RAIRO-Inf. Theor. Appl. **39** (2005) 125-131
DOI: 10.1051/ita:2005007

SOME DECISION PROBLEMS ON INTEGER MATRICES *

Christian Choffrut[1] and Juhani Karhumäki[2]

Abstract. Given a finite set of matrices with integer entries, consider the question of determining whether the semigroup they generated 1) is free; 2) contains the identity matrix; 3) contains the null matrix or 4) is a group. Even for matrices of dimension 3, questions 1) and 3) are undecidable. For dimension 2, they are still open as far as we know. Here we prove that problems 2) and 4) are decidable by proving more generally that it is recursively decidable whether or not a given non singular matrix belongs to a given finitely generated semigroup.

Mathematics Subject Classification. 20M05, 68R15.

1. Introduction

The purpose of this work is to tackle a few issues on semigroup of matrices over the integers $\mathbb{Z}$. Very natural and simple questions are already undecidable for low dimensions. *E.g.*, it has long been observed that given a finite set of matrices of dimension 3 with entries in $\mathbb{Z}$, it is undecidable whether or not they generate the zero matrix, (the mortality problem [16]). More recently, it was proved that it is recursively undecidable whether or not such a finite set generates a free monoid [10]. The case of dimension 2 is still unsettled and apparently simple examples let us think that even this restriction is not easy. The dual problem of trying to determine a matrix representation for a given semigroup was considered in [3] where all trace monoids admitting a faithful representation as 2×2-matrices with non-negative integer entries were characterized.

There seems to be little space for decidable issues. Here we show the decidability of a few questions concerning matrices of dimension 2. Indeed, given a finite

* *The authors acknowledge the support of the Academy of Finland under grant #44087.*

[1] L.I.A.F.A, Université Paris VII, Tour 55-56, 1er étage, 2 pl. Jussieu, 75 251 Paris Cedex, France; Christian.Choffrut@liafa.jussieu.fr

[2] Dept. of Mathematics and TUCS, University of Turku, 20014 Turku, Finland; Juhani.Karhumaki@cs.utu.fi

set of matrices of dimension 2 with integer entries, we prove that it can be decided whether or not the semigroup they generate contains the identity and more generally whether or not it contains a given non singular matrix. To our knowledge, for higher dimensions the problem is open. Observe that as a consequence, the property of being a group is also decidable. These results rely on the simple structure of the group of unimodular matrices of dimension 2 which allows us to reformulate the problem in terms of pure automata theory.

2. Preliminaries

In order to give a reasonable limit to our ambition, we recall some results to be found in the literature concerning integer matrices. We do not discuss the well-known problem of the finiteness of a semigroup of matrices (the "Burnside problem"). The reader is referred to [8, 13].

When working with decision procedures for matrices, the case of dimension 3 is already difficult. The main reason is that a direct product of two free monoids has a faithful representation in the multiplicative semigroup $\mathbb{N}^{3\times 3}$ (which extends naturally that of a free monoid in the multiplicative semigroup of $\mathbb{N}^{2\times 2}$). This allows us to encode Post Correspondence Problem and therefore to establish the undecidability of certain problems, see [16], also [10], [2] or [7]. *E.g.*, the freeness of the subsemigroup of a finite number of matrices can be shown to be undecidable when one observes that the "uniquely decipherability property" in $A^* \times B^*$ is undecidable, [4]. Thus, we restrict ourselves to matrices of dimension 2. For a mathematical motivation of studying these matrices we refer to [12], Section 8.

2.1. General decision problems

Though we are mainly interested in the case of the semiring $\mathbb{Z}$, we pose the following general problems for an arbitrary finite subset E of $n \times n$-matrices with coefficients in an integral ring $\mathbb{K}$, see [6, 9].

Identity problem
Does the subsemigroup generated by E contain the identity matrix I?

Group problem
Is the subsemigroup generated by E a group?

Inverse problem
Given $X \in E$ does it have an inverse in the monoid generated by E?

Membership problem
Given $X \in \mathbb{K}^{n\times n}$ does it belong to the monoid generated by E?

As a particular case of the latter we have

Mortality problem
Does the set E generate the null matrix 0?

Observe that the semigroup generated by E contains the identity if and only if it contains the inverse of some element of E and that it is a group if and only if it contains the inverse of all elements of E. In other words, decidability of the Inverse Problem yields decidability of both the Identity and the Group Problems. Also the decidabilty of the Membership Problem entails the decidability of the remaining problems. The Membership Problem is also known as the generalized word problem: if M is a monoid with a recursive presentation $\langle A|R\rangle$ ($R \subset A^* \times A^*$), the generalized word problem asks whether or not there exists an algorithm which given a word $w \in A^*$ and a submonoid $N \subseteq M$, decides if w belongs to N.

2.2. Rational subsets of a monoid

We assume the reader familiar with the elementary theory of finite automata and rational subsets of a monoid. Numerous textbooks give a thorough presentation of the topic, (*e.g.*, [1,5]).

Given a monoid M, the family of *rational* subsets of M is the least family $\mathcal{F}$ of subsets of M containing the empty set $\emptyset$ and all finite subsets and which is closed under *set union* ($X, Y \in \mathcal{F}$ implies $X \cup Y \in \mathcal{F}$), *subset product* ($X, Y \in \mathcal{F}$ implies $X \cdot Y = \{xy \mid x \in X, y \in Y\} \in \mathcal{F}$) and *Kleene product* ($X \in \mathcal{F}$ implies $X^* = \bigcup_{n \geq 0} X^n \in \mathcal{F}$).

Assume the monoid M has a finite monoid presentation, *i.e.*, it is isomorphic to a quotient of a finitely generated free monoid by some finitely generated congruence $\equiv$. Then an arbitry rational subset H of M is *defined* by some finite automaton $\mathcal{A}$ in the following sense. Each word recognized by $\mathcal{A}$ is a representative of an element of H and conversely, each element of H is represented by some word recognized by the automaton. Equivalently, if $|\mathcal{A}|$ denotes the set of words recognized by $\mathcal{A}$, this automaton represents the subset $|\mathcal{A}|/_{\equiv}$ of M.

The following particular case plays a special role in the rest of the paper.

Proposition 1. *Given a rational subset of a free product of finite cyclic groups $G \cong \mathbb{Z}/p_1\mathbb{Z} * \ldots * \mathbb{Z}/p_n\mathbb{Z}$ defined by some finite automaton as explained above, it is recursively decidable whether or not it contains the unit of G.*

Proof. The group G has the monoid presentation $\langle a_1, a_2, \ldots, a_n | a_1^{p_1} = a_2^{p_2} = \ldots = a_n^{p_n} = 1\rangle$, *i.e.*, it is given as the quotient of the free monoid $\{a_1, a_2, \ldots, a_n\}^*$ by the (monoid) congruence generated by the relators $a_1^{p_1} \equiv 1$, $\ldots$, $a_n^{p_n} \equiv 1$. It is well-known that each word is equivalent to a unique reduced word, *i.e.*, a word containing no occurrence of $a_i^{p_i}$ for $i = 1, \ldots, n$. Such a word is obtained by applying the reduction rules $a_i^{p_i} \to 1$ deleting all occurrences of $a_i^{p_i}$, one after the other in any possible order. Let $\mathcal{A}$ be a finite automaton defining a rational subset H of G. It suffices to show that the set of reduced words congruent to the words accepted by $\mathcal{A}$ is also recognized by a finite automaton. The idea consists of augmenting $\mathcal{A}$ with transitions which do not modify $|\mathcal{A}|/\equiv$ but which add words obtained by reduction. It then suffices to select the reduced words by intersecting the subset with all reduced words, which is a rational set of words.

More technically, the procedure does the following: add an empty transition, *i.e.*, draw a transition labelled by the empty word between state q and q' whenever there is a path labelled by $a_i^{p_i}$ for $i = 1, \ldots, n$ between state q and q' and stop whenever no new empty transition can be added. Let $L \subseteq \{a_1, a_2, \ldots, a_n\}^*$ be the subset recognized by the modified automaton $(L/\equiv = |\mathcal{A}|/\equiv)$. Then the subset of reduced words is the rational subset $L - \{a_1, a_2, \ldots, a_n\}^*(a_1^{p_1} + \ldots + a_n^{p_n})\{a_1, a_2, \ldots, a_n\}^*$. □

3. Decidable properties in $\mathbb{Z}^{2\times 2}$

The main ingredient of our proof is the following well-known result on the group $\mathrm{GL}(2,\mathbb{Z})$ of invertible matrices in the monoid $\mathbb{Z}^{2\times 2}$. The subgroup consisting of *unimodular* matrices (*i.e.*, with determinant equal to 1) is the *special linear group* $\mathrm{SL}(2,\mathbb{Z})$. This group is generated by the two matrices

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}.$$

Furthermore, the quotient of $\mathrm{SL}(2,\mathbb{Z})$ by its center $\pm I$, which is the *projective special linear group* $\mathrm{PSL}(2,\mathbb{Z})$, has a finite presentation as a free product of two finite cyclic groups

$$\mathrm{PSL}(2,\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/3\mathbb{Z}. \tag{1}$$

A morphism of $\mathrm{SL}(2,\mathbb{Z})$ onto the group $\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/3\mathbb{Z}$ presented by $\langle a, b | a^2, b^3 \rangle$ is obtained by assigning a to the matrix A and b to the matrix B, *cf., e.g.,* [17], Exercise 11.24.

The following theorem implies that the membership problem for finitely subsemigroups of $\mathrm{GL}(2,\mathbb{Z})$ is recursively decidable. Now, substitute the term subgroup for subsemigroup. A theorem of Mikhailova, [11], p. 193, says that the direct product of two free finitely generated groups may have unsolvable membership problem. Since the group $\mathrm{GL}(4,\mathbb{Z})$ of invertible 4×4-matrices with entries in $\mathbb{Z}$ has a subgroup which is a direct product of two copies of $\mathrm{GL}(2,\mathbb{Z})$ and since each copy has a subgroup which is freely generated by an arbitrary number of generators, the membership problem for $\mathrm{GL}(4,\mathbb{Z})$ is recursively unsolvable, see also [14]. The case of $\mathrm{GL}(3,\mathbb{Z})$ remains open, see [15].

Theorem 1. *Given a rational subset of matrices in $\mathbb{Z}^{2\times 2}$ and a non singular matrix $Y \in \mathbb{Z}^{2\times 2}$, it is recursively decidable whether or not Y belongs to this rational subset.*

Proof. We reformulate the problem as follows. We are given a rational expression $\mathcal{R}(X_1, \ldots, X_n)$ over the set of symbols X_i, $i = 1, \ldots, n$ defining a set of words over these symbols. Furthermore, we are given a substitution ϕ which assigns a matrix

in $\mathbb{Z}^{2\times 2}$ to each symbol X_i. We are asked, for a given matrix Y with $\mathrm{Det}(Y) = \pm 1$ wether or not the condition

$$Y \in \phi(\mathcal{R}(X_1, \ldots, X_n)) \tag{2}$$

holds. We shall proceed by successive simplifications until reducing the problem to determining whether or not the unit matrix belongs to a rational set of the group $\mathrm{PSL}(2, \mathbb{Z})$.

Claim 1. Without loss of generality we may assume $Y = I$. Indeed, let X be a new symbol, consider the rational expression $X \cdot \mathcal{R}(X_1, \ldots, X_n)$ and extend ϕ by defining $\phi(X) = Y^{-1}$. Then the condition $Y \in \phi(\mathcal{R}(X_1, \ldots, X_n))$ is equivalent to the condition $I \in \phi(X \cdot \mathcal{R}(X_1, \ldots, X_n))$.

Claim 2. Without loss of generality we may assume that the determinant of all X_i's is equal to 1 or -1. Indeed, let J be the subset of integers $1 \leq i \leq n$ for which the determinant of X_i is equal to 1 or -1. Then Condition 2 is equivalent to the condition $I \in \phi\left((\mathcal{R}(X_1, \ldots, X_n) \cap \{X_i \mid i \in J\}^*\right)$.

Claim 3. Without loss of generality we may assume that the determinant of all X_i's is equal to 1. Indeed, first we may assume that in all the words defined by the expression $\mathcal{R}(X_1, \ldots, X_n)$, the number of occurrences of symbols X_i for which the determinant is equal to -1 is even: let J be the subset of integers $1 \leq i \leq n$ for which the determinant of X_i is equal to -1. Then Condition 2 is equivalent to the condition

$$I \in \phi\left(\mathcal{R}(X_1, \ldots, X_n) \cap (\{X_i \mid i \notin J\}^* \{X_i \mid i \in J\})^2)^* \{X_i \mid i \notin J\}^*\right)$$

where the expression under the function ϕ is equivalent to a rational expression, by Kleene's Theorem. Now we observe that for all X_i, $i \in J$ and all X_k, $k \notin J$ there exists a unique matrix $Y_{i,k}$ with determinant equal to 1 such that $\phi(X_i)Y_{i,k} = \phi(X_k)\phi(X_i)$ holds. Let $X_{i,k}$ be a new symbol for $i \in J$ and $k \notin J$ and extend ϕ by posing $\phi(X_{i,k}) = Y_{i,k}$ for all the new symbols thus introduced. Let τ be the mapping which transforms every word defined by the rational expression $\mathcal{R}$ as follows. Consider, if they exist, the leftmost two symbols X_i and X_j, $i, j \in J$, $i < j$ in the word and replace the factor $X_i X_{i+1} \ldots X_{j-1} X_j$ by the factor $X_{i,i+1} \ldots X_{i,j-1} X_i X_j$. Proceed in this way until exhausting all symbols X_i with $i \in J$. *E.g.*, for $n = 4$, $J = \{2, 4\}$ and the word $W = X_3 X_2 X_1 X_3 X_4 X_3 X_4 X_1 X_2$ we would have $\tau(W) = X_3 X_{2,1} X_{2,3} X_2 X_4 X_3 X_{4,1} X_4 X_2$. The function τ is rational and there exists a rational expression $\mathcal{R}'$ over the symbols X_i, $i = 1, \ldots, n$ and the symbols $X_{i,k}$, $i \in J$, $k \notin J$ which defines exactly the images of the words defined by $\mathcal{R}$ in the transformation τ. Observe that in the words defined by $\mathcal{R}'$, the symbols X_i with $i \in J$ appear in consecutive positions. We group them by creating a new symbol $Z_{i,k}$ for all factors $X_i X_j$, $i, k \in J$. This yields a new equivalent rational expression $\mathcal{R}''$ where the symboles are the X_i's with $i \notin J$, the $X_{i,k}$'s for $i \in J$, $k \notin J$ and the symbols $Z_{i,k}$, $i, k \in J$. A final extension of ϕ is obtained by posing $\phi(Z_{i,k}) = \phi(X_i)\phi(X_k)$. This completes the proof of the third claim.

The previous three claims prove that we can start up from a rational expression $\mathcal{R}$ and a morphism ϕ assigning a matrix in $\mathrm{SL}(2,\mathbb{Z})$ to each symbol X_i, in other words, that $\phi(\mathcal{R})$ is a rational subset of $\mathrm{SL}(2,\mathbb{Z})$. The mapping ι which identifies each matrix of $\mathrm{SL}(2,\mathbb{Z})$ with its opposite, maps $\phi(\mathcal{R})$ onto the rational subset of $\iota(\phi(\mathcal{R}))$ of $\mathrm{PSL}(2,\mathbb{Z})$ for which we can apply Proposition 1 and find out whether I or its opposite belongs to $\phi(\mathcal{R})$. If it does, in order to lift the ambiguity between I and $-I$, we consider the morphism θ which assigns to every matrix of $\mathrm{SL}(2,\mathbb{Z})$ the matrix in the finite group $(\mathbb{Z}/3\mathbb{Z})^{2\times 2}$ obtained by considering its entries modulo the integer 3. Intersect $\mathcal{R}$ with the set of all products whose image in the morphism θ is the identity matrix of $(\mathbb{Z}/3\mathbb{Z})^{2\times 2}$ which we simply denote by 1

$$\mathcal{R}' = \mathcal{R} \cap \{W \in \{X_1, \ldots, X_n\}^* \mid \theta(\phi(W)) = 1\}.$$

This intersection is again rational, and we have the condition $I \in \phi(\mathcal{R}')$ if and only if $\iota(I) \in \iota(\phi(\mathcal{R}'))$ and we may conclude *via* Proposition 1.

Now, we apply the previous considerations. Assume a non-singular matrix Y belongs to the semigroup generated by a finite set E of matrices: $Y = Z_1 \ldots Z_n$. Consider the set of increasing indices corresponding to the matrices with determinant different from 1 or -1 in this product.

$$\{0 < i_1 < i_2 < \ldots i_p \leq n\} = \{0 < i \leq n \mid \mathrm{Det}(Z_i) \neq \pm 1\}. \tag{3}$$

For every matrix $X \in E$ with $\mathrm{Det}(X) = \pm 1$, we define the sequence

$$X^{(0)} = X, Z_{i_1}X = X^{(1)}Z_{i_1}, \ldots, Z_{i_1}Z_{i_2}\ldots Z_{i_p}X = X^{(p)}Z_{i_1}Z_{i_2}\ldots Z_{i_p}.$$

For $k = 1, \ldots, p$, define $E^{(k)}$ as the submonoid generated by the finite set of matrices $X^{(k)}$. Compute the matrix $M = Y(Z_{i_1}\ldots Z_{i_p})^{-1}$. Then M belongs to the rational subset of $\mathrm{SL}(2,\mathbb{Z})$

$$E^{(0)}E^{(1)}\ldots E^{(p)}.$$

Conversely, if M belongs to this subset, then Y can be expressed by a product $Y = Z_1 \ldots Z_n$ with the condition (3), which we proved to be recursively decidable in the first part. Finally, in order to verify whether or not Y is generated by E, we test all possible sequences $Z_{i_1}, \ldots, Z_{i_p}$ with $p \leq \lceil \log_2 |\mathrm{Det}(Y)| \rceil$. This completes the proof. □

As a corollary we get

Theorem 2. *Given a finite set of matrices in* $\mathbb{Z}^{2\times 2}$*, the* IDENTITY*, the* GROUP *and the* INVERSE *problem are recursively decidable.*

References

[1] J. Berstel, *Transductions and context-free languages*. B.G. Teubner (1979).

[2] J. Cassaigne, T. Harju and J. Karhumäki, On the undecidability of freeness of matrix semigroups. *Internat. J. Algebra Comput.* **9** (1999) 295–305.

[3] C. Choffrut, A remark on the representation of trace monoids. *Semigroup Forum* **40** (1990) 143–152.

[4] M. Chrobak and W. Rytter, Unique decipherability for partially commutative alphabets. *Fund. Inform.* **X** (1987) 323–336.

[5] S. Eilenberg, *Automata, Languages and Machines*, Vol. A. Academic Press (1974).

[6] T. Harju, Decision questions on integer matrices. *Lect. Notes Comp. Sci.* **2295** (2002) 57–68.

[7] T. Harju and J. Karhumäki, Morphisms, in *Handbook of Formal Languages*, edited by G. Rozenberg and A. Salomaa. Springer-Verlag **1** (1997) 439–510.

[8] G. Jacob, La finitude des représentations linéaires de semigroupes est décidable. *J. Algebra* **52** (1978) 437–459.

[9] J. Karhumäki, Some opem problems in combinatorics of words and related areas, in *Proc. of RIMS Symposium on Algebraic Systems, Formal Languages and Computation*. RIMS Institute **1166** (2000) 118–130.

[10] D.A. Klarner, J.-C. Birget and W. Satterfield, On the undecidability of the freeness of integer matrix semigroups monoids. *Internat. J. Algebra Comput.* **1** (1991) 223–226.

[11] R. Lyndon and P. Schupp, *Combinatorial Group Theory*, of *Ergebnisse der Mathematik und ihrer Grenzgebiete*. Springer-Verlag **89** (1977).

[12] W. Magnus, The use of 2 by 2 matrices in combinatorial group theory. *Resultate der Mathematik* **4** (1981) 171–192.

[13] A. Mandel and I. Simon, On finite semigroups of matrices. *Theoret. Comput. Sci.* **5** (1978) 101–112.

[14] A.A. Markov, On certain insoluble problems concerning matrices (russian). *Doklady Akad. Nauk SSSR (N.S.)* **57** (1947) 539–542.

[15] Open problems in group theory: `http://zebra.sci.ccny.edu/cgi-bin/LINK.CGI?/www/web/problems/oproblems.html`

[16] M.S. Paterson, Unsolvability in 3×3 matrices. *Stud. Appl. Math.* **49** (1970) 105–107.

[17] J.J. Rotman, *An introduction to the Theory of Groups*. Ally and Bacon Inc. (1965).