Glasgow Math. J. **54** (2012) 193–199. © Glasgow Mathematical Journal Trust 2011.
doi:10.1017/S001708951100053X.

THE COMPLEXITY OF THE EQUIVALENCE PROBLEM OVER FINITE RINGS

GÁBOR HORVÁTH

Institute of Mathematics, University of Debrecen, Pf. 12, Debrecen, 4010, Hungary
e-mail: ghorvath@science.unideb.hu

(Received 1 December 2010; revised 17 August 2011; accepted 24 September 2011)

Abstract. We investigate the complexity of the equivalence problem over a finite ring when the input polynomials are written as sum of monomials. We prove that for a finite ring if the factor by the Jacobson radical can be lifted in the centre, then this problem can be solved in polynomial time. This result provides a step in proving a dichotomy conjecture of Lawrence and Willard (J. Lawrence and R. Willard, The complexity of solving polynomial equations over finite rings (manuscript, 1997)).

2010 *Mathematics Subject Classification.* 16Z05, 16P10.

1. Introduction. Investigations into the algorithmic aspects of the equivalence problem for various finite algebraic structures were started in the early 1990s. The equivalence problem for a finite algebra $\mathcal{A}$ asks whether or not two expressions p and q are equivalent over $\mathcal{A}$ (denoted by $\mathcal{A} \models p \approx q$), i.e. whether p and q determine the same function over $\mathcal{A}$. This question is decidable for a finite algebra $\mathcal{A}$: checking all substitutions from $\mathcal{A}$ yields to an answer of this question. The equivalence problem is in coNP, since the 'no' answer can be verified by a substitution, where the two expressions differ. In this paper we investigate the computational complexity of the equivalence problem for finite rings. That is, for a given finite ring $\mathcal{R}$ what is the complexity of deciding whether or not two input polynomials determine the same function over $\mathcal{R}$?

First, Hunt and Stearnes [**5**] investigated the equivalence problem for finite rings. They proved that for finite nilpotent rings the polynomial equivalence problem could be solved in polynomial time in the length of the two input polynomials. Moreover, they proved that for commutative, non-nilpotent rings the equivalence problem is coNP-complete. Later, Burris and Lawrence [**2**] generalised their result to non-commutative rings, and established a dichotomy theorem for rings.

Theorem 1. *Let $\mathcal{R}$ be a finite ring. If $\mathcal{R}$ is nilpotent, then the (polynomial) equivalence problem can be solved in polynomial time. If $\mathcal{R}$ is not nilpotent, then the (polynomial) equivalence problem is coNP-complete.*

The proof given by Burris and Lawrence reduces the satisfiability (SAT) problem to the equivalence problem by using long products of sums. Nevertheless, polynomials are usually given as 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

This research was partially supported by the Hungarian National Foundation for Scientific Research grant K67870.

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. For this reason, Lawrence and Willard [**6**] introduced the sigma equivalence problem, i.e. when the input polynomials over the given ring are presented as sums of monomials where each monomial has the form $\alpha_1 \ldots \alpha_m$ with each α_i being a variable or an element of the ring. They investigated the equation solvability problem for finite rings, that is whether or not two input polynomial can attain the same value for at least one substitution. They formulated a conjecture about the complexity of the sigma equivalence and sigma equation solvability problem. In this paper we investigate their conjecture on the sigma equivalence problem.

Conjecture 2. *Let $\mathcal{R}$ be a finite ring and $\mathcal{J}$ be its Jacobson radical. If $\mathcal{R}/\mathcal{J}$ is commutative, then the sigma equivalence problem for $\mathcal{R}$ is solvable in polynomial time. If $\mathcal{R}/\mathcal{J}$ is not commutative, then the sigma equivalence problem for $\mathcal{R}$ is coNP-complete.*

Szabó and Vértesi proved the coNP-complete part of the conjecture in [**9**]. For matrix rings they proved a stronger theorem, that is the 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 [**4**]. For most matrix rings, arguments of Lawrence and Willard [**6**] establish coNP-completeness as well.

In this paper we investigate the case when $\mathcal{R}/\mathcal{J}$ is commutative. 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. Let $\mathcal{Z}$ be the centre of $\mathcal{R}$ and assume that $\mathcal{R}/\mathcal{J} = \mathcal{Z}/(\mathcal{Z} \cap \mathcal{J})$. Then the sigma equivalence problem for $\mathcal{R}$ is solvable in polynomial time.*

Theorem 3 establishes polynomial time complexity for an abundant class of rings for which $\mathcal{R}/\mathcal{J}$ is commutative.

Corollary 4. *Let $\mathcal{R}$ be a not necessarily unital, finite ring, and let $\mathcal{J}$ denote its Jacobson radical. The sigma equivalence problem for $\mathcal{R}$ is solvable in polynomial time*

(1) *if $\mathcal{R}$ is commutative, or*
(2) *if $\mathcal{R}$ is nilpotent, or*
(3) *if $\mathcal{R}$ is unital and $\mathcal{R}/\mathcal{J}$ is a sum of finite fields of different prime order.*

The conditions of Theorem 3 trivially hold in case (1) or in case (2). In the manuscript [**6**] one can find an independent argument for the sigma equation solvability problem in the case of unital commutative rings. Case (2) has already been proven earlier in [**5**], we just mention it as a consequence of our main theorem. In case (3) the unit of $\mathcal{R}$ additively generates $\mathcal{R}/\mathcal{J}$ by the Chinese Remainder Theorem, thus the conditions of Theorem 3 hold. For the proof of Theorem 3 we apply the theory of Galois rings. We summarise some of the most important properties of Galois rings in Section 2. Then we prove Theorem 3 in Section 3. The case where not every element of the factor by the Jacobson radical can be lifted into the centre remains open.

Problem 1. Let $\mathcal{R}$ be a ring and $\mathcal{J}$ be its Jacobson radical. Let $\mathcal{Z}$ be the centre of $\mathcal{R}$ and assume that $\mathcal{R}/\mathcal{J} \neq \mathcal{Z}/(\mathcal{Z} \cap \mathcal{J})$. Prove that the sigma equivalence problem is solvable in polynomial time for $\mathcal{R}$.

https://doi.org/10.1017/S001708951100053X Published online by Cambridge University Press

2. Galois rings. In this section we recall the theory of Galois rings necessary for our proof. The reader 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 by Raghavendran [**8**], and later by Wilson [**10**]. In the following we list some of the most important properties of Galois rings (see e.g. [**7**]). Let $h_d(x)$ 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 characterised 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, 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 [**10**, 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 the p^d-element field.

Let $\mathcal{R}$ be a finite local ring and let $\mathcal{J}$ be its Jacobson radical. Assume that the characteristic of $\mathcal{R}$ is p^c and that $\mathcal{R}/\mathcal{J}$ is a field containing p^d-many elements. Then $\mathcal{R}$ contains a subring isomorphic to $\mathcal{GR}(p^c, d)$ [**10**, p. 80, Theorem B]. Moreover, there exists an element r in this subring, which has multiplicative order $(p^d - 1)$ [**8**, p. 215, Theorem 9]. For such element r the set $\mathcal{S} = \{0\} \cup \left\{ r^j \mid 1 \leq j \leq p^d - 1 \right\}$ is a representation system for $\mathcal{R}/\mathcal{J}$.

3. Proof of Theorem 3. We prove Theorem 3 in this section. First, we fix the setting and the notations of the proof. Then we sketch a polynomial time algorithm for deciding whether or not two polynomials are identically equal if the conditions of Theorem 3 hold. Finally, we explain every step in detail.

Note first that for a ring $\mathcal{R}$ and polynomials p, q over $\mathcal{R}$ we have $\mathcal{R} \models p \approx q$ if and only if $\mathcal{R} \models p - q \approx 0$. Therefore, from now on we assume that the input of the equivalence problem is one polynomial f and we need to check whether or not $f \approx 0$. Secondly, the sigma equivalence 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 we only consider rings having prime power characteristic.

Now, we fix the notations for the proof. Let the characteristic of $\mathcal{R}$ be p^c for some prime p. Let $\mathcal{J}$ be the Jacobson radical of $\mathcal{R}$ and let t be the smallest positive integer for which $\mathcal{J}^t = \{0\}$. Let $\mathcal{Z}$ be the centre of $\mathcal{R}$. By the Pierce decomposition theorem (see e.g. [**3**]) the ring $\mathcal{Z}$ is the direct sum of a commutative nilpotent ring $\mathcal{Z}_0$ and some commutative, unital, local rings $\mathcal{Z}_1, \dots, \mathcal{Z}_l$, i.e. $\mathcal{Z} = \oplus_{i=0}^{l} \mathcal{Z}_i$. Here $\mathcal{Z}_0 \subseteq \mathcal{J}$. The unique maximal ideal of $\mathcal{Z}_i$ is its Jacobson radical $\mathcal{Z}_i \cap \mathcal{J}$ $(1 \leq i \leq l)$. Let the characteristic of $\mathcal{Z}_i$ be p^{c_i}. As $\mathcal{Z}_i$ is commutative and local, $\mathcal{Z}_i / (\mathcal{Z}_i \cap \mathcal{J})$ is a field. Let $\mathcal{F}_i$ denote the field $\mathcal{Z}_i / (\mathcal{Z}_i \cap \mathcal{J})$, and let $q_i = p^{d_i}$ be the number of its elements. By assumption,

$$\mathcal{R}/\mathcal{J} = \mathcal{Z}/(\mathcal{Z} \cap \mathcal{J}) = \oplus_{i=1}^{l} \mathcal{Z}_i / (\mathcal{Z}_i \cap \mathcal{J}) = \oplus_{i=1}^{l} \mathcal{F}_i.$$

We find a central representation system for $\mathcal{R}/\mathcal{J}$ in $\mathcal{R}$ with the help of Galois rings. Every commutative finite local ring contains a Galois subring (see Section 2), i.e. for

https://doi.org/10.1017/S001708951100053X Published online by Cambridge University Press

each $1 \leq i \leq l$ there exists a subring $\mathcal{R}_i \leq \mathcal{Z}_i$ such that $\mathcal{R}_i$ is isomorphic to the Galois ring $\mathcal{GR}(p^{c_i}, d_i)$. Moreover, there exists an element $r_i \in \mathcal{R}_i$, which has multiplicative order $p^{d_i} - 1$. Then, the element $r_i + (\mathcal{J} \cap \mathcal{Z}_i)$ generates $\mathcal{F}_i \setminus \{ 0 \}$ multiplicatively. For every $1 \leq i \leq l$ let $\mathcal{S}_i = \{ 0 \} \cup \{ r_i^j \mid 1 \leq j \leq p^{d_i} - 1 \}$ and let

$$\mathcal{S} = \oplus_{i=1}^{l} \mathcal{S}_i = \left\{ s_1 + \cdots + s_l \mid s_i \in \mathcal{S}_i, 1 \leq i \leq l \right\}.$$

Now, $\mathcal{S}_i$ is a representation system for the field $\mathcal{F}_i$, and is central as $\mathcal{S}_i \subseteq \mathcal{R}_i \subseteq \mathcal{Z}_i$. Hence, $\mathcal{S} \subseteq \mathcal{Z}$ is a central representation system for $\mathcal{R}/\mathcal{J}$, i.e. $\mathcal{R} = \left\{ s + u \mid s \in \mathcal{S}, u \in \mathcal{J} \right\}$.

The idea of the proof is the following. Let f be a polynomial over $\mathcal{R}$ written as a sum of monomials having non-commuting variables and elements of $\mathcal{R}$. Then we have $\mathcal{R} \models f \approx 0$ if for every $u_1, \ldots, u_n \in \mathcal{J}$ the polynomials $f(x_1 + u_1, \ldots, x_n + u_n)$ attain value 0 for substitutions from $\mathcal{S}$. In Lemma 5 we will prove that it is enough to consider such n-tuples $\overline{u} = (u_1, \ldots, u_n)$, where the number of non-zero coordinates are at most t. Thus, we only need to check polynomially many new polynomials instead of exponentially many new ones. We need to consider these polynomials for substitutions from $\mathcal{S} = \oplus_{i=1}^{l} \mathcal{S}_i$, which is equivalent to check them for substitutions from $\mathcal{S}_i$ for every $1 \leq i \leq l$. Now, the Galois ring $\mathcal{R}_i$ contains $\mathcal{S}_i$, and we consider $\mathcal{R}$ as an $\mathcal{R}_i$-module. Then $\mathcal{R}$ is a direct sum of cyclic $\mathcal{R}_i$-modules, and a polynomial is equivalent to 0 if and only if it is equivalent to 0 in every submodule. This way we reduce the problem to check polynomials over a Galois ring and consider substitutions only from $\mathcal{S}_i$. Finally, in Lemma 6 we characterise those polynomials that are equivalent to 0 over a Galois ring for substitutions from $\mathcal{S}_i$.

Let f be a polynomial over $\mathcal{R}$ written as a sum of monomials having non-commuting variables and elements of $\mathcal{R}$. We denote the length of f by $\|f\|$. First we 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

$$f_{\overline{u}}(x_1, \ldots, x_n) = f(x_1 + u_1, \ldots, x_n + u_n) \tag{1}$$

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 arbitrary substitution. Thus, $f_{\overline{u}}$ can be calculated in $O(\|f\|^t)$ time and $\|f_{\overline{u}}\| = O(\|f\|^t)$. Consider the polynomials $f_{\overline{u}}$ for every possible $u_1, \ldots, u_n \in \mathcal{J}$. We say that $\mathcal{R} \models f_{\overline{u}} \approx 0$ *for substitutions from* $\mathcal{S}$ if for every $s_1, \ldots, s_n \in \mathcal{S}$ we have $f_{\overline{u}}(s_1, \ldots, s_n) = 0$. It is clear that $\mathcal{R} \models f \approx 0$ if and only if for every $\overline{u}$ we have $\mathcal{R} \models f_{\overline{u}} \approx 0$ for substitutions from $\mathcal{S}$. Now, the number of the $f_{\overline{u}}$ polynomials is $|\mathcal{J}|^n$, which is an exponential number in $\|f\|$. Nevertheless, by the following lemma we only need to consider those $f_{\overline{u}}$ polynomials for which the number of non-zero u_i coordinates in $\overline{u}$ is less than t.

LEMMA 5. *We have $\mathcal{R} \models f \approx 0$ if and only if $\mathcal{R} \models f_{\overline{u}} \approx 0$ for substitutions from $\mathcal{S}$ for every $\overline{u}$ for which $\left|\left\{ 1 \leq i \leq n \mid u_i \neq 0 \right\}\right| < t$.*

Proof. If $\mathcal{R} \models f \approx 0$, then $\mathcal{R} \models f_{\overline{u}} \approx 0$ for substitutions from $\mathcal{S}$ for every $\overline{u}$, in particular $\mathcal{R} \models f_{\overline{u}} \approx 0$ for substitutions from $\mathcal{S}$ for $\overline{u}$ with less than t non-zero coordinates. For the other direction let $u_1, \ldots, u_n \in \mathcal{J}$ be arbitrary. For a subset $I \subseteq \{ 1, \ldots, n \}$ let $\overline{u}_I = \left(u_1', \ldots, u_n'\right)$ be the n-tuple for which $u_i' = u_i$ for $i \in I$ and $u_i' = 0$ for $i \notin I$. Now separate the monomials in $f_{\overline{u}}$ depending on which u_is occur in them: for every $I \subseteq \{ 1, \ldots, n \}$ let g_I be the sum of those monomials of $f_{\overline{u}}$ in which u_i occurs if

https://doi.org/10.1017/S001708951100053X Published online by Cambridge University Press

$i \in I$ and u_i does not occur if $i \notin I$. Now, for a fixed subset $H \subseteq \{1, \dots, n\}$ we have

$$g_H = \sum_{I \subseteq H} (-1)^{|I|} f_{\overline{u}_I}. \tag{2}$$

Assume that $\mathcal{R} \models f_{\overline{u}_I} \approx 0$ for substitutions from $\mathcal{S}$ if $|I| < t$. Since every monomial in $f_{\overline{u}}$ contains less than t-many u_is, the right-hand side of (2) always attains the value 0. Hence, $\mathcal{R} \models g_H \approx 0$ for substitutions from $\mathcal{S}$ for arbitrary $H \subseteq \{1, \dots, n\}$. Now, $f_{\overline{u}} = \sum_{H \subseteq \{1,\dots,n\}} g_H$, thus $\mathcal{R} \models f_{\overline{u}} \approx 0$ for substitutions from $\mathcal{S}$. This holds for arbitrary $\overline{u}$ from $\mathcal{J}$, hence $\mathcal{R} \models f \approx 0$. □

Let T_t be the set of $\overline{u}$-tuples for which the number of non-zero u_i coordinates is less than t:

$$T_t = \left\{ (u_1, \dots, u_n) \mid u_i \in \mathcal{J}, 1 \le i \le n, |\{ 1 \le i \le n : u_i \neq 0 \}| < t \right\}.$$

Then

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

which is polynomial in $\|f\|$. Thus, $\mathcal{R} \models f \approx 0$ if and only if for every $\overline{u} \in T_t$ we have $f_{\overline{u}} \approx 0$ for substitutions from $\mathcal{S}$. Each of these polynomials is computable in $O(\|f\|^t)$ time, thus the reduction is polynomial.

Now, fix $\overline{u} = (u_1, \dots, u_n)$, where the number of non-zero u_is is less than t. Let $g = f_{\overline{u}}$. We prove that it can be checked in polynomial time whether or not $\mathcal{R} \models g \approx 0$ for substitutions only from $\mathcal{S}$. Now, $\mathcal{S} = \oplus_{i=1}^{l} \mathcal{S}_i$, and $\mathcal{S}_i\mathcal{S}_j = \{0\}$ for $i \neq j$. If the constant coefficient of g is not 0, then $g(0, \dots, 0) \neq 0$ and $\mathcal{R} \models g \not\approx 0$. Otherwise, for arbitrary $s_1^{(i)}, \dots, s_n^{(i)} \in \mathcal{S}_i$ $(1 \le i \le l)$ we have

$$g\left(\sum_{i=1}^{l} s_1^{(i)}, \dots, \sum_{i=1}^{l} s_n^{(i)}\right) = \sum_{i=1}^{l} g\big(s_1^{(i)}, \dots, s_n^{(i)}\big).$$

Therefore, $\mathcal{R} \models g \approx 0$ for substitutions from $\mathcal{S}$ if and only if for every $1 \le i \le l$ we have $\mathcal{R} \models g \approx 0$ for substitutions from $\mathcal{S}_i$.

Let i be fixed. Recall that $\mathcal{Z}_i$ is a local ring in the centre of $\mathcal{R}$ with characteristic p^{c_i}. The factor $\mathcal{Z}_i/\mathcal{Z}_i \cap \mathcal{J}$ is a field $\mathcal{F}_i$ of $p^{d_i} = q_i$ elements. Moreover, $r_i \in \mathcal{Z}_i$ was an element of multiplicative order $q_i - 1$ and $\mathcal{S}_i = \{0\} \cup \left\{ r_i^j \mid 1 \le j \le q_i - 1 \right\}$. Note that $s^{q_i} = s$ for every $s \in \mathcal{S}_i$. Let us rearrange every monomial of g into the form $x_1^{k_1} x_2^{k_2} \dots x_n^{k_n} \cdot r$, where $r \in \mathcal{R}$. The resulting polynomial and g attains the same values for substitutions from $\mathcal{S}_i$, since $\mathcal{S}_i$ is in the centre of $\mathcal{R}$. For every $1 \le j \le n$ let us execute polynomial long division by $\left(x_j^{q_i} - x_j\right)$ to obtain the remainder: replace the exponent of x_j by its modulo $(q_i - 1)$ equivalent from the set $\{1, 2, \dots, q_i - 1\}$. This requires $O(n \cdot \|g\|)$ time. Finally, we collect together every monomial for which the exponents of $x_1, \dots, x_n$ are respectively equal. The resulting polynomial attains the same values for substitutions from $\mathcal{S}_i$, thus we may assume that these steps are already executed on g.

The Galois ring $\mathcal{R}_i \le \mathcal{Z}_i$ lies in the centre of $\mathcal{R}$. Every finite module over a Galois ring is a direct sum of cyclic modules. Let us consider $\mathcal{R}$ as an $\mathcal{R}_i$-module. Thus, $\mathcal{R}$ is

https://doi.org/10.1017/S001708951100053X Published online by Cambridge University Press

a direct sum of $\mathcal{R}_i$-modules, i.e. there exist $b_1, \dots, b_k \in \mathcal{R}$ such that

$$\mathcal{R} = \mathcal{R}_i b_1 \oplus \cdots \oplus \mathcal{R}_i b_k,$$

as an $\mathcal{R}_i$-module. Every element $r \in \mathcal{R}$ can be written in the form $\sum_{j=1}^{k} r_j b_j$, where $r_j \in \mathcal{R}_i$ $(1 \leq j \leq k)$. Let us write every coefficient of g in the form $\sum_{j=1}^{k} r_j b_j$. Then, let us write g as the sum of the corresponding components:

$$g(x_1, \dots, x_n) = \sum_{j=1}^{k} g_j(x_1, \dots, x_n) \cdot b_j,$$

where each $g_j \in \mathcal{R}_i[x_1, \dots, x_n]$ is now a polynomial over $\mathcal{R}_i$ (instead of a polynomial over $\mathcal{R}$); moreover, every variable in every monomial of g_j has exponent at most $(q_i - 1)$. Every g_j can be computed in $O(\|g\|)$ time, and $\|g_j\| = O(\|g\|)$ $(1 \leq j \leq k)$. Thus, $\mathcal{R} \models g \approx 0$ for substitutions from $\mathcal{S}_i$ if and only if for every $1 \leq j \leq k$ and for every $s_1, \dots, s_n \in \mathcal{S}_i$ we have $g_j(s_1, \dots, s_n) \in \mathrm{Ann}\{b_j\}$. Since $\mathrm{Ann}\{b_j\}$ is an ideal in the Galois ring $\mathcal{R}_i \simeq \mathcal{GR}(p^{c_i}, d_i)$, for every $1 \leq j \leq k$ there exists $0 \leq e_j \leq c_i$ such that $\mathrm{Ann}\{b_j\} = (p^{e_j})$. Thus, $g_j(s_1, \dots, s_n) \in \mathrm{Ann}\{b_j\}$ if and only if $p^{c_i - e_j} \cdot g_j(s_1, \dots, s_n) = 0$. In summary: $\mathcal{R} \models g \approx 0$ for substitutions from $\mathcal{S}_i$ if and only if for every $1 \leq j \leq k$ we have $\mathcal{R}_i \models p^{c_i - e_j} \cdot g_j \approx 0$ for substitutions from $\mathcal{S}_i$. This latter condition can be decided in polynomial time, as it is equivalent to $p^{c_i - e_j} \cdot g_j$ being the 0-polynomial by the following lemma.

LEMMA 6. *Let $\mathcal{R}$ be isomorphic to the Galois ring $\mathcal{GR}(p^c, d)$. Let $q = p^d$, r be an element of multiplicative order $(q-1)$, and $\mathcal{S} = \{0\} \cup \left\{ r^j \mid 1 \leq j \leq q - 1 \right\}$. Let $h \in \mathcal{R}[x_1, \dots, x_n]$ be a polynomial, written as a sum of monomials such that every exponent of every variable in each monomial is at most $(q-1)$ and every monomial appears at most once. Then $\mathcal{R} \models h \approx 0$ for substitutions from $\mathcal{S}$ if and only if each coefficient of every monomial in h is 0.*

Proof. If each coefficient in h is 0, then $h \approx 0$. We prove the other direction by induction on c. The case of $c = 1$, i.e. when $\mathcal{R}$ is isomorphic to the q-element field, is proved in **[1]** by induction on the number of variables. Assume that $c \geq 2$ and that $\mathcal{R} \models h \approx 0$ for substitutions from $\mathcal{S}$. Let $\mathcal{F} = \mathcal{GR}(p^c, d)/(p)$, then $\mathcal{F}$ is the q-element field. Now $\mathcal{S}$ is a representation system for $\mathcal{F}$ in $\mathcal{R}$, thus $\mathcal{F} \models h \approx 0$. By the induction hypothesis, every coefficient of h is divisible by p, i.e. $h = p \cdot h'$ for some polynomial h'. Hence, $\mathcal{R} \models h \approx 0$ for substitutions from $\mathcal{S}$ yields that h' attains values from the ideal (p^{c-1}). Thus, $\mathcal{R}/(p^{c-1}) \models h' \approx 0$ for substitutions from $\mathcal{S}$. Since $\mathcal{GR}(p^c, d)/(p^{c-1}) \simeq \mathcal{GR}\left(p^{c-1}, d\right)$, by induction every coefficient of h' is 0 in the factor ring $\mathcal{R}/\left(p^{c-1}\right)$, i.e. every coefficient of h' is divisible by p^{c-1} in $\mathcal{R}$. Thus, every coefficient of h is divisible by p^c. □

REFERENCES

1. S. Burris and J. Lawrence, Term rewrite rules for finite fields, *Int. J. Algebr. Comput.* **1** (1991), 353–369.

2. S. Burris and J. Lawrence, The equivalence problem for finite rings, *J. Symb. Comp.* **15** (1993), 67–71.

3. M. Hazewinkel, N. Gubareni and V. V. Kirichenko, *Algebras, rings and modules*, vol. 1 (Springer, New York, 2004).

https://doi.org/10.1017/S001708951100053X Published online by Cambridge University Press

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

5. H. Hunt and R. Stearns, The complexity for equivalence for commutative rings, *J. Symb. Comp.*. **10** (1990), 411–436.

6. J. Lawrence and R. Willard, The complexity of solving polynomial equations over finite rings (manuscript, 1997).

7. B. R. MacDonald, *Finite rings with identity* (M. Dekker, New York, 1974).

8. R. Raghavendran, Finite associative rings, *Comp. Math.* **21**(2) (1969), 195–229.

9. Cs. Szabó and V. Vértesi, The equivalence problem over finite rings, *Internat. J. Algebra Comput.* **21**(3) (2011), 449–457.

10. R. S. Wilson, On the structure of finite rings, *Comp. Math.* **26**(1) (1973), 79–93.

https://doi.org/10.1017/S001708951100053X Published online by Cambridge University Press