THE COMPLEXITY OF THE EQUATION SOLVABILITY PROBLEM OVER NILPOTENT GROUPS

ATTILA FÖLDVÁRI

Abstract. Let $\mathbf{G}$ be a finite, nilpotent group. The computational complexity of the equation solvability problem over $\mathbf{G}$ is known to be in P. The complexity is understood in the length of the equation over $\mathbf{G}$. So far the fastest algorithm to decide whether or not an equation of length n has a solution over $\mathbf{G}$ was running in $O\left(n^{|\mathbf{G}|^{|\mathbf{G}|^{\cdots^{|\mathbf{G}|^{|\mathbf{G}|}}}}}\right)$ time. Here the height of the tower is the nilpotency class of $\mathbf{G}$. We prove that one can decide in $O\left(n^{\frac{1}{2}|\mathbf{G}|^2\log|\mathbf{G}|}\right)$ time whether an equation of length n has a solution over $\mathbf{G}$. The key ingredient of the proof is to represent group expressions using the polycyclic presentation of p-groups.

1. Introduction

One of the earliest problems of algebra is the equation solvability problem. This question asks whether or not an equation over a finite algebraic structure has a solution. Typical examples are finding a root of a polynomial over a field, or solving a congruence over the residue class ring $\mathbb{Z}_m$. Recently, many such classical problems arise in a new perspective, namely to consider their computational complexity.

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 from $\mathbf{G}$. In other words, for group expressions S, T one needs to find whether or not the equation $S = T$ has a solution over $\mathbf{G}$. Since $\mathbf{G}$ is finite, this problem is decidable by checking all possible substitutions from $\mathbf{G}$. In this paper we investigate the computational complexity of the equation solvability problem where $\mathbf{G}$ is a finite nilpotent group.

Date: October 5, 2017.

2010 *Mathematics Subject Classification.* 20F10, 20F18, 13P15.

Key words and phrases. nilpotent groups, equation solvability, equivalence, computational complexity, polynomial time algorithm.

The research was supported by the National Research, Development and Innovation Fund of Hungary, financed under the K109185 and FK 124814 funding schemes.

Goldmann and Russel [1, 2] proved that if $\mathbf{G}$ is not solvable, then the equation solvability problem is NP-complete, while if $\mathbf{G}$ is nilpotent then the equation solvability problem over $\mathbf{G}$ is in P. Here, the computational complexity is understood in the length of the two input group expressions. In their papers, Goldmann and Russell [1, 2] reduce the equation solvability problem over a finite nilpotent group $\mathbf{G}$ to recognizing languages by non-uniform finite automata over $\mathbf{G}$. In their reduction they apply the results of Péladeau and Thérien [10, 11] in a fundamental manner. This way, it is easy to get lost in the chain of thoughts if one wants to recover how the algorithm of Goldmann and Russel manipulates the input group expressions S and T in order to determine whether or not the equation $S = T$ has a solution over $\mathbf{G}$. Furthermore, the algorithm is known to be polynomial in the sizes of S and T, but the degree of this polynomial is not explicitly stated. The reduction in [1, 2] applies Ramsey's theorem, suggesting that the degree of the polynomial is multiply exponential.

Later Horváth [4] gave a straight proof for nilpotent groups only using group expressions and directly arriving at the Ramsey argument. Horváth proves that for a finite nilpotent group $\mathbf{G}$ the image of any group expression can be computed by substitutions where at most $|\mathbf{G}|^{|\mathbf{G}|^{\cdots^{|\mathbf{G}|^{|\mathbf{G}|}}}}$-many variables differ from the identity element. Here, the height of the tower is the nilpotency class of $\mathbf{G}$. This yields to an $O\left(n^{|\mathbf{G}|^{|\mathbf{G}|^{\cdots^{|\mathbf{G}|^{|\mathbf{G}|}}}}}\right)$ time algorithm for checking equations of length n. Horváth explicitly asks in [4, Problem 3] whether the exponent of the time complexity can be bounded by a polynomial in the size of the group $\mathbf{G}$.

In this paper we answer Horváth's question [4, Problem 3] by decreasing the exponent of the time complexity significantly. With the polycyclic presentation of p-groups we give a completely new approach to representing group expressions. We prove that for a p-group of order p^α, and for a group expression T over $\mathbf{P}$ of length n, the image of T can be computed in $O\left(n^{\frac{1}{2}(2p-2)^\alpha \alpha}\right)$ time (see Lemma 4 for details). Let log denote the base 2 logarithm. An immediate consequence for a nilpotent group $\mathbf{G}$ is that equation solvability over $\mathbf{G}$ can be decided in polynomial time, where the degree of the polynomial is $\frac{1}{2}|\mathbf{G}|^2 \log|\mathbf{G}|$:

Theorem 1. *Let $\mathbf{G}$ be a nilpotent group, S, T be group expressions over $\mathbf{G}$ with length at most n. Then it can be decided in $O\left(n^{\frac{1}{2}|\mathbf{G}|^2 \log|\mathbf{G}|}\right)$ time whether or not the equation $S = T$ has a solution in $\mathbf{G}$.*

Not much is known for solvable, non-nilpotent groups. Horváth and Szabó proved that the equation solvability problem over $\mathbf{G}$ is decidable in polynomial time if $|\mathbf{G}| = pq$ for primes $p \neq q$ [7], or if $\mathbf{G}$ is the alternating group acting on four points [8]. Later, Horváth [6] proved

that the equation solvability problem over $\mathbf{G}$ is decidable in polynomial time for 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.

In Section 2 we give the necessary definitions and preliminary results. In Section 2.3 we introduce the notion of a basis of a p-group $\mathbf{P}$ and for a basis $\mathcal{B}$ we introduce the $\mathcal{B}$-form of an arbitrary element of $\mathbf{P}$. Then in Lemma 3 we characterize the exponents of the $\mathcal{B}$-form of a product in $\mathbf{P}$ using polynomials over the p-element field $\mathbb{Z}_p$. With the help of this characterization in Lemma 4 we reduce finding the image of a group expression over $\mathbf{P}$ to deciding whether a system of equations (see system (19)) is solvable over the p-element field $\mathbb{Z}_p$. This reduction and the proof of Theorem 1 can be found in Section 3.

2. Preliminaries

2.1. **Polynomials.** In the paper $\mathbb{Z}_p$ denotes the p-element field with base set $\{0, 1, \ldots, p-1\}$. To avoid confusion with other operations, the modulo p addition is denoted by $\oplus$ and the modulo p multiplication is denoted by $\odot$, while $+$ and $\cdot$ denote the usual addition and multiplication between integers. Our leading reference on polynomials over $\mathbb{Z}_p$ is [9]. We say that a polynomial $f \in \mathbb{Z}_p[x_1; \ldots; x_n]$ is in *reduced* form (or is a *reduced polynomial*) if f is presented as a sum of monomials, where each variable in every monomial is raised to a power of at most $p-1$. Namely, if

$$f(x_1; \ldots; x_n) = \bigoplus_{0 \le s_1, \ldots, s_n \le p-1} c_{s_1,\ldots,s_n} \odot x_1^{s_1} \odot \cdots \odot x_n^{s_n}$$

for some $c_{s_1,\ldots,s_n} \in \mathbb{Z}_p$ ($0 \le s_k \le p-1$, $1 \le k \le n$). For convenience, in polynomials we separate the variables by semicolons instead of the usual colons. Furthermore, recall that for an arbitrary n-ary function $f\colon \mathbb{Z}_p^n \to \mathbb{Z}_p$ there exists a reduced polynomial in $\mathbb{Z}_p[x_1; \ldots; x_n]$ representing f.

The degree of the monomial $c \odot x_1^{s_1} \odot \cdots \odot x_n^{s_n}$ is $s_1 + \cdots + s_n$. The length of a monomial is the number of variables and elements of $\mathbb{Z}_p$ occurring in the monomial with multiplicity. For example, the length of the monomial $c \odot x_1^{s_1} \odot \cdots \odot x_n^{s_n}$ is $1 + s_1 + \cdots + s_n$. The length of a reduced polynomial f is the sum of the lengths of the monomials occurring in f (with multiplicity), and is denoted by $\|f\|$. For example, the length of $2 \odot x_1 \odot x_2^2 \oplus 3 \odot x_1^3 \odot x_2^4 \in \mathbb{Z}_5[x_1; x_2]$ is $(1+1+2)+(1+3+4) = 12$. Finally, the following result is going to play a key role in the proof of our Lemma 4 [5].

Lemma 2 ([5, Corollary 4])**.** *Let $F \in \mathbb{Z}_p[x_1; \ldots; x_n]$ be a polynomial presented as a sum of monomials. Then it can be decided in $O(\|F\|)$ time whether or not F attains 0 for* every *substitution from $\mathbb{Z}_p$.*

2.2. **Group expressions.** Let $\mathbf{G}$ be a finite group. For a variable x and a positive integer k, let x^k denote the k-fold formal product $xx\dots x$. A group expression over $\mathbf{G}$ is a formal product of variables, and elements from $\mathbf{G}$. Note, that we do not use inverses of variables in group expressions, but rather substitute every occurrence of x^{-1} by the formal product $x^{|\mathbf{G}|-1}$. Let $T = y_1 \dots y_n$ be a group expression over $\mathbf{G}$, that is each y_k $(1 \le k \le n)$ is either a variable or an element of $\mathbf{G}$. The length of the group expression T is denoted by $\|T\|$ and is defined as $\|T\| = n$. Finally, the commutator of $a, b \in G$ is defined as $[a,b] = aba^{|\mathbf{G}|-1}b^{|\mathbf{G}|-1}$, and therefore we have $ab = aba^{|\mathbf{G}|-1}b^{|\mathbf{G}|-1}ba = [a,b]\,ba$.

2.3. p**-groups.** For a prime p let $\mathbf{P}$ be a p-group of order p^α. Let us fix a chief series of $\mathbf{P}$: $\{1\} = \mathbf{N}_0 \lhd \mathbf{N}_1 \lhd \dots \lhd \mathbf{N}_\alpha = \mathbf{P}$. Then $\mathbf{N}_i/\mathbf{N}_{i-1}$ is isomorphic to the cyclic group of order p $(1 \le i \le \alpha)$. For every $1 \le i \le \alpha$ let $b_i \in \mathbf{N}_i \setminus \mathbf{N}_{i-1}$ be arbitrary. Then, $b_i\mathbf{N}_{i-1}$ is a generator of $\mathbf{N}_i/\mathbf{N}_{i-1}$. We call the sequence $\mathcal{B} = (b_1, \dots, b_\alpha)$ a *basis* of $\mathbf{P}$. Let $g \in \mathbf{P}$ be arbitrary. Then there exist unique $u_1, \dots, u_\alpha \in \{0, 1, \dots, p-1\}$ such that

$$g = b_1^{u_1} b_2^{u_2} \dots b_\alpha^{u_\alpha}. \tag{1}$$

For a basis $\mathcal{B}$ we call (1) the *$\mathcal{B}$-form of the element g*.

The following lemma shows how the $\mathcal{B}$-form of the product of n elements can be calculated from the $\mathcal{B}$-forms of the elements with the help of some reduced polynomials over $\mathbb{Z}_p$.

Lemma 3. *Let $\mathbf{P}$ be a p-group of order p^α, let $\mathcal{B} = (b_1, \dots, b_\alpha)$ be a basis of $\mathbf{P}$. For an arbitrary positive integer n let*

$$X_{n,\alpha} = \{ x_{k,i} \mid 1 \le k \le n, 1 \le i \le \alpha \}.$$

Then there exist reduced polynomials $f_1, \dots, f_\alpha \in \mathbb{Z}_p[X_{n,\alpha}]$ such that for arbitrary $g_1, \dots, g_n \in \mathbf{P}$ with $\mathcal{B}$-forms

$$g_k = b_1^{u_{k,1}} \dots b_\alpha^{u_{k,\alpha}} \qquad (1 \le k \le n),$$

the $\mathcal{B}$-form of the product $g_1 \dots g_n$ is

$$g_1 \dots g_n = b_1^{f_1(u_{1,1};\dots;u_{n,\alpha})} \dots b_\alpha^{f_\alpha(u_{1,1};\dots;u_{n,\alpha})}. \tag{2}$$

Furthermore, with $C_\alpha = (2p-2)^{\alpha-1}$, each monomial of f_l $(1 \le l \le \alpha)$ has degree at most C_α, each polynomial f_l $(1 \le l \le \alpha)$ can be computed in $O\left(n^{C_\alpha}\right)$ time, and $\|f_l\| = O\left(n^{C_\alpha}\right)$ $(1 \le l \le \alpha)$.

Proof. We prove Lemma 3 by induction on α. If $\alpha = 1$, then $\mathbf{P}$ is a cyclic group of order p. Thus $\mathcal{B} = (b_1)$ for some $b_1 \in \mathbf{P}$, and b_1 generates $\mathbf{P}$. Let $g_1, \dots, g_n \in \mathbf{P}$ be arbitrary, and let their $\mathcal{B}$-forms be $g_k = b_1^{u_{k,1}}$ $(1 \le k \le n)$. Let $f_1(x_1, \dots, x_n) = x_1 \oplus \dots \oplus x_n$. Then every monomial of f_1 has degree at most 1. Furthermore, the length of f_1 is $\|f_1\| = O(n)$, and f_1 is computable in $O(n)$ time. Finally,

$g_1 \dots g_n = b_1^{f_1(u_{1,1};\dots;u_{n,1})}$. Therefore, f_1 satisfies the requirements of Lemma 3 with $C_1 = 1$.

Assume now that for some $\alpha \geq 1$ Lemma 3 holds for p-groups of order p^α, and let $\mathbf{P}$ be a p-group of order $p^{\alpha+1}$. Fix a chief series of $\mathbf{P}$: $\{1\} = \mathbf{N}_0 \lhd \mathbf{N}_1 \lhd \dots \lhd \mathbf{N}_\alpha \lhd \mathbf{N}_{\alpha+1} = \mathbf{P}$. Let $\mathcal{B} = (b_1, \dots, b_\alpha, b_{\alpha+1})$ be a basis of $\mathbf{P}$. Let $g_1, \dots, g_n \in \mathbf{P}$ be arbitrary, let their $\mathcal{B}$-forms be

$$g_k = b_1^{u_{k,1}} \dots b_\alpha^{u_{k,\alpha}} b_{\alpha+1}^{u_{k,\alpha+1}} \qquad (1 \leq k \leq n).$$

We are going to compute the $\mathcal{B}$-form of the product

$$g_1 \dots g_n = b_1^{u_{1,1}} \dots b_\alpha^{u_{1,\alpha}} b_{\alpha+1}^{u_{1,\alpha+1}} \dots b_1^{u_{n,1}} \dots b_\alpha^{u_{n,\alpha}} b_{\alpha+1}^{u_{n,\alpha+1}}. \tag{3}$$

The calculation of this $\mathcal{B}$-form is technical, hence we first sketch the main steps, and then explain all the details.

(a) By applying $xy = [x,y]\,yx$ we collect the factors $b_{\alpha+1}^{u_{k,\alpha+1}}$ $(1 \leq k \leq n)$ next to each other to the right of the product (3) in the following way. First, we move $b_{\alpha+1}^{u_{1,\alpha+1}}$ to the right step-by-step by exchanging with the factors $b_i^{u_{2,i}}$ $(1 \leq i \leq \alpha)$, until it arrives at next to $b_{\alpha+1}^{u_{2,\alpha+1}}$. Every exchange introduces a commutator expression $\left[b_{\alpha+1}^{u_{1,\alpha+1}}, b_i^{u_{2,i}}\right]$. Now, $b_{\alpha+1}^{u_{1,\alpha+1}}$ and $b_{\alpha+1}^{u_{2,\alpha+1}}$ are next to each other in the product. There exists a carry-on polynomial $\chi \in \mathbb{Z}_p[x,y]$ for the addition in base p:

$$\chi(x;y) = \begin{cases} 1, & \text{if } x+y \geq p, \\ 0, & \text{otherwise.} \end{cases} \tag{4}$$

Since $b_{\alpha+1}^{u_{1,\alpha+1}}$ and $b_{\alpha+1}^{u_{2,\alpha+1}}$ are next to each other in the product, we can multiply them as

$$b_{\alpha+1}^{u_{1,\alpha+1}} b_{\alpha+1}^{u_{2,\alpha+1}} = b_{\alpha+1}^{u_{1,\alpha+1}+u_{2,\alpha+1}} = \left(b_{\alpha+1}^{p}\right)^{\chi(u_{1,\alpha+1};u_{2,\alpha+1})} b_{\alpha+1}^{u_{1,\alpha+1} \oplus u_{2,\alpha+1}}. \tag{5}$$

Then, in a similar fashion, we move the factor $b_{\alpha+1}^{u_{1,\alpha+1}\oplus u_{2,\alpha+1}}$ to the right, etc. In general, at the kth step $(1 \leq k \leq n-1)$ we move $b_{\alpha+1}^{u_{1,\alpha+1}\oplus\dots\oplus u_{k,\alpha+1}}$ to the right step-by-step by exchanging with the factors $b_i^{u_{k+1,i}}$ $(1 \leq i \leq \alpha)$, until it arrives at next to $b_{\alpha+1}^{u_{k+1,\alpha+1}}$. Then, as in (5), we multiply $b_{\alpha+1}^{u_{1,\alpha+1}\oplus\dots\oplus u_{k,\alpha+1}}$ and $b_{\alpha+1}^{u_{k+1,\alpha+1}}$ to obtain

$$\begin{aligned} b_{\alpha+1}^{u_{1,\alpha+1}\oplus\dots\oplus u_{k,\alpha+1}} b_{\alpha+1}^{u_{k+1,\alpha+1}} &= b_{\alpha+1}^{\left(u_{1,\alpha+1}\oplus\dots\oplus u_{k,\alpha+1}\right)+u_{k+1,\alpha+1}} \\ &= \left(b_{\alpha+1}^{p}\right)^{\chi\left(u_{1,\alpha+1}\oplus\dots\oplus u_{k,\alpha+1};u_{k+1,\alpha+1}\right)} b_{\alpha+1}^{u_{1,\alpha+1}\oplus\dots\oplus u_{k,\alpha+1}\oplus u_{k+1,\alpha+1}}. \end{aligned} \tag{6}$$

We finish when we collect all factors $b_{\alpha+1}^{u_{k,\alpha+1}}$ $(1 \leq k \leq n)$ to the right into the factor $b_{\alpha+1}^{u_{1,\alpha+1}\oplus\dots\oplus u_{n,\alpha+1}}$. Let S denote the formal product obtained from (3) by these steps. Then the last factor of S is $b_{\alpha+1}^{u_{1,\alpha+1}\oplus\dots\oplus u_{n,\alpha+1}}$. Let T denote the formal product of all but the last factor of S. That is, $S = T b_{\alpha+1}^{u_{1,\alpha+1}\oplus\dots\oplus u_{n,\alpha+1}}$. Now, the factors of the product T are either

- powers of b_i for some $1 \leq i \leq \alpha$, or
- commutator expressions $\left[b_{\alpha+1}^x, b_i^y\right]$ obtained by applying $b_{\alpha+1}^x b_i^y = \left[b_{\alpha+1}^x, b_i^y\right] b_i^y b_{\alpha+1}^x$, or
- powers of $b_{\alpha+1}^p$ obtained by the multiplications in (6).

That is, all factors of T are elements from the normal subgroup $\mathbf{N}_\alpha$ of order p^α. Now, $\mathcal{B}_\alpha = (b_1, \dots, b_\alpha)$ is a basis of $\mathbf{N}_\alpha$. Thus, we can apply the induction hypothesis for $\mathbf{N}_\alpha$ on the product T. For this some further preparation is required in steps (b) and (c).

(b) We find the $\mathcal{B}$-form of all commutator expressions $\left[b_{\alpha+1}^x, b_i^y\right]$ $(x, y \in \mathbb{Z}_p,\ 1 \leq i \leq \alpha)$ occurring in T. Furthermore, we prove that there exist reduced polynomials $\psi_{i,j}^{(k)} \in \mathbb{Z}_p[x_1; \dots; x_k; y]$ $(1 \leq i, j \leq \alpha, 1 \leq k \leq n)$ such that

$$\left[b_{\alpha+1}^{u_{1,\alpha+1} \oplus \dots \oplus u_{k,\alpha+1}}, b_i^{u_{k+1,i}}\right] = b_1^{\psi_{i,1}^{(k)}\left(u_{1,\alpha+1}; \dots; u_{k,\alpha+1}; u_{k+1,i}\right)} \dots b_\alpha^{\psi_{i,\alpha}^{(k)}\left(u_{1,\alpha+1}; \dots; u_{k,\alpha+1}; u_{k+1,i}\right)}, \tag{7}$$

and the degree of every monomial in $\psi_{i,j}^{(k)}$ is at most $2p-2$, $\psi_{i,j}^{(k)}$ is computable in $O\left(k^{p-1}\right) \leq O\left(n^{p-1}\right)$ time, and $\left\|\psi_{i,j}^{(k)}\right\| = O\left(k^{p-1}\right) \leq O\left(n^{p-1}\right)$.

(c) Similarly, we find the $\mathcal{B}$-form of all $\left(b_{\alpha+1}^p\right)^u$ $(u \in \mathbb{Z}_p)$ occurring in T. Moreover, we prove that there exist reduced polynomials $\chi_i^{(k)} \in \mathbb{Z}_p[x_1; \dots; x_k; y]$ $(1 \leq i \leq \alpha, 1 \leq k \leq n)$ such that

$$\left(b_{\alpha+1}^p\right)^{\chi\left(u_{1,\alpha+1} \oplus \dots \oplus u_{k,\alpha+1}; u_{k+1,\alpha+1}\right)} = b_1^{\chi_1^{(k)}\left(u_{1,\alpha+1}; \dots; u_{k,\alpha+1}; u_{k+1,\alpha+1}\right)} \dots b_\alpha^{\chi_\alpha^{(k)}\left(u_{1,\alpha+1}; \dots; u_{k,\alpha+1}; u_{k+1,\alpha+1}\right)}, \tag{8}$$

and the degree of every monomial in $\chi_i^{(k)}$ is at most $2p-2$, $\chi_i^{(k)}$ is computable in $O\left(k^{p-1}\right) \leq O\left(n^{p-1}\right)$ time, and $\left\|\chi_i^{(k)}\right\| = O\left(k^{p-1}\right) \leq O\left(n^{p-1}\right)$.

(d) Finally, with the help of polynomials $\psi_{i,j}^{(k)}$, $\chi_i^{(k)}$ obtained in steps (b) and (c), we apply the induction hypothesis on T for $\mathbf{N}_\alpha$ of order p^α, and prove Lemma 3 on S for $\mathbf{P}$ of order $p^{\alpha+1}$.

We start with step (a) by moving $b_{\alpha+1}^{u_{k,\alpha+1}}$ $(1 \leq k \leq n)$ to the right in (3). First, by applying $xy = [x, y]\, yx$ with $x = b_{\alpha+1}^{u_{1,\alpha+1}}$ and $y = b_1^{u_{2,1}}$ we move $b_{\alpha+1}^{u_{1,\alpha+1}}$ next to $b_2^{u_{2,2}}$ in the product $g_1 g_2$. That is, $b_{\alpha+1}^{u_{1,\alpha+1}} b_1^{u_{2,1}} = \left[b_{\alpha+1}^{u_{1,\alpha+1}}, b_1^{u_{2,1}}\right] b_1^{u_{2,1}} b_{\alpha+1}^{u_{1,\alpha+1}}$, and thus

$$\begin{aligned} g_1 g_2 &= b_1^{u_{1,1}} \dots b_\alpha^{u_{1,\alpha}} b_{\alpha+1}^{u_{1,\alpha+1}} b_1^{u_{2,1}} b_2^{u_{2,2}} b_3^{u_{2,3}} \dots b_\alpha^{u_{2,\alpha}} b_{\alpha+1}^{u_{2,\alpha+1}} \\ &= b_1^{u_{1,1}} \dots b_\alpha^{u_{1,\alpha}} \left[b_{\alpha+1}^{u_{1,\alpha+1}}, b_1^{u_{2,1}}\right] b_1^{u_{2,1}} b_{\alpha+1}^{u_{1,\alpha+1}} b_2^{u_{2,2}} b_3^{u_{2,3}} \dots b_\alpha^{u_{2,\alpha}} b_{\alpha+1}^{u_{2,\alpha+1}}. \end{aligned}$$

Again, by applying $xy = [x,y]\,yx$ with $x = b_{\alpha+1}^{u_{1,\alpha+1}}$ and $y = b_2^{u_{2,2}}$, we move $b_{\alpha+1}^{u_{1,\alpha+1}}$ next to $b_3^{u_{2,3}}$:

$$g_1g_2 = b_1^{u_{1,1}} \dots b_\alpha^{u_{1,\alpha}} \left[b_{\alpha+1}^{u_{1,\alpha+1}}, b_1^{u_{2,1}}\right] b_1^{u_{2,1}} \left[b_{\alpha+1}^{u_{1,\alpha+1}}, b_2^{u_{2,2}}\right] b_2^{u_{2,2}} b_{\alpha+1}^{u_{1,\alpha+1}} b_3^{u_{2,3}} \\ b_4^{u_{2,4}} \dots b_\alpha^{u_{2,\alpha}} b_{\alpha+1}^{u_{2,\alpha+1}}.$$

Continuing in this fashion, we move $b_{\alpha+1}^{u_{1,\alpha+1}}$ next to $b_{\alpha+1}^{u_{2,\alpha+1}}$:

$$g_1g_2 = b_1^{u_{1,1}} \dots b_\alpha^{u_{1,\alpha}} \left[b_{\alpha+1}^{u_{1,\alpha+1}}, b_1^{u_{2,1}}\right] b_1^{u_{2,1}} \left[b_{\alpha+1}^{u_{1,\alpha+1}}, b_2^{u_{2,2}}\right] b_2^{u_{2,2}} \\ \left[b_{\alpha+1}^{u_{1,\alpha+1}}, b_3^{u_{2,3}}\right] b_3^{u_{2,3}} \dots \left[b_{\alpha+1}^{u_{1,\alpha+1}}, b_\alpha^{u_{2,\alpha}}\right] b_\alpha^{u_{2,\alpha}} b_{\alpha+1}^{u_{1,\alpha+1}} b_{\alpha+1}^{u_{2,\alpha+1}}.$$

This way α new commutator expressions are created: $\left[b_{\alpha+1}^{u_{1,\alpha+1}}, b_i^{u_{2,i}}\right]$ for all $1 \le i \le \alpha$. Now, we multiply $b_{\alpha+1}^{u_{1,\alpha+1}}$ and $b_{\alpha+1}^{u_{2,\alpha+1}}$ to obtain $b_{\alpha+1}^{u_{1,\alpha+1}+u_{2,\alpha+1}}$. However, the exponent $u_{1,\alpha+1} + u_{2,\alpha+1}$ is not necessarily and element of the set $\{0, 1, \dots, p-1\}$. Let $\chi\colon \mathbb{Z}_p^2 \to \mathbb{Z}_p$ be the carry-on function of the modulo p addition defined in (4). Since every function is a polynomial over $\mathbb{Z}_p$, there exists a reduced polynomial from $\mathbb{Z}_p[x;y]$ representing χ. With the help of Bernoulli numbers, one can give an explicit formula for the reduced polynomial χ over $\mathbb{Z}_p$ [3]. We do not need the exact formula for χ, only that χ contains monomials of degree at most $2p-2$. By slightly abusing the notation, we denote by χ not only the carry-on function modulo p, but its representing reduced polynomial, as well. Now,

$$b_{\alpha+1}^{u_{1,\alpha+1}+u_{2,\alpha+1}} = \left(b_{\alpha+1}^p\right)^{\chi(u_{1,\alpha+1};u_{2,\alpha+1})} b_{\alpha+1}^{u_{1,\alpha+1}\oplus u_{2,\alpha+1}},$$

and therefore

$$g_1g_2 = b_1^{u_{1,1}} \dots b_\alpha^{u_{1,\alpha}} \left[b_{\alpha+1}^{u_{1,\alpha+1}}, b_1^{u_{2,1}}\right] b_1^{u_{2,1}} \dots \left[b_{\alpha+1}^{u_{1,\alpha+1}}, b_\alpha^{u_{2,\alpha}}\right] b_\alpha^{u_{2,\alpha}} \\ \left(b_{\alpha+1}^p\right)^{\chi(u_{1,\alpha+1},u_{2,\alpha+1})} b_{\alpha+1}^{u_{1,\alpha+1}\oplus u_{2,\alpha+1}}.$$

Now, we move $b_{\alpha+1}^{u_{1,\alpha+1}\oplus u_{2,\alpha+1}}$ next to $b_2^{u_{3,2}}$ in the product $g_1g_2g_3$:

$$\begin{aligned} g_1g_2g_3 &= b_1^{u_{1,1}} \dots b_\alpha^{u_{1,\alpha}} \left[b_{\alpha+1}^{u_{1,\alpha+1}}, b_1^{u_{2,1}}\right] b_1^{u_{2,1}} \dots \left[b_{\alpha+1}^{u_{1,\alpha+1}}, b_\alpha^{u_{2,\alpha}}\right] b_\alpha^{u_{2,\alpha}} \\ &\quad \left(b_{\alpha+1}^p\right)^{\chi(u_{1,\alpha+1};u_{2,\alpha+1})} b_{\alpha+1}^{u_{1,\alpha+1}\oplus u_{2,\alpha+1}} \quad b_1^{u_{3,1}} b_2^{u_{3,2}} \dots b_\alpha^{u_{3,\alpha}} b_{\alpha+1}^{u_{3,\alpha+1}} \\ &= b_1^{u_{1,1}} \dots b_\alpha^{u_{1,\alpha}} \left[b_{\alpha+1}^{u_{1,\alpha+1}}, b_1^{u_{2,1}}\right] b_1^{u_{2,1}} \dots \left[b_{\alpha+1}^{u_{1,\alpha+1}}, b_\alpha^{u_{2,\alpha}}\right] b_\alpha^{u_{2,\alpha}} \\ &\quad \left(b_{\alpha+1}^p\right)^{\chi(u_{1,\alpha+1};u_{2,\alpha+1})} \left[b_{\alpha+1}^{u_{1,\alpha+1}\oplus u_{2,\alpha+1}}, b_1^{u_{3,1}}\right] b_1^{u_{3,1}} b_{\alpha+1}^{u_{1,\alpha+1}\oplus u_{2,\alpha+1}} b_2^{u_{3,2}} \\ &\quad b_3^{u_{3,3}} \dots b_\alpha^{u_{3,\alpha}} b_{\alpha+1}^{u_{3,\alpha+1}}. \end{aligned}$$

Continuing in this fashion, we move $b_{\alpha+1}^{u_{1,\alpha+1}\oplus u_{2,\alpha+1}}$ next to $b_{\alpha+1}^{u_{3,\alpha+1}}$:

$$g_1g_2g_3 = b_1^{u_{1,1}} \dots b_\alpha^{u_{1,\alpha}} \left[b_{\alpha+1}^{u_{1,\alpha+1}}, b_1^{u_{2,1}}\right] b_1^{u_{2,1}} \dots \left[b_{\alpha+1}^{u_{1,\alpha+1}}, b_\alpha^{u_{2,\alpha}}\right] b_\alpha^{u_{2,\alpha}} \\ \left(b_{\alpha+1}^p\right)^{\chi(u_{1,\alpha+1};u_{2,\alpha+1})} \left[b_{\alpha+1}^{u_{1,\alpha+1}\oplus u_{2,\alpha+1}}, b_1^{u_{3,1}}\right] b_1^{u_{3,1}} \dots \\ \left[b_{\alpha+1}^{u_{1,\alpha+1}\oplus u_{2,\alpha+1}}, b_\alpha^{u_{3,\alpha}}\right] b_\alpha^{u_{3,\alpha}} b_{\alpha+1}^{u_{1,\alpha+1}\oplus u_{2,\alpha+1}} b_{\alpha+1}^{u_{3,\alpha+1}}.$$

Then we multiply $b_{\alpha+1}^{u_{1,\alpha+1}\oplus u_{2,\alpha+1}}$ and $b_{\alpha+1}^{u_{3,\alpha+1}}$ to obtain

$$b_{\alpha+1}^{u_{1,\alpha+1}\oplus u_{2,\alpha+1}} b_{\alpha+1}^{u_{3,\alpha+1}} = \left(b_{\alpha+1}^{p}\right)^{\chi(u_{1,\alpha+1}\oplus u_{2,\alpha+1};u_{3,\alpha+1})} b_{\alpha+1}^{u_{1,\alpha+1}\oplus u_{2,\alpha+1}\oplus u_{3,\alpha+1}},$$

and therefore

$$\begin{aligned} g_1g_2g_3 = {} & b_1^{u_{1,1}} \dots b_\alpha^{u_{1,\alpha}} \left[b_{\alpha+1}^{u_{1,\alpha+1}}, b_1^{u_{2,1}}\right] b_1^{u_{2,1}} \dots \left[b_{\alpha+1}^{u_{1,\alpha+1}}, b_\alpha^{u_{2,\alpha}}\right] b_\alpha^{u_{2,\alpha}} \\ & \left(b_{\alpha+1}^{p}\right)^{\chi(u_{1,\alpha+1};u_{2,\alpha+1})} \left[b_{\alpha+1}^{u_{1,\alpha+1}\oplus u_{2,\alpha+1}}, b_1^{u_{3,1}}\right] b_1^{u_{3,1}} \dots \\ & \left[b_{\alpha+1}^{u_{1,\alpha+1}\oplus u_{2,\alpha+1}}, b_\alpha^{u_{3,\alpha}}\right] b_\alpha^{u_{3,\alpha}} \left(b_{\alpha+1}^{p}\right)^{\chi(u_{1,\alpha+1}\oplus u_{2,\alpha+1};u_{3,\alpha+1})} \\ & b_{\alpha+1}^{u_{1,\alpha+1}\oplus u_{2,\alpha+1}\oplus u_{3,\alpha+1}}. \end{aligned}$$

Again, α new commutator expressions are created: $\left[b_{\alpha+1}^{u_{1,\alpha+1}\oplus u_{2,\alpha+1}}, b_i^{u_{3,i}}\right]$ for all $1 \le i \le \alpha$; and yet another power of $b_{\alpha+1}^{p}$. Now, we move $b_{\alpha+1}^{u_{1,\alpha+1}\oplus u_{2,\alpha+1}\oplus u_{3,\alpha+1}}$ to the right, etc. In general, at the kth step ($1 \le k < n$) we move $b_{\alpha+1}^{u_{1,\alpha+1}\oplus\dots\oplus u_{k,\alpha+1}}$ to the right step-by-step by exchanging it with $b_i^{u_{k+1,i}}$ for all $1 \le i \le \alpha$. These exchanges create α new commutator expressions of the form

$$\left[b_{\alpha+1}^{u_{1,\alpha+1}\oplus\dots\oplus u_{k,\alpha+1}}, b_i^{u_{k+1,i}}\right] \tag{9}$$

for all $1 \le i \le \alpha$. At this point $b_{\alpha+1}^{u_{1,\alpha+1}\oplus\dots\oplus u_{k,\alpha+1}}$ and $b_{\alpha+1}^{u_{\alpha+1,k+1}}$ are next to each other. We multiply $b_{\alpha+1}^{u_{1,\alpha+1}\oplus\dots\oplus u_{k,\alpha+1}}$ and $b_{\alpha+1}^{u_{\alpha+1,k+1}}$ to obtain

$$\begin{aligned} & b_{\alpha+1}^{u_{1,\alpha+1}\oplus\dots\oplus u_{k,\alpha+1}} b_{\alpha+1}^{u_{\alpha+1,k+1}} \\ & \qquad = \left(b_{\alpha+1}^{p}\right)^{\chi(u_{1,\alpha+1}\oplus\dots\oplus u_{k,\alpha+1};u_{k+1,\alpha+1})} b_{\alpha+1}^{u_{1,\alpha+1}\oplus\dots\oplus u_{k,\alpha+1}\oplus u_{k+1,\alpha+1}}. \end{aligned} \tag{10}$$

This way, for all $1 \le k \le n$ we move the factors $b_{\alpha+1}^{u_{k,\alpha+1}}$ to the right and multiply them by (10) to obtain $b_{\alpha+1}^{u_{1,\alpha+1}\oplus\dots\oplus u_{n,\alpha+1}}$ as their product. Let S denote the formal product obtained from (3) by these steps. Then the last factor of S is $b_{\alpha+1}^{u_{1,\alpha+1}\oplus\dots\oplus u_{n,\alpha+1}}$. Let T denote the formal product of all but the last factor of S. That is, $S = T b_{\alpha+1}^{u_{1,\alpha+1}\oplus\dots\oplus u_{n,\alpha+1}}$. Now, the factors of the product T are either

- powers of b_i for some $1 \le i \le \alpha$, or
- commutator expressions $\left[b_{\alpha+1}^{x}, b_i^{y}\right]$ (for some $x, y \in \mathbb{Z}_p$) obtained by applying $xy = [x,y]\,yx$, or
- powers of $b_{\alpha+1}^{p}$ obtained by the multiplications in (10).

That is, all factors of T are elements from the normal subgroup $\mathbf{N}_\alpha$ of order p^α. Furthermore, $(b_1, \dots, b_\alpha)$ is a basis of $\mathbf{N}_\alpha$. Thus, each factor of T has a $\mathcal{B}$-form, where $b_{\alpha+1}$ is raised to power 0.

We continue with step (b) by computing the $\mathcal{B}$-form of the commutator expressions (9). Let $\psi_{i,j}\colon \mathbb{Z}_p^2 \to \mathbb{Z}_p$ ($1 \le i, j \le \alpha$) be functions for which

$$\left[b_{\alpha+1}^{x}, b_i^{y}\right] = b_1^{\psi_{i,1}(x;y)} \dots b_\alpha^{\psi_{i,\alpha}(x;y)}.$$

Since every function is a polynomial over $\mathbb{Z}_p$, there exist reduced polynomials from $\mathbb{Z}_p[x;y]$ representing $\psi_{i,j}$ $(1 \leq i,j \leq \alpha)$. By slightly abusing the notation, we denote these reduced polynomials by $\psi_{i,j}$, as well. The time required constructing these polynomials depends only on the group, and not on n. Furthermore, the degree of each monomial of each $\psi_{i,j}$ is at most $2p-2$, and there exist $c_{s,t} \in \mathbb{Z}_p$ $(0 \leq s,t \leq p-1)$ such that

$$\psi_{i,j}(x;y) = \bigoplus_{0 \leq s,t \leq p-1} c_{s,t} \odot x^s \odot y^t.$$

For each $1 \leq i,j \leq \alpha$ and $1 \leq k < n$, let us replace in $\psi_{i,j}(x;y)$ the variable x by the sum $x_1 \oplus \cdots \oplus x_k$, and expand the resulting polynomial into a sum of monomials. Let $\psi_{i,j}^{(k)} \in \mathbb{Z}_p[x_1;\ldots;x_k;y]$ $(1 \leq i,j \leq \alpha, 1 \leq k < n)$ denote the obtained reduced polynomial. Then the $\mathcal{B}$-form of (9) is

$$\left[b_{\alpha+1}^{u_{1,\alpha+1} \oplus \cdots \oplus u_{k,\alpha+1}}, b_i^{u_{k+1,i}}\right] = b_1^{\psi_{i,1}^{(k)}(u_{1,\alpha+1};\ldots;u_{k,\alpha+1};u_{k+1,i})} \ldots b_\alpha^{\psi_{i,\alpha}^{(k)}(u_{1,\alpha+1};\ldots;u_{k,\alpha+1};u_{k+1,i})}. \tag{11}$$

Furthermore, by the multinomial theorem

$$\psi_{i,j}^{(k)}(x_1;\ldots;x_k;y) = \bigoplus_{\substack{0 \leq s,t \leq p-1 \\ 0 \leq s_1,\ldots,s_k \\ s_1+\cdots+s_k=s}} \frac{s!}{s_1! \ldots s_k!} c_{s,t} \odot x_1^{s_1} \odot \cdots \odot x_k^{s_k} \odot y^t.$$

The number of monomials in $\psi_{i,j}^{(k)}$ is

$$\sum_{s=0}^{p-1} \binom{s+k-1}{s} = \binom{p+k-1}{p-1} = O\left(k^{p-1}\right).$$

Moreover, the degree of each monomial in $\psi_{i,j}^{(k)}$ is at most $2p-2$. Furthermore, $\left\|\psi_{i,j}^{(k)}\right\| \leq O\left(k^{p-1}\right)$, and all $\psi_{i,j}^{(k)}$ $(1 \leq i,j \leq \alpha,\ 1 \leq k < n)$ can be constructed in $O\left(\sum_{k=1}^{n-1} k^{p-1}\right) \leq O\left(n^p\right)$ time.

We continue with step (c) by computing the $\mathcal{B}$-form of the $\left(b_{\alpha+1}^p\right)$-powers in (10). As $b_{\alpha+1}^p \in \mathbf{N}_\alpha$, there exists $c_1,\ldots,c_\alpha \in \mathbb{Z}_p$ such that

$$b_{\alpha+1}^p = b_1^{c_1} \ldots b_\alpha^{c_\alpha}$$

and thus

$$\left(b_{\alpha+1}^p\right)^{\chi(x;y)} = b_1^{c_1 \odot \chi(x;y)} \ldots b_\alpha^{c_\alpha \odot \chi(x;y)}.$$

For each $1 \leq i \leq \alpha$, $1 \leq k < n$ let us replace the variable x by the sum $x_1 \oplus \cdots \oplus x_k$, and expand the resulting polynomial into a sum of monomials. Let $\chi_i^{(k)} \in \mathbb{Z}_p[x_1;\ldots;x_k;y]$ $(1 \leq i \leq \alpha, 1 \leq k < n)$ denote

the obtained reduced polynomial. Then the $\mathcal{B}$-form of the $\left(b_{\alpha+1}^p\right)$-power in (10) is

$$\left(b_{\alpha+1}^p\right)^{\chi(u_{1,\alpha+1}\oplus\dots\oplus u_{k,\alpha+1};u_{k+1,\alpha+1})} = b_1^{\chi_1^{(k)}(u_{1,\alpha+1};\dots;u_{k,\alpha+1};u_{k+1,\alpha+1})}\dots b_\alpha^{\chi_\alpha^{(k)}(u_{1,\alpha+1};\dots;u_{k,\alpha+1};u_{k+1,\alpha+1})}. \tag{12}$$

The degree of each monomial of χ is at most $2p-2$, and there exist $c'_{s,t}\in\mathbb{Z}_p$ $(0\le s,t\le p-1)$ such that

$$\chi(x;y)=\bigoplus_{0\le s,t\le p-1} c'_{s,t}\odot x^s\odot y^t.$$

Hence, by the multinomial theorem

$$\chi_i^{(k)}(x_1;\dots;x_k;y)=\bigoplus_{\substack{0\le s,t\le p-1\\ 0\le s_1,\dots,s_k\\ s_1+\dots+s_k=s}}\frac{s!}{s_1!\dots s_k!}c'_{s,t}\odot x_1^{s_1}\odot\dots\odot x_k^{s_k}\odot y^t.$$

Therefore, the number of monomials in $\chi_i^{(k)}$ is

$$\sum_{s=0}^{p-1}\binom{s+k-1}{s}=\binom{p+k-1}{p-1}=O\left(k^{p-1}\right).$$

Moreover, the degree of each monomial in $\chi_i^{(k)}$ is at most $2p-2$. Furthermore, $\left\|\chi_i^{(k)}\right\|\le O\left(k^{p-1}\right)$, and all $\chi_i^{(k)}$ $(1\le i\le\alpha,\ 1\le k<n)$ can be constructed in $O\left(\sum_{k=1}^{n-1}k^{p-1}\right)\le O\left(n^p\right)$ time.

Now, we are ready to continue with step (d) and apply the induction hypothesis on T. Let us rewrite the $(n-1)\alpha$-many commutator expressions from (9) and the $(n-1)$-many $\left(b_{\alpha+1}^p\right)$-powers from (10) into their $\mathcal{B}$-forms by applying (11) and (12). Furthermore, there are $n\alpha$-many factors of T of the form $b_i^{u_{k,i}}$ $(1\le i\le\alpha,\ 1\le k\le n)$. Let $\tilde{n}$ denote the number of factors of T:

$$\tilde{n}=(n-1)\alpha+n-1+n\alpha=(2\alpha+1)n-\alpha-1=O(n).$$

Since each factor of T is in $\mathbf{N}_\alpha$, for every $1\le\tilde{k}\le\tilde{n}$, $1\le j\le\alpha$ there exists $\tilde{u}_{\tilde{k},j}$ such that the $\mathcal{B}$-form of the $\tilde{k}$th factor of T is $b_1^{\tilde{u}_{\tilde{k},1}}\dots b_\alpha^{\tilde{u}_{\tilde{k},\alpha}}$. Precisely, if the $\tilde{k}$th factor of T is $b_i^{u_{k,i}}$ for some $1\le i\le\alpha$, $1\le k\le n$, then

$$\tilde{u}_{\tilde{k},j}=\begin{cases}u_{k,i}, & \text{if } j=i,\\ 0, & \text{if } j\ne i.\end{cases} \tag{13}$$

If the $\tilde{k}$th factor of T is the commutator expression (9) for some $1\le i\le\alpha$, $1\le k<n$, then

$$\tilde{u}_{\tilde{k},j}=\psi_{i,j}^{(k)}(u_{1,\alpha+1};\dots,u_{k,\alpha+1};u_{k+1,i}). \tag{14}$$

Finally, if the $\tilde{k}$th factor of T is the $\left(b_{\alpha+1}^{p}\right)$-power in (10) for some $1 \leq k < n$, then

$$\tilde{u}_{\tilde{k},j} = \chi_j^{(k)}\left(u_{1,\alpha+1}; \ldots, u_{k,\alpha+1}; u_{k+1,\alpha+1}\right). \tag{15}$$

Let $\tilde{X}_{\tilde{n},\alpha} = \left\{ \tilde{x}_{\tilde{k},i} \;\middle|\; 1 \leq \tilde{k} \leq \tilde{n}, 1 \leq i \leq \alpha \right\}$, $C_\alpha = (2p-2)^{\alpha-1}$. By the induction hypothesis for each $1 \leq l \leq \alpha$ there exists a reduced polynomial $\tilde{f}_l \in \mathbb{Z}_p\left[\tilde{X}_{\tilde{n},\alpha}\right]$ such that each monomial of $\tilde{f}_l$ has degree at most C_α, $\left\|\tilde{f}_l\right\| = O\left(\tilde{n}^{C_\alpha}\right) = O\left(n^{C_\alpha}\right)$, and the $\mathcal{B}$-form of T is

$$T = b_1^{\tilde{f}_1(\tilde{u}_{1,1};\ldots;\tilde{u}_{\tilde{n},\alpha})} \ldots b_\alpha^{\tilde{f}_\alpha(\tilde{u}_{1,1};\ldots;\tilde{u}_{\tilde{n},\alpha})}.$$

Moreover, computing all polynomials $\tilde{f}_l$ takes $O\left(\tilde{n}^{C_\alpha}\right) = O\left(n^{C_\alpha}\right)$ time.

Let $X_{n,\alpha} = \{ x_{k,i} \mid 1 \leq k \leq n, 1 \leq i \leq \alpha+1 \}$. Now, for each $1 \leq l \leq \alpha$ we define f_l from $\tilde{f}_l$ by substituting an appropriate reduced polynomial from $\mathbb{Z}_p[X_{n,\alpha}]$ into each variable $\tilde{x}_{\tilde{k},j}$ (for all $1 \leq \tilde{k} \leq \tilde{n}$, $1 \leq j \leq \alpha$) according to (13), (14), and (15) as follows. Let $1 \leq \tilde{k} \leq \tilde{n}$ be fixed. If the $\tilde{k}$th factor of T is $b_i^{u_{k,i}}$ for some $1 \leq i \leq \alpha$, $1 \leq k \leq n$, then

$$\text{we replace } \tilde{x}_{\tilde{k},j} \text{ by } \begin{cases} x_{k,i}, \text{ if } j = i, \text{ or} \\ 0, \text{ if } j \neq i. \end{cases} \tag{16}$$

If the $\tilde{k}$th factor of T is the commutator expression (9) for some $1 \leq i \leq \alpha$, $1 \leq k < n$, then

$$\text{we replace } \tilde{x}_{\tilde{k},j} \text{ by } \psi_{i,j}^{(k)}\left(x_{1,\alpha+1}; \ldots, x_{k,\alpha+1}; x_{k+1,i}\right). \tag{17}$$

Finally, if the $\tilde{k}$th factor of T is the $\left(b_{\alpha+1}^{p}\right)$-power in (10) for some $1 \leq k < n$, then

$$\text{we replace } \tilde{x}_{\tilde{k},j} \text{ by } \chi_j^{(k)}\left(x_{1,\alpha+1}; \ldots, x_{k,\alpha+1}; x_{k+1,\alpha+1}\right). \tag{18}$$

Let f_l denote the reduced polynomial obtained from $\tilde{f}_l$ after we make the substitutions (16), (17) and (18) and expand the resulting polynomial into a sum of monomials. From (13), (14), and (15) the $\mathcal{B}$-form of T is

$$T = b_1^{f_1(u_{1,1};\ldots;u_{n,\alpha+1})} \ldots b_\alpha^{f_\alpha(u_{1,1};\ldots;u_{n,\alpha+1})}.$$

Let

$$f_{\alpha+1}\left(x_{1,1}; \ldots; x_{n,\alpha+1}\right) = \bigoplus_{k=1}^{n} x_{k,\alpha+1},$$

then the $\mathcal{B}$-form of $g_1 \ldots g_n$ is

$$g_1 \ldots g_n = b_1^{f_1(u_{1,1};\ldots;u_{n,\alpha+1})} \ldots b_\alpha^{f_\alpha(u_{1,1};\ldots;u_{n,\alpha+1})} b_{\alpha+1}^{f_{\alpha+1}(u_{1,1};\ldots;u_{n,\alpha+1})}.$$

Thus, $f_1, \ldots, f_{\alpha+1}$ satisfies (2). Let $C_{\alpha+1} = (2p-2)^{\alpha}$, $C_{\alpha} = (2p-2)^{\alpha-1}$. The degree of each monomial of $\tilde{f}_l$ is at most C_{α} by the induction hypothesis. We obtain f_l by substituting into every variable either another variable in (16), or $\psi_{i,j}^{(k)}$ in (17), or $\chi_i^{(k)}$ in (18). The degree of each monomial of $\psi_{i,j}^{(k)}$ or of $\chi_i^{(k)}$ is at most $(2p-2)$. Thus the degree of each monomial in f_l is at most

$$(2p-2) \cdot C_{\alpha} = (2p-2) \cdot (2p-2)^{\alpha-1} = (2p-2)^{\alpha} = C_{\alpha+1}.$$

Furthermore, $\left\|\psi_{i,j}^{(k)}\right\| = O\left(n^{p-1}\right)$, $\left\|\chi_i^{(k)}\right\| = O\left(n^{p-1}\right)$, thus every monomial of $\tilde{f}_l$ is expanded into at most $O\left(\left(n^{(p-1)}\right)^{C_{\alpha}}\right) = O\left(n^{(p-1)C_{\alpha}}\right)$-many monomials. Therefore,

$$\begin{aligned}\|f_l\| &\leq O\left(n^{(p-1)C_{\alpha}}\right) \cdot \left\|\tilde{f}_l\right\| \leq O\left(n^{(p-1)C_{\alpha}}\right) \cdot O\left(n^{C_{\alpha}}\right) \leq O\left(n^{pC_{\alpha}}\right) \\ &\leq O\left(n^{(2p-2)C_{\alpha}}\right) \leq O\left(n^{C_{\alpha+1}}\right).\end{aligned}$$

□

3. Equation solvability

We prove Theorem 1 in this section. We need the following.

Lemma 4. *Let $\mathbf{P}$ be a finite p-group of order p^{α}, $g \in \mathbf{P}$ be arbitrary, and T be a group expression over $\mathbf{P}$ of length n. Then it can be decided in $O\left(n^{\frac{1}{2}(2p-2)^{\alpha}\alpha}\right)$ time whether or not the equation $T = g$ has a solution over $\mathbf{P}$.*

Proof. Let $\mathbf{P}$ be a p-group of order p^{α}. Let $\mathcal{B} = (b_1, \ldots, b_{\alpha})$ be a basis of $\mathbf{P}$. Let $T = y_1 \ldots y_n$ be a group expression over $\mathbf{P}$, where every y_k $(1 \leq k \leq n)$ is either a variable or an element of $\mathbf{P}$. For every $1 \leq k \leq n$ we replace y_k by its $\mathcal{B}$-form in the following way:

- If y_k is an element of $\mathbf{P}$, then let $x_{k,i}$ $(1 \leq i \leq \alpha)$ be elements of $\mathbb{Z}_p$ such that the $\mathcal{B}$-form of y_k is $y_k = b_1^{x_{k,1}} \ldots b_{\alpha}^{x_{k,\alpha}}$, and replace y_k by its $\mathcal{B}$-form $b_1^{x_{k,1}} \ldots b_{\alpha}^{x_{k,\alpha}}$.
- If y_k is a variable over $\mathbf{P}$ then let $x_{k,i}$ $(1 \leq i \leq \alpha)$ denote a variable over $\mathbb{Z}_p$ such that x_{k_1,i_1} and x_{k_2,i_2} (for some $1 \leq k_1, k_2 \leq n$, $1 \leq i_1, i_2 \leq \alpha$) denote the same variable if and only if y_{k_1} and y_{k_2} denote the same variable over $\mathbf{P}$ and $i_1 = i_2$. Now, every element of $\mathbf{P}$ has a unique $\mathcal{B}$-form. Thus, when the values of the variables $x_{k,1}, \ldots, x_{k,\alpha}$ run through the elements of $\mathbb{Z}_p$, the value of the expression $b_1^{x_{k,1}} \ldots b_{\alpha}^{x_{k,\alpha}}$ runs through the elements of $\mathbf{P}$. Now, replace y_k by the formal product $b_1^{x_{k,1}} \ldots b_{\alpha}^{x_{k,\alpha}}$.

Rewriting T by replacing every y_k by its corresponding $\mathcal{B}$-form takes $O(n)$ time.

We are going to apply Lemma 3 to compute the $\mathcal{B}$-form of the product $y_1 \ldots y_n$. Let $X_{n,\alpha} = \{ x_{k,i} \mid 1 \leq k \leq n, 1 \leq i \leq \alpha \}$, $C_{\alpha} =$

$(2p-2)^{\alpha-1}$. Let us compute the reduced polynomials $f_1, \ldots, f_\alpha \in \mathbb{Z}_p[X_{n,\alpha}]$ from Lemma 3 in $O\left(n^{C_\alpha}\right)$ time. Now, for all $1 \leq l \leq \alpha$ every monomial of f_l has degree at most C_α, $\|f_l\| = O\left(n^{C_\alpha}\right)$, and by Lemma 3

$$y_1 \ldots y_n = b_1^{f_1(x_{1,1};\ldots;x_{n,\alpha})} \ldots b_\alpha^{f_\alpha(x_{1,1};\ldots;x_{n,\alpha})}$$

is the $\mathcal{B}$-form of the product $y_1 \ldots y_n$. Let the $\mathcal{B}$-form of g be $g = b_1^{v_1} \ldots b_\alpha^{v_\alpha}$. Since the $\mathcal{B}$-form is unique, every solution of $y_1 \ldots y_n = g$ over $\mathbf{P}$ corresponds to a solution of the system

$$\begin{aligned} f_1(x_{1,1};\ldots;x_{n,\alpha}) &= v_1, \\ &\vdots \\ f_\alpha(x_{1,1};\ldots;x_{n,\alpha}) &= v_\alpha, \end{aligned} \tag{19}$$

over $\mathbb{Z}_p$. That is, $T = g$ has a solution over $\mathbf{P}$ if and only if the system (19) has a solution over $\mathbb{Z}_p$. Let

$$F(x_{1,1};\ldots;x_{n,\alpha}) = \prod_{l=1}^{\alpha} \left(1 - \left(f_l(x_{1,1};\ldots;x_{n,\alpha}) - v_l\right)^{p-1}\right)$$

expanded as a sum of monomials. Let $u_{k,i} \in \mathbb{Z}_p$ $(1 \leq k \leq n, 1 \leq i \leq \alpha)$ be arbitrary. Then for each $1 \leq l \leq \alpha$ we have

$$1 - \left(f_l(u_{1,1};\ldots;u_{n,\alpha}) - v_l\right)^{p-1} = \begin{cases} 1, & \text{if } f_l(u_{1,1};\ldots;u_{n,\alpha}) = v_l, \\ 0, & \text{otherwise.} \end{cases}$$

Thus, $F(u_{1,1};\ldots;u_{n,\alpha}) = 1$ if and only if $f_l(u_{1,1};\ldots;u_{n,\alpha}) = v_l$ for all $1 \leq l \leq \alpha$, and $F(u_{1,1};\ldots;u_{n,\alpha}) = 0$, otherwise. Therefore, the system (19) is *not* solvable if and only if F attains 0 for every substitution from $\mathbb{Z}_p$. The latter can be decided in $O(\|F\|)$ time by Lemma 2.

The running time of the algorithm to decide whether or not $T = g$ has a solution over $\mathbf{P}$ consists of the following:

- $O(n)$ time to replace every y_k by its $\mathcal{B}$-form,
- $O\left(n^{C_\alpha}\right)$ time to compute the reduced polynomials $f_1, \ldots, f_\alpha$,
- $O(\|F\|)$ time to compute F and decide whether or not F attains 0 for all substitutions from $\mathbb{Z}_p$ by Lemma 2.

Thus, the algorithm has total running time $O\left(n + n^{C_\alpha} + \|F\|\right)$. As F is presented as a sum of monomials,

$$\|F\| \leq \prod_{l=1}^{\alpha} \left(1 + \|f_l - v_l\|^{p-1}\right) \leq 2^\alpha \cdot \max_{1 \leq l \leq \alpha} \|f_l - v_l\|^{(p-1)\alpha}.$$

By Lemma 3, $\|f_l - v_l\| \leq 2\|f_l\| = O\left(n^{C_\alpha}\right)$. Then,

$$\|F\| \leq 2^\alpha \cdot \max_{1 \leq l \leq \alpha} \|f_l - v_l\|^{(p-1)\alpha} = O\left(n^{C_\alpha(p-1)\alpha}\right),$$

since 2^α does not depend on the input group expression T, only on $\mathbf{G}$.

By Lemma 3, $C_\alpha = (2p-2)^{\alpha-1}$, thus the time needed to decide whether or not $T = g$ has a solution over $\mathbf{P}$ is

$$O\left(n + n^{C_\alpha} + \|F\|\right) \leq O\left(n + n^{C_\alpha} + n^{C_\alpha(p-1)\alpha}\right)$$
$$\leq O\left(n^{C_\alpha(p-1)\alpha}\right) \leq O\left(n^{(2p-2)^{\alpha-1}(p-1)\alpha}\right) = O\left(n^{\frac{1}{2}(2p-2)^\alpha\alpha}\right).$$

□

Finally, we prove Theorem 1.

Proof of Theorem 1. Let $S = x_1 \dots x_k$ and $T = y_1 \dots y_n$ be two group expressions over $\mathbf{G}$, such that $k \leq n$. Let $T' = x_k^{|\mathbf{G}|-1} \dots x_1^{|\mathbf{G}|-1} y_1 \dots y_n$. Then $S = T$ has a solution over $\mathbf{G}$ if and only if the group expression T' attains the identity element of $\mathbf{G}$ for some substitution. Now, $\|T'\| \leq |\mathbf{G}| \cdot n = O(n)$, since $|\mathbf{G}|$ does not depend on S and T, hence does not depend on n, either. In the following we consider the equation $T' = \mathrm{id}$.

First, we investigate the case where $\mathbf{G}$ is a p-group of order p^α. By Lemma 4 one can decide in $O\left(n^{\frac{1}{2}(2p-2)^\alpha\alpha}\right)$ time whether or not $T' = \mathrm{id}$ has a solution in $\mathbf{G}$. Here, $|\mathbf{G}| = p^\alpha$, $\alpha \leq \log|\mathbf{G}|$, $2p-2 \leq p^2$, hence

$$\frac{1}{2}(2p-2)^\alpha \alpha \leq \frac{1}{2}p^{2\alpha}\alpha \leq \frac{1}{2}|\mathbf{G}|^2 \log|\mathbf{G}|.$$

Now, let $\mathbf{G}$ be an arbitrary nilpotent group, and its Sylow subgroups be $\mathbf{P}_1, \dots, \mathbf{P}_m$. Then $\mathbf{G}$ is the direct product of its Sylow subgroups. Hence, $T' = \mathrm{id}$ can be solved over $\mathbf{G}$ if and only $T' = \mathrm{id}$ can be solved over $\mathbf{P}_i$ for all $1 \leq i \leq m$. For every $1 \leq i \leq m$ one can decide in $O\left(n^{\frac{1}{2}|\mathbf{P}_i|^2\log|\mathbf{P}_i|}\right) \leq O\left(n^{\frac{1}{2}|\mathbf{G}|^2\log|\mathbf{G}|}\right)$ time whether or not $T' = \mathrm{id}$ is solvable over $\mathbf{P}_i$. For all $\mathbf{P}_i$ it takes $O\left(m \cdot n^{\frac{1}{2}|\mathbf{G}|^2\log|\mathbf{G}|}\right) = O\left(n^{\frac{1}{2}|\mathbf{G}|^2\log|\mathbf{G}|}\right)$ time, since m does not depend on T', only on $\mathbf{G}$. □

References

[1] M. Goldmann and A. 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.

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

[3] G. Grasegger, G. Horváth, and K. A. Kearnes. Polynomial equivalence of finite rings. *J. Aust. Math. Soc.*, 96(2):244–257, 2014.

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

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

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

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

[8] G. Horváth and Cs. Szabó. Equivalence and equation solvability problems for the group A_4. *J. Pure Appl. Algebra*, 216(10):2170–2176, 2012.
[9] B. R. MacDonald. *Finite rings with identity*. M. Dekker, 1974.
[10] P. Péladeau and D. Thérien. Sur les langages reconnus par des groupes nilpotents. *C. R. Acad. Sci. Paris Sér. I Math*, 306(2):93–95, 1988.
[11] D. Thérien. Subword counting and nilpotent groups. In *Combinatorics on words (Waterloo, Ont., 1982)*, pages 297–305. Academic Press, Toronto, Ont., 1983.

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

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