THE COMPLEXITY OF THE EQUIVALENCE AND EQUATION SOLVABILITY PROBLEMS OVER META-ABELIAN GROUPS

GÁBOR HORVÁTH

Abstract. We provide polynomial time algorithms for deciding equation solvability and identity checking over groups that are semidirect products of two finite Abelian groups. Our main method is to reduce these problems to the sigma equation solvability and sigma equivalence problems over modules for commutative unital rings.

1. Introduction

Investigations into the algorithmic aspects of the equivalence problem for various finite algebraic structures commenced in the early 1990s. The *equivalence problem* for a finite ring $\mathcal{R}$ asks whether or not two polynomials p and q are equivalent over $\mathcal{R}$ (denoted by $\mathcal{R} \models p \approx q$), i.e. if p and q determine the same function over $\mathcal{R}$. The *equation solvability problem* is one of the oldest problems of algebra: it asks whether or not two expressions p and q can attain the same value for some substitution over a finite ring $\mathcal{R}$, i.e. if the equation $p = q$ can be solved over $\mathcal{R}$. Note, that these problems usually have a 'term' version, as well, where the input polynomials cannot contain constants from the ring $\mathcal{R}$. In this paper we deal with these problems for which the inputs are polynomials, but the term versions of our theorems follow from the proofs, as well. From now on, we refer to these problems as the equivalence problem and the equation solvability problem.

First Hunt and Stearnes [19] investigated the equivalence problem for finite commutative rings. Later Burris and Lawrence [3] generalized

Date: March 30, 2015.

2010 *Mathematics Subject Classification.* 20F10, 13M10, 20F70, 68Q17.

Key words and phrases. finite meta-Abelian groups, equivalence, equation solvability, computational complexity, polynomial time algorithm, module equivalence, module equation solvability.

Institute of Mathematics, University of Debrecen, Pf. 12, Debrecen, 4010, Hungary

Phone: +36 52 512900/22798

E-mail address: ghorvath@science.unideb.hu.

their result to non-commutative rings, and established a dichotomy theorem for rings: for finite nilpotent rings the equivalence problem can be solved in polynomial time in the length of the two input polynomials, and for non-nilpotent rings the equivalence problem is coNP-complete. Similar result can be proved for the equation solvability problem: for non-nilpotent rings the NP-completeness follows from the argument of Burris and Lawrence, for nilpotent rings the equation solvability problem is in P [12].

The proof of Burris and Lawrence reduces the satisfiability (SAT) problem to the equivalence problem by using long products of sums of variables. Nevertheless, a polynomial is usually given as a sum of monomials. Of course, the length of a polynomial may change if expanded into a sum of monomials. For example, the polynomial $\prod_{i=1}^{n}(x_i + y_i)$ has linear length in n written as a product of sums, but has exponential length if expanded into a sum of monomials. Such a change in the length suggests that the complexity of the equivalence problem might be different if the input polynomials are restricted to be written as sums of monomials. Thus, Lawrence and Willard [25] introduced the sigma equivalence and sigma equation solvability problems, i.e. when the input polynomials over the given ring are presented as sums of monomials where each monomial has the form $\alpha_1 \dots \alpha_m$ with each α_i a variable or an element of the ring. They formulated a conjecture about the complexity of the sigma equivalence and sigma equation solvability problems. Namely, if the factor by the Jacobson radical is commutative, then the sigma equivalence and sigma equation solvability problems are solvable in polynomial time, otherwise the sigma equivalence problem is coNP-complete, and the sigma equation solvability problem is NP-complete.

Szabó and Vértesi proved the coNP-complete part of the conjecture in [33]. They prove a stronger result for matrix rings: the equivalence problem is coNP-complete even if the input polynomials are restricted to only one monomial, that is the equivalence problem is coNP-complete for the multiplicative semigroup of matrix rings. To this problem they reduce the equivalence problem over the multiplicative subgroup of matrix rings, which is coNP-complete by [15]. Almeida, Volkov and Goldberg proved an even more general result about semigroups (showing that the equivalence problem is coNP-complete for a semigroup if the equivalence problem is coNP-complete for the direct product of its maximal subgroups) yielding the same result for matrix rings [2]. For most matrix rings, arguments of [25] establish coNP-completeness, as well. Moreover, NP-completeness for the equation solvability problem follows from any of these arguments.

For commutative rings, the equivalence problem is indeed solvable in polynomial time [13]. The polynomial part of this conjecture is completely proved in the manuscript [16].

The interest in the computational complexity of the equivalence and equation solvability problems of a finite algebraic structure has been steadily increasing in the past decade. Several results have been published about the complexity of these problems for general algebras (e.g. [8, 9, 10]) or for finite semigroups and monoids (e.g. [2, 6, 20, 21, 22, 23, 24, 29, 31, 33]). Just to mention some of the most recent results: following up on [2], Klíma finished the characterization for the transformation monoids [24], or Gorazd and Krzaczkowski characterized the complexity of these problems for all two-element general algebras [9, 10]. Although the literature is fairly extensive for monoids, the equivalence and equation solvability problems even for the simplest case, the case of finite groups, proved to be a far more challenging topic than for finite rings.

A group expression for a group $\mathbf{G}$ is a product of variables, inverses of variables and elements from $\mathbf{G}$. The *equivalence problem* for a finite group $\mathbf{G}$ asks whether or not two group expressions are equivalent over $\mathbf{G}$, i.e. if the two products determine the same function over $\mathbf{G}$. The *equation solvability problem* for $\mathbf{G}$ asks whether or not two group expressions can attain the same value for some substitution over the finite group $\mathbf{G}$. Burris and Lawrence [4] proved that if a group $\mathbf{G}$ is nilpotent or $\mathbf{G} \simeq \mathbf{D}_n$, the dihedral group for odd n, then the equivalence problem for $\mathbf{G}$ has polynomial time complexity. They 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. This conjecture has been verified for $\mathbf{G} \simeq \mathbf{A} \rtimes \mathbf{B}$, where $\mathbf{A}$ and $\mathbf{B}$ are Abelian groups such that the exponent of $\mathbf{A}$ is squarefree and $(|\mathbf{A}|, |\mathbf{B}|) = 1$ in [17], and for nonsolvable groups in [15].

Even less is known about the equation solvability problem over groups. Goldmann and Russel [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. Little is known for solvable, nonnilpotent groups. In [7] Goldmann and Russel explicitly ask for the complexity of the equation solvability problem for $\mathbf{S}_3$. In [17] 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 [18].

1.1. **The structure of the paper.** In this paper we consider both the equivalence and the equation solvability problems for groups of the

form $\mathbf{G} = \mathbf{A} \rtimes \mathbf{B}$, where $\mathbf{A}$ is Abelian. Here, $\mathbf{B}$ acts on $\mathbf{A}$, and this action generates a subring $\mathcal{R}$ of the endomorphism ring $\operatorname{End}\mathbf{A}$. We will consider $\mathbf{A}$ as a faithful $\mathcal{R}$-module. That way, we will be able to translate both the equivalence and the equation solvability problems into the language of modules. Motivated by this perspective, we introduce so-called 'module polynomials' in Section 2, and define the sigma equivalence and sigma equation solvability problems for modules over rings. Here, we need to define a slightly more general version of these problems: where one can substitute into the variables elements from a subset $\mathcal{S}$ instead of necessarily from the whole ring $\mathcal{R}$. Therefore, Section 2 is a more technical section. Apart from the fact that these results are interesting on their own, we mainly use them for proving theorems on groups in Section 3. In particular, in Section 2 we prove that for modules over commutative rings the sigma equivalence problem is in P, and if $\mathcal{S}$ is 'nice' then the sigma equation solvability problem is in P, as well. The precise statements can be found in Corollaries 4 and 5.

In Section 3 we consider groups of the form $\mathbf{G} = \mathbf{A} \rtimes \mathbf{B}$, where $\mathbf{A}$ is Abelian. Denote the centralizer of $\mathbf{A}$ in $\mathbf{B}$ by $C_{\mathbf{B}}(\mathbf{A})$. For the equivalence problem we prove the following:

Theorem 1. *Let $\mathbf{G} = \mathbf{A} \rtimes \mathbf{B}$, and assume that both $\mathbf{A}$ and $\mathbf{B}/C_{\mathbf{B}}(\mathbf{A})$ are commutative. If the equivalence problem over $\mathbf{B}$ is in P, then so is the equivalence problem over $\mathbf{G}$.*

Thus, we sharpen the results of [17], where Theorem 1 is proved under various additional conditions. For Abelian groups $\mathbf{A}$, $\mathbf{B}$, groups of the form $\mathbf{G} = \mathbf{Z}_{n_1} \rtimes (\mathbf{Z}_{n_2} \rtimes \cdots \rtimes (\mathbf{Z}_{n_k} \rtimes (\mathbf{A} \rtimes \mathbf{B})))$ are examples where Theorem 1 can be easily applied (see Corollary 8).

For the equation solvability problem, we can prove the following (for the details see Theorem 9 in Section 3.4): Let $\mathbf{G} = \mathbf{A} \rtimes \mathbf{B}$, and assume that both $\mathbf{A}$ and $\mathbf{B}$ are commutative. Let $\mathcal{S}$ denote the action of $\mathbf{B}$ over $\mathbf{A}$ in the ring $\operatorname{End}\mathbf{A}$, and let $\mathcal{R}$ be the subring of $\operatorname{End}\mathbf{A}$ generated by $\mathcal{S}$. If the module sigma equation solvability problem over $(\mathcal{R}, \mathbf{A})$ for substitutions from $\mathcal{S}$ is in P, then so is the equation solvability problem over $\mathbf{G}$. In particular, if the generated ring $\mathcal{R}$ is direct indecomposable, or $\mathcal{R}^\times$ is cyclic, then the equation solvability problem over $\mathbf{G}$ is in P.

The most obvious examples for which Theorem 9 can be applied are the following:

Corollary 2. *Let $\mathbf{B}$ be a finite commutative group. The equation solvability problem is in P for the following groups.*

(a) $\mathbf{G} = \mathbf{Z}_n \rtimes \mathbf{B}$, *where $n = p^\alpha$ or $n = 2p^\alpha$ for some prime p;*

(b) $\mathbf{G} = \mathbf{Z}_p^n \rtimes \mathbf{B}$, *such that* $|\mathbf{B}/C_{\mathbf{B}}(\mathbf{A})| \in \{1, q\}$ *for some distinct primes* p, q, *where* p *is a primitive root modulo* q.
(c) $\mathbf{G} = \mathbf{Z}_p^n \rtimes \mathbf{B}$, *such that* $|\mathbf{B}/C_{\mathbf{B}}(\mathbf{A})| \in \{1, q\}$ *for some distinct primes* p, q, *where the order of* p *modulo* q *is some* $d \geq 2$ *and* $n \leq d + 1$.

Theorem 9 in Section 3.4 generalizes all existing results about the complexity of the equation solvability problem for solvable, not nilpotent groups [17, 18]. Examples for item (b) are $\mathbf{Z}_2^2 \rtimes \mathbf{B}$, where $2 \nmid |\mathbf{B}|$ (e.g. $\mathbf{A}_4$), or $\mathbf{Z}_p^n \rtimes \mathbf{Z}_q$ for $q \neq p$ where p is a primitive root modulo q. If, for example, $q = 2$, then any odd prime p is a primitive root modulo q, hence the equation solvability problem over $\mathbf{Z}_p^n \rtimes \mathbf{Z}_2$ is in P. Examples for item (c) are $\mathbf{Z}_2^3 \rtimes \mathbf{Z}_7$ or $\mathbf{Z}_2^4 \rtimes \mathbf{Z}_7$.

We wrote a computer program for Theorems 1 and 9 in GAP [5] using the SONATA package [1], and ran it on the supercomputer of University of Debrecen [28] to determine the smallest groups for which the complexities of the equivalence and equation solvability problems are yet unknown. Based on these computations, in Section 4 we close the paper by reviewing what questions remain open about the complexity of these problems over groups. Sections 6 and 7 contain the GAP SmallGroup identifications and StructureDescriptions of the groups of order at most 60 with currently unknown equivalence and equation solvability complexities. The GAP source code and the full list can be found on the website [14].

2. Module polynomials

In this section we extend the definitions of the equivalence and equation solvability problems from rings to modules. These problems could be defined for modules over arbitrary rings. However, the definitions and theorems would become quite tedious and technical. Since in Section 3 we only need the results about modules over *commutative unital rings*, we restrict ourselves for considering only such rings.

2.1. **Definitions.** Let $\mathcal{R}$ be a commutative, unital ring, $\mathcal{M}$ be a module over $\mathcal{R}$. For nonnegative integers n, k, let $X = \{x_1, \ldots, x_n\}$, $Y = \{y_1, \ldots, y_k\}$ be disjoint sets of variables. For polynomials $f_i, f_a \in$

$\mathcal{R}[x_1, \ldots, x_n]$ $(1 \leq i \leq k,\ a \in \mathcal{M})$ the *module polynomials* are expressions of the form

$$(1) \quad f(X;Y) = f(x_1, \ldots, x_n; y_1, \ldots, y_k) = \sum_{i=1}^{k} f_i(x_1, \ldots, x_n) \cdot y_i + \sum_{a \in \mathcal{M}} f_a(x_1, \ldots, x_n) \cdot a.$$

For an evaluation of the module polynomial $f(X;Y)$ the variables from X (i.e. before the semi-colon) are evaluated over $\mathcal{R}$, and the variables from Y (i.e. after the semi-colon) are evaluated over $\mathcal{M}$. Expressions of the form $m \cdot y_i$ and $m \cdot a$ for some monomial m over $\mathcal{R}$ $(1 \leq i \leq k,\ a \in \mathcal{M})$ are called *module monomials*. If all f_i and f_a $(1 \leq i \leq k,\ a \in \mathcal{M})$ are written as sums of monomials then we say that f is written as sums of module monomials. Let $\mathcal{S} \subseteq \mathcal{R}$. We say that the module polynomials f and g are *equivalent over* $(\mathcal{R}, \mathcal{M})$ *for substitutions from* $\mathcal{S}$ (and write $(\mathcal{R}, \mathcal{M}) \models f|_{\mathcal{S}} \approx g|_{\mathcal{S}}$) if for every $s_1, \ldots, s_n \in \mathcal{S}$ and for every $a_1, \ldots, a_k \in \mathcal{M}$ the two polynomials agree on this evaluation:

$$f(s_1, \ldots, s_n; a_1, \ldots, a_k) = g(s_1, \ldots, s_n; a_1, \ldots, a_k).$$

Similarly, we say $f = g$ is solvable over $(\mathcal{R}, \mathcal{M})$ for some substitution from $\mathcal{S}$ (and write $f|_{\mathcal{S}} = g|_{\mathcal{S}}$ is solvable over $(\mathcal{R}, \mathcal{M})$) if there exist $s_1, \ldots, s_n \in \mathcal{S}$ and $a_1, \ldots, a_k \in \mathcal{M}$ such that the two polynomials attain the same value on this evaluation:

$$f(s_1, \ldots, s_n; a_1, \ldots, a_k) = g(s_1, \ldots, s_n; a_1, \ldots, a_k).$$

When we want to emphasize which variable is substituted from where, then we write $(\mathcal{R}, \mathcal{M}) \models f(X|_{\mathcal{S}}, Y|_{\mathcal{M}}) \approx g(X|_{\mathcal{S}}, Y|_{\mathcal{M}})$ for the equivalence and $f(X|_{\mathcal{S}}, Y|_{\mathcal{M}}) = g(X|_{\mathcal{S}}, Y|_{\mathcal{M}})$ for the equation solvability.

The *module sigma equivalence problem* over $(\mathcal{R}, \mathcal{M})$ for substitutions from $\mathcal{S}$ asks whether or not two input module polynomials f and g (written as sums of monomials) are equivalent for substitutions from $\mathcal{S}$, that is whether or not $(\mathcal{R}, \mathcal{M}) \models f|_{\mathcal{S}} \approx g|_{\mathcal{S}}$ holds. The *module sigma equation solvability problem* over $(\mathcal{R}, \mathcal{M})$ for substitutions from $\mathcal{S}$ asks whether or not for two input module polynomials f and g (written as sums of monomials) the equation $f|_{\mathcal{S}} = g|_{\mathcal{S}}$ can be solved. If the input module polynomials are not restricted to be written as sums of module monomials, then we talk about the *module equivalence* and the *module equation solvability* problems. These latter two problems can be handled easily by the ideas from [3, 19], Since we do not need them later, we only consider the sigma problems in the following.

Note, that the module problems are generalizations of the original (sigma) equivalence and (sigma) equation solvability problems for rings.

Indeed, if $\mathcal{M} = \mathcal{R}$ and $\mathcal{S} = \mathcal{R}$, then we have the original problems for rings. Furthermore, note that for module polynomials f, g we have $(\mathcal{R}, \mathcal{M}) \models f \approx g$ if and only if $(\mathcal{R}, \mathcal{M}) \models f - g \approx 0$, and $f = g$ is solvable if and only if $f - g = 0$ is solvable. Therefore, it is enough to consider whether or not one input polynomial is equivalent to 0 or can attain the value 0. The main result of the section is the following.

Theorem 3. *Let $\mathcal{R}$ be a commutative, unital, local ring of prime power characteristic. Let $\mathcal{M}$ be a module over $\mathcal{R}$. Let $\mathcal{S} \leq \mathcal{R}^\times$ be a subgroup of the multiplicative group $\mathcal{R}^\times$. Let a module polynomial f be written as a sum of module monomials over $(\mathcal{R}, \mathcal{M})$ (see (1)). Then it can be decided in polynomial time in $||f||$ whether or not $f|_{\mathcal{S}} = 0$ is solvable over $(\mathcal{R}, \mathcal{M})$.*

Theorem 3 has the following consequences that will be used in Section 3.

Corollary 4. *Let $\mathcal{R} = \oplus_{i=1}^{l} \mathcal{R}_i$ be a commutative unital ring, where each $\mathcal{R}_i$ $(1 \leq i \leq l)$ is a commutative, unital, local ring of prime power characteristic. Let $\mathcal{M}$ be a module over $\mathcal{R}$. Let $\mathcal{S} = \oplus_{i=1}^{l} \mathcal{S}_i$, where each $\mathcal{S}_i$ $(1 \leq i \leq l)$ is a subgroup of the multiplicative group $\mathcal{R}_i^\times$. Let a module polynomial f be written as a sum of module monomials over $(\mathcal{R}, \mathcal{M})$ (see (1)). Then it can be decided in polynomial time in $||f||$ whether or not $f|_{\mathcal{S}} = 0$ is solvable over $(\mathcal{R}, \mathcal{M})$.*

Corollary 5. *Let $\mathcal{R}$ be a commutative unital ring, $\mathcal{M}$ be a module over $\mathcal{R}$. Let $\mathcal{S}$ be a subgroup of the multiplicative group $\mathcal{R}^\times$. Let a module polynomial f be written as a sum of module monomials over $(\mathcal{R}, \mathcal{M})$ (see (1)). Then it can be decided in polynomial time in $||f||$ whether or not $(\mathcal{R}, \mathcal{M}) \models f|_{\mathcal{S}} \approx 0$.*

The remaining part of this section is structured as follows. In Section 2.2 we show that Corollaries 4 and 5 follow from Theorem 3. We prove that it is enough to consider commutative local rings of prime power characteristic. Galois rings play an important role in the theory of finite commutative local rings, therefore we summarize their basic properties in Section 2.3. Then in Section 2.4 we introduce the notations used throughout the proof of Theorem 3. In Section 2.5 we give the main steps for the (algorithmic) proof of Theorem 3. Finally, in Section 2.6 we give the detailed proof of Theorem 3.

2.2. **Reduction to local rings.** Here, we show that Corollaries 4 and 5 follow from Theorem 3. Let $\mathcal{R}$ be a finite, commutative, unital ring. By the Pierce decomposition theorem (see e.g. [11, p. 48, 50]) $\mathcal{R}$ is the direct sum of some commutative, unital, local rings of prime power

characteristic. Thus, there exist commutative, unital, local rings $\mathcal{R}_i$ ($1 \leq i \leq l$ for some l) of prime power characteristic such that $\mathcal{R} = \oplus_{i=1}^{l} \mathcal{R}_i$. In case of Corollary 4 the Pierce decomposition is given in the statement.

Let $\mathcal{M}$ be a module over $\mathcal{R}$. Now, $\mathcal{M} = \mathcal{R}\mathcal{M} = \oplus_{i=1}^{l} \mathcal{R}_i\mathcal{M}$, and thus $\mathcal{M}$ is the direct sum of submodules $\mathcal{R}_i\mathcal{M}$, where $\mathcal{R}_i\mathcal{M}$ is a module over $\mathcal{R}_i$ and $\mathcal{R}_j\mathcal{R}_i\mathcal{M} = \{0\}$. Let $\mathcal{S} \leq \mathcal{R}^\times$ be a subgroup of the multiplicative group, and let $\mathcal{S}_i$ be the projection of $\mathcal{S}$ onto $\mathcal{R}_i$, then $\mathcal{S}_i \leq \mathcal{R}_i^\times$. Let f be a module polynomial over $(\mathcal{R}, \mathcal{M})$, written as a sum of module monomials. For $1 \leq i \leq l$ let f_i be the module polynomial obtained from f by replacing every constant from $\mathcal{R}$ with their projection onto $\mathcal{R}_i$ and every constant from $\mathcal{M}$ with their projection onto $\mathcal{R}_i\mathcal{M}$. Then it is easy to see that $(\mathcal{R}, \mathcal{M}) \models f|_{\mathcal{S}} \approx 0$ if and only if for all $1 \leq i \leq l$ we have $(\mathcal{R}_i, \mathcal{R}_i\mathcal{M}) \models f_i|_{\mathcal{S}_i} \approx 0$. Moreover, if $\mathcal{S} = \oplus_{i=1}^{l} \mathcal{S}_i$, then $f|_{\mathcal{S}} = 0$ is solvable over $(\mathcal{R}, \mathcal{M})$ if and only if for all $1 \leq i \leq l$ the equations $f_i|_{\mathcal{S}_i} = 0$ are solvable over $(\mathcal{R}_i, \mathcal{R}_i\mathcal{M})$. That is, both the equivalence and the equation solvability problems can be decided componentwise, and hence it is enough to prove Corollaries 4 and 5 for commutative, unital, local rings of prime power characteristic.

Corollary 4 now follows directly from Theorem 3. Furthermore, if $\mathcal{R}$ is a commutative, unital, local ring of prime power characteristic, $\mathcal{M}$ is a module over $\mathcal{R}$, $\mathcal{S} \subseteq \mathcal{R}$, and f is a module polynomial over $(\mathcal{R}, \mathcal{M})$, then $(\mathcal{R}, \mathcal{M}) \models f|_{\mathcal{S}} \approx 0$ if and only if $f|_{\mathcal{S}} = a$ is not solvable for any $0 \neq a \in \mathcal{M}$. That is, if the module sigma equation solvability problem can be decided in polynomial time, then so can be the module sigma equivalence problem. Hence Corollary 5 follows from Theorem 3, as well.

2.3. **Galois rings.** In this subsection we review the theory of Galois rings necessary for our proofs. The reader may skip this part if they are familiar with the literature.

Galois rings play an important role in the theory of commutative rings. They were first examined in [30], and later in [34]. In the following we list some of the most important properties of Galois rings (see e.g. [27]). Let $h_d(x) \in \mathbb{Z}[x]$ be a monic polynomial of degree d which is irreducible modulo p. Then the *Galois ring* $\mathcal{GR}(p^c, d)$ is by definition the factor ring $\mathbb{Z}[x] / (p^c, h_d(x))$.

The Galois ring $\mathcal{GR}(p^c, d)$ is completely characterized by the numbers p, c, d, and does not depend on the choice of the polynomial h_d. The Galois ring $\mathcal{GR}(p^c, d)$ is a finite, commutative, unital, local ring. The characteristic of $\mathcal{GR}(p^c, d)$ is p^c, the number of its elements is p^{cd}. In particular, $\mathcal{GR}(p, d)$ is isomorphic to the p^d-element field

$\mathbb{F}_{p^d}$, and $\mathcal{GR}(p^c, 1)$ (where h_d is of degree 1) is isomorphic to $\mathbb{Z}_{p^c}$. For every ideal $\mathcal{I} \lhd \mathcal{GR}(p^c, d)$ there exists a number $0 \leq i \leq c$ such that $\mathcal{I} = (p^i)$. That is every ideal is a principal ideal, thus every finitely generated $\mathcal{GR}(p^c, d)$-module is a direct sum of cyclic $\mathcal{GR}(p^c, d)$-modules [34, p. 81, Corollary 2]. The Galois ring $\mathcal{GR}(p^c, d)$ is local, the unique maximal ideal is the Jacobson radical (p). For every $1 \leq i \leq c$ the factor ring $\mathcal{GR}(p^c, d) / (p^i)$ is isomorphic to the Galois ring $\mathcal{GR}(p^i, d)$. In particular, the factor by the Jacobson radical is isomorphic to $\mathbb{F}_{p^d}$. Finally, we will need the following (here $\lfloor x \rfloor$ denotes the greatest integer not greater than x):

Lemma 6. *For a prime p and for arbitrary positive integers c, t let $m \geq c + \lfloor \log_p (t-1) \rfloor$ be an integer. Then $p^c \mid \binom{p^m}{i}$ for all integers $1 \leq i \leq t-1$ and $p \mid \binom{p^m}{i}$ for all integers $1 \leq i \leq p^m - 1$.*

Proof. Let $1 \leq i \leq p^m - 1$ be arbitrary. Now,

$$\binom{p^m}{i} = \frac{p^m (p^m - 1) \dots (p^m - i + 1)}{1 \dots (i-1) \cdot i} = \frac{p^m}{i} \cdot \prod_{j=1}^{i-1} \frac{p^m - j}{j}.$$

Here, the p-part of $p^m - j$ and j are the same. As $p^m \nmid i$, the exponent of the p-part of i is at most $m-1$, and thus the p-part of the first factor is at least p. Furthermore, if $i \leq t-1$, then the exponent of the p-part of i is at most $\lfloor \log_p i \rfloor \leq \lfloor \log_p (t-1) \rfloor \leq m - c$, and thus the p-part of the first factor is at least p^c. □

2.4. **Notations.** In the following, let $\mathcal{R}$ be a commutative, unital, local ring of characteristic p^c for some prime p. Let $\mathcal{M}$ be a module over $\mathcal{R}$, and let $\mathcal{S}$ be a subgroup of the multiplicative group $\mathcal{R}^\times$. Let

$$f(x_1, \dots, x_n; y_1, \dots, y_k) = \sum_{i=1}^{k} f_i(x_1, \dots, x_n) \cdot y_i + \sum_{a \in \mathcal{M}} f_a(x_1, \dots, x_n) \cdot a$$

be a module polynomial over $(\mathcal{R}, \mathcal{M})$ written as a sum of monomials.

Let $\mathcal{J}$ denote the Jacobson radical of $\mathcal{R}$ and let t be the smallest positive integer for which $\mathcal{J}^t = \{0\}$. Let $\mathcal{F}$ denote the factor field $\mathcal{R}/\mathcal{J}$, and assume $\mathcal{F} \simeq \mathbb{F}_{p^d}$. Then $\mathcal{R}$ contains a (unique) subring $\mathcal{R}_0 \leq \mathcal{R}$ isomorphic to $\mathcal{GR}(p^c, d)$ [34, p. 80, Theorem B]. Let t be the smallest positive integer for which $\mathcal{J}^t = \{0\}$. Let $m \geq c + \lfloor \log_p (t-1) \rfloor$ be a positive integer such that $d \mid m$.

Consider the map $r \mapsto r^{p^m}$ $(r \in \mathcal{R})$. As $d \mid m$, we have $\mathcal{F} \models x^{p^m} \approx x$, hence $r^{p^m} - r \in \mathcal{J}$. For arbitrary $r \in \mathcal{R}$ and $u \in \mathcal{J}$ we have

$$(r+u)^{p^m} - r^{p^m} = \sum_{i=1}^{t-1} \binom{p^m}{i} r^{p^m - i} u^i + \sum_{i=t}^{p^m} \binom{p^m}{i} r^{p^m - i} u^i = 0.$$

Here, the first sum is 0 since p^c is a divisor of every binomial coefficient by Lemma 6. The second sum is 0 as any product containing at least t elements from $\mathcal{J}$ is 0. Thus $r \mapsto r^{p^m}$ is a projection onto a multiplicatively closed set $\mathcal{S}_0$ such that $\mathcal{S}_0$ is a representation system for $\mathcal{F}$. In particular, there exists an element $s^* \in \mathcal{R}$ which has multiplicative order $\left(p^d - 1\right)$, and $\mathcal{S}_0 = \{\,0\,\} \cup \left\{\, (s^*)^j \mid 1 \leq j \leq p^d - 1 \,\right\}$. Then $\mathcal{R}^\times$ is the direct product of the subgroups $\mathcal{S}_0 \setminus \{\,0\,\}$ and $1 + \mathcal{J} = \{\,1 + u \mid u \in \mathcal{J}\,\}$ [30, p. 200, p. 215]. Note, that the sizes of the subgroups $\mathcal{S}_0 \setminus \{\,0\,\}$ and $1 + \mathcal{J}$ are coprime, thus the subgroup $\mathcal{S} \leq \mathcal{R}^\times$ is a direct product of a subgroup $\mathcal{S}' \leq \mathcal{S}_0 \setminus \{\,0\,\}$ and $1 + \mathcal{J}'$ for some $\mathcal{J}' \subseteq \mathcal{J}$. Since $\mathcal{S}_0 \setminus \{\,0\,\}$ is generated by s^*, there exists a positive integer e such that $\mathcal{S}'$ is generated by $(s^*)^e$, that is

$$\mathcal{S} = \mathcal{S}' \cdot (1 + \mathcal{J}') = \{\, s^e \cdot (1 + u) \mid s \in \mathcal{S}_0 \setminus \{\,0\,\}, u \in \mathcal{J}' \,\}. \tag{2}$$

Note, that $s^{p^d} = s$ for every $s \in \mathcal{S}_0$, and the range of the map $\mathcal{S}_0 \to \mathcal{S}_0$, $s \mapsto s^{p^d - 1}$ is $\{\,0, 1\,\}$. Furthermore, $\mathcal{S}_0$ is a subset of the unique subring $\mathcal{R}_0$ isomorphic to $\mathcal{GR}\left(p^c, d\right)$ contained in $\mathcal{R}$. Finally, for every element $r \in \mathcal{R}_0$, there exist unique elements $s_0, \ldots, s_{c-1} \in \mathcal{S}_0$ such that $r = \sum_{i=0}^{c-1} s_i p^i$. We continue by proving Theorem 3.

2.5. **Sketch of the proof of Theorem 3.** We consider $\mathcal{M}$ and $\mathcal{R}$ as a direct sum of cyclic $\mathcal{R}_0$-modules. Then every element of $\mathcal{M}$ and $\mathcal{R}$ can be written as $\sum_{b \in B} r_b b$ and $\sum_{b' \in B'} r_{b'} b'$, respectively, for some $r_b, r_{b'} \in \mathcal{R}_0$, where B and B' are (weak) bases of $\mathcal{M}$ and $\mathcal{R}$. Furthermore, every element of $\mathcal{R}_0$ can be written as $\sum_{i=0}^{c-1} s_i p^i$ for some $s_i \in \mathcal{S}_0$.

(a) Thus first, by introducing new sets of variables X, Y and Z, we will be able to rewrite the module polynomial f over $(\mathcal{R}, \mathcal{M})$ into a module polynomial g over $(\mathcal{R}_0, \mathcal{M})$ such that $f|_{\mathcal{S}} = 0$ is solvable if and only if $g\left(X|_{\mathcal{S}_0 \setminus \{\,0\,\}}, Y|_{\mathcal{S}_0}, Z|_{\mathcal{S}_0}\right) = 0$ is solvable.

(b) Again, we use the fact that $\mathcal{M}$ is a direct sum of cyclic $\mathcal{R}_0$-modules, that is $\mathcal{M} = \oplus_{b \in \mathcal{B}} \mathcal{R}_0 b$ for some (weak) basis $\mathcal{B}$. Then we can find polynomials $h_b \in \mathcal{R}_0[X, Y, Z]$ for every $b \in \mathcal{B}$ such that the module equation $g\left(X|_{\mathcal{S}_0 \setminus \{\,0\,\}}, Y|_{\mathcal{S}_0}, Z|_{\mathcal{S}_0}\right) = 0$ can be solved if and only if the *system of equations*

$$h_b\left(X|_{\mathcal{S}_0 \setminus \{\,0\,\}}, Y|_{\mathcal{S}_0}, Z|_{\mathcal{S}_0}\right) = 0 \qquad (b \in \mathcal{B}) \tag{3}$$

is solvable over the Galois ring $\mathcal{R}_0$. That is, we reduced the original problem to solving a system of equations over the Galois ring $\mathcal{R}_0$.

(c) Then we reduce this system over $\mathcal{R}_0$ to a system of $c \cdot |\mathcal{B}|$-many equations over $\mathcal{F} = \mathcal{R}/\mathcal{J}$. In particular, we find $h_{i,b} \in$

$\mathcal{F}[X,Y,Z]$ $(0 \le i \le c-1, b \in \mathcal{B})$ such that the system (3) can be solved simultaneously if and only if the system

$$h_{i,b}\left(X|_{\mathcal{F}\setminus\{0\}}, Y|_{\mathcal{F}}, Z|_{\mathcal{F}}\right) = 0 \qquad (1 \le i \le c-1, b \in \mathcal{B}) \tag{4}$$

can be solved over $\mathcal{F}$.

(d) Let

$$q = \left(\prod_{x\in X} x\right) \cdot \prod_{i=0}^{c-1} \prod_{b\in\mathcal{B}} \left(1 - h_{i,b}^{p^d-1}\right) \in \mathcal{F}[X,Y,Z]. \tag{5}$$

We prove that the system (4) is *not* solvable over $\mathcal{F}$ if and only if $\mathcal{F} \models q|_{\mathcal{F}} \approx 0$.

That is, $f|_{\mathcal{S}} = 0$ is *not* solvable over $(\mathcal{R}, \mathcal{M})$ if and only if $\mathcal{F} \models q|_{\mathcal{F}} \approx 0$. Throughout the proof we compute the time-complexity of calculating every set of new polynomials. In particular, the final polynomial q can be calculated in polynomial time of $O(||f||)$. By [13] it can be decided in polynomial time in $||q||$ whether or not $\mathcal{F} \models q|_{\mathcal{F}} \approx 0$.

2.6. **Detailed proof of Theorem 3.** Consider $\mathcal{M}$ and $\mathcal{R}$ as $\mathcal{R}_0$-modules. The ring $\mathcal{R}_0$ is isomorphic to a Galois ring, both $\mathcal{M}$ and $\mathcal{R}$ are direct sums of cyclic $\mathcal{R}_0$-modules. Let $\mathcal{B}$ denote a (weak) basis for $\mathcal{M}$, that is $\mathcal{M} = \oplus_{b\in\mathcal{B}} \mathcal{R}_0 b$ such that $\sum_{b\in\mathcal{B}} r_b b = 0$ if and only if $r_b \in \operatorname{Ann}\{b\}$. Now, every element $a \in \mathcal{M}$ can be written in the form of $\sum_{b\in\mathcal{B}} r_b b$ for some $r_b \in \mathcal{R}_0$, $b \in \mathcal{B}$. Further, let $\mathcal{B}'$ denote a (weak) basis for $\mathcal{R}$ for which $1 \in \mathcal{B}'$, $\mathcal{B}' \setminus \{1\} \subseteq \mathcal{J}$, and $\mathcal{R} = \oplus_{b'\in\mathcal{B}'} \mathcal{R}_0 b'$. Every element $r \in \mathcal{R}$ can be written in the form of $\sum_{b\in\mathcal{B}} r_{b'} b'$ for some $r_{b'} \in \mathcal{R}_0$, $b' \in \mathcal{B}'$. Moreover, every element of $\mathcal{R}_0$ can be (uniquely) written in the form of $\sum_{i=0}^{c-1} s_i p^i$, where $s_i \in \mathcal{S}_0$.

Hence, every element $a \in \mathcal{M}$ can be written in the form of $\sum_{i=0}^{c-1} \sum_{b\in\mathcal{B}} s_{i,b} p^i b$ for some $s_{i,b} \in \mathcal{S}_0$, $0 \le i \le c-1$, $b \in \mathcal{B}$, and every element $r \in \mathcal{R}$ can be written in the form of $\sum_{i=0}^{c-1} \sum_{b'\in\mathcal{B}'} s_{i,b'} p^i b'$ for some $s_{i,b'} \in \mathcal{S}_0$, $0 \le i \le c-1$, $b' \in \mathcal{B}'$. We use these presentations in order to reduce solving $f = 0$ to solving a module equation over $\mathcal{R}_0$. For this we introduce the following disjoint sets of new variables (recall that n was the number of x variables in f, and k was the number of y variables of f):

$$\begin{aligned} X &= \{ x_j \mid 1 \le j \le n \}, \\ Y &= \{ y_{j,i,b} \mid 1 \le j \le k, 0 \le i \le c-1, b \in \mathcal{B} \}, \\ Z &= \{ z_{j,u} \mid 1 \le j \le n, u \in \mathcal{J}' \}. \end{aligned}$$

(a) Firstly, replace the variables and constants from $\mathcal{M}$: Replace every element $a \in \mathcal{M}$ occurring in f with one of its equivalents of the form $\sum_{i=0}^{c-1} \sum_{b\in\mathcal{B}} s_{i,b} p^i b$ ($s_{i,b} \in \mathcal{S}_0$, $0 \le i \le c-1$, $b \in$

$\mathcal{B}$). Further, replace every occurrence of the old variable y_j ($1 \leq j \leq k$) with the expression $\sum_{i=0}^{c-1} \sum_{b \in \mathcal{B}} y_{j,i,b} p^i b$. Let the resulting module polynomial be $f^{(i)}$. Note that $f^{(i)}$ does not have variables substituted from $\mathcal{M}$, but rather only constants from $\mathcal{M}$ and variables from $\mathcal{R}$. Further,

$$(\mathcal{R}, \mathcal{M}) \models f|_{\mathcal{S}} \approx f^{(i)}\left(X|_{\mathcal{S}}, Y|_{\mathcal{S}_0}\right).$$

Secondly, replace every occurrence of x_j ($1 \leq j \leq n$) in $f^{(i)}$ with the expression $x_j^e \cdot \prod_{u \in \mathcal{J}'} \left(1 + u \cdot z_{j,u}^{p^d-1}\right)$, where e was the exponent for which $\mathcal{S}'$ is generated by $(s^*)^e$. Let the resulting module polynomial be $f^{(ii)}$. By (2) one can observe that

$$(\mathcal{R}, \mathcal{M}) \models f^{(i)}\left(X|_{\mathcal{S}}, Y|_{\mathcal{S}_0}\right) \approx f^{(ii)}\left(X|_{\mathcal{S}_0 \setminus \{0\}}, Y|_{\mathcal{S}_0}, Z|_{\mathcal{S}_0}\right).$$

because $z_{j,u}^{p^d-1}$ can attain values either 0 or 1.

Thirdly, replace every constant $r \in \mathcal{R}$ occurring in $f^{(ii)}$ with one of its equivalents of the form $\sum_{i=0}^{c-1} \sum_{b' \in \mathcal{B}'} s_{i,b'} p^i b'$ ($s_{i,b'} \in \mathcal{S}_0$, $0 \leq i \leq c-1$, $b' \in \mathcal{B}'$). Let $f^{(iii)}$ be the resulting module polynomial over $(\mathcal{R}_0, \mathcal{M})$ in variables $X \cup Y \cup Z$. The resulting module polynomial $f^{(iii)}$ has no variables substituted from $\mathcal{M}$, and

$$(\mathcal{R}, \mathcal{M}) \models f^{(ii)}\left(X|_{\mathcal{S}_0 \setminus \{0\}}, Y|_{\mathcal{S}_0}, Z|_{\mathcal{S}_0}\right) \approx f^{(iii)}\left(X|_{\mathcal{S}_0 \setminus \{0\}}, Y|_{\mathcal{S}_0}, Z|_{\mathcal{S}_0}\right).$$

Fourthly, let us expand $f^{(iii)}$ as a sum of module monomials, and remove module monomials containing at least t elements from $\mathcal{J}$. Let $f^{(iv)}$ denote the resulting module polynomial. Module monomials containing at least t elements from $\mathcal{J}$ attain value 0 for arbitrary substitution.

$$(\mathcal{R}, \mathcal{M}) \models f^{(iii)}\left(X|_{\mathcal{S}_0 \setminus \{0\}}, Y|_{\mathcal{S}_0}, Z|_{\mathcal{S}_0}\right) \approx f^{(iv)}\left(X|_{\mathcal{S}_0 \setminus \{0\}}, Y|_{\mathcal{S}_0}, Z|_{\mathcal{S}_0}\right).$$

By not calculating module monomials containing at least t elements from $\mathcal{J}$, one can execute the expansion in $O\left(||f||^t\right)$ time, and the resulting module polynomial $f^{(iv)}$ has length $O\left(||f||^t\right)$.

Finally, let us rearrange every monomial of $f^{(iv)}$ into the form $\prod_{x \in X} x^{k_x} \cdot \prod_{y \in Y} y^{k_y} \cdot \prod_{z \in Z} z^{k_z} \cdot s' \cdot p^{k'} \cdot b' \cdot b$, where $b' \in \mathcal{B}'$, $b \in \mathcal{B}$ and $s' \in \mathcal{S}_0$. Since $\mathcal{R}$ is commutative, the resulting polynomial attains the same values as $f^{(iv)}$. Moreover, replace every occurring $s' \cdot p^{k'} \cdot b' \cdot b$ with one of its equivalents of the form $\sum_{i=0}^{c-1} \sum_{b \in \mathcal{B}} s_{i,b} p^i b$ ($s_{i,b} \in \mathcal{S}_0$, $0 \leq i \leq c-1$, $b \in \mathcal{B}$), and expand the resulting module polynomial. Let the resulting

module polynomial over $(\mathcal{R}_0, \mathcal{M})$ be denoted by g. Now, g has no variables substituted from $\mathcal{M}$, and

$$(\mathcal{R}, \mathcal{M}) \models f|_{\mathcal{S}} \approx g\left(X|_{\mathcal{S}_0 \setminus \{0\}}, Y|_{\mathcal{S}_0}, Z|_{\mathcal{S}_0}\right).$$

Furthermore, the rearranging of the monomials and the expansion can be done in $O\left(\left|\left|f^{(iv)}\right|\right|^2\right)$ time. Thus, g can be computed in $O\left(||f||^{2t}\right)$ time and $||g|| = O\left(||f||^{2t}\right)$.

(b) Now,

$$g(X, Y, Z) = \sum_{b \in \mathcal{B}} g_b(X, Y, Z) \cdot b$$

for some polynomials $g_b \in \mathcal{R}_0[X, Y, Z]$, written as sums of monomials. As $\mathcal{M} = \oplus_{b \in \mathcal{B}} \mathcal{R}_0 b$, the module polynomial g attains 0 for a substitution if and only if each polynomial g_b attains a value from $\mathrm{Ann}\{b\}$ for the same substitution. Since $\mathrm{Ann}\{b\}$ is an ideal in the Galois ring $\mathcal{R}_0 \simeq \mathcal{GR}(p^c, d)$, for every $b \in \mathcal{B}$ there exists $0 \leq c_b \leq c$ such that $\mathrm{Ann}\{b\} = (p^{c_b})$. Thus g_b attains a value from $\mathrm{Ann}\{b\}$ if and only if $p^{c-c_b} \cdot g_b$ attains the value 0 in $\mathcal{R}_0$. Let $h_b = p^{c-c_b} \cdot g_b$. Summarizing our observations,

- $f|_{\mathcal{S}} = 0$ can be solved over $(\mathcal{R}, \mathcal{M})$ if and only if
- $g\left(X|_{\mathcal{S}_0 \setminus \{0\}}, Y|_{\mathcal{S}_0}, Z|_{\mathcal{S}_0}\right)$ can be solved over $(\mathcal{R}_0, \mathcal{M})$ if and only if
- the system of equations

$$h_b\left(X|_{\mathcal{S}_0 \setminus \{0\}}, Y|_{\mathcal{S}_0}, Z|_{\mathcal{S}_0}\right) = 0 \qquad (b \in \mathcal{B}) \tag{3}$$

can be solved over $\mathcal{R}_0$.

(c) For simplicity, let $h = h_b$ for some $b \in \mathcal{B}$. Let V_0 denote the set of monomials in h whose coefficients are not divisible by p, and let $h^{(i)}$ denote $\left(h - \sum_{v \in V_0} v\right)/p$. That is $h = \sum_{v \in V_0} v + p \cdot h^{(i)}$. Recall that $s^{p^d} = s$ for every $s \in \mathcal{S}_0$. Thus $d \mid m$ implies $s^{p^m} = s$ for every $s \in \mathcal{S}_0$. For every $v \in V_0$ its coefficient is in $\mathcal{S}_0$. Thus for every $v \in V_0$ we have

$$\mathcal{R}_0 \models v|_{\mathcal{S}_0} \approx v^{p^m}\big|_{\mathcal{S}_0}.$$

Consider $\left(\sum_{v \in V_0} v\right)^{p^m}$. By Lemma 6, one can prove by induction on $|V|$ that

$$\left(\sum_{v \in V_0} v\right)^{p^m} = \left(\sum_{v \in V_0} v^{p^m}\right) + p \cdot h^{(ii)}$$

for some polynomial $h^{(ii)}$. Therefore,

$$\mathcal{R}_0 \models \sum_{v\in V_0} v|_{\mathcal{S}_0} \approx \sum_{v\in V_0} v^{p^m}\big|_{\mathcal{S}_0} \approx \left(\sum_{v\in V_0} v\right)^{p^m}\Bigg|_{\mathcal{S}_0} - p\cdot h^{(ii)}|_{\mathcal{S}_0}.$$

Let $h_0 = \sum_{v\in V_0}$. Then we have

$$\mathcal{R}_0 \models h|_{\mathcal{S}_0} \approx h_0|_{\mathcal{S}_0} + p\cdot h^{(i)}|_{\mathcal{S}_0} \approx h_0^{p^m}\Big|_{\mathcal{S}_0} + p\cdot \left(h^{(i)} - h^{(ii)}\right)\big|_{\mathcal{S}_0}.$$

Now, repeat the process with $h^{(i)} - h^{(ii)}$, then in

$$O\left(\left|\left|h^{(i)} - h^{(ii)}\right|\right|^{p^m}\right) = O\left(\left(||h||^{p^m}\right)^{p^m}\right) = O\left(||h||^{p^{2m}}\right)$$

time we obtain polynomials $h_1, (h^{(iii)} - h^{(iv)})$ such that the coefficients in h_1 are from $\mathcal{S}_0$ and

$$\mathcal{R}_0 \models \left(h^{(i)} - h^{(ii)}\right)\big|_{\mathcal{S}_0} \approx h_1^{p^m}\Big|_{\mathcal{S}_0} + p\cdot \left(h^{(iii)} - h^{(iv)}\right)\big|_{\mathcal{S}_0}.$$

Then repeat the process with $h^{(iii)} - h^{(iv)}$, etc. Then after $O\left(||h||^{p^{cm}}\right)$-many steps we arrive at polynomials $h_0, h_1, \ldots, h_{c-1}$, each is written as a sum of monomials, such that all coefficients are from $\mathcal{S}_0$, and

$$\mathcal{R}_0 \models h|_{\mathcal{S}_0} \approx h_0^{p^m}\Big|_{\mathcal{S}_0} + p\cdot h_1^{p^m}\Big|_{\mathcal{S}_0} + \cdots + p^{c-1}\cdot h_{c-1}^{p^m}\Big|_{\mathcal{S}_0}.$$

Recall that $r \mapsto r^{p^m}$ is a projection onto $\mathcal{S}_0$ and for every element $r \in \mathcal{R}_0$, there exist unique elements $s_0, \ldots, s_{c-1} \in \mathcal{S}_0$ such that $r = \sum_{i=0}^{c-1} s_i p^i$. Thus $h(s_1, \ldots, s_n) = 0$ if and only if for every $0 \le i \le c-1$ we have $h_i(s_1, \ldots, s_n)^{p^m} = 0$. Consider h_i as a polynomial over $\mathcal{F}$ by the natural map $\psi\colon \mathcal{R}_0 \to \mathcal{F}$. Now, $h_i(s_1, \ldots, s_n)^{p^m} = 0$ in $\mathcal{R}_0$ for some $s_1, \ldots, s_n \in \mathcal{S}_0$ if and only if $h_i(\psi(s_1), \ldots, \psi(s_n)) = 0$ in $\mathcal{F}$. That is, $h = 0$ can be solved over $\mathcal{R}$ by a substitution $s_1, \ldots, s_n \in \mathcal{S}_0$ if and only if $h_0 = 0, \ldots, h_{c-1} = 0$ can be solved over $\mathcal{F}$ by $\psi(s_1), \ldots, \psi(s_n)$.

Executing this procedure for every h_b ($b \in \mathcal{B}$) we obtain polynomials $h_{i,b} \in \mathcal{F}[X, Y, Z]$ ($0 \le i \le c-1, b \in \mathcal{B}$) such that the system (3) can be solved simultaneously if and only if the system

$$h_{i,b}\left(X|_{\mathcal{F}\setminus\{0\}}, Y|_{\mathcal{F}}, Z|_{\mathcal{F}}\right) = 0 \qquad (1 \le i \le c-1, b \in \mathcal{B}) \tag{4}$$

can be solved over $\mathcal{F}$. Furthermore, each $h_{i,b}$ can be computed from g in $O\left(||g||^{p^{cm}}\right)$ time.

(d) Let

$$q = \left(\prod_{x\in X} x\right) \cdot \prod_{i=0}^{c-1} \prod_{b\in\mathcal{B}} \left(1 - h_{i,b}^{p^d-1}\right) \in \mathcal{F}[X,Y,Z]\,. \tag{5}$$

We prove that the system (4) is *not* solvable over $\mathcal{F}$ if and only if $\mathcal{F} \models q|_{\mathcal{F}} \approx 0$. For some $s_x, s_y, s_z \in \mathcal{F}$ $(x \in X, y \in Y, z \in Z)$ we introduce $\bar{s}$ to denote the vector $((s_x)_{x\in X}, (s_y)_{y\in Y}, (s_z)_{z\in Z})$

For one direction, assume that there exist $s_x, s_y, s_z \in \mathcal{F}$ $(x \in X, y \in Y, z \in Z)$ such that $q(\bar{s}) \neq 0$. Then from (5) we have $s_x \neq 0$ (that is $s_x \in \mathcal{F} \setminus \{0\}$) for every $x \in X$. Furthermore, we have $h_{i,b}^{p^d-1} \in \{0,1\}$. Thus $q(\bar{s}) \neq 0$ implies $1 - h_{i,b}^{p^d-1} = 1$, that is $h_{i,b} = 0$ for every $1 \leq i \leq c-1, b \in \mathcal{B}$. Hence $\bar{s}$ is a solution of the system (4).

For the other direction, assume that there exist $s_x \in \mathcal{F}\setminus\{0\}$, $s_y, s_z \in \mathcal{F}$ such that $\bar{s}$ is a solution of the system (4). Now, every s_x is invertible in $\mathcal{F}$, and $1 - h_{i,b}^{p^d-1} = 1$, yielding $q(\bar{s}) \neq 0$.

Finally, q can be expressed into a sum of monomials in at most

$$O\left(\max_{1\leq i\leq c-1, b\in\mathcal{B}} ||h_{i,b}||^{|\mathcal{B}|cp^d}\right) = O\left(||g||^{|\mathcal{B}|cp^{d+cm}}\right) = O\left(||f||^{2t|\mathcal{B}|cp^{d+cm}}\right)$$

time. Note, that the exponent only depends on $\mathcal{R}$ and $\mathcal{M}$, and can be bounded by

$$\log|\mathcal{M}| \cdot |\mathcal{R}|^{O(\log|\mathcal{R}|)}\,.$$

By [13] it can be decided in polynomial time in $||q||$, whether or not $\mathcal{F} \models q|_{\mathcal{F}} \approx 0$. As $||q||$ is polynomial in $||f||$ (where the exponent depends only on $\mathcal{R}$ and $\mathcal{M}$), it can be decided in polynomial time in $||f||$, whether or not $\mathcal{F} \models q|_{\mathcal{F}} \approx 0$, that is whether or not $f|_{\mathcal{S}} = 0$ is solvable over $(\mathcal{R}, \mathcal{M})$.

3. Groups

In this section we consider the equivalence and equation solvability problems for groups which are semidirect products of two Abelian groups. In Section 3.2 we recall and apply the idea of the collection procedure from [17]. Then, for such groups we give polynomial time algorithms for the equivalence problem in Section 3.3, and for the equation solvability problem in Section 3.4. First, we introduce some notations that we use throughout this section.

3.1. **Notations.** Let $\mathbf{G} = \mathbf{A} \rtimes \mathbf{B}$ be a finite group, where $\mathbf{A}$ is Abelian. The semidirect product is defined by a homomorphism $\varphi\colon \mathbf{B} \to \operatorname{Aut}\mathbf{A}$ determining how $\mathbf{B}$ acts on $\mathbf{A}$ by conjugation. We denote this action by putting it in the exponent: $a^{\varphi(b)} = a^b = b^{-1}ab$ for $a \in \mathbf{A}$, $b \in \mathbf{B}$. Let $\operatorname{End}\mathbf{A}$ denote the endomorphism ring of $\mathbf{A}$, then $\operatorname{Aut}\mathbf{A}$ is the multiplicative group $(\operatorname{End}\mathbf{A})^\times$. Let $\mathcal{S} = \varphi(\mathbf{B}) \subseteq \operatorname{End}\mathbf{A}$. Note, that if the semidirect product is a direct product, then $\mathcal{S} = \varphi(\mathbf{B}) = \{1\}$. Let $\mathcal{R}$ denote the subring of $\operatorname{End}\mathbf{A}$ generated by $\mathcal{S}$: $\mathcal{R} = \langle\mathcal{S}\rangle = \langle\varphi(\mathbf{B})\rangle$. Let $\mathcal{R}^\times$ denote the multiplicative group of $\mathcal{R}$, then $\mathcal{S} \leq \mathcal{R}^\times$, and $1 \in \mathcal{R}$. If $\mathcal{S}$ or $\operatorname{End}\mathbf{A}$ are commutative, then so is $\mathcal{R}$. Furthermore, $\mathbf{A}$ is a faithful left module over $\operatorname{End}\mathbf{A}$, and thus over $\mathcal{R}$, as well. Let $r = \sum_{i=1}^{k} s_k$ for some $s_i = \varphi(b_i)$ ($b_i \in \mathbf{B}$, $1 \leq i \leq k$), then we denote the action of $r \in \mathcal{R}$ on some $a \in \mathbf{A}$ by writing a^r, that is

$$a^r = \prod_{i=1}^{k} a^{s_i} = \prod_{i=1}^{k} a^{\varphi(b_i)} = \prod_{i=1}^{k} a^{b_i} = \prod_{i=1}^{k} \left(b_i^{-1}ab_i\right).$$

The order of the multiplication can be arbitrary as $\mathbf{A}$ is commutative.

3.2. **Collecting precedure.** Let $t(x_1, \ldots, x_n) = t_1 t_2 \ldots t_k$ be a polynomial over $\mathbf{G}$, where each t_i is either a variable or a constant from $\mathbf{G}$ ($1 \leq i \leq k$). Now, the length of t is defined to be $||t|| = k$. Let $X = \{x_1, \ldots, x_n\}$. Since $\mathbf{G} = \mathbf{A} \rtimes \mathbf{B}$, every element $g \in \mathbf{G}$ can be uniquely written as a product ba such that $a \in \mathbf{A}$ and $b \in \mathbf{B}$. Let $Y = \{y_1, \ldots, y_n\}$ and $Z = \{z_1, \ldots, z_n\}$ be sets of new variables such that the sets X, Y and Z are pairwise disjoint. For $1 \leq i \leq k$ let $a_i = a_i(y_1, \ldots, y_n)$ and $b_i = b_i(z_1, \ldots, z_n)$ be the following expressions:

- if $t_i = x_j$ then let $a_i = y_j$, $b_i = z_j$,
- if $t_i \in \mathbf{G}$, then let $a_i \in \mathbf{A}$ and $b_i \in \mathbf{B}$ be the unique constants such that $t_i = b_i a_i$.

We replace every x_j with $z_j y_j$ (where y_j is going to be a variable over $\mathbf{A}$ and z_j is going to be a variable over $\mathbf{B}$), and the constants are replaced by their representatives from $\mathbf{A} \rtimes \mathbf{B}$. Thus a_i is either a variable over $\mathbf{A}$ or a constant from $\mathbf{A}$, and b_i is either a variable over $\mathbf{B}$ or a constant from $\mathbf{B}$. Now, $t = b_1 a_1 b_2 a_2 \ldots b_k a_k$. Collecting every b_i to the left we obtain

$$t = (b_1 b_2 \ldots b_k) \cdot \left(a_1^{b_2 b_3 \ldots b_k} a_2^{b_3 \ldots b_k} \ldots a_{k-1}^{b_k} a_k\right).$$

Let

$$t_b = t_b(z_1, \ldots, z_n) = b_1 b_2 \ldots b_k, \tag{6}$$

$$t_a = t_a(z_1, \ldots, z_n; y_1, \ldots, y_n) = a_1^{b_2 b_3 \ldots b_k} a_2^{b_3 \ldots b_k} \ldots a_{k-1}^{b_k} a_k. \tag{7}$$

Here, t_b is a polynomial over $\mathbf{B}$ using variables from Z. In t_a the expressions $a_i^{b_{i+1}\dots b_k}$ are module monomials over $(\mathcal{R}, \mathbf{A})$, that is t_a is a module polynomial over $(\mathcal{R}, \mathbf{A})$ written as a sum of module monomials. Furthermore, $||t_b|| = O(||t||)$, $||t_a|| = O\left(||t||^2\right)$. The main observation is that t attains the value 1 for a substitution from $\mathbf{G}$ if and only if t_a and t_b attain 1 simultaneously for the corresponding substitution.

Proposition 7. *Let $\mathbf{G} = \mathbf{A} \rtimes \mathbf{B}$. Let $t(x_1, \dots, x_n) = t_1 t_2 \dots t_k$ be a polynomial over $\mathbf{G}$. Let t_b and t_a be the expressions defined by (6) and (7). Then $t_b(u_1, \dots, u_n) \in \mathbf{B}$, $t_a(u_1, \dots, u_n; v_1, \dots, v_n) \in \mathbf{A}$ for arbitrary $u_1, \dots, u_n \in \mathbf{B}$, $v_1, \dots, v_n \in \mathbf{A}$, and for $g_i = u_i v_i$ we have*

$$t(g_1, \dots, g_n) = t_b(u_1, \dots, u_n) \cdot t_a(u_1, \dots, u_n; v_1, \dots, v_n).$$

3.3. **Equivalence.** We prove Theorem 1.

Proof of Theorem 1. Let $\mathcal{S}$ denote the action of $\mathbf{B}$ over $\mathbf{A}$ in the ring $\operatorname{End}\mathbf{A}$, and let $\mathcal{R}$ be the subring of $\operatorname{End}\mathbf{A}$ generated by $\mathcal{S}$. Now, $\mathcal{S} \simeq \mathbf{B}/C_{\mathbf{B}}(\mathbf{A})$ is commutative, and so is $\mathcal{R}$. Let 1 denote the unit element of $\mathbf{B}$ and $\mathbf{G}$, and 0 denote the unit element of $\mathbf{A}$. Let t_b and t_a be the expressions defined by (6) and (7). By Proposition 7 we have that $\mathbf{G} \models t \approx 1$ if and only if $\mathbf{B} \models t_b \approx 1$ and $(\mathcal{R}, \mathbf{A}) \models t_a \approx 0$ for every substitution from $\mathcal{S}$. The first condition can be checked in polynomial time in $||t_b|| = O(||t||)$ by the assumption. The second condition can be checked in polynomial time in $||t_a|| = O\left(||t||^2\right)$ by Corollary 5. □

Corollary 8. *The equivalence problem is in P for the following finite groups:*

(a) $\mathbf{G} = \mathbf{A} \rtimes \mathbf{B}$, *where both* $\mathbf{A}$ *and* $\mathbf{B}$ *are Abelian,*
(b) $\mathbf{G} = \mathbf{Z}_n \rtimes \mathbf{B}$, *where the (polynomial) equivalence problem over* $\mathbf{B}$ *is in P,*
(c) $\mathbf{G} = \mathbf{Z}_{n_1} \rtimes (\mathbf{Z}_{n_2} \rtimes \dots \rtimes (\mathbf{Z}_{n_k} \rtimes (\mathbf{A} \rtimes \mathbf{B})))$, *where both* $\mathbf{A}$ *and* $\mathbf{B}$ *are Abelian.*

Proof. Item (a) follows directly from Theorem 1. For item (b) note that $\operatorname{End}\mathbf{Z}_n = \mathbb{Z}_n$ is Abelian, hence so is $\mathbf{B}/C_{\mathbf{B}}(\mathbf{A})$. Finally, one can prove item (c) by induction on k using items (a) and (b). □

3.4. **Equation solvability.**

Theorem 9. *Let $\mathbf{G} = \mathbf{A} \rtimes \mathbf{B}$, and assume that both $\mathbf{A}$ and $\mathbf{B}$ are commutative. Let $\mathcal{S}$ denote the action of $\mathbf{B}$ over $\mathbf{A}$ in the ring $\operatorname{End}\mathbf{A}$, and let $\mathcal{R}$ be the subring of $\operatorname{End}\mathbf{A}$ generated by $\mathcal{S}$. If the module sigma equation solvability problem over $(\mathcal{R}, \mathbf{A})$ for substitutions from $\mathcal{S}$ is in P, then so is the equation solvability problem over $\mathbf{G}$. In particular, if $\mathcal{R}$*

is direct indecomposable, or $\mathcal{R}^\times$ is cyclic, then the equation solvability problem over $\mathbf{G}$ is in P.

Proof. Let 1 denote the unit element of $\mathbf{B}$ and $\mathbf{G}$, and 0 denote the unit element of $\mathbf{A}$. Let t_b and t_a be the expressions defined by (6) and (7). By Proposition 7 the equation $t = 1$ can be solved over $\mathbf{G}$ if and only if there exist $a_1, \dots, a_n \in \mathbf{A}$, $b_1, \dots, b_n \in \mathbf{B}$ such that $t_b(b_1, \dots, b_n) = 1$ and $t_a(b_1, \dots, b_n; a_1, \dots, a_n) = 0$. Using the algorithm providing the Smith normal form for modules over principal ideal domains [32], one can solve the equation $t_b = 1$ in $O\left(||t_b||^2\right)$ time by expressing one variable using the other variables. Let the solutions of $t_b = 1$ be $z_j = \prod_{k=1}^{n} u_k^{c_{jk}}$ $(1 \leq j \leq n)$, where $u_1 = b\prod_{k=2}^{n} u_k^{d_k}$ for some nonnegative integers c_{jk}, d_k and $b \in \mathbf{B}$. Substitute these solutions into t_a to obtain a module polynomial $t'_a = t'_a(u_2, \dots, u_n; y_1, \dots, y_n)$ over $(\mathcal{R}, \mathbf{A})$ written as a sum of module monomials, where variables u_i $(2 \leq i \leq n)$ are substituted from $\mathcal{S}$. Whether $t'_a(u_2, \dots, u_n; y_1, \dots, y_n) = 0$ has a solution can be decided in polynomial time in $||t'_a|| = O(||t_a||) = O\left(||t||^2\right)$ by the assumption.

In particular, if $\mathcal{R}$ is direct indecomposable, or $\mathcal{R}^\times$ is cyclic, then the conditions of Corollary 4 clearly hold, and the module sigma equation solvability problem over $(\mathcal{R}, \mathbf{A})$ for substitutions from $\mathcal{S}$ is in P. □

Finally, we prove Corollary 2.

Proof of Corollary 2. (a) $\mathbf{G} = \mathbf{Z}_n \rtimes \mathbf{B}$, where $n = p^\alpha$ or $n = 2p^\alpha$ for some prime p. Now, $\operatorname{End}\mathbf{Z}_n = \mathbb{Z}_n$, and $1 \in \mathcal{S}$ yields $\mathcal{R} = \mathbb{Z}_n$, as well. If n is a 2-power, then $\mathcal{R}$ is direct indecomposable, and Theorem 9 finishes the proof. If $n = p^\alpha$ or $n = 2p^\alpha$ for some odd prime p, then $\mathcal{R}^\times$ is cyclic, and again, the statement follows from Theorem 9.

(b) $\mathbf{G} = \mathbf{Z}_p^n \rtimes \mathbf{B}$, such that $|\mathbf{B}/C_{\mathbf{B}}(\mathbf{A})| \in \{1, q\}$ for some distinct primes p, q, where p is a primitive root modulo q. Now, the action of $\mathbf{B}$ on $\mathbf{Z}_p^n$ is cyclic, let the matrix $B \in \mathbb{Z}_p^{n\times n}$ denote a generator of this action. Consider the minimal polyomial $m_B(x)$ of B over the p-element field $\mathbb{Z}_p$. Since $B^q = I$, we have $m_B(x) \mid x^q - 1$. Here, $x^q - 1 = (x-1)\cdot\Phi_q(x)$, where the cyclotomic polynomial $\Phi_q(x)$ is irreducible over $\mathbb{Z}_p$, because p is a primitive root modulo q (see e.g. [26, Theorem 2.47]). Thus, $m_B(x) \in \{x - 1, \Phi_q(x), x^q - 1\}$. We distinguish two cases.

If either $m_B(x) = x - 1$ or $m_B(x) = \Phi_q(x)$, then $m_B(x)$ is irreducible, and B generates a subring $\mathcal{R}$ in $\mathbb{Z}_p^{n\times n}$ isomorphic to a field. Thus, $\mathcal{R}$ is a field, hence $\mathcal{R}$ is indecomposable, and Theorem 9 finishes the proof.

If $m_B(x) = x^q - 1$, then 1 is an eigenvalue of $m_A(x)$. Changing the basis we can assume that $B = \begin{pmatrix} I & 0 \\ 0 & C \end{pmatrix}$, where I denotes the identity matrix, and $m_C(x) = \Phi_q(x)$. Now, B generates a subring $\mathcal{R}$ in $\mathbb{Z}_p^{n\times n}$ isomorphic to the direct sum of two fields $\mathcal{F}_1 \oplus \mathcal{F}_2$. Furthermore, $\mathcal{S} = \mathcal{S}_1 \oplus \mathcal{S}_2$, where $\mathcal{S}_1 = \{ 1 \} \subseteq \mathcal{F}_1$ and $\mathcal{S}_2 \subseteq \mathcal{F}_2^\times$. Hence the conditions of Corollary 4 are fulfilled, and our statement follows.

(c) $\mathbf{G} = \mathbf{Z}_p^n \rtimes \mathbf{B}$, such that $|\mathbf{B}/C_{\mathbf{B}}(\mathbf{A})| \in \{ 1, q \}$ for some distinct primes p, q, where the order of p modulo q is some $d \geq 2$ and $n \leq d + 1$. The proof is essentially the same as for item (b). Again, the action of $\mathbf{B}$ is cyclic, let B denote a generator of this action. Again, $m_B(x) \mid x^q - 1 = (x - 1) \cdot \Phi_q(x)$, but now $\Phi_q(x)$ is not necessarily irreducible over $\mathbb{Z}_p$, $\Phi_q(x)$ splits into $(q-1)/d$-many distinct irreducible polynomials of degree d (see e.g. [26, Theorem 2.47]). Since the degree of $m_B(x)$ is at most $n \leq d + 1$, there exists an irreducible factor $r(x)$ of $\Phi_q(x)$ such that $m_B(x) \mid (x - 1) \cdot r(x)$. From here, the proof is literally the same as for item (b).

□

4. Remarks, open problems

We wrote a computer program for Theorems 1 and 9 in GAP [5] using the SONATA package [1], and ran it on the supercomputer of University of Debrecen [28] to determine the smallest groups for which the complexities of the equivalence and equation solvability problems are yet unknown. In fact, we determined all such groups up to order 767 for the equivalence problem and up to order 383 for the equation solvability problem. Up to order 23, every group has polynomial time equivalence and polynomial time equation solvability. In Sections 6 and 7 we list the GAP SmallGroup identifications and StructureDescriptions of the groups of order at most 60 with currently unknown equivalence and equation solvability complexities. The GAP source code and the full list can be found on the website [14].

First, we list open questions about the equivalence problem in Section 4.1, then about the equation solvability problem in Section 4.2.

4.1. **Equivalence.** There are two groups of order 24 for which the complexity of the equivalence problem is not known: $\mathbf{S}_4$ and $\mathbf{SL_2}(\mathbb{Z}_3)$. The complexity of the equation solvability problem is unknown for these groups, either.

Problem 1. Determine the complexity of the equivalence and equation solvability problems over the group $\mathbf{S}_4$.

Now, $\mathbf{S}_4$ is a semidirect product of $\mathbf{A} = \mathbf{Z}_2^2$ and $\mathbf{B} = \mathbf{S}_3$. Here, $\operatorname{End}\mathbf{A} = \mathbb{Z}_2^{2\times 2}$, the action of $\mathbf{B}$ over $\mathbf{A}$ is $\mathcal{S} = \operatorname{Aut}\mathbf{A} = (\operatorname{End}\mathbf{A})^\times$. Thus, $\mathcal{R} = \mathbb{Z}_2^{2\times 2}$ and $\mathcal{S} = \mathbf{GL_2}(\mathbb{Z}_\mathbf{2})$. That is, in order to determine the complexities of the equivalence and equation solvability problems for $\mathbf{S}_4$, one needs to consider (module) sigma problems over *noncommutative* rings $\mathcal{R}$ with substitutions from a *proper subset* of $\mathcal{R}$. The currently existing results consider either commutative rings or noncommutative rings without the restriction on substitutions.

Problem 2. Let $\mathcal{R}$ be a noncommutative, unital ring, $\mathcal{S} \leq \mathcal{R}^\times$. Determine the complexity of the (module) sigma equivalence and (module) sigma equation solvability problems over $\mathcal{R}$ for substitutions from $\mathcal{S}$. In particular, determine these complexities in the case $\mathcal{R} = \mathbb{Z}_2^{2\times 2}$ and $\mathcal{S} = \mathbf{GL_2}(\mathbb{Z}_\mathbf{2})$.

For $\mathbf{SL_2}(\mathbb{Z}_\mathbf{3})$ the problem is different: $\mathbf{SL_2}(\mathbb{Z}_\mathbf{3})$ is the semidirect product of the *non-Abelian* Quaternion group $\mathbf{Q}$ and $\mathbf{Z}_3$. Current techniques can only handle semidirect products if the normal subgroup is Abelian.

Problem 3. Determine the complexity of the equivalence and equation solvability problems over the group $\mathbf{SL_2}(\mathbb{Z}_\mathbf{3})$.

A similar obstacle arises with a 54-element group $\mathbf{G}$, namely, that the normal subgroup is not commutative. This group $\mathbf{G}$ is the semidirect product of the non-Abelian group of strictly upper triangular 3×3 matrices over $\mathbb{Z}_3$ (denoted by $\mathbf{U}(\mathbf{3}, \mathbb{Z}_\mathbf{3})$ and the group $\mathbf{Z}_2$.

Problem 4. Determine the complexity of the equivalence and equation solvability problems over the group $\mathbf{U}(\mathbf{3}, \mathbb{Z}_\mathbf{3}) \rtimes \mathbf{Z}_2$.

Note, that the complexity of the equivalence problem is unknown for some 48-element groups, but those are all extensions of $\mathbf{S}_4$ or $\mathbf{SL_2}(\mathbb{Z}_\mathbf{3})$, therefore their examination should come after these two groups are handled.

4.2. **Equation solvability.** As for the equation solvability problem, there are much more groups for which our method does not work. For example, one might wonder if item (a) in Corollary 2 can be further generalized. The smallest group which is not handled by that statement is $\mathbf{Z}_{12} \rtimes \mathbf{Z}_2 = \mathbf{D}_{12}$.

Problem 5. Determine the complexity of the equation solvability problem over the group $\mathbf{D}_{12}$.

Indeed, in this situation $\mathcal{R} = \mathbb{Z}_{12} \simeq \mathbb{Z}_3 \times \mathbb{Z}_4$, but $\mathcal{S} = \{ 1, -1 \}$ does not split into a direct product of subgroups of $\mathbb{Z}_3^\times$ and of $\mathbb{Z}_4^\times$, hence Corollary 4 cannot be applied directly. There is a similar problem with a lot of other dihedral groups.

Problem 6. Determine the complexity of the (module) sigma equation solvability problem over $\mathcal{R} = \mathbb{Z}_{12}$ for substitutions from $\mathcal{S} = \{ 1, -1 \}$.

One might wonder, whether the splitting of $\mathcal{S}$ into direct factors is really necessary. For example, consider the group $(\mathbf{Z}_5 \times \mathbf{Z}_5) \rtimes \mathbf{Z}_4$ with generators a, b, c, respectively, where $a^c = a^2$ and $b^c = b^3$. Now, $\mathcal{R} = \mathbb{Z}_5 \oplus \mathbb{Z}_5$, but $\mathcal{S}$ is not a direct product, and Corollary 4 cannot be applied directly. Nevertheless, the elements of $\mathcal{S}$ can be written nicely as $\{ (s, -s) : s \in \mathbb{Z}_5 \}$. With this representation, an equation $f(x_1, \ldots, x_n) = 0$ can be solved over $\mathbb{Z}_5 \oplus \mathbb{Z}_5$ by substitutions from $\mathcal{S}$ if and only if the system of equations

$$\begin{aligned} f(x_1, \ldots, x_n) &= 0, \\ f(-x_1, \ldots, -x_n) &= 0 \end{aligned}$$

can be solved over $\mathbb{Z}_5$ by substituting from $\mathbb{Z}_5^\times$. Therefore the condition of $\mathcal{S}$ being a direct product in Corollary 4 is not essential: in some situations one can have further results with some clever observations.

Problem 7. Determine the complexity of the (module) sigma equation solvability problem over an arbitrary commutative ring $\mathcal{R}$ for substitutions from an arbitrary $\mathcal{S} \leq \mathcal{R}^\times$.

There are two more groups of order 24 for which the complexity of the equation solvability problem is unknown. One of them is $\mathbf{Z}_3 \rtimes \mathbf{Q}$, where $\mathbf{Q}$ is the Quaternion group. The other one is $(\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_3) \rtimes \mathbf{Z}_2$, where the action switches the two generators of $\mathbf{Z}_2 \times \mathbf{Z}_2$ and the two generators of $\mathbf{Z}_3$.

Problem 8. Determine the complexity of the equation solvability problem over the groups $\mathbf{Z}_3 \rtimes \mathbf{Q}$ and $(\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_3) \rtimes \mathbf{Z}_2$.

5. Acknowledgements

We are indebted to the anonymous referee for their useful suggestions which extremely improved the presentation of the paper.

This paper was supported by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences, by the European Union and the European Social Fund through project Supercomputer, the national virtual lab (grant no.: TAMOP-4.2.2.C-11/1/KONV-2012-0010), by the European Union's Seventh Framework Programme (FP7/2007-2013)

under grant agreement no. 318202, and by the Hungarian Scientific Research Fund (OTKA) grant no. K109185.

References

[1] E. Aichinger, F. Binder, J. Ecker, P. Mayr, and C. Nöbauer. *SONATA - system of near-rings and their applications, GAP package, Version 2.6*, 2012. `http://www.algebra.uni-linz.ac.at/Sonata/`.

[2] J. Almeida, M. V. Volkov, and S. V. Goldberg. Complexity of the identity checking problem for finite semigroups. *Journal of Mathematical Sciences*, 158(5):605–614, 2009.

[3] S. Burris and J. Lawrence. The equivalence problem for finite rings. *J. of Symb. Comp.*, 15:67–71, 1993.

[4] S. Burris and J. Lawrence. Results on the equivalence problem for finite groups. *Alg. Univ.*, 52(4):495–500, 2004. (2005).

[5] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.7.7*, 2015, `http://www.gap-system.org`

[6] S. Goldberg. Complexity of the identity checking problem over semigroups of rank 2 (in Russian). *Proceedings of Ural State University*, 74:27–38, 2010.

[7] 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.

[8] T. A. Gorazd and J. Krzaczkowski. Term equation satisfiability over finite algebras. *Internat. J. Algebra Comput.*, 20(8):1001–1020, 2010.

[9] T. A. Gorazd and J. Krzaczkowski. The complexity of problems connected with two-element algebras. *Rep. Math. Logic*, 46:91–108, 2011.

[10] T. A. Gorazd and J. Krzaczkowski. Term satisfiability problem for two-element algebras is in QL or is NQL-complete. *J.UCS*, 19(10):1375–1395, 2013.

[11] M. Hazewinkel, N. Gubareni, and V. V. Kirichenko. *Algebras, Rings and Modules*, volume 1. Springer, 2004.

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

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

[14] G. Horváth. Gap programs. `http://math.unideb.hu/horvath-gabor/research.html`, 2015.

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

[16] G. Horváth, J. Lawrence, and R. Willard. The complexity of the equation solvability problem over finite rings. 2015. manuscript.

[17] G. Horváth and Cs. Szabó. The complexity of checking identities over finite groups. *Internat. J. Algebra Comput.*, 16(5):931–939, 2006.

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

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

[20] A. Kisielewicz. Complexity of semigroup identity checking. *Int. J. of Alg. and Comp.*, 14(4):455–464, 2004.

[21] S. Kitaev and S. Seif. Word problem of the Perkins semigroup via directed acyclic graphs. *Order*, 25(3):177–194, 2008.
[22] O. Klíma. *Unification Modulo Associativity and Idempotency*. PhD thesis, Masarik University, Brno, 2004.
[23] O. Klíma. Complexity issues of checking identities in finite monoids. *Semigroup Forum*, 79(3):435–444, 2009.
[24] O. Klíma. Identity checking problem for transformation monoids. *Semigroup Forum*, 84(3):487–498, 2012.
[25] J. Lawrence and R. Willard. The complexity of solving polynomial equations over finite rings. manuscript, 1997.
[26] R. Lidl and H. Niederreiter. *Introduction to finite fields and their applications*. Cambridge University Press, Cambridge, first edition, 1994.
[27] B. R. MacDonald. *Finite rings with identity*. M. Dekker, 1974.
[28] University of Debrecen. HPC-NVL supercomputer. `http://hpc-nvl.unideb.hu`, 2015.
[29] S. Plescheva and V. Vértesi. Checking identities in 0-simple semigroups (in Russian). *Journal of Ural State University*, 43:72–102, 2006.
[30] R. Raghavendran. Finite associative rings. *Compositio Math.*, 21(2):195–229, 1969.
[31] S. Seif and Cs. Szabó. Computational complexity of checking identites in 0-simple semigroups and matrix semigroups over finite fields. *Semigroup Forum*, 72(2):207–222, 2006.
[32] H. J. S. Smith. On systems of linear indeterminate equations and congruences. *Philosophical Transactions of the Royal Society of London*, 151:pp. 293–326, 1861.
[33] Cs. Szabó and V. Vértesi. The equivalence problem over finite rings. *Internat. J. Algebra Comput.*, 21(3):449–457, 2011.
[34] R. S. Wilson. On the structure of finite rings. *Compositio Math.*, 26(1):79–93, 1973.

6. Appendix A: Groups of size at most 60 with unknown complexity for equivalence

```
[ 24,  3 ] SL(2,3)
[ 24, 12 ] S4
[ 48, 28 ] C2 . S4 = SL(2,3) . C2
[ 48, 29 ] GL(2,3)
[ 48, 30 ] A4 : C4
[ 48, 32 ] C2 x SL(2,3)
[ 48, 33 ] SL(2,3) : C2
[ 48, 48 ] C2 x S4
[ 54,  8 ] ((C3 x C3) : C3) : C2
```

7. Appendix B: Groups of size at most 60 with unknown complexity for equation solvability

```
[ 24,  3 ] SL(2,3)
[ 24,  4 ] C3 : Q8
[ 24,  6 ] D24
[ 24,  8 ] (C6 x C2) : C2
[ 24, 12 ] S4
[ 30,  3 ] D30
[ 40,  4 ] C5 : Q8
[ 40,  6 ] D40
[ 40,  8 ] (C10 x C2) : C2
[ 42,  5 ] D42
[ 48,  5 ] C24 : C2
[ 48,  6 ] C24 : C2
[ 48,  7 ] D48
[ 48,  8 ] C3 : Q16
[ 48, 10 ] (C3 : C8) : C2
[ 48, 12 ] (C3 : C4) : C4
[ 48, 13 ] C12 : C4
[ 48, 14 ] (C12 x C2) : C2
[ 48, 15 ] (C3 x D8) : C2
[ 48, 16 ] (C3 : C8) : C2
[ 48, 17 ] (C3 x Q8) : C2
[ 48, 18 ] C3 : Q16
[ 48, 19 ] (C2 x (C3 : C4)) : C2
[ 48, 28 ] C2 . S4 = SL(2,3) . C2
[ 48, 29 ] GL(2,3)
[ 48, 30 ] A4 : C4
[ 48, 32 ] C2 x SL(2,3)
[ 48, 33 ] SL(2,3) : C2
[ 48, 34 ] C2 x (C3 : Q8)
[ 48, 36 ] C2 x D24
[ 48, 37 ] (C12 x C2) : C2
[ 48, 39 ] (C2 x (C3 : C4)) : C2
[ 48, 41 ] (C4 x S3) : C2
[ 48, 43 ] C2 x ((C6 x C2) : C2)
[ 48, 48 ] C2 x S4
[ 54,  8 ] ((C3 x C3) : C3) : C2
[ 56,  3 ] C7 : Q8
[ 56,  5 ] D56
[ 56,  7 ] (C14 x C2) : C2
```

[60, 3] C15 : C4
[60, 7] C15 : C4
[60, 12] D60