THE COMPLEXITY OF THE WORD-PROBLEM FOR
FINITE MATRIX RINGS

CSABA SZABÓ AND VERA VÉRTESI

Abstract. We analyze the so called word-problem for $M_2(Z_2)$, the ring of $2 \times 2$ 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 notations 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 $x(1,2)y x^2(1,2,3)$ 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 TERM-EQ and POL-EQ are both in coNP and TERM-SAT (POL-SAT) is in NP.
2. Preliminaries

2.1. Rings. It has been already known [4] that for a commutative ring \( R \) the TERM-EQ problem is in \( P \) if \( R \) 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 \( R \) the problem POL-EQ\( R \) is in \( P \). A straightforward consequence of their result is that if the ring is not nilpotent, then POL-EQ\( R \) 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 \( \Sigma \) 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 [6] that

\begin{align*}
\text{Theorem 1.} & \quad \text{Let } R \text{ be a ring and } J(R) \text{ denote its Jacobson radical. If } R/J(R) \text{ is commutative, then } \text{TERM-EQ } R \text{ is in } P. \\
& \quad \text{If } R = M_n(F) \text{ is a finite matrix ring whose invertible elements form a non-solvable group, then } \text{TERM}_{\Sigma}\text{-EQ } R \text{ is coNP-complete. That is if } n \geq 3 \text{ or } |F| \geq 4, \text{ then } \text{TERM}_{\Sigma}\text{-EQ } M_n(F) \text{ is coNP-complete.}
\end{align*}

They ask, what happens for \( n = 2 \) and \( |F| = 2, 3 \) (see Problem 2 in [6]). We examine this question in Section 4.

2.2. Groups. The group case is only partially solved.

An unpublished result of Lawrence and Burris is the following:

\begin{align*}
\text{Theorem 2.} & \quad \text{Let } G \text{ be a group. If } G \text{ is nilpotent, then } \text{TERM-EQ } G \text{ is in } P. \text{ If } G \text{ is non-solvable, then } \text{TERM-EQ } G \text{ is coNP-complete.}
\end{align*}

For example \( A_5 \), the 60 element alternating group on 5 letters has a coNP-complete TERM-EQ problem. They also showed that the problem is in \( P \) for the dihedral groups.

As a generalization of the TERM-SAT (POL-SAT) problem-field in [3] the authors defined the term-system satisfaction problem (EQN\( ^* \)). The input of this problem are some terms \( t_1, t_2, \ldots, t_n \) and some constants \( a_1, a_2, \ldots, a_n \) and the question is whether there exists a substitution for which the evaluated terms are equal to the constants, respectively (i.e. are there any solution for the \( t_1 = a_1, t_2 = a_2, \ldots, t_n = a_n \) system of equations). In [3] it is proved that
Theorem 3. For finite Abelian groups $EQ^*$ is in P. For finite non-Abelian groups $EQ^*$ is NP-complete.

2.3. Semigroups. 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. What they really do is that they investigate the equation satisfiability problem. The authors study the POL-SAT problem and their results naturally apply to the POL-EQ problem. For combinatorial 0-simple semigroups it is shown in [8] that for every bipartite graph $\Gamma$ there is a semigroup $S$ such that POL-EQ $S$ and RET $\Gamma$ are polynomially equivalent. As a corollary, it is shown that POL-EQ $M_2(Z_2)$ is coNP-complete. In [9] they proved that

Theorem 4. POL-EQ $M_n(F)$ and POL-SAT $M_n(F)$ are coNP-complete.

It is also shown that

Theorem 5. 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 [7] the authors exhibit a semigroup of size $\leq 2^{1700}$ with a coNP-complete TERM-EQ problem. Later Kisieliewicz in [5] presented an example of a few hundred size. In this paper we investigate the word-problem for the matrix ring $M_2(Z_2)$. We prove in Section 4 that

Theorem 6. TERM-EQ is coNP-complete for the semigroup $M_2(Z_2)$.

This result does not only provide a 16 element example of a semigroup with coNP-complete word problem, that is significantly smaller then 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 $\Lambda$ 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 \( a^2 = a^3 = a^4 = \ldots \).

**Example 7.** 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 \( \lambda = j \).

It is easy to see that the possible expressions over \( S \) are of the form \( x_1 x_2 \cdots x_k \).

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

**Lemma 8.** Let \( S = S_M \) be a combinatorical Rees-matrix semigroup with elements \( a_1, \ldots, a_n \in S \), 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 vector of the vectorspace \( Z_2^3 \):

\[
\begin{align*}
\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} &\rightarrow id \\
\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} &\rightarrow (1, 3) \\
\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} &\rightarrow (2, 3)
\end{align*}
\]

\[
\begin{align*}
\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} &\rightarrow (1, 2, 3) \\
\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} &\rightarrow (1, 3, 2) \\
\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} &\rightarrow (1, 2).
\end{align*}
\]

The semigroup of singular matrices (\( L \)) is isomorphic to the combinatorical 0-simple semigroup \( S_A \), where \( A \) was defined in Example 7.

Indeed, let \( v_1 = u_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \), \( v_2 = u_1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \), \( v_3 = u_3 = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \in Z_2^2 \).

Let us define the map \( \phi : M_2(Z_2) \rightarrow S_A \) on the following way:
\[ \phi(v_i \cdot u_j^T) = \langle i, \lambda \rangle \text{ and } \phi \left( \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \right) = 0. \]

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 \( \phi \) 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 \( \langle i, j \rangle \in S_A \)

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

It is easy to see that

**Lemma 9.** Let \( m_1, \ldots, m_n \in M_2(Z_2) = S_3 \cup S_A, \langle i, \lambda \rangle, \langle j, \mu \rangle \in S_A \) 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 analogous of Lemma 8.

**Lemma 10.** Let \( a_1, \ldots, a_n \in S_A \) where \( a_j = \langle i_j, \lambda_j \rangle \) for \( 1 \leq j \leq n \) and \( \pi_1, \pi_2, \ldots, \pi_{n+1} \in S_3 \). 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 6.

**Proof of Theorem 6.** For every simple graph we exhibit two terms over \( M_2(Z_2) \), 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 \( \text{TERM-EQ } M_2(Z_2) \). Let \( \Gamma = (V, E) \) 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
\[ P = \prod_{i \in E}(xw_i^4)^6, \]
\[ Q = \prod_{i \in E}(xw_i^3)^6, \]
\[ H = \prod_{i,j \in E}(w_i w_j w_i^2 w_j^2)^6. \]

Here
\[ w_i = e_i^5 v_j^5 e_i v_k^5, \]
where \( i \) is the edge connecting the vertices \( j \) and \( k \). The products, \( P \) and \( Q \) are running through the edges of \( \Gamma \) in the same order. Finally, let
\[ p = PPP xH, \]
\[ q = PQP xH. \]

We claim that \( p \equiv q \) if and only if \( \Gamma \) is not 6-colorable.

For this, first we analyze the expression \( w_i = e_i^5 v_j^5 e_i v_k^5 \). If the variables \( e_i, v_j, v_k \) are all from the group \( S_3 \), then \( w_i = [e_i, v_k v_j^{-1}] \) that is the commutator of the group elements \( e_i \) and \( v_k v_j^{-1} \).

In \( S_3 \) the commutator subgroup is \( A_3 = \{\text{id}, (1, 2, 3), (1, 3, 2)\} \). As the centre of \( S_3 \) is trivial, we have the following

**Lemma 11.** Let us assume that \( w_i, a \in S_3 \).

1. \( a^6 = \text{id} \);
2. \( w_i \in A_3 \), the commutator subgroup of \( S_3 \);
3. \( w_i^3 = \text{id} \);
4. \( w_i^4 = w_i \);
5. \( w_i \) stabilizes 1 if and only if \( w_i = \text{id} \).
6. For \( v_j, v_k \in S_3 \) there is an \( e_i \in S_3 \) such that \( w_i = [e_i, v_k v_j^{-1}] \neq \text{id} \), if and only if \( v_k v_j^{-1} \neq v_j \) that is if and only if \( v_i \neq v_j \).
7. If \( w_i \in S_3 \setminus \{\text{id}\} \), then the set \( \{w_i, w_i^2, \text{id}\} \) is transitive on \( \{1, 2, 3\} \).
8. If \( w_i \in S_3 \setminus \{\text{id}\} \), 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 is described in Table 1.

In the following we will show that except for Case 4b \( p \) is always equivalent to \( q \).
Table 1. The four different cases

<table>
<thead>
<tr>
<th>Case</th>
<th>Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Case 1</td>
<td>When all variables are in $S_3$. If all variables are from $S_3$, then $(xw_i^k)^6 = id$ for every edge and $(w_iw_jw_iw_j^2w_i^2)^6 = id$ for every pair of edges, hence both terms are equal to $x$.</td>
</tr>
<tr>
<td>Case 2</td>
<td>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 11 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 $H = 0$, so $p = q = 0$.</td>
</tr>
<tr>
<td>Case 3</td>
<td>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.</td>
</tr>
<tr>
<td>Case 4</td>
<td>When $w_i \in S_3$ for every $i \in E$ and $x \in S_A$.</td>
</tr>
<tr>
<td>Case 4a</td>
<td>First, let $x = \langle i, \lambda \rangle$, where $i \neq \lambda$. In this case by item 3 of Lemma 11 we obtain $q = P x \cdot id \cdot x \cdots id \cdot x P x H = PP x H = PPP x H = p$.</td>
</tr>
<tr>
<td>Case 4b</td>
<td>Finally, without loss of generality, we may assume that $x = \langle 1, 1 \rangle$. Now, $p = PPP x$ and $q = PQP x$ and — because of item 3 of Lemma 11 — $Q = \langle 1, 1 \rangle^k = 0$, where $k \geq 2$, hence $q = 0$. Thus $p \neq q$ if and only if there is a substitution, where $p = PPP x \neq 0$, by item 4 of Lemma 11 that holds if and only if $xw_i x w_2 x \cdots w_k x \neq 0$. By Lemma 9 and 10 we got that it is true if and only if none of the $w_i$-s stabilize 1 which is by item 5 of Lemma 11 equivalent to $w_i \neq id$. Recall that $w_i = e_i^{-1} v_j v_k^{-1} e_i v_k v_j^{-1} = [e_i, v_k v_j^{-1}]$, 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 11 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 $\Gamma$ is 6-colorable.</td>
</tr>
</tbody>
</table>
Corollary 12. TERM-EQ and TERM$_2$-EQ are coNP-complete for the ring $M_2(Z_2)$.

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

Proof. Namely, let $T = A_3 \cup S_A$ 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 $\Gamma$ 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 let $w_i = v_jv_k^{-1}$. We will prove that $p \not\equiv q$ if and only if $\Gamma$ is 3-colorable. We can claim similar statement to Lemma 11.

Lemma 14. 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 $sw_isw_i^2s^2 = 0$.

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 $x = (1, 1)$. Here by item 1 of Lemma 14 $q = 0$. $p = PPPx \neq q = 0$ holds if and only if $xw_1xw_2x \cdots w_kx \neq 0$. It is true if and only if non of the $w_i$-s stabilize 1 which is by item 3 of Lemma 14 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 $\Gamma$ 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 set of words \{w_1, w_2, \ldots, w_n\} and \{v_1, v_2, \ldots, v_m\} over \(G \leq S_k\) the symmetric group acting on the set \(\Omega = \{1, 2, \ldots, k\}\). For an evaluation of the variables and for \(l \in \Omega\) let \(I_l = \{w_1(l), w_2(l), \ldots, w_n(l)\}\) and \(J_l = \{v_1(l), v_2(l), \ldots, v_m(l)\}\). Find the complexity of the question whether the set-equation system \(I_1 = J_1, I_2 = J_2, \ldots, I_k = J_k\) holds for every evaluation.

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

6. Acknowledgements

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

References


Eötvös Loránd University, Department of Algebra and Number Theory, 1117 Budapest, Pázmány Péter sétány 1/c, Hungary
E-mail address: csaba@cs.elte.hu
E-mail address: wera13@cs.elte.hu