Algebra univers. **51** (2004) 439–445
0002-5240/04/040439 – 07
DOI 10.1007/s00012-004-1873-1
©Birkhäuser Verlag, Basel, 2004

Algebra Universalis

The complexity of checking identities for finite matrix rings

Csaba Szabó and Vera Vértesi

Abstract. We complete the investigations into the word-problem for finite matrix rings. Namely we prove that $M_2(Z_3)$, the ring of 2×2 matrices over Z_3, has a coNP-complete term-equivalence (or identity checking) problem.

1. Introduction

In this paper we study the computational complexity of the term-equivalence problem (shortly TERM-EQ) for the semigroup $M_2(Z_3)$. The term-equivalence problem over a finite algebra $\mathcal{A}$ (TERM-EQ $\mathcal{A}$) asks whether two given terms agree for every substitution in the given algebra. 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.

We shall use the standard notations for computational complexity, as P, NP, coNP, etc.

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. 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, and an expression of the form $(x+y)^n$ is too long when expanded. This is the reason why Willard and Lawrence introduced the $_\Sigma$ version of the problem: the instance when every polynomial is a sum of monomials. The TERM$_\Sigma$-EQ problem asks whether two terms that are sums of monomials are equal at every substitution. The following is proved in [4].

Theorem 1. *Let F be a finite field. If the invertible elements of $\mathcal{R} = M_n(F)$ 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 $\mathcal{R}$ *is coNP-complete.*

Presented by R. W. Quackenbush.
Received March 30, 2003; accepted in final form May 3, 2004.
2000 *Mathematics Subject Classification*: 08A50, 68Q17.
Key words and phrases: Matrix ring, term, complexity.

Problem 2 in [4] asks what happens for $n = 2$ and $|F| = 2, 3$. In [7] the following is proved.

Theorem 2. TERM-EQ *is coNP-complete for the semigroup* $M_2(Z_2)$.

This result implies the hardness of the TERM-EQ and TERM$_\Sigma$-EQ problems for the ring $M_2(Z_2)$ as well. Indeed, if the TERM-EQ problem for the multiplicative semigroup of a ring $\mathcal{R}$ is coNP-complete then it is hard to decide whether or not two monomials are equivalent over the ring itself. Hence both the TERM-EQ and the TERM$_\Sigma$-EQ problems are hard over $\mathcal{R}$.

So the only question that has remained open is the case $M_2(Z_3)$. In this note we settle this problem. Namely, we prove that the TERM-EQ is coNP-complete for the semigroup $M_2(Z_3)$.

The importance of TERM-EQ and other term related problems has increased in computer science as well. Using ideas and tools from automata theory, a number of algebraic characterizations of complexity problems have been found (for a general reference see for example [5]). This leads to the study of problems whose computational complexity is described by the properties of terms over an underlying monoid. In [5] and [1] (and other papers) these problems are connected with the so-called PROGRAM SATISFIABILITY problem and are solved for several classes of monoids, such as abelian groups, monoids with irregular $\mathcal{H}$-classes, commutative aperiodic monoids, etc. Popov and Volkov ([6]) gave the first example of a semigroup with computationally hard term-equivalence problem. The size of their semigroup is 2^{1700}. $M_2(Z_3)$ is a reasonably small, natural semigroup to study.

2. The semigroup $M_2(Z_3)$

The semigroup of 2 by 2 matrices over the 3 element field is the union of the group of invertible elements and the semigroup of singular matrices. They are of size 48 and 33, respectively. We can characterize the matrices by their action on the 1-dimensional subspaces of Z_3^2. Let $\sim$ be defined as follows: for a matrix $A \in M_2(Z_3)$ let $A \sim 2A$. Now $\sim$ is an equivalence relation and $A \sim B$ if and only if the matrices A and B induce the same transformation on the set of 1-dimensional subspaces. By this property it is easy to see that $\sim$ is compatible with the matrix multiplication, hence $\sim$ is a congruence of the semigroup $M_2(Z_3)$. Let $PM_2(Z_3) = M_2(Z_3)/\sim$.

As it is easier to handle and understand, at first we will prove a theorem for $PM_2(Z_3)$ similar to the main result of the paper.

Theorem 3. TERM-EQ *is coNP-complete for the semigroup* $PM_2(Z_3)$.

Before proving Theorem 3 we give a similar description for $PM_2(Z_3)$ as we did for $M_2(Z_2)$ in [7]. We split $PM_2(Z_3)$ into two parts: the group of invertible elements and the semigroup of singular elements.

Looking at the action of the invertible matrices on the 1-dimensional subspaces of the vector space Z_3^2 (there are 4 such), we can observe that the group of invertible matrices is isomorphic to the 4-letter symmetric group, S_4.

Every nonzero singular matrix has rank 1, hence it can be written in the form $v \cdot u^T$ for some $u, v \in Z_3^2$. Put

$$v_1 = u_2 = \begin{pmatrix}1\\0\end{pmatrix}, v_2 = u_1 = \begin{pmatrix}0\\1\end{pmatrix}, v_3 = u_4 = \begin{pmatrix}1\\1\end{pmatrix}, v_4 = u_3 = \begin{pmatrix}1\\2\end{pmatrix} \in Z_3^2$$

Here u_i is representing the unique line orthogonal to v_i, thus $u_t^T v_s = 0$ if and only if $t = s$. Every nonzero singular element of $PM_2(Z_3)$ has a unique representant of the form $v_s u_t^T$. Let us denote this class by the symbol $\langle s, t\rangle$. As every class of invertible matrices induces a natural right and left action on the representants of the lines, they can be considered simply as permutations of the set $\{1, 2, 3, 4\}$. Now, $PM_2(Z_3) = S_4 \bigcup \{\langle s, t\rangle \mid 1 \le s, t \le 4\} \cup \{0\}$ and the multiplication can be described in the following way: $0 \cdot a = a \cdot 0 = 0$ for every $a \in PM_2(Z_3)$ and

$$\langle s, t\rangle\pi = \langle s, \pi(t)\rangle, \;\; \pi\langle s, t\rangle = \langle \pi^{-1}(s), t\rangle, \;\; \langle s_1, t_1\rangle\langle s_2, t_2\rangle = \begin{cases} 0 & \text{if } t_1 = s_2 \\ \langle s_1, t_2\rangle & \text{if } t_1 \ne s_2 \end{cases}.$$

For a longer product of elements we will need the following observation.

Lemma 4. *Let $a_j = \langle s_j, t_j\rangle$ for $1 \le j \le n$ and $\pi_1, \pi_2 \dots, \pi_{n+1} \in S_4$. Then*

(1) $a_j^2 = a_j^3$*;*

(2) $a_1\pi_1 a_2 = 0$ *if and only if* $\pi(t_1) = s_2$*;*

(3) $\pi_1 a_1 \pi_2 a_2 \cdots \pi_n a_n \pi_{n+1} = 0$ *if and only if there exists* $1 < k \le n$ *such that* $a_{k-1}\pi_k a_k = 0$ *(i.e.* $\pi_k(t_{k-1}) = s_k$*).*

(4) *If* $\pi_1 a_1 \pi_2 a_2 \cdots \pi_n a_n \pi_{n+1} \ne 0$*, then*

$$\pi_1 a_1 \pi_2 a_2 \cdots \pi_n a_n \pi_{n+1} = \langle \pi_1^{-1}(s_1), \pi_{n+1}(t_n)\rangle.$$

Let

$$D = \{(1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$$

be the set of products of two disjoint transpositions and

$$T = \{(1,2,3), (1,3,2), (1,2,4), (1,4,2), (1,3,4), (1,4,3), (2,3,4), (2,4,3)\}$$

be the set of 3-cycles in S_4. The commutator subgroup of S_4 is A_4 and $A_4 = \{id\} \cup D \cup T$. We list a few properties of S_4.

Lemma 5. *Let $u, v, y, a \in S_4$ and put $w = [y, uv^{-1}] = y^{-1}(uv^{-1})^{-1}y(uv^{-1})$ for $y \in S_4$. Then the following hold:*

(1) *$a^{12} = id$;*
(2) *$w \in A_4$, the commutator subgroup of S_4;*
(3) *$w^6 = id$;*
(4) *w^3 stabilizes 1 if and only if $w \in id \cup T$.*
(5) *For $u, v \in S_4$ there exists an $e \in S_4$ such that $[e, uv^{-1}] \in D$ if and only if $uv^{-1} \neq id$, that is, if and only if $u \neq v$.*
(6) *If $w \in D$, then the subgroup generated by $\{u, v, y\}$ is transitive on $\{1, 2, 3, 4\}$.*
(7) *If $w \in D$, then the set $\{abc \,|\, a, b, c \in \{u, v, y\}\}$ is transitive on $\{1, 2, 3, 4\}$.*

Lemma 6. *Let u, v, $y \in S_4$ and w as in Lemma 5, and let b be a non-invertible element of $PM_2(Z_3)$. If $w^3 \neq id$, then $(\prod_{c_r \in \{y,u,v\}}(bc_1c_2c_3))b = 0$.*

Proof. Let $b = \langle s, t\rangle$. By (4) of Lemma 5, $w \in D$ and by (7) of Lemma 5, there is a product of the form $c_1c_2c_3$ mapping t to s. Hence by Lemma 4 the product is equal to 0. □

We are ready to prove Theorem 3.

Proof of Theorem 3. We reduce graph 24-colorability (a problem which is known to be coNP-complete) to the term equivalence problem. Let $\Gamma = (V, E)$ be an arbitrary simple graph with no loops, $V = \{v_1, \dots, v_n\}$ and $E = \{e_1, \dots, e_m\}$. To every edge and vertex we assign a variable denoted by the same letter. We shall exhibit two terms, p and q, such that the graph Γ is 24 colorable if and only if p is not equivalent to q.

Let

$$\begin{aligned} P &= \prod_{e_i \in E} (xw_i^3)^{12}, \\ Q &= \prod_{e_i \in E} (xw_i^6)^{12}. \end{aligned}$$

Here $w_i = e_i^{11}v_lv_k^{11}e_iv_kv_l^{11}$, where v_l and v_k denote the endpoints of e_i in an arbitrary order. Note that if $e_i, v_l, v_k \in S_4$ then $w_i = e_i^{-1}v_lv_k^{-1}e_iv_kv_l^{-1} = [e_i, v_kv_l^{-1}]$. The order of the edges in the products can be arbitrarily chosen.

For any two edges of e_i and e_j of Γ define

$$H_{i,j} = \prod_{c_r \in \{e_i, v_l, v_k\}} (w_jc_1c_2c_3w_j)^{12},$$

where v_l, v_k denote the endpoints of the edge e_i. Note that by Lemma 6, if $w_i \in D$ and $w_j \in PM_2(Z_3) \setminus S_4$, then $H_{i,j} = 0$, and if $w_i \in D$ and $w_l \in S_4$, then $H_{i,l} = id$.

Define

$$H = \prod_{e_i, e_j \in E} H_{i,j}.$$

Finally, let

$$p = PPPxH,$$
$$q = PQPxH.$$

We will distinguish some cases as can be seen in Table 1.

		$x \in S_4$	$x = \langle s, t\rangle$	
			$s \neq t$	$s = t$
$\forall w_j \in S_4$		Case 1	Case 4a	Case 4b
$\exists w_j \notin S_4$	$\exists w_i \in D$	Case 2		
	$\forall w_i \in PM_2(Z_3) \setminus D$	Case 3		

TABLE 1. The four different cases

In the following we will show that, except for the Case 4b, p is always equivalent to q.

Case 1: When all variables are in S_4. If all variables are from S_4, then $(xw_i^r)^{12} = id$ for every edge and $(w_j g w_j)^{12} = id$ for every pair of edges; hence both terms are equal to x.

Case 2: When there exists $w_j \notin S_4$ and there is an i such that $w_i \in D$. Substituting $b = w_j$, u and v for the endpoints of e_i, and $e = e_i$ in Lemma 6, we obtain $H_{i,j} = 0$ and then $H = 0$, so $p = q = 0$.

Case 3: When there exists $w_j \notin S_4$ and besides $w_i \in PM_2(Z_3) \setminus D$ for every $e_i \in E$. Now, we only have to see that if $w_i \in T \cup \{id\}$ then $w_i^3 = id$. So either $w_i \in T \cup \{id\}$ or $w_i \notin S_4$, and we have $w_i^6 = w_i^3$ by Lemma 4; hence the two terms are equal.

Case 4: When $w_i \in S_4$ for every $i \in E$ and $x = \langle s, t\rangle$.

(1) First, let $x = \langle s, t\rangle$, where $s \neq t$. In this case by item 3 of Lemma 5 we obtain

$$q = Px \cdot id \cdot x \cdots id \cdot xPxH = PPxH = PPPxH = p.$$

(2) 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 5 — $Q = \langle 1, 1\rangle^{\geq 2} = 0$; hence $q = 0$. Thus $p \neq q$ if and only if there is a substitution making $p = PPPx \neq 0$.

By Lemma 4, that holds if and only if $xw_1^3 x w_2^3 x \dots w_k^3 x \neq 0$. By item 4 of Lemma 5, this takes place if and only if none of the w_i^3-s stabilizes 1, which is equivalent to $w_i \notin T \cup id$. 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 5 of Lemma 5, we can choose an $e_i \in S_4$ such that $w_i \notin T \cup id$ if and only if $v_k \neq v_j$. Hence p is not identically 0 if and only if the group elements assigned to neighboring vertices are distinct; hence if and only if $\mathbf{\Gamma}$ is 24-colorable.

□

Finally, we are able to prove the main result of the paper.

Theorem 7. TERM-EQ *is coNP-complete for the semigroup* $M_2(Z_3)$.

Proof. The train of thought is very similar to the case $PM_2(Z_3)$. Let

$$\begin{aligned} P &= \prod_{i \in E} (x w_i^3)^{24}, \\ Q &= \prod_{i \in E} (x w_i^6)^{24}. \end{aligned}$$

and

$$\begin{aligned} p &= PPPPxH, \\ q &= PQQPxH. \end{aligned}$$

The only difference is that instead of equivalence classes we have to consider the elements of $M_2(Z_3)$. We have to distinguish A and $2A$; that is, occasionally a constant factor "2" may appear. This is why we had to change the exponents in the terms, but this does not mean any essential change in the proof.

□

As an immediate consequence of Theorem 7 we have:

Corollary 8. TERM-EQ *and* TERM$_\Sigma$-EQ *are coNP-complete for the ring* $M_2(Z_3)$.

At last, according to Theorems 1 and 2 we get:

Corollary 9. *Let* $\mathcal{R} = M_n(F)$ *be a finite matrix ring.* TERM$_\Sigma$-EQ$\,\mathcal{R}$ *is in* P *if* $n = 1$, *and coNP-complete otherwise.*

3. Acknowledgments

The authors are greatfull to László Márki for his instructions to write and organize the second version of the paper. The research of the authors was supported by the Hungarian National Foundation for Scientific Research, Grant numbers F32325, T038059 and T043671.

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.

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

[3] H. Hunt and R. Stearns, *The complexity for equivalence for commutative rings*, Journal of Symbolic Computation, **10** (1990), 411–436.

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

[5] C. Moore, P. Tesson and D. Thérien, *Satisfiability of systems of equations over finite monoids*, Mathematical foundations of computer science, 2001 (Mariánské Lázně), 537–547.

[6] V. Yu. Popov and M. V. Volkov, *Complexity of checking identities and quasi-identities in finite semigroups*, Journal of Symbolic logic., (to appear, 2003).

[7] Cs. Szabó and V. Vértesi, *The complexity of the word-problem for finite matrix rings*, Proc. Amer. Math. Soc., (to appear, 2003).

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