THE COMPLEXITY OF THE EQUATION SOLVABILITY PROBLEM OVER SEMIPATTERN GROUPS

ATTILA FÖLDVÁRI

ABSTRACT. The complexity of the equation solvability problem is known for nilpotent groups, for not solvable groups and for some semidirect products of Abelian groups. We provide a new polynomial time algorithm for deciding the equation solvability problem over certain semidirect products, where the first factor is not necessarily Abelian. Our main idea is to represent such groups as matrix groups, and reduce the original problem to equation solvability over the underlying field. Further, we apply this new method to give a much more efficient algorithm for equation solvability over nilpotent rings than previously existed.

1. INTRODUCTION

One of the oldest problems of algebra is the equation solvability problem over a given algebraic structure. Nowadays, many such classical problems arise in a new perspective, namely to consider their computational complexity. In this paper we investigate the complexity of the equation solvability problem over finite groups and rings.

The *equation solvability problem* over a finite group $\mathbf{G}$ asks whether or not two group expressions (i.e. products of variables and elements of $\mathbf{G}$) can attain the same value for some substitution over $\mathbf{G}$. In other words, for the equation solvability problem, one needs to find if there exists at least one substitution satisfying the equation. Another interesting problem is whether or not *all* substitutions satisfy the equation. The *equivalence problem* over a finite group $\mathbf{G}$ asks whether or not two group expressions f and g are equivalent over $\mathbf{G}$ (denoted by $\mathbf{G} \models f \approx g$), that is whether or not f and g determine the same function over $\mathbf{G}$. We investigate the complexities of these problems in the length of the input polynomials, that is in the number of operations occurring in them. We denote the length of a polynomial f by $||f||$.

First Burris and Lawrence [2] investigated the complexity of the equivalence problem over finite groups. They proved that if a group $\mathbf{G}$ is nilpotent or $\mathbf{G} \simeq \mathbf{D}_n$, the dihedral group for odd n, then the equivalence problem for $\mathbf{G}$ has polynomial time complexity. They conjectured that the equivalence problem for $\mathbf{G}$ is in polynomial time if $\mathbf{G}$ is solvable, and coNP-complete otherwise. Horváth and Szabó [11] confirmed the conjecture for $\mathbf{G} \simeq \mathbf{A} \rtimes \mathbf{B}$, where $\mathbf{A}$ and $\mathbf{B}$ are Abelian groups such that the exponent of $\mathbf{A}$ is squarefree and $(|\mathbf{A}|, |\mathbf{B}|) = 1$. Later Horváth [8] generalized this result to semidirect products $\mathbf{A} \rtimes \mathbf{B}$, where $\mathbf{A}$ and $\mathbf{B}/C_{\mathbf{B}}(\mathbf{A})$ are Abelian groups (here $C_{\mathbf{B}}(\mathbf{A})$ denotes the centralizer of $\mathbf{A}$ in $\mathbf{B}$). Horváth, Lawrence, Mérai and Szabó [10] proved the coNP-complete part of the conjecture. But the complexity of the equivalence problem over many solvable, not nilpotent groups is not determined, yet. Three of the smallest groups, for which this complexity is not known, are $\mathbf{S}_4$, $\mathbf{SL}(2, \mathbb{Z}_3)$ and a non-commutative group of order 54. See [8] for a more comprehensive list.

Even less is known about the equation solvability problem. Goldmann and Russel [4, 5] proved that if $\mathbf{G}$ is nilpotent then the equation solvability problem over $\mathbf{G}$ is solvable in polynomial time, while if $\mathbf{G}$ is not solvable, then the equation solvability problem is NP-complete. Little is known for solvable, not nilpotent groups. Horváth proved in [8, Corollary 2] that the equation solvability problem over $\mathbf{G}$ is solvable in polynomial time for certain groups $\mathbf{G} \simeq \mathbf{A} \rtimes \mathbf{B}$, where $\mathbf{A} \simeq \mathbf{Z}_{p^k}$ or $\mathbf{Z}_{2p^k}$ or $\mathbf{Z}_p^k$ and $\mathbf{B}$ is commutative. Note that all results for both the equivalence and the equation solvability problem over solvable, not nilpotent groups are about groups $\mathbf{A} \rtimes \mathbf{B}$, where $\mathbf{A}$ is Abelian.

One of the groups of small order, for which the computational complexity of the equation solvability problem is unknown, is the group $\mathbf{U}(3, \mathbb{Z}_3) \rtimes \mathbb{Z}_3^{\times}$. Here, $\mathbf{U}(3, \mathbb{Z}_3)$ denotes the noncommutative group of 3×3 upper unitriangular matrices over $\mathbb{Z}_3$. Horváth explicitly asks in [8, Problem 4] the complexity of the equivalence and equation solvability problems over this group. The group $\mathbf{U}(3, \mathbb{Z}_3) \rtimes \mathbb{Z}_3^{\times}$ is isomorphic to a special subgroup of the 3×3 upper triangular matrices over $\mathbb{Z}_3$. Motivated by the definition of pattern groups from [3, 13], we call a group $\mathbf{A} \rtimes \mathbf{B}$ a *semipattern* group, if $\mathbf{A}$ is a subgroup of the group of upper unitriangular matrices, and $\mathbf{B}$ is a subgroup of the diagonal matrices. We give the precise definition of semipattern groups in Section 2.1. The main result of the paper is the following.

Theorem 1.1. *The equation solvability problem over semipattern groups is solvable in polynomial time.*

The group $\mathbf{U}(3, \mathbb{Z}_3) \rtimes \mathbb{Z}_3^{\times}$ defined in [8, Problem 4] is in fact a semipattern group, thus Theorem 1.1 answers Horváth's question completely. Further, from Theorem 1.1 the equivalence problem over semipattern groups is solvable in polynomial time, as well. Indeed, it is

known that for a group $\mathbf{G}$ if the equation solvability problem is solvable in polynomial time, then the equivalence problem is solvable in polynomial time, as well.

In the proof of Theorem 1.1 we reduce the solvability of the input equation over a matrix group over a finite field to the solvability of a system of equations over the same field. Then we apply some results over finite rings. Therefore, we summarize the known results over rings.

The *equation solvability problem* over a finite ring $\mathcal{R}$ asks whether or not two polynomials can attain the same value for some substitution over $\mathcal{R}$. The *equivalence problem* over a finite ring $\mathcal{R}$ asks whether or not two polynomials are equivalent over $\mathcal{R}$ i.e. if they determine the same function over $\mathcal{R}$.

The complexity of these questions was completely characterized in the past two decades. Hunt and Stearnes [12] investigated the equivalence problem for finite commutative rings. Later Burris and Lawrence [1] generalized their result to non-commutative rings. They proved that the equivalence problem for $\mathcal{R}$ is solvable in polynomial time if $\mathcal{R}$ is nilpotent, and is coNP-complete otherwise.

The proof of Burris and Lawrence reduces the satisfiability (SAT) problem to the equivalence problem by using long products of sums of variables. Nevertheless, if we expand this polynomial into a sum of monomials then the length of the new polynomial may become exponential in the length of the original polynomial. Such a change in the length suggests that the complexity of the equivalence problem might be different if the input polynomials are restricted to be written as sums of monomials. This motivated Lawrence and Willard [15] to introduce the *sigma equivalence* and *sigma equation solvability problems*, where the input polynomials are given as sums of monomials. Lawrence and Willard conjectured that if the factor by the Jacobson radical is commutative then the sigma equivalence problem is solvable in polynomial time, and is coNP-complete otherwise. Szabó and Vértesi proved the coNP-complete part of the conjecture in [16]. Horváth confirmed the conjecture for commutative rings in [7]. The polynomial part of this conjecture is completely proved in the manuscript [9].

Most of the results for the [sigma] equation solvability problem follow from the corresponding result for the [sigma] equivalence problem. In particular, from the argument of Szabó and Vértesi follows that if the factor by the Jacobson radical is not commutative then the sigma equation solvability problem is NP-complete. Horváth, Lawrence and Willard [9] proved that if this factor is commutative then the sigma equation solvability problem is solvable in polynomial time. Thus, the sigma equation solvability problem is completely characterized.

For the general equation solvability, arguments of Burris and Lawrence from [1] yield that if the ring is not nilpotent then the problem is NP-complete. Horváth in [6] proved that the equation solvability problem is solvable in polynomial time otherwise.

Theorem 1.2 ([6, Theorem 1.2]). *If $\mathcal{R}$ is a finite, nilpotent ring then the equation solvability problem over $\mathcal{R}$ is solvable in polynomial time.*

Horváth uses Ramsey's theorem in the proof of Theorem 1.2. He defines a number r that depends only on the ring $\mathcal{R}$. Then he proves that the image of every polynomial can be obtained by substituting 0 into all but r-many variables. Thus one can decide whether or not $f = 0$ is solvable over $\mathcal{R}$ in $O\left(\|f\|^r\right)$ time. However, this number r is huge in the size of the ring. In fact, r is greater than $|\mathcal{R}|^{|\mathcal{R}|^{\cdots^{|\mathcal{R}|}}}$, where the height of the tower in the exponent is the nilpotency class of $\mathcal{R}$. Horváth specifically asks in [6, Problem 3] whether or not this number r can be decreased.

In the second half of the paper we give a new proof of Theorem 1.2. Our algorithm is much more efficient than Horváth's. Wilson [17] characterizes nilpotent rings with the help of special kind of nilpotent matrix rings. We can decide the equation solvability problem over these special matrix rings similarly as we do over semipattern groups in Theorem 1.1. In particular, we show that over a nilpotent ring $\mathcal{R}$ we can decide in $O\left(\|f\|^{|\mathcal{R}|^{2\log \mathcal{R}}\log^5|\mathcal{R}|}\right)$ time whether or not $f = 0$ is solvable, thus providing a partial answer to Problem 3 in [6], as well. We mention that in a completely independent way, Károlyi and Szabó also found a way to decrease the exponent r in [14].

In Section 2 we summarize the notations, definitions and theorems, that we use in the paper. In particular, in Section 2.1 we review the definition of pattern groups, then we define semipattern groups. In Section 2.2 we discuss the generalization of the equation solvability problem over rings for systems of equations. We are going to apply these results in order to prove Theorems 1.1 and 1.2. In Section 2.3 we lay the groundwork for the proof of Theorem 1.2. In Section 3 we prove Theorem 1.1. We use ideas of this proof in Section 4, where we prove Theorem 1.2.

2. Preliminaries

2.1. **Semipattern groups.** Let $\mathbb{F}_q$ denote the finite field of q elements. Let us consider the group $\mathbf{T}\left(m, \mathbb{F}_q\right)$ of $m \times m$ upper triangular matrices, that is those matrices whose elements under the diagonal are zero and the elements in the diagonal are non-zero:

$$\mathbf{T}(m, \mathbb{F}_q) = \left\{ \begin{pmatrix} s_1 & a_{1,2} & a_{1,3} & \ldots & a_{1,m} \\ 0 & s_2 & a_{2,3} & \ldots & a_{2,m} \\ 0 & 0 & s_3 & \ldots & a_{3,m} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & s_m \end{pmatrix} : s_i \in \mathbb{F}_q^\times, a_{i,j} \in \mathbb{F}_q, 1 \leq i < j \leq m \right\}.$$

Here the group operation is the matrix multiplication.

Let the $m \times m$ identity matrix denoted by I. Let $I_{i,j}$ denote the $m \times m$ matrix whose elements are all zero except for the jth element in the ith row, which is 1. Let $P \subseteq \{(i,j) : 1 \leq i < j \leq m\}$. Let

$$\mathbf{N}_P = \{I + \sum_{(i,j) \in P} a_{i,j} I_{i,j} : a_{i,j} \in \mathbb{F}_q\}.$$

Thus, $\mathbf{N}_P$ contains all those upper triangular matrices, where every element in the diagonal is 1, and every element whose position is not occurring in P has to be 0. If $\mathbf{N}_P$ is a subgroup of $\mathbf{T}(m, \mathbb{F}_q)$, then we call $\mathbf{N}_P$ a *pattern* group. For more details on pattern groups, see e.g. [3, 13]. Let $\mathbf{S}_1, \mathbf{S}_2, \ldots, \mathbf{S}_m$ be subgroups of $\mathbb{F}_q^\times$ and let $\mathbf{D}$ be the set of $m \times m$ matrices over $\mathbb{F}_q$ whose i^{th} element in the diagonal is from $\mathbf{S}_i$ $(1 \leq i \leq m)$:

$$\mathbf{D} = \left\{ \begin{pmatrix} s_1 & 0 & 0 & \ldots & 0 \\ 0 & s_2 & 0 & \ldots & 0 \\ 0 & 0 & s_3 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & s_m \end{pmatrix} : s_1 \in \mathbf{S}_1, s_2 \in \mathbf{S}_2, \ldots, s_m \in \mathbf{S}_m \right\}.$$

If $\mathbf{N}_P$ is a pattern group then $\mathbf{N}_P \mathbf{D}$ is a subgroup of $\mathbf{T}(m, \mathbb{F}_q)$. Then we call $\mathbf{N}_P \mathbf{D}$ a *semipattern group* and we denote such a group by $\mathbf{SP}(m, \mathbb{F}_q)$. Further, we note that $\mathbf{N}_P \lhd \mathbf{N}_P \mathbf{D}$ and $\mathbf{N}_P \mathbf{D} \cong \mathbf{N}_P \rtimes \mathbf{D}$. The group $\mathbf{U}(3, \mathbb{Z}_3) \rtimes \mathbb{Z}_3^\times$ defined in [8, Problem 4] is in fact a semipattern group:

$$\mathbf{U}(3, \mathbb{Z}_3) \rtimes \mathbb{Z}_3^\times = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & s & c \\ 0 & 0 & 1 \end{pmatrix} : s \in \mathbb{Z}_3^\times, a, b, c \in \mathbb{Z}_3 \right\}.$$

2.2. **Further notations.** Let $\mathcal{R}$ be a commutative, unital ring, $S_1, \ldots \ldots, S_m$ be subsets of $\mathcal{R}$. For nonnegative integers $n, l_1, \ldots l_m$, let $X = \{x_1, \ldots, x_n\}$, $Y_1 = \{y_{1,1}, \ldots, y_{1,l_1}\}$, $\ldots$, $Y_m = \{y_{m,1}, \ldots, y_{m,l_m}\}$ be pairwise disjoint sets of variables. We say that $f = g$ *is solvable over* $\mathcal{R}$ *for substitutions from* $\mathcal{R}, S_1, \ldots, S_m$ (and write $f|_{\mathcal{R}, S_1, \ldots, S_m} = g|_{\mathcal{R}, S_1, \ldots, S_m}$ is solvable over $\mathcal{R}$) if there exist $a_1, \ldots a_n \in \mathcal{R}$, $s_{1,1}, \ldots s_{1,l_1} \in S_1$, $\ldots$, $s_{m,1}, \ldots, s_{m,l_m} \in S_m$ such that the two polynomials attain the same

value on this substitution:

$$f(a_1, \ldots a_n, s_{1,1}, \ldots s_{1,l_1}, \ldots, s_{m,1}, \ldots, s_{m,l_m}) =$$
$$g(a_1, \ldots a_n, s_{1,1}, \ldots s_{1,l_1}, \ldots, s_{m,1}, \ldots, s_{m,l_m})$$

For proving Theorem 1.1, we will directly apply the following result of Horváth [8].

Theorem 2.1 ([8, p. 221, case (d)]). *Let $\mathbb{F}_q$ be a finite field. Let $\mathbf{S}_1, \ldots, \mathbf{S}_m$ be subgroups of $\mathbb{F}_q^\times$. Let $f_1, \ldots, f_k \in \mathbb{F}_q[x_1, \ldots x_n, y_{1,1}, \ldots, y_{m,l_m}]$ be a polynomial, written as a sum of monomials. Then it can be decided whether the system of equations*

$$f_1|_{\mathbb{F}_q, \mathbf{S}_1, \ldots, \mathbf{S}_m} = 0$$
$$\vdots$$
$$f_k|_{\mathbb{F}_q, \mathbf{S}_1, \ldots, \mathbf{S}_m} = 0$$

is solvable over $\mathbb{F}_q$ in $O\left(max_{1 \leq i \leq k}||f_i||^{k \cdot q}\right)$ time.

To prove Theorem 1.2 we are going to use the following from [9].

Theorem 2.2 ([9]). *Let $f_1, \ldots, f_k \in \mathbb{Z}_{p^\alpha}[y_1, \ldots, y_n]$ be polynomials, written as sums of monomials. Then it can be decided whether the system of equations*

$$f_1 = 0$$
$$\vdots$$
$$f_k = 0$$

is solvable over $\mathbb{Z}_{p^\alpha}$ in $O\left(max_{1 \leq i \leq k}||f_i||^{\alpha^2 k \cdot p^{2\alpha^2}}\right)$ time.

2.3. **Equation solvability problem over nilpotent rings.** The complexity of the equation solvability problem over finite nilpotent rings is known. Horváth [6] proved that the equation solvability problem is solvable in polynomial time. We give a new algorithm in Section 4 that is much more efficient than Horváth's. In this part we show that we can characterize the complexity of the equation solvability problem over nilpotent rings using the sigma equation solvability problem over special kind of nilpotent matrix rings. Hence we can apply the same ideas that we used in the proof of Theorem 1.1.

Horváth proved Theorem 1.2 using Ramsey's theory. He defined a number r that depends only on the ring $\mathcal{R}$. Then he proved that the image of every polynomial can be obtained by substituting 0 into all but r-many variables. Thus one can decide whether or not $f = 0$ is solvable over $\mathcal{R}$ in $O(||f||^r)$ time. But the number r is huge in the size

of the ring. Let c be the characteristic of $\mathcal{R}$ and t be the nilpotency class of $\mathcal{R}$. Let furthermore $m = (t-1)! \cdot c$. Then r is greater than $m^{m^{\cdots^{m}}}$, where the height of the tower in the exponent is t. We give a new proof of Theorem 1.2 in Section 4. Our algorithm is much more efficient than Horváth's. We prove that $O\left(||f||^{|\mathcal{R}|^{2\log|\mathcal{R}|}\log^{5}|\mathcal{R}|}\right)$ time is enough.

First, we show that we can handle the equation solvability problem over nilpotent rings using the sigma equation solvability problem over special kind of nilpotent matrix rings. If $\mathcal{R}$ is a nilpotent ring then the complexity of the *general* equation solvability problem over $\mathcal{R}$ is the same as the complexity of the *sigma* equation solvability over $\mathcal{R}$. Indeed, we can rewrite every polynomial f over $\mathcal{R}$ as a sum of monomials in $O\left(||f||^{t}\right)$ time, where t is the nilpotency class of $\mathcal{R}$. Now, $t = O\left(\log|\mathcal{R}|\right)$. Hence, at the cost of an extra $\log|\mathcal{R}|$ factor in the exponent, we may assume that every input polynomial is given as a sum of monomials. Furthermore it is enough to consider the equation solvability problem over nilpotent rings with prime power characteristic, because every ring is a direct sum of rings of prime power characteristic, and the equation solvability problem can be handled componentwise. Wilson [17] characterizes finite nilpotent rings with prime power characteristic.

Theorem 2.3 (Wilson). *Let $\mathcal{R}$ be a finite nilpotent ring with characteristic p^{α}, and let $\mathcal{R}$ have an independent generating set consisting of m generators over $\mathbb{Z}_{p^{\alpha}}$. Then $\mathcal{R}$ is a homomorphic image of a ring $\mathcal{M}(m, \mathbb{Z}_{p^{\alpha}})$ of matrices over $\mathbb{Z}_{p^{\alpha}}$ where every entry on or below the main diagonal is a multiple of p.*

In fact for nilpotent rings it is enough to consider the equation solvability problem over such a matrix ring $\mathcal{M}$, since if the equation solvability problem is solvable in polynomial time for $\mathcal{M}$, then it is solvable in polynomial time for a quotient $\mathcal{M}/\mathcal{I}$, as well. Indeed, let $\widetilde{f}$ be a polynomial over $\mathcal{M}/\mathcal{I}$ and f be any polynomial over $\mathcal{M}$ whose quotient by $\mathcal{I}$ is $\widetilde{f}$. Then $\widetilde{f} = 0$ is solvable over $\mathcal{M}/\mathcal{I}$ if and only if $f = a$ is solvable over $\mathcal{M}$ for some $a \in \mathcal{I}$. This gives an extra $|\mathcal{I}|$ factor to the running time. However, $|\mathcal{I}| \leq |\mathcal{M}| \leq (p^{\alpha})^{m^{2}}$, and we have $p^{\alpha} = O\left(|\mathcal{R}|\right)$, $m = O\left(\log|\mathcal{R}|\right)$. Thus, $|\mathcal{I}| = O\left(|\mathcal{R}|^{\log^{2}|\mathcal{R}|}\right)$, which only depends on $\mathcal{R}$, and thus can be forgotten about.

Thus it is enough to consider the sigma equation solvability problem over such a matrix ring of matrices over $\mathbb{Z}_{p^{\alpha}}$ where every entry on or below the main diagonal of each matrix is a multiple of p. We can handle such matrix rings similarly as we do with the semmipattern groups. Hence we can use ideas of the proof described in Section 3. We give a new, efficient algorithm that decides the equation solvability problem over nilpotent matrix rings in Section 4.

3. Equation solvability problem over semipattern groups

In this section we consider the equation solvability problem over semimipattern groups. First we characterize the multiplication of matrices from $\mathbf{T}\left(m, \mathbb{F}_q\right)$ in Lemma 3.1. We use this formula in our algorithm.

Lemma 3.1. *Let n be a natural number. For every $1 \leq k \leq n$ let*

$$A_k = \begin{pmatrix} s_{1,k} & a_{1,2,k} & a_{1,3,k} & \cdots & a_{1,m,k} \\ 0 & s_{2,k} & a_{2,3,k} & \cdots & a_{2,m,k} \\ 0 & 0 & s_{3,k} & \cdots & a_{3,m,k} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & s_{m,k} \end{pmatrix} \in \mathbf{T}\left(m, \mathbb{F}_q\right).$$

Let

$$A_1 A_2 \ldots A_n = \begin{pmatrix} \sigma_1 & \alpha_{1,2} & \alpha_{1,3} & \cdots & \alpha_{1,m} \\ 0 & \sigma_2 & \alpha_{2,3} & \cdots & \alpha_{2,m} \\ 0 & 0 & \sigma_3 & \cdots & \alpha_{3,m} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \sigma_m \end{pmatrix}.$$

Then

- *for every $i = 1, 2, \ldots, n$ we have*

$$\sigma_i = \prod_{k=1}^{n} s_{i,k};$$

- *for every $1 \leq i < j \leq m$ we have*

$$
\begin{aligned}
\alpha_{i,j} = &\sum_{b=0}^{j-i-1} \sum_{i<l_1<\cdots<l_b<j} \sum_{k_{b+1}=b+1}^{n} \sum_{k_b=b}^{k_{b+1}-1} \cdots \sum_{k_2=2}^{k_3-1} \sum_{k_1=1}^{k_2-1} \left(\prod_{c_0=1}^{k_1-1} s_{i,c_0}\right) a_{i,l_1,k_1} \\
&\left(\prod_{c_1=k_1+1}^{k_2-1} s_{l_1,c_1}\right) a_{l_1,l_2,k_2} \left(\prod_{c_2=k_2+1}^{k_3-1} s_{l_2,c_2}\right) a_{l_2,l_3,k_3} \left(\prod_{c_3=k_3+1}^{k_4-1} s_{l_3,c_3}\right) \\
&\ldots a_{l_{b-1},l_b,k_b} \left(\prod_{c_b=k_b+1}^{k_{b+1}-1} s_{l_b,c_b}\right) a_{l_b,j,k_{b+1}} \left(\prod_{c_{b+1}=k_{b+1}+1}^{n} s_{j,c_{b+1}}\right).
\end{aligned}
$$

(1)

The length of (1) *is $O\left(n^m\right)$, and in particular is polynomial in n.*

Proof. The lemma can be proved by induction on n. However, instead of giving the technical induction proof, we explain how one can arrive at this formula.

Let us consider the jth element of the ith row $\alpha_{i,j}$ of the matrix $A_1 A_2 \ldots A_n$ $(1 \leq i < j \leq m)$. We can express this element $\alpha_{i,j}$ with a sum of some appropriate products. In every such product we multiply one element from each matrix A_k $(1 \leq k \leq n)$. (In the notation the index k appears as the last index.) Furthermore the index of the column

of a term must equal with the index of the row of the following term in every such product. (Therefore a term of the form $s_{l_c,.}$ or $a_{l_c,l_{c+1},.}$ follows the term of the form $s_{l_c,.}$ or $a_{l_{c-1},l_c,.}$.) The row index of the first term is i, the column index of the last term is j. The matrices $A_1, A_2, \ldots, A_n$ are upper triangular matrices, hence the row index of every term of every product is less than or equal to the column index. (Thus for every term of the form $a_{l_c,l_{c+1},.}$, that are above the diagonal, we have $l_c < l_{c+1}$.) Thus the jth element of the ith row $\alpha_{i,j}$ of the matrix $A_1 A_2 \ldots A_n$ is a sum of products of n terms such that

- the row index of the first term is i, the column index of the last term is j;
- the column index of every term equals to the row index of the next term;
- the row index of a term is at most the row index of the next term.

Notice, that every n-term product is uniquely determined by those terms where the row index differs from the column index. Let two such consecutive terms of the product be a_{l_{c-1},l_c,k_c} and $a_{l_c,l_{c+1},k_{c+1}}$. (Here $i \le l_{c-1} < l_c < l_{c+1} \le j$ and $1 \le k_c < k_{c+1} \le n$.) The product of the terms between these two terms have row and column index l_c and their last index is more than k_c and less than k_{c+1}. Thus between the terms a_{l_{c-1},l_c,k_c} and $a_{l_c,l_{c+1},k_{c+1}}$ can only be the product $s_{l_c,k_c+1} \cdot s_{l_c,k_c+2} \cdot \ldots \cdot s_{l_c,k_{c+1}-1}$. Thus formula (1) is proved.

Now, we calculate the length of formula (1). Formula (1) is a sum of products. The length of every product is n, thus we need to calculate the number of products. Notice, that every product is uniquely determined by the column indices of the terms. More exactly we need to know the column indices of the first $n-1$ terms, because the column index of the last term is j. We can choose these indices from the set $\{i, i+1, \ldots, j-1, j\}$. The order of the selected elements does not matter. We only need to determine how many indices are equal to i or to $i+1$, etc, or to j. Thus we need to choose $n-1$ element from a set of $j-i+1$ elements such that repetitions are allowed. Hence the number of products is

$$\binom{n-1+j-i+1-1}{n-1} = \binom{n+j-i-1}{j-i}.$$

Since every product has length n, the length of $\alpha_{i,j}$ is

$$\binom{n+j-i-1}{j-i} \cdot n = O\left(n^{j-i+1}\right) = O\left(n^m\right).$$

Thus the length of $\alpha_{i,j}$ is at most $O\left(n^m\right)$ for every index $1 \le i < j \le m$. $\qquad\square$

Let $\mathbf{SP}(m, \mathbb{F}_q)$ be a semipattern group. Let $F = T_1 T_2 \ldots T_n$ be a polynomial over $\mathbf{SP}(m, \mathbb{F}_q)$. Thus T_k can indicate a constant or a

variable over $\mathbf{SP}(m, \mathbb{F}_q)$ $(1 \le k \le n)$. Of course T_k and T_l can indicate the same constant or variable. Let

$$
T_k = \begin{pmatrix}
y_{1,k} & x_{1,2,k} & x_{1,3,k} & \cdots & x_{1,m,k} \\
0 & y_{2,k} & x_{2,3,k} & \cdots & x_{2,m,k} \\
0 & 0 & y_{3,k} & \cdots & x_{3,m,k} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \cdots & y_{m,k}
\end{pmatrix}.
$$

If $T_k \in \mathbf{SP}(m, \mathbb{F}_q)$ indicates constant then $y_{i,k}$ is a constant in $\mathbf{S}_i \le \mathbb{F}_q^\times$ and $x_{i,j,k}$ is a constant in $\mathbb{F}_q$ $(1 \le i < j \le m)$. If $T_k \in \mathbf{SP}(m, \mathbb{F}_q)$ is a variable, then $y_{i,k}$ is a variable, that we can substitute from $\mathbf{S}_i$, and $x_{i,j,k}$ is a variable that we can substitute from $\mathbb{F}_q$. Furthermore $T_k = T_l$ if and only if $y_{i,k} = y_{i,l}$ (for every $1 \le i \le k$) and $x_{i,j,k} = x_{i,j,l}$ for every $1 \le i < j \le m$.

We can rewrite the polynomial F with this notation as

$$
F = \begin{pmatrix}
y_{1,1} & x_{1,2,1} & x_{1,3,1} & \cdots & x_{1,m,1} \\
0 & y_{2,1} & x_{2,3,1} & \cdots & x_{2,m,1} \\
0 & 0 & y_{3,1} & \cdots & x_{3,m,1} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \cdots & y_{m,1}
\end{pmatrix}
\begin{pmatrix}
y_{1,2} & x_{1,2,2} & x_{1,3,2} & \cdots & x_{1,m,2} \\
0 & y_{2,2} & x_{2,3,2} & \cdots & x_{2,m,2} \\
0 & 0 & y_{3,2} & \cdots & x_{3,m,2} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \cdots & y_{m,2}
\end{pmatrix} \cdots
$$

$$
\cdots \begin{pmatrix}
y_{1,n} & x_{1,2,n} & x_{1,3,n} & \cdots & x_{1,m,n} \\
0 & y_{2,n} & x_{2,3,n} & \cdots & x_{2,m,n} \\
0 & 0 & y_{3,n} & \cdots & x_{3,m,n} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \cdots & y_{m,n}
\end{pmatrix}.
$$

After multiplying these matrices using Lemma 3.1 we obtain

$$
F = \begin{pmatrix}
f_1 & g_{1,2} & g_{1,3} & \cdots & g_{1,m} \\
0 & f_2 & g_{2,3} & \cdots & g_{2,m} \\
0 & 0 & f_3 & \cdots & g_{3,m} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \cdots & f_m
\end{pmatrix},
$$

where

$$
f_i = \prod_{k=1}^n y_{i,k}, \text{ and}
$$

$$
g_{i,j} = \sum_{b=0}^{j-i-1} \sum_{i<l_1<\cdots<l_b<j} \sum_{k_{b+1}=b+1}^n \sum_{k_b=b}^{k_{b+1}-1} \cdots \sum_{k_2=2}^{k_3-1} \sum_{k_1=1}^{k_2-1} \left(\prod_{c_0=1}^{k_1-1} y_{i,c_0} \right) x_{i,l_1,k_1}
$$

$$
\left(\prod_{c_1=k_1+1}^{k_2-1} y_{l_1,c_1} \right) x_{l_1,l_2,k_2} \cdots \left(\prod_{c_b=k_b+1}^{k_{b+1}-1} y_{l_b,c_b} \right) x_{l_b,j,k_{b+1}} \left(\prod_{c_{b+1}=k_{b+1}+1}^n y_{j,c_{b+1}} \right).
$$

The polynomial F can attain the unit matrix for a substitution if and only if f_i attains 1 ($1 \leq i \leq m$) and $g_{i,j}$ attains 0 for the same substitution ($1 \leq i < j \leq m$). Thus $F = I$ is solvable over $\mathbf{SP}(m, \mathbb{F}_q)$ if and only if the system of equations

$$\begin{aligned} f_i|_{\mathbb{F}_q, \mathbf{s}_1, \ldots, \mathbf{s}_m} &= 1 & (1 \leq i \leq j) \\ g_{i,j}|_{\mathbb{F}_q, \mathbf{s}_1, \ldots, \mathbf{s}_m} &= 0 & (1 \leq i < j \leq m) \end{aligned}$$

is solvable over $\mathbb{F}_q$. This is a system of equations over $\mathbb{F}_q$ where the polynomials are given as sums of monomials. Hence we can decide the solvability of this system of equations in polynomial time by Theorem 2.1.

The rewriting of F over $\mathbf{SP}(m, \mathbb{F}_q)$ into the system of equations

$$\begin{aligned} f_i|_{\mathbb{F}_q, \mathbf{s}_1, \ldots, \mathbf{s}_m} &= 1 & (1 \leq i \leq j) \\ g_{i,j}|_{\mathbb{F}_q, \mathbf{s}_1, \ldots, \mathbf{s}_m} &= 0 & (1 \leq i < j \leq m) \end{aligned}$$

over $\mathbb{F}_q$ can be done in $O(n^m)$ time by Lemma 3.1, and the length of each equation is $O(n^m)$. The number of equations is $\frac{m \cdot (m+1)}{2} = O(m^2)$, which does not depend on n, only on the group $\mathbf{SP}(m, \mathbb{F}_q)$. By Theorem 2.1 one can decide whether this system has a solution in $O\left(n^{m^3 \cdot q}\right)$ time.

4. The complexity of equation solvability problem over nilpotent matrix rings

Let $\mathcal{M}$ be a ring of $m \times m$ matrices over $\mathbb{Z}_{p^\alpha}$ where every entry on or below the main diagonal of each matrix in $\mathcal{M}$ is a multiple of p. Let F be a polynomial over $\mathcal{M}$ given as a sum of monomials. Let $T_1 \ldots T_n$ denote a monomial in the sum. Let

$$T_k = \begin{pmatrix} a_{1,1,k} \cdot p & s_{1,2,k} & s_{1,3,k} & \cdots & s_{1,m,k} \\ a_{2,1,k} \cdot p & a_{2,2,k} \cdot p & s_{2,3,k} & \cdots & s_{2,m,k} \\ a_{3,1,k} \cdot p & a_{3,2,k} \cdot p & a_{3,3,k} \cdot p & \cdots & s_{3,m,k} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{m,1,k} \cdot p & a_{m,2,k} \cdot p & a_{m,3,k} \cdot p & \cdots & a_{m,m,k} \cdot p \end{pmatrix}.$$

If $T_k \in \mathcal{M}$ indicates constant then $a_{i,j,k}, s_{i,j,k}$ are constants in $\mathbb{Z}_{p^\alpha}$. If $T_k \in \mathcal{M}$ is a variable, then $a_{i,j,k}, s_{i,j,k}$ are variables, that we can substitute from $\mathbb{Z}_{p^\alpha}$. Furthermore, $T_k = T_l$ if and only if $a_{i,j,k} \cdot p = a_{i,j,l} \cdot p$ and $s_{i,j,k} = s_{i,j,l}$ for every $i, j \in \{1, \ldots, m\}$.

We can rewrite the monomial $T_1 \ldots T_n$ with this notation as

$$T_1 \ldots T_n = \begin{pmatrix} a_{1,1,1} \cdot p & s_{1,2,1} & s_{1,3,1} & \cdots & s_{1,m,1} \\ a_{2,1,1} \cdot p & a_{2,2,1} \cdot p & s_{2,3,1} & \cdots & s_{2,m,1} \\ a_{3,1,1} \cdot p & a_{3,2,1} \cdot p & a_{3,3,1} \cdot p & \cdots & s_{3,m,1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{m,1,1} \cdot p & a_{m,2,1} \cdot p & a_{m,3,1} \cdot p & \cdots & a_{m,m,1} \cdot p \end{pmatrix} \cdots$$

$$\cdots \begin{pmatrix} a_{1,1,n} \cdot p & s_{1,2,n} & s_{1,3,n} & \cdots & s_{1,m,n} \\ a_{2,1,n} \cdot p & a_{2,2,n} \cdot p & s_{2,3,n} & \cdots & s_{2,m,n} \\ a_{3,1,n} \cdot p & a_{3,2,n} \cdot p & a_{3,3,n} \cdot p & \cdots & s_{3,m,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{m,1,n} \cdot p & a_{m,2,n} \cdot p & a_{m,3,n} \cdot p & \cdots & a_{m,m,n} \cdot p \end{pmatrix}.$$

After multiplying these matrices we obtain

$$T_1 \ldots T_n = \begin{pmatrix} g_{1,1} & g_{1,2} & g_{1,3} & \cdots & g_{1,m} \\ g_{2,1} & g_{2,2} & g_{2,3} & \cdots & g_{2,m} \\ g_{3,1} & g_{3,2} & g_{3,3} & \cdots & g_{3,m} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ g_{m,1} & g_{m,2} & g_{m,3} & \cdots & g_{m,m} \end{pmatrix}.$$

We could compute the expressions for every $g_{i,j}$, similarly as in Lemma 3.1. However, we do not need to know the actual formulas, we only need to understand how they look like.

First $g_{i,j}$ is a polynomial given as a sum of monomials over $\mathbb{Z}_{p^\alpha}$. In every such monomial we multiply one term from each matrix T_k $(1 \le k \le n)$. Hence the length of every monomial is n. There are at most m^{n-1} monomials in every polynomial $g_{i,j}$ according to the usual multiplication of matrices. However, every nonzero monomial contains at most $\alpha - 1$ terms from on or below the main diagonal, since the characteristic of $\mathbb{Z}_{p^\alpha}$ is p^α. Therefore every nonzero monomial is of the form

$$\underbrace{s_{i,i_1,1} \cdot s_{i_i,i_2,2} \cdots s_{i_{k_1-1},i_{k_1},k_1}}_{k_1\text{- many terms}} \cdot a_{i_{k_1},l_1,k_1+1} \cdot p \cdot \underbrace{s_{l_1,\bar{i}_1,k_1+2} \cdot s_{\bar{i}_1,\bar{i}_2,.} \cdots s_{\bar{i}_{k_2-1},\bar{i}_{k_2},.}}_{k_2\text{- many terms}}$$

$$\cdot a_{\bar{i}_{k_2},l_2,.} \cdot p \cdots a_{\hat{i}_{k_{b-1}},l_{b-1},.} \cdot p \cdot \underbrace{s_{l_{b-1},\tilde{i}_1,.} \cdots s_{\tilde{i}_{k_b-1},\tilde{i}_{k_b},n}}_{k_b\text{- many terms}}$$

where $1 \le b \le \alpha$ and $0 \le k_1, k_2, \ldots k_b$. Notice that $k_1, k_2, \ldots k_b \le m - 1$ holds as well. Indeed, every term $s_{i,j,k}$ is from above the main diagonal, hence $i < j$. Therefore $1 < i_1 < i_2 < \cdots < i_{k_1} \le m$ and thus $k_1 \le m - 1$. Similarly $k_2, \ldots, k_b \le m - 1$. Hence the length of every nonzero monomial is at most $(m - 1) \cdot \alpha + \alpha - 1 = m\alpha - 1$. In particular, if $m\alpha - 1 < n$ then every monomial in $g_{i,j}$ equals 0. Therefore there are at most $m^{m\alpha-2}$ monomials in every polynomial $g_{i,j}$ and thus $||g_{i,j}|| \le (m\alpha - 1) \cdot m^{m\alpha-2} \le \alpha \cdot m^{m\alpha-1}$.

The input polynomial F is a sum of at most $||F||$ monomials $T_1 \ldots T_n$. Let

$$F = \begin{pmatrix} f_{1,1} & f_{1,2} & f_{1,3} & \cdots & f_{1,m} \\ f_{2,1} & f_{2,2} & f_{2,3} & \cdots & f_{2,m} \\ f_{3,1} & f_{3,2} & f_{3,3} & \cdots & f_{3,m} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ f_{m,1} & f_{m,2} & f_{m,3} & \cdots & f_{m,m} \end{pmatrix}.$$

Then $f_{i,j}$ is the sum of at most $||F||$-many polynomials $g_{i,j}$ for every $i, j \in \{1, \ldots m\}$. Thus $||f_{i,j}|| \leq ||F|| \cdot \alpha m^{m\alpha - 1} = O(||F||)$, as α and m depend only on the ring $\mathcal{R}$.

The polynomial F can attain the zero matrix for a substitution if and only if $f_{i,j}$ attains zero for the same substitution for every $i, j \in \{1, \ldots, m\}$. Thus $F = 0$ is solvable over $\mathcal{M}$ if and only if the system of equations

$$f_{i,j} = 0 \qquad\qquad i, j \in \{1, \ldots, m\}$$

is solvable over $\mathbb{Z}_{p^\alpha}$. This is a system of equations over $\mathbb{Z}_{p^\alpha}$ where the polynomials are given as sums of monomials. Hence we can decide the solvability of this system of equations in polynomial time by Theorem 2.2.

The rewriting of F over $\mathcal{M}$ into the system of equations

$$f_{i,j} = 0 \qquad\qquad i, j \in \{1, \ldots, m\}$$

can be done in $O(||F||)$ time, and $||f_{i,j}|| = O(||F||)$. The number of equations is m^2, which does not depend on $||F||$, only on the ring $\mathcal{M}$. By Theorem 2.2 one can decide whether this system has a solution in $O\left(||F||^{\alpha^2 \cdot m^2 \cdot p^{2\alpha^2}}\right)$ time.

Finally, we explain how this result can be applied to determine if an equation $f = 0$ is solvable over an *arbitrary* nilpotent ring $\mathcal{R}$ of characteristic p^α. Let $\mathcal{M}$ be the matrix ring as in Theorem 2.3, and let $\mathcal{R} \cong \mathcal{M}/\mathcal{I}$. Further, let F denote the polynomial in $\mathcal{M}$ corresponding to f. Notice, that p^α was the characteristic of $\mathcal{R}$ in Theorem 2.3, hence $\alpha = O(\log |\mathcal{R}|)$. Furthermore $m = O(\log |\mathcal{R}|)$ and $p^\alpha = O(|\mathcal{R}|)$. Therefore $\alpha^2 \cdot m^2 \cdot p^{2\alpha^2} = O\left(|\mathcal{R}|^{2\log \mathcal{R}} \log^4 |\mathcal{R}|\right)$. Hence, one can decide if $F = 0$ is solvable over $\mathcal{R} \cong \mathcal{M}/\mathcal{I}$ in $O\left(||F||^{|\mathcal{R}|^{2\log \mathcal{R}} \log^4 |\mathcal{R}|}\right)$ time. Thus, one can decide if the equation $f = 0$ is solvable over $\mathcal{R}$ in $O\left(|\mathcal{I}| \cdot ||F||^{|\mathcal{R}|^{2\log \mathcal{R}} \log^4 |\mathcal{R}|}\right)$ time. Now, $|\mathcal{I}| \leq |\mathcal{M}| \leq (p^\alpha)^{m^2} = O\left(|\mathcal{R}|^{\log^2 |\mathcal{R}|}\right)$, which only depends on $\mathcal{R}$. Therefore, if f is given as a *sum of monomials*, then $||F|| = O(||f||)$, and one can decide $f = 0$ over an arbitrary nilpotent ring $\mathcal{R}$ in $O\left(||f||^{|\mathcal{R}|^{2\log \mathcal{R}} \log^4 |\mathcal{R}|}\right)$ time, as well. If, however, f is an arbitrary polynomial over $\mathcal{R}$, then after rewriting it as a sum of monomials we have $||F|| = O\left(||f||^{\log |\mathcal{R}|}\right)$, giving an extra

$\log |\mathcal{R}|$ factor in the exponent. Thus, one can decide $f = 0$ over an arbitrary nilpotent ring $\mathcal{R}$ in $O\left(||f||^{|\mathcal{R}|^{2\log\mathcal{R}}\log^5|\mathcal{R}|}\right)$ time.

References

[1] Stanley Burris and John Lawerence. The equivalence problem for finite rings. *Journal of Symbolic Computation*, 15:67–71, 1993.

[2] Stanley Burris and John Lawrence. Results on the equivalence problem for finite groups. *Algebra Universalis*, 52(4):495–500, 2005.

[3] Persi Diaconis and I.M. Isaacs. Counting characters of upper triangular groups. *Trans. Amer. Math. Soc.*, 360:2359–2392, 2008.

[4] Mikael Goldmann and Alexander Russell. The complexity of solving equations over finite groups. In *Proceedings of the 14th Annual IEEE Conference on Computational Complexity*, pages 80–86, Atlanta, Georgia, 1999.

[5] Mikael Goldmann and Alexander Russell. The complexity of solving equations over finite groups. *Information and Computation*, 178:253–262, 2002.

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

[7] Gábor Horváth. The complexity of the equivalence problem over finite rings. *Glasgow Mathematical Journal*, 54(1):193–199, 2012.

[8] Gábor Horváth. The complexity of the equivalence end equation solvability problems over meta-abelian groups. *Journal of Algebra*, 433:208–230, 2015.

[9] Gábor Horváth, John Lawerence, and Ross Willard. The equation solvability problem over finite rings. 2016. manuscript.

[10] Gábor Horváth, John Lawrence, László Mérai, and Csaba Szabó. The complexity of the equivalence problem for non-solvable groups. *Bulletin of the London Mathematical Society*, 39(3):433–438, 2007.

[11] Gábor Horváth and Csaba Szabó. The complexity of checking identities over finite groups. *International Journal of Algebra Computation*, 16(5):931–940, 2006.

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

[13] I.M. Isaacs. Counting characters of upper triangular groups. *Journal of Algebra*, 315(2):698–719, 2007.

[14] Gyula Károlyi and Csaba Szabó. The complexity of the equation solvablity problem over nilpotent rings. 2016. submitted.

[15] John Lawrence and R. Willard. The complexity of solving polynomial equations over finite rings. 1997. manuscript.

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

[17] Robert S. Wilson. On the stucture of finite rings. *Compositio Mathematica*, 26(1):79–93, 1973.

University of Debrecen, Institute of Mathematics, Pf. 400, Debrecen, 4002, Hungary

E-mail address: foldvari.attila@science.unideb.hu