International Journal of Algebra and Computation
Vol. 30, No. 3 (2020) 607–623
© World Scientific Publishing Company
DOI: 10.1142/S0218196720500137

The complexity of the equation solvability and equivalence problems over finite groups

Attila Földvári[*,‡] and Gábor Horváth[†,§]

[*]*Department of Algebra, Charles University, Sokolovska 83*
186 00 Praha 8, Czech Republic

[†]*Institute of Mathematics, University of Debrecen*
Pf. 400, Debrecen, 4002, Hungary
[‡]*foldatti@gmail.com*
[§]*ghorvath@science.unideb.hu*

Received 11 January 2019
Accepted 24 October 2019
Published 4 December 2019

Communicated by M. Volkov

We provide a polynomial time algorithm for deciding the equation solvability problem over finite groups that are semidirect products of a p-group and an Abelian group. As a consequence, we obtain a polynomial time algorithm for deciding the equivalence problem over semidirect products of a finite nilpotent group and a finite Abelian group. The key ingredient of the proof is to represent group expressions using a special polycyclic presentation of these finite solvable groups.

Keywords: Semidirect product of groups; equation solvability; equivalence; computational complexity; polynomial time algorithm.

Mathematics Subject Classification 2020: 20F10, 20F14, 20F16, 13P15

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 $\mathbb{Z}_m$. In the past decades, 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 $\mathbf{G}$. Equation solvability is closely related to the so-called equivalence problem. The *equivalence problem over a finite group* $\mathbf{G}$ asks whether or not two group expressions S, T attain the same value for *each* substitution from $\mathbf{G}$, that is whether S and T determine the same function over $\mathbf{G}$ (denoted by $S \approx T$ over $\mathbf{G}$). Since the group $\mathbf{G}$ is finite, these problems are decidable by checking all possible substitutions from $\mathbf{G}$. We investigate the complexity of these problems over finite groups.

Burris and Lawrence [2] 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. Here, the computational complexity is understood in the length of the two input expressions, where group multiplication is assumed to be performed in unit time. Note, that $\mathbf{G}$ is fixed in advance and is not part of the input. Hence any computation that involves only $\mathbf{G}$ is independent of the input expressions, and therefore takes constant time.

In [2], Burris and Lawrence conjecture that a dichotomy theorem exists. Namely, that the equivalence problem for $\mathbf{G}$ is solvable in polynomial time if $\mathbf{G}$ is solvable, and coNP-complete otherwise. The coNP-complete part of the conjecture was proved in [13]. The polynomial part of the conjecture has been verified in several cases: e.g. for semidirect products $\mathbf{A} \rtimes \mathbf{B}$, where $\mathbf{A}$ and $\mathbf{B}$ are Abelian groups such that the exponent of $\mathbf{A}$ is squarefree and $(|\mathbf{A}|, |\mathbf{B}|) = 1$ [14]. Later [11], this result has been generalized for semidirect products $\mathbf{A} \rtimes \mathbf{B}$, where $\mathbf{A}$ and $\mathbf{B}/C_{\mathbf{B}}(\mathbf{A})$ are both Abelian and the equivalence problem over $\mathbf{B}$ has polynomial time complexity (here $C_{\mathbf{B}}(\mathbf{A})$ denotes the centralizer of $\mathbf{A}$ in $\mathbf{B}$). At that time, the three smallest groups, for which the complexity of the equivalence problem was unknown, were $\mathbf{S}_4$, $\mathbf{SL}(2, \mathbb{Z}_3)$, and the noncommutative semidirect product $\mathbf{U}(3, \mathbb{Z}_3) \rtimes \mathbb{Z}_3^{\times}$ of the 3×3 unitriangular matrices over $\mathbb{Z}_3$ with the two-element group (see [11] for a comprehensive list). Since then, the equivalence problem for the latter group is known to be decidable in polynomial time [3]. However, the complexities of the equivalence problem over the groups $\mathbf{S}_4$ and $\mathbf{SL}(2, \mathbb{Z}_3)$ remained elusive.

Even less is known about the complexity of the equation solvability problem over groups. Goldmann and Russell [6, 7] proved that if $\mathbf{G}$ is nilpotent then the equation solvability problem over $\mathbf{G}$ is in P, while if $\mathbf{G}$ is not solvable, then the equation solvability problem is NP-complete. Since then, the result on nilpotent groups has been reproved using different approaches, first in [10], later in [4]. In particular, in [4] (similarly as in the "Deep Thought" algorithm for torsion-free nilpotent groups, see e.g. [16], which is based on [8, 9] and [19, pp. 441–445]) the polycyclic presentation of p-groups is applied to provide a much faster algorithm than those in [6, 7, 10]. Very little is known for solvable, nonnilpotent groups. In [6, 7], Goldmann and Russell explicitly ask for the complexity of the equation solvability problem for $\mathbf{S}_3$. In [14] it is proved that this problem is in P for groups of order pq for primes p and q. Furthermore, the equation solvability problem is in P for the group $\mathbf{A}_4$, as well [15]. Later, in [11] the ideas of [14, 15] were brought under a unified method, and it was 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 a commutative group satisfying some technical conditions. In [11], six small groups were identified with unknown complexity for equation solvability: $\mathbf{U}(3, \mathbb{Z}_3) \rtimes \mathbb{Z}_3^\times$, $\mathbf{S}_4$, $\mathbf{SL}(2, \mathbb{Z}_3)$, $\mathbf{D}_{12}$, $\mathbf{Z}_3 \rtimes \mathbf{Q}$ and $(\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_3) \rtimes \mathbf{Z}_2$. Again, the case of $\mathbf{U}(3, \mathbb{Z}_3) \rtimes \mathbb{Z}_3^\times$ has been resolved in [3].

In this paper, we investigate the computational complexity of the equation solvability problem over semidirect products of p-groups and Abelian groups, and thus generalize several previous results. Let log denote the base 2 logarithm. Our main result is the following.

Theorem 1. *Let* $\mathbf{G} \simeq \mathbf{P} \rtimes \mathbf{A}$, *where* $\mathbf{P}$ *is a finite* p*-group and* $\mathbf{A}$ *is a finite Abelian group. Let* S, T *be group expressions over* $\mathbf{G}$ *with length at most* n. *Then it can be decided in* $O(n^{|\mathbf{G}|^{|\mathbf{G}|}\log|\mathbf{G}|})$ *time whether or not the equation* $S = T$ *has a solution in* $\mathbf{G}$.

Note, that the condition of Theorem 1 is equivalent to $\mathbf{G}'$ being a p-group (see Lemma 4 in Sec. 2.3). Since the commutator subgroup of $\mathbf{SL}(2, \mathbb{Z}_3)$ coincides with the 2-Sylow subgroup of $\mathbf{SL}(2, \mathbb{Z}_3)$, Theorem 1 yields that the equation solvability problem can be solved in polynomial time for the group $\mathbf{SL}(2, \mathbb{Z}_3)$. In particular, Theorem 1 answers the question [11, Problem 3]. Another consequence of Theorem 1 is a similar result about the equivalence problem.

Theorem 2. *Let* $\mathbf{G} \simeq \mathbf{N} \rtimes \mathbf{A}$, *where* $\mathbf{N}$ *is a finite nilpotent group and* $\mathbf{A}$ *is a finite Abelian group. Let* S, T *be group expressions over* $\mathbf{G}$ *with length at most* n. *Then it can be decided in* $O(n^{|\mathbf{G}|^{|\mathbf{G}|}\log|\mathbf{G}|})$ *time whether or not* $S \approx T$ *over* $\mathbf{G}$.

In Sec. 2, we give the necessary definitions and preliminary results. In particular, in Sec. 2.3, we consider semidirect products, and we show in Lemma 4 that it is enough to prove Theorem 1 in the case where p does not divide the size of $\mathbf{A}$. Then, expanding on the ideas of [4], we introduce the notion of a basis of semidirect products $\mathbf{P} \rtimes \mathbf{A}$, and for a basis $\mathcal{B}$ we introduce the $\mathcal{B}$-form of an arbitrary element of $\mathbf{P} \rtimes \mathbf{A}$. Lemma 6 (generalizing a similar result from [4]) characterizes the exponents of a $\mathcal{B}$-form of a product in $\mathbf{P} \rtimes \mathbf{A}$ using polynomials over an appropriate finite field $\mathbb{F}_q$. With the help of this characterization in Lemma 7 we reduce finding the image of a group expression over $\mathbf{P} \rtimes \mathbf{A}$ to deciding whether a system of equations (see system (17)) is solvable over $\mathbb{F}_q$. This reduction and the proof of Theorem 1 can be found in Sec. 3. Section 4 contains how Theorem 2 follows from Theorem 1.

Using Theorems 1 and 2, we updated the GAP [1, 5] computer programs from [11, 12] to determine the smallest groups for which the complexities of the equivalence and equation solvability problems are yet unknown. This GAP program essentially goes through the SmallGroups library in increasing order of the groups, and for each group checks if they satisfy any of the theorems mentioned in [11], or any of Theorem 1 or 2. Based on these computations, in Sec. 5 we review what questions remain open about the complexities of these problems over finite groups. The GAP source code and the full list can be found on the website [12].

2. Preliminaries

2.1. *Polynomials*

Let $\mathbb{F}_q$ denote the q element field. Our leading reference on polynomials over $\mathbb{F}_q$ is [17]. We say that a polynomial $f \in \mathbb{F}_q[x_1; \ldots; x_n]$ is in *reduced* form (or is a *reduced polynomial*) if f is of the form

$$f(x_1; \ldots; x_n) = \sum_{0 \leq s_1, \ldots, s_n \leq q-1} c_{s_1, \ldots, s_n} x_1^{s_1} \ldots x_n^{s_n}$$

for some $c_{s_1, \ldots, s_n} \in \mathbb{F}_q$ $(0 \leq s_k \leq q-1,\ 1 \leq k \leq n)$. Namely, if f is presented as a sum of monomials, where each variable in every monomial is raised to a power of at most $q-1$. For convenience, in polynomials we separate the variables by semicolons instead of the usual colons. Furthermore, recall that for an arbitrary n-ary function $f : \mathbb{F}_q^n \to \mathbb{F}_q$ there exists a (unique) reduced polynomial in $\mathbb{F}_q[x_1; \ldots; x_n]$ representing f.

The degree of the monomial $cx_1^{s_1} \ldots x_n^{s_n}$ is $s_1 + \cdots + s_n$. The length of a monomial is the number of variables and elements of $\mathbb{F}_q$ occurring in the monomial with multiplicity. For example, the length of the monomial $cx_1^{s_1} \ldots x_n^{s_n}$ 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, and is denoted by $\|f\|$.

Let β be a nonnegative integer, and $\mathcal{S}, \mathcal{S}_1, \ldots, \mathcal{S}_\beta \subseteq \mathbb{F}_q$. For positive integers $n, n_1, \ldots, n_\beta$, let

$$X = \{\, x_k : 1 \leq k \leq n \,\}, \quad Y_j = \{\, y_{j,k} : 1 \leq k \leq n_j \,\} \quad (1 \leq j \leq \beta)$$

be pairwise disjoint sets. Let $f_1, f_2 \in \mathbb{F}_q[X; Y_1; \ldots; Y_\beta]$ be two polynomials. We say that $f_1 = f_2$ *is solvable over* $\mathbb{F}_q$ *for substitutions from* $\mathcal{S}, \mathcal{S}_1, \ldots, \mathcal{S}_\beta$ (and write $f_1|_{\mathcal{S}, \mathcal{S}_1, \ldots, \mathcal{S}_\beta} = f_2|_{\mathcal{S}, \mathcal{S}_1, \ldots, \mathcal{S}_\beta}$ is solvable over $\mathbb{F}_q$) if there exists $s_1, \ldots, s_n \in \mathcal{S}$, $s_{1,1}, \ldots, s_{1,n_1} \in \mathcal{S}_1, \ldots, s_{\beta,1}, \ldots, s_{\beta,n_\beta} \in \mathcal{S}_\beta$, such that

$$\begin{aligned} &f_1(s_1; \ldots; s_n; s_{1,1}; \ldots; s_{1,n_1}; \ldots; s_{\beta,1}; \ldots; s_{\beta,n_\beta}) \\ &\quad = f_2(s_1; \ldots; s_n; s_{1,1}; \ldots; s_{1,n_1}; \ldots; s_{\beta,1}; \ldots; s_{\beta,n_\beta}). \end{aligned}$$

The following result is going to play a key role in the proof of Theorem 1.

Lemma 3 ([11, p. 221, case (d)]). *Let* $\mathbb{F}_q$ *be a finite field. Let* $\mathbf{S}_1, \ldots \mathbf{S}_\beta$ *be subgroups of the multiplicative group* $\mathbb{F}_q^\times$. *Let* $X = \{\, x_k : 1 \leq k \leq n \,\}$, $Y_j = \{\, y_{j,k} : 1 \leq k \leq n_j \,\}$ $(1 \leq j \leq \beta)$ *be pairwise disjoint sets. Let* $f_1, \ldots, f_m \in \mathbb{F}_q[X; Y_1; \ldots; Y_\beta]$ *be reduced polynomials. Then it can be decided in* $O(\max_{1 \leq i \leq m} \|f_i\|^{(q-1)m})$ *time whether or not the system of equations*

$$\begin{gathered} f_1|_{\mathbb{F}_q, \mathbf{S}_1, \ldots, \mathbf{S}_\beta} = 0 \\ \vdots \\ f_m|_{\mathbb{F}_q, \mathbf{S}_1, \ldots, \mathbf{S}_\beta} = 0 \end{gathered}$$

is solvable over $\mathbb{F}_q$.

2.2. *Groups*

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 $T = t_1 \dots t_n$ be a group expression over $\mathbf{G}$, that is each t_k ($1 \leq k \leq n$) 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, conjugation of h by a is defined as $h^a = aha^{|\mathbf{G}|-1}$, and therefore $ah = h^a a$.

Group multiplication is assumed to be performed in unit time. That is, computing the product $g_1 \dots g_n$ takes $O(n)$ time, and computing $h^a = aha^{|\mathbf{G}|-1}$ takes $O(|\mathbf{G}|+1)$ time. Since $\mathbf{G}$ is not part of our input, $O(|\mathbf{G}|+1) = O(1)$.

2.3. *Semidirect products*

Note first that it is enough to prove Theorem 1 if $p \nmid |\mathbf{A}|$.

Lemma 4. *The following are equivalent for a finite group* $\mathbf{G}$:

(a) $\mathbf{G} \simeq \mathbf{P} \rtimes \mathbf{A}$, *where* $\mathbf{P}$ *is a p-group and* $\mathbf{A}$ *is an Abelian group.*
(b) $\mathbf{G} \simeq \mathbf{P} \rtimes \mathbf{A}$, *where* $\mathbf{P}$ *is a p-group and* $\mathbf{A}$ *is an Abelian group such that p does not divide* $|\mathbf{A}|$.
(c) $\mathbf{G}'$ *is a p-group.*

Proof. (a) ⇒ (b) Trivial.

(a) ⇒ (c) If $\mathbf{G} \simeq \mathbf{P} \rtimes \mathbf{A}$, then $\mathbf{G}/\mathbf{P} \simeq \mathbf{A}$ is Abelian. Hence $\mathbf{G}' \subseteq \mathbf{P}$, and therefore $\mathbf{G}'$ is a p-group.

(c) ⇒ (b) Assume that $\mathbf{G}'$ is a p-group, and let $\mathbf{P}_{\mathrm{Syl}}$ be a Sylow p-subgroup of $\mathbf{G}$ containing the p-group $\mathbf{G}'$. Now, $\mathbf{G}' \subseteq \mathbf{P}_{\mathrm{Syl}}$ yields $\mathbf{P}_{\mathrm{Syl}}$ being normal in $\mathbf{G}$, and $\mathbf{G}/\mathbf{P}_{\mathrm{Syl}}$ is Abelian. Since $\mathbf{P}_{\mathrm{Syl}}$ is a Sylow p-subgroup, $|\mathbf{G}/\mathbf{P}_{\mathrm{Syl}}|$ is not divisible by p, and therefore $(|\mathbf{P}_{\mathrm{Syl}}|, |\mathbf{G}/\mathbf{P}_{\mathrm{Syl}}|) = 1$. By the theorem of Schur and Zassenhaus [18, 9.1.2], there exists a subgroup $\mathbf{A}$ in $\mathbf{G}$ such that $\mathbf{G} \simeq \mathbf{P}_{\mathrm{Syl}} \rtimes \mathbf{A}$. Finally, $\mathbf{A} \simeq \mathbf{G}/\mathbf{P}_{\mathrm{Syl}}$, therefore $\mathbf{A}$ is Abelian and p does not divide $|\mathbf{A}|$. □

For a prime p let $\mathbf{P}$ be a p-group of order p^α. Let $\mathbf{A}$ be an Abelian group for which $p \nmid |\mathbf{A}|$, and consider a semidirect product $\mathbf{G} = \mathbf{P} \rtimes \mathbf{A}$. Let us fix a chief series of $\mathbf{P}$, and extend it to a composition series of $\mathbf{G}$: $\{\,\mathrm{id}\,\} = \mathbf{N}_0 \lhd \mathbf{N}_1 \lhd \cdots \lhd \mathbf{N}_\alpha = \mathbf{P} = \mathbf{M}_0 \lhd \mathbf{M}_1 \lhd \cdots \lhd \mathbf{M}_\beta = \mathbf{G}$. Note, that $\mathbf{M}_j \lhd \mathbf{G}$ for all $1 \leq j \leq \beta$, and $\mathbf{N}_i \lhd \mathbf{P}$ for all $1 \leq j \leq \alpha$, but $\mathbf{N}_i$ is not necessarily a normal subgroup of $\mathbf{G}$. Now, $\mathbf{N}_i/\mathbf{N}_{i-1}$ is isomorphic to the cyclic group of order p ($1 \leq i \leq \alpha$), and $\mathbf{M}_j/\mathbf{M}_{j-1}$ is isomorphic to the cyclic group of order p_j for some prime $p_j \neq p$ ($1 \leq j \leq \beta$). For every $1 \leq i \leq \alpha$ let $b_i \in \mathbf{N}_i \backslash \mathbf{N}_{i-1}$ be arbitrary, and for every $1 \leq j \leq \beta$ let $c_j \in \mathbf{M}_j \backslash \mathbf{M}_{j-1}$ be arbitrary. Then, $b_i\mathbf{N}_{i-1}$ is a generator of the quotient $\mathbf{N}_i/\mathbf{N}_{i-1}$ and $c_j\mathbf{M}_{j-1}$ is a generator of the quotient $\mathbf{M}_j/\mathbf{M}_{j-1}$. We call the sequence $\mathcal{B} = (b_1, \ldots, b_\alpha, c_1, \ldots, c_\beta)$ a *basis* of $\mathbf{G}$. Let $g \in \mathbf{G}$ be arbitrary. Then there exist unique $u_1, \ldots, u_\alpha \in \{ 0, 1, \ldots, p-1 \}$, and $v_j \in \{ 0, 1, \ldots, p_j - 1 \}$ for all $1 \le j \le \beta$ such that

$$g = b_1^{u_1} \ldots b_\alpha^{u_\alpha} c_1^{v_1} \ldots c_\alpha^{v_\beta}. \tag{1}$$

For a basis $\mathcal{B}$ we call (1) the *$\mathcal{B}$-form of the element* g, and denote it by

$$[\, u_1, \ldots, u_\alpha; v_1, \ldots, v_\beta \,]_{\mathcal{B}}.$$

Note, that for a given $\mathbf{G}$, calculating a basis $\mathcal{B}$ of $\mathbf{G}$ depends only on $\mathbf{G}$. Since $\mathbf{G}$ is not part of the input, but is given in advance, calculating a basis $\mathcal{B}$ takes constant time. Similarly, for any (or even all) $g \in \mathbf{G}$, calculating the $\mathcal{B}$-form of g takes constant time.

Let $\mathbb{F}_q$ be the smallest finite field of characteristic p such that the multiplicative group $\mathbb{F}_q^\times$ contains a cyclic subgroup of order p_j for all $1 \le j \le \beta$. We call $\mathbb{F}_q$ the *base field of* $\mathbf{G}$. For example, if $|\mathbf{A}| = 1$, that is $\mathbf{G} = \mathbf{P}$, then the base field of $\mathbf{G}$ is $\mathbb{Z}_p$. The base field always exists: note first, that the condition that the multiplicative group $\mathbb{F}_q^\times$ contains a cyclic subgroup of order p_j is equivalent to $q \equiv 1 \pmod{p_j}$. Let m be the least common multiple of $p_1, \ldots, p_\beta$. Now, $p \nmid |\mathbf{A}|$, hence $(p, m) = 1$, therefore the congruence

$$p^x \equiv 1 \pmod{m} \tag{2}$$

has a smallest positive solution $x = s$. Let $q = p^s$. Note that $s \le m \le |\mathbf{A}|$, and therefore

$$q = p^s \le p^{|\mathbf{A}|}. \tag{3}$$

We claim that the finite field $\mathbb{F}_q$ is the base field of $\mathbf{G}$. Indeed, $\mathbb{F}_q$ has characteristic p, its multiplicative subgroup is a cyclic group of order $q-1$, and since $p_j \mid q-1$ by (2), $\mathbb{F}_q^\times$ contains a (unique) cyclic group of order p_j $(1 \le j \le \beta)$. Let $\mathbf{S}_j$ denote this order p_j cyclic subgroup of $\mathbb{F}_q^\times$ $(1 \le j \le \beta)$. Let $\oplus_{p_j}$ denote the modulo p_j addition on the set $\{ 0, 1, \ldots, p_j - 1 \}$, and let $\mathbf{Z}_{p_j}$ denote the cyclic group $(\{ 0, 1, \ldots, p_j - 1 \}, \oplus_{p_j})$ $(1 \le j \le \beta)$. For each $1 \le j \le \beta$ let us fix an isomorphism

$$\varphi_j : \mathbf{Z}_{p_j} \to \mathbf{S}_j. \tag{4}$$

Note, that the base field $\mathbb{F}_q$, and the isomorphisms φ_j all depend only on $\mathbf{G}$, and therefore can be computed in advance in constant time.

In the special case $|\mathbf{A}| = 1$, the following lemma from [4] 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 5 ([4, Lemma 3]). *Let* $\mathbf{P}$ *be a p-group of order* p^α, *let* $\mathcal{B} = (b_1, \ldots, b_\alpha)$ *be a basis of* $\mathbf{P}$. *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*

$$g_k = [\,u_{k,1}, \dots, u_{k,\alpha}\,]_{\mathcal{B}} \quad (1 \le k \le n),$$

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

$$g_1 \dots g_n = [\,u_1, \dots, u_\alpha\,]_{\mathcal{B}}\,, \quad \textit{where}$$

$$u_l = f_l(u_{1,1}; \dots; u_{n,\alpha}) \quad (1 \le l \le \alpha).$$

Furthermore, with the constant $C_\alpha = (2p-2)^{\alpha-1}$, *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* $O(n^{C_\alpha})$ *time, and* $\|f_l\| = O(n^{C_\alpha})$ $(1 \le l \le \alpha)$. *Here, the constant* C_α *and the multiplying constant in the* $O()$ *expression depend only on* $\mathbf{G}$ *and are independent of* n.

We need a generalized version of Lemma 5 for semidirect products $\mathbf{P} \rtimes \mathbf{A}$.

Lemma 6. *For a prime* p *let* $\mathbf{P}$ *be a* p*-group of order* p^α. *Let* $\mathbf{A}$ *be an Abelian group for which* $p \nmid |\mathbf{A}|$, *and consider a semidirect product* $\mathbf{G} = \mathbf{P} \rtimes \mathbf{A}$. *Let* $\mathcal{B} = (b_1, \dots, b_\alpha, c_1, \dots, c_\beta)$ *be a basis of* $\mathbf{G}$, *and let* $\mathbb{F}_q$ *denote the base field of* $\mathbf{G}$. *Let* $\varphi_1, \dots, \varphi_\beta$ *be the isomorphisms defined by* (4). *For an arbitrary positive integer* n *let*

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

$$Y_{n-1,\beta} = \{\, y_{k,j} \mid 1 \le k \le n-1, 1 \le j \le \beta \,\}$$

be disjoint sets of variables. Then there exist reduced polynomials $f_1, \dots, f_\alpha \in \mathbb{F}_q[X_{n,\alpha}; Y_{n-1,\beta}]$ *such that for arbitrary* $h_1, \dots, h_n \in \mathbf{P}$, $a_1, \dots, a_n \in \mathbf{A}$ *with* $\mathcal{B}$*-forms*

$$h_k = [\,u_{k,1}, \dots, u_{k,\alpha}; 0, \dots, 0\,]_{\mathcal{B}}\,,$$

$$a_k = [\,0, \dots, 0; v_{k,1}, \dots, v_{k,\beta}\,]_{\mathcal{B}} \quad (1 \le k \le n)$$

the $\mathcal{B}$*-form of the product* $h_1 a_1 \dots h_n a_n$ *is*

$$h_1 a_1 \dots h_n a_n = [\,u_1, \dots, u_\alpha; v_1, \dots, v_\beta\,]_{\mathcal{B}}\,, \quad \textit{where}$$

$$u_i = f_i(u_{1,1}; \dots; u_{n,\alpha}; \varphi_1(v_{1,1}); \dots; \varphi_\beta(v_{n-1,\beta})) \quad (1 \le i \le \alpha),$$

$$v_j = v_{1,j} \oplus_{p_j} \dots \oplus_{p_j} v_{n,j} \quad (1 \le j \le \beta).$$

Furthermore, with the constant $C_\alpha = (2p-2)^{\alpha-1}$, *each monomial of* f_l $(1 \le l \le \alpha)$ *contains at most* $\alpha^{C_\alpha}(q-1)^{C_\alpha}$*-many variables from* $X_{n,\alpha}$, *each polynomial* f_l $(1 \le l \le \alpha)$ *can be computed in* $O(n^{C_\alpha+1})$ *time, and* $\|f_l\| = O(n^{C_\alpha+1})$ $(1 \le l \le \alpha)$. *Here, the constant* C_α *and the multiplying constant in the* $O()$ *expression depend only on* $\mathbf{G}$ *and are independent of* n.

Proof. First, for each $1 \le k \le n$ collect the factor a_k of the product $h_1 a_1 \dots h_n a_n$ to the right by applying $ah = h^a a$:

$$\begin{aligned} h_1 a_1 h_2 a_2 h_3 a_3 \dots h_n a_n &= h_1 h_2^{a_1} a_1 a_2 h_3 a_3 \dots h_n a_n \\ &= h_1 h_2^{a_1} h_3^{a_1 a_2} a_1 a_2 a_3 \dots h_n a_n \\ &= \underbrace{h_1 h_2^{a_1} h_3^{a_1 a_2} \dots h_n^{a_1 \cdots a_{n-1}}}_{\in \mathbf{P}} \underbrace{a_1 a_2 a_3 \dots a_n}_{\in \mathbf{A}}. \end{aligned}$$

Let

$$T_{\mathbf{P}} = h_1 h_2^{a_1} \cdots h_n^{a_1 \cdots a_{n-1}}, \quad T_{\mathbf{A}} = a_1 \cdots a_n. \tag{5}$$

Since $\mathbf{A}$ is Abelian, the $\mathcal{B}$-form of $T_{\mathbf{A}}$ is

$$\begin{aligned} T_{\mathbf{A}} = a_1 \dots a_n &= \prod_{k=1}^{n} [\, 0, \dots, 0; v_{k,1}, \dots, v_{k,\beta} \,]_{\mathcal{B}} \\ &= \prod_{k=1}^{n} c_1^{v_{k,1}} \dots c_\beta^{v_{k,\beta}} = c_1^{v_{1,1} \oplus_{p_1} \dots \oplus_{p_1} v_{n,1}} \cdots c_\beta^{v_{1,\beta} \oplus_{p_\beta} \dots \oplus_{p_\beta} v_{n,\beta}} \\ &= [\, 0, \dots, 0; v_1, \dots, v_\beta \,]_{\mathcal{B}}, \text{ where} \end{aligned}$$

$$v_j = v_{1,j} \oplus_{p_j} \dots \oplus_{p_j} v_{n,j} \quad (1 \le j \le \beta). \tag{6}$$

Now, we compute the $\mathcal{B}$-form of $h_k^{a_1 \cdots a_{k-1}}$. The $\mathcal{B}$-form of h_k is

$$h_k = [\, u_{k,1}, \dots, u_{k,\alpha}; 0, \dots, 0 \,]_{\mathcal{B}}, \tag{7}$$

and the $\mathcal{B}$-form of $a_1 \cdots a_{k-1}$ is

$$a_1 \cdots a_{k-1} = [\, 0, \dots, 0; \tilde{v}_{k-1,1}, \dots, \tilde{v}_{k-1,\beta} \,]_{\mathcal{B}}, \text{ where}$$

$$\tilde{v}_{k-1,j} = v_{1,j} \oplus_{p_j} \dots \oplus_{p_j} v_{k-1,j} \quad (1 \le j \le \beta). \tag{8}$$

Since φ_j (defined by (4)) is an isomorphism between $\mathbf{Z}_{p_j}$ and $\mathbf{S}_j$, we have

$$\varphi_j(v_{1,j} \oplus_{p_j} \dots \oplus_{p_j} v_{k-1,j}) = \varphi_j(v_{1,j}) \dots \varphi_j(v_{k-1,j}). \tag{9}$$

Let $\chi_i : \mathbb{F}_q^{\alpha+\beta} \to \mathbb{F}_q$ $(1 \le i \le \alpha)$ be functions such that for each $h \in \mathbf{P}$, $a \in \mathbf{A}$ with $\mathcal{B}$-forms

$$h = [\, \check{u}_1, \dots, \check{u}_\alpha; 0, \dots, 0 \,]_{\mathcal{B}}, \quad a = [\, 0, \dots, 0; \check{v}_1, \dots, \check{v}_\beta \,]_{\mathcal{B}}$$

we have that the $\mathcal{B}$-form of h^a is

$$h^a = [\, \bar{u}_1, \dots, \bar{u}_\alpha; 0, \dots, 0 \,]_{\mathcal{B}}, \text{ where}$$

$$\bar{u}_i = \chi_i(\check{u}_1; \dots; \check{u}_\alpha; \varphi_1(\check{v}_1); \dots; \varphi_\beta(\check{v}_\beta)) \quad (1 \le i \le \alpha). \tag{10}$$

If, for some $1 \le i \le \alpha$, multiple functions χ_i satisfy (10), then we fix one for the proof.

Let $X_\alpha = \{\, x_1, \dots, x_\alpha \,\}$, $Y_\beta = \{\, y_1, \dots, y_\beta \,\}$ be disjoint sets from each other and from $X_{n,\alpha} \cup Y_{n-1,\beta}$. Since every function is a polynomial over $\mathbb{F}_q$, there exist reduced polynomials from $\mathbb{F}_q[X_\alpha; Y_\beta]$ representing χ_i $(1 \le i \le \alpha)$. By slightly abusing the notation, we denote these reduced polynomials by χ_i, as well. The time required constructing these polynomials depends only on the group $\mathbf{G}$, and not on n. Furthermore, the degree of each monomial of each χ_i is at most $(\alpha + \beta) \cdot (q - 1)$, and χ_i is the sum of at most $q^{\alpha+\beta}$-many monomials $(1 \le i \le \alpha)$.

For each $1 \le i \le \alpha$, $2 \le k \le n$, let us replace in $\chi_i(X_\alpha; Y_\beta)$ the variable y_j by the product $y_{1,j} \dots y_{k-1,j}$ $(1 \le j \le \beta)$. Let $\chi_i^{(k)} \in \mathbb{F}_q[X_\alpha; Y_{n-1,\beta}]$ $(1 \le i \le \alpha, 2 \le k \le n)$ denote the obtained reduced polynomial. Then the $\mathcal{B}$-form of $h_k^{a_1 \cdots a_{k-1}}$ is

$$h_k^{a_1 \cdots a_{k-1}} = [\, \tilde{u}_{k,1}, \dots, \tilde{u}_{k,\alpha}; 0, \dots, 0\,]_{\mathcal{B}}\,, \tag{11}$$

where by (7)–(10) we have

$$\tilde{u}_{k,i} = \begin{cases} u_{k,i}, & \text{if } k = 1, \\ \chi_i^{(k)}(u_{k,1}; \dots; u_{k,\alpha}; \varphi_1(v_{1,1}); \dots; \varphi_\beta(v_{k-1,\beta})), & \text{if } 2 \le k \le n. \end{cases} \tag{12}$$

The number of monomials in $\chi_i^{(k)}$ is at most $q^{\alpha+\beta}$, since χ_i was the sum of at most $q^{\alpha+\beta}$-many monomials. Moreover, the degree of each monomial in $\chi_i^{(k)}$ is at most $(q-1)(\alpha+\beta(n-1)) = O(n)$, since $|X_\alpha| = \alpha$, and $|Y_{n-1,\beta}| = \beta(n-1)$. Furthermore, each monomial of $\chi_i^{(k)}$ contains at most $\alpha(q-1)$-many occurrences of variables from X_α. Thus, $\|\chi_i^{(k)}\| = O(n)$, and all $\chi_i^{(k)}$ $(1 \le i \le \alpha,\ 2 \le k \le n)$ can be constructed in $O(n^2)$ time.

Finally, with the help of Lemma 5 we compute the $\mathcal{B}$-form of $T_{\mathbf{P}}$ in (5). Each factor $h_k^{a_1 \dots a_{k-1}}$ $(2 \le k \le n)$ of the product $T_{\mathbf{P}}$ is in $\mathbf{P}$. The $\mathcal{B}$-form $h_k^{a_1 \dots a_{k-1}}$ $(2 \le k \le n)$ is given by (11). Since $(b_1, \dots, b_\alpha)$ is a basis of $\mathbf{P}$, we can apply Lemma 5. Let $C_\alpha = (2p-2)^{\alpha-1}$. By Lemma 5 there exist reduced polynomials $\tilde{f}_l \in \mathbb{Z}_p[X_{n,\alpha}]$ $(1 \le l \le \alpha)$ such that each monomial of $\tilde{f}_l$ has degree at most C_α, $\|\tilde{f}_l\| = O(n^{C_\alpha})$, and the $\mathcal{B}$-form of $T_{\mathbf{P}}$ is

$$\begin{aligned} &T_{\mathbf{P}} = [\, u_1, \dots, u_\alpha; 0, \dots, 0\,]_{\mathcal{B}}\,, \quad \text{where} \\ &u_i = \tilde{f}_i(\tilde{u}_{1,1}; \dots; \tilde{u}_{n,\alpha}) \quad (1 \le i \le \alpha), \end{aligned} \tag{13}$$

and $\tilde{u}_{k,i}$ is defined by (12). Moreover, computing all polynomials $\tilde{f}_l$ takes $O(n^{C_\alpha})$ time.

Since $\mathbb{Z}_p \le \mathbb{F}_q$, we may consider $\tilde{f}_l$ as a polynomial from $\mathbb{F}_q[X_{n,\alpha}]$ $(1 \le l \le \alpha)$. Now, for each $1 \le l \le \alpha$ let us replace in $\tilde{f}_l$ each variable $x_{k,i}$ $(1 \le i \le \alpha$, $2 \le k \le n)$ by the reduced polynomial $\chi_i^{(k)}(x_{k,1}; \dots; x_{k,\alpha}; Y_{n-1,\beta})$, and expand the resulting polynomials into a sum of monomials. Let $f_l \in \mathbb{F}_q[X_{n,\alpha}; Y_{n-1,\beta}]$ denote the obtained reduced polynomial $(1 \le l \le \alpha)$. By (11)–(13) the $\mathcal{B}$-form of $T_{\mathbf{P}}$ is

$$\begin{aligned} &T_{\mathbf{P}} = [u_1, \dots, u_\alpha; 0, \dots, 0]_{\mathcal{B}}\,, \quad \text{where} \\ &u_i = f_i(u_{1,1}; \dots; u_{n,\alpha}; \varphi_1(v_{1,1}); \dots; \varphi_\beta(v_{n-1,\beta})) \quad (1 \le i \le \alpha). \end{aligned} \tag{14}$$

Thus, by (6) and (14) the $\mathcal{B}$-form of the product $h_1a_1 \dots h_na_n$ is

$$h_1a_1 \dots h_na_n = T_{\mathbf{P}}T_{\mathbf{A}} = [u_1, \dots, u_\alpha; v_1, \dots, v_\beta]_{\mathcal{B}}, \text{ where}$$

$$u_i = f_i(u_{1,1}; \dots; u_{n,\alpha}; \varphi_1(v_{1,1}); \dots; \varphi_\beta(v_{n-1,\beta})) \quad (1 \le i \le \alpha),$$

$$v_j = v_{1,j} \oplus_{p_j} \dots \oplus_{p_j} v_{n,j} \quad (1 \le j \le \beta).$$

The degree of each monomial of $\tilde{f}_l$ is at most C_α by Lemma 5. We obtain f_l by substituting into every variable $x_{k,i}$ the polynomial $\chi_i^{(k)}$. Each monomial of $\chi_i^{(k)}$ contains at most $\alpha(q-1)$-many occurrences of variables from $X_{n,\alpha}$. Thus, each monomial of f_l contains at most $\alpha^{C_\alpha}(q-1)^{C_\alpha}$-many occurrences of variables from $X_{n,\alpha}$. Furthermore, the number of monomials in $\chi_i^{(k)}$ is at most $q^{\alpha+\beta}$, and the degree of each monomial of $\chi_i^{(k)}$ is $O(n)$. Thus, expanding any monomial of $\tilde{f}_l$ produces at most $(q^{\alpha+\beta})^{C_\alpha}$-many monomials, and the degree of each monomial in f_l is at most $C_\alpha \cdot O(n)$. Hence

$$\|f_l\| \le \left\|\tilde{f}_l\right\| \cdot (q^{\alpha+\beta})^{C_\alpha} \cdot C_\alpha \cdot O(n) = O(n^{C_\alpha}) \cdot O(n) = O(n^{C_\alpha+1}),$$

and computing f_l from $\tilde{f}_l$ and $\chi_i^{(k)}$ takes $O(n^{C_\alpha+1})$ time.

That is, the running time of computing f_l consists of the following:

- $O(n^{C_\alpha})$ time to compute the polynomial $\tilde{f}_l$,
- $O(n^2)$ time to compute the polynomials $\chi_i^{(k)}$ for all $1 \le i \le \alpha$, $2 \le k \le n$,
- $O(n^{C_\alpha+1})$ time to compute the polynomial f_l from $\tilde{f}_l$ and $\chi_i^{(k)}$.

Since $2 \le C_\alpha$, the time needed to compute the polynomial f_l is

$$O(n^{C_\alpha} + n^2 + n^{C_\alpha+1}) = O(n^{C_\alpha+1}). \qquad \square$$

3. Equation Solvability

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

Lemma 7. *For a prime p let $\mathbf{P}$ be a p-group of order p^α. Let $\mathbf{A}$ be an Abelian group for which $p \nmid |\mathbf{A}|$, and consider a semidirect product $\mathbf{G} = \mathbf{P} \rtimes \mathbf{A}$. Assume $|\mathbf{A}| = p_1 \dots p_\beta$ for some (not necessarily distinct) primes. Let $C_\alpha = (2p-2)^{\alpha-1}$, and let the base field of $\mathbf{G}$ be $\mathbb{F}_q$. Let $g \in \mathbf{P}$ be arbitrary, and T be a group expression over $\mathbf{P}$ of length n. Then it can be decided in $O(n^{(C_\alpha+1)(q-1)(\alpha+\beta)})$ time whether or not the equation $T = g$ has a solution over $\mathbf{G}$. Here, the constants $C_\alpha, q, \alpha, \beta$ and the multiplying constant in the $O()$ expression depend only on $\mathbf{G}$ and are independent of n.*

Proof. Let us fix a chief series of $\mathbf{P}$, and extend it to a composition series of $\mathbf{G}$: $\{\mathrm{id}\} = \mathbf{N}_0 \lhd \mathbf{N}_1 \lhd \dots \lhd \mathbf{N}_\alpha = \mathbf{P} = \mathbf{M}_0 \lhd \mathbf{M}_1 \lhd \dots \lhd \mathbf{M}_\beta = \mathbf{G}$. Assume $\mathbf{M}_j/\mathbf{M}_{j-1} \simeq \mathbf{Z}_{p_j}$ for all $1 \le j \le \beta$. Let $\mathcal{B} = (b_1, \dots, b_\alpha, c_1, \dots, c_\beta)$ be a basis of $\mathbf{G}$ corresponding to this composition series. The time required constructing these depends only on the group $\mathbf{G}$, and not on n. Let $T = t_1 \dots t_n$ be a group expression over $\mathbf{G}$, where every t_k $(1 \le k \le n)$ is either a variable or an element of $\mathbf{G}$. For every $1 \le k \le n$ we replace t_k by its $\mathcal{B}$-form in the following way:

- If t_k is an element of $\mathbf{G}$, then let $x_{k,i}$ $(1 \le i \le \alpha)$ be elements of $\mathbb{Z}_p$ and let $z_{k,j}$ $(1 \le j \le \beta)$ be elements of $\mathbf{Z}_{p_j}$ such that $t_k = b_1^{x_{k,1}} \dots b_\alpha^{x_{k,\alpha}} c_1^{z_{k,1}} \dots c_\beta^{z_{k,\beta}}$, and replace t_k by its $\mathcal{B}$-form $[x_{k,1}, \dots, x_{k,\alpha}; z_{k,1}, \dots z_{k,\beta}]_{\mathcal{B}}$.
- If t_k is a variable over $\mathbf{G}$ then let $x_{k,i}$ $(1 \le i \le \alpha)$ denote a variable over $\mathbb{Z}_p$ such that x_{k_1,i_1} and x_{k_2,i_2} (for some $1 \le k_1, k_2 \le n$, $1 \le i_1, i_2 \le \alpha$) denote the same variable if and only if t_{k_1} and t_{k_2} denote the same variable over $\mathbf{G}$ and $i_1 = i_2$. Similarly, let $z_{k,j}$ $(1 \le j \le \alpha)$ denote a variable over $\mathbf{Z}_{p_j}$ such that z_{k_1,j_1} and z_{k_2,j_2} (for some $1 \le k_1, k_2 \le n$, $1 \le j_1, j_2 \le \beta$) denote the same variable if and only if t_{k_1} and t_{k_2} denote the same variable over $\mathbf{G}$ and $j_1 = j_2$. Now, every element of $\mathbf{G}$ has a unique $\mathcal{B}$-form. Thus, when the values of the variables $x_{k,1}, \dots, x_{k,\alpha}$ run through the elements of $\mathbb{Z}_p$, and the values of the variables $z_{k,j}$ run through the elements of $\mathbf{Z}_{p_j}$ $(1 \le j \le \beta)$, the value of the expression $b_1^{x_{k,1}} \dots b_\alpha^{x_{k,\alpha}} c_1^{z_{k,1}} \dots c_\beta^{z_{k,\beta}}$ runs through the elements of $\mathbf{G}$. Now, replace t_k by the $\mathcal{B}$-form expression $[x_{k,1}, \dots, x_{k,\alpha}; z_{k,1}, \dots z_{k,\beta}]_{\mathcal{B}}$.

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

For each $1 \le j \le \beta$ let $\varphi_j \colon \mathbf{Z}_{p_j} \to \mathbf{S}_j$ be the isomorphism defined by (4). For every $1 \le k \le n$, $1 \le j \le \beta$ we define $y_{k,j}$ in the following way:

- If $z_{k,j}$ is an element of $\mathbf{Z}_{p_j}$, then let $y_{k,j} = \varphi(z_{k,j}) \in \mathbf{S}_j$.
- If $z_{k,j}$ is a variable over $\mathbf{Z}_{p_j}$ then let $y_{k,j}$ denote a variable over $\mathbf{S}_j$ such that y_{k_1,j_1} and y_{k_2,j_2} (for some $1 \le k_1, k_2 \le n$, $1 \le j_1, j_2 \le \beta$) denote the same variable if and only if z_{k_1,j_1} and z_{k_2,j_2} denote the same variable over $\mathbf{Z}_{p_j}$. When the value of the variable $z_{k,j}$ runs through the elements of $\mathbf{Z}_{p_j}$, the value of the expression $\varphi(z_{k,j})$ runs through the elements of $\mathbf{S}_j$.

We are going to apply Lemma 6 to compute the $\mathcal{B}$-form of the product $t_1 \dots t_n$. Let $X_{n,\alpha} = \{\, x_{k,i} \mid 1 \le k \le n, 1 \le i \le \alpha \,\}$, $Y_{n-1,\beta} = \{\, y_{k,j} \mid 1 \le k \le n-1, 1 \le j \le \beta \,\}$, and assume that $X_{n,\alpha}$ and $Y_{n-1,\beta}$ are disjoint. Let $C_\alpha = (2p-2)^{\alpha-1}$. Let us compute the reduced polynomials $f_1, \dots, f_\alpha \in \mathbb{F}_q[X_{n,\alpha}; Y_{n-1,\beta}]$ from Lemma 6 in $O(n^{C_\alpha+1})$ time. Now, for all $1 \le l \le \alpha$ each monomial of f_l contains at most $\alpha^{C_\alpha}(q-1)^{C_\alpha}$-many variables from $X_{n,\alpha}$, $\|f_l\| = O(n^{C_\alpha+1})$, and by Lemma 6

$$t_1 \dots t_n = [\,\bar{u}_1, \dots, \bar{u}_\alpha; \bar{v}_1, \dots, \bar{v}_\beta\,]_{\mathcal{B}}\,, \text{where}$$

$$\bar{u}_i = f_i(x_{1,1}; \dots; x_{n,\alpha}; y_{1,1}; \dots; y_{n-1,\beta}) \quad (1 \le i \le \alpha),$$

$$\bar{v}_j = z_{1,j} \oplus_{p_j} \dots \oplus_{p_j} z_{n,j} \quad (1 \le j \le \beta)$$

is the $\mathcal{B}$-form of the product $t_1 \dots t_n$. Here, $x_{k,i}$ is an element of $\mathbb{Z}_p$ or a variable over $\mathbb{Z}_p$, $y_{k,j}$ is an element of $\mathbf{S}_j$ or a variable over $\mathbf{S}_j$, $z_{k,j}$ is an element of $\mathbf{Z}_{p_j}$ or a variable over $\mathbf{Z}_{p_j}$. Let the $\mathcal{B}$-form of g be $[\,u_1, \dots, u_\alpha; v_1, \dots, v_\beta\,]_{\mathcal{B}}$. Since the $\mathcal{B}$-form is unique, every solution of $t_1 \dots t_n = g$ over $\mathbf{G}$ corresponds to such a solution of the system

$$\begin{aligned} f_1|_{\mathbb{Z}_p,\mathbf{S}_1,\dots,\mathbf{S}_\beta}(x_{1,1};\dots;x_{n,\alpha};y_{1,1};\dots;y_{n-1,\beta}) &= u_1, \\ &\vdots \\ f_\alpha|_{\mathbb{Z}_p,\mathbf{S}_1,\dots,\mathbf{S}_\beta}(x_{1,1};\dots;x_{n,\alpha};y_{1,1};\dots;y_{n-1,\beta}) &= u_\alpha, \\ z_{1,1} \oplus_{p_1} \dots \oplus_{p_1} z_{n,1} &= v_1, \\ &\vdots \\ z_{1,\beta} \oplus_{p_\beta} \dots \oplus_{p_\beta} z_{n,\beta} &= v_\beta, \end{aligned} \tag{15}$$

which satisfies $\varphi_j(z_{k,j}) = y_{k,j}$ for each $1 \le k \le n$, $1 \le j \le \beta$. The first α-many equations of (15) are over $\mathbb{F}_q$, the next β-many equations are over $\mathbf{Z}_{p_1}, \dots, \mathbf{Z}_{p_\beta}$, respectively. We translate these latter β-many equations to equations over $\mathbb{F}_q$, as well. By the definition of φ_j and $y_{k,j}$, for each $1 \le j \le \beta$ we have

$$z_{1,j} \oplus_{p_j} \dots \oplus_{p_j} z_{n,j} = v_j, \quad \text{if and only if } y_{1,j} \dots y_{n,j} = \varphi(v_j).$$

For each $1 \le j \le \beta$ let $g_j(y_{1,j};\dots;y_{n,j}) = y_{1,j} \dots y_{n,j}$. That is, the system (15) has a solution satisfying $\varphi_j(z_{k,j}) = y_{k,j}$ if and only if the system

$$\begin{aligned} f_1|_{\mathbb{Z}_p,\mathbf{S}_1,\dots,\mathbf{S}_\beta}(x_{1,1};\dots;x_{n,\alpha};y_{1,1};\dots;y_{n-1,\beta}) &= u_1, \\ &\vdots \\ f_\alpha|_{\mathbb{Z}_p,\mathbf{S}_1,\dots,\mathbf{S}_\beta}(x_{1,1};\dots;x_{n,\alpha};y_{1,1};\dots;y_{n-1,\beta}) &= u_\alpha, \\ g_1|_{\mathbf{S}_1}(y_{1,1};\dots;y_{n,1}) &= \varphi(v_1), \\ &\vdots \\ g_\beta|_{\mathbf{S}_\beta}(y_{1,\beta};\dots;y_{n,\beta}) &= \varphi(v_\beta) \end{aligned} \tag{16}$$

has a solution over $\mathbb{F}_q$.

Let π be a (monic) reduced polynomial over $\mathbb{F}_q$ whose range is $\mathbb{Z}_p$. Thus, while the value of the variable $x_{k,i}$ ($1 \le i \le \alpha$, $1 \le k \le n$) runs through the elements of $\mathbb{F}_q$, the value of the polynomial $\pi(x_{k,i})$ runs through the elements of $\mathbb{Z}_p$. For each $1 \le l \le \alpha$ let us replace in f_l each variable $x_{k,i}$ ($1 \le i \le \alpha$, $1 \le k \le n$) by the reduced polynomial $\pi(x_{k,i})$, and expand the resulting polynomials into a sum of monomials. Let $\hat{f}_l \in \mathbb{F}_q[X_{n,\alpha}; Y_{n-1,\beta}]$ denote the obtained reduced polynomial ($1 \le l \le \alpha$). Each monomial of f_l contains at most $\alpha^{C_\alpha}(q-1)^{C_\alpha}$-many variables from $X_{n,\alpha}$, thus

$$\|\hat{f}_l\| \le \|f_l\| \cdot \|\pi\|^{\alpha^{C_\alpha}(q-1)^{C_\alpha}} = O(\|f_l\|),$$

since $\|\pi\|$ only depends on q and p (that is, on $\mathbf{G}$), and not on n. Moreover, computing $\hat{f}_l$ from f_l takes $O(n^{C_\alpha+1})$ time.

Now, (16) has a solution over $\mathbb{F}_q$ if and only if the system

$$\begin{aligned}\hat{f}_1|_{\mathbb{F}_q,\mathbf{s}_1,\dots,\mathbf{s}_\beta}(x_{1,1};\dots;x_{n,\alpha};y_{1,1};\dots;y_{n-1,\beta})-u_1&=0,\\ &\vdots\\ \hat{f}_\alpha|_{\mathbb{F}_q,\mathbf{s}_1,\dots,\mathbf{s}_\beta}(x_{1,1};\dots;x_{n,\alpha};y_{1,1};\dots;y_{n-1,\beta})-u_\alpha&=0,\\ g_1|_{\mathbf{s}_1}(y_{1,1};\dots;y_{n,1})-\varphi(v_1)&=0,\\ &\vdots\\ g_\beta|_{\mathbf{s}_\beta}(y_{1,\beta};\dots;y_{n,\beta})-\varphi(v_\beta)&=0\end{aligned}\tag{17}$$

has a solution over $\mathbb{F}_q$. Here, $\|\hat{f}_l-u_l\|\le O(\|f_l\|)=O(n^{C_\alpha+1})$ $(1\le l\le\alpha)$, $\|g_j-\varphi_j(v_j)\|=n+1=O(n)$ $(1\le j\le\beta)$. By Lemma 3 it can be decided in $O(n^{(C_\alpha+1)(q-1)(\alpha+\beta)})$ time whether or not (17) is solvable over $\mathbb{F}_q$.

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

- $O(n)$ time to replace every t_k by its $\mathcal{B}$-form $(1\le k\le n)$,
- $O(n)$ time to create each $y_{k,j}$ $(1\le k\le n,\ 1\le j\le\beta)$,
- $O(n^{C_\alpha+1})$ time to compute the reduced polynomials $f_1,\dots,f_\alpha$,
- $O(n^{C_\alpha+1})$ time to compute the reduced polynomials $\hat{f}_1,\dots,\hat{f}_\alpha$,
- $O(n^{(C_\alpha+1)(q-1)(\alpha+\beta)})$ time to decide whether or not (17) has a solution over $\mathbb{F}_q$.

Thus the time needed to decide whether or not $T=g$ has a solution over $\mathbf{G}$ is

$$O(n+n+n^{C_\alpha+1}+n^{C_\alpha+1}+n^{(C_\alpha+1)(q-1)(\alpha+\beta)})=O(n^{(C_\alpha+1)(q-1)(\alpha+\beta)}).\qquad\square$$

Finally, we prove Theorem 1.

Proof of Theorem 1. Let $\mathbf{G}\simeq\mathbf{P}\rtimes\mathbf{A}$ for a finite p-group $\mathbf{P}$ and an Abelian group $\mathbf{A}$. By Lemma 4 we may assume that p does not divide $|\mathbf{A}|$. Assume $|\mathbf{P}|=p^\alpha$, and $|\mathbf{A}|=p_1\dots p_\beta$ for some (not necessarily distinct) primes.

Let $S=x_1\dots x_k$ and $T=y_1\dots y_n$ be two group expressions over $\mathbf{G}$, such that $k\le n$. 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, $\|T'\|\le|\mathbf{G}|\cdot n=O(n)$, since $|\mathbf{G}|$ does not depend on S and T, hence does not depend on n, either. In the following we consider the equation $T'=\mathrm{id}$.

By Lemma 7 one can decide in $O(n^{(C_\alpha+1)(q-1)(\alpha+\beta)})$ time whether or not $T' = \mathrm{id}$ has a solution in $\mathbf{G}$. Here, $|\mathbf{G}| = p^\alpha p_1 \dots p_\beta$, therefore

$$\alpha + \beta \leq \log |\mathbf{G}|,$$
$$C_\alpha + 1 = (2p-2)^{\alpha-1} + 1 \leq 2 \cdot (2p)^{\alpha-1} \leq p^{2\alpha-1}.$$

Moreover, from (3) we have $q \leq p^{|\mathbf{A}|}$. Now, $2\alpha + |\mathbf{A}| \leq 2^\alpha + |\mathbf{A}| \leq |\mathbf{P}| + |\mathbf{A}| \leq |\mathbf{G}| + 1$, hence

$$(C_\alpha + 1)(q-1) < p^{2\alpha-1} p^{|\mathbf{A}|} \leq |\mathbf{G}|^{|\mathbf{G}|}.$$

Thus,

$$(C_\alpha + 1)(q-1)(\alpha+\beta) \leq |\mathbf{G}|^{|\mathbf{G}|} \log |\mathbf{G}|. \qquad \square$$

4. Equivalence

We prove Theorem 2 in this section.

Let $\mathbf{G} \simeq \mathbf{N} \rtimes \mathbf{A}$, where $\mathbf{N}$ is a finite nilpotent group and $\mathbf{A}$ is a finite Abelian group. 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 $S \approx T$ over $\mathbf{G}$ if and only if the group expression T' attains the identity element of $\mathbf{G}$ for every 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 equivalence $T' \approx \mathrm{id}$.

Let $\mathbf{P}_1, \dots, \mathbf{P}_m$ be the Sylow subgroups of $\mathbf{N}$. On the one hand, $\mathbf{N}$ is the direct product of $\mathbf{P}_1, \dots, \mathbf{P}_m$. On the other hand, $\mathbf{P}_1, \dots, \mathbf{P}_m$ are characteristic in the normal subgroup $\mathbf{N}$, thus $\mathbf{P}_1, \dots, \mathbf{P}_m$ are all normal in $\mathbf{G}$, as well. That is, the action of $\mathbf{A}$ over $\mathbf{N}$ is the direct product of the actions of $\mathbf{A}$ over $\mathbf{P}_1, \dots, \mathbf{P}_m$. In particular, $T' \approx \mathrm{id}$ holds over $\mathbf{G}$ if and only if for each $1 \leq i \leq m$ we have $T' \approx \mathrm{id}$ over $\mathbf{P}_i \rtimes \mathbf{A}$. Now, for some $1 \leq i \leq m$ we have that $T' \approx \mathrm{id}$ does *not* hold over $\mathbf{P}_i \rtimes \mathbf{A}$, if and only if $T' = g$ is solvable for some $g \in \mathbf{P}_i \rtimes \mathbf{A}$, $g \neq \mathrm{id}$. By Theorem 1, for some $1 \leq i \leq m$, $g \in \mathbf{P}_i \rtimes \mathbf{A}$, $g \neq \mathrm{id}$, one can check in

$$O(n^{|\mathbf{P}_i \rtimes A|^{|\mathbf{P}_i \rtimes A|} \log |\mathbf{P}_i \rtimes A|}) \leq O(n^{|\mathbf{G}|^{|\mathbf{G}|} \log |\mathbf{G}|})$$

time whether or not $T' = g$ is solvable. For each $1 \leq i \leq m$, $g \in \mathbf{P}_i \rtimes \mathbf{A}$, $g \neq \mathrm{id}$ checking whether or not $T' = g$ is solvable takes $O(m|\mathbf{G}|n^{|\mathbf{G}|^{|\mathbf{G}|} \log |\mathbf{G}|}) = O(n^{|\mathbf{G}|^{|\mathbf{G}|} \log |\mathbf{G}|})$ time, since neither m nor $\mathbf{G}$ depends on T', only on $\mathbf{G}$.

5. Final Remarks and Open Problems

By Lemma 4, the condition of Theorem 1 is equivalent to an easily verifiable condition, namely that $\mathbf{G}'$ is a p-group. In particular, this is the condition we check in the updated GAP [1, 5] computer program from [12] when we want to determine if Theorem 1 can be applied to a group. We could not find a similarly nice, equivalent version of the condition of Theorem 2, only stronger or weaker conditions.

Let $F(\mathbf{G})$ denote the Fitting subgroup of $\mathbf{G}$, that is the largest (unique) nilpotent normal subgroup in $\mathbf{G}$. Then the condition of Theorem 2 clearly implies $\mathbf{G}' \subseteq F(\mathbf{G})$, but is not equivalent to it. For example, if $\mathbf{Q}$ denotes the eight-element quaternion group, then $\mathbf{G} = \mathbf{Z}_3 \rtimes \mathbf{Q}$ has $\mathbf{G}' \simeq \mathbf{Z}_6$, $F(\mathbf{G}) \simeq \mathbf{Z}_{12}$ and $\mathbf{G}' \subseteq F(\mathbf{G})$, but $\mathbf{G}$ cannot be written as $\mathbf{N} \rtimes \mathbf{A}$ for some nilpotent group $\mathbf{N}$ and Abelian group $\mathbf{A}$.

Furthermore, the condition of Theorem 2 holds for all finite groups, for which the product of all *normal* Sylow subgroups contains $\mathbf{G}'$. Indeed, assume that for some positive k and for each $1 \leq i \leq k$ we have that $\mathbf{P}_i$ is a normal Sylow p_i-subgroup for some prime p_i such that the product $\mathbf{P}_1 \dots \mathbf{P}_k$ contains $\mathbf{G}'$. Let $\mathbf{N} = \mathbf{P}_1 \dots \mathbf{P}_k$, then $\mathbf{N}$ is normal, because it is a product of normal subgroups. Furthermore, $\mathbf{G}/\mathbf{N}$ is Abelian, because $\mathbf{G}' \subseteq \mathbf{N}$. Finally, $(|\mathbf{N}|, |\mathbf{G}/\mathbf{N}|) = 1$, therefore by the theorem of Schur and Zassenhaus [18, 9.1.2], there exists a subgroup $\mathbf{A}$ in $\mathbf{G}$ such that $\mathbf{G} \simeq \mathbf{N} \rtimes \mathbf{A}$. Since $\mathbf{A} \simeq \mathbf{G}/\mathbf{N}$ and $\mathbf{G}' \subseteq \mathbf{N}$, the subgroup $\mathbf{A}$ is Abelian.

However, this latter condition is not equivalent to the condition in Theorem 2, either. For example, $\mathbf{D}_{12} \simeq \mathbf{Z}_{12} \rtimes \mathbf{Z}_2$, $\mathbf{D}_{12}' \simeq \mathbf{Z}_{12}$, but the Sylow 2-subgroup is not normal in $\mathbf{D}_{12}$. As it is computationally exhaustive to check if a group can be written as a semidirect product of a nilpotent and an Abelian group, it would be useful to have an equivalent condition to that of Theorem 2.

Problem 1. Find an easily verifiable equivalent condition to that of Theorem 2.

Recall that (so far) the smallest size of a group with coNP-complete equivalence problem is 60. Amongst groups of order less than 60, there are five for which the complexity of the equivalence problem remains unknown. The smallest of them is the symmetric group $\mathbf{S}_4$ of order 24. The complexity of the equation solvability problem for $\mathbf{S}_4$ is unknown, either. Here, $\mathbf{S}_4$ can be written as a semidirect product in two different ways: $\mathbf{S}_4 \simeq \mathbf{A}_4 \rtimes \mathbf{Z}_2 \simeq \mathbf{V} \rtimes \mathbf{S}_3$, where $\mathbf{V}$ is the normal Klein subgroup in $\mathbf{S}_4$. Whether our method can somehow be extended to any of these semidirect products is unclear. The four other groups of order less than 60 with unknown complexity of the equivalence problem are all of order 48. Three of these are $\mathbf{S}_4 \times \mathbf{Z}_2, \mathbf{GL}(2, \mathbb{Z}_3),\ \mathbf{A}_4 \rtimes \mathbf{Z}_4$. The fourth is a group $\mathbf{G}$ that cannot be written as a semidirect product, whose commutator subgroup is $\mathbf{G}' \simeq \mathbf{SL}(2, \mathbb{Z}_3)$, and whose center is $Z(\mathbf{G}) \simeq \mathbf{Z}_2$ such that $\mathbf{G}/Z(\mathbf{G}) \simeq \mathbf{S}_4$.

Problem 2. Determine the complexity of the equivalence and equation solvability problems over the group $\mathbf{S}_4$.

There are 3 groups of order 24 for which the complexity of the equivalence problem is known, but the complexity of the equation solvability problem is unknown. The first is $\mathbf{D}_{12} \simeq \mathbf{Z}_{12} \rtimes \mathbf{Z}_2$, the other two are $\mathbf{Z}_3 \rtimes \mathbf{Q}$ and $(\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_3) \rtimes \mathbf{Z}_2$. The main obstacle in the case of $\mathbf{D}_{12}$ or $(\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_3) \rtimes \mathbf{Z}_2$ is that the normal subgroup is not a p-group, while in the case of $\mathbf{Z}_3 \rtimes \mathbf{Q}$ the main problem is that $\mathbf{Q}$ is not commutative.

Problem 3. Determine the complexity of the equation solvability problem over the groups $\mathbf{D}_{12}$, $\mathbf{Z}_3 \rtimes \mathbf{Q}$ and $(\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_3) \rtimes \mathbf{Z}_2$.

Overall, there are 35 groups of order less than 60 for which the complexity of the equation solvability problem is unknown. Among these are the three mentioned in Problem 3, and the five for which the complexity of the equivalence problem is unknown, as well. The complete list can be found on the website [12].

Acknowledgments

We would like to thank an anonymous referee for their helpful suggestions.

This research was supported by the National Research, Development and Innovation Fund of Hungary, financed under the K109185 and FK 124814 funding schemes. The first author was partially supported by the PRIMUS/SCI/12 project of the Charles University.

References

[1] E. Aichinger, F. Binder, J. Ecker, P. Mayr and C. Nöbauer, SONATA — system of near-rings and their applications, GAP package, Version 2.8 (2015), http://www.algebra.uni-linz.ac.at/Sonata/.

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

[3] A. Földvári, The complexity of the equation solvability problem over semipattern groups, *Internat. J. Algebra Comput.* **27**(2) (2017) 259–272.

[4] A. Földvári, The complexity of the equation solvability problem over nilpotent groups, *J. Algebra* **495** (2018) 289–303.

[5] The GAP Group, GAP — Groups, algorithms, and programming, version 4.9.3 (2018).

[6] M. Goldmann and A. Russell, The complexity of solving equations over finite groups, in *Proc. 14th Annual IEEE Conf. Computational Complexity*, Atlanta, GA, 1999, pp. 80–86.

[7] M. Goldmann and A. Russell, The complexity of solving equations over finite groups, *Inform. Comput.* **178** (2002) 253–262.

[8] P. Hall, A Contribution to the theory of groups of prime-power order, *Proc. London Math. Soc. (2)* **36** (1934) 29–95.

[9] P. Hall, *The Edmonton Notes on Nilpotent Groups*, Queen Mary College Mathematics Notes (Mathematics Department, Queen Mary College, London, 1969).

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

[11] G. Horváth, The complexity of the equivalence and equation solvability problems over meta-abelian groups, *J. Algebra* **433** (2015) 208–230.

[12] G. Horváth, Gap programs, http://math.unideb.hu/horvath-gabor/research.html (2018).

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

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

[15] G. Horváth and Cs. Szabó, Equivalence and equation solvability problems for the group A_4. *J. Pure Appl. Algebra* **216**(10) (2012) 2170–2176.

[16] C. R. Leedham-Green and L. H. Soicher, Symbolic collection using Deep Thought, *LMS J. Comput. Math.* **1** (1998) 9–24.

[17] B. R. MacDonald, *Finite Rings with Identity* (Marcel Dekker, 1974).

[18] D. J. S. Robinson. *A Course in the Theory of Groups*, Graduate Texts in Mathematics, Vol. 80, 2nd edn. (Springer-Verlag, New York, 1996).

[19] C. C. Sims, *Computation with Finitely Presented Groups*, Encyclopedia of Mathematics and Its Applications, Vol. 48 (Cambridge University Press, Cambridge, 1994).