Discrete Mathematics and Theoretical Computer Science DMTCS vol. **13:4**, 2011, 23–32

The extended equivalence and equation solvability problems for groups

Gábor Horváth[1†] and Csaba Szabó[2 ‡]

[1] *Institute of Mathematics, University of Debrecen, Hungary*
[2] *Department of Algebra and Number Theory, Eötvös Loránd University, Budapest, Hungary*

received 30th September 2010, *revised 27th April 2011*, *accepted 28th April 2011.*

We prove that the extended equivalence problem is solvable in polynomial time for finite nilpotent groups, and coNP-complete, otherwise. We prove that the extended equation solvability problem is solvable in polynomial time for finite nilpotent groups, and NP-complete, otherwise.

Keywords: complexity, extended equation solvability, extended equivalence, groups

1 Introduction

The algorithmic aspects of the equivalence problem and the equation solvability problem have received increasing attention in the past two decades. The equivalence problem for a finite algebra $\mathbf{A}$ asks whether or not two (term or polynomial) expressions s and t are equivalent over $\mathbf{A}$ (denoted by $\mathbf{A} \models s \approx t$), i.e. if s and t determine the same function over $\mathbf{A}$. The equation solvability is one of the oldest problems of algebra: it asks whether or not two (term or polynomial) expressions s, t can attain the same value for some substitution over a finite algebra $\mathbf{A}$, i.e. if the equation $s = t$ can be solved. The complexity of the equivalence and equation solvability problems have been thoroughly investigated for finite classical algebras, e.g. for finite rings Burris and Lawrence (1993); Hunt and Stearns (1990); Lawrence and Willard (1997); Szabó and Vértesi (2011), for finite groups Burris and Lawrence (2004); Goldmann and Russell (2002); Horváth (2011); Horváth et al. (2007); Horváth and Szabó (2006), or for finite semigroups and monoids Almeida et al. (2009); Kisielewicz (2004); Klíma (2004, 2009); Plescheva and Vértesi (2006); Seif and Szabó (2006). The complexity of these questions is determined with respect to the length of the input term or polynomial expressions.

In many situations a term or polynomial can be expressed in a more concise way using new operations, not only the basic operations of the algebra. For example, the length of $[[[x_1, x_2], x_3], \ldots, x_n]$ is n if expressed by using the commutator, and is $O(2^n)$ if expressed by using the group multiplication. Such a change in the length suggests that the complexity of the equivalence or of the equation solvability

†Email: `ghorvath@science.unideb.hu`
‡Email: `csaba@cs.elte.hu`

problems may change as well. It is indeed the case in some situation: in Horváth and Szabó (2011) it is shown that for the alternating group on four elements these problems have complexity in P; but if the group is extended by the commutator as an extra operation, then the equivalence problem is coNP-complete and the equation solvability problem is NP-complete. Such a complexity change cannot occur for two element algebras Gorazd and Krzaczkowski (2011). To further investigate whether or not additional operations can affect the complexity of the equivalence and equation solvability problems, we introduce their extended version for finite groups.

Definition 1 *Let* $\mathbf{G} = (G, \cdot)$ *be a finite group. We say that the* extended equivalence (equation solvability) problem *over* $\mathbf{G}$ *is in P, if for arbitrary terms* $f_1, \ldots, f_k$ *the equivalence (equation solvability) problem over* $(G, \cdot, f_1, \ldots, f_k)$ *is in P. We say that the extended equivalence problem over* $\mathbf{G}$ *is coNP-complete (the equation solvability problem is NP-complete), if there exist terms* $f_1, \ldots, f_k$ *such that the equivalence problem over* $(G, \cdot, f_1, \ldots, f_k)$ *is coNP-complete (the equation solvability problem over* $(G, \cdot, f_1, \ldots, f_k)$ *is NP-complete).*

It is clear that the complexity of an extended problem is at least as hard as the original problem. Definition 1 can be extended to arbitrary algebras, e.g. for rings. Considering finite rings and applying the methods described in Burris and Lawrence (1993); Horváth (2011); Hunt and Stearns (1990) one can arrive at a similar dichotomy theorem for the extended problems as for the one about the original problems.

Theorem 2 *Let* $\mathcal{R}$ *be a finite ring. If* $\mathcal{R}$ *is nilpotent, then the extended equivalence and extended equation solvability problems can be solved in polynomial time. If* $\mathcal{R}$ *is non-nilpotent, then the extended equivalence problem is coNP-complete, and the extended equation solvability problem is NP-complete.*

The main results of this paper are two similar theorems for groups.

Theorem 3 *Let* $\mathbf{G} = (G, \cdot)$ *be a finite group. If* $\mathbf{G}$ *is nilpotent, then the equivalence problem over* $\mathbf{G}$ *can be solved in polynomial time. If* $\mathbf{G}$ *is non-nilpotent, then there exists a term* f *over* $\mathbf{G}$ *such that the equivalence problem over* $(G, \cdot, f)$ *is coNP-complete.*

Theorem 4 *Let* $\mathbf{G} = (G, \cdot)$ *be a finite group. If* $\mathbf{G}$ *is nilpotent, then the equation solvability problem over* $\mathbf{G}$ *can be solved in polynomial time. If* $\mathbf{G}$ *is non-nilpotent, then there exists a term* f *over* $\mathbf{G}$ *such that the equation solvability problem over* $(G, \cdot, f)$ *is NP-complete.*

For non-nilpotent, solvable groups we prove Theorems 3 and 4 by induction. The initial case of the induction is considered in Section 2, then we prove Theorems 3 and 4 in general in Section 3. We finish the paper by mentioning some open problems in Section 4.

2 Abelian normal subgroup

Let $\mathbf{G} = (G, \cdot)$ be a finite, solvable, non-nilpotent group. Let us consider the lower central series of $\mathbf{G}$: $\gamma_0(\mathbf{G}) = \mathbf{G}$, $\gamma_i(\mathbf{G}) = [\mathbf{G}, \gamma_{i-1}(\mathbf{G})]$. Let us denote by $\gamma(\mathbf{G})$ the normal subgroup in which this decreasing sequence terminates, and let T be the smallest positive integer such that $\gamma_T(\mathbf{G}) = \gamma(\mathbf{G})$. We prove the solvable, non-nilpotent group case of Theorems 3 and 4 by induction on the order of the group. The initial case is where both $\gamma(\mathbf{G})$ and $\mathbf{G}/C_{\mathbf{G}}\big(\gamma(\mathbf{G})\big)$ are commutative.

Theorem 5 *Let* $\mathbf{G} = (G, \cdot)$ *be a finite, solvable, non-nilpotent group. Assume that the groups* $\gamma(\mathbf{G})$ *and* $\mathbf{G}/C_{\mathbf{G}}\big(\gamma(\mathbf{G})\big)$ *are commutative. Then there exists a term* f *such that the equivalence problem over* $(G, \cdot, f)$ *is coNP-complete, and the equation solvability problem over* $(G, \cdot, f)$ *is NP-complete.*

Proof: We prove that there exists a term f such that the equivalence problem over $(G, \cdot, f)$ is coNP-complete. Let $\mathbf{A} = \gamma(\mathbf{G})$ and $\mathbf{B} = \mathbf{G}/C_{\mathbf{G}}\big(\gamma(\mathbf{G})\big)$. Let $\mathrm{End}\ \mathbf{A}$ denote the endomorphism ring of $\mathbf{A}$. The group $\mathbf{G}$ acts on $\mathbf{A}$ by conjugation. This action of $\mathbf{G}$ is isomorphic to $\mathbf{B}$. We identify $\mathbf{B}$ with its image in $\mathrm{End}\ \mathbf{A}$. Let $\varphi\colon \mathbf{G} \to \mathbf{B}$ denote the natural homomorphism from $\mathbf{G}$ onto $\mathbf{B}$. Let $\mathcal{R}$ be the ring generated by $\mathbf{B}$ in $\mathrm{End}\ \mathbf{A}$, i.e. $\mathcal{R} = \langle \mathbf{B} \rangle_{\mathrm{End}\ \mathbf{A}}$. Since $\mathbf{B}$ is commutative, $\mathcal{R}$ is commutative as well. Moreover $1 \in \mathbf{B}$ implies $1 \in \mathcal{R}$. Note that $\mathbf{A}$ is a faithful left-module over $\mathrm{End}\ \mathbf{A}$, and therefore it is a faithful module over the commutative ring $\mathcal{R}$.

Denote the action of the ring element $r \in \mathcal{R}$ on $a \in \mathbf{A}$ by a^r. For example, if $a \in \mathbf{A}$, $g \in \mathbf{G}$, $b = \varphi(g)$, then $a^1 = a$, $a^b = a^{\varphi(g)} = g^{-1}ag$, and

$$a^{b-1} = a^{\varphi(g)-1} = a^{-1+\varphi(g)} = a^{-1}g^{-1}ag = [a, g].$$

Let us denote the set of commutator actions in $\mathrm{End}\ \mathbf{A}$ by $\mathcal{C}$: $\mathcal{C} = \{\, b - 1 \mid b \in \mathbf{B} \,\}$. Let $\mathcal{R}_c \leq \mathrm{End}\ \mathbf{A}$ be the subring of $\mathcal{R}$ generated by the commutator actions:

$$\mathcal{R}_c = \langle \mathcal{C} \rangle_{\mathcal{R}} = \langle b - 1 \mid b \in \mathbf{B} \rangle_{\mathcal{R}} = \langle \varphi(g) - 1 \mid g \in \mathbf{G} \rangle_{\mathcal{R}}.$$

Note, that $\mathbf{A}$ is a faithful $\mathcal{R}_c$-module, as well. Note that $|\mathbf{B}| = |\mathcal{C}|$. Let $c = |\mathcal{C}|$, and let $d = |R_c|$. Let $\mathcal{J}_c$ denote the Jacobson radical of $\mathcal{R}_c$.

We prove the theorem in the following steps.

1. We prove in Lemma 6 that there exists a polynomial p with integer coefficients such that $\mathcal{R}_c = p(\varphi(\mathbf{G}))$.

2. We prove in Lemma 7 that the ring $\mathcal{R}_c$ is non-nilpotent, that is $\mathcal{R}_c/\mathcal{J}_c$ is a direct sum of finite fields $\mathcal{F}_1, \ldots, \mathcal{F}_l$. Assume that $|\mathcal{F}_1| \geq \cdots \geq |\mathcal{F}_l|$.

3. Let q_1 denote the number of elements of $\mathcal{F}_1$. We prove in Lemma 8 that $q_1 \geq 3$.

4. We introduce the term f using the polynomial p from Step 1. We polynomially reduce the GRAPH q_1-coloring problem to the equivalence problem over $(G, \cdot, f)$. The instance of the GRAPH q_1-coloring problem is a graph Γ, and it asks whether or not the vertices of Γ can be colored by q_1 colors such that no two adjacent vertices share the same color. This problem is well-known to be NP-complete Karp (1972). For an arbitrary graph Γ we construct a term expression t_Γ over $(G, \cdot, f)$ such that $(G, \cdot, f) \models t_\Gamma \approx 1$ if and only if the graph Γ is *not* q_1-colorable. The length of t_Γ will be linear in the size of Γ.

In step 1 we prove that $\mathcal{R}_c$ is a verbal subring of $\mathcal{R}$.

Lemma 6 *There exists a polynomial p with integer coefficients such that* $\mathcal{R}_c = p(\mathbf{B}) = p(\varphi(\mathbf{G}))$.

Proof: Let $\mathcal{C} = \{\, u_1, \ldots, u_c \,\}$ and $\mathcal{R}_c = \{\, r_1, \ldots, r_d \,\}$. As $\mathcal{R}_c = \langle \mathcal{C} \rangle_{\mathcal{R}}$, for every $r_i \in \mathcal{R}_c$ there exist a polynomial p_i with integer coefficients such that p_i has no constant coefficient and $r_i = p_i(u_1, \ldots, u_c)$. For every $r_i \in \mathcal{R}_c$ let us fix such a polynomial p_i. Let

$$p(x_{1,1}, \ldots, x_{d,c}) = \sum_{i=1}^{d} p_i(x_{i,1} - 1, x_{i,2} - 1, \ldots, x_{i,c} - 1).$$

Clearly, $p(\mathbf{B}) \subseteq \mathcal{R}_c$. Let $b_j = u_j + 1$ for $1 \leq j \leq c$. Then $\mathbf{B} = \{ b_1, \dots, b_c \}$. Let us fix $1 \leq i \leq d$ and consider the substitution $x_{i,j} = b_j$, $x_{l,j} = 1$ $(l \neq i)$. For this substitution the value of p is $p_i(u_1, \dots, u_c) = r_i$. Hence $r_i \in p(\mathbf{B})$ yielding $\mathcal{R}_c = p(\mathbf{B}) = p(\varphi(\mathbf{G}))$. □

We continue with step 2 of the proof.

Lemma 7 *The ring $\mathcal{R}_c$ is non-nilpotent.*

Proof: Let $F(\mathbf{G})$ denote the Fitting subgroup of $\mathbf{G}$, the unique largest nilpotent normal subgroup of $\mathbf{G}$ Robinson (1995). As $\mathbf{G}$ is non-nilpotent, $F(\mathbf{G}) \neq \mathbf{G}$, and $F(\mathbf{G})$ is the set of left-Engel elements Baer (1957). An element $g \in \mathbf{G}$ is a left-Engel element, if for every $h \in \mathbf{G}$ there exists a positive integer k_h, such that the k_h-iterated commutator of h by g is the identity element: $[[[h, g], g] \dots g] = 1$. Let $g \in \mathbf{G}$ be arbitrary, and let $r = \varphi(g) - 1$. We prove that g is a left-Engel element if and only if r is nilpotent.

Assume that g is a left-Engel element. Now, for every $h \in \mathbf{G}$ there exists a positive integer k_h, such that the k_h-iterated commutator of h by g is the identity element: $[[[h, g], g] \dots g] = 1$. Let k be the maximum of these numbers: $k = \max \{ k_h \mid h \in \mathbf{G} \}$. Recall that as $\gamma(\mathbf{G}) \lhd \mathbf{G}$ and $\gamma(\mathbf{G})$ is abelian, we have $\gamma(\mathbf{G}) \subseteq F(\mathbf{G})$. Then for every $a \in \mathbf{A}$ we have $[[[a, g], g] \dots g] = 1$. By $[a, g] = a^{\varphi(g)-1} = a^r$ we obtain $a^{r^k} = 1$, yielding $r^k = 0$, i.e. r is nilpotent.

Now, assume that r is nilpotent. Let k be the smallest positive integer such that $r^k = 0$. That is, for every $a \in \mathbf{A}$ we have $a^{r^k} = 1$. From $a^r = [a, g]$, we obtain that the k-iterated commutator of a by g is the identity of $\mathbf{G}$: $[[[a, g], g] \dots g] = 1$. Let T be the positive integer for which $\mathbf{A} = \gamma_T(\mathbf{G})$. Let $h \in \mathbf{G}$ be arbitrary, then the T-iterated commutator of h by g is an element of $\mathbf{A}$: $[[[h, g], g] \dots g] \in \mathbf{A}$. Thus the $(T + k)$-iterated commutator of h by g is the identity element of $\mathbf{G}$: $[[[h, g], g] \dots g] = 1$ Therefore g is a left-Engel element. □

Let $\mathcal{J}_c$ denote the Jacobson radical of $\mathcal{R}_c$. Now, $\mathcal{R}_c / \mathcal{J}_c$ is a direct sum of finite fields (Jacobson, 1945, Theorem 27). In step 3 we prove that at least one of these fields contains more than two elements.

Lemma 8 *For the ring $\mathcal{R}_c$ we have $\mathcal{R}_c / \mathcal{J}_c \neq \mathbb{Z}_2^l$.*

Proof: We prove the lemma indirectly: assume that $\mathcal{R}_c / \mathcal{J}_c = \mathbb{Z}_2^l$ for some positive integer l. Now, $\left(r^2 + r\right) \in \mathcal{J}_c$ for every $r \in \mathcal{R}_c$. Let t be the smallest positive integer for which r^t is idempotent for every $r \in \mathcal{R}_c$ and the exponent of $\mathbf{G}$ divides t. Thus $\mathcal{R}_c / \mathcal{J}_c = \mathbb{Z}_2^l$ implies $\left(r^2 + r\right)^t = 0$ for every $r \in \mathcal{R}_c$. Let $b = \varphi(g)$ for some $g \in \mathbf{G} \setminus F(\mathbf{G})$. In the proof of Lemma 7 it is shown that commuting with g is a non-nilpotent action, that is $(b - 1)$ is non-nilpotent. Let $r = (b - 1)$, then $r \in \mathcal{R}_c$. Let us calculate the value of $\left(r^2 + r\right)^t$ in the ring $\mathcal{R}$. Since $\mathcal{R}$ is a commutative unital ring, $\left(r^2 + r\right)^t = r^t \cdot (r + 1)^t = r^t \cdot b^t$. The exponent of $\mathbf{G}$ divides t, hence $b^t = \varphi(g)^t = \varphi(g^t) = \varphi(1) = 1$. Thus $\left(r^2 + r\right)^t = 0$ yields $r^t = 0$, contradicting that r is a non-nilpotent element. □

We continue with step 4 of the proof. Let $\mathcal{F}_1, \dots, \mathcal{F}_l$ be the fields occurring as a direct summand in $\mathcal{R}_c / \mathcal{J}_c$ (with multiplicity), i.e. $\mathcal{R}_c / \mathcal{J}_c = \oplus_{i=1}^l \mathcal{F}_i$. Assume that $|\mathcal{F}_1| \geq \dots \geq |\mathcal{F}_l|$, and let $q_1 = |\mathcal{F}_1|$. By Lemma 8 we have $q_1 \geq 3$. By Lemma 6 we can define the term f. Let p be the polynomial in Lemma 6. The polynomial p depends on dc variables, where $c = |\mathcal{C}|$, $d = |\mathcal{R}_c|$. Let $\bar{x}_1$ and $\bar{x}_2$ be disjoint vectors of dc variables, that is the set of variables of $\bar{x}_1$ is disjoint from the set of variables of $\bar{x}_2$. Let f be defined in the following way:

$$f(y, \bar{x}_1, \bar{x}_2) = y^{(p(\bar{x}_1) - p(\bar{x}_2))}, \tag{1}$$

Now, f is a term over $\mathbf{G}$ and it depends on $2dc+1$ variables. We shall polynomially reduce the GRAPH q_1-coloring to the equivalence problem over $(G,\cdot,f)$. By Lemma 8 we have $q_1 \geq 3$, thus the GRAPH q_1-coloring is NP-complete Karp (1972). Let $\Gamma = (V,E)$ be an arbitrary simple graph with no loops. Let $V = \{ v_1, \dots, v_n \}$ be its set of vertices and let $E = \{ e_1, \dots, e_m \}$ be the set of its edges. Let t be the smallest positive integer such that for every $r \in \mathcal{R}_c$ the element r^t is idempotent. In particular, if $r \in \mathcal{J}_c$ then $r^t = 0$. Let

$$u_\Gamma(z_1,\dots,z_n) = \prod_{v_i v_j \in E} (z_i - z_j)^t. \tag{2}$$

We would like to express $y^{u_\Gamma(z_1,\dots,z_n)}$ using f defined by (1), where each z_i runs through $\mathcal{R}_c$ and y runs through $\mathbf{A}$. We achieve this in two steps. We construct

$$W(y,\bar{x}_1,\dots,\bar{x}_n) = y^{u_\Gamma(p(\bar{x}_1),\dots,p(\bar{x}_n))} = y^{\prod_{v_i v_j \in E}(p(\bar{x}_i)-p(\bar{x}_j))^t}$$

for disjoint $\bar{x}_1,\dots,\bar{x}_n$ vectors of dc variables, ensuring that the arguments of u_Γ will be in $\mathcal{R}_c$. Then we guarantee that the value of y will be in $\mathbf{A}$.

Let $\bar{x}$ denote the vector of all 'x' variables, i.e. $\bar{x} = (\bar{x}_1,\dots,\bar{x}_n)$. Now, we want to express $W(y,\bar{x})$. Although, W is a term over $\mathbf{G}$, its length would be exponential in the size of Γ using only the group multiplication. We shall express W using f, and thus the length of W will be linear in the size of Γ. For every edge $e = v_i v_j$ let $w_e(y,\bar{x})$ be the t-times iterated version of $f(y,\bar{x}_i,\bar{x}_j)$:

$$w_e(y,\bar{x}) = f \circ f \circ \dots \circ f(y,\bar{x}_i,\bar{x}_j) = y^{(p(\bar{x}_i)-p(\bar{x}_j))^t}.$$

Let $W(y,\bar{x})$ denote the composition of the terms w_e:

$$W(y,\bar{x}) = w_{e_1} \circ w_{e_2} \circ \dots \circ w_{e_m}(y,\bar{x}) = y^{u_\Gamma(p(\bar{x}_1),\dots,p(\bar{x}_n))}.$$

As $\mathbf{A}$ is a verbal normal subgroup of $\mathbf{G}$, there exists a term $s(\bar{y})$ of variables $\bar{y} = (y_1,\dots,y_k)$ such that $s(\mathbf{G}) = \mathbf{A}$. Finally, let

$$t_\Gamma(\bar{y},\bar{x}) = W(s(\bar{y}),\bar{x}). \tag{3}$$

The length of t_Γ is linear in the size of Γ: for every edge $e \in E$ we have $\|w_e\| \leq 2tcd+1 = O(1)$. Moreover, $\|W\| \leq \|w_{e_1}\| + \dots + \|w_{e_m}\| + 1 = O(m)$. Finally, $\|t_\Gamma\| \leq \|W\| \cdot \|s\| = O(m)$, as s depends only on $\mathbf{G}$ and not on Γ.

We prove that Γ is *not* colorable by q_1 colors if and only if $(G,\cdot,f) \models t_\Gamma \approx 1$. Assume that Γ is q_1-colorable. Color the vertices of Γ by the elements of $\mathcal{F}_1$. Thus there exist elements $r_1,\dots,r_n \in \mathcal{R}_c$ such that the color of v_i is the $\mathcal{F}_1$-component of r_i. That is, if $\psi\colon \mathcal{R}_c \to \mathcal{F}_1$ is the natural homomorphism, then $\psi(r_i)$ is the color of v_i. Now, for every edge $v_i v_j$ the $\mathcal{F}_1$-component of $(r_i - r_j)$ is not 0. Hence $(r_i - r_j)^t = 1$ in $\mathcal{F}_1$ for every edge $v_i v_j$. That is, the $\mathcal{F}_1$-component of $u_\Gamma(r_1,\dots,r_n)$ is 1, and $u_\Gamma(r_1,\dots,r_n) \neq 0$. Therefore there exists an element $a \in \mathbf{A}$ such that $a^{u_\Gamma(r_1,\dots,r_n)} \neq 1$. For every $1 \leq i \leq n$ let $\bar{g}_i \in \mathbf{G}^{dc}$ such that $r_i = p(\bar{g}_i)$ and let $\bar{g} = (\bar{g}_1,\dots,\bar{g}_n)$. Let $\bar{h} \in \mathbf{G}^k$ such that $a = s(\bar{h})$. Now,

$$t_\Gamma(\bar{h},\bar{g}) = s(\bar{h})^{u_\Gamma(p(\bar{g}_1),\dots,p(\bar{g}_n))} = a^{u_\Gamma(r_1,\dots,r_n)} \neq 1.$$

Assume now, that Γ is not q_1-colorable. Consider an arbitrary substitution of t_Γ. Let $\bar{h} \in \mathbf{G}^k$ be arbitrary and for every $1 \leq i \leq n$ let $\bar{g}_i \in \mathbf{G}^{dc}$ be arbitrary. Let $\bar{g} = (\bar{g}_1,\dots,\bar{g}_n)$. Let $a = s(\bar{h})$ and let

$r_i = p_i(\bar{g}_i)$. Now, $a \in \mathbf{A}$ and

$$t_\Gamma\left(\bar{h}, \bar{g}\right) = s\left(\bar{h}\right)^{u_\Gamma(p(\bar{g}_1),\ldots,p(\bar{g}_n))} = a^{u_\Gamma(r_1,\ldots,r_n)}.$$

We prove that $u_\Gamma(r_1, \ldots, r_n) = 0$. For this substitution, let us define the color of v_i to be the $\mathcal{F}_1$-component of r_i. Since Γ is not q_1-colorable, there exists an edge $v_i v_j$ such that the $\mathcal{F}_1$-components of r_i and r_j are the same. Thus the $\mathcal{F}_1$-component of $\prod_{v_i v_j \in E}(r_i - r_j)$ is 0. For every $1 \le k \le l$ we have $q_1 \ge |\mathcal{F}_k|$, i.e. the graph Γ is not $|\mathcal{F}_k|$-colorable. Thus, in a similar fashion, it follows that the $\mathcal{F}_k$-component of $\prod_{v_i v_j \in E}(r_i - r_j)$ is 0, as well. That is $\prod_{v_i v_j \in E}(r_i - r_j) \in \mathcal{J}_c$ yielding $u_\Gamma(r_1, \ldots, r_n) = \left(\prod_{v_i v_j \in E}(r_i - r_j)\right)^t = 0$ in $\mathcal{R}_c$. Note that Lemma 8 was used for $q_1 = |\mathcal{F}_1| \ge 3$, i.e. the GRAPH q_1-coloring is NP-complete.

Finally, we prove that the equation solvability over $(G, \cdot, f)$ is NP-complete. The proof is literally the same as the proof of the coNP-completeness of the equivalence problem, apart from the following differences. Let $r \in \mathcal{R}_c$ be an idempotent such that its $\mathcal{F}_1$-component is 1, and its $\mathcal{F}_k$-component is 0 (for $2 \le k \le l$). If Γ is q_1-colorable then, as we proved in the coNP-completeness part, there exists elements $r_1, \ldots, r_n \in \mathcal{R}_c$ such that $u_\Gamma(r_1, \ldots, r_n) \ne 0$. From the same argument, $r \cdot u_\Gamma(r_1, \ldots, r_n) = r$ follows, as well. Let $a \in \mathbf{A}$, $a \ne 1$ be arbitrary for which $a^r = a$. Then $t_\Gamma = a$ is solvable if and only if Γ is q_1-colorable. □

3 Proof of Theorems 3 and 4

In this section we prove Theorems 3 and 4. By the following lemma the equivalence and equation solvability problems can be reduced to verbal subgroups.

Lemma 9 *Let $\mathbf{V} = (V, \cdot)$ be a verbal subgroup of the group $\mathbf{G} = (G, \cdot)$. Let f be a group term.*

1. *If the equivalence problem over $(V, \cdot, f)$ is coNP-complete, then the equivalence problem over $(G, \cdot, f)$ is coNP-complete.*
2. *If the equation solvability problem over $(V, \cdot, f)$ is NP-complete, then the equation solvability problem over $(G, \cdot, f)$ is NP-complete.*

Proof: We prove only (1), as the proof of (2) is similar. We give a polynomial reduction from the equivalence problem of $(V, \cdot, f)$ to the equivalence problem of $(G, \cdot, f)$. For every term $t(x_1, \ldots, x_n)$ over $(V, \cdot, f)$ we present a term t' over $(G, \cdot, f)$ such that $t \approx 1$ over $(V, \cdot, f)$ if and only if $t' \approx 1$ over $(G, \cdot, f)$. As $\mathbf{V}$ is verbal, there exists a term $s(x_1, \ldots, x_k)$ over $\mathbf{G}$ such that $s(\mathbf{G}) = \mathbf{V}$. Let $\bar{y}_i = (y_{i1}, \ldots, y_{ik})$ $(i = 1, \ldots, n)$ and let

$$t'(\bar{y}_1, \ldots, \bar{y}_n) = t\left(s(\bar{y}_1), \ldots, s(\bar{y}_n)\right).$$

While $\bar{y}_i$ runs through all the k-tuples of $\mathbf{G}$, the value of $s(\bar{y}_i)$ attains every element of $\mathbf{V}$. Thus if $t \ne 1$ at some evaluation $(h_1, \ldots, h_n) \in \mathbf{V}^n$, then we can choose the tuples $\bar{y}_i$ such that $s(\bar{y}_i) = h_i$. Thus there exists an evaluation of t' such that $t' \ne 1$.

On the other hand, if $t' \not\approx 1$ over $(G, \cdot, f)$, then there exists an evaluation $\bar{y}_1, \dots, \bar{y}_k$ such that $t' \neq 1$. Now, for the elements $h_i = s(\bar{y}_i)$ we have $t(h_1, \dots, h_n) \neq 1$, hence $t \not\approx 1$ over $(V, \cdot, f)$.

Thus $t \approx 1$ over $(V, \cdot, f)$ if and only if $t' \approx 1$ over $(G, \cdot, f)$. The reduction is polynomial in the length of t because the length of t' is the product of the length of t and the length of s, and s depends only on the group $\mathbf{G}$. □

Note that the converses of the statements of Lemma 9 are not true. With $G = A_4$ (the alternating group on 4 elements), $V = G'$ and f being the commutator we have that the equivalence problem for $(G, \cdot, f)$ is coNP-complete and is in P for $(V, \cdot, f)$, and similarly, equation solvability for $(G, \cdot, f)$ is NP-complete and is in P for $(V, \cdot, f)$.

By the following lemma the equivalence problem can be reduced to the factor by the centralizer of a verbal subgroup, while the equation solvability problem can be reduced to the factor by a verbal subgroup.

Lemma 10 *Let $\mathbf{V}$ be a verbal subgroup of $\mathbf{G} = (G, \cdot)$. Let $\mathbf{H}_1 = (H_1, \cdot) = \mathbf{G}/C_{\mathbf{G}}(\mathbf{V})$ and let $\mathbf{H}_2 = (H_2, \cdot) = \mathbf{G}/\mathbf{V}$. Let f be a group term.*

1. *If the equivalence problem over $(H_1, \cdot, f)$ is coNP-complete, then the equivalence problem over $(G, \cdot, f)$ is coNP-complete.*

2. *If the equation solvability problem over $(H_2, \cdot, f)$ is NP-complete, then the equation solvability problem over $(G, \cdot, f)$ is NP-complete.*

Proof: We prove (1). We give a polynomial reduction from the equivalence problem of $(H_1, \cdot, f)$ to the equivalence problem of $(G, \cdot, f)$. For every term $t(x_1, \dots, x_n)$ over $(H_1, \cdot, f)$ we present a term t' over $(G, \cdot, f)$ such that $t \approx 1$ over $(H_1, \cdot, f)$ if and only if $t' \approx 1$ over $(G, \cdot, f)$. As $\mathbf{V}$ is verbal, there exists a term $s(x_1, \dots, x_k)$ over $\mathbf{G}$ such that $s(\mathbf{G}) = \mathbf{V}$. Let $\bar{y} = (y_1, \dots, y_k)$. Let $t(x_1, \dots, x_n)$ be a term over $(H_1, \cdot, f)$ and let $\bar{x} = (x_1, \dots, x_n)$. Let the exponent of $\mathbf{G}$ be N. Consider the following term over $(G, \cdot, f)$:

$$t'(\bar{x}, \bar{y}) = t(\bar{x})^{N-1} s(\bar{y})^{N-1} t(\bar{x}) s(\bar{y}) = [t(\bar{x}), s(\bar{y})] .$$

Assume first that $(H_1, \cdot, f) \models t \approx 1$. Then for every $\bar{g} \in \mathbf{G}^n$ we have $t(\bar{g}) \in C_{\mathbf{G}}(\mathbf{V})$. For arbitrary $\bar{h} \in \mathbf{G}^k$ we have $s(\bar{h}) \in \mathbf{V}$. Thus $[t(\bar{g}), s(\bar{h})] = 1$, that is $(G, \cdot, f) \models t' \approx 1$.

Assume now that $(G, \cdot, f) \models t' \approx 1$. If $\bar{y}$ runs through $\mathbf{G}^k$, then $s(\bar{y})$ runs through $\mathbf{V}$. Then for every $\bar{g} \in \mathbf{G}^n$ we have $t(\bar{g}) \in C_{\mathbf{G}}(\mathbf{V})$, i.e. $(H_1, \cdot, f) \models t \approx 1$.

Thus $t \approx 1$ over $(H_1, \cdot, f)$ if and only if $t' \approx 1$ over $(G, \cdot, f)$. The reduction is polynomial in the length of t because $\|t'\| \leq N(\|t\| + \|s\|)$.

The proof of (2) is the same, except that instead of t' one should consider the following term:

$$t''(\bar{x}, \bar{y}) = t(\bar{x}) s(\bar{y})^{N-1} .$$

□

Now, we prove Theorems 3 and 4. If $\mathbf{G}$ is not solvable, then the equivalence problem over $(G, \cdot)$ is coNP-complete Horváth et al. (2007), and the equation solvability problem over $(G, \cdot)$ is NP-complete Goldmann and Russell (2002). Thus for an arbitrary term f the equivalence problem over $(G, \cdot, f)$ is coNP-complete, and the equation solvability problem over $(G, \cdot, f)$ is NP-complete.

If $\mathbf{G}$ is nilpotent, then by Lemma 5 in Horváth (2011) there exists a positive integer d (depending only on $\mathbf{G}$) such that for an arbitrary polynomial $t\,(x_1, \dots, x_n)$ we have

$$t\,(\mathbf{G}, \dots, \mathbf{G}) = \{\, t\,(h_1, \dots, h_n) \mid (h_1, \dots, h_n) \in T_d \,\},$$

where

$$T_d = \{\, (h_1, \dots, h_n) \mid |\{\, h_i : h_i \neq 1 \,\}| \leq d \,\}.$$

That is we can obtain $t\,(\mathbf{G}, \dots, \mathbf{G})$ by substituting only from T_d. Now,

$$|T_d| \leq \sum_{j=0}^{d} \binom{n}{j} \cdot |\mathbf{G}|^j \leq \sum_{j=0}^{d} (n \cdot |\mathbf{G}|)^j \leq (d+1) \cdot (n\,|\mathbf{G}|)^d = O\left(\|t\|^d\right).$$

Hence we can obtain $t\,(\mathbf{G}, \dots, \mathbf{G})$ with $O(n^d)$ many substitutions, thus in polynomial time of the length of t. Now, $t \approx 1$ if and only if $t\,(\mathbf{G}, \dots, \mathbf{G}) = \{\, 1 \,\}$. Moreover, $t = 1$ can be solved if and only if $1 \in t\,(\mathbf{G}, \dots, \mathbf{G})$.

Now, we prove Theorem 3 for solvable, non-nilpotent groups by induction on the order of $\mathbf{G}$.

Case 1: $\mathbf{G}' = (G', \cdot)$ is non-nilpotent. As $|\mathbf{G}'| < |\mathbf{G}|$, by the induction hypothesis there exists a term f such that the equivalence problem over $(G', \cdot, f)$ is coNP-complete. By (1) of Lemma 9 the equivalence problem over $(G, \cdot, f)$ is coNP-complete.

Case 2: $\mathbf{G}'$ is nilpotent, but $\mathbf{G}/C_{\mathbf{G}}\,(\mathbf{G}')$ is non-nilpotent. Let $\mathbf{H} = \mathbf{G}/C_{\mathbf{G}}\,(\mathbf{G}')$. As $\mathbf{G}'$ is nilpotent $\mathbf{1} \neq Z(\mathbf{G}') \leq C_{\mathbf{G}}(\mathbf{G}')$, hence $|\mathbf{H}| < |\mathbf{G}|$. Since $\mathbf{H} = (H, \cdot)$ is non-nilpotent, by the induction hypothesis there exists a term f such that the equivalence problem over $(H, \cdot, f)$ is coNP-complete. By (1) of Lemma 10 the equivalence problem over $(G, \cdot, f)$ is coNP-complete.

Case 3: $\mathbf{G}'$ and $\mathbf{G}/C_{\mathbf{G}}\,(\mathbf{G}')$ are both nilpotent. Let $\mathbf{A}$ be the terminal element of the lower central series of $\mathbf{G}$, i.e. $\mathbf{A} = \gamma\,(\mathbf{G})$. We prove that $\mathbf{A}$ and $\mathbf{G}/C_{\mathbf{G}}\,(\mathbf{A})$ are commutative groups. Now, $\mathbf{G}/C_{\mathbf{G}}\,(\mathbf{G}')$ is nilpotent, and $\mathbf{A}$ is the terminal element of the lower central series, thus $\mathbf{A} \leq C_{\mathbf{G}}\,(\mathbf{G}')$. Moreover, $\mathbf{A} \leq \mathbf{G}'$ implies $\mathbf{A} \leq C_{\mathbf{G}}\,(\mathbf{G}') \cap \mathbf{G}' = C_{\mathbf{G}'}\,(\mathbf{G}') = Z(\mathbf{G}')$, i.e. $\mathbf{A}$ is commutative. From $\mathbf{A} \leq C_{\mathbf{G}}\,(\mathbf{G}')$ we have $C_{\mathbf{G}}\,(\mathbf{A}) \geq C_{\mathbf{G}}\,(C_{\mathbf{G}}\,(\mathbf{G}')) \geq \mathbf{G}'$. Therefore $\mathbf{G}/C_{\mathbf{G}}\,(\mathbf{A}) \leq \mathbf{G}/\mathbf{G}'$, and $\mathbf{G}/C_{\mathbf{G}}\,(\mathbf{A})$ is commutative. Hence $\mathbf{A}$ and $\mathbf{G}/C_{\mathbf{G}}\,(\mathbf{A})$ are both commutative. Theorem 5 finishes the proof.

Finally, we prove Theorem 4 for solvable, non-nilpotent groups by induction on the order of $\mathbf{G}$.

Case 1: $\mathbf{G}' = (G', \cdot)$ is non-nilpotent. As $|\mathbf{G}'| < |\mathbf{G}|$, by the induction hypothesis there exists a term f such that the equation solvability problem over $(G', \cdot, f)$ is NP-complete. By (2) of Lemma 9 the equation solvability problem over $(G, \cdot, f)$ is NP-complete.

Case 2: $\mathbf{G}'$ is nilpotent, and $\mathbf{G}'' \neq \mathbf{1}$. Since $\mathbf{G}$ is non-nilpotent and $\mathbf{G}'$ is nilpotent, we see from (Robinson, 1995, 5.2.10) that $\mathbf{G}/\mathbf{G}''$ is non-nilpotent. Let $\mathbf{H} = \mathbf{G}/\mathbf{G}''$. As $\mathbf{G}'' \neq \mathbf{1}$, we have $|\mathbf{H}| < |\mathbf{G}|$. Since $\mathbf{H} = (H, \cdot)$ is non-nilpotent, by the induction hypothesis there exists a term f such that the equation solvability problem over $(H, \cdot, f)$ is NP-complete. By (2) of Lemma 10 the equation solvability problem over $(G, \cdot, f)$ is NP-complete.

Case 3: $\mathbf{G}'$ is nilpotent, $\mathbf{G}'' = \mathbf{1}$. Let $\mathbf{A}$ be the terminal element of the lower central series of $\mathbf{G}$, i.e. $\mathbf{A} = \gamma\,(\mathbf{G})$. We prove that $\mathbf{A}$ and $\mathbf{G}/C_{\mathbf{G}}\,(\mathbf{A})$ are commutative groups. Now, $\mathbf{G}'' = \mathbf{1}$ thus $\mathbf{G}'$ is commutative and $\mathbf{A} \leq \mathbf{G}'$ yields that $\mathbf{A}$ is commutative, as well. Moreover, from $\mathbf{A} \leq \mathbf{G}'$ we have $C_{\mathbf{G}}\,(\mathbf{A}) \geq C_{\mathbf{G}}\,(\mathbf{G}') \geq C_{\mathbf{G}'}\,(\mathbf{G}') = Z\,(\mathbf{G}') = \mathbf{G}'$. Thus $\mathbf{G}/C_{\mathbf{G}}\,(\mathbf{A}) \leq \mathbf{G}/\mathbf{G}'$ and $\mathbf{G}/C_{\mathbf{G}}\,(\mathbf{A})$ is commutative. Hence $\mathbf{A}$ and $\mathbf{G}/C_{\mathbf{G}}\,(\mathbf{A})$ are both commutative. Theorem 5 finishes the proof. □

4 Open questions

The term f in Theorems 3 and 4 varies from group to group. As it is mentioned in the Introduction, the commutator can significantly change the length of expressions. It is proved in Horváth and Szabó (2011) that the complexities of the equivalence and equation solvability problems change if we extend the alternating group $\mathbf{A}_4$ by the commutator. One may wonder if f can be chosen as the commutator for every finite group.

Problem 1 *For every finite group* $\mathbf{G} = (G, \cdot)$*, determine the complexity of the equivalence and equation solvability problems for* $(G, \cdot, [,])$.

The smallest group for which it would be interesting to know how the commutator affects the complexity of the equivalence and equation solvability problems is $\mathbf{S}_3$.

Problem 2 *Determine the complexity of the equivalence and equation solvability problems for* $(S_3, \cdot, [,])$.

Acknowledgements

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

References

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

R. Baer. Engelsche elemente noetherscher gruppen. *Math. Ann.*, 133:256–270, 1957.

S. Burris and J. Lawrence. The equivalence problem for finite rings. *J. of Symb. Comp.*, 15:67–71, 1993.

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

M. Goldmann and A. Russell. The complexity of solving equations over finite groups. *Information and Computation*, 178(253–262), 2002.

T. A. Gorazd and J. Krzaczkowski. The complexity of problems connected with two-element algebras. *Reports on Mathematical Logic*, 46:91–108, 2011.

G. Horváth. The complexity of the equivalence and equation solvability problems over nilpotent rings and groups. *Algebra Universalis*, 2011. to appear.

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

G. Horváth and Cs. Szabó. Equivalence and equation solvability problems for the group A_4. *J. Pure Appl. Algebra*, 2011. to appear.

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

H. Hunt and R. Stearns. The complexity for equivalence for commutative rings. *Journal of Symbolic Computation*, 10:411–436, 1990.

N. Jacobson. The radical and semi-simplicity for arbitrary rings. *Amer. J. Math.*, 67:300–320, 1945.

R. M. Karp. Reducibility among combinatorial problems. In *Complexity of computer computations (Proc. Sympos., IBM Thomas J. Watson Res. Center, Yorktown Heights, N.Y., 1972)*, pages 85–103. Plenum, New York, 1972.

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

O. Klíma. *Unification Modulo Associativity and Idempotency*. PhD thesis, Masarik University, Brno, 2004.

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

J. Lawrence and R. Willard. The complexity of solving polynomial equations over finite rings. manuscript, 1997.

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

D. J. S. Robinson. *A course in the theory of groups*. Springer-Verlag, New York, Berlin, Heidelberg, 1995.

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

Cs. Szabó and V. Vértesi. The equivalence problem over finite rings. *Internat. J. Algebra Comput.*, 21(3): 449–457, 2011.