THE COMPLEXITY OF THE EQUATION SOLVABILITY PROBLEM OVER FINITE RINGS

GÁBOR HORVÁTH, JOHN LAWRENCE, AND ROSS WILLARD

ABSTRACT. Given a finite ring $\mathcal{R}$, the *sum-of-monomials equation solvability problem* for $\mathcal{R}$ is the decision problem which, given a polynomial in noncommuting variables over $\mathcal{R}$ expressed as a sum of monomials, asks whether the polynomial has a zero in $\mathcal{R}$. We prove that this problem can be decided in polynomial time if the quotient of $\mathcal{R}$ by its Jacobson radical is commutative. An immediate consequence is that for such $\mathcal{R}$ the *sum-of-monomials equivalence problem* for $\mathcal{R}$, which asks if the input polynomial is identically zero for all substitutions from $\mathcal{R}$, is also decidable in polynomial time. As these problems were known to be NP-complete and coNP-complete respectively for all other finite rings, our result completes the proof of dichotomy theorems for these two problems. As a stepping stone to our proofs, we give an upper bound to the time complexity of deciding whether a system of polynomial equations over a finite commutative ring has a solution in the ring. Our algorithm and the proof of its correctness depend heavily on the theory of Galois rings.

1. INTRODUCTION

Investigations into the algorithmic aspects of various classical algebraic problems has received increasing attention in the past half century. The *equation solvability problem* is one of the most basic problems of algebra: it asks for a commutative finite ring $\mathcal{R}$ whether or not a polynomial $p \in \mathcal{R}[x_1, \ldots, x_n]$ can attain the value zero for some substitution, i.e. if the equation $p = 0$ can be solved over $\mathcal{R}$. A related problem is the *equivalence problem* which asks whether or not a polynomial $p \in \mathcal{R}[x_1, \ldots, x_n]$ is identically zero over $\mathcal{R}$ (denoted by

Date: July 31, 2017.

2010 *Mathematics Subject Classification.* 16Z05, 13P15, 13M10, 16-04, 16P10.

Key words and phrases. finite rings, equation solvability, computational complexity, polynomial time algorithm, commutative rings, solvability of system of equations, equivalence.

The first author was partially supported by the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 318202, by the Hungarian National Research, Development and Innovation Office (NKFIH) grant no. K109185 and grant no. FK124814, and by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences. The third author was partially supported by a Discovery Grant from the Natural Sciences and Engineering Research Council of Canada.

$\mathcal{R} \models p \approx 0$), i.e. if p determines the constant zero function over $\mathcal{R}$. Analogous problems can be naturally formulated for noncommutative rings, at the expense of passing to polynomials in noncommuting variables.

These are computational problems, parametrized by the finite ring $\mathcal{R}$, whose complexity we wish to understand. Their complexity depends (assuming P $\neq$ NP) on the choice of $\mathcal{R}$. For example, if $\mathcal{R}$ is the 2-element field, then equation solvability includes 3-SAT and so is NP-complete, while if $\mathcal{R}$ is a non-unital ring in which all products are 0, then both the equation solvability and equivalence problems are easily seen to be in P. Hunt and Stearns [10] fully classified all finite commutative rings according to the complexity of their equation solvability and equivalence problems in 1990. Burris and Lawrence [2] generalized the context to non-commutative rings and determined the complexities if the rings were not nilpotent. Finally, the first author [6] handled equation solvabililty for nilpotent rings, establishing the following dichotomy:

Theorem 1 ([10, 2, 6])**.** *Let $\mathcal{R}$ be a finite, not necessarily unital ring. If $\mathcal{R}$ is nilpotent, then both the equation solvability and equivalence problems can be solved in polynomial time. If $\mathcal{R}$ is not nilpotent, then the equation solvability problem is NP-complete and the equivalence problem is coNP-complete.*

This is not, however, the end of the story. In [10, 2, 6], polynomials were permitted to be given to the solver as arbitrary formal expressions built from variables and elements of $\mathcal{R}$, using addition and multiplication. This is natural from the perspective of logic (in which a ring is merely an example of a formal algebraic structure), but less natural to ring theorists for whom polynomials "are" sums of monomials. The distinction matters: a formal expression of the form

$$(x_1 + x_5)(x_2 + x_3 + 1)(x_2 + x_7 + r) \dots (x_i + x_j + s) \quad (n \text{ factors})$$

has length $O(n)$, while the sum of monomials that it represents (obtained from the expression by formally expanding it) is exponentially longer. As the computational complexities of the equation solvability and equivalence problems are, by definition, measured against the space used to describe their inputs, the complexities may decrease when formal expressions of the kind displayed above are disallowed as inputs.

In this paper we study the equation solvability and equivalence problems restricted to "honest" inputs being sums of monomials (we will define these precisely in Section 2.1). We call these restricted problems the *sum-of-monomial (SM) equation solvability* and *sum-of-monomial (SM) equivalence* problems, respectively. The SM equation solvability and SM equivalence problems were introduced by the second and third author in the unpulished manuscript [12], and a dichotomy conjecture was formulated about their complexities.

Conjecture 2 ([12]). *Let $\mathcal{R}$ be a finite ring and $\mathcal{J}$ be its Jacobson radical. If $\mathcal{R}/\mathcal{J}$ is commutative, then the SM equation solvability and the SM equivalence problems are decidable in polynomial time. If $\mathcal{R}/\mathcal{J}$ is not commutative, then the SM equation solvability problem is NP-complete, and the SM equivalence problem is coNP-complete.*

For most matrix rings, arguments of [12] establish NP-completeness for the SM equation solvability problem and coNP-completeness for the SM equivalence problem. For commutative rings, polynomial-time algorithms for both problems were drafted in [12] as well. However, [12] was never submitted for publication. Meanwhile, the first author (Horváth) tackled the commutative ring case of the SM equivalence problem in [7], and the SM equation solvability problem in the special situation when the variables are substituted from the multiplicative subgroup of the ring [8]. The latter approach was then applied to bring all previously existing positive complexity results about the analogous equation solvability and equivalence problems over finite groups under a unified roof.

Szabó and Vértesi in [15] proved coNP-completeness for the SM equivalence part of Conjecture 2. For matrix rings they prove a stronger theorem, that is the SM equivalence problem is coNP-complete even if the input polynomials are restricted to only one monomial. To this problem they reduce the equivalence problem over the multiplicative subgroup of matrix rings, which is coNP-complete by [9]. For matrix rings [1] proves coNP-completeness, as well. The NP-completeness of the SM equation solvability follows from the methods of [15, 1].

In this paper we confirm Conjecture 2 in the case where $\mathcal{R}/\mathcal{J}$ is commutative, thereby completing the proof of the dichotomy conjecture. The main result of the paper is the following.

Theorem 3. *Let $\mathcal{R}$ be a not necessarily unital, finite ring, and let $\mathcal{J}$ denote its Jacobson radical. Assume that $\mathcal{R}/\mathcal{J}$ is commutative. Then the SM equation solvability and SM equivalence problems for $\mathcal{R}$ are decidable in polynomial time.*

The structure of the paper is the following. We summarize most of the definitions and notations in Section 2.1. For the proofs we apply the theory of Galois rings, and summarize some of their most important properties in Section 2.2. In Section 2.3 we establish how tensor products of Galois rings behave. Then in Section 2.4 we reduce both the SM equivalence and the SM equation solvability problems to checking these problems over finite rings of prime power characteristic. For commutative rings a similar reduction yields to checking these problems over finite, commutative, local rings of prime power characteristic.

The main result of the paper (Theorem 3) is proved in Section 4. The proof of Theorem 3 contains many technical steps, and ultimately reduces SM equation solvability over a ring $\mathcal{R}$ to solvability of a *system*

of equations over a Galois ring $\mathcal{R}^*$. To this end, first we need a technical statement (see Theorem 6 introduced in Section 2.4) for finite, commutative, unital, local rings establishing the time complexity for deciding solvability of a system of equations. Theorem 6 is proved in Section 3. In particular, Theorem 6 already proves Theorem 3 if the ring $\mathcal{R}$ is commutative. For proving Theorem 3 in the general case, we need to apply Theorem 6 in the special case of Galois rings, which we assert as Corollary 7 at the end of Section 3. Note, that tensor products of Galois rings are not needed for the proof of Theorem 6, and the readers may skip Section 2.3 if they are only interested in the commutative ring case.

Section 4 contains the rather technical proof of Theorem 3. For easier readability, we divide Section 4 into several subsections. We start by introducing the notations for the proof in Section 4.1. Then in Section 4.2 we introduce the Galois ring $\mathcal{R}^*$. Then in Section 4.3 we sketch the idea of the proof and how we reduce SM equation solvability over $\mathcal{R}$ to deciding solvability of a system of equations over $\mathcal{R}^*$. Finally, in Sections 4.4–4.9 we explain all the details of the proof. We finish the paper by giving some remarks and open problems in Section 5.

2. Preliminaries

2.1. **Definitions and notations.** Let $\mathcal{R}$ be a (not necessarily commutative, not necessarily unital) ring. A *monomial over* $\mathcal{R}$ is a formal product of noncommuting variables and elements of $\mathcal{R}$. The length of a monomial v (denoted by $\|v\|$) is the number of variables and elements of $\mathcal{R}$ occurring in v with multiplicity. A *polynomial written as sum of monomials* is a formal sum of monomials over $\mathcal{R}$. The length of a polynomial f is the sum of the lengths of the monomials occurring in f (with multiplicity), and is denoted by $\|f\|$.

Let $\mathcal{S} \subseteq \mathcal{R}$. We say that the polynomials f and g are *equivalent over* $\mathcal{R}$ *for substitutions from* $\mathcal{S}$ (and write $\mathcal{R} \models f|_{\mathcal{S}} \approx g|_{\mathcal{S}}$) if for every $s_1, \ldots, s_n \in \mathcal{S}$ the two polynomials agree on this evaluation:

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

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

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

If for disjoint sets of variables X and Y we want to emphasize that variables in X are substituted from $\mathcal{S}$ and variables in Y are substituted from $\mathcal{S}'$, then we write $\mathcal{R} \models f(X|_{\mathcal{S}}, Y|_{\mathcal{S}'}) \approx g(X|_{\mathcal{S}}, Y|_{\mathcal{S}'})$ for the equivalence and $f(X|_{\mathcal{S}}, Y|_{\mathcal{S}'}) = g(X|_{\mathcal{S}}, Y|_{\mathcal{S}'})$ for the equation solvability.

The *SM equation solvability problem over* $\mathcal{R}$ receives for input a polynomial p over $\mathcal{R}$ written as sums of monomials, and asks whether or not $f = 0$ is solvable over $\mathcal{R}$. The *SM equivalence problem over* $\mathcal{R}$ receives for input a polynomial p over $\mathcal{R}$ written as sums of monomials, and asks whether or not $\mathcal{R} \models f \approx 0$ holds.

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

Galois rings play an important role in the theory of commutative rings. They were first examined in [14], and later in [16]. In the following we list some of the most important properties of Galois rings (see e.g. [13, Chapters XVI–XVII]). Let p be a prime, c, d positive integers, and let $h_d \in \mathbb{Z}[x]$ be a monic polynomial of degree d which is irreducible modulo p. Then the *Galois ring* $\mathcal{GR}(p^c, d)$ is the factor ring $\mathbb{Z}[x] / (p^c, h_d(x))$.

The Galois ring $\mathcal{GR}(p^c, d)$ is completely characterized (up to isomorphism) 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 $\mathcal{I} = (p^i)$. Hence, every ideal is principal, thus every finitely generated $\mathcal{GR}(p^c, d)$-module is a direct sum of cyclic $\mathcal{GR}(p^c, d)$-modules [16, 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 $\mathbb{F}_{p^d}$.

There are exactly d different homomorphisms from $\mathcal{GR}(p^c, d)$ onto $\mathcal{GR}(p^i, d)$ [14, p. 214, Proposition 3] for $1 \leq i \leq c$, and the automorphisms of $\mathcal{GR}(p^c, d)$ are the maps $r \mapsto r^{p^j}$ for $j \in \{0, 1, \ldots, d-1\}$ [14, p. 213, Proposition 2]. Any (non-nilpotent) subring of $\mathcal{GR}(p^c, d)$ is isomorphic to $\mathcal{GR}(p^c, d_1)$ for some $d_1 \mid d$, and for every $d_1 \mid d$ there exists a unique subring of $\mathcal{GR}(p^c, d)$ isomorphic to $\mathcal{GR}(p^c, d_1)$, which is the range of the map $r \mapsto r^{(p^d-1)/(p^{d_1}-1)}$ [14, p. 213, Proposition 1]. In particular, if a (nonzero) ring is both a subring and a homomorphic image of $\mathcal{GR}(p^c, d)$, then it is isomorphic to $\mathcal{GR}(p^c, d)$. Further, we will need the following (here $\lfloor x \rfloor$ denotes the greatest integer not greater than x):

Lemma 4. *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,

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

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. □

2.3. **Tensor products of Galois rings.** Every tensor product occurring in the paper is considered over the ring of integers $\mathbb{Z}$. For positive integers c_1, c_2, d_1, d_2 and for $c = \min\{c_1, c_2\}$, $d = \operatorname{lcm}\{d_1, d_2\}$, and $d' = \gcd\{d_1, d_2\}$ we have $\mathcal{GR}(p^{c_1}, d_1) \otimes \mathcal{GR}(p^{c_2}, d_2) \simeq \sum_1^{d'} \mathcal{GR}(p^c, d)$ [16, Proposition 1.2]. In particular, the $(k+1)$-fold tensor product $\mathcal{GR}(p^c, d) \otimes \cdots \otimes \mathcal{GR}(p^c, d) \otimes \mathcal{GR}(p^c, d)$ is isomorphic to the direct sum of d^k-many copies of $\mathcal{GR}(p^c, d)$. Moreover, the following lemma establishes how the d^k-many primitive idempotents of $\mathcal{GR}(p^c, d) \otimes \cdots \otimes \mathcal{GR}(p^c, d) \otimes \mathcal{GR}(p^c, d)$ project onto the $\mathcal{GR}(p^c, d)$ summands.

Lemma 5. *Let $\mathcal{R}^* = \mathcal{GR}(p^c, d)$, and consider the $(k+1)$-fold tensor product $\mathcal{R}^* \otimes \cdots \otimes \mathcal{R}^* \otimes \mathcal{R}^*$. Then there is a one-to-one correspondence between the primitive idempotents E of $\mathcal{R}^* \otimes \cdots \otimes \mathcal{R}^* \otimes \mathcal{R}^*$ and the k-tuples of $\left(\varphi_1^{(E)}, \ldots, \varphi_k^{(E)}\right)$, where $\varphi_i^{(E)}$ is an automorphism of $\mathcal{R}^*$ and*

$$E(q_1 \otimes \cdots \otimes q_k \otimes q_{k+1}) = E\left(1 \otimes \cdots \otimes 1 \otimes \varphi_1^{(E)}(q_1)\ldots\varphi_k^{(E)}(q_k)\, q_{k+1}\right),$$

for every $q_1, \ldots, q_k, q_{k+1} \in \mathcal{R}^*$.

Proof. We prove the lemma for $k = 1$, the statement follows for $k \geq 2$ by induction. There are exactly d automorphisms of $\mathcal{GR}(p^c, d)$ and there are exactly d primitive idempotents in $\mathcal{GR}(p^c, d) \otimes \mathcal{GR}(p^c, d)$ corresponding to the d copies of $\mathcal{GR}(p^c, d)$ summands.

Let E be a primitive idempotent in $\mathcal{GR}(p^c, d) \otimes \mathcal{GR}(p^c, d)$. Now, multiplying by E is a homomorphism from $1 \otimes \mathcal{R}^* = \mathcal{GR}(p^c, d)$ onto a subring of $E(\mathcal{R}^* \otimes \mathcal{R}^*) \simeq \mathcal{GR}(p^c, d)$. There exist $a, b \in \mathcal{R}^*$ such that $0 \neq E(a \otimes b) = E(1 \otimes b)(a \otimes 1)$, thus $0 \neq E(1 \otimes \mathcal{R}^*)$ is both a subring of $\mathcal{GR}(p^c, d)$ and a homomorphic image of $\mathcal{GR}(p^c, d)$. That is $E(1 \otimes \mathcal{R}^*) \simeq \mathcal{GR}(p^c, d)$. Similarly, $E(\mathcal{R}^* \otimes 1) \simeq \mathcal{GR}(p^c, d)$, and hence $E(1 \otimes \mathcal{R}^*) = E(\mathcal{R}^* \otimes \mathcal{R}^*) = E(\mathcal{R}^* \otimes 1)$. Thus, there exists a unique automorphism $\varphi^{(E)} \colon \mathcal{GR}(p^c, d) \to \mathcal{GR}(p^c, d)$, attained by composing the isomorphisms $\mathcal{GR}(p^c, d) \simeq E(\mathcal{R}^* \otimes 1) = E(1 \otimes \mathcal{R}^*) \simeq$

$\mathcal{GR}(p^c, d)$ (see Diagram (1)).

$$
\begin{array}{ccccc}
 & & & & 1 \otimes \mathcal{R}^* = \mathcal{GR}(p^c, d) \\
 & & & \overset{\varphi^{(E)}}{\dashrightarrow} & \Big\downarrow E \\
\mathcal{GR}(p^c, d) = \mathcal{R}^* \otimes 1 & \xrightarrow[\simeq]{E} & E(\mathcal{R}^* \otimes \mathcal{R}^*) & \simeq & \mathcal{GR}(p^c, d).
\end{array} \tag{1}
$$

For the other direction we only need to observe that for different idempotents different automorphisms correspond. Assume that the automorphism $\varphi\colon \mathcal{GR}(p^c, d) \to \mathcal{GR}(p^c, d)$ corresponds to primitive idempotents E and F, that is $E(b \otimes 1) = E(1 \otimes \varphi(b))$ and $F(b \otimes 1) = F(1 \otimes \varphi(b))$ for every $b \in \mathcal{R}^*$. Then

$$\ker E = \left\{ \sum_i a_i \otimes b_i : \sum_i \varphi(a_i)\, b_i = 0 \right\} = \ker F$$

implies $E = F$. □

2.4. **SM equation solvability over rings.** Note first, that if for a finite ring $\mathcal{R}$ the SM equation solvability problem can be decided in polynomial time, then the same is true for the SM equivalence problem. Indeed, for a polynomial f over $\mathcal{R}$ we have that $\mathcal{R} \models f \approx 0$ if and only if none of the equations $f = r$ can be solved over $\mathcal{R}$ for some $0 \neq r \in \mathcal{R}$. Thus, from now on we only consider the SM equation solvability problem.

Secondly, the SM equation solvability problem can be checked componentwise for a direct sum of finite rings. It is well known that every finite ring can be decomposed into a direct sum of finite rings with prime power characteristic. Therefore in the proof of Theorem 3 we only consider rings having prime power characteristic.

By the Pierce decomposition theorem (see e.g. [5, p. 48, 50]) every finite *commutative* ring is the direct sum of a commutative nilpotent ring and some commutative, unital, local rings. For nilpotent rings the equation solvability can be decided in polynomial time [6]. Thus for proving Theorem 3 for commutative rings, it is enough to prove that SM equation solvability can be decided in polynomial time over a finite commutative, unital, local ring of prime power characteristic. In particular, we prove the following in Section 3.

Theorem 6. *Let $\mathcal{R}$ be a finite commutative, unital local ring of prime power characteristic, and let $f_1, \ldots, f_\ell \in \mathcal{R}[x_1, \ldots, x_n]$ be polynomials written as sums of monomials. Let* log *denote base 2 logarithm, and let*

$$L = \ell \cdot |\mathcal{R}|^{2+\log|\mathcal{R}|+\log\log|\mathcal{R}|} \cdot \log|\mathcal{R}|.$$

Then it can be decided in

$$O\left((\log|R|)^L \cdot \max_{1 \leq k \leq \ell} \|f_k\|^L \right) \tag{2}$$

time whether or not the system $f_1 = 0, \dots, f_\ell = 0$ *is solvable over* $\mathcal{R}$.

3. Commutative rings

We prove Theorem 6 in this section.

3.1. **Notations.** Let $\mathcal{R}$ be a finite, commutative, unital, local ring of characteristic p^c for some prime p. 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 $\mathcal{GR}\,(p^c, d)$ [16, p. 80, Theorem B]. Let $m \geq c + \lfloor \log_p (t-1) \rfloor$ be the smallest 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 4. 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 $\mathcal{S}$ such that $\mathcal{S}$ is a representation system for $\mathcal{F}$. Note, that $s^{p^d} = s$ for every $s \in \mathcal{S}$, and $\mathcal{S}$ is a subset of the unique subring $\mathcal{R}_0$ isomorphic to $\mathcal{GR}\,(p^c, d)$ contained in $\mathcal{R}$.

Consider $\mathcal{R}$ as an $\mathcal{R}_0$-module. Thus $\mathcal{R}$ is a direct sum of cyclic $\mathcal{R}_0$-modules. Then every element of $\mathcal{R}$ can be written as $\sum_{b \in \mathcal{B}} r_b b$ for some $r_b, \in \mathcal{R}_0$, where $\mathcal{B}$ is a (weak) basis of $\mathcal{R}$. That is $\mathcal{R} = \oplus_{b \in \mathcal{B}} \mathcal{R}_0 b$ such that $\sum_{b \in \mathcal{B}} r_b b = 0$ if and only if $r_b \in \operatorname{Ann}\{\,b\,\}$ for all $b \in \mathcal{B}$. Since $\operatorname{Ann}\{\,b\,\}$ is an ideal in the Galois ring $\mathcal{R}_0 \simeq \mathcal{GR}\,(p^c, d)$, for every $b \in \mathcal{B}$ there exists $1 \leq c_b \leq c$ such that $\operatorname{Ann}\{\,b\,\} = (p^{c_b})$. Furthermore, every element of $\mathcal{R}_0$ can be uniquely written as $\sum_{i=0}^{c-1} s_i p^i$ for some $s_i \in \mathcal{S}$, and thus every element of $\mathcal{R}$ can be written in the form of $\sum_{i=0}^{c-1} \sum_{b \in \mathcal{B}} s_{i,b} p^i b$. Let $\mathcal{P}$ contain all pairs (i, b) for which $0 \leq i \leq c_b - 1$, that is

$$\mathcal{P} = \{\,(i,b) : b \in \mathcal{B}, 0 \leq i \leq c_b - 1\,\}. \tag{3}$$

Now, for every element $r \in \mathcal{R}$ there exist *unique* elements $s_{i,b} \in \mathcal{S}$ $((i,b) \in \mathcal{P})$ such that $r = \sum_{(i,b) \in \mathcal{P}} s_{i,b} p^i b$.

3.2. **Sketch of the proof of Theorem 6.** Let $X = \{\,x_1, \dots, x_n\,\}$ and let $f_1, \dots, f_\ell$ be polynomials from $\mathcal{R}[X]$ written as sums of monomials.

(a) First, by introducing a new set of variables Y, and using the unique representation $r = \sum_{(i,b) \in \mathcal{P}} s_{i,b} p^i b$, we rewrite the polynomials $f_1, \dots, f_\ell \in \mathcal{R}[X]$ into polynomials $g_1, \dots, g_\ell \in \mathcal{R}[Y]$ such that $f_1\,(X|_{\mathcal{R}}) = 0, \dots, f_\ell\,(X|_{\mathcal{R}}) = 0$ is solvable over $\mathcal{R}$ if and only if $g_1\,(Y|_{\mathcal{S}}) = 0, \dots, g_\ell\,(Y|_{\mathcal{S}}) = 0$ is solvable over $\mathcal{R}$.

(b) Again, we use the fact that $\mathcal{R}$ is a direct sum of cyclic $\mathcal{R}_0$-modules, that is $\mathcal{R} = \oplus_{b\in\mathcal{B}}\mathcal{R}_0 b$ for the (weak) basis $\mathcal{B}$. Then we can find polynomials $h_{k,b} \in \mathcal{R}_0[Y]$ for every $1 \le k \le \ell$, $b \in \mathcal{B}$ such that the system $g_1(Y|_{\mathcal{S}}) = 0, \ldots, g_\ell(Y|_{\mathcal{S}}) = 0$ can be solved over $\mathcal{R}$ if and only if the system

$$h_{k,b}(Y|_{\mathcal{S}}) = 0 \qquad (1 \le k \le \ell, b \in \mathcal{B}) \tag{4}$$

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 $\mathcal{R}_0$ for substitutions from $\mathcal{S}$.

(c) Then we reduce this system over $\mathcal{R}_0$ to a system of $\ell \cdot |\mathcal{P}|$-many equations over $\mathcal{F} = \mathcal{R}/\mathcal{J}$. In particular, we find $h_{k,i,b} \in \mathcal{F}[Y]$ $(1 \le k \le \ell, (i,b) \in \mathcal{P})$ such that the system (4) over $\mathcal{R}_0$ can be solved simultaneously if and only if the system

$$h_{k,i,b}(Y|_{\mathcal{F}}) = 0 \qquad (1 \le k \le \ell, (i,b) \in \mathcal{P}) \tag{5}$$

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

(d) Let $q = \prod_{k=1}^{\ell} \prod_{(i,b)\in\mathcal{P}} (1 - h_{k,i,b})^{p^d-1} \in \mathcal{F}[Y]$. We prove that the system (5) is *not* solvable over $\mathcal{F}$ if and only if $\mathcal{F} \models q|_{\mathcal{F}} \approx 0$.

That is, $f_1|_{\mathcal{R}} = 0, \ldots, f_\ell|_{\mathcal{R}} = 0$ is *not* solvable over $\mathcal{R}$ 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 time (2) as stated in Theorem 6. By [7] it can be decided in linear time in $\|q\|$ whether or not $\mathcal{F} \models q|_{\mathcal{F}} \approx 0$.

3.3. **Detailed proof of Theorem 6.** Let $f_1, \ldots, f_\ell \in \mathcal{R}[x_1, \ldots, x_n]$. Recall that every element $r \in \mathcal{R}$ can be uniquely written in the form $r = \sum_{(i,b)\in\mathcal{P}} s_{i,b} p^i b$ for some $s_{i,b} \in \mathcal{S}$, where $\mathcal{P}$ is defined by (3). We use this presentation in order to reduce solving $f_1 = 0, \ldots, f_\ell = 0$ over $\mathcal{R}$ to solving a system of equations over $\mathcal{R}_0$. For this we introduce the following disjoint sets of variables:

$$X = \{ x_j \mid 1 \le j \le n \},$$
$$Y = \{ y_{j,i,b} \mid 1 \le j \le n, (i,b) \in \mathcal{P} \}.$$

(a) Let $1 \le k \le \ell$ be fixed and rewrite f_k in the following manner. Replace every occurrence of x_j $(1 \le j \le n)$ in f_k with the expression $\sum_{(i,b)\in\mathcal{P}} y_{j,i,b} p^i b$. Let the resulting polynomial be $f_k^{(i)}$. Now,

$$\mathcal{R} \models f_k(X\,|_{\mathcal{R}}) \approx f_k^{(i)}(Y|_{\mathcal{S}}).$$

Let us expand $f_k^{(i)}$ as a sum of monomials, and remove monomials containing at least t elements from $\mathcal{J}$. Let $f_k^{(ii)}$ denote the resulting polynomial. Monomials containing at least t elements from $\mathcal{J}$ attain value 0 for arbitrary substitution, hence

$$\mathcal{R} \models f_k^{(i)}(Y|_{\mathcal{S}}) \approx f_k^{(ii)}(Y|_{\mathcal{S}}).$$

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

Let us rearrange every monomial of $f_k^{(ii)}$ into the form of $\prod_{y\in Y} y^{k_y} \cdot r$, where $r \in \mathcal{R}$. Since $\mathcal{R}$ is commutative, the resulting polynomial attains the same values as $f_k^{(ii)}$. Moreover, replace every constant $r \in \mathcal{R}$ occurring in $f_k^{(ii)}$ with its equivalent of the form $\sum_{(i,b)\in\mathcal{P}} s_{i,b} p^i b$ ($s_{i,b} \in \mathcal{S}$), and expand the resulting polynomial. Let the resulting polynomial be denoted by g_k. Now,

$$\mathcal{R} \models f_k\left(X|_{\mathcal{R}}\right) \approx g_k\left(Y|_{\mathcal{S}}\right).$$

Furthermore, the rearranging of the monomials and the expansion can be done in $O\left(|\mathcal{P}| \cdot \left\|f_k^{(ii)}\right\|\right)$ time. Thus, g_k can be computed in $O\left(|\mathcal{P}|^{t+1} \cdot \|f_k\|^t\right)$ time and $\|g_k\| = O\left(|\mathcal{P}|^{t+1} \cdot \|f_k\|^t\right)$.

(b) Again, fix $1 \leq k \leq \ell$. Now,

$$g_k\left(Y\right) = \sum_{k=1}^{\ell} \sum_{b\in\mathcal{B}} g_{k,b}\left(Y\right) \cdot b$$

for some polynomials $g_{k,b} \in \mathcal{R}_0[Y]$ over $\mathcal{R}_0$ (and not $\mathcal{R}$), written as sums of monomials. As $\mathcal{R} = \oplus_{b\in\mathcal{B}} \mathcal{R}_0 b$, the polynomial g_k attains 0 for a substitution if and only if each polynomial $g_{k,b}$ attains a value from $\mathrm{Ann}\{b\}$ for the same substitution. Now, for every $b \in \mathcal{B}$ there exists $1 \leq c_b \leq c$ such that $\mathrm{Ann}\{b\} = (p^{c_b})$. Thus $g_{k,b}$ attains a value from $\mathrm{Ann}\{b\}$ if and only if $p^{c-c_b} \cdot g_{k,b}$ attains the value 0 in $\mathcal{R}_0$. Let $h_{k,b} = p^{c-c_b} \cdot g_{k,b}$. Summarizing our observations,

- $f_1\left(X|_{\mathcal{R}}\right) = 0, \ldots, f_\ell\left(X|_{\mathcal{R}}\right) = 0$ can be solved over $\mathcal{R}$ if and only if
- $g_1\left(Y|_{\mathcal{S}}\right) = 0, \ldots, g_\ell\left(Y|_{\mathcal{S}}\right) = 0$ can be solved over $\mathcal{R}$ if and only if
- the system of equations

$$h_{k,b}\left(Y|_{\mathcal{S}}\right) = 0 \qquad (1 \leq k \leq \ell, b \in \mathcal{B}) \tag{4}$$

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

(c) For simplicity, let $h = h_{k,b}$ for some $1 \leq k \leq \ell$, $b \in \mathcal{B}$. 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 $s \in \mathcal{S}$. Thus $d \mid m$ implies $s^{p^m} = s$ for every $s \in \mathcal{S}$. For every $v \in V_0$ its coefficient is in $\mathcal{S}$. Thus, for every $v \in V_0$ we have

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

Consider $\left(\sum_{v\in V_0} v\right)^{p^m}$. By Lemma 4, one can prove by induction on $|V_0|$ 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 $h^{(ii)} \in \mathcal{R}_0[Y]$. Therefore,

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

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

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

Note, that $h^{(i)}$ and $h^{(ii)}$ can be computed in $O\left(\|h\|^{p^m}\right)$ time, and $\left\|h^{(i)}\right\| = O\left(\|h\|^{p^m}\right)$, $\left\|h^{(ii)}\right\| = O\left(\|h\|^{p^m}\right)$. Now, repeat the process with $h^{(i)} - h^{(ii)}$, then in

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

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

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

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

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

Recall that $r \mapsto r^{p^m}$ is a projection onto $\mathcal{S}$ and for every element $r \in \mathcal{R}_0$, there exist unique elements $s_0, \ldots, s_{c-1} \in \mathcal{S}$ 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 $s_1, \ldots, s_n \in \mathcal{S}$ 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 $s_1, \ldots, s_n \in \mathcal{S}$ 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 $h_{k,b}$ $(1 \le k \le \ell,\ b \in \mathcal{B})$ we obtain polynomials $h_{k,i,b} \in \mathcal{F}[Y]$ $(1 \le k \le \ell,\ (i,b) \in \mathcal{P})$

such that the system (4) can be solved over $\mathcal{R}_0$ if and only if the system

$$h_{k,i,b}(Y|_{\mathcal{F}}) = 0 \qquad (1 \le k \le \ell, (i,b) \in \mathcal{P}) \tag{5}$$

can be solved over $\mathcal{F}$. Furthermore, all $h_{k,i,b}$ can be computed from $g_{k,b}$ in $O\left(c\,\|g_{k,b}\|^{p^{cm}}\right) \le O\left(c\,\|g_k\|^{p^{cm}}\right)$ time, and $\|h_{k,i,b}\| = O\left(\|g_k\|^{p^{cm}}\right)$.

(d) Let $q = \prod_{k=1}^{\ell} \prod_{(i,b)\in\mathcal{P}} (1 - h_{k,i,b})^{p^d-1} \in \mathcal{F}[Y]$. Note, that $\mathcal{F} \models q \approx 0$ if and only if the system $h_{k,i,b} = 0$ $(1 \le k \le \ell, (i,b) \in \mathcal{P})$ has no solution in $\mathcal{F}$. Moreover, q can be expanded into sum of monomials in $O\left(\prod_{1\le k\le\ell,(i,b)\in\mathcal{P}} \|h_{k,i,b}\|^{p^d}\right)$ time. By [7] it can be decided in linear time in $\|q\|$, whether or not $\mathcal{F} \models q \approx 0$.

Now,

$$\begin{aligned}
\|q\| &\le O\left(\prod_{1\le k\le\ell,(i,b)\in\mathcal{P}} \|h_{k,i,b}\|^{p^d}\right) = O\left(\prod_{1\le k\le\ell} \prod_{b\in\mathcal{B}} \prod_{(i,b)\in\mathcal{P}} \|h_{k,i,b}\|^{p^d}\right) \\
&\le O\left(\prod_{1\le k\le\ell} \prod_{b\in\mathcal{B}} \|g_k\|^{c_b p^{cm} p^d}\right) = O\left(\prod_{1\le k\le\ell} \|g_k\|^{|\mathcal{P}|p^{d+cm}}\right) \\
&\le O\left(\prod_{1\le k\le\ell} |\mathcal{P}|^{(t+1)|\mathcal{P}|p^{d+cm}} \|f_k\|^{t|\mathcal{P}|p^{d+cm}}\right) \\
&\le O\left(|\mathcal{P}|^{\ell(t+1)|\mathcal{P}|p^d p^{cm}} \max_{1\le k\le\ell} \|f_k\|^{\ell t|\mathcal{P}|p^d p^{cm}}\right).
\end{aligned}$$

Here, $|\mathcal{P}| \le \log|\mathcal{R}|$, $|\mathcal{P}| \cdot p^d \le |\mathcal{P}| \cdot |\mathcal{S}| \le |\mathcal{S}|^{|\mathcal{P}|} = |\mathcal{R}|$, $c \le t \le \log|\mathcal{J}| \le \log|\mathcal{R}| - 1$, $m \le d + c + \log t$, $p^c \le p^{cd} \le |\mathcal{R}|$, giving the required upper bound on the time complexity. This finishes the proof of Theorem 6. □

Note, that if $\mathcal{R}$ is a Galois ring, parts (c) and (d) of the proof of Theorem 6 immediately yield the following.

Corollary 7. *Let $\mathcal{R}$ be isomorphic to the Galois ring $\mathcal{GR}(p^c, d)$ for some prime p and positive integers c, d. Let $m \ge c + \lfloor \log_p(c-1) \rfloor$ be the smallest positive integer divisible by d, and let $\mathcal{S}$ be the representation system of $\mathcal{R}/(p)$ obtained as the image of the map $r \mapsto r^{p^m}$. Then it can be decided in $O\left(\max_{1\le k\le\ell} \|f_k\|^{\ell c p^{d+cm}}\right)$ time whether or not the system $f_1|_{\mathcal{S}} = 0, \ldots, f_\ell|_{\mathcal{S}} = 0$ is solvable over $\mathcal{R}$.*

4. Noncommutative rings

We prove Theorem 3 in this section.

4.1. **Notations.** Let $\mathcal{R}$ be a not necessarily commutative, not necessarily unital ring with prime power characteristic, $\mathcal{J}$ be its Jacobson radical. Assume that $\mathcal{R}/\mathcal{J}$ is commutative. If $\mathcal{R}$ is nilpotent, then the (SM) equation solvability problem can be decided in polynomial time by [6]. If $\mathcal{R}$ is not nilpotent, then $\mathcal{R}/\mathcal{J}$ is the sum of finite fields: $\mathcal{R}/\mathcal{J} = \oplus_{i=1}^{l}\mathcal{F}_i$. Let $e_1, \dots, e_l$ be a complete set of primitive, pairwise orthogonal idempotents (yielding $e_i e_j = 0$ if $1 \le i \ne j \le l$) such that $e_i + \mathcal{J}$ is the identity element of $\mathcal{F}_i$, and $e_i + \mathcal{J}$ is zero in $\mathcal{F}_j$ for $j \ne i$. Let $e = e_1 + \dots + e_l$. Motivated by the Pierce decomposition theorem (see e.g. [5, p. 48, 50]), for $0 \le i, j \le l$ we define the subrings $\mathcal{R}_{i,j} \le \mathcal{R}$ as follows:

$$
\begin{aligned}
R_{0,0} &= \{\, r \in \mathcal{R} \mid ere = 0 \,\} = (1-e)\,\mathcal{R}\,(1-e)\,, \\
R_{i,0} &= \{\, r \in e_i\mathcal{R} \mid re = 0 \,\} = e_i\mathcal{R}\,(1-e)\,, && (1 \le i \le l), \\
R_{0,j} &= \{\, r \in \mathcal{R}e_j \mid er = 0 \,\} = (1-e)\,\mathcal{R}e_j, && (1 \le j \le l), \\
R_{i,j} &= e_i\mathcal{R}e_j, && (1 \le i, j \le l).
\end{aligned}
$$

Then every element of $\mathcal{R}$ can be uniquely written as a sum of elements from $\mathcal{R}_{i,j}$ for $0 \le i, j \le l$. Note that $\mathcal{R}_{i,j} \le \mathcal{J}$ if $i \ne j$ or if $i = j = 0$, and $\mathcal{R}_{i,i}/\left(\mathcal{J} \cap \mathcal{R}_{i,i}\right) \simeq \mathcal{F}_i$ for $1 \le i \le l$. Moreover,

$$
\mathcal{R}_{i_1,j_1}\mathcal{R}_{i_2,j_2} \subseteq \begin{cases} \{\, 0 \,\}, & \text{if } j_1 \ne i_2, \\ \mathcal{R}_{i_1,j_2}, & \text{otherwise.} \end{cases} \tag{6}
$$

Let the characteristic of $\mathcal{R}_{i,i}$ be p^{c_i} and let $|\mathcal{F}_i| = p^{d_i}$. Now, $\mathcal{R}_{i,i}$ is local, thus there exists a Galois subring $\mathcal{R}_i \le \mathcal{R}_{i,i}$ such that $\mathcal{R}_i \simeq \mathcal{GR}\,(p^{c_i}, d_i)$ [16, p. 80, Theorem B]. Let t be the smallest positive integer for which $\mathcal{J}^t = \{\, 0 \,\}$. Let $d = \operatorname{lcm}(d_1, \dots, d_l)$, $c = \max\{\, c_1, \dots, c_l \,\}$, then $t \ge c$. Let $m \ge c + \left\lfloor \log_p(t-1) \right\rfloor$ be the smallest positive integer divisible by d. Then by Section 3.1 the map $r \mapsto r^{p^m}$ is a projection from $\mathcal{R}_i$ onto a set $\mathcal{S}_i$ such that $\mathcal{S}_i$ is a multiplicatively closed representation system for $\mathcal{F}_i$, and $s_i^{p^{d_i}} = s_i$ for every $s_i \in \mathcal{S}_i$. Let $\mathcal{S} = \oplus_{i=1}^{l}\mathcal{S}_i$, then $s^{p^d} = s$ for all $s \in \mathcal{S}$. Every element $r \in \mathcal{R}$ can be uniquely written as $r = \sum_{i=1}^{l} s_i + \sum_{0 \le i,j \le l} r_{i,j}$, where $s_i \in \mathcal{S}_i$ $(1 \le i \le l)$ and $r_{i,j} \in \mathcal{J} \cap \mathcal{R}_{i,j}$ $(0 \le i, j \le l)$.

4.2. **The ring $\mathcal{R}^*$.** Let $\mathcal{R}^* = \mathcal{GR}\,(p^c, d)$. Since $t \ge c$, by Section 3.1 the map $r \mapsto r^{p^m}$ is a projection from $\mathcal{R}^*$ onto a set $\mathcal{S}^*$ such that $\mathcal{S}^*$ is a multiplicatively closed representation system for $\mathcal{R}^*/(p)$, such that $s^{p^d} = s$ for every $s \in \mathcal{S}^*$. For every $1 \le i \le l$ there exists a unique subring $\mathcal{R}_i^* \le \mathcal{R}^*$ such that $\mathcal{R}_i^* \simeq \mathcal{GR}\,(p^c, d_i)$, which is the range of the map $\mathcal{R}^* \to \mathcal{R}^*$, $r \mapsto r^{(p^d-1)/(p^{d_i}-1)}$. Now, let $\mathcal{S}_i^*$ be the range of the map $\mathcal{R}^* \to \mathcal{R}^*$, $r \mapsto r^{p^m(p^d-1)/(p^{d_i}-1)}$, then $\mathcal{S}_i^* \subseteq \mathcal{R}_i^*$. Let $\psi_i \colon \mathcal{R}_i^* \to \mathcal{R}_i$ be an arbitrary surjective homomorphism. Note, that each ψ_i is bijective between $\mathcal{S}_i^*$ and $\mathcal{S}_i$, and preserves the multiplicative

structure. Diagram (7) summarizes these properties, where the dashed arrow represents a bijection preserving the multiplicative structure.

(7)

$$\begin{array}{ccccc}
\mathcal{GR}(p^c,d) \simeq \mathcal{R}^* & \xrightarrow{r \mapsto r^{\frac{p^d-1}{p^{d_i}-1}}} & \mathcal{GR}(p^c,d_i) \simeq \mathcal{R}_i^* & \xrightarrow{\psi_i} & \mathcal{R}_i \simeq \mathcal{GR}(p^{c_i},d_i) \\
r \mapsto r^{p^m} \downarrow & & r \mapsto r^{p^m} \downarrow & & \downarrow r \mapsto r^{p^m} \\
\mathcal{S}^* & \xrightarrow[r \mapsto r^{\frac{p^d-1}{p^{d_i}-1}}]{} & \mathcal{S}_i^* & \xrightarrow[\psi_i]{} & \mathcal{S}_i.
\end{array}$$

4.3. **The sketch of the proof.** For a polynomial f over $\mathcal{R}$ written as a sum of monomials having noncommuting variables and elements of $\mathcal{R}$, $f = 0$ can be solved over $\mathcal{R}$ if and only if for some $\overline{u} = (u_1, \ldots, u_n) \in \mathcal{J} \times \cdots \times \mathcal{J}$ the polynomial $f_{\overline{u}}(x_1, \ldots, x_n) = f(x_1 + u_1, \ldots, x_n + u_n)$ can attain value 0 by a substitution from $\mathcal{S}$. According to Lemma 8 (see below) it is enough to consider such n-tuples $\overline{u} = (u_1, \ldots, u_n)$, where the number of nonzero coordinates are at most D for some D depending on $\mathcal{R}$. Thus we only need to check polynomially many new polynomials $f_{\overline{u}}$ instead of exponentially-many ones. We need to consider these polynomials for substitutions from $\mathcal{S}$. This reduction is carried out in Section 4.4.

In Section 4.5 for a fixed $f_{\overline{u}}$ we substitute $x_j = \sum_{i=1}^{l} x_{i,j}$ $(1 \leq j \leq n)$ (and think that every variable $x_{i,j}$ can attain values from $\mathcal{S}_i$), and every constant r by its form of $\sum_{i=1}^{l} s_i + \sum_{0 \leq i,j \leq l} r_{i,j}$, where $s_i \in \mathcal{S}_i$ $(1 \leq i \leq l)$ and $r_{i,j} \in \mathcal{J} \cap \mathcal{R}_{i,j}$ $(0 \leq i,j \leq l)$. We expand the resulting polynomial into g. If we denote the set $\{x_{i,1}, \ldots, x_{i,n}\}$ by X_i, then $\mathcal{R} \models f_{\overline{u}}|_{\mathcal{S}} \approx g(X_1|_{\mathcal{S}_1}, \ldots, X_l|_{\mathcal{S}_l})$. Using (6) we can execute the expansion in $O\left(\|f_{\overline{u}}\|^t\right)$ time. Then in Section 4.6 we group the monomials of g into types. A *type of a monomial* is $(v_1, \ldots, v_k)$ if v_1, $\ldots$, v_k are the elements from $\mathcal{J}$ occurring in the monomial from left to right. Let $g_{(v_1,\ldots,v_k)}$ denote the sum of those monomials in g which are of type $(v_1, \ldots, v_k)$. Note that the number of types depend only on $\mathcal{R}$ and neither on f nor on g.

A monomial of type $(v_1, \ldots, v_k)$ is of the form $q_1 v_1 q_2 v_2 \ldots q_k v_k q_{k+1}$, where $q_1, \ldots, q_k, q_{k+1}$ are monomials containing no constants from $\mathcal{J}$. If $v_1 \in \mathcal{R}_{i_1,j_1}, \ldots, v_k \in \mathcal{R}_{i_k,j_k}$, then it is not hard to see that $j_1 = i_2 \neq 0, \ldots, j_{k-1} = i_k \neq 0$, and q_1 attains values from $\mathcal{R}_{i_1}$, q_2 attains values from $\mathcal{R}_{i_2}$, etc., Moreover, the map $\mathcal{R}_{i_1} \times \mathcal{R}_{i_2} \times \ldots \mathcal{R}_{i_k} \times \mathcal{R}_{j_k} \to \mathcal{R}$, $(r_1, r_2, \ldots, r_k, r_{k+1}) \mapsto r_1 v_1 r_2 v_2 \ldots r_k v_k r_{k+1}$ is multilinear in $r_1, r_2, \ldots, r_k, r_{k+1}$. This motivates to consider the tensor product $\mathcal{R}_{(v_1,\ldots,v_k)} = \mathcal{R}_{i_1} \otimes \mathcal{R}_{i_2} \otimes \cdots \otimes \mathcal{R}_{i_k} \otimes \mathcal{R}_{j_k}$ for every type $(v_1, \ldots, v_k)$ in Section 4.7. Then we are going to polynomially reduce the equation $g(X_1|_{\mathcal{S}_1}, \ldots, X_l|_{\mathcal{S}_l}) = 0$ over $\mathcal{R}$ to solving several systems of equations

over the introduced tensor products $\mathcal{R}_{(v_1,\ldots,v_k)}$. Both the number of systems and the number of equations in each system depend only on the ring $\mathcal{R}$ and neither on f nor on g. However, we are not able to simply apply Theorem 6 or Corollary 7 at this point, because the equations occurring in these systems are over *different* commutative rings. First, we need to translate these systems of equations to systems of equations over a common commutative ring, which is going to be $\mathcal{R}^*$. The key argument is found in Lemma 10 in Section 4.8, where we polynomially reduce a system of such equations to a system of equations over the ring $\mathcal{R}^*$ such that the number of equations depends only on the ring $\mathcal{R}$. Finally, in Section 4.9 we wrap up the proof.

4.4. **Reducing to substitutions only from $\mathcal{S}$.** Let f be a polynomial over $\mathcal{R}$ written as a sum of monomials having noncommuting variables $x_1, \ldots, x_n$ and elements of $\mathcal{R}$. We first reduce the problem to check substitutions of the variables only from $\mathcal{S}$. Let $u_1, \ldots, u_n \in \mathcal{J}$ be arbitrary, and let $\overline{u} = (u_1, \ldots, u_n)$. Let

$$f_{\overline{u}}(x_1, \ldots, x_n) = f(x_1 + u_1, \ldots, x_n + u_n) \tag{8}$$

be the polynomial attained by replacing every variable x_i by $(x_i + u_i)$ and expanding as a sum of monomials. We do not compute the monomials that contain at least t-many of u_is as these attain value 0 for an arbitrary substitution. Thus $f_{\overline{u}}$ can be calculated in $O\left(\|f\|^t\right)$ time and $\|f_{\overline{u}}\| = O\left(\|f\|^t\right)$. Consider the polynomials $f_{\overline{u}}$ for every possible $u_1, \ldots, u_n \in \mathcal{J}$. It is clear that $f|_{\mathcal{R}} = 0$ is solvable over $\mathcal{R}$ if and only if for some $\overline{u}$ the equation $f_{\overline{u}}|_{\mathcal{S}} = 0$ is solvable over $\mathcal{R}$. Now, the number of the $f_{\overline{u}}$ polynomials is $|\mathcal{J}|^n$, which is an exponential number in $\|f\|$. Nevertheless, by Lemma 8 below, one only needs to consider those $f_{\overline{u}}$ polynomials, for which the number of nonzero u_i coordinates in $\overline{u}$ is less than D for some D depending only on $\mathcal{R}$.

Lemma 8. *Let $\mathcal{R}$ be a finite ring, $\mathcal{J}$ be its Jacobson radical. Let $\mathcal{S}$ be any representation system of $\mathcal{R}/\mathcal{J}$, and let f be a polynomial over $\mathcal{R}$ in not necessarily commuting variables $x_1, \ldots, x_n$. Then there exists $D = D(\mathcal{R})$ such that $f|_{\mathcal{R}} = 0$ is solvable over $\mathcal{R}$ if and only if $f_{\overline{u}}|_{\mathcal{S}} = 0$ is solvable over $\mathcal{R}$ for some $\overline{u}$ for which $|\{\, 1 \leq i \leq n \mid u_i \neq 0 \,\}| < D$.*

Proof. Lemma 2.1 in [6] asserts the statement for $\mathcal{R} = \mathcal{J}$, and almost the same proof shows the validity of Lemma 8, as well. For the sake of completeness, we provide the proof here.

Assume $f = 0$ is solvable over $\mathcal{R}$, and a solution is $x_1 = s_1 + u_1, \ldots, x_n = s_n + u_n$ for some $s_1, \ldots, s_n \in \mathcal{S}$, $u_1, \ldots, u_n \in \mathcal{J}$. Let

$$g(y_1, \ldots, y_n) = f(s_1 + y_1, \ldots, s_n + y_n)$$

be the polynomial attained by replacing every variable x_j by $(s_j + y_j)$ and expanding as a sum of monomials. We do not compute the monomials that contain at least t-many of y_js as these attain value 0 for

an arbitrary substitution from $\mathcal{J}$. Now, $g(\overline{u}) = 0$. For every subset $I \subseteq \{1, \ldots, n\}$ let g_I be the sum of those monomials in g which depend on the variables y_j for every $j \in I$. Note that the monomials in g_I may depend on y_j for $j \notin I$, as well. For example, $g_\emptyset = g$.

Let $\overline{u} = (u_1, \ldots, u_n) \in \mathcal{J}^n$, and for an arbitrary $I \subseteq \{1, \ldots, n\}$ let $\overline{u}_I$ be the n-tuple $(r_1, \ldots, r_n)$ for which $r_i = u_i$ if $i \in I$ and $r_i = 0$, otherwise. Consider $g(\overline{u})$. Let S denote the indices of nonzero u_i, i.e. $S = \{1 \leq i \leq n \mid u_i \neq 0\}$. If $|S| > D$, then we find a proper subset H of S such that $g\left(\overline{u}_{S\setminus H}\right) = g(\overline{u}) = 0$. The value of D will be determined later. First, let $H \subset S$ be arbitrary. We compute the value of g for the substitution where we replace u_j by 0 in $\overline{u}$ for every $j \in H$. Every monomial containing a variable y_j for some $j \in H$ attains value 0 for the substitution $\overline{u}_{S\setminus H}$. Thus by inclusion-exclusion we have

$$g\left(\overline{u}_{S\setminus H}\right) = \sum_{I \subseteq H} (-1)^{|I|} g_I(\overline{u}).$$

Since all products containing at least t-many u_js are 0, we obtain

$$\begin{aligned} g\left(\overline{u}_{S\setminus H}\right) &= \sum_{\substack{I \subseteq H \\ |I| < t}} (-1)^{|I|} g_I(\overline{u}) \\ &= g(\overline{u}) - \sum_{i \in H} g_{\{i\}}(\overline{u}) + \sum_{\substack{i,j \in H \\ i<j}} g_{\{i,j\}}(\overline{u}) - \sum_{\substack{i,j,k \in H \\ i<j<k}} g_{\{i,j,k\}}(\overline{u}) + \ldots . \end{aligned}$$

We prove that there exists a subset $H \subseteq S$, such that every sum $\sum_{i \in H} g_{\{i\}}(\overline{u})$, $\sum_{i,j \in I} g_{\{i,j\}}(\overline{u})$, etc. attains the value 0. To this end we color the less than t-element subsets of S by the elements of $\mathcal{J}$: for every subset $I \subseteq S$ let $g_I(\overline{u})$ be the color of I.

For positive integers t, k, p^m let $R_2(k, p^m) = kp^m$ and for $t > 2$ let $R_t(k, p^m) = k^{R_{t-1}(k,p^m)^{t-1}}$. Let $T_2(k, p^m) = R_2(k, p^m)$ and let $T_t(k, p^m) = R_t(k, T_{t-1}(k, p^m))$. We use the following form of Ramsey's theorem, which follows from [4, Section 1.2, Theorem 2] and [4, Section 4.7]:

Theorem 9 (Ramsey's Theorem)**.** *Let t, k and p^m be positive integers, $t > 1$. Then there exists a positive integer $D \leq T_t(k, p^m)$ such that if we color the less than t-element subsets of a set S by k colors and $|S| > D$, then S has a subset H with p^m elements, such that any two subsets of the same size have the same color, that is for every $H_1, H_2 \subseteq H$, $|H_1| = |H_2| < t$ the color of H_1 and H_2 are the same.*

Recall that t is the nilpotency class of $\mathcal{J}$, and $m \geq c + \lfloor \log_p(t-1) \rfloor$, where $p^c \cdot r = 0$ for every $r \in \mathcal{R}$. Let $k = |\mathcal{J}|$. By Ramsey's theorem for t, k, p^m there exists D such that if $|S| > D$, then there exists a subset $H \subseteq S$, $|H| = p^m$ such that every one-element subset of H has the same color, every two-element subset of H has the same color,

etc., every subset of H with $(t-1)$ elements has the same color. Let $\gamma(i)$ denote the color of the subsets of H with i elements. Hence, $\gamma(i) = g_I(\overline{u})$, where $I \subset H$ is arbitrary such that $|I| = i$. Now, the value of g for the substitution $\overline{u}_{S\setminus H}$ is

$$g\left(\overline{u}_{S\setminus H}\right) = g(\overline{u}) - \sum_{i\in H} g_{\{i\}}(\overline{u}) + \sum_{\substack{i,j\in H\\ i<j}} g_{\{i,j\}}(\overline{u}) - \dots$$

$$= g(\overline{u}) + \sum_{i=1}^{t-1} (-1)^i \binom{p^m}{i} \gamma(i).$$

We chose m such that all binomial coefficients $\binom{p^m}{i}$ for $1 \le i \le t-1$ are divisible by p^c (Lemma 4), thus $g\left(\overline{u}_{S\setminus H}\right) = g(\overline{u})$ holds. Hence if $|S| > D$ then we have found an $H \subseteq S$, such that $g\left(\overline{u}_{S\setminus H}\right) = g(\overline{u})$. If $|S \setminus H| > D$, then we can repeat the procedure for $S = S \setminus H$ until $|S \setminus H| \le D$ holds. □

Let D be the constant defined in Lemma 8. Let T be the set of $\overline{u}$-tuples for which the number of nonzero u_i coordinates is less than D:

$$T = \{ (u_1, \dots, u_n) \mid u_i \in \mathcal{J}, 1 \le i \le n, |\{ 1 \le i \le n : u_i \ne 0 \}| < D \}.$$

Then

$$|T| \le \sum_{j=0}^{D-1} \binom{n}{j} \cdot |\mathcal{J}|^j \le \sum_{j=0}^{D} (n \cdot |\mathcal{R}|)^j \le (D+1) \cdot (n\,|\mathcal{R}|)^D = O\left(\|f\|^D\right),$$

which is polynomial in $\|f\|$. By Lemma 8, $f = 0$ is solvable over $\mathcal{R}$ if and only if for some $\overline{u} \in T$ the equation $f_{\overline{u}} = 0$ is solvable by a substitution from $\mathcal{S}$. Each of these polynomials is computable in $O\left(\|f\|^t\right)$ time, there are $O\left(\|f\|^D\right)$ polynomials to be computed, thus the reduction is polynomial.

4.5. **Transforming $f_{\overline{u}}$.** Now, fix $\overline{u} = (u_1, \dots, u_n) \in T$, where the number of nonzero u_is is less than D and consider $f_{\overline{u}}$ for substitutions from $\mathcal{S} = \oplus_{i=1}^{l} \mathcal{S}_i$. That is, write $x_j = \sum_{i=1}^{l} x_{i,j}$ $(1 \le j \le n)$, where every variable $x_{i,j}$ can attain values from $\mathcal{S}_i$. Let us call a substitution $x_{i,j} = s_{i,j}$ $(1 \le i \le l,\ 1 \le j \le n)$ *valid* if $s_{i,j} \in \mathcal{S}_i$ for every $1 \le i \le l,\ 1 \le j \le n$. We say that the variable $x_{i,j}$ has *type* e_i. Collect together the neighboring constants in every monomial. Then write every constant as $\sum_{i=1}^{l} s_i + \sum_{0\le i,j\le l} r_{i,j}$, where $s_i \in \mathcal{S}_i$ $(1 \le i \le l)$ and $r_{i,j} \in \mathcal{J} \cap \mathcal{R}_{i,j}$ $(0 \le i,j \le l)$. We say that the element $s_i \in \mathcal{S}_i$ has *type* e_i, and $r_{i,j} \in \mathcal{J}$ has *type* $r_{i,j}$ (i.e. itself). Note that if an element or variable has type e_i, then it attains values only from the Galois ring $\mathcal{R}_i$. Finally, expand the resulting polynomial as sum of monomials. This expansion would take exponential time in $O(\|f_{\overline{u}}\|)$ if we computed every monomial. However, by not computing those monomials which attain 0 for every valid substitution, the expansion

can be done in polynomial time. That is, we do not compute the monomials containing at least t elements from $\mathcal{J}$, or those containing two neighboring variables or constants which multiply to 0 according to (6). Precisely, we do not compute a monomial if it contains at least t elements of type from $\mathcal{J}$, or if it has two neighboring variables with different types, or if a variable of type e_i is multiplied from the left by a constant from $\mathcal{R}_{i_1,j_1}$ for some $j_1 \neq i$, or if a variable of type e_i is multiplied from the right by a constant from $\mathcal{R}_{i_1,j_1}$ for some $i \neq i_1$, or if the monomial contains two neighboring constants, whose product must be 0 by (6). This expansion can be done in $O\left(\|f_{\overline{u}}\|^t\right)$ time. Finally, if there are neighboring constants in a monomial, then we replace their formal product by their product in $\mathcal{R}$. Let us denote the resulting polynomial by g, then $\|g\| = O\left(\|f_{\overline{u}}\|^t\right)$. Here, g is a polynomial over $\mathcal{R}$ having noncommuting variables $x_{i,j}$ $(1 \leq i \leq l, 1 \leq j \leq n)$. Let $X_i = \{\, x_{i,1}, \ldots, x_{i,n} \,\}$ for $1 \leq i \leq l$. Now, $\mathcal{R} \models f_{\overline{u}}|_{\mathcal{S}} \approx g\left(X_1|_{\mathcal{S}_1}, \ldots, X_l|_{\mathcal{S}_l}\right)$. In particular, $f_{\overline{u}} = 0$ can be solved by a substitution from $\mathcal{S}$ if and only if $g = 0$ is solvable by a valid substitution $x_{i,j} \in \mathcal{S}_i$.

4.6. **Type of monomials.** We say that the *type of a monomial* in g is $(v_1, \ldots, v_k)$ if the monomial contains exactly k elements from $\mathcal{J}$, which are $v_1, \ldots, v_k$, from left to right. Assume that $v_1 \in \mathcal{R}_{i_1,j_1}, \ldots, v_k \in \mathcal{R}_{i_k,j_k}$. Note, that $j_1 = i_2$, and between v_1 and v_2 only elements of type $e_{j_1} = e_{i_2}$ can occur, otherwise the monomial attains 0 for every substitution by (6). Consequently, $j_1 = i_2 \neq 0$. Similarly, $j_2 = i_3 \neq 0$, and between v_2 and v_3 only elements of type $e_{j_2} = e_{i_3}$ can occur, etc. Moreover, if $i_1 = 0$, then neither variables nor constants can occur before v_1, and if $j_k = 0$, then neither variables nor constants can occur after v_k. If a monomial in g does not contain any element from $\mathcal{J}$, then every element of the monomial is of the same type e_i for some $1 \leq i \leq l$. In such a case we say that the *type of the monomial* is e_i. Let Typ denote the set of all possible types of monomials occurring in g. Considering that a monomial can contain at most $t-1$ elements from $\mathcal{J}$,

$$|\mathrm{Typ}| \leq l + |\mathcal{J}| + |\mathcal{J}|^2 + \cdots + |\mathcal{J}|^{t-1},$$

and does not depend on f. For a type $(v_1, \ldots, v_k) \in \mathrm{Typ}$, let $g_{(v_1,\ldots,v_k)}$ denote the sum of those monomials in g which are of type $(v_1, \ldots, v_k)$, then $g = \sum_{(v_1,\ldots,v_k)\in\mathrm{Typ}} g_{(v_1,\ldots,v_k)}$. Finally, we say that a polynomial is of type $(v_1, \ldots, v_k)$, if it is written as a sum of monomials of type $(v_1, \ldots, v_k)$. That is, $g_{(v_1,\ldots,v_k)}$ is of type $(v_1, \ldots, v_k)$. Monomials of type v for some $v \in \mathcal{R}_{0,0}$ do not contain variables. Let $g_0 = \sum_{v\in\mathcal{R}_{0,0}} g_v \in \mathcal{R}_{0,0}$. From now on, we exclude v from Typ if $v \in \mathcal{R}_{0,0}$.

4.7. **Tensor products.** Let $(v_1, \ldots, v_k) \in \mathrm{Typ}$ be a type, where $v_1 \in \mathcal{R}_{i_1,j_1}, \ldots, v_k \in \mathcal{R}_{i_k,j_k}$. As noted earlier, $j_1 = i_2 \neq 0, \ldots, j_{k-1} = i_k \neq 0$. Assume first that $i_1 \neq 0 \neq j_k$. Let $\mathcal{R}_{(v_1,\ldots,v_k)} = \mathcal{R}_{i_1} \otimes \mathcal{R}_{i_2} \otimes \cdots \otimes \mathcal{R}_{i_k} \otimes \mathcal{R}_{j_k}$

be the *tensor ring corresponding to* $(v_1, \dots, v_k)$. Let $\omega\colon \mathcal{R}_{(v_1,\dots,v_k)} \to \mathcal{R}$ be

$$r_1 \otimes r_2 \otimes \cdots \otimes r_k \otimes r_{k+1} \mapsto r_1 v_1 r_2 v_2 \dots r_k v_k r_{k+1} \tag{9}$$

extended multilinearly. If $i_1 = 0$, then we use the same definition, except we omit the $\mathcal{R}_{i_1}$-part. If $j_k = 0$, then we use the same definition, except we omit the $\mathcal{R}_{j_k}$-part. Note, that even though ω depends on the type, we abuse the notation and denote every map defined by (9) by ω. We believe this does not create confusion but simplifies the notations.

We define the *corresponding tensor expression* to a polynomial of type $(v_1, \dots, v_k)$ inductively: for a monomial $q = q_1 v_1 q_2 \dots q_k v_k q_{k+1}$ of type $(v_1, \dots, v_k)$, let the *corresponding tensor expression* be the formal tensor product $q' = q_1 \otimes \cdots \otimes q_k \otimes q_{k+1}$. For a polynomial of type $(v_1, \dots, v_k)$ define the *corresponding tensor expression* as the sum of the corresponding tensor expressions of its monomials. That is, if $h = \sum_j q_{1,j} v_1 q_{2,j} \dots q_{k,j} v_k q_{k+1,j}$, then its corresponding tensor expression is $h' = \sum_j q_{1,j} \otimes \cdots \otimes q_{k,j} \otimes q_{k+1,j}$. Consider a valid substitution $\overline{s}$. Let $h'(\overline{s}) = \sum_j q_{1,j}(\overline{s}) \otimes \cdots \otimes q_{k,j}(\overline{s}) \otimes q_{k+1,j}(\overline{s})$, then $h(\overline{s}) = \omega(h'(\overline{s}))$.

Let $g'_{(v_1,\dots,v_k)}$ denote the corresponding tensor expression of $g_{(v_1,\dots,v_k)}$. Let $\mathcal{M}$ denote the set of tuples A, indexed by Typ, for which $A_{(v_1,\dots,v_k)}$ ($(v_1, \dots, v_k) \in \mathrm{Typ}$) is an element of the tensor product $\mathcal{R}_{(v_1,\dots,v_k)}$ corresponding to $(v_1, \dots, v_k)$ such that

$$g_0 + \sum_{(v_1,\dots,v_k)\in \mathrm{Typ}} \omega\left(A_{(v_1,\dots,v_k)}\right) = 0.$$

Then $g = 0$ is solvabe by a valid substitution $x_{i,j} \in \mathcal{S}_i$ if and only if for some $A \in \mathcal{M}$ the system of equations

$$g'_{(v_1,\dots,v_k)} = A_{(v_1,\dots,v_k)} \qquad ((v_1, \dots, v_k) \in \mathrm{Typ}) \tag{10}$$

can be solved simultaneously over the appropriate tensor rings by a valid substitution $x_{i,j} \in \mathcal{S}_i$. That is, we reduced the original equation to $|\mathcal{M}|$-many systems, each consisting of $|\mathrm{Typ}|$-many equations over the corresponding tensor rings, where variables $x_{i,j}$ are substituted from $\mathcal{S}_i$ ($1 \le i \le l$, $1 \le j \le n$). The reduction is polynomial, as $\mathcal{M}$ only depends on $\mathcal{R}$ and does not depend on f, and hence can be computed in advance.

4.8. **Solutions of tensor expressions.** Let us fix $(v_1, \dots, v_k) \in \mathrm{Typ}$ and $A \in \mathcal{M}$. Let h be the tensor expression $g'_{(v_1,\dots,v_k)} - A_{(v_1,\dots,v_k)}$. Recall the definitions of d, $\mathcal{R}^*$, $\mathcal{S}^*$ and ψ_i from Section 4.2. By Lemma 10 there exists a one-to-one correspondence between the solutions of $h = 0$ over $\mathcal{R}_{(v_1,\dots,v_k)}$ and the solutions of a system of d^k-many equations over $\mathcal{R}^*$.

Lemma 10. *There exist polynomials $h_1, \dots, h_{d^k}$ over $\mathcal{R}^*$ such that $x_{i,j} = s^*_{i,j} \in \mathcal{S}^*$ is a solution to the system $h_1 = 0, \dots, h_{d^k} = 0$ if and*

only if $x_{i,j} = s_{i,j} = \psi_i\left(\left(s_{i,j}^*\right)^{(p^d-1)/(p^{d_i}-1)}\right) \in \mathcal{S}_i$ *is a solution of* $h = 0$ *over* $\mathcal{R}_{(v_1,\dots,v_k)}$. *Moreover, the polynomials* $h_1, \dots, h_{d^k}$ *can be obtained from* h *in polynomial time in* $\|h\|$.

Proof. Assume $v_1 \in \mathcal{R}_{i_1,j_1}, \dots, v_k \in \mathcal{R}_{i_k,j_k}$, then $j_1 = i_2 \neq 0, \dots, j_{k-1} = i_k \neq 0$. We only prove the lemma in the case $i_1 \neq 0 \neq j_k$, the other three cases can be handled in exactly the same way. Now, $\mathcal{R}_{(v_1,\dots,v_k)} = \mathcal{R}_{i_1} \otimes \cdots \otimes \mathcal{R}_{i_k} \otimes \mathcal{R}_{j_k}$. Recall that $d = \operatorname{lcm}\{d_1, \dots, d_l\}$. Let $c' = \min\{c_{i_1}, \dots, c_{i_k}, c_{j_k}\}$, $\mathcal{R}' = \mathcal{R}^*/(p^{c'})$, and let $\chi\colon \mathcal{R}^* \to \mathcal{R}'$ be the natural map. Similarly to the "star" notations in Section 4.2, we define some "primed" notations.

Let $\mathcal{R}_i' = \mathcal{R}_i^*/(p^{c'})$ for every $1 \leq i \leq l$, then $\mathcal{R}_i'$ is the unique subring of $\mathcal{R}'$ isomorphic to $\mathcal{GR}\left(p^{c'}, d_i\right)$. In fact, $\mathcal{R}_i'$ is the range of the map $\mathcal{R}' \to \mathcal{R}'$, $r \mapsto r^{(p^d-1)/(p^{d_i}-1)}$. For every $i \in \{i_1, \dots, i_k, j_k\}$ let $\chi_i\colon \mathcal{R}_i \to \mathcal{R}_i'$ be a surjective homomorphism such that $\chi_i \circ \psi_i$ equals to the homomorphism χ restricted to $\mathcal{R}_i^*$ (such homomorphism χ_i exists since $c' \leq c_i \leq c$). Recall that $m \geq c + \lfloor \log_p(t-1) \rfloor$ is the smallest positive integer divisible by d. Then by Section 3.1 the map $r \mapsto r^{p^m}$ is a projection from $\mathcal{R}'$ onto a set $\mathcal{S}'$ such that $\mathcal{S}'$ is a multiplicatively closed representation system for $\mathcal{R}'/(p)$, such that $s^{p^d} = s$ for every $s \in \mathcal{S}'$. Let $\mathcal{S}_i'$ be the range of the map $\mathcal{R}' \to \mathcal{R}'$, $r \mapsto r^{p^m(p^d-1)/(p^{d_i}-1)}$, then $\mathcal{S}_i' \subseteq \mathcal{R}_i'$. Note, that χ is a bijection from $\mathcal{S}^*$ to $\mathcal{S}'$ and from $\mathcal{S}_i^*$ to $\mathcal{S}_i'$, and χ_i is a bijection from $\mathcal{S}_i$ to $\mathcal{S}_i'$. Diagram (11) summarizes these properties, where the dashed arrows represent maps, which are bijections between the corresponding $\mathcal{S}$-sets and preserve their multiplicative structure.

(11)

$$\begin{array}{ccccc}
\mathcal{GR}\left(p^c, d\right) \simeq \mathcal{R}^* & \xrightarrow{r \mapsto r^{\frac{p^d-1}{p^{d_i}-1}}} & \mathcal{GR}\left(p^c, d_i\right) \simeq \mathcal{R}_i^* & \overset{\psi_i}{\dashrightarrow} & \mathcal{R}_i \simeq \mathcal{GR}\left(p^{c_i}, d_i\right) \\
\chi \downarrow & & \chi \downarrow & \swarrow_{\chi_i} & \\
\mathcal{GR}\left(p^{c'}, d\right) \simeq \mathcal{R}' & \xrightarrow[r \mapsto r^{\frac{p^d-1}{p^{d_i}-1}}]{} & \mathcal{GR}\left(p^{c'}, d_i\right) \simeq \mathcal{R}_i'. & &
\end{array}$$

We lift the tensor expression h from $\mathcal{R}_{(v_1,\dots,v_k)}$ to the $(k+1)$-fold tensor ring $\mathcal{R}' \otimes \cdots \otimes \mathcal{R}' \otimes \mathcal{R}'$ in two steps. Note first, that the characteristic of the tensor product $\mathcal{R}_{(v_1,\dots,v_k)}$ is $p^{c'}$. That is, by replacing every constant $r_1 \in \mathcal{R}_{i_1}$ by $\chi_{i_1}(r_1) \in \mathcal{R}_{i_1}'$, $\dots$, $r_k \in \mathcal{R}_{i_k}$ by $\chi_{i_k}(r_k) \in \mathcal{R}_{i_k}'$ and $r_{k+1} \in \mathcal{R}_{j_k}$ by $\chi_{j_k}(r_{k+1}) \in \mathcal{R}_{j_k}'$ in h we obtain a tensor expression h' over $\mathcal{R}_{i_1}' \otimes \cdots \otimes \mathcal{R}_{i_k}' \otimes \mathcal{R}_{j_k}'$ such that a substitution $x_{i,j} = s_{i,j} \in \mathcal{S}_i$ is a solution to $h = 0$ over $\mathcal{R}_{(v_1,\dots,v_k)}$ if and only if the substitution $x_{i,j} = \chi_i(s_{i,j}) \in \mathcal{S}_i$ is a solution to $h' = 0$ over $\mathcal{R}_{i_1}' \otimes \cdots \otimes \mathcal{R}_{i_k}' \otimes \mathcal{R}_{j_k}'$. Second, as $\mathcal{R}_{i_1}'$, $\dots$, $\mathcal{R}_{i_k}'$, $\mathcal{R}_{j_k}'$ are subrings of $\mathcal{R}'$, we can consider h'

over the $(k+1)$-fold tensor ring $\mathcal{R}' \otimes \cdots \otimes \mathcal{R}' \otimes \mathcal{R}'$. After replacing every occurrence of $x_{i,j}$ by $x_{i,j}^{(p^d-1)/(p^{d_i}-1)}$ for all $1 \leq i \leq l$, $1 \leq j \leq n$, we obtain a tensor expression h'' over $\mathcal{R}' \otimes \cdots \otimes \mathcal{R}' \otimes \mathcal{R}'$ such that $x_{i,j} = s'_{i,j} \in \mathcal{S}'$ is a solution to $h'' = 0$ over $\mathcal{R}' \otimes \cdots \otimes \mathcal{R}' \otimes \mathcal{R}'$ if and only if $x_{i,j} = \chi_i^{-1}\left(\left(s'_{i,j}\right)^{(p^d-1)/(p^{d_i}-1)}\right) \in \mathcal{S}_i$ is a solution to $h = 0$ over $\mathcal{R}_{(v_1,\ldots,v_k)}$. That way, we reduced our tensor equation over $\mathcal{R}_{(v_1,\ldots,v_k)}$ (substituting $x_{i,j} \in \mathcal{S}_i$) to another tensor equation over $\mathcal{R}' \otimes \cdots \otimes \mathcal{R}' \otimes \mathcal{R}'$ (substituting $x_{i,j} \in \mathcal{S}'$). The reduction is polynomial, as h'' can be computed in polynomial time in $\|h\|$.

Now, we consider $h'' = 0$ over the $(k+1)$-fold tensor ring $\mathcal{R}' \otimes \cdots \otimes \mathcal{R}' \otimes \mathcal{R}' = \sum_1^{d^k} \mathcal{R}'$ (see Section 2.3). Let E_1, …, E_{d^k} denote the primitive idempotents in $\mathcal{R}' \otimes \cdots \otimes \mathcal{R}' \otimes \mathcal{R}'$. Let us denote a substitution $x_{i,j} = s'_{i,j} \in \mathcal{S}'$ by $\overline{s'}$. Now, $h''\left(\overline{s'}\right) = 0$ if and only if $E\left(h\left(\overline{s'}\right)\right) = 0$ for every $E \in \{E_1, \ldots, E_{d^k}\}$. By Lemma 5, there is a bijection between the primitive idempotents $E \in \{E_1, \ldots, E_{d^k}\}$ and k-tuples $\left(\varphi_1^{(E)}, \ldots, \varphi_k^{(E)}\right)$ of $\mathcal{R}' \to \mathcal{R}'$ automorphisms. Assume $h'' = \sum_j q_{1,j} \otimes \cdots \otimes q_{k,j} \otimes q_{k+1,j}$, then by Lemma 5

$$
\begin{aligned}
&E\left(\sum_j q_{1,j}\left(\overline{s'}\right) \otimes q_{2,j}\left(\overline{s'}\right) \otimes \cdots \otimes q_{k,j}\left(\overline{s'}\right) \otimes q_{k+1,j}\left(\overline{s'}\right)\right) \\
&= E\left(1 \otimes \cdots \otimes 1 \otimes \sum_j \varphi_1^{(E)}\left(q_{1,j}\left(\overline{s'}\right)\right) \ldots \varphi_k^{(E)}\left(q_{k,j}\left(\overline{s'}\right)\right) q_{k+1,j}\left(\overline{s'}\right)\right),
\end{aligned}
$$

which is 0 if and only if $\sum_j \varphi_1^{(E)}\left(q_{1,j}\left(\overline{s'}\right)\right) \ldots \varphi_k^{(E)}\left(q_{k,j}\left(\overline{s'}\right)\right) q_{k+1,j}\left(\overline{s'}\right) = 0$. That is, we reduced the tensor equation $h = 0$ over $\mathcal{R}_{(v_1,\ldots,v_k)}$ to the system of equations

$$
\sum_j \varphi_1^{(E)}\left(q_{1,j}\right) \ldots \varphi_k^{(E)}\left(q_{k,j}\right) q_{k+1,j} = 0 \quad \left(E \in \{E_1, \ldots, E_{d^k}\}\right) \tag{12}
$$

such that $x_{i,j} = s'_{i,j} \in \mathcal{S}'$ is a solution to (12) if and only if $x_{i,j} = \chi_i^{-1}\left(\left(s'_{i,j}\right)^{(p^d-1)/(p^{d_i}-1)}\right) \in \mathcal{S}_i$ is a solution to $h = 0$ over $\mathcal{R}_{(v_1,\ldots,v_k)}$. Every $\mathcal{R}' \to \mathcal{R}'$ automorphism is just raising to a p-power. That is, $\varphi_1^{(E)}\left(q_{1,j}\right)$, …, $\varphi_k^{(E)}\left(q_{k,j}\right)$ can be computed by raising the monomials to the corresponding p-power, and thus they are monomials, as well. The reduction is polynomial, because the number of automorphisms and the corresponing p-powers only depend on $\mathcal{R}$ and not on h.

Finally, we lift the whole system (12) into $\mathcal{R}^*$ by multiplying every equation by $p^{c-c'}$. That is, let

$$h_1 = p^{c-c'} \cdot \sum_j \varphi_1^{(E_1)}(q_{1,j}) \dots \varphi_k^{(E_1)}(q_{k,j})\, q_{k+1,j},$$

$$\vdots$$

$$h_{d^k} = p^{c-c'} \cdot \sum_j \varphi_1^{(E_{d^k})}(q_{1,j}) \dots \varphi_k^{(E_{d^k})}(q_{k,j})\, q_{k+1,j}.$$

Then (by $\chi = \chi_i \circ \psi$) $x_{i,j} = \chi^{-1}\left(s'_{i,j}\right) = s^*_{i,j} \in \mathcal{S}^*$ is a solution to the system $h_1 = 0, \dots, h_{d^k} = 0$ over $\mathcal{R}^*$ if and only if $x_{i,j} = s_{i,j} = \psi_i\left(\left(s^*_{i,j}\right)^{(p^d-1)/(p^{d_i}-1)}\right) \in \mathcal{S}_i$ is a solution of $h = 0$ over $\mathcal{R}_{(v_1,\dots,v_k)}$. Moreover, the polynomials $h_1, \dots, h_{d^k}$ can be obtained from h in polynomial time in $\|h\|$. □

4.9. **Finishing the proof.** Using Lemma 10, the system (10) for valid substitutions can be reduced to a system of equations over $\mathcal{R}^*$ for substitutions from $\mathcal{S}^*$ such that there is a natural correspondence between the solutions of (10) and the solutions of the obtained system over $\mathcal{R}^*$. The number of equations over $\mathcal{R}^*$ is at most d^{t-1} times the number of equations of (10), and thus only depends on the original ring $\mathcal{R}$. The reduction is polynomial in $\|f\|$. Finally, solvability of a system of fixed many equations over $\mathcal{R}^*$ for substitutions from $\mathcal{S}^*$ can be decided in polynomial time over $\mathcal{R}^*$ by Corollary 7. □

Remark 11. Note that our proof shows that an equation over $\mathcal{R}$ is equivalent to some fixed many ($|\mathrm{Typ}| \cdot d^{t-1}$-many) equations over $\mathcal{R}^*$. Using the same argument, one can prove that if a system has at most ℓ-many equations over $\mathcal{R}$, then they can be reduced to $\ell \cdot |\mathrm{Typ}| \cdot d^{t-1}$-many equations over $\mathcal{R}^*$. Thus, if ℓ is not part of the input, then solvability of the system over $\mathcal{R}$ can still be decided in polynomial time in the length of the longest polynomial of the system.

5. Concluding remarks and open problems

Reduction to substitutions over $\oplus_{i=1}^{l} \mathcal{S}_i$ in Section 4.4 needed the rather technical Lemma 8, compared to the very natural way of finding a basis as we did for commutative rings in part (a) of Section 3.3. Note, however, that if $\mathcal{R}$ is a finite *unital* ring for which $\mathcal{R}/\mathcal{J}$ is commutative, then one can apply the same idea as for commutative rings, and Lemma 8 can be avoided. Indeed, then $\mathcal{R} = \sum_{i=1}^{l} e_i\mathcal{R}$, and each $e_i\mathcal{R}$ is a left $\mathcal{R}_i$-module, therefore a sum of cyclic left $\mathcal{R}_i$-modules. In particular, for every $1 \le i \le l$ one could find a (weak) basis $\mathcal{B}_i$ of $e_i\mathcal{R}$ over $\mathcal{R}_i$ such that every element $r \in \mathcal{R}$ can be written in the form $r = \sum_{i=1}^{l} \sum_{b \in \mathcal{B}_i} r_{i,b} b$, where $r_{i,b}$ is an element of the Galois ring $\mathcal{R}_i$. Then the elements of $\mathcal{R}_i$ can be written using elements from $\mathcal{S}_i$ as in

Section 3.1, and reducing to substitutions from $\oplus_{i=1}^{l}\mathcal{S}_i$ can be handled similarly as in case (a) in Sections 3.2 and 3.3. This method (whenever applicable, e.g. if $\mathcal{R}$ is unital) would be not only simpler but much faster, as well, than applying Lemma 8.

Unfortunately, this technique only works if $\mathcal{R}$ is unital, therefore Lemma 8 is essential to handle the general case. Lemma 8 proves the existence of an integer D, depending only on the ring $\mathcal{R}$, such that to obtain the range of a polynomial f over $\mathcal{R}$ one has to consider polynomials $f_{\overline{u}}$ for $\overline{u} \in \mathcal{J} \times \cdots \times \mathcal{J}$, where the number of nonzero entries in $\overline{u}$ is bounded by D. Note that the upper bound for the integer D obtained in this paper is multiply exponential in the size of the ring $\mathcal{R}$. Recent work [3, 11] suggests that the upper bound on D can be decreased significantly. Applying intriguing computational techniques over upper triangular matrix rings, Földvári [3] proved that solvability of $f = 0$ can be decided in $O\left(\|f\|^{|\mathcal{R}|^{2\log|\mathcal{R}|}(\log|\mathcal{R}|)^5}\right)$ time if $\mathcal{R} = \mathcal{J}$. Károlyi and Szabó [11] managed to reduce the exponent of $\|f\|$ to $O(|\mathcal{R}|\log|\mathcal{R}|)$ in the case $\mathcal{R} = \mathcal{J}$ by applying some current results in additive combinatorics. One might wonder if any of these techniques might be applicable to reduce the exponent D in Lemma 8.

Problem 1. Determine if the integer D in Lemma 8 can be bounded by a polynomial in the size of the ring $\mathcal{R}$.

For practical applications (such as solving a system of equations over commutative, finite rings) Theorem 6 could be a starting point. In Section 3 some of the estimates we gave were rather generous, and the upper bound (2) on the time complexity probably can be sharpened.

Problem 2. Determine if the integer L in Theorem 6 can be bounded by a polynomial in the size of the ring $\mathcal{R}$.

References

[1] 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.

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

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

[4] R. L. Graham, B. L. Rotschild, and J. H. Spencer. *Ramsey Theory*. Wiley-Interscience Series in Discrete Mathematics and Optimization. John Wiley & Sons, 2nd edition, 1990.

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

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

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

[8] G. Horváth. The complexity of the equivalence and equation solvability problems for meta-Abelian groups. *J. Algebra*, 433:208–230, 2015.
[9] 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.
[10] H. Hunt and R. Stearns. The complexity for equivalence for commutative rings. *Journal of Symbolic Computation*, 10:411–436, 1990.
[11] G. Károlyi and Cs. Szabó. Evaluation of polynomials over finite rings via additive combinatorics. 2016. submitted.
[12] J. Lawrence and R. Willard. The complexity of solving polynomial equations over finite rings. manuscript, 1997.
[13] B. R. MacDonald. *Finite rings with identity*. M. Dekker, 1974.
[14] R. Raghavendran. Finite associative rings. *Compositio Math.*, 21(2):195–229, 1969.
[15] Cs. Szabó and V. Vértesi. The equivalence problem over finite rings. *Internat. J. Algebra Comput.*, 21(3):449–457, 2011.
[16] R. S. Wilson. On the structure of finite rings. *Compositio Math.*, 26(1):79–93, 1973.

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

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

Department of Pure Mathematics, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada

E-mail address: rdwillar@uwaterloo.ca

Department of Pure Mathematics, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada