $s_i = \mathbf{V}$, then again by Lemma 8 $s_{i+1} = \mathbf{1}$ if $g_{i+1} \in \mathbf{V}$ and $s_{i+1} = \mathbf{V}$ if $g_{i+1} \notin \mathbf{V}$. Thus $s_m = \mathbf{1}$ if and only if $g_i \in \mathbf{V}$ for some i and $s_m = \mathbf{V}$, otherwise. □

Let $\Gamma = (V, E)$ be an arbitrary simple graph with no loops or multiple edges, $V = \{ v_1, \ldots, v_n \}$ and $E = \{ e_1, \ldots, e_m \}$. Let $h_1, \ldots, h_n \in \mathbf{A}_4$ be arbitrary elements. Let us color the vertex v_i by the coset $h_i\mathbf{V}$. This is a 3-coloring of Γ. We exhibit a term expression $t_\Gamma\left(x_1, x_2, y_1, \ldots, y_n\right)$ over $\mathbf{A}_4$ such that

1. $t_\Gamma(\mathbf{A}_4, \mathbf{A}_4, h_1, \ldots, h_n) = \mathbf{1}$ if this 3-coloring is not a proper 3-coloring of Γ, and
2. $t_\Gamma(\mathbf{A}_4, \mathbf{A}_4, h_1, \ldots, h_n) = \mathbf{V}$ if this 3-coloring is a proper 3-coloring of Γ.

Definition 11. To every vertex, v_i of Γ we associate a variable y_i. For an edge $e_k = v_i v_j$ let $z_k = y_i y_j^5$. Define

$$t_\Gamma\left(x_1, x_2, y_1, y_2, \ldots, y_n\right) = s_m\left(x_1, x_2, z_1, z_2, \ldots, z_m\right),$$

where z_k runs through all edges of Γ.

Note that by Lemma 3 we have $\|t_\Gamma\| \leq 6 \cdot \|s_m\| \leq 6m + 12$.

Lemma 12. *Let $h_1, \ldots, h_n \in \mathbf{A}_4$. Let us color the vertex v_i by the coset $h_i\mathbf{V}$ for every $1 \leq i \leq n$.*

1. *If the coloring is* not *a proper 3-coloring, then $t_\Gamma\left(\mathbf{A}_4, \mathbf{A}_4, h_1, \ldots, h_n\right) = \mathbf{1}$.*
2. *If the coloring is a proper 3-coloring, then $t_\Gamma\left(\mathbf{A}_4, \mathbf{A}_4, h_1, \ldots, h_n\right) = \mathbf{V}$.*

Proof. For an edge $e_k = v_i v_j$ let $g_k = h_i h_j^{-1}$. Thus

$$t_\Gamma(x_1, x_2, h_1, h_2, \ldots, h_n) = s_m(x_1, x_2, g_1, g_2, \ldots, g_m). \tag{3}$$

First we prove (1). Assume that $h_1\mathbf{V}, \ldots, h_n\mathbf{V}$ is *not* a proper 3-coloring of Γ. Then there exists an edge $e_k = v_i v_j$ such that the vertices v_i and v_j are colored by the same coset. Thus $g_k = h_i h_j^{-1} \in \mathbf{V}$. Hence by (3) and by Proposition 10 we have $t_\Gamma(\mathbf{A}_4, \mathbf{A}_4, h_1, h_2, \ldots, h_n) = \mathbf{1}$.

Now we prove (2). Assume that $h_1\mathbf{V}, \ldots, h_n\mathbf{V}$ is a proper 3-coloring of Γ. Then for every edge $e_k = v_i v_j$ $(1 \leq k \leq m)$ the vertices v_i and v_j are colored by different cosets. Thus $g_k = h_i h_j^{-1} \notin \mathbf{V}$ for every $1 \leq k \leq m$. Hence by (3) and by Proposition 10 we have $t_\Gamma(\mathbf{A}_4, \mathbf{A}_4, h_1, h_2, \ldots, h_n) = \mathbf{V}$. □

We are ready to prove the two important results of the section.

Theorem 13. *The (polynomial) equivalence problem for* $\mathbf{A}_4^{[,]}$ *is coNP-complete.*

Proof. We polynomially reduce the graph 3-colorability problem to the equivalence problem of $\mathbf{A}_4$. Let $\Gamma = (V, E)$ be an arbitrary simple graph with no loops or multiple edges, $V = \{v_1, \ldots, v_n\}$ and $E = \{e_1, \ldots, e_m\}$. Let t_Γ be the term expression defined in Definition 11. We claim that $\mathbf{A}_4 \models t_\Gamma \approx 1$ if and only if Γ is *not* 3-colorable.

Assume first that Γ is 3-colorable. Let the 3-coloring of the vertices $v_1, \ldots, v_n$ be the cosets $h_1\mathbf{V}, \ldots, h_n\mathbf{V}$ for some $h_1, \ldots, h_n \in \mathbf{A}_4$. By (2) of Lemma 12 we have $t_\Gamma(\mathbf{A}_4, \mathbf{A}_4, h_1, \ldots, h_n) = \mathbf{V}$, i.e. there exist $u, v \in \mathbf{A}_4$ such that $t_\Gamma(u, v, h_1, \ldots, h_n) \neq 1$. Hence $\mathbf{A}_4 \not\models t_\Gamma \approx 1$.

Now assume that Γ is *not* 3-colorable, i.e. for every $h_1, \ldots, h_n \in \mathbf{A}_4$ the coloring $h_1\mathbf{V}, \ldots, h_n\mathbf{V}$ of the vertices $v_1, \ldots, v_n$ is not a proper coloring. By (1) of Lemma 12 we can conclude that $t_\Gamma(\mathbf{A}_4, \mathbf{A}_4, h_1, \ldots, h_n) = \mathbf{1}$ for every $h_1, \ldots, h_n \in \mathbf{A}_4$. Hence $\mathbf{A}_4 \models t_\Gamma \approx 1$. This proves the theorem, considering that $\|t_\Gamma\| \leq 6m + 12$. □

Theorem 14. *The equation solvability problem for* $\mathbf{A}_4^{[,]}$ *is NP-complete.*

Proof. The proof is similar to the one given for Theorem 13. We polynomially reduce the graph 3-colorability problem to the equation solvability problem for $\mathbf{A}_4$. Let $\Gamma = (V, E)$ be an arbitrary simple graph with no loops or multiple edges, $V = \{v_1, \ldots, v_n\}$ and $E = \{e_1, \ldots, e_m\}$. Let a be an arbitrary

element of $\mathbf{V}$ such that $a \neq 1$. Let t_Γ be the term expression defined in Definition 11. We claim that $t_\Gamma = a$ is solvable if and only if Γ is 3-colorable.

Assume first that Γ is 3-colorable. Let the 3-coloring of the vertices $v_1, \ldots, v_n$ be the cosets $h_1\mathbf{V}, \ldots, h_n\mathbf{V}$ for some $h_1, \ldots, h_n \in \mathbf{A}_4$. We have $t_\Gamma(\mathbf{A}_4, \mathbf{A}_4, h_1, \ldots, h_n) = \mathbf{V}$ by (2) of Lemma 12, i.e. for $a \in \mathbf{V}$ there exist $u, v \in \mathbf{A}_4$ such that $t_\Gamma(u, v, h_1, \ldots, h_n) = a$. Hence $t_\Gamma = a$ is solvable.

Now assume that Γ is *not* 3-colorable, i.e. for every $h_1, \ldots, h_n \in \mathbf{A}_4$ the coloring $h_1\mathbf{V}, \ldots, h_n\mathbf{V}$ of the vertices $v_1, \ldots, v_n$ is not a proper coloring. By (1) of Lemma 12 we can conclude that $t_\Gamma(\mathbf{A}_4, \mathbf{A}_4, h_1, \ldots, h_n) = \mathbf{1}$ for every $h_1, \ldots, h_n \in \mathbf{A}_4$. Hence $t_\Gamma = a$ is not solvable. This proves the theorem, considering that $\|t_\Gamma\| \leq 6m + 12$. □

5. Further comments, open problems

As we already mentioned in the Introduction, the characterization of the complexity of the equivalence and equation solvability problems for finite groups is not yet complete. The smallest group for which we do not know these complexities is $\mathbf{S}_4$:

Problem 1. Determine the complexity of the equivalence and equation solvability problems for the group $\mathbf{S}_4$.

As $\mathbf{S}_4 \simeq \mathbf{Z}_2^2 \rtimes \mathbf{S}_3$, one could use the collecting procedure for determining these complexities. There are two main obstacles: the first is that one needs to be able to solve equations over $\mathbf{S}_3$ in general, not only decide if they have a solution or not. The other obstacle is that $\mathbf{S}_3$ generates a non-commutative subring in $\mathbf{M}_2(\mathbf{Z}_2)$ (in fact, it generates $\mathbf{M}_2(\mathbf{Z}_2)$ itself), and there are no theorems about the complexity for the equivalence or equation solvability problems for non-commutative rings *when only substitutions from the multiplicative subgroup are considered.*

This paper disproves the subconscious conjecture that the complexity of the equivalence problem or of the equation solvability problem is determined by the clone of the algebra. In particular it is observed that the commutator can significantly shorten the length of expressions over $\mathbf{A}_4$, as it changes the complexity of the equivalence and equation solvability problems. One might wonder if other group operations have a similar property, or in general: if some expressions taken as basic operations can change the complexity of the equivalence or the equation solvability problems. This question is not only

interesting for groups, but for arbitrary algebraic structures. This motivates the following definition:

Definition 15. The *extended (polynomial) equivalence problem* for $\mathbf{V}$. Let $\mathbf{V} = (A, g_1, \ldots, g_m)$ be a finite algebra with underlying set A and with basic operations $g_1, \ldots, g_m$. Let $f_1, \ldots, f_n$ be polynomial expressions over the algebra $\mathbf{V}$. Let us denote by $(\mathbf{V}, f_1, \ldots, f_n)$ the algebra $(A, g_1, \ldots, g_m, f_1, \ldots, f_n)$, i.e. the algebra with underlying set A and with basic operations $g_1, \ldots, g_m$ together with $f_1, \ldots, f_n$ as well.

We say that the extended (polynomial) equivalence problem for $\mathbf{V}$ is in P if for all possible term (polynomial) expressions $f_1, \ldots, f_n$, built up from variables (and constants from $\mathbf{V}$) and the basic operations of $\mathbf{V}$, the (polynomial) equivalence problem over $(\mathbf{V}, f_1, \ldots, f_n)$ is in P.

We say that the extended (polynomial) equivalence problem for $\mathbf{V}$ is coNP-complete if there exist some term (polynomial) expressions $f_1, \ldots, f_n$, built up from variables (and constants from $\mathbf{V}$) and the basic operations of $\mathbf{V}$, such that the (polynomial) equivalence problem over $(\mathbf{V}, f_1, \ldots, f_n)$ is coNP-complete.

The extended equation solvability problem can be defined in a similar fashion. One can immediately observe that the extended problem is always 'at least as hard' as the original problem, since the length of an expression does not increase by using more operations to express it. Moreover, as every term expression is a polynomial expression, the extended polynomial problems are 'at least as hard' as the extended problems. With this new terminology we proved the following in this paper:

Theorem 16. *The extended (polynomial) equivalence problem for* $\mathbf{A}_4$ *is coNP-complete. The extended equation solvability problem for* $\mathbf{A}_4$ *is NP-complete.*

One might wonder about the situation of other finite groups. If $\mathbf{G}$ is not solvable, then the equivalence problem is coNP-complete [14], therefore the extended equivalence problem is coNP-complete as well. Similarly, if $\mathbf{G}$ is not solvable, then the equation solvability problem is NP-complete [15], therefore the extended equivalence problem is NP-complete as well. It is proved in [18], that if $\mathbf{G}$ is a nilpotent group, then the extended equivalence and the extended equation solvability problems are all in P, as are the (original) equivalence and equation solvability problems. Thus for nilpotent- and for

non-solvable groups the complexities of these problems do not change. It does change for $\mathbf{A}_4$, as we proved in this paper. If for an algebra the complexity of the extended problem does not coincide with the complexity of the original problem, it would be interesting to determine those operations which 'cause' the complexity change. The intuition is that these operation somehow play a significant role in the structure of the algebra in question. The smallest group to which our proof does not apply directly is $\mathbf{S}_3$:

Problem 2. Determine the complexity of the equivalence and equation solvability problems for $\mathbf{S}_3^{[,]}$.

Finally, a complete characterization of the extended problems for finite groups would be interesting. In order to achieve such a result, investigating the case of the smallest non-nilpotent group can be of importance.

Problem 3. Determine the complexity of the extended equivalence and extended equation solvability problems for groups in general. In particular find the complexity of the problems for $\mathbf{S}_3$.

6. Acknowledgements

This research was partially supported by the Hungarian National Foundation for Scientific Research grants K67870 and N67867.

References

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

[2] S. Burris, J. Lawrence, The equivalence problem for finite rings, J. of Symb. Comp. 15 (1993) 67–71.

[3] J. Almeida, M. V. Volkov, S. V. Goldberg, Complexity of the identity checking problem for finite semigroups, Journal of Mathematical Sciences 158 (5) (2009) 605–614.

[4] A. Kisielewicz, Complexity of semigroup identity checking, Int. J. of Alg. and Comp. 14 (4) (2004) 455–464.

[5] O. Klíma, Complexity issues of checking identities in finite monoids, Semigroup Forum 79 (3) (2009) 435–444.

[6] O. Klíma, Unification modulo associativity and idempotency, Ph.D. thesis, Masarik University, Brno (2004).

[7] S. Plescheva, V. Vértesi, Checking identities in 0-simple semigroups (in Russian), Journal of Ural State University 43 (2006) 72–102.

[8] S. Seif, Cs. Szabó, Algebra complexity problems involving graph homomorphism, semigroups and the constraint satisfaction problem, J. Complexity 19 (2) (2003) 153–160.

[9] S. Seif, Cs. Szabó, Computational complexity of checking identites in 0-simple semigroups and matrix semigroups over finite fields, Semigroup Forum 72 (2) (2006) 207–222.

[10] P. Tesson, Computational complexity questions related to finite monoids and semigroups, Ph.D. thesis, McGill University, Montreal (2004).

[11] P. Tesson, D. Thérien, Monoids and computations, International Journal of Algebra and Computation 14 (5-6) (2004) 801–816.

[12] S. Burris, J. Lawrence, Results on the equivalence problem for finite groups, Alg. Univ. 52 (4) (2004) 495–500, (2005).

[13] G. Horváth, Cs. Szabó, The complexity of checking identities over finite groups, Internat. J. Algebra Comput. 16 (5) (2006) 931–940.

[14] G. Horváth, J. Lawrence, L. Mérai, Cs. Szabó, The complexity of the equivalence problem for non-solvable groups, Bull. Lond. Math. Soc. 39 (3) (2007) 433–438.

[15] M. Goldmann, A. Russell, The complexity of solving equations over finite groups, in: Proceedings of the 14th Annual IEEE Conference on Computational Complexity, Atlanta, Georgia, 1999, pp. 80–86.

[16] T. A. Gorazd, J. Krzaczkowski, The complexity of problems connected with two-element algebras, Reports on Mathematical Logic 46 (2011) 91–108.

[17] M. R. Garey, D. S. Johnson, Computers and Intractability: A Guide to the Theory of NP-completeness, W. H. Freeman & Co., San Francisco, 1979.

[18] G. Horváth, The complexity of the equivalence and equation solvability problems over nilpotent rings and groups, Algebra Universalis 66 (4) (2011) 391–403.