Algebra Univers. (2021) 82:12

1420-8911/21/010001-13
published online January 14, 2021
https://doi.org/10.1007/s00012-020-00701-6

Algebra Universalis

Solving a fixed number of equations over finite groups

Philipp Nuspl

Abstract. We investigate the complexity of solving systems of polynomial equations over finite groups. In 1999 Goldmann and Russell showed NP-completeness of this problem for non-Abelian groups. We show that the problem can become tractable for some non-Abelian groups if we fix the number of equations. Recently, Földvári and Horváth showed that a single equation over groups which are semidirect products of a p-group with an Abelian group can be solved in polynomial time. We generalize this result and show that the same is true for systems with a fixed number of equations. This shows that for all groups for which the complexity of solving one equation has been proved to be in P so far, solving a fixed number of equations is also in P. Using the collecting procedure presented by Horváth and Szabó in 2006, we furthermore present a faster algorithm to solve systems of equations over groups of order pq.

Mathematics Subject Classification. 20F10, 13P15.

Keywords. Polynomial equations, Equation solvability, Computational complexity, Semidirect products.

1. Introduction

In the past two decades large efforts were made to understand the complexity of solving polynomial equations over finite groups. A polynomial over a group G is a product of variables, inverses of variables and elements of G. For a fixed finite group G the (*polynomial*) *equation solvability problem*—PolSat(G) for short—asks whether two polynomials r, t over G attain the same value for some evaluation of the variables in G. In [7] and [8] it was shown that for nilpotent groups G the problem PolSat(G) can be solved in polynomial time. Furthermore, it was shown that the problem PolSat(G) is NP-complete for non-solvable groups G. The result for nilpotent groups has been revisited several

Presented by B. Larose.
The research was supported by the Austrian Science Fund (FWF), P29931.

times using different approaches, e.g. in [12] and [5]. Some results are known for non-nilpotent solvable groups. There is, however, no complete classification for non-nilpotent solvable groups. In [16], it was shown that $\textsc{PolSat}(\mathbb{Z}_p \rtimes \mathbb{Z}_q) \in \mathrm{P}$ for primes p, q. Most of the previously known results were generalized in [6], where it was shown that $\textsc{PolSat}(P \rtimes A) \in \mathrm{P}$ for all p-groups P and Abelian groups A. These are the two tractability results which we generalize in Theorems 1.1 and 1.2 from a single equation to a fixed number of equations. One of the groups not covered by these results is the group S_4. A list of these groups of small order which are not covered by the known tractability results is given in [11].

It has been shown recently in [17] that, under the Exponential Time Hypothesis (ETH), the problem $\textsc{PolSat}(S_4)$ cannot be solved faster than in quasi-polynomial time. In particular, under the ETH it cannot be solved in polynomial time. Similar hardness-results have been shown in [19]: under the ETH the problem $\textsc{PolSat}(G)$ is not decidable in polynomial time if the group G has Fitting length at least four. The same result has been shown for certain groups with Fitting length three. Under a different open conjecture it has been shown in [3] that a quasi-polynomial time algorithm indeed exists for solvable groups.

The complexity of the (*polynomial*) *system equation solvability problem*—$\textsc{PolSysSat}(G)$ for short—was completely classified in [7] and [8]. In this problem it is checked whether a system $t_1 = r_1, \ldots, t_s = r_s$ for group polynomials t_l, r_l for $l = 1, \ldots, s$ has a solution. It was shown that $\textsc{PolSysSat}(A) \in \mathrm{P}$ for Abelian groups A and $\textsc{PolSysSat}(G) \in \mathrm{NPC}$ for non-Abelian groups G, i.e. a dichotomy holds for this problem.

The s-$\textsc{PolSysSat}$ problem asks whether a system of s many equations has a solution. This problem for general algebras is different from the problem for one equation and from the problem for systems. Namely, in [9] it was shown that $\textsc{PolSat}(L) \in \mathrm{P}$ for the two-element lattice $L = \langle \{0, 1\}, \wedge, \vee \rangle$ but 2-$\textsc{PolSysSat}(L) \in \mathrm{NPC}$. In [1] it was shown that s-$\textsc{PolSysSat}(G) \in \mathrm{P}$ for nilpotent groups G. Hence, any nilpotent non-Abelian group is a witness for the fact that the problem of solving systems in general becomes easier if we fix the number of equations.

In Section 3 we generalize Theorem 16 from [16] which states that $\textsc{PolSat}(G) \in \mathrm{P}$ for groups of order $|G| = pq$ for primes p, q. We measure the length $\|t\|$ of a polynomial t by the length of the string which defines it. Then our new version of the theorem can be formulated in the following way:

Theorem 1.1. *Let G be a finite group with $|G| = pq$ for primes $p \geq q$ and $s \in \mathbb{N}$ fixed. Then s-$\textsc{PolSysSat}(G) \in \mathrm{P}$. In particular, we can decide in time $\mathcal{O}(\max_{1 \leq l \leq s} \|t^{(l)}\|^{2(p-1)s})$ whether a given system $t^{(1)} = \cdots = t^{(s)} = 1$ has a solution.*

Theorem 1 from [6] states that for a finite group $G \cong P \rtimes A$ for a p-group P and Abelian group A we have $\textsc{PolSat}(G) \in \mathrm{P}$. In Section 4 we prove a generalized version and show that the same argument can be used for systems with a fixed number of equations.

Theorem 1.2. *Let $G \cong P \rtimes A$, where P is a finite p-group and A a finite Abelian group and $s \in \mathbb{N}$ fixed. Then s-PolSysSat$(G) \in$ P. In particular, we can decide in time $\mathcal{O}(\max_{1\le l\le s}\|t^{(l)}\|^{s|G|^{|G|}\log_2|G|})$ whether a given system $t^{(1)} = \cdots = t^{(s)} = 1$ has a solution.*

As a corollary of Theorem 1.2 we get:

Corollary 1.3. *Let $G \cong \mathbb{Z}_{2p^\alpha} \rtimes A$, where p is a prime, $\alpha \in \mathbb{N}$ and A is a finite Abelian group. Then s-PolSysSat$(G) \in$ P for all $s \in \mathbb{N}$.*

2. Preliminaries

A polynomial $t(x_1, \ldots, x_m)$ over a finite group G is a formal product of variables, their inverses and constants from G, i.e. $t(x_1, \ldots, x_m) = g_1 \cdots g_n$, with $g_i \in \{x_1, \ldots, x_m\} \cup \{x_1^{-1}, \ldots, x_m^{-1}\} \cup G$. The length of the polynomial is defined as $\|t\|{:=}n$. Sometimes we are going to use the word 'polynomial' also for the operation $t\colon G^m \to G$ defined by t, but this will never cause confusion, as it will be clear from the context. If a polynomial contains the inverse of a variable, say x_i^{-1}, then we can replace it with $x_i^{|G|-1}$. These replacements of inverses only increase the length linearly for a fixed group G. Hence, we can assume that a polynomial is given as a product of variables and group elements. Let r be a second polynomial over the group G, then the length of the equation

$$t(x_1, \ldots, x_m) = r(x_1, \ldots, x_m)$$

is defined as $\|t\| + \|r\|$. Furthermore, this equation has a solution if and only if $(tr^{-1})(x_1, \ldots, x_m) = 1$ has a solution. The length of this new equation only grows linearly. Hence, for studying the complexity we can assume that $r = 1$.

Let q be a prime power, let $\mathbb{F}_q$ be the finite field with q elements and let $\mathbb{F}_q[x_1, \ldots, x_n]$ be the ring of polynomials over $\mathbb{F}_q$. We denote the multiplicative group of the field by $\mathbb{F}_q^\times{:=}(\mathbb{F}_q{-}\{0\}, \cdot)$ and the function induced by a polynomial $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ by $f^{\mathbb{F}_q}$. A polynomial $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ is given in *expanded form* if f is given as

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

with $c_{s_1,\ldots,s_n} \in \mathbb{F}_q$, i.e. f is written as a sum of monomials with reduced exponents. Then we define the length of f as

$$\|f\|{:=} \sum_{c_{s_1,\ldots,s_n}\neq 0} 1 + s_1 + \cdots + s_n.$$

Solving equations over groups can, in many cases, be reduced in polynomial time to the problem of solving one or a system of equations over a finite field. Frequently, the polynomials in these equations over finite fields are given in expanded form. These solvability problems where the input is restricted to polynomials given in expanded form are called *sigma solvability problems* and we write e.g. PolSat$_\Sigma(\mathbb{F}_q)$. For general rings these problems were considered

for instance in [12]. If f, g are polynomials over $\mathbb{F}_q$, the equation $f = g$ has a solution if and only if $f - g = 0$ has a solution. Hence, we can assume that the right-hand sides of the equations are 0.

Additionally to the solvability problems we also consider the *sigma equivalence problem*, $\textsc{PolEqv}_\Sigma(\mathbb{F}_q)$. Here we are given two polynomials f, g over $\mathbb{F}_q$ and we want to decide whether they induce the same function on $\mathbb{F}_q$. We write $f \approx g$ in this case. Of course $f \approx g$ holds if and only if $f - g \approx 0$ holds, so we can again assume that the right-hand side is 0. This problem was considered for general rings in [13,15].

The following lemma shows that the sigma equivalence problem for finite fields can be solved in linear time with respect to the length of the input polynomial if the polynomial is given in expanded form. This is even true if some of the variables are restricted to the multiplicative subgroup $\mathbb{F}_q^\times$.

Lemma 2.1. *Let q be a prime power and $\mathbb{F}_q$ the finite field with q elements. Furthermore, let $f \in \mathbb{F}_q[x_1, \dots, x_n, y_1, \dots, y_m]$ be a polynomial given in expanded form. Then it can be decided in time $\mathcal{O}(\|f\|)$ whether $f^{\mathbb{F}_q}(s_1, \dots, s_n, u_1, \dots, u_m) = 0$ for all $s_1, \dots, s_n \in \mathbb{F}_q$ and $u_1, \dots, u_m \in \mathbb{F}_q^\times$. In particular, $\textsc{PolEqv}_\Sigma(\mathbb{F}_q) \in \mathrm{P}$.*

Proof. The polynomial $x^q - x = \prod_{s \in \mathbb{F}_q}(x - s)$ clearly vanishes for all evaluations of x from $\mathbb{F}_q$. Analogously, $y^{q-1} - 1 = \prod_{s \in \mathbb{F}_q^\times}(y - s)$ vanishes for all evaluations from $\mathbb{F}_q^\times$. We define the Gröbner basis

$$B := \{\, x_i^q - x_i \mid 1 \le i \le n \,\} \cup \left\{\, y_j^{q-1} - 1 \;\middle|\; 1 \le j \le m \right\}.$$

Then $f^{\mathbb{F}_q}(s_1, \dots, s_n, u_1, \dots, u_m) = 0$ for all $s_1, \dots, s_n \in \mathbb{F}_q, u_1, \dots, u_m \in \mathbb{F}_q^\times$ if and only if $f \in \mathrm{Ideal}_{\mathbb{F}_q[x_1,\dots,x_n,y_1,\dots,y_m]}(B)$: clearly, if f is in the ideal generated by B, the statement holds by the construction of B. The other implication follows from the Combinatorial Nullstellensatz [2, Theorem 1.1].

To check if f is contained in the ideal generated by B, we need to check whether f reduces to 0 modulo B. Reduction modulo B is particularly easy as we only need to reduce all the exponents. This reduction and collection of monomials can be done in time $\mathcal{O}(\|f\|)$ as f is given in expanded form. □

Let $n, \beta, n_1, \dots, n_\beta \in \mathbb{N}$ and let $S_1, \dots, S_\beta$ be subgroups of $\mathbb{F}_q^\times$. Furthermore, let $X = \{x_1, \dots, x_n\}$ and $Y_j = \{y_{j,1}, \dots, y_{j,n_j}\}$ denote pairwise disjoint sets of variables for $j = 1, \dots, \beta$. Additionally, let $f, g \in \mathbb{F}_q[X, Y_1, \dots, Y_\beta]$ be polynomials in expanded form. We then say (following the notation from [4]) that

$$f|_{\mathbb{F}_q, S_1, \dots, S_\beta} = g|_{\mathbb{F}_q, S_1, \dots, S_\beta}$$

is solvable if there exist field elements $s_1, \dots, s_n \in \mathbb{F}_q$ and $s_{j,1}, \dots, s_{j,n_j} \in S_j$ for $j = 1, \dots, \beta$ such that

$$\begin{aligned} &f^{\mathbb{F}_q}(s_1, \dots, s_n, s_{1,1}, \dots, s_{1,n_1}, \dots, s_{\beta,1}, \dots, s_{\beta,n_\beta}) \\ &\quad = g^{\mathbb{F}_q}(s_1, \dots, s_n, s_{1,1}, \dots, s_{1,n_1}, \dots, s_{\beta,1}, \dots, s_{\beta,n_\beta}). \end{aligned}$$

Analogously, we say that

$$f|_{\mathbb{F}_q,S_1,\dots,S_\beta} \approx g|_{\mathbb{F}_q,S_1,\dots,S_\beta}$$

holds if for all $s_1,\dots,s_n \in \mathbb{F}_q$ and $s_{j,1},\dots,s_{j,n_j} \in S_j$ for $j = 1,\dots,\beta$ we have

$$\begin{aligned} &f^{\mathbb{F}_q}(s_1,\dots,s_n,s_{1,1},\dots,s_{1,n_1},\dots,s_{\beta,1},\dots,s_{\beta,n_\beta}) \\ &\quad = g^{\mathbb{F}_q}(s_1,\dots,s_n,s_{1,1},\dots,s_{1,n_1},\dots,s_{\beta,1},\dots,s_{\beta,n_\beta}). \end{aligned}$$

The following lemma appears as a part of a proof in [14, p. 221]. We include a different self-contained proof following an approach from [16] and using Lemma 2.1.

Lemma 2.2 [14]. *Let q be a prime power and $\mathbb{F}_q$ the finite field with q elements. Let $S_1,\dots,S_\beta$ be subgroups of $\mathbb{F}_q^\times$. Furthermore, let $X = \{x_1,\dots,x_n\}$ and $Y_j = \{y_{j,1},\dots,y_{j,n_j}\}$ denote pairwise disjoint sets of variables for every $j = 1,\dots,\beta$. Let $f_1,\dots,f_s \in \mathbb{F}_q[X,Y_1,\dots,Y_\beta]$ be polynomials given in expanded form. Then it can be decided in time*

$$\mathcal{O}\left(\max_{1\le i\le s}\|f_i\|^{(q-1)s}\right)$$

whether the system of equations

$$\begin{aligned} f_1|_{\mathbb{F}_q,S_1,\dots,S_\beta} &= 0 \\ &\vdots \\ f_s|_{\mathbb{F}_q,S_1,\dots,S_\beta} &= 0 \end{aligned} \tag{2.1}$$

has a solution. In particular, $\textsc{PolSat}_\Sigma(\mathbb{F}_q) \in \mathrm{P}$ *and* s-$\textsc{PolSysSat}_\Sigma(\mathbb{F}_q) \in \mathrm{P}$ *for fixed* $s \in \mathbb{N}$.

Proof. Since $\mathbb{F}_q^\times$ is cyclic, we can write $\mathbb{F}_q^\times = \langle a\rangle$ for some $a \in \mathbb{F}_q^\times$. Then $S_j = \langle a^{l_j}\rangle = \{y^{l_j} \mid y \in \mathbb{F}_q^\times\}$ for some $l_j \in \{1,\dots,q-1\}$ for $j = 1,\dots,\beta$. Now, let

$$\tilde{f}_i := f_i\left(x_1,\dots,x_n,y_{1,1}^{l_1},\dots,y_{1,n_1}^{l_1},\dots,y_{\beta,1}^{l_\beta},\dots,y_{\beta,n_\beta}^{l_\beta}\right)$$

be polynomials in expanded form. Then (2.1) has a solution if and only if the system

$$\begin{aligned} \tilde{f}_1|_{\mathbb{F}_q,\mathbb{F}_q^\times,\dots,\mathbb{F}_q^\times} &= 0 \\ &\vdots \\ \tilde{f}_s|_{\mathbb{F}_q,\mathbb{F}_q^\times,\dots,\mathbb{F}_q^\times} &= 0 \end{aligned} \tag{2.2}$$

has a solution. These polynomials $\tilde{f}_i$ can be computed in time $\mathcal{O}(\|f_i\|)$ and we have $\|\tilde{f}_i\| = \mathcal{O}(\|f_i\|)$. Let f be the expanded form of the product

$$f := \prod_{i=1}^{s}\left(1-(\tilde{f}_i)^{q-1}\right).$$

Then for fixed s, the polynomial f can be computed in polynomial time from the $\tilde{f}_i$ and we have $\|f\| = \mathcal{O}(\max_{1\le i\le s}\|f_i\|^{(q-1)s})$. First, suppose the system

(2.2) has no solution. Then for all $s_1, \dots, s_n \in \mathbb{F}_q$ and $s_{1,1}, \dots, s_{\beta,n_\beta} \in \mathbb{F}_q^\times$ there exists an $i \in \{1, \dots, s\}$ such that $\tilde{f}_i^{\mathbb{F}_q}(s_1, \dots, s_n, s_{1,1}, \dots, s_{\beta,n_\beta}) \neq 0$. Therefore, by the definition of f,

$$f(X, Y_1, \dots, Y_\beta)|_{\mathbb{F}_q, \mathbb{F}_q^\times, \dots, \mathbb{F}_q^\times} \approx 0 \tag{2.3}$$

holds. Conversely, if (2.3) holds, then (2.2) has no solution. Hence, the system (2.1) has no solution if and only if (2.3) holds. The latter equation can be checked in time $\mathcal{O}(\|f\|)$ by Lemma 2.1. □

3. Proof of Theorem 1.1

In order to prove Theorem 1.1 we are going to reduce solving equations over G with $|G| = pq$ for primes p, q to the sigma solvability problem over the finite fields $\mathbb{Z}_p$ and $\mathbb{Z}_q$. We are going to write the operations of G multiplicatively whereas the additive group of a field $\mathbb{Z}_p$ is written additively as $(\mathbb{Z}_p, +)$.

Proof of Theorem 1.1. Let G be a finite group with $|G| = pq$ for primes $p \geq q$. If $p = q$ or $q \nmid p-1$, then G is Abelian and the result follows from [7]. Otherwise, if $q \mid p - 1$, we can write $G = \mathbb{Z}_p \rtimes \mathbb{Z}_q$. This semidirect product is defined by some homomorphism

$$\psi \colon (\mathbb{Z}_q, +) \to (\mathbb{Z}_p - \{0\}, \cdot) = \mathbb{Z}_p^\times \cong \mathrm{Aut}(\mathbb{Z}_p).$$

Then the product of $(a_1, b_1), (a_2, b_2) \in G$ is given by

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 + \psi(b_1) \cdot a_2, b_1 + b_2).$$

For polynomials $t^{(1)}, \dots, t^{(s)}$ we want to decide whether the system

$$\begin{aligned} t^{(1)} &= (a_1^{(1)}, b_1^{(1)}) \cdot (a_2^{(1)}, b_2^{(1)}) \cdots (a_{n_1}^{(1)}, b_{n_1}^{(1)}) = (0, 0) \\ &\vdots \\ t^{(s)} &= (a_1^{(s)}, b_1^{(s)}) \cdot (a_2^{(s)}, b_2^{(s)}) \cdots (a_{n_s}^{(s)}, b_{n_s}^{(s)}) = (0, 0) \end{aligned}$$

has a solution. Here, the $a_i^{(l)}$ are either constants or variables over $\mathbb{Z}_p$ and the $b_i^{(l)}$ are either constants or variables over $\mathbb{Z}_q$. This system can be rewritten using the definition of the semidirect product to get

$$\sum_{i=1}^{n_1} a_i^{(1)} \prod_{j=1}^{i-1} \psi(b_j^{(1)}) = \cdots = \sum_{i=1}^{n_s} a_i^{(s)} \prod_{j=1}^{i-1} \psi(b_j^{(s)}) = 0 \tag{3.1a}$$

$$\sum_{i=1}^{n_1} b_i^{(1)} = \cdots = \sum_{i=1}^{n_s} b_i^{(s)} = 0 \tag{3.1b}$$

where the first part (3.1a) is a system of s equations over $\mathbb{Z}_p$ and the second part (3.1b) is a system of s equations over $\mathbb{Z}_q$. This technique was introduced in [16] as *collecting procedure*. The system (3.1b) is a linear system over a finite field. We denote the variables of this second part by $y_1, \dots, y_n$. This system over $\mathbb{Z}_q$ can be solved using Gaussian elimination. If there is no solution, then the overall system does not have a solution. If it has at least one solution,

we can write the solutions parametrized by some variables $z_1, \dots, z_k$ over $\mathbb{Z}_q$, i.e. $y_i = \sum_{j=1}^{k} c_{i,j} z_j + d_i$ for all $i = 1, \dots, n$ with $c_{i,j}, d_i \in \mathbb{Z}_q$. Then $\psi(y_i) = \psi(d_i) \prod_{j=1}^{k} \psi(z_j)^{c_{i,j}}$ which we can substitute in the first system (3.1a). Hence, the system (3.1a) is now a system of s polynomial equations over $\mathbb{Z}_p$ given in expanded form with some variables $a_i^{(l)}$ over $\mathbb{Z}_p$ and some variables $\psi(z_j)$ over $\mathrm{Im}(\psi)$. As $\mathrm{Im}(\psi)$ is a subgroup of $\mathbb{Z}_p^\times$, we can apply Lemma 2.2.

The l-th equation in (3.1a) contains $\|t^{(l)}\|$ monomials. Each monomial has at most length $n(p-1)+1$ where n is the number of variables in the equation. Hence, the length of every polynomial in equation (3.1a) after all replacements is at most $\|t^{(l)}\| n(p-1)$. Since $n \leq s \max_{1 \leq l \leq s} \|t^{(l)}\|$, we can decide with Lemma 2.2 in time

$$\mathcal{O}\left(\max_{1 \leq l \leq s} (\|t^{(l)}\|^2 s(p-1))^{(p-1)s} \right)$$

whether a given system has a solution. For fixed s this is

$$\mathcal{O}\left(\max_{1 \leq l \leq s} \|t^{(l)}\|^{2(p-1)s} \right).$$

This dominates the complexity of applying Gaussian elimination to the second part (3.1b). Note that for general systems—i.e. s is not fixed—we see that this algorithm has exponential time. □

4. Proof of Theorem 1.2

Let $G = P \rtimes A$, where P is a finite p-group of order $|P| = p^\alpha$ for $\alpha \in \mathbb{N}$ and A is a finite Abelian group. Lemma 4 in [6] shows that these are exactly the finite groups where the commutator subgroup is a p-group. Furthermore, one can choose P and A in such a way that $p \nmid |A|$. In [6] it was also shown that there exists a subnormal series

$$\{e\} = N_0 \triangleleft N_1 \triangleleft \cdots \triangleleft N_\alpha = P = M_0 \triangleleft M_1 \triangleleft \cdots \triangleleft M_\beta = G$$

with $N_i \triangleleft P$ and $N_i / N_{i-1} \cong \mathbb{Z}_p$ for $i = 1, \dots, \alpha$. Moreover, $M_j \triangleleft G$ and $M_j / M_{j-1} \cong \mathbb{Z}_{p_j}$ for primes p_j and $j = 1, \dots, \beta$. We can fix a polycyclic sequence $\mathcal{B} = (b_1, \dots, b_\alpha, c_1, \dots, c_\beta)$, i.e. $b_i \in N_i - N_{i-1}$ for $i = 1, \dots, \alpha$ and $c_j \in M_j - M_{j-1}$ for $j = 1, \dots, \beta$. Then for every element $g \in G$ there exists a unique sequence $(u_1, \dots, u_\alpha, v_1, \dots, v_\beta)$ with $u_i \in \{0, \dots, p-1\}$ for $i = 1, \dots, \alpha$ and $v_j \in \{0, \dots, p_j - 1\}$ for $j = 1, \dots, \beta$ such that $g = b_1^{u_1} \cdots b_\alpha^{u_\alpha} c_1^{v_1} \cdots c_\beta^{v_\beta}$, cf. [10, Lemma 8.3]. The tuple $(u_1, \dots, u_\alpha, v_1, \dots, v_\beta)$ is called the *exponent vector of* g and the expression $b_1^{u_1} \cdots b_\alpha^{u_\alpha} c_1^{v_1} \cdots c_\beta^{v_\beta}$ the *normal form of* g (with respect to the fixed polycyclic sequence $\mathcal{B}$). In [6] it was shown that there exists a finite field $\mathbb{F}_q$ with characteristic p and $q \leq p^{|A|}$ such that the multiplicative group $\mathbb{F}_q^\times$ contains a cyclic subgroup S_j of order p_j for all $j = 1, \dots, \beta$. Such a field $\mathbb{F}_q$ is called a *base field* of the group G. We denote the respective isomorphisms by $\varphi_j \colon \mathbb{Z}_{p_j} \to S_j$ for $j = 1, \dots, \beta$.

The following lemma from [6] shows how we can reduce multiplication in G to evaluation of polynomials over $\mathbb{F}_q$. In particular, it shows that we can find polynomials over $\mathbb{F}_q$ which describe the exponent vector of the product $g_1 \cdots g_n$ for arbitrary $g_1, \ldots, g_n \in G$. These polynomials can be computed in expanded form in polynomial time and the number of variables in the monomials are bounded. This can be used to reduce solving an equation over G to solving a fixed number of equations over $\mathbb{F}_q$.

Lemma 4.1 [6]. *For a prime p let P be a p-group of order p^α. Let A be an Abelian group with $p \nmid |A|$ and consider the group $G = P \rtimes A$. Let $\mathcal{B} = (b_1, \ldots, b_\alpha, c_1, \ldots, c_\beta)$ be a polycyclic sequence of G. Let $\mathbb{F}_q$ denote a base field of G and $\varphi_1, \ldots, \varphi_\beta$ the isomorphisms which embed $\mathbb{Z}_{p_j}$ into $\mathbb{F}_q^\times$. For an arbitrary positive integer n let*

$$X_{n,\alpha} = \{ x_{k,i} \mid 1 \leq k \leq n, 1 \leq i \leq \alpha \}$$
$$Y_{n-1,\beta} = \{ y_{k,j} \mid 1 \leq k \leq n-1, 1 \leq j \leq \beta \}$$

be disjoint sets of variables. Then there exist $f_1, \ldots, f_\alpha \in \mathbb{F}_q[X_{n,\alpha}, Y_{n-1,\beta}]$ given in expanded form such that for arbitrary elements $h_1, \ldots, h_n \in P$ and $a_1, \ldots, a_n \in A$ with normal forms

$$h_k = b_1^{u_{k,1}} \cdots b_\alpha^{u_{k,\alpha}} c_1^0 \cdots c_\beta^0,$$
$$a_k = b_1^0 \cdots b_\alpha^0 c_1^{v_{k,1}} \cdots c_\beta^{v_{k,\beta}}$$

for $k = 1, \ldots, n$, the normal form of the product $h_1 a_1 \cdots h_n a_n$ is

$$h_1 a_1 \cdots h_n a_n = b_1^{f_1^{\mathbb{F}_q}(u_{1,1},\ldots,u_{n,\alpha},\varphi_1(v_{1,1}),\ldots,\varphi_\beta(v_{n-1,\beta}))} \cdots b_\alpha^{f_\alpha^{\mathbb{F}_q}(u_{1,1},\ldots,u_{n,\alpha},\varphi_1(v_{1,1}),\ldots,\varphi_\beta(v_{n-1,\beta}))} c_1^{v_{1,1}+\cdots+v_{n,1}} \cdots c_\beta^{v_{1,\beta}+\cdots+v_{n,\beta}}.$$

Furthermore, with $C_\alpha := (2p-2)^{\alpha-1}$ each monomial of f_i for $i = 1, \ldots, \alpha$ contains at most $\alpha^{C_\alpha}(q-1)^{C_\alpha}$ variables from $X_{n,\alpha}$, each polynomial f_i can be furthermore computed in time $\mathcal{O}(n^{C_\alpha+1})$ and $\|f_i\| = \mathcal{O}(n^{C_\alpha+1})$.

Proof of Theorem 1.2. We follow the proofs from Lemma 7 and Theorem 1 in [6] and point out the differences which occur when we consider s equations instead of one. We consider a system

$$t^{(1)} := t_1^{(1)} \cdots t_{n_1}^{(1)} = 1$$
$$\vdots$$
$$t^{(s)} := t_1^{(s)} \cdots t_{n_s}^{(s)} = 1$$

of length $n := \sum_{l=1}^{s} n_l$ where all the $t_k^{(l)}$ for $l = 1, \ldots, s$ and $k = 1, \ldots, n_l$ are either variables over G or elements (i.e. constants) in G. We fix a polycyclic sequence $\mathcal{B} = (b_1, \ldots, b_\alpha, c_1, \ldots, c_\beta)$ of G and a base field $\mathbb{F}_q$ of characteristic p. First, we compute the normal form of all elements $t \in \{t_1^{(1)}, \ldots, t_{n_s}^{(s)}\}$: if $t_k^{(l)}$ is

a constant in the group, we can replace it with its respective normal form. If $t_k^{(l)}$ is a variable, we replace it with

$$t_k^{(l)} = b_1^{x_{k,1}^{(l)}} \dots b_\alpha^{x_{k,\alpha}^{(l)}} c_1^{z_{k,1}^{(l)}} \dots c_\beta^{z_{k,\beta}^{(l)}},$$

where $x_{k,i}^{(l)}$ are variables over $\mathbb{Z}_p$ and $z_{k,j}^{(l)}$ are variables over $\mathbb{Z}_{p_j}$ for $l = 1, \dots, s$, $k = 1, \dots, n_l$, $i = 1, \dots, \alpha$ and $j = 1, \dots, \beta$. We write $y_{k,j}^{(l)} := \varphi_j(z_{k,j}^{(l)})$. Then these $y_{k,j}^{(l)}$ are variables over S_j. Replacing all t with their normal form and creating all variables $x_{k,i}^{(l)}, y_{k,j}^{(l)}, z_{k,j}^{(l)}$ can be done in time $\mathcal{O}(n)$.

Now, for every $l = 1, \dots, s$ we define two sets of variables

$$X^{(l)} := \left\{ x_{k,i}^{(l)} \mid 1 \le k \le n_l, 1 \le i \le \alpha \right\}$$
$$Y^{(l)} := \left\{ y_{k,j}^{(l)} \mid 1 \le k \le n_l - 1, 1 \le j \le \beta \right\}$$

where we identify $x_{k,i}^{(l)}$ with $x_{\tilde{k},\tilde{i}}^{(\tilde{l})}$ if and only if $i = \tilde{i}$ and $t_k^{(l)}$ and $t_{\tilde{k}}^{(\tilde{l})}$ are the same variables over G and analogously for $y_{k,j}^{(l)}$. We furthermore write

$$Z^{(l)} := \left\{ z_{k,j}^{(l)} \mid 1 \le k \le n_l, 1 \le j \le \beta \right\}.$$

Now, applying Lemma 4.1 on every group polynomial $t^{(l)}$ yields polynomials $f_1^{(l)}, \dots, f_\alpha^{(l)} \in \mathbb{F}_q[X^{(l)}, Y^{(l)}]$ such that

$$t^{(l)} = b_1^{f_1^{(l)}(X^{(l)}, Y^{(l)})} \cdots b_\alpha^{f_\alpha^{(l)}(X^{(l)}, Y^{(l)})} c_1^{g_1^{(l)}(Z^{(l)})} \cdots c_\beta^{g_\beta^{(l)}(Z^{(l)})} \tag{4.1}$$

for all $l = 1, \dots, s$ where the polynomials $g_j^{(l)}$ are of the form

$$g_j^{(l)} := z_{1,j}^{(l)} + \dots + z_{n_l,j}^{(l)} \in \mathbb{Z}_{p_j}[Z^{(l)}].$$

Computing these polynomials $f_i^{(l)}, g_j^{(l)}$ in expanded form can be done with Lemma 4.1 in time $\mathcal{O}(\sum_{l=1}^{s} n_l^{C_\alpha+1}) = \mathcal{O}(\max_{1 \le l \le s} s\, n_l^{C_\alpha+1})$ and we have $\|f_i^{(l)}\| = \mathcal{O}(n_l^{C_\alpha+1})$.

Since $1 = b_1^0 \cdots b_\alpha^0 c_1^0 \cdots c_\beta^0$ and by the uniqueness of the normal form, the equations (4.1) yield the system

$$f_1^{(1)}\left(X^{(1)}, Y^{(1)}\right)|_{\mathbb{Z}_p, S_1, \dots, S_\beta} = \dots = f_1^{(s)}\left(X^{(s)}, Y^{(s)}\right)|_{\mathbb{Z}_p, S_1, \dots, S_\beta} = 0$$
$$\vdots \tag{4.2a}$$
$$f_\alpha^{(1)}\left(X^{(1)}, Y^{(1)}\right)|_{\mathbb{Z}_p, S_1, \dots, S_\beta} = \dots = f_\alpha^{(s)}\left(X^{(s)}, Y^{(s)}\right)|_{\mathbb{Z}_p, S_1, \dots, S_\beta} = 0$$
$$g_1^{(1)}\left(Z^{(1)}\right) = \dots = g_1^{(s)}\left(Z^{(s)}\right) = 0$$
$$\vdots \tag{4.2b}$$
$$g_\beta^{(1)}\left(Z^{(1)}\right) = \dots = g_\beta^{(s)}\left(Z^{(s)}\right) = 0.$$

Now, (4.2a) is a system of $s\alpha$ many equations over $\mathbb{F}_q$ and (4.2b) a system of s many equations over $\mathbb{Z}_{p_j}$ for every $j = 1, \ldots, \beta$. We define $h_j^{(l)} := y_{1,j}^{(l)} \cdots y_{n_j,j}^{(l)}$. Then $g_j^{(l)}\left(Z^{(l)}\right) = 0$ over $\mathbb{Z}_{p_j}$ if and only if $h_j^{(l)}\left(Y^{(l)}\right)|_{S_j} = 1$ over $\mathbb{F}_q$. Hence, we can translate the system (4.2b) into equations over $\mathbb{F}_q$. The variables in $X^{(l)}$ are over $\mathbb{Z}_p$. Since every function over a finite field can be written as a polynomial, we have a polynomial $\pi \in \mathbb{F}_q[x]$ given in expanded form with $\mathrm{Im}(\pi) = \mathbb{Z}_p \subseteq \mathbb{F}_q$. We can now replace every $x_{k,i}^{(l)}$ with $\pi(x_{k,i}^{(l)})$ in $f_i^{(l)}$. Because of Lemma 4.1 the monomials in $f_i^{(l)}$ contain at most $\alpha^{C_\alpha}(q-1)^{C_\alpha}$ number of variables of $X_{n,\alpha}$. Then, since the length of π only depends on the group, we have

$$\|\tilde{f}_i^{(l)}\| \leq \|f_i^{(l)}\| \cdot \|\pi\|^{\alpha^{C_\alpha}(q-1)^{C_\alpha}} = \mathcal{O}(\|t^{(l)}\|^{C_\alpha+1})$$

and we can compute the expanded form $\tilde{f}_i^{(l)}$ of the new polynomials in time $\mathcal{O}(\max_{1\leq l\leq s} s\, n_l^{C_\alpha+1})$. We now have the system

$$\begin{aligned}
\tilde{f}_1^{(1)}\left(X^{(1)}, Y^{(1)}\right)|_{\mathbb{F}_q,S_1,\ldots,S_\beta} = \cdots = \tilde{f}_1^{(s)}\left(X^{(s)}, Y^{(s)}\right)|_{\mathbb{F}_q,S_1,\ldots,S_\beta} = 0 \\
\vdots \\
\tilde{f}_\alpha^{(1)}\left(X^{(1)}, Y^{(1)}\right)|_{\mathbb{F}_q,S_1,\ldots,S_\beta} = \cdots = \tilde{f}_\alpha^{(s)}\left(X^{(s)}, Y^{(s)}\right)|_{\mathbb{F}_q,S_1,\ldots,S_\beta} = 0 \\
h_1^{(1)}\left(Y^{(1)}\right)|_{S_1} - 1 = \cdots = h_1^{(s)}\left(Y^{(s)}\right)|_{S_1} - 1 = 0 \\
\vdots \\
h_\beta^{(1)}\left(Y^{(1)}\right)|_{S_\beta} - 1 = \cdots = h_\beta^{(s)}\left(Y^{(s)}\right)|_{S_\beta} - 1 = 0
\end{aligned}$$

which we can solve in time

$$\mathcal{O}\left(\max_{1\leq l\leq s} n_l^{s(C_\alpha+1)(q-1)(\alpha+\beta)}\right)$$

because of Lemma 2.2. This also dominates the time complexity of the rewriting steps. Now, we adopt the argument from the proof of Theorem 1 in [6] to show that

$$(C_\alpha + 1)(q-1)(\alpha+\beta) \leq |G|^{|G|} \log_2 |G|.$$

Since $|G| = p^\alpha p_1 \cdots p_\beta$ for primes $p, p_1, \ldots, p_\beta$, we have

$$\log_2 |G| = \alpha \log_2(p) + \sum_{j=1}^{\beta} \log_2(p_j) \geq \alpha + \beta$$

and

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

Furthermore, as $q \leq p^{|A|}$ we have

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

If $|A| = 1$, then

$$p^{2\alpha+|A|-1} = p^{2\alpha} \leq (p^\alpha)^{p^\alpha} = |G|^{|G|}.$$

Otherwise, we have $|P| + |A| \leq |P| \cdot |A| = |G|$ and

$$p^{2\alpha+|A|-1} \leq p^{2^\alpha+|A|} \leq p^{|P|+|A|} \leq |G|^{|G|}.$$

Therefore, we have $(C_\alpha+1)(q-1)(\alpha+\beta) \leq |G|^{|G|}\log_2|G|$. Hence, in total we can check in time $\mathcal{O}(\max_{1\leq l\leq s}\|t^{(l)}\|^{s|G|^{|G|}\log_2|G|})$ whether a given system has a solution. □

Proof of Corollary 1.3. If $p = 2$, then $\mathbb{Z}_{2p^\alpha}$ is a p-group and we can apply Theorem 1.2 directly. So let $p \neq 2$. Then we have $\mathbb{Z}_{2p^\alpha} = \mathbb{Z}_2 \times \mathbb{Z}_{p^\alpha}$. Automorphisms on $\mathbb{Z}_2 \times \mathbb{Z}_{p^\alpha}$ act identically on $\mathbb{Z}_2$ and as an arbitrary automorphism on the second part $\mathbb{Z}_{p^\alpha}$, cf. [18]. Hence,

$$(\mathbb{Z}_2 \times \mathbb{Z}_{p^\alpha}) \rtimes A \cong \mathbb{Z}_2 \times (\mathbb{Z}_{p^\alpha} \rtimes A).$$

Therefore, if we have a system over G, we can separately solve a system over $\mathbb{Z}_2$ and a system over $\mathbb{Z}_{p^\alpha} \rtimes A$. We can solve entire systems over $\mathbb{Z}_2$ using Gaussian elimination. In particular, we can check whether s given equations have a solution. For the second part we can apply Theorem 1.2 and can check whether there is a solution in polynomial time as well. □

Acknowledgements

The author thanks Erhard Aichinger for introducing him to this problem and for many helpful discussions. Furthermore, the author thanks the anonymous referees for many thoughtful remarks.

Funding Open Access funding provided by Johannes Kepler University Linz.

References

[1] Aichinger, E.: Solving systems of equations in supernilpotent algebras. In: 44th International Symposium on Mathematical Foundations of Computer Science (MFCS 2019), Leibniz International Proceedings in Informatics (LIPIcs), vol. 138, pp. 72:1–72:9 (2019)

[2] Alon, N.: Combinatorial Nullstellensatz. Combin. Probab. Comput. **8**(1–2), 7–29 (1999)

[3] Barrington, D.M., McKenzie, P., Moore, C., Tesson, P., Thérien, D.: Equation satisfiability and program satisfiability for finite monoids. Math. Found. Comput. Sci. **2000**, 172–181 (2000)

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

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

[6] Földvári, A., Horváth, G.: The complexity of the equation solvability and equivalence problems over finite groups. Int. J. Algebra Comput. **20**, 20 (2019)

[7] Goldmann, M., Russell, A.: The complexity of solving equations over finite groups. In: Proceedings of Fourteenth Annual IEEE Conference on Computational Complexity, pp. 80–86 (1999)

[8] Goldmann, M., Russell, A.: The complexity of solving equations over finite groups. Inform. Comput. **178**(1), 253–262 (2002)

[9] Gorazd, T.A., Krzaczkowski, J.: The complexity of problems connected with two-element algebras. Rep. Math. Logic **2011**, 46 (2011)

[10] Holt, D.F., Eick, B., O'Brien, E.A.: Handbook of Computational Group Theory. Discrete Mathematics and Its Applications. CRC Press, New York (2005)

[11] Horváth, G.: IdGroup and StructureDescription for groups of size <384 with unknown equation solvability complexity. http://math.unideb.hu/media/horvath-gabor/complexities/SATUnknown.txt. Accessed 29 Oct (2020)

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

[13] Horváth, G.: The complexity of the equivalence problem over finite rings. Glasg. Math. J. **54**, 20 (2012)

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

[15] Horváth, G., Lawrence, J., Willard, R.: The complexity of the equation solvability problem over finite rings. Preprint (2017)

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

[17] Idziak, P.M., Krzaczkowski, J., Kawałek, P.: Intermediate problems in modular circuits satisfiability. In: Proceedings of the 35th Annual ACM/IEEE Symposium on Logic in Computer Science, LICS '20, pp. 578–590. Association for Computing Machinery (2020)

[18] Rotman, J.J.: An Introduction to the Theory of Groups. Graduate Texts in Mathematics. Springer, New York (1999)

[19] Weiß, A.: Hardness of equations over finite solvable groups under the Exponential Time Hypothesis. In: 47th International Colloquium on Automata, Languages, and Programming (ICALP 2020), Leibniz International Proceedings in Informatics (LIPIcs), vol. 168, pp. 102:1–102:19 (2020)

Philipp Nuspl
Institute for Algebra
Johannes Kepler University Linz
4040 Linz
Austria
e-mail: philipp.nuspl@jku.at

Received: 2 June 2020.
Accepted: 19 December 2020.