

THE COMPLEXITY OF THE WORD-PROBLEM FOR FINITE MATRIX RINGS

CSABA SZABÓ AND VERA VÉRTESI

(Communicated by Lance W. Small)

ABSTRACT. We analyze the so-called word-problem for $M_2(Z_2)$, the ring of 2×2 matrices over Z_2 . We prove that the term-equivalence problem for the semigroup (and so for the ring) $M_2(Z_2)$ is coNP-complete.

1. INTRODUCTION

In this paper we study the computational complexity of the word-problem for $M_2(Z_2)$. We shall use the standard notation for computational complexity, as P, NP, coNP, etc.

The word-problem for an algebra \mathcal{A} has two different versions for terms and for polynomials. We call an expression *term* if it contains only variables and we call it *polynomial* if it may contain elements of \mathcal{A} . The term-equivalence problem over \mathcal{A} (TERM-EQ \mathcal{A}) asks whether two given terms agree for every substitution. For example x^6 and id are terms over the group S_3 , and they are equivalent because the exponent of S_3 is 6. The polynomial-equivalence problem (POL-EQ \mathcal{A}) asks the same for polynomials, for example $x(1, 2)yx^2(1, 2, 3)$ and x^2y are polynomials over the group S_3 , but they are not equivalent, e.g. by substituting $x = y = id$ the two values are not equal. Here $(1, 2)$ denotes the transposition flipping 1 and 2 and $(1, 2, 3)$ denotes the 3-cycle mapping 1 to 2, 2 to 3 and 3 to 1.

Let TERM-SAT \mathcal{A} and POL-SAT \mathcal{A} denote the term- and polynomial-satisfiability problems, respectively. The instance of TERM-SAT (POL-SAT) is a term (polynomial) t and an element $a \in \mathcal{A}$. The question is whether there is an evaluation of t such that $t = a$. Observe that for any finite algebra, TERM-EQ and POL-EQ are both in coNP and TERM-SAT (POL-SAT) is in NP.

2. PRELIMINARIES

We present a few recent results for some algebraic structures.

It is already known [3] that for a commutative ring \mathcal{R} the TERM-EQ problem is in P if \mathcal{R} is nilpotent and coNP-complete otherwise. Burris and Lawrence proved in [2] that the same holds for rings in general. Following their proof it is easy to see that for a nilpotent ring \mathcal{R} the problem POL-EQ \mathcal{R} is in P. A straightforward

Received by the editors September 5, 2002 and, in revised form, July 24, 2003.
2000 *Mathematics Subject Classification*. Primary 68Q17, 03C13.
Key words and phrases. 0-simple semigroup, term, complexity.

consequence of their result is that if the ring is not nilpotent, then POL-EQ \mathcal{R} is coNP-complete.

So, for example, for the ring Z_2 , the coNP-completeness of TERM-EQ Z_2 is an easy consequence of the NP-completeness of 3-SAT. But the proof uses high powers of sums. This is the reason why Willard and Lawrence introduced the Σ version of the problems, where every polynomial is a sum of monomials, e.g. an expression of the form $(x+y)^n$ is too long when expanded. The TERM $_{\Sigma}$ -EQ (POL $_{\Sigma}$ -EQ) problem asks whether two terms (polynomials), p and q — that are sums of monomials — are equal at every substitution. They proved in [5] that

Theorem 1. *Let \mathcal{R} be a ring and $\mathbf{J}(\mathcal{R})$ denote its Jacobson radical.*

If $\mathcal{R}/\mathbf{J}(\mathcal{R})$ is commutative, then TERM $_{\Sigma}$ -EQ \mathcal{R} is in P.

If $\mathcal{R} = M_n(F)$ is a finite matrix ring whose invertible elements form a non-solvable group, then TERM $_{\Sigma}$ -EQ \mathcal{R} is coNP-complete. That is, if $n \geq 3$ or $|F| \geq 4$, then TERM $_{\Sigma}$ -EQ $M_n(F)$ is coNP-complete.

They ask what happens for $n = 2$ and $|F| = 2, 3$ (see Problem 2 in [5]). We examine this question in Section 4.

The group case is only partially solved. An unpublished result of Lawrence and Burris is the following:

Theorem 2. *Let \mathcal{G} be a group. If \mathcal{G} is nilpotent, then TERM-EQ \mathcal{G} is in P. If \mathcal{G} is non-solvable, then TERM-EQ \mathcal{G} is coNP-complete.*

The answer for semigroups is less complete. In [1] the authors show for a special class of aperiodic monoids that the POL-EQ problem is tractable. In [7] the authors prove that

Theorem 3. *POL-EQ $M_n(F)$ and POL-SAT $M_n(F)$ are coNP-complete.*

It is also shown that

Theorem 4. *Let S be a combinatorial 0-simple semigroup. Then POL-EQ S , POL-SAT S , TERM-EQ S , and TERM-SAT S are in P.*

In [6] V. Yu. Popov and M. V. Volkov exhibit a semigroup of size $\leq 2^{1700}$ with a coNP-complete TERM-EQ problem. Later Kisieliewicz in [4] presented an example of size a few hundred. In this paper we investigate the word-problem for the matrix semigroup $M_2(Z_2)$. We prove in Section 4 that

Theorem 5. *TERM-EQ is coNP-complete for the semigroup $M_2(Z_2)$.*

This result not only provides a 16 element example of a semigroup with coNP-complete word problem that is significantly smaller than the previously known examples, but also, as an easy corollary we get that the TERM $_{\Sigma}$ -EQ is coNP-complete for the matrix ring as well. Moreover, following the idea of the proof we exhibit an example of a semigroup of size 13 with a coNP-complete word problem.

3. COMBINATORIAL COMPLETELY 0-SIMPLE SEMIGROUPS

We give a description of combinatorial completely 0-simple semigroups. Let M be a 0-1 matrix such that each row and column contains at least one 1 entry. We define $S = S_M$, the completely 0-simple semigroup belonging to the regular matrix M . Let Λ and I denote the index set for the rows and columns of M . The

underlying set of S consists of all pairs of the form $\langle i, \lambda \rangle$ where $i \in I$, and $\lambda \in \Lambda$, along with 0. An associative multiplication is given by the following rule:

$$\langle i, \lambda \rangle \langle j, \mu \rangle = \begin{cases} \langle i, \mu \rangle & \text{if } M(\lambda, j) = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Note, that for $a \in S_M$, $a^2 = a$ or 0 according to the matrix M , and for every case $a^2 = a^3 = a^4 = \dots$.

Example 6. Let

$$A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix},$$

where $\Lambda = I = \{1, 2, 3\}$. Then $\langle 1, 2 \rangle \langle 3, 1 \rangle = \langle 1, 1 \rangle$ as $A(2, 3) = 1$ and $\langle 1, 2 \rangle \langle 2, 1 \rangle = 0$ as $A(2, 2) = 0$. In S_A the product $\langle i, \lambda \rangle \langle j, \mu \rangle = 0$ if and only if $\lambda \neq j$.

Note that the completely 0-simple semigroups are also called Rees-matrix semigroups. We continue with an observation:

Lemma 7. Let $S = S_M$ be a combinatorial Rees-matrix semigroup with elements $a_1, \dots, a_n \in S$, where $a_j = \langle i_j, \lambda_j \rangle$ for $1 \leq j \leq n$.

- (1) $a_1 \cdots a_n = 0$ if and only if there exists a k , $1 < k \leq n$, such that $a_{k-1}a_k = 0$.
- (2) If $a_1 \cdots a_n \neq 0$, then $a_1 \cdots a_n = \langle i_1, \lambda_1 \rangle \cdots \langle i_n, \lambda_n \rangle = \langle i_1, \lambda_n \rangle$.

4. THE SEMIGROUP $M_2(Z_2)$

We split the semigroup $M_2(Z_2)$ into two parts: the group of invertible matrices and the multiplicative semigroup of the 10 singular matrices.

The group of invertible matrices is isomorphic to the symmetric group S_3 . An isomorphism is given by simply the action of the matrix on the 3 nonzero vectors of the vectorspace Z_2^2 : $\begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}$:

$$\begin{matrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \rightarrow id & \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \rightarrow (1, 3) & \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \rightarrow (2, 3) \\ \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \rightarrow (1, 2, 3) & \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \rightarrow (1, 3, 2) & \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \rightarrow (1, 2). \end{matrix}$$

The semigroup of singular matrices (L) is isomorphic to the combinatorial 0-simple semigroup S_A , where A was defined in Example 6. Indeed, let $v_1 = u_2 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $v_2 = u_1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, $v_3 = u_3 = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \in Z_2^2$.

Let us define the map ϕ from the semigroup of singular matrices in $M_2(Z_2)$ to S_A in the following way:

$$\phi(v_i \cdot u_\lambda^T) = \langle i, \lambda \rangle \text{ and } \phi\left(\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\right) = 0.$$

Here, $u_\lambda^T \cdot v_j = \begin{cases} 0 & \text{if } \lambda = j \\ 1 & \text{if } \lambda \neq j. \end{cases}$ Hence

$$(v_i \cdot u_\lambda^T) \cdot (v_j \cdot u_\mu^T) = v_i \cdot (u_\lambda^T \cdot v_j) \cdot u_\mu^T = \begin{cases} v_i \cdot u_\mu^T & \text{if } u_\lambda^T \cdot v_j = 1, \\ 0 & \text{if } u_\lambda^T \cdot v_j = 0. \end{cases}$$

This verifies that ϕ is an isomorphism between the multiplicative semigroup of singular matrices of $M_2(Z_2)$ and S_A . These two isomorphisms extend a map between $M_2(Z_2)$ and $S_3 \cup S_A$ that is an isomorphism where the multiplication between the elements of S_3 and S_A is defined as follows. For $\pi \in S_3$ and $\langle i, j \rangle \in S_A$ let

$$\langle i, \lambda \rangle \pi = \langle i, \pi(\lambda) \rangle \quad \text{and} \quad \pi \langle i, \lambda \rangle = \langle \pi^{-1}(i), \lambda \rangle.$$

It is easy to see that

Lemma 8. *Let $m_1, \dots, m_n \in M_2(Z_2) = S_3 \cup S_A$, $\langle i, \lambda \rangle, \langle j, \mu \rangle \in S_A$ and $\pi \in S_3$.*

- (1) $m_1 \cdots m_n \in S_A$ if and only if there exists a k for which $m_k \in S_A$, i.e. a product is in S_A if and only if at least one of the factors is in S_A .
- (2) $\langle i, \lambda \rangle \pi \langle j, \mu \rangle = 0$ if and only if $\pi(\lambda) = j$.

We shall need the analogue of Lemma 7.

Lemma 9. *Let $a_1, \dots, a_n \in S_A$ where $a_j = \langle i_j, \lambda_j \rangle$ for $1 \leq j \leq n$ and $\pi_1, \pi_2, \dots, \pi_{n+1} \in S_3$. Then*

- (1) $\pi_1 a_1 \pi_2 a_2 \cdots \pi_n a_n \pi_{n+1} = 0$ if and only if there exists k , $1 < k \leq n$, such that $a_{k-1} \pi_k a_k = 0$ (i.e. $\pi_k(\lambda_{k-1}) = i_k$).
- (2) If $\pi_1 a_1 \pi_2 a_2 \cdots \pi_n a_n \pi_{n+1} \neq 0$, then

$$\pi_1 a_1 \pi_2 a_2 \cdots \pi_n a_n \pi_{n+1} = \langle \pi_1^{-1}(i_1), \pi_{n+1}(\lambda_n) \rangle.$$

Now, we prove Theorem 5.

Proof of Theorem 5. For every simple graph we exhibit two terms over $M_2(Z_2)$, whose lengths are polynomial in the size of the graph, such that the graph is not 6-colorable if and only if the two terms are equivalent. Thus, we reduce the graph 6-coloring problem into TERM-EQ $M_2(Z_2)$. Let $\Gamma = \Gamma(V, E)$ be a simple graph (with no loops and double edges). Notice that any possible isolated vertex can be ignored, so we can assume that the graph does not contain isolated vertices. For every vertex $j \in V$ we introduce a vertex-variable v_j and for every edge $i \in E$ we introduce an edge-variable e_i . We define a few terms. Let

$$\begin{aligned} P &= \prod_{i \in E} (xw_i^4)^6, \\ Q &= \prod_{i \in E} (xw_i^3)^6, \\ H &= \prod_{(i,j) \in E^2} (w_i w_j w_i w_j^2 w_i^2)^6. \end{aligned}$$

Here

$$w_i = e_i^5 v_j v_k^5 e_i v_k v_j^5,$$

where i is the edge connecting the vertices j and k . The arguments will neither depend on the order of v_j and v_k in the definition of w_i nor on the order in which the product defining H is arranged. The products P and Q are running through the edges of Γ in the same order. Finally, let

$$\begin{aligned} p &= PPPxH, \\ q &= PQPxH. \end{aligned}$$

We claim that $p \equiv q$ if and only if Γ is not 6-colorable.

For this, first we analyze the expression $w_i = e_i^5 v_j v_k^5 e_i v_k v_j^5$. If the variables e_i, v_j, v_k are all from the group S_3 , then $w_i = e_i^{-1} v_j v_k^{-1} e_i v_k v_j^{-1} = [e_i, v_k v_j^{-1}]$, that is, the commutator of the group elements e_i and $v_k v_j^{-1}$. In S_3 the commutator subgroup is $A_3 = \{id, (1, 2, 3), (1, 3, 2)\}$. Since the centre of S_3 is trivial, we have the following.

Lemma 10. Fix $i = \{j, k\} \in E$. Let us assume $v_j, v_k, e_i, a \in S_3$ and put $w_i = [e_i, v_k v_j^{-1}]$. Then

- (1) $a^6 = id$;
- (2) $w_i \in A_3$, the commutator subgroup of S_3 ;
- (3) $w_i^3 = id$;
- (4) $w_i^4 = w_i$;
- (5) w_i stabilizes 1 if and only if $w_i = id$.
- (6) For $u, v \in S_3$ there is an $e \in S_3$ such that $w = [e, uv^{-1}] \neq id$, if and only if $uv^{-1} \neq id$, that is, if and only if $u \neq v$.
- (7) If $w_i \in S_3 \setminus \{id\}$, then the set $\{w_i, w_i^2, id\}$ is transitive on $\{1, 2, 3\}$.
- (8) If $w_i \in S_3 \setminus \{id\}$, and $s \in S_A$, then $sw_i s w_i^2 s^2 = 0$.

Note that there exists at least one edge or vertex variable taking a value from S_A if and only if there exists at least one word w_i such that the value of w_i is in S_A .

We will distinguish some cases that are described in Table 1.

TABLE 1. The four different cases

		$x \in S_3$	$\langle i, \lambda \rangle = x \in S_A$	
			$i \neq \lambda$	$i = \lambda$
$\exists w_j \in S_A$	$\exists w_i \in S_3 \setminus \{id\}$	Case 2 $p = q = 0$		
	$w_i \notin S_A \Rightarrow w_i = id$	Case 3 $P = Q$ hence $p = q$		
$\forall w_j \in S_3$		Case 1 $p = q = x$	Case 4a $q = P^2 x = P^3 x = p$	Case 4b 6-coloring

In the following we will show that except for Case 4b p is always equivalent to q .
Case 1: When all variables are in S_3 . If all variables are from S_3 , then $(xw_i^k)^6 = id$ for every edge and $(w_i w_j w_i w_j^2 w_i^2)^6 = id$ for every pair of edges, hence both terms are equal to x .

Case 2: When there exists $w_j \in S_A$ and there is an i such that $w_i \in S_3 \setminus \{id\}$. The last item of Lemma 10 says the following: If there is an edge j , such that $w_j \in S_3 \setminus \{id\}$ and at least one $w_j \in S_A$, then $H = 0$, and so $p = q = 0$.

Case 3: When there exists $w_j \in S_A$ and besides $w_i \in S_A \cup \{id\}$ for every $i \in E$. In both cases $w_i^4 = w_i^3 = w_i^2$, hence the two terms are equal.

Case 4: When $w_i \in S_3$ for every $i \in E$ and $x \in S_A$.

- a) First, let $x = \langle i, \lambda \rangle$, where $i \neq \lambda$. In this case by item 3 of Lemma 10 $H^3 = id$ and so either $P = 0$ or both sides are equal to x , hence the equation is obvious.

b) Finally, without loss of generality, we may assume that $x = \langle 1, 1 \rangle$. Now, $p = PPPx$ and $q = PQPx$ and — because of item 3 of Lemma 10 — $Q = \langle 1, 1 \rangle^k = 0$, where $k \geq 2$, hence $q = 0$. Thus $p \neq q$ if and only if there is a substitution, where $p = PPPx \neq 0$, by item 4 of Lemma 10 that holds if and only if $xw_1xw_2x \cdots w_kx \neq 0$. By Lemmas 8 and 9 we get that it is true if and only if none of the w_i -s stabilize 1, which is by item 5 of Lemma 10 equivalent to $w_i \neq id$. Recall that $w_i = e_i^{-1}v_jv_k^{-1}e_iv_kv_j^{-1} = [e_i, v_kv_j^{-1}]$, where e_i is the edge variable and v_k and v_j are the elements assigned to the endpoints of e_i . According to item 6 of Lemma 10 we can choose an $e_i \in S_3$ such that $w_i \neq id$ if and only if $v_k \neq v_j$, that is, if and only if the group elements assigned to the neighbor vertices are distinct, that is, if and only if Γ is 6-colorable. □

Corollary 11. TERM-EQ and TERM_{Σ} -EQ are coNP-complete for the ring $M_2(Z_2)$.

Theorem 12. There exists a 13 element semigroup T for which the TERM-EQ problem is coNP-complete.

Proof. Namely, let $T = A_3 \cup S_A$ be a subsemigroup of $M_2(Z_2)$. The proof is based on the same idea as the case of $M_2(Z_2)$: for an arbitrary simple graph Γ with no isolated vertices we define the same polynomials as we did in the case of $M_2(Z_2)$ with the difference that here we let $w_i = v_jv_k^{-1}$. We will prove that $p \neq q$ if and only if Γ is 3-colorable. We can claim a similar statement to Lemma 10.

Lemma 13. Let us assume that $w_i \in A_3$.

- (1) $w_i^3 = id$;
- (2) $w_i^4 = w_i$;
- (3) w_i stabilizes 1 if and only if $w_i = id$, i.e. $v_j \neq v_k$.
- (4) If $w_i \in A_3 \setminus \{id\}$, then the set $\{w_i, w_i^2, id\}$ is transitive on $\{1, 2, 3\}$.
- (5) If $w_i \in A_3 \setminus \{id\}$, and $s \in S_A$, then $sw_i s w_i^2 s^2 = 0$.

Accordingly, we can distinguish the same cases and in these cases except for Case 4b the proof is word-by-word the same as for $M_2(Z_2)$. For Case 4b again we may assume without loss of generality that $x = \langle 1, 1 \rangle$. Here by item 1 of Lemma 13, $q = 0$. $p = PPPx \neq q = 0$ holds if and only if $xw_1xw_2x \cdots w_kx \neq 0$. This is true if and only if none of the w_i -s stabilize 1, which is by item 3 of Lemma 13 equivalent to $v_j \neq v_k$, that is, if and only if the group elements assigned to the neighboring vertices are distinct, that is, if and only if Γ is 3-colorable. □

5. FURTHER REMARKS

At this point the following two problems arise.

Problem 1. Find the smallest semigroup for which the TERM-EQ is coNP-complete.

Problem 2. Find the computational complexity of TERM-EQ for the semigroup $M_n(F)$.

However, it is not clear from the final version of the paper. During the proof we had the following interesting problem, which is the generalization of EQN* in some sense.

Problem 3. Given two sets of words $\{w_1, w_2, \dots, w_n\}$ and $\{v_1, v_2, \dots, v_m\}$ over $G \leq S_k$, the symmetric group acting on the set $\Omega = \{1, 2, \dots, k\}$. For an evaluation of the variables and for $l \in \Omega$ let $I_l = \{w_1(l), w_2(l), \dots, w_n(l)\}$ and $J_l = \{v_1(l), v_2(l), \dots, v_m(l)\}$. Find the complexity of the question whether the set-equation system $I_1 = J_1, I_2 = J_2, \dots, I_k = J_k$ holds for every evaluation.

If $n = m = 1$, then we get the word-problem for the fixed permutation group.

ACKNOWLEDGEMENTS

The research of the authors was supported by the Hungarian National Foundation for Scientific Research, Grant F32325, T043671 and T038059.

REFERENCES

1. D. M. Barrington, P. McKenzie, C. Moore, P. Tesson, and D. Thérien, *Equation satisfiability and program satisfiability for finite monoids*, Math. Found. Comp. Sci. (2000, Bratislava), 127–181. MR 1844742 (2002f:68053)
2. S. Burris and J. Lawrence, *The equivalence problem for finite rings*, Journal of Symbolic Computation **15** (1993), 67–71. MR 1210448 (94c:16030)
3. H. Hunt and R. Stearns, *The complexity for equivalence for commutative rings*, Journal of Symbolic Computation **10** (1990), 411–436. MR 1087713 (92g:68062)
4. A. Kisieliewicz, personal communication, 2002.
5. J. Lawrence and R. Willard, *The complexity of solving polynomial equations over finite rings*, manuscript, 1997.
6. V. Yu. Popov and M. V. Volkov, *Complexity of checking identities and quasi-identities in finite semigroups*, Journal of Symbolic logic (to appear).
7. S. Seif and Cs. Szabó, *The computational complexity of checking identities in simple semigroups and matrix semigroups over finite fields*, Semigroup Forum (to appear 2002).

DEPARTMENT OF ALGEBRA AND NUMBER THEORY, EÖTVÖS LORÁND UNIVERSITY, 1117 BUDAPEST, PÁZMÁNY PÉTER SÉTÁNY 1/C, HUNGARY
E-mail address: csaba@cs.elte.hu

DEPARTMENT OF ALGEBRA AND NUMBER THEORY, EÖTVÖS LORÁND UNIVERSITY, 1117 BUDAPEST, PÁZMÁNY PÉTER SÉTÁNY 1/C, HUNGARY
E-mail address: wera13@cs.elte.hu