International Journal of Algebra and Computation
Vol. 21, No. 3 (2011) 449–457

DOI: 10.1142/S021819671100625X

World Scientific
www.worldscientific.com

THE EQUIVALENCE PROBLEM OVER FINITE RINGS

CSABA SZABÓ* and VERA VÉRTESI†

Department of Algebra and Number Theory
Eötvös Loránd University, 1117 Budapest
Pázmány Péter sétány 1/c, Hungary
**csaba@cs.elte.hu*
†*wera13@cs.elte.hu*

Received 21 May 2010
Revised 1 September 2010

Communicated by R. McKenzie

We investigate the computational complexity of deciding whether or not a given polynomial, presented as the sum of monomials, is identically 0 over a ring. It is proved that if the factor by the Jacobson-radical is not commutative, then the problem is coNP-complete.

Keywords: Term; equivalence problem; ring; complexity.

Mathematics Subject Classification 2010:

1. Introduction

A *ring* is a set equipped with three operations: the multiplication $\cdot$, the addition $+$ and the additive inverse operation $-$. A *term* over a ring is an expression $t(x_1, \ldots, x_n)$ built up from variables and the fundamental operation symbols in the usual manner. In other words terms over rings are polynomials with integer coefficients. A term $t(x_1, \ldots, x_n)$ over any ring R defines a so-called *term-function* $t^R : R^n \to R$. A ring R *satisfies* an equation $s(\vec{x}) \approx t(\vec{x})$ or $R \models s \approx t$ if the corresponding term-functions s^R and t^R are the same functions.

The (*term*) *equivalence problem* for a ring R is the problem of deciding which equations are satisfied by R. Over a given ring R the instance of the equivalence problem is an equation $s(\vec{x}) \approx t(\vec{x})$, and the goal is to decide whether it is satisfied by R or not. If $s(\vec{x}) \not\approx t(\vec{x})$, then there is a substitution form R where the two term-functions s^R and t^R do not agree, so the equivalence problem is in coNP.

Early investigations into the equivalence problem for various finite algebraic structures were carried out by computer scientists at Syracuse University where the terminology the *term equivalence problem* was introduced. In particular they considered finite commutative rings and finite lattices. In the early 1990s it was

shown by Hunt and Stearns [7] that for a commutative ring R the equivalence problem is in P if R is nilpotent and coNP-complete otherwise. Burris and Lawrence [2] proved that the same holds for rings in general.

The formal definitions of terms and polynomials allow us to use iterated addition and multiplication, for example, the expression $(x_1 + y_1)(x_2 + y_2)\cdots(x_n + y_n)$ is a term over a ring. If we expand this term into a sum of monomials, we obtain a sum of 2^n many monomials of length n. The length of a term is crucial from the computational point of view. Moreover, when a ring-term is presented, in most cases it is given as a sum of monomials. If one restricts the terms that are allowed as instances of the equivalence problem, e.g. to monomials or to sum of monomials, then the complexity of the problem can change. This is the reason why Horváth, Lawrence and Willard introduced the Σ version of the identity checking problem for rings [6]. In the following we investigate a version of the equivalence problem where the instance terms must be given as sums of monomials. Of course every term over a ring can be written in such a form, but, as we saw, during the expansion its length can grow exponentially.

The complexity of the problem changes, indeed, as it is shown in [4]: if R is commutative, then the equivalence problem over R for sum of monomials is in P. The proof is heavily based on the structure of commutative finite rings. They reduce the equivalence problem for commutative rings to the same problem over Galois-rings. The following conjecture is formulated.

Conjecture [4, 6]. *Let R be a finite ring, and let $J(R)$ denote its Jacobson-radical. Then*

(1) *if $R/J(R)$ is commutative, then the equivalence problem for sum of monomials is in P;*
(2) *the equivalence problem for sum of monomials is coNP-complete, otherwise.*

In this paper we prove the second part of the conjecture.

Theorem 1. *Let R be a finite ring, and let $J(R)$ denote its Jacobson-radical. If $R/J(R)$ is not commutative, then the equivalence problem for sum of monomials is coNP-complete.*

For matrix rings the complexity of this version of the equivalence problem has been determined; the equivalence problem for sum of monomials is in P, if the matrix ring is commutative and coNP-complete otherwise. This result was shown by Lawrence and Willard [6] for matrix rings whose group of units forms a non-solvable group, and by Szabó and Vértesi [8, 9] for the remaining cases, $M_2(\mathbb{Z}_2)$ and $M_2(\mathbb{Z}_3)$.

If we restrict the inputs of the equivalence problem to monomials, then in fact we are working in the multiplicative semigroup of the ring R. In this paper we characterize the complexity of the equivalence problem over matrix semigroups.

Theorem 2. *For a matrix semigroup $(M_n(q), \cdot)$, the equivalence problem is in P if the semigroup is commutative and coNP-complete otherwise.*

For groups the characterization of the equivalence problem is far less complete. In 2004 Burris and Lawrence [3] proved that if G is nilpotent or $G \simeq D_n$, the dihedral group for odd ns, then the equivalence problem for G is in P. Toward the hard side Horváth *et al.* [5] proved that for a non-solvable group G the equivalence problem is coNP-complete.

2. Preliminaries

Let $M_n(q)$ denote the ring of $n \times n$ matrices over the q element field $\mathbb{F}_q$, where $q = p^\beta$ for some prime p. The *general linear group* $\mathrm{GL}_n(q)$ is the group of invertible elements of $M_n(q)$, and the *special linear group* $\mathrm{SL}_n(q)$ is the subgroup containing the elements of determinant 1. All normal subgroups of $\mathrm{SL}_n(q)$ are contained in its center, $Z(\mathrm{SL}_n(q))$, if $n > 2$ or $q > 3$. The *projective linear group* $\mathrm{PSL}_n(q)$ is defined as the factor of $\mathrm{SL}_n(q)$ by $Z(\mathrm{SL}_n(q))$. If $n > 2$ or $q > 3$, then $\mathrm{PSL}_n(q)$ is simple.

The proof of Theorem 2 is a reduction to the equivalence problem to its group of units. For this first we will focus on properties of matrix groups, and then show how our reduction works.

2.1. *Verbal subgroups*

First we will list here some definitions and easy observations about verbal subgroups of groups and commutators from [5], extending them to $\mathrm{GL}_n(q)$.

Let G be a finite group. Given a set T of group terms let

$$T(G) = \bigcup_{t \in T} \mathsf{Range}(t^G)$$

be the union of the ranges of the term functions t^G. The subgroup generated by $T(G)$, which we denote by

$$T^*(G) = \langle T(G) \rangle$$

is called a *verbal* subgroup of G. The subgroups $\{\mathrm{id}\}$ and G are verbal subgroups of G. If these are the only verbal subgroups of G, then we say G is *verbally simple*. Every simple group is verbally simple as a verbal subgroup is always normal. Moreover,

$$T^*(G_1 \times G_2) = T^*(G_1) \times T^*(G_2).$$

Given two terms $s(x_1, \ldots, x_m)$ and $t(x_1, \ldots, x_n)$, we define the term s_t by

$$s_t(x_1, \ldots, x_{mn}) = s(t(x_1, \ldots, x_n), t(x_{n+1}, \ldots, x_{2n}), \ldots, t(x_{mn-n+1}, \ldots, x_{mn})).$$

For a finite group G let d_G be the minimal positive integer such that for any set X of generators of G we have

$$G = \bigcup_{0 \le k \le d_G} X^k.$$

Given a term $s(x_1, \dots, x_m)$ and an integer k define the term s_k by

$$s_k(x_1, \dots, x_{mk}) := \underbrace{s(x_1, \dots, x_m) \cdot s(x_{m+1}, \dots, x_{2m}) \cdots}_{\text{a product of } k \text{ terms } s(\cdots), \text{ with distinct variables}} .$$

Note that $s^*(G) = s_{d_G}(G)$ is the verbal subgroup generated by the image of s. The *commutator* is a group term defined by $c(x, y) = [x, y] = x^{-1}y^{-1}xy$. For $a \in G$ let $[a, G] = \langle\{[a, g] : g \in G\}\rangle$. $[a, G]$ is a normal subgroup of G. If G is a non-abelian simple group, then

$$[a, G] = \begin{cases} \{\mathrm{id}\} & \text{if } a = \mathrm{id}, \\ G & \text{if } a \neq \mathrm{id}. \end{cases}$$

If $n > 2$ or $q > 3$, the commutator subgroup of $\mathrm{GL}_n(q)$ is $\mathrm{SL}_n(q)$ and

$$[a, \mathrm{GL}_n(q)] = \begin{cases} \{\mathrm{id}\} & \text{if } a \in Z(\mathrm{GL}_n(q)), \\ \mathrm{SL}_n(q) & \text{if } a \notin Z(\mathrm{GL}_n(q)). \end{cases}$$

Our starting point will be the following result from [5].

Lemma 3. *For every graph Γ and for every positive integer k, there exists a group term $t_{\Gamma,k}$, such that the size of $t_{\Gamma,k}$ is polynomial in k and in the size of Γ, and for every simple group G if $k \geq d_G$ then $G \models t_{\Gamma,k} \approx \mathrm{id}$ if and only if Γ is not $|G|$-colorable. Moreover, for every group H the image of $t_{\Gamma,k}$ is contained in the commutator subgroup: $t_{\Gamma,k}(H) \leq H'$. Furthermore, if Γ has at least nine edges, then $t_{\Gamma,k}(H)$ is contained in the fourth commutator subgroup of H.*

Now we are able to make the first step toward the reduction.

Lemma 4. *Let p be a prime, $q = p^\beta, q_1 = p^{\alpha_1}, \dots, q_m = p^{\alpha_m}$.*

(1) *Let n be a positive integer and let $k = |\mathrm{PSL}_n(q)|$. Then for every positive integer $d > d_{\mathrm{PSL}_n(q)}$ and for every graph Γ containing at least nine edges, there exists a group word s (over the group $\mathrm{GL}_n(q)$) such that*

- $\mathrm{GL}_n(q) \models s_d \approx \mathrm{id}$ *if Γ is not k-colorable or $n = 2$ and $q = 2, 3$;*
- $s(\mathrm{GL}_n(q)) = \mathrm{SL}_n(q)$ *otherwise.*

(2) *Let $\mathrm{GL}_{n_1}(q_1), \dots, \mathrm{GL}_{n_m}(q_m)$ be matrix groups. Suppose that $n_1 > 2$ or $q_1 > 3$, and let $k = \max_{1 \leq i \leq m}\{|\mathrm{PSL}_{n_i}(p^{\alpha_i})|\}$. Then for every graph Γ there is a group term s such that*

- *if Γ is not k-colorable, then $\mathrm{GL}_{n_i}(q_i) \models s \approx \mathrm{id}$ for every i;*
- *if Γ is k-colorable, then $s(\mathrm{GL}_{n_i}(q_i)) = \mathrm{SL}_{n_i}(q_i)$ for some $1 \leq i \leq m$.*

Proof. (1) Let Γ be a graph and let $s = t_{\Gamma,d}$ be the term constructed in Lemma 3 with $G = \mathrm{PSL}_n(q)$. Assume first that $n > 2$ or $q > 3$, and Γ is k-colorable. We claim that $s^*(\mathrm{GL}_n(q)) = \mathrm{SL}_n(q)$. By Lemma 3 we have $s^*(\mathrm{GL}_n(q)) \leq \mathrm{GL}_n(q)' = \mathrm{SL}_n(q)$. As $\mathrm{PSL}_n(q)$ is simple, $s^*(\mathrm{PSL}_n(q)) = \mathrm{PSL}_n(q)$, hence, as

$\mathrm{SL}_n(q)/Z(\mathrm{SL}_n(q)) = \mathrm{PSL}_n(q)$, the image of s over $\mathrm{SL}_n(q)$ is not contained in the center of $\mathrm{SL}_n(q)$. As $s^*(\mathrm{GL}_n(q))$ is normal in $\mathrm{GL}_n(q)$, we have $s^*(\mathrm{GL}_n(q)) = \mathrm{SL}_n(q)$. If $n = 2$ and $q = 2$ or 3, the solvable lengths of $\mathrm{GL}_2(2)$ and $\mathrm{GL}_2(3)$ are 2 and 4, thus s satisfies the conditions of the lemma.

Now, for (2), let Γ be a graph and let s be the term constructed in (1) with $d = \max_i d_{\mathrm{GL}_{n_i}(q_i)}$. Now, $s(\mathrm{GL}_2(2)) = 1$ and $s(\mathrm{GL}_2(3)) = 1$. For every i, where $n_i > 2$ or $q_i > 3$ we have $s(\mathrm{GL}_{n_i}(q_i)) = \mathrm{SL}_{n_i}(q_i)$ if Γ is not $|\mathrm{PSL}_{n_i}(q_i)|$-colorable and $s(\mathrm{GL}_{n_i}(q_i)) = \mathrm{id}$ otherwise. Let us assume that Γ is not k-colorable. Then Γ is not l-colorable for any $l \leq k$. Thus $s^*(\mathrm{GL}_{n_i}(q_i)) = \{\mathrm{id}\}$ for every $1 \leq i \leq m$. Now, assume that Γ is k-colorable. Then $s^*(\mathrm{GL}_{n_j}(q_j)) = \mathrm{SL}_{n_j}(q_j)$ whenever $|\mathrm{PSL}_{n_j}(p^{\alpha_j})| = k = \max_{1\leq i\leq m}\{|\mathrm{PSL}n_i(p^{\alpha_i})|\}$. Thus $s = s_d$ satisfies the conditions. □

2.2. *Matrix semigroups*

Next, for every matrix ring we present an integer N such that for all but a few invertible matrices M the matrix M^N is idempotent. For the sizes of the groups $\mathrm{GL}_m(q)$ and $\mathrm{SL}_m(q)$ one has the following well-known formulas:

$$\begin{aligned}|\mathrm{GL}_m(p^\beta)| &= (p^{\beta m} - 1)(p^{\beta m} - p^\beta)\cdots(p^{\beta m} - p^{\beta(m-1)}) \\ &= p^{\beta(m(m-1)/2)}(p^{\beta m} - 1)(p^{\beta(m-1)} - 1)\cdots(p^\beta - 1)\end{aligned}$$

and

$$|\mathrm{SL}_m(p^\beta)| = \frac{|\mathrm{GL}_m(p^\beta)|}{p^\beta - 1}.$$

Our main lead will be the following theorem of Zsigmondy.

Theorem 5 (Zsigmondy [10]). *Let a, k be integers both greater than 1. Then except in the cases $k = 2$, $a = 2^\gamma - 1$ and $k = 6, a = 2$, there is a prime r with the following properties*:

(1) *r divides $a^k - 1$;*
(2) *r does not divide $a^i - 1$ whenever $0 < i < k$;*
(3) *r does not divide k.*

In particular, k is the order of a modulo r.

Lemma 6. *Let $M_n(q)$ be a matrix ring where $n > 1$. There is a positive integer N such that for every $A \in M_n(q)$ either A^N is idempotent (a projection) or A^N is invertible in $M_n(q)$. Moreover, there is at least one element in $A \in \mathrm{SL}_n(q)$, such that $A^N \neq \mathrm{id}$.*

Proof. Case 1. Let $q = a$ and $n = k$ be not among the exceptional cases of Zsigmondy's theorem. Let r be the prime from Zsigmondy's theorem and t such

that

$$r^t \,|\, p^\alpha - 1 \quad \text{and} \quad r^{t+1} \nmid p^\alpha - 1.$$

Moreover, let

$$N = \alpha \frac{|\mathrm{GL}_\alpha(p)|}{r^t}.$$

Let A be an arbitrary matrix in $M_n(q)$. For every $m \geq n$ the matrix A^m acts on $W = \operatorname{Im} A^m$ as a linear transformation and the action is invertible. Thus if $\dim W = l$, then $(A^m)^{|\mathrm{GL}_l(q)|}$ is a projection (idempotent). Obviously,

- $\alpha \geq n$ and
- $|\mathrm{GL}_l(q)|$ divides $|\mathrm{GL}_n(q)|$ for every $n > l$, and
- $(r, |\mathrm{GL}_l(q)|) = 1$ for every $n > l$.

Hence, if $l < n$, then $|\mathrm{GL}_l(q)|$ divides $|\mathrm{GL}_n(q)|/r^t$. Thus for every matrix $A \in M_n(q)$, where A is not invertible, the matrix A^N is idempotent. Finally, r divides $|\mathrm{SL}_n(q)|$, because $|\mathrm{SL}_n(q)| = |\mathrm{GL}_n(q)|/(q-1)$. Thus by Cauchy's theorem there is an element $B \in \mathrm{SL}_n(q)$ of order r. Clearly, $B^N \neq \mathrm{id}$.

Case 2. Let $p = 2^\gamma - 1$. Then $N = 2(p-1)$ works. Now, $|\mathrm{GL}_1(p)| = p - 1$ and $|\mathrm{SL}_2(p)| = [(p^2-1)(p^2-p)]/(p-1)$. Every non-zero, not invertible matrix $A \in M_2(p)$ is of rank 1. Thus $A^{2(p-1)}$ is a projection. If A is of order p (such an A exists by Cauchy's theorem), then $A^{2(p-1)} = A^{p-2} \neq \mathrm{id}$.

Case 3. Finally, let us consider the most unlucky case, where $\max\{q_i^{n_i}\} = 2^6$. The following tables will be useful in our investigations:

The exponents of $\mathrm{GL}_m(2^\beta)$:

β \ m	1	2	3	4	5	6
1	1	6	84	420	26040	78120
2	3	30	1260			
3	7	126				

The exponents of $\mathrm{SL}_m(2^\beta)$.

β \ m	1	2	3	4	5	6
1	1	6	84	420	26040	78120
2	1	30	420			
3	1	126				

Let A be an arbitrary matrix in $M_n(q)$. As in the previous two cases, for every $m \geq n$ the matrix A^m acts on $W = \operatorname{Im} A^m$ as a linear transformation and the action is invertible. Now, $11 \geq n$ in each case, and it is relatively prime to the exponent of each group. So we need a number K such that $\exp \mathrm{SL}_n(q) \nmid K$ and $\exp \mathrm{GL}_l(q) \,|\, K$ for every $l < n$, and then $N = 11\,K$ will do. For $\mathrm{SL}_6(2)$ we can choose $K = 26040$, for $\mathrm{SL}_3(4)$ we can choose $K = 30$ and for $\mathrm{SL}_2(8)$ we can choose $K = 7$. □

We are able to prove Theorem 2.

Proof of Theorem 2 . For $M_2(\mathbb{Z}_2)$ and $M_2(\mathbb{Z}_3)$ the theorem was proved in [8, 9]. Assume $n > 2$ or $q > 3$. We reduce the equivalence problem of $M_n(\mathbb{F})$ to graph k-coloring where $k = |\mathrm{PSL}_n(q)|$. Let Γ be a graph. By Lemma 4 there is a group term s (of polynomial length in the size of Γ) such that $s \approx \mathrm{id}$ over $\mathrm{GL}_n(q)$ if and only if Γ is not k-colorable and if $s \not\approx \mathrm{id}$ then $s(\mathrm{GL}_n(q)) = \mathrm{SL}_n(q)$. Let us substitute $x^{|\mathrm{GL}_n(q)|-1}$ for every occurrence of the inverse of the variable x to obtain a semigroup word t. The terms t and s are equivalent over the (semi)group $\mathrm{GL}_n(q)$. The length of t is at most $(|\mathrm{GL}_n(q)| - 1)$-times the length of s, hence polynomial in the size of Γ. Let N be the integer chosen in Lemma 6. We claim that $t \approx \mathrm{id}$ over the (semi)group $\mathrm{GL}_n(q)$ if and only if $t^{2N} \approx t^N$ over the semigroup $M_n(q)$. For a non-invertible matrix A the identity $A^N = A^{2N}$ holds by assumption, hence $t^{2N} \approx t^N$ over $M_n(q)$ if and only if $t^{2N} \approx t^N$ over $\mathrm{GL}_n(q)$. If $t \approx \mathrm{id}$, then $t^{2N} \approx t^N$ obviously holds. Let us assume that $t \not\approx \mathrm{id}$. Then $t(\mathrm{GL}_n(q)) = \mathrm{SL}_n(q)$ and by Lemma 6 there is an $A \in \mathrm{SL}_n(q)$, such that $A^N \neq \mathrm{id}$, hence $t^{2N} \not\approx t^N$. Thus $t \approx \mathrm{id}$ if and only if Γ is k-colorable, and the equivalence problem for the semigroup $M_n(q)$ is coNP-complete. □

Note that in the proof we used the coNP-completenes of the equivalence problem for the monoid $\mathrm{GL}_n(q)$. In case of a finite group the monoid and group versions of the equivalence problem have the same complexity. In case of a group of size n any occurrence of x^{-1} can be substituted by x^{n-1}. The coNP-complete part of Theorem 2 also follows from [1], where the so-called implicite group operator is used to establish connection between identities over semigroups and identities over their subgroups.

3. The Equivalence Problem for Rings

Lemma 7. *Let $M_{n_1}(q_1), \ldots, M_{n_m}(q_m)$ be matrix rings, where $q_i = p^{\alpha_i}$ for a fixed prime p. Let $\alpha = \max\{n_i\alpha_i\}$. Then there exists a polynomial $f(x)$ over the p-element field $\mathbb{F}_p$ such that for every i and every non-invertible matrix $A \in M_{n_i}(q_i)$ the equation $f(A) = 0$ holds. Moreover, $f(\mathrm{id}) = 0$ holds. Furthermore, if $n_j\alpha_j = \alpha$, then there exists a matrix $B \in \mathrm{SL}_{n_j}(q_j)$ such that $f(B) \in \mathrm{GL}_{n_j}(q_j)$.*

Proof. Consider a $\delta \in \mathbb{F}_{p^\alpha}$ such that the degree of δ is α over $\mathbb{F}_p$ and the norm of δ is 1 over $\mathbb{F}_{q_j}$. Such an element exists, e.g. if $\mathbb{F}^*_{p^\alpha} = \langle h \rangle$, then $\delta = h^{1-q_j}$ will do. Let $m(x)$ be the minimal polynomial of δ over $\mathbb{F}_p$. Let $B \in M_{n_j}(q_j)$ be a matrix with minimal polynomial $m(x)$ over $\mathbb{F}_p$. Since m splits over $\mathbb{F}_{q_j}$ to a product of α_j-many polynomials of degree n_j, the matrix $B \in M_{n_j}(q_j)$ suffices if its minimal polynomial over $\mathbb{F}_{q_j}$ is one of the factors of m. Note that $B \in \mathrm{SL}_{n_j}(q_j)$, because $\det B$ is the norm of δ. Let $g(x)$ be the least common multiple of all $\mathbb{F}_p$-polynomials of degree at most α which are irreducible over $\mathbb{F}_p$, and let $f(x) = g(x)/(m(x))$.

Now $(m(x), f(x)) = 1$, hence none of the eigenvalues of $f(B)$ is 0. Therefore $f(B) \in \mathrm{GL}_{n_j}(q_j)$.

Let $A \in M_{n_i}(q_i)$ for some i and let $m_A(x) \neq m(x)$ be its minimal polynomial over $\mathbb{F}_p$. The degree of $m_A(x)$ is at most α, hence $m_A(x) \,|\, f(x)$ and $f(A) = 0$. In particular if A is not invertible or A is the identity matrix then $m_A(x) \neq m(x)$, thus $f(A) = 0$ as we wanted. □

Now we are able to prove of our main theorem.

Proof of Theorem 1. Let d denote the least integer such that $J(R)^d = 0$ and let $R/J(R) = M_{n_1}(q_1) \oplus M_{n_2}(q_2) \oplus \cdots \oplus M_{n_l}(q_l)$. Assume first that $n_i > 2$ or $q_i > 3$ for some i. By reindexing we may assume that $n_1 > 2$ or $q_1 > 3$. Let $q_1 = p^{\alpha_1}$. By reindexing we may assume that $M_{n_1}(q_1)$, $M_{n_2}(q_2)$, $M_{n_m}(q_m)$ are those matrix rings in the product, where $q_i = p^{\alpha_i}$ for some α_i. Let Γ be a graph with at least nine edges, and let s be the term constructed in Lemma 4(2) for the graph Γ and for the groups $\mathrm{GL}_{n_1}(q_1), \ldots, \mathrm{GL}_{n_m}(q_m)$. Let $k = \max_{1 \leq i \leq m}\{|\mathrm{PSL}n_i(p^{\alpha_i})|\}$. Let $f(x)$ be the polynomial from Lemma 7 for $M_{n_1}(q_1), \ldots, M_{n_m}(q_m)$ and let $\alpha = \max\{n_i\alpha_i \,|\, i = 1, 2, \ldots, m\}$. Finally, let P be the product of all primes p_i not equal to p, where there is a q_i such that $q_i = p_i^{\alpha_i}$.

Then

(i) $P \cdot M_{n_i}(q_i) = \begin{cases} M_{n_i}(q_i) & \text{if } q_i = p^{\alpha_i}, \\ 0 & \text{otherwise;} \end{cases}$

(ii) $s(\mathrm{GL}_{n_i}(q_i)) = \begin{cases} \mathrm{SL}_{n_i}(q_i) & \text{if } \Gamma \text{ is } k\text{-colorable and } \alpha = n_i\alpha_i, \\ \mathrm{id} & \text{otherwise;} \end{cases}$

(iii) $f(A) = 0$ if $\alpha \neq n_i\alpha_i$;

(iv) if $\alpha = n_i\alpha_i$, then $f(A) \in \mathrm{SL}_{n_i}(q_i)$ for some $A \in \mathrm{SL}_{n_i}(q_i)$.

Here, $Px = x + x + \cdots + x$, the addition is iterated P times.

We reduce the graph k-coloring to the equivalence problem for sum of monomials over R. For a graph Γ with at least nine edges, let us consider the polynomial $(P \cdot f(s))^d$ written as sum of monomials. We claim that $R \models (P \cdot f(s))^d \approx 0$ if and only if Γ is not k-colorable.

To this end, we prove that $P \cdot f(s) \approx 0$ over $R/J(R)$ if and only if Γ is not k-colorable. We check this identity coordinatewise. If $q_i \neq p^\beta$ for some β, then multiplying by P annihilates the ith coordinate. For $q = p^{\alpha_i}$ if Γ is not k-colorable, then $s(\mathrm{GL}_{n_i}(q_i)) = \mathrm{id}$ for every i and every other value of s is not invertible. Thus $f(s(M_{n_i}(q_i))) = 0$ for every i, which yields $R \models (P \cdot f(s))^d \approx 0$.

If Γ is k-colorable, then $s(\mathrm{GL}_{n_i}(q_i)) = \mathrm{SL}_{n_i}(q_i)$ for some i and thus $f(s(M_{n_i}(q_i)))$ attains at least one invertible element from $\mathrm{GL}_{n_i}(q_i)$ for some i. Hence $P \cdot f(s)$ attains an element C, which is invertible in coordinate i. Then $(P \cdot f(s))^d$ attains C^d as value, which is invertible in coordinate i of $R/J(R)$, therefore $R \models (P \cdot f(s))^d \approx 0$ fails.

The length of s is polynomial in the size of Γ. The length of $f(x)$ and the integers P, d depend only on R. Thus the length of the term is polynomial in the size of Γ, when expanded as a sum of monomials.

Similarly, if $\max n_i = 2$ and $\max q_i = 3$, then we can polynomially reduce the equivalence problem over the semigroup $M_2(3)$ to the equivalence problem for sum of monomials over R. For any two semigroup polynomials f_1, f_2 over $M_2(3)$ and for variables y, z occurring neither in f_1 nor in f_2 consider the polynomial $(2y(f_1 - f_2)z)^d$. We claim that $M_2(3) \models f_1 \approx f_2$ if and only if $R \models (2y(f_1 - f_2)z)^d \approx 0$. If $M_2(3) \models f_1 \approx f_2$, then $M_2(3) \models 2y(f_1 - f_2)z \approx 0$ and $M_2(2) \models 2y(f_1 - f_2)z$. Thus $R/J(R) \models 2y(f_1 - f_2)z$, and $R \models (2y(f_1 - f_2)z)^d \approx 0$. Conversely, if $M_2(3) \models f_1 \approx f_2$ fails, then $f_1 - f_2$ attains a non-zero value from $M_2(3)$. Thus $2y(f_1 - f_2)z$ attains a matrix $C \in M_2(3)$ which has a non-zero eigenvalue. Therefore $(2y(f_1 - f_2)z)^d$ attains a value in R which has $C^d \neq 0$ in the $M_2(3)$ coordinate of $R/J(R)$, and $R \models (2y(f_1 - f_2)z)^d \approx 0$ fails. The length of $(2y(f_1 - f_2)z)^d$ is polynomial in the length of f_1 and f_2, when expanded as sum of monomials, as d depends only on R.

Finally, the case $\max n_i = 2$ and $\max q_i = 2$ can be handled similarly: for any two semigroup polynomials f_1, f_2 over $M_2(2)$ and for variables y, z occurring neither in f_1 nor in f_2 one needs to consider the polynomial $(y(f_1 - f_2)z)^d$. □

Acknowledgment

The research of the authors was supported by OTKA grants K67870 and K100246.

References

[1] J. Almeida, M. V. Volkov and S. V. Goldberg, Complexity of the identity checking problem for finite semigroups, *Notes of Scientific Seminars of the St Petersburg*, Vol. 358, Department of the Steklov Mathematical Institute, Russian Academy of Sciences, (2008), pp. 5–22 [in Russian].

[2] S. Burris and J. Lawrence, The equivalence problem for finite rings, *J. Symbolic Comput.* **15** (1993) 67–71.

[3] S. Burris and J. Lawrence, Results on the equivalence problem for finite groups, *Algebra Universalis* **52**(4) (2004) 495–500.

[4] G. Horváth, The complexity of the equivalence problem over finite rings, Manuscript, 2010.

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

[6] G. Horváth, J. Lawrence and R. Willard, The sigma equivalence problem over commutative finite rings, Manuscript, 2010.

[7] H. Hunt and R. Stearns, The complexity for equivalence for commutative rings, *J. Symbolic Comput.* **10** (1990) 411–436.

[8] Cs. Szabó and V. Vértesi, The complexity of the checking identities for finite matrix rings, *Algebra Universalis* **51** (2004) 439–445.

[9] Cs. Szabó and V. Vértesi, The complexity of the word-problem for finite matrix rings, *Proc. Amer. Math. Soc.* **132** (2004) 3689–3695.

[10] K. Zsigmondy, Zur Theorie der Potenzreste, *Monatsh. Math. Phys.* **3**(1) (1892) 265–284 [in German].