Algebra Univers. 66 (2011) 391–403
DOI 10.1007/s00012-011-0163-y
Published online October 30, 2011

Algebra Universalis

The complexity of the equivalence and equation solvability problems over nilpotent rings and groups

Gábor Horváth

Abstract. It is proved that the equation solvability problem can be solved in polynomial time for finite nilpotent rings. Ramsey's theorem is employed in the proof. Then, using the same technique, a theorem of Goldmann and Russell is reproved: the equation solvability problem can be solved in polynomial time for finite nilpotent 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 two term 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 problem* is one of the oldest problems of algebra: it asks whether two term 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. If the input expressions are polynomials, i.e., expressions that can contain constants from $\mathbf{A}$, then we talk about the *polynomial equivalence problem* and the *polynomial equation solvability problem.*

These questions are decidable for a finite algebra $\mathbf{A}$: checking all substitutions, i.e., all mappings from the set of variables to $\mathbf{A}$, yields an answer to any of these questions. The term and polynomial equation solvability problems are in NP, as the 'yes' answer can be verified in polynomial time by a substitution which satisfies the equation. Similarly, the term and polynomial equivalence problems are in coNP, since now the 'no' answer can be verified in polynomial time by a substitution, where the two expressions differ. As every term is a polynomial, the polynomial versions of these problems are always 'at least as hard' as the term versions of them. In this paper we investigate the computational complexity of these questions for finite rings and groups. Note that the term equation solvability problem is uninteresting in the case of rings and

Presented by M. Valeriote.
Received August 26, 2010; accepted in final form May 30, 2011.
2010 *Mathematics Subject Classification*: Primary: 08A50; Secondary: 20F10, 16N40, 20F18.
Key words and phrases: complexity, equation solvability, equivalence, nilpotent ring, nilpotent group.
This research was partially supported by the Hungarian National Foundation for Scientific Research grants K67870, N67867 and K100246.

groups, because an arbitrary equation has the trivial solution. In the trivial solution all variables are evaluated to 0 in the ring case and to 1 in the group case. From now on we refer to the polynomial equation solvability problem as the equation solvability problem.

Investigations into the equivalence problem for various finite algebraic structures were started in the early 1990s. First, Hunt and Stearnes [11] investigated the equivalence problem for finite rings. They proved that for finite nilpotent rings, the polynomial equivalence problem can be solved in polynomial time in the length of the two input polynomials. Moreover, they proved that for commutative, non-nilpotent rings, the equivalence problem is coNP-complete. Later, Burris and Lawrence [2] generalized their result to non-commutative rings, and established a dichotomy theorem for rings:

Theorem 1.1. *Let $\mathcal{R}$ be a finite ring. If $\mathcal{R}$ is nilpotent, then both the term and the polynomial equivalence problems can be solved in polynomial time. If $\mathcal{R}$ is not nilpotent, then both the term and the polynomial equivalence problems are coNP-complete.*

A thorough examination of the proof in [2] shows that the equation solvability problem is NP-complete for non-nilpotent rings. In Section 2, we provide the missing half of a similar dichotomy theorem for the equation solvability problem for finite rings, i.e., we prove that the equation solvability problem can be solved in polynomial time for finite nilpotent rings. This is a new result which is not formulated in the literature. Note that the polynomial decidability of the term and polynomial equivalence problems follows from this result.

Theorem 1.2. *Let $\mathcal{R}$ be a finite nilpotent ring. Then the equation solvability problem over $\mathcal{R}$ is solvable in polynomial time.*

The interest in the computational complexity of the equivalence and equation solvability problems of a finite algebraic structure has been steadily increasing. Several results have been published about the complexity of these problems for finite semigroups and monoids. For recent results and detailed references, see e.g. [1], [12], [13], [14], [17], [18], [21]. Although the literature is fairly extensive for monoids, the equivalence and equation solvability problems even for the simplest case, the case of finite groups, proved to be a far more challenging topic than for finite rings.

Goldmann and Russell [4] proved that for a finite group $\mathbf{G}$, the equation solvability problem has polynomial time complexity if $\mathbf{G}$ is nilpotent. Burris and Lawrence [3] proved that if the group $\mathbf{G}$ is nilpotent or $\mathbf{G} \simeq \mathbf{D}_n$, the dihedral group for odd n, then the polynomial equivalence problem for $\mathbf{G}$ can be solved in polynomial time. Other groups which originate as semidirect products of certain groups were investigated in [9] and [10]. Most of the groups considered were semidirect products of two Abelian groups, and in all consid-

ered cases the equivalence and equation solvability problems were decidable in polynomial time. However, the equivalence and equation solvability problems for groups do not always have polynomial time complexities. For non-solvable groups, the complexity of the equation solvability problem is NP-complete [4] and the complexity of the equivalence problem is coNP-complete [7]. For some groups, the question is still open: the smallest group for which the complexities of neither the equivalence nor the equation solvability problems are known is $\mathbf{S}_4$, the symmetric group on four elements.

Comparing these results for nilpotent groups and rings, one might wonder whether they can be generalized for arbitrary nilpotent algebras. For such a generalization, a starting point could be to understand the proof for finite nilpotent groups in [3, 4]. Goldmann and Russell in [4] reduced the equation solvability problem over nilpotent groups to recognizing languages by non-uniform finite automata (NUDFA) over nilpotent groups. They apply the results proved by Péladeau and Thérien in the paper [16], where NUDFAs were investigated, but even in this latter work, many properties of NUDFAs crucial to the proof in [4] are proved in [22]. That way the core of the proof of Goldmann and Russell is lost in this chain of citations and reformulated statements, and is hard to use for any generalization.

Burris and Lawrence in [3] gave a polynomial algorithm for checking equivalence by giving a polynomial test set. Using commutator theory, they showed the following: let $\mathbf{G}$ be a nilpotent group and c its nilpotency class. Let t be an n-ary polynomial over $\mathbf{G}$ and let $T = \{ (g_1, \dots, g_k) \in \mathbf{G}^n : |\{ i : g_i \neq 1 \}| \leq c \}$. Then $\mathbf{G} \models t \approx 1$ if and only if $t(g_1, \dots, g_n) = 1$ for every $(g_1, \dots, g_n) \in T$. Although their proof is very short and concise, it does not seem to generalize easily for the equation solvability problem.

In Section 3, we give a direct proof for the equation solvability problem in the case of nilpotent groups, which uses similar arguments as the proof of Theorem 1.2 and does not require further references.

Theorem 1.3. *Let $\mathbf{G}$ be a finite nilpotent group. Then the equation solvability problem over $\mathbf{G}$ is solvable in polynomial time.*

Therefore, the goal of the paper is twofold. Firstly, in Section 2, we prove Theorem 1.2 completing the characterization of the equation solvability problem for finite rings. Secondly, in Section 3, we show how the arguments can be carried forward to the case of finite nilpotent groups by giving a concise proof of Theorem 1.3. The method described in the proof of Theorem 1.3 could be generalized to arbitrary nilpotent algebras, which would be a significant step in characterizing the equivalence and equation solvability problems for finite algebras:

Problem 1. *Prove that the equivalence and the equation solvability problems can be decided in polynomial time for finite nilpotent algebras.*

2. Nilpotent rings

In this section, we prove Theorem 1.2, i.e., that the equation solvability problem can be decided in polynomial time over a finite nilpotent ring. Note that the polynomial decidability of the term and polynomial equivalence problems will follow from the proof, as well.

For a ring $\mathcal{R}$ and for polynomials p, q, we have that $p = q$ is solvable if and only if $p - q = 0$ is solvable. Furthermore, we have $\mathcal{R} \models p \approx q$ if and only if $\mathcal{R} \models p - q \approx 0$. Thus, we assume that the instance of the equation solvability problem is a polynomial f, and we need to decide whether $f = 0$ is solvable.

Let $\mathcal{R}$ be a finite nilpotent ring and c be its nilpotency class. Now, c is the smallest positive integer such that every product of at least c-many elements is 0 in $\mathcal{R}$. A polynomial over $\mathcal{R}$ is defined inductively: a variable or a constant is a polynomial, and if p and q are polynomials, then so are $p + q$ and $p \cdot q$. Every polynomial p is equivalent to a sum of monomials: one can obtain such a form by expanding the polynomial using the distributive law. The length of the expanded polynomial can be significantly different than that of the original polynomial. Therefore, the sigma equivalence and sigma equation solvability problems were introduced, where the input polynomials are sums of monomials. Results on the sigma problems can be found in e.g. [6, 8, 19, 20, 21]. For nilpotent rings, there is no difference between the sigma and the original variants of these problems: the expansion using the distributive law leads to a polynomial algorithm when any product representing the result of at least c-many multiplications is not expanded but replaced by 0 (see [11, page 428] for more details). Thus, we may assume that the instance of the equation solvability problem is a polynomial written as a sum of monomials.

Let $f \in \mathcal{R}[x_1, \dots, x_n]$ be an arbitrary polynomial over $\mathcal{R}$, written as a sum of monomials. Every monomial of degree at least c is 0 for any substitution. Therefore, without loss of generality, we can assume that every monomial in f depends on less than c-many variables. For every $\bar{r} = (r_1, \dots, r_n) \in \mathcal{R}^n$ and for arbitrary $I \subseteq \{1, \dots, n\}$, let $\bar{r}_I$ be the n-tuple $(u_1, \dots, u_n)$ for which $u_i = r_i$ if $i \in I$ and $u_i = 0$, otherwise. By the following lemma, the range of a polynomial can be obtained by substituting n-tuples for which the number of nonzero coordinates is bounded:

Lemma 2.1. *Let $\mathcal{R}$ be a finite nilpotent ring. Then there exists a positive integer $d = d(\mathcal{R})$ that depends only on $\mathcal{R}$, such that for every polynomial $f \in \mathcal{R}[x_1, \dots, x_n]$ and for every $\bar{r} = (r_1, \dots, r_n) \in \mathcal{R}^n$, there exists a subset $I \subseteq \{1, \dots, n\}$ such that $|I| \leq d$, and $f(\bar{r}_I) = f(\bar{r})$.*

Proof. Let c be the nilpotency class of $\mathcal{R}$. Write the polynomial f as a sum of monomials. For every subset $I \subseteq \{1, \dots, n\}$, let f_I be the sum of those monomials in f which depend on the variables x_i for every $i \in I$. Note that the monomials in f_I may depend on x_j for $j \notin I$, as well. For example, $f_\emptyset = f$.

Let $\bar{r} = (r_1, \ldots, r_n) \in \mathcal{R}^n$ be arbitrary and consider $f(\bar{r})$. Let S denote the indices of nonzero r_i, i.e., $S = \{\, 1 \le i \le n \mid r_i \neq 0 \,\}$. If $|S| > d$, then we find a proper subset H of S such that $f(\bar{r}_{S\setminus H}) = f(\bar{r})$. The value of d will be determined later. First, let $H \subset S$ be arbitrary. We compute the value of f for the substitution where we replace r_i by 0 in $\bar{r}$ for every $i \in H$. Every monomial containing a variable x_i for some $i \in H$ attains value 0 for the substitution $\bar{r}_{S\setminus H}$. Thus, by inclusion-exclusion we have

$$f(\bar{r}_{S\setminus H}) = \sum_{I\subseteq H} (-1)^{|I|} f_I(\bar{r}).$$

Since all products of length c are 0, we obtain

$$\begin{aligned} f(\bar{r}_{S\setminus H}) &= \sum_{\substack{I\subseteq H\\ |I|<c}} (-1)^{|I|} f_I(\bar{r}) \\ &= f(\bar{r}) - \sum_{i\in H} f_{\{\,i\,\}}(\bar{r}) + \sum_{\substack{i,j\in H\\ i<j}} f_{\{\,i,j\,\}}(\bar{r}) - \sum_{\substack{i,j,k\in H\\ i<j<k}} f_{\{\,i,j,k\,\}}(\bar{r}) + \cdots . \end{aligned}$$

We prove that there exists a subset $H \subseteq S$ such that every sum $\sum_{i\in H} f_{\{\,i\,\}}(\bar{r})$, $\sum_{i,j\in I} f_{\{\,i,j\,\}}(\bar{r})$, etc. attains the value 0. To this end, we color the less than c-element subsets of S by the elements of $\mathcal{R}$: for every subset $I \subseteq S$, let $f_I(\bar{r})$ be the color of I.

For positive integers c, k, m, let $R_2(k,m) = km$, and for $c > 2$, let $R_c(k,m) = k^{R_{c-1}(k,m)^{c-1}}$. Let $T_2(k,m) = R_2(k,m)$ and $T_c(k,m) = R_c(k, T_{c-1}(k,m))$. We use the following form of Ramsey's theorem, which follows from [5, Section 1.2, Theorem 2] and [5, Section 4.7]:

Theorem 2.2 (Ramsey's Theorem)**.** *Let c, k and m be positive integers with $c > 1$. Then there exists a positive integer $d \le T_c(k,m)$ such that if we color the less than c-element subsets of a set S by k colors and $|S| > d$, then S has a subset H with m elements, such that any two subsets of the same size have the same color, that is, for every $H_1, H_2 \subseteq H$, $|H_1| = |H_2| < c$, the color of H_1 and H_2 are the same.*

Recall that c is the nilpotency class of $\mathcal{R}$. Let $k = |\mathcal{R}|$. Let e be the smallest positive integer such that $e \cdot r = 0$ holds for every $r \in \mathcal{R}$. Note that e is the exponent of the Abelian group $(R, +)$. Let $m = (c-1)! \cdot e$. By Ramsey's theorem, for c, k, m there exists d such that if $|S| > d$, then there exists a subset $H \subseteq S$, $|H| = m$ such that every one-element subset of H has the same color, every two-element subset of H has the same color, ..., every subset of H with $(c-1)$ elements has the same color. Let $\gamma(i)$ denote the color of the subsets of H with i elements. Hence, $\gamma(i) = f_I(\bar{r})$, where $I \subset H$ is arbitrary

such that $|I| = i$. Now, the value of f for the substitution $\bar{r}_{S\setminus H}$ is

$$f(\bar{r}_{S\setminus H}) = f(\bar{r}) - \sum_{i\in H} f_{\{\,i\,\}}(\bar{r}) + \sum_{\substack{i,j\in H\\ i<j}} f_{\{\,i,j\,\}}(\bar{r}) - \cdots$$

$$= f(\bar{r}) + \sum_{i=1}^{c-1}(-1)^i \binom{m}{i}\gamma(i).$$

We chose m such that all binomial coefficients $\binom{m}{i}$ for $1 \le i \le c-1$ are divisible by e; thus, $f(\bar{r}_{S\setminus H}) = f(\bar{r})$ holds. Hence, if $|S| > d$, then we have found an $H \subseteq S$ such that $f(\bar{r}_{S\setminus H}) = f(\bar{r})$. If $|S \setminus H| > d$, then we can repeat the procedure for $S = S \setminus H$ until $|S \setminus H| \le d$ holds. □

Note that the value of d obtained by Ramsey's theorem is rather big compared to the size of the ring. It is more than $k^{k^{\cdots^{k^m}}}$, where $k = |\mathcal{R}|$, where m was defined in the proof of Lemma 2.1, and where the height of the tower is c, the nilpotency class of $\mathcal{R}$. Now, we prove Theorem 1.2.

Proof of Theorem 1.2. Let d be the positive integer defined in Lemma 2.1. Let $f \in \mathcal{R}[x_1, \ldots, x_n]$ be an arbitrary polynomial. Let T_d denote the set of n-tuples $(r_1, \ldots, r_n)$ for which the number of nonzero coordinates is at most d:

$$T_d = \{\,(r_1, \ldots, r_n) \mid |\{\,i : r_i \neq 0\,\}| \le d\,\}.$$

By Lemma 2.1, we have

$$f(\mathcal{R}, \ldots, \mathcal{R}) = \{\,f(r_1, \ldots, r_n) \mid (r_1, \ldots, r_n) \in T_d\,\}.$$

That is, we can obtain the range of f by substituting only from the set T_d. Now,

$$|T_d| \le \sum_{j=0}^{d} \binom{n}{j} \cdot |\mathcal{R}|^j \le \sum_{j=0}^{d} (n \cdot |\mathcal{R}|)^j \le (d+1) \cdot (n|\mathcal{R}|)^d.$$

Hence, we can obtain $f(\mathcal{R}, \ldots, \mathcal{R})$ with $O(n^d)$ many substitutions, thus in polynomial time in the length of f. Now, $\mathcal{R} \models f \approx 0$ if and only if $f(\mathcal{R}, \ldots, \mathcal{R}) = \{\,0\,\}$. Moreover, $f = 0$ can be solved if and only if $0 \in f(\mathcal{R}, \ldots, \mathcal{R})$. □

3. Nilpotent groups

In this section, we consider the equivalence and equation solvability problems for finite nilpotent groups and prove Theorem 1.3. The proof has much in common with the proof of Theorem 1.2. It uses Ramsey's theorem with an analogous argument. Therefore, we mostly point out the differences and similarities, rather than just copying the earlier proof.

For a group $\mathbf{G}$ and for polynomials p, q, we have that $p = q$ is solvable if and only if $pq^{-1} = 1$ is solvable. Furthermore, we have $\mathbf{G} \models p \approx q$ if and only if $\mathcal{R} \models pq^{-1} \approx 1$. Any expression can be rewritten (in polynomial time) equivalently to a product of variables and constants from $\mathbf{G}$ using the rules

$(ab)^{-1} = b^{-1}a^{-1}$, $(a^{-1})^{-1} = a$ and $a^{-1} = a^{|\mathbf{G}|-1}$. Thus, we may assume that the instance of the equation solvability problem is a product of variables and constants from $\mathbf{G}$, and the question is whether this product can attain the value 1 for some substitution.

Let $\mathbf{G}$ be a finite nilpotent group and $c-1$ its nilpotency class. We define the *commutator expression over* $\mathbf{G}$ and its *weight* inductively. A variable or a constant from $\mathbf{G}$ is a commutator expression with weight 1. If s and t are commutator expressions with weights k and l, then $[s,t]$ is a commutator expression with weight $k+l$. From basic commutator calculus (see e.g. [15, Lemma 33.35, p. 86]), if the weight of a commutator expression s is at least c, then $\mathbf{G} \models s \approx 1$. In particular, if a commutator expression s depends on at least c-many variables, then s attains 1 for arbitrary substitutions.

For every $\bar{h} = (h_1, \dots, h_n) \in \mathbf{G}^n$ and for an arbitrary subset $I \subseteq \{1, \dots, n\}$, let $\bar{h}_I$ denote the n-tuple $(u_1, \dots, u_n)$ for which $u_i = h_i$ if $i \in I$, and $u_i = 1$ if $i \notin I$. As in Lemma 2.1, we prove that computing the range of a polynomial expression over $\mathbf{G}$ requires checking substitutions of those n-tuples for which the number of non-identity coordinates is bounded.

Lemma 3.1. *For every finite nilpotent group $\mathbf{G}$, there exists a positive integer $d = d(\mathbf{G})$ that depends only on $\mathbf{G}$, such that for every polynomial $t(x_1, \dots, x_n)$ over $\mathbf{G}$ and for every $\bar{h} = (h_1, \dots, h_n) \in \mathbf{G}^n$, there exists a subset $I \subseteq \{1, \dots, n\}$ such that $|I| \leq d$ and $t(\bar{h}_I) = t(\bar{h})$.*

Proof. Let $\mathbf{G}$ be a nilpotent group. Let $t(x_1, \dots, x_n)$ be a group polynomial over $\mathbf{G}$, and let $\bar{h} = (h_1, \dots, h_n) \in \mathbf{G}^n$ be arbitrary. Consider $t(\bar{h})$. We want to understand how the value of t changes if we replace some coordinates of $\bar{h}$ by 1. For rings, it was instructive to consider the polynomial as sum of products, as every product attains the value 0 if any factor is 0. For groups, the commutator has a similar property: a commutator expression attains the value 1 if any variable attains 1. In the proof, the group multiplication will correspond to the ring addition and the group commutator will correspond to the ring multiplication. We will rewrite t as a product of commutator expressions $t' = t'_1 \cdots t'_m$. This way, if we change any variable from h_i to 1, then the value of every commutator expression t'_j depending on the variable x_i becomes 1 as well.

An obstacle still remains, namely that the group multiplication is not commutative, as is the ring addition. To overcome this difficulty, we will introduce a linear order $\prec$ on $\mathbf{G}$. Then we rewrite t to $t' = t'_1 \cdots t'_m$ in such a way that the elements $t'_1(\bar{h}), \dots, t'_m(\bar{h})$ are in decreasing order with respect to $\prec$. In this way, we will be able to track how the value of t changes when we change the substitution of the variables.

Let us introduce the linear order first. Let $c-1$ be the nilpotency class of $\mathbf{G}$. Consider the upper central series of $\mathbf{G}$: $\{1\} = \mathbf{Z}_0 \leq \mathbf{Z}_1 \leq \cdots \leq \mathbf{Z}_{c-1} = \mathbf{G}$,

where

$$\mathbf{Z}_i = \{\, h \in \mathbf{G} \mid [g,h] \in \mathbf{Z}_{i-1} \text{ for every } g \in \mathbf{G} \,\} \qquad (1 \leq i \leq c-1).$$

We define a linear order $\prec$ on $\mathbf{G}$ using a preorder $\prec'$. First, let $a \prec' b$ for every $a, b \in \mathbf{G}$ for which there exists $0 \leq i < c-1$ such that $a \in \mathbf{Z}_i$ and $b \notin \mathbf{Z}_i$. Let $\prec$ be a linear extension of $\prec'$. If $g \prec h$, then we say that g is smaller than h, or equivalently, h is greater than g. For every $g, h \in \mathbf{G} \setminus \{\, 1 \,\}$, we have $[g,h] \prec g$ and $[g,h] \prec h$.

Let $t(x_1, \ldots, x_n)$ be a polynomial over $\mathbf{G}$. Let $\bar{h} = (h_1, \ldots, h_n) \in \mathbf{G}^n$ be arbitrary. Let S denote the indices of the non-identity coordinates, i.e., $S = \{\, 1 \leq i \leq n \mid h_i \neq 1 \,\}$. If $|S| > d$ (d will be determined later), then we find a proper subset H of S such that if h_i is replaced by 1 for all $i \in I$ in $\bar{h} = (h_1, \ldots, h_n)$, then the value of t at this new substitution is again $t(\bar{h})$. To this end, we first define an expression $t' = t'_1 \cdots t'_m$ such that $\mathbf{G} \models t \approx t'$, every t'_i is a commutator expression, and the elements $t'_1(\bar{h})$, $t'_2(\bar{h}), \ldots, t'_m(\bar{h})$ are in decreasing order with respect to the relation $\prec$. We give an algorithm which computes t' from t. We note that later we use only the existence of t', and not how t' is computed. Therefore, we do not calculate the number of steps the algorithm takes, we only prove that it ends and gives an appropriate expression t'.

In the following, we introduce the inductive step of the algorithm. Let $s(x_1, \ldots, x_n) = s_1 \cdots s_l$, where every s_i is a commutator expression over $\mathbf{G}$ and $\mathbf{G} \models t \approx s$. Note that every polynomial over $\mathbf{G}$ is a product of commutator expressions; thus, at the beginning of the algorithm, $s_i = t_i$ for every $1 \leq i \leq l$ and $s = t$. Let u_i denote the value of s_i at the substitution $\bar{h}$, i.e., $u_i = s_i(\bar{h})$. Let u denote the sequence $(u_1, \ldots, u_l)$. The elements $u_1, \ldots, u_l$ are not necessarily in decreasing order with respect to $\prec$. We say that for some $1 \leq j \leq l$, the factor u_j *is at the wrong place* j if there exists $i < j$ such that $u_i \prec u_j$. We say that u_j *is at its proper place* j if u_j is not at the wrong place j. Note that if for every $1 \leq j \leq l$ the factor u_j is at its proper place j, then $u_1 \succeq \cdots \succeq u_l$. In such a case, s is of the required form and the algorithm stops with $t' = s$. Otherwise, let g be the greatest element of $\mathbf{G}$ (with respect to $\prec$) which is at the wrong place j for some j:

$$g = \max_{\prec}\{\, h \in \mathbf{G} \mid \text{exist } i < j, \text{ such that } u_i \prec u_j = h \,\}.$$

Here $\max_{\prec}$ denotes the maximum with respect to the linear order $\prec$. Let u_i be the first occurrence of an element smaller than g and let u_j be the first occurrence of g after u_i:

$$i = \min_{<}\{\, 1 \leq i' < l \mid u_{i'} \prec g \,\},$$
$$j = \min_{<}\{\, i < j' \leq l \mid u_{j'} = g \,\}.$$

Let r be the number of occurrences of g after u_i:

$$r = |\{\, i < j' \leq l \mid u_{j'} = g \,\}|.$$

Note that r is the number of indices j' such that g is at the wrong place j'. We say that (g, r) is the *ordering pair assigned to the sequence* $u = (u_1, \dots, u_l)$. The general step of the algorithm will compute a sequence $u' = (u'_1, \dots, u'_{l+j-i})$ from the sequence $u = (u_1, \dots, u_l)$ such that $u'_1 \cdots u'_{l+j-i} = u_1 \cdots u_l$ and the ordering pair (g', r') assigned to u' is lexicographically smaller than the pair (g, r), i.e., either $g' = g$ and $r' < r$, or $g' \prec g$.

Now $u_1 \cdots u_l = u_1 \cdots u_i \cdots u_j \cdots u_l$, where the elements greater than g are all in the subproduct $u_1 \cdots u_{i-1}$ and in decreasing order with respect to $\prec$. Secondly, $i < j$, $u_i \prec u_j = g$, and g does not appear between u_i and u_j. Using $ab = ba[a, b]$, let us shift u_j to the left step by step until it precedes u_i:

$$\begin{aligned} u_1 \cdots u_l &= u_1 \cdots u_{j-2} u_{j-1} u_j \cdots u_l \\ &= u_1 \cdots u_{j-2} u_j u_{j-1} [u_{j-1}, u_j] \cdots u_l \\ &= u_1 \cdots u_j u_{j-2} [u_{j-2}, u_j] u_{j-1} [u_{j-1}, u_j] \cdots u_l \\ &= \cdots \\ &= u_1 \cdots u_{i-1} u_j u_i [u_i, u_j] \cdots u_{j-1} [u_{j-1}, u_j] u_{j+1} \cdots u_l. \end{aligned}$$

Denote the sequence formed by the factors after the last equation by u'. That is, $u' = (u'_1, \dots, u'_{l+j-i})$, where every $u'_k \in \mathbf{G}$ is the following:

$$u'_k = u_k \qquad (1 \le k \le i-1), \tag{3.1}$$

$$u'_k = u_j \qquad (k = i), \tag{3.2}$$

$$u'_k = u_{(k+i-1)/2} \qquad (i < k \le 2j - i,\ 2 \mid k - i - 1), \tag{3.3}$$

$$u'_k = [u_{(k+i-2)/2}, u_j] \qquad (i < k \le 2j - i,\ 2 \mid k - i), \tag{3.4}$$

$$u'_k = u_{k-j+i} \qquad (2j - i < k \le l + j - i). \tag{3.5}$$

Repeat the same steps on the product $s_1 \cdots s_l$, i.e., let

$$s' = s'_1 \cdots s'_{l+j-i} = s_1 \cdots s_{i-1} s_j s_i [s_i, s_j] \cdots s_{j-1} [s_{j-1}, s_j] s_{j+1} \cdots s_l.$$

Formally, we write the symbol s instead of every occurrence of u in formulas (3.1–3.5). Clearly, $u'_k = s'_k(\bar{h})$ for every $1 \le k \le l + j - i$. As every s'_k is a commutator expression, s' is a product of commutator expressions. Moreover, s' is equivalent to s and thus to t, i.e., $\mathbf{G} \models s \approx s'$ and $\mathbf{G} \models t \approx s'$. Finally, in the sequence u', the element $u'_i = u_j$ is at its proper place i. That is, $u'_1 \succeq \cdots \succeq u'_{i-1} \succeq u'_i$.

Let (g', r') be the pair assigned to the sequence u', i.e., g' is the greatest element of $\mathbf{G}$ (with respect to $\prec$) which (for some k) is at the wrong place k in u' and r' is the number of indices k such that g' is at its wrong place k in u'. Left-shifting introduced only elements smaller than g. Moreover, any element greater than g has index at most $i - 1$ in u, and thus left-shifting did not touch it. Hence, $g' \prec g$ or $g' = g$. Finally, $u'_i = g$ is at its proper place i; thus, if $g' = g$, then $r' = r - 1$.

Since the lexicographical ordering is a well-order on $\mathbf{G}\times\mathbb{Z}$, by iterating the left-shifting over and over again, we can obtain an expression $t' = t'_1\cdots t'_m$ such that

- $\mathbf{G}\models t'\approx t$,
- every t'_j is a commutator expression ($1\le j\le m$), and
- $t'_1(\bar h)\succeq t'_2(\bar h)\succeq\cdots\succeq t'_m(\bar h)$.

For every $g\in\mathbf{G}$, let α_g be the number of occurrences of g in the sequence $(t'_1(\bar h),\dots,t'_m(\bar h))$. Let $N=|\mathbf{G}|$ and let $g_1\succ g_2\succ\cdots\succ g_N$ be the elements of $\mathbf{G}$ in decreasing order. Since the elements $t'_1(\bar h),\dots,t'_m(\bar h)$ are in decreasing order, we have

$$t'(\bar h) = g_1^{\alpha_{g_1}} g_2^{\alpha_{g_2}}\dots g_N^{\alpha_{g_N}}.$$

From now on, we start copying the proof of Lemma 2.1. First, we compute the value of t' for the substitution $\bar h_{S\setminus H}$, i.e., for the substitution where h_i is replaced by 1 for each $i\in H$. The nilpotency class of $\mathbf{G}$ is $c-1$; hence, if a commutator expression t'_j depends on at least c-many variables, then t'_j attains 1 for arbitrary substitutions. Therefore, we can assume that every t'_j in t' depends on less than c-many variables. Moreover, if t'_j depends on x_i for some $i\in H$, then $t'_j(\bar h_{S\setminus H})=1$. Thus,

$$t'(\bar h_{S\setminus H}) = g_1^{\beta_{g_1}} g_2^{\beta_{g_2}}\dots g_N^{\beta_{g_N}},$$

for some $\beta_{g_1},\dots,\beta_{g_N}$. Let $e_{\mathbf{G}}$ be the exponent of $\mathbf{G}$ (corresponding to the characteristic of the ring in Lemma 2.1). We find $H\subseteq S$ such that for every $g\in\mathbf{G}$ we have $\beta_g\equiv\alpha_g \pmod{e_{\mathbf{G}}}$, yielding $t'(\bar h_{S\setminus H}) = t'(\bar h)$. To this end we will color the less than c-element subsets of S.

In the proof of Lemma 2.1, we used the polynomials f_I for coloring a subset $I\subseteq S$. Now we need vectors $(\gamma_{g_1}(I),\dots,\gamma_{g_N}(I))$ for the coloring: for every $g\in\mathbf{G}$ and for every $I\subseteq S$, let $\gamma_g(I)$ be the number of commutator expressions t'_j such that $t'_j(\bar h)=g$ and t'_j depends on variable x_i for every $i\in I$. (Note that t'_j may depend on variable x_i for some $i\notin I$.) Now, if t'_j depends on variable x_i for some $i\in H$, then $t'_j(\bar h_{S\setminus H})=1$; thus, for every $g\in\mathbf{G}$, by inclusion-exclusion we have

$$\beta_g-\alpha_g = \sum_{I\subseteq H,|I|<c}(-1)^{|I|}\gamma_g(I) = -\sum_{i\in H}\gamma_g(\{\,i\,\}) + \sum_{\substack{i,j\in H\\ i<j}}\gamma_g(\{\,i,j\,\}) - \cdots.$$

We prove that there exists a subset $H\subseteq S$ such that for every $g\in\mathbf{G}$, every sum $\sum_{i\in H}\gamma_g(\{\,i\,\})$, $\sum_{i,j\in H,i\ne j}\gamma_g(\{\,i,j\,\})$, etc., is divisible by the exponent of the group, $e_{\mathbf{G}}$. To this end, we consider $\gamma_g(I)$ modulo $e_{\mathbf{G}}$: let $\gamma'_g(I)\in\{\,0,1,\dots,e_{\mathbf{G}}-1\,\}$ be such that $\gamma'_g(I)\equiv\gamma_g(I) \pmod{e_{\mathbf{G}}}$. We color the subsets of S by vectors of dimension $|\mathbf{G}|=N$: the color of a subset $I\subseteq S$ is the vector $(\gamma'_{g_1}(I),\gamma'_{g_2}(I),\dots,\gamma'_{g_N}(I))$, where $g_1\succ g_2\succ\cdots\succ g_N$ are the elements of $\mathbf{G}$ in decreasing order. Now we have $k=e_{\mathbf{G}}^N$-many colors since every coordinate is an element of the set $\{\,0,1,\dots,e_{\mathbf{G}}-1\,\}$. Thus, we have colored the less

than c-element subsets of S by $k = e_{\mathbf{G}}^N$ colors. Let $m = (c-1)! \cdot e_{\mathbf{G}}$. By Theorem 2.2 for c, k, m, there exists a d such that

> if $|S| > d$, then S has a subset H with m elements, such that any two less than c-element subsets of the same size have the same color.

That is, if $|S| > d$, then there exists a subset $H \subseteq S$, $|H| = m$ such that every one element subset of H has the same color, every two element subset of H has the same color, ..., every subset of H with $(c-1)$ elements has the same color. Let $\gamma'_g(i)$ denote the g-coordinate of the color of the subsets of H with i elements. That is, $\gamma'_g(i) = \gamma'_g(I)$, where $I \subseteq H$ is arbitrary such that $|I| = i$. Now,

$$t'(\bar{h}_{S\setminus H}) = g_1^{\beta_{g_1}} g_2^{\beta_{g_2}} \cdots g_N^{\beta_{g_N}},$$

where for every $g \in \mathbf{G}$ we have

$$\begin{aligned}\beta_g - \alpha_g &= -\sum_{i\in H} \gamma_g(\{\, i \,\}) + \sum_{\substack{i,j\in H\\ i<j}} \gamma_g(\{\, i,j \,\}) - \cdots \\ &\equiv \sum_{i=1}^{c-1} (-1)^i \binom{m}{i} \gamma'_g(i) \pmod{e_{\mathbf{G}}}.\end{aligned}$$

We chose m such that all binomial coefficients $\binom{m}{i}$ for $1 \le i \le c-1$ are divisible by $e_{\mathbf{G}}$ (the exponent of $\mathbf{G}$); thus, $t'(\bar{h}_{S\setminus H}) = t'(\bar{h})$, and $t(\bar{h}_{S\setminus H}) = t(\bar{h})$ follows. Hence, if $|S| > d$, then we have found $H \subseteq S$ such that $t(\bar{h}_{S\setminus H}) = t(\bar{h})$. If $|S \setminus H| > d$, then we can repeat the procedure for $S = S \setminus H$ until $|S \setminus H| \le d$ holds. □

Note that the value of d obtained by Ramsey's theorem is rather big compared to the size of the group. It is more than $e_{\mathbf{G}}^{e_{\mathbf{G}}^{\cdots^{e_{\mathbf{G}}^{Nm}}}}$, where $N = |\mathbf{G}|$, $e_{\mathbf{G}}$ is the exponent of $\mathbf{G}$, c is the nilpotency class of $\mathbf{G}$, and $m = (c-1)! \cdot e_{\mathbf{G}}$, as defined in the proof of Lemma 3.1, and the height of the tower is c. Finally we prove Theorem 1.3.

Proof of Theorem 1.3. Let d be the Ramsey number as in Lemma 3.1. Let $t(x_1, \ldots, x_n)$ be an arbitrary expression over $\mathbf{G}$. Let T_d denote the set of n-tuples $(h_1, \ldots, h_n)$ for which the number of non-identity coordinates is at most d:

$$T_d = \{\, (h_1, \ldots, h_n) \mid |\{\, i : h_i \neq 1 \,\}| \le d \,\}.$$

By Lemma 3.1 we have

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

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

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

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, $\mathbf{G} \models t \approx 1$ if and only if $t(\mathbf{G},\dots,\mathbf{G}) = \{1\}$. Moreover, $t = 1$ can be solved if and only if $1 \in t(\mathbf{G},\dots,\mathbf{G})$. □

4. Open problems

The characterization of the complexities of the equivalence and equation solvability problems are far from complete. As mentioned in the introduction, one direction could be to generalize the methods of this paper for arbitrary nilpotent algebras:

Problem 1. *Prove that the equivalence and the equation solvability problems can be decided in polynomial time for finite nilpotent algebras.*

The characterization of these complexities are incomplete even for finite groups. The results in the different cases imply that a dichotomy theorem similar to Theorem 1.1 might hold. We conjecture that the complexity depends on whether the group is solvable or not solvable:

Conjecture. *For a finite group* $\mathbf{G}$*, the complexity of the equivalence and the equation solvability problems can be solved in polynomial time if* $\mathbf{G}$ *is solvable, and is (co)NP-complete if* $\mathbf{G}$ *is not solvable.*

The smallest group for which the complexity of neither the equivalence nor the equation solvability problem is known is $\mathbf{S}_4$.

Problem 2. *Characterize the equivalence and equation solvability problems for finite groups. In particular, determine the complexity of the equivalence and equation solvability problems for the finite group* $\mathbf{S}_4$*.*

The proofs of Theorem 1.2 and 1.3 relied on the existence of an integer d, depending only on the ring $\mathcal{R}$ or on the group $\mathbf{G}$, such that to obtain the range of a polynomial one has to consider substitutions bounded by d. Note that the bound for this integer d obtained in this paper is multiply exponential in the size of the ring $\mathcal{R}$ or of the group $\mathbf{G}$. For the polynomial equivalence problem, d can be chosen to be the nilpotency class of the ring $\mathcal{R}$ (see [11]) or the group $\mathbf{G}$ (see [3]). It would be interesting to find a reasonably small upper bound on the integer d for the equation solvability problem, as well.

Problem 3. *Determine if the integer d in Lemmas 2.1 and 3.1 can be bounded by a polynomial in the size of the ring or group.*

References

[1] Almeida, J., Volkov, M.V., Goldberg, S.V.: Complexity of the identity checking problem for finite semigroups. J. Math. Sci. (N. Y.) **158**, no. 5, 605–614 (2009)
[2] Burris, S., Lawrence, J.: The equivalence problem for finite rings. J. Symbolic Comput. **15**, 67–71 (1993)

[3] Burris, S., Lawrence, J.: Results on the equivalence problem for finite groups. Algebra Universalis **52**, no. 4, 495–500 (2004)
[4] Goldmann, M., Russell, A.: The complexity of solving equations over finite groups. In: Proceedings of the 14th Annual IEEE Conference on Computational Complexity, pp. 80–86. Atlanta, Georgia (1999)
[5] Graham, R.L., Rotschild, B.L., Spencer, J.H.: Ramsey Theory, 2nd edn. Wiley-Interscience Series in Discrete Mathematics and Optimization. John Wiley & Sons (1990)
[6] Horváth, G.: The complexity of the equivalence problem over finite rings. Glasg. Math. J. (in press)
[7] Horváth, G., Lawrence, J., Mérai, L., Szabó, Cs.: The complexity of the equivalence problem for non-solvable groups. Bull. Lond. Math. Soc. **39**, no. 3, 433–438 (2007)
[8] Horváth, G., Lawrence, J., Willard, R.: The complexity of the equation solvability problem over finite rings (2011, preprint)
[9] Horváth, G., Szabó, Cs.: The complexity of checking identities over finite groups. Internat. J. Algebra Comput. **16**, no. 5, 931–940 (2006)
[10] Horváth, G., Szabó, Cs.: Equivalence and equation solvability problems for the alternating group A_4. J. Pure Appl. Algebra (in press)
[11] Hunt, H., Stearns, R.: The complexity for equivalence for commutative rings. J. Symbolic Comput. **10**, 411–436 (1990)
[12] Kisielewicz, A.: Complexity of semigroup identity checking. Internat. J. Algebra Comput. **14**, no. 4, 455–464 (2004)
[13] Klíma, O.: Complexity issues of checking identities in finite monoids. Semigroup Forum **79**, no. 3, 435–444 (2009)
[14] Klíma, O.: Unification Modulo Associativity and Idempotency. PhD thesis, Masarik University, Brno (2004)
[15] Neumann, H.: Varieties of Groups. Springer, Berlin (1967)
[16] Péladeau, P., Thérien, D.: Sur les langages reconnus par des groupes nilpotents. C. R. Acad. Sci. Paris Sér. I Math **306**, no. 2, 93–95 (1988) (French)
[17] Plescheva, S., Vértesi, V.: Checking identities in 0-simple semigroups. Journal of Ural State University **43**, 72–102 (2006) (Russian)
[18] Seif, S., Szabó, Cs.: Computational complexity of checking identites in 0-simple semigroups and matrix semigroups over finite fields. Semigroup Forum **72**, no. 2, 207–222 (2006)
[19] Szabó, Cs., Vértesi, V.: The complexity of checking identities for finite matrix rings. Algebra Universalis **51**, 439–445 (2004)
[20] Szabó, Cs., Vértesi, V.: The complexity of the word-problem for finite matrix rings. Proc. Amer. Math. Soc. **132**, 3689–3695 (2004)
[21] Szabó, Cs., Vértesi, V.: The equivalence problem over finite rings. Internat. J. Algebra Comput. **21**, no. 3, 449–457 (2011)
[22] Thérien, D.: Subword counting and nilpotent groups. In: Combinatorics on Words (Waterloo, 1982), pp. 297–305. Academic Press, Toronto (1983)

Gábor Horváth

Institute of Mathematics, University of Debrecen, Pf. 12, Debrecen, 4010, Hungary
e-mail: ghorvath@science.unideb.hu