Available online at www.sciencedirect.com
SCIENCE DIRECT®
Advances in Applied Mathematics 33 (2004) 747–752
ADVANCES IN Applied Mathematics
www.elsevier.com/locate/yaama

# Undecidability in matrices over Laurent polynomials

Vesa Halava *, Tero Harju

*Department of Mathematics and TUCS–Turku Centre for Computer Science, University of Turku, FIN-20014 Turku, Finland*

Received 16 March 2004; accepted 21 April 2004

Available online 18 September 2004

**Abstract**

We show that it is undecidable for finite sets $S$ of upper triangular $(4 \times 4)$-matrices over $\mathbb{Z}[x, x^{-1}]$ whether or not all elements in the semigroup generated by $S$ have a nonzero constant term in some of the Laurent polynomials of the first row. This result follows from a representations of the integer weighted finite automata by matrices over Laurent polynomials.


## 1. Introduction

Let $R$ be a ring. A *Laurent polynomial* $p \in R[x, x^{-1}]$ with coefficients in $R$ is a series

$$p(x) = \cdots + a_{-2}x^{-2} + a_{-1}x^{-1} + a_0 + a_1 x + a_2 x^2 + \cdots,$$

where there are only finitely many nonzero coefficients $a_i \in R$. The *constant term* of the Laurent polynomial $p \in R[x, x^{-1}]$ is $a_0$. The family of Laurent polynomials with coefficients in $R$ forms a ring with respect to the operations of sum and multiplication, that are

* Corresponding author.
*E-mail addresses:* vehalava@utu.fi (V. Halava), harju@utu.fi (T. Harju).

0196-8858/$ – see front matter 
doi:10.1016/j.aam.2004.04.002

defined in the usual way, that is, the sum is defined componentwise and the multiplication is the Cauchy product of the polynomials:

$$\left(\sum_{i=-\infty}^{\infty} a_i x^i\right)\left(\sum_{i=-\infty}^{\infty} b_i x^i\right) = \sum_{i=-\infty}^{\infty}\left(\sum_{j+k=i} a_j b_k\right)x^i.$$

Our results will be stated for the ring of integers, and therefore we concentrate on matrices over Laurent polynomials with integer coefficients, that is, the elements of $\mathbb{Z}[x, x^{-1}]^{n\times n}$ for $n \geqslant 1$. A Laurent polynomial matrix

$$M = (c_{ij})_{n\times n} \in \mathbb{Z}\big[x, x^{-1}\big]^{n\times n}$$

is a $n \times n$-square matrix the entries of which are Laurent polynomials from $\mathbb{Z}[x, x^{-1}]$. For these matrices, multiplication is defined in the usual way using the multiplication of the ring $\mathbb{Z}[x, x^{-1}]$. Indeed, if $M_1 = (c_{ij})_{n\times n}$ and $M_2 = (d_{ij})_{n\times n}$, then

$$M_1 \cdot M_2 = (e_{ij})_{n\times n},$$

where

$$e_{ij} = \sum_{k=1}^{n} c_{ik} d_{kj} \in \mathbb{Z}\big[x, x^{-1}\big].$$

Also the sum for these matrices can be defined, but we are interested in the semigroups generated by a finite number of Laurent polynomials under multiplication.

For a set $S \subseteq \mathbb{Z}[x, x^{-1}]^{n\times n}$, denote by $\langle S\rangle$ the semigroup of matrices generated by the elements of $S$. Our main result states that it is undecidable for finite sets $S$ of $4 \times 4$ upper triangular Laurent polynomial matrices over $\mathbb{Z}[x, x^{-1}]$ whether or not all elements of $\langle S\rangle$ have a nonzero constant term in some of the Laurent polynomials of the first row. This result is obtained by translating an undecidability result concerning weighted automata to Laurent polynomial matrices.

## 2. Laurent polynomials and weighted automata

Let $A$ be a finite set of symbols, called an *alphabet*. A *word* over $A$ is a finite sequence of symbols in $A$. We denote by $A^*$ the set of all words over $A$. Note that also the *empty word*, denoted by $\varepsilon$, is in $A^*$.

Let $u = u_1 \dots u_n$ and $v = v_1 \dots v_m$ be two words in $A^*$, where each $u_i$ and $v_j$ are in $A$ for $1 \leqslant i \leqslant n$ and $1 \leqslant j \leqslant m$. The *concatenation* of $u$ and $v$ is the word $u \cdot v = uv = u_1 \dots u_n v_1 \dots v_m$. The operation of concatenation is associative on $A^*$, and thus $A^*$ is a semigroup (containing an identity element $\varepsilon$). Let $A^+ = A^* \setminus \{\varepsilon\}$ be the semigroup of all nonempty words over $A$. A subset $L$ of $A^*$ is called a *language*.

We consider a generalization of finite automata where the transitions have integer weights. The type of automata we consider is closely related to the 1-turn counter automata as considered by Baker and Book [1], Greibach [3], and especially by Ibarra [6]. Also, regular valence grammars are related to these automata, see [5]. Moreover, the extended finite automata of Mitrana and Stiebe [9] are generalizations of these automata.

Consider the additive group of $\mathbb{Z}$ of integers. A ($\mathbb{Z}$-)*weighted finite automaton* $\mathcal{A}^\gamma$ consists of a *finite automaton* $\mathcal{A} = (Q, A, \delta, q_\mathcal{A}, F)$, where $Q$ is a *finite* set of *states*, $A$ is a finite *input alphabet*, $\delta$ is a *finite multiset* of transitions in $Q \times A \times Q$, $q_\mathcal{A} \in Q$ is an *initial state* and $F$ is the set of *final states*, and a *weight function* $\gamma : \delta \to \mathbb{Z}$.

A transition $(q, a, p) \in \delta$, where $p, q \in Q$ and $a \in A$, and $\delta$ is regarded as a relation (and sometimes also as an alphabet). We let $\delta$ be a multiset in order to be able to define (finitely) many different weights for each transition of $\mathcal{A}$. For example, it is possible that for $t_1, t_2 \in \delta$, $t_1 = (p, a, q) = t_2$ and $\gamma(t_1) \neq \gamma(t_2)$.

Without loss of generality, we can assume that

$$Q = \{1, 2, \ldots, n\} \quad \text{for some } n \geqslant 1, \qquad \text{and} \qquad q_\mathcal{A} = 1.$$

Indeed, renaming of the states will not change the accepted language.

A *path* $\pi$ of $\mathcal{A}$ (from $q_1$ to $q_{n+1}$) is a sequence

$$\pi = t_1 t_2 \ldots t_k \quad \text{where } t_i = (q_i, a_i, q_{i+1}) \in \delta \tag{2.1}$$

for $i = 1, 2, \ldots, k$. The *label* of the path $\pi$ in (2.1) is the word $\|\pi\| = a_1 a_2 \ldots a_k$. Let

$$\mathcal{A}(w : p \to q) = \big\{\pi \mid \pi \text{ a path from } p \text{ to } q \text{ with } \|\pi\| = w\big\}.$$

Moreover, a path $\pi \in \mathcal{A}(w : p \to q)$ is *successful* (for $w$), if $p = 1$ and $q \in F$.

Let $\pi = t_1 t_2 \ldots t_k$ be a path of $\mathcal{A}$, where $t_i = (q_i, a_i, q_{i+1})$ for $i = 1, 2, \ldots, k$. The *weight* of $\pi$ is the element

$$\gamma(\pi) = \gamma(t_1) + \gamma(t_2) + \cdots + \gamma(t_k).$$

Furthermore, we let

$$L(\mathcal{A}^\gamma) = \big\{w \in A^* \mid \gamma(\pi) = 0,\ \pi \in \mathcal{A}(w : 1 \to q) \text{ for some } q \in F\big\},$$

be the *language of* $\mathcal{A}^\gamma$. In other words, a word is accepted by $\mathcal{A}^\gamma$ if and only if there is a successful path of weight 0 in $\mathcal{A}^\gamma$.

Note that the underlying finite automaton $\mathcal{A}$ of $\mathcal{A}^\gamma$ is a classical nondeterministic finite automaton, see [2].

Next we shall introduce a matrix representation of integer weighted finite automata with the matrices over the Laurent polynomials $\mathbb{Z}[x, x^{-1}]$.

Let $\mathcal{A}^\gamma$ be a weighted finite automaton, where $\mathcal{A} = (Q, A, \delta, 1, F)$ and $\gamma : \delta \to \mathbb{Z}$. Let again $Q = \{1, 2, \ldots, n\}$. Define for each element $a \in A$ and a pair of states $i, j \in Q$ the Laurent polynomial

$$p_{ij}^a = \sum_{t=(i,a,j)\in\delta} x^{\gamma(t)}.$$

Moreover, define the Laurent polynomial matrix $M_a \in \mathbb{Z}[x, x^{-1}]^{n\times n}$ for all $a \in A$ by

$$(M_a)_{ij} = p^a_{ij}. \tag{2.2}$$

Let $\mu : A^* \to \mathbb{Z}[x, x^{-1}]^{n\times n}$ be the morphism defined by $\mu(a) = M_a$. Let $\iota = (1, 0, \dots, 0)$, where only the first term is nonzero, and let $\rho = (\rho_1, \rho_2, \dots, \rho_n)$ in $\mathbb{Z}^n$ where

$$\rho_i = \begin{cases} 1, & \text{if } q_i \in F, \\ 0, & \text{otherwise.} \end{cases} \tag{2.3}$$

The triple $(\iota, \mu, \rho)$ is called a *Laurent representation* of $\mathcal{A}^\gamma$. Note that classical finite automata have so called *linear representation* with matrices from $\mathbb{N}^{n\times n}$, see [2] or [7].

**Lemma 2.1.** *Let $(\iota, \mu, \rho)$ be a Laurent representation of $\mathcal{A}^\gamma$, and let $w \in A^*$. Then the coefficient of $x^z$ in $\mu(w)_{ij}$ is equal to the number of paths $\pi \in \mathcal{A}(w : i \to j)$ of weight $z$.*

**Proof.** We write $M_u = \mu(w)$ for each word $w$. We prove the claim by induction on the length of the words. The claim is trivial, if $w \in A$. Assume then that the claim holds for the words $u, v \in A^+$, and let $(M_u)_{ij} = p^u_{ij} = \sum_z \alpha^z_{ij} x^z$, where $\alpha^z_{rs}$ is the number of paths from $\mathcal{A}(u : i \to j)$ of weight $z$. Similarly, let $(M_v)_{ij} = p^v_{ij} = \sum_z \beta^z_{ij} x^z$, where $\beta^z_{rs}$ is the number of paths from $\mathcal{A}(v : i \to j)$ of weight $z$. Now,

$$\begin{aligned}(M_u M_v)_{ij} &= \sum_{k=1}^n p^u_{ik} p^v_{kj} = \sum_{k=1}^n \left( \sum_{z_1} \alpha^{z_1}_{ik} x^{z_1} \sum_{z_2} \beta^{z_2}_{kj} x^{z_2} \right) \\ &= \sum_{k=1}^n \sum_{z_1, z_2} \alpha^{z_1}_{ik} \beta^{z_2}_{kj} x^{z_1+z_2} = \sum_{z_1, z_2} \sum_{k=1}^n \alpha^{z_1}_{ik} \beta^{z_2}_{kj} x^{z_1+z_2}.\end{aligned}$$

In other words, the coefficient of $x^z$ is equal to $\sum_{z_1+z_2=z} \sum_{k=1}^n \alpha^{z_1}_{ik} \beta^{z_2}_{kj}$, wherefrom the claim easily follows. □

The following result is an immediate corollary to Lemma 2.1.

**Theorem 2.2.** *Let $(\iota, \mu, \rho)$ be a Laurent representation of $\mathcal{A}^\gamma$, and let $w \in A^*$ Then the constant term $c$ of $\iota\mu(w)\rho^T$ equals the number of different successful paths of $w$ in $\mathcal{A}^\gamma$. In particular, $w \in L(\mathcal{A}^\gamma)$ if and only if $c > 0$.*

## 3. The main results

We turn now to our main result on undecidability of Laurent polynomial matrices.

In the *universe problem* we ask, whether or not $L(\mathcal{A}^\gamma) = A^*$ for a given weighted automaton $\mathcal{A}^\gamma$ with the input alphabet $A$. The universe problem for the weighted finite automata is known to be undecidable. Indeed, it was shown in [4] that this undecidability result holds for very restricted class of weighted automata. A weighted automaton $\mathcal{A}^\gamma$ with the set $Q = \{1, 2, \ldots, n\}$ is called *acyclic*, if in each transition $(i, a, j) \in \delta$, we have $i \leqslant j$, that is, $\mathcal{A}$ does not have directed cycles possibly excepting loops $(i, a, i)$. Note that acyclicity condition is not mentioned explicitly in the main theorem of [4] (Theorem 3.1), but it is immediate from the construction (as mentioned on page 191 of [4]).

**Theorem 3.1.** *The universe problem is undecidable for the class of acyclic* 4*-state weighted finite automata* $\mathcal{A}^\gamma$ *where every state is final.*

For an acyclic weighted automaton $\mathcal{A}^\gamma$, the Laurent polynomial matrix obtained in (2.2) is upper triangular. The fact that Theorem 3.1 allows all states to be final means that in the matrix representation of Theorem 2.2, the vectors ($\imath$ and $\rho$) can be chosen as

$$\imath = (1, 0, 0, 0) \quad \text{and} \quad \jmath = (1, 1, 1, 1).$$

Recall that $\langle S\rangle$ denotes the matrix semigroup generated by the set $S$. From Theorem 2.2, we have

**Theorem 3.2.** *It is undecidable for finite sets $S$ of upper triangular* $(4 \times 4)$*-matrices over* $\mathbb{Z}[x, x^{-1}]$ *whether or not for all matrices $M \in \langle S\rangle$, the constant term of the Laurent polynomial $\imath M \jmath^T$ is nonzero.*

In other words,

**Theorem 3.3.** *It is undecidable for finite sets $S$ of upper triangular* $(4 \times 4)$*-matrices over* $\mathbb{Z}[x, x^{-1}]$ *whether or not all matrices $M \in \langle S\rangle$ have a nonzero constant term in some of the Laurent polynomials of the first row.*

A result attributed to R.W. Floyd in [8] states that it is undecidable for finite subsets $S \subseteq \mathbb{Z}^{3\times 3}$ whether there exists a matrix $M \in \langle S\rangle$ such that the upper right corner of $M$ is zero. We shall consider now a similar problem for Laurent polynomial matrices.

**Theorem 3.4.** *It is undecidable for finite sets $S$ of upper triangular* $(5 \times 5)$*-matrices over* $\mathbb{Z}[x, x^{-1}]$ *whether or not there exists matrix $M \in \langle S\rangle$ having a zero constant term in the upper right corner polynomial $M_{1,5}$.*

**Proof.** Let $\mathcal{A}^\gamma$ be a weighted finite automaton with $\mathcal{A} = (A, Q, \delta, 1, Q)$, where all states in $Q = \{1, 2, \ldots, n\}$ are final. We define an $(n + 1)$-state weighted automaton

$$\mathcal{A}_f^\gamma = \big(A, Q \cup \{n + 1\}, \delta_f, 1, \{n + 1\}\big)$$

with one final state $n + 1$ by adding to $\delta$ the transitions $t' = (q, a, n + 1)$ for all $t = (q, a, p) \in \delta$ with $p \in Q$. The weights of these new transitions $t'$ are defined by $\gamma(t') = \gamma(t)$. Now for all paths $\pi \in \mathcal{A}(u : p \to q)$ in $\mathcal{A}^\gamma$, there corresponds a unique path $\pi' \in \mathcal{A}_f(u : p \to n + 1)$ in $\mathcal{A}_f^\gamma$, which satisfies $\gamma(\pi') = \gamma(\pi)$. (In $\pi'$ only the last transition is changed.) It is then clear that $L(\mathcal{A}_f^\gamma) = L(\mathcal{A}^\gamma) \setminus \{\varepsilon\}$, i.e., only the empty word is excluded from $L(\mathcal{A}_f^\gamma)$. Note that the empty word in always in $L(\mathcal{A}^\gamma)$, since the initial state 1 is also a final state in the original $\mathcal{A}^\gamma$. Now, by Theorem 2.2, for all nonempty words $w$, the constant term of the Laurent polynomial $(1, 0, \dots, 0)\mu(w)(0, 0, \dots, 0, 1)^T$ is nonzero if and only if $w \in L(\mathcal{A}^\gamma)$. From Theorem 3.1, it follows that it is undecidable whether or not all matrices $M \in \langle S \rangle$ have a nonzero constant term in the upper right corner polynomial $M_{1,5}$. Therefore, it is necessarily undecidable whether or not one of the matrices has a zero constant term in right upper corner. $\square$

## Acknowledgment

We are grateful for a referee of this journal for useful comments.

## References

[1] B. Baker, R. Book, Reversal-bounded multipushdown machines, J. Comput. System Sci. 8 (1974) 315–332.
[2] S. Eilenberg, Automata, Languages and Machines, vol. A, Academic Press, 1974.
[3] S.A. Greibach, An infinite hierarchy of context-free languages, J. Assoc. Comput. Mach. 16 (1969) 91–106.
[4] V. Halava, T. Harju, Undecidability in integer weighted finite automata, Fund. Inform. 38 (1–2) (1999) 189–200.
[5] V. Halava, T. Harju, H.J. Hoogeboom, M. Latteux, Valence languages generated by generalized equality sets, J. Autom. Lang. Comb., in press.
[6] O.H. Ibarra, Restricted one-counter machines with undecidable universe problems, Math. Systems Theory 13 (1979) 181–186.
[7] W. Kuich, A. Salomaa, Semirings, Automata, Languages, Springer-Verlag, 1986.
[8] Z. Manna, Mathematical Theory of Computations, McGraw–Hill, 1974.
[9] V. Mitrana, R. Stiebe, The accepting power of finite automata over groups, in: G. Păun, A. Salomaa (Eds.), New Trends in Formal Language, in: Lecture Notes in Comput. Sci., vol. 1218, Springer-Verlag, 1997, pp. 39–48.