# Decidable and Undecidable Problems in Matrix Theory

# Vesa Halava

University of Turku, Department of Mathematics, FIN-20014 Turku, Finland vehalava@utu.fi Supported by the Academy of Finland under the grant 14047



Turku Centre for Computer Science TUCS Technical Report No 127 September 1997 ISBN 952-12-0059-6 ISSN 1239-1891

#### Abstract

This work is a survey on decidable and undecidable problems in matrix theory. The problems studied are simply formulated, however most of them are undecidable. The method to prove undecidabilities is the one found by Paterson [Pat] in 1970 to prove that the mortality of finitely generated matrix monoids is undecidable. This method is based on the undecidability of the Post Correspondence Problem. We shall present a new proof to this mortality problem, which still uses the method of Paterson, but is a bit simpler.

**Keywords:** decidability, undecidability, matrix semigroups, mortality, freeness, finiteness, zero in the right upper-corner, Skolem's problem

# Contents

1	Introduction	1
<b>2</b>	Preliminaries	3
	2.1 Basics	3
	2.2 Semigroups and monoids	3
	2.3 Matrix semigroups and monoids	3
	2.4 Decidability and undecidability	6
	2.5 Word monoids and morphisms	7
	2.6 The Post Correspondence Problem	8
	2.7 The Mixed Modification of PCP	8
3	Mortality of Matrix Monoids	11
	3.1 The undecidability of the mortality problem	11
	3.2 The mortality of semigroups with two generators	15
	3.3 The existence of the zero element in matrix semigroups	17
	3.4 The mortality problem in dimension two	18
4	Freeness of Matrix Semigroups	21
	4.1 The undecidability of the freeness	21
	4.2 The freeness problem in dimension two	23
	4.3 Common elements in semigroups	24
<b>5</b>	Finiteness of Matrix Semigroups	25
	5.1 The decidability of the finiteness	25
6	Zero in the Right Upper Corner	33
	6.1 The undecidability of the zero in the right upper corner	33
	6.2 The two generator case	35
7	Skolem's Problem	37
	7.1 Skolem's problem in dimension two	37
	7.2 Skolem's problem and the mortality problem	42
	7.3 Skolem's problem for matrices over natural numbers	45
8	An Infinite Number of Zeros in Skolem's Problem	46
	8.1 Rational series	46
	8.2 Skolem's theorem	51
	8.3 Decidability of the infinite number of zeros	58
9	Summary	60

## 1 Introduction

This thesis deals with decidable and undecidable problems in matrix theory. The matrices we consider are over integers, and the problems we study are simply formulated and elementary, but it turns out that many of these problems are algorithmically undecidable, which means that there exists no computer program to solve these problems.

We use mainly only basic properties of matrices. These and other basic definitions, notations and properties are presented in the next chapter. Occasionally we need more advanced properties of matrices that are stated when they are needed. The definitions and proofs of such properties can be found from [Gan].

We are going to show that many simply formulated problems are actually undecidable. Our undecidability proofs are based on the fact that the so called Post Correspondence Problem is undecidable. This undecidable problem was introduced by E. Post [Pos] in 1946 and it is a very important problem in formal language theory. As we shall see, it is also suitable for our purposes in proving undecidability results. In the third chapter we study the existence of the zero matrix in matrix semigroups, i.e. the so called mortality problem. The proof of the undecidability of the mortality problem for  $3 \times 3$  matrices by M.S. Paterson [Pat] in 1970 provides a tool to prove other undecidability results for matrices. Paterson used the Post Correspondence Problem in his proof, and throughout this work we shall use the very same method.

We shall present a shorter and simplified proof for the undecidability of the mortality problem, however, using the same method than the original proof of Paterson.

We shall also consider the special case where the semigroup is generated by two matrices. It turns out that also in this case the mortality problem is undecidable if the dimension of the matrices is at least 45. This result is from [CKa].

In the third chapter we shall show that the method of Paterson does not suit for problems of  $2 \times 2$  matrices. This result is from [CHK]. It follows that for many problems, when we consider such matrices, it is not known whether they are decidable or not.

In the fourth chapter we study the freeness of matrix semigroups. This problem is important from the point of view of semigroup theory, especially for  $2 \times 2$  matrices. Results in that chapter is mainly from [CHK].

In the fifth chapter we consider the finiteness of matrix monoids. We will prove that it is decidable whether a matrix semigroup of matrices over natural numbers is finite or not. The proof we present is from [MaS]. The decidability of finiteness helps us also to prove some other simple properties of matrix semigroups generated by one matrix. These results are mentioned at the end of the chapter.

In the sixth chapter the existence of a zero in the right upper corner in a matrix semigroup is treated. We shall prove that this problem is undecidable for matrices with dimension at least 3. The proof we present is from [Man].

We shall also consider the case where semigroup is generated by two matrices and we prove that this problem is undecidable, when the dimension of the matrices is at least 24. This result is from [CKa].

In the seventh and eighth chapters we study the existence of a zero in the right upper corner in a matrix semigroup generated by one matrix. This problem is so called Skolem's problem. In the seventh chapter we will show that Skolem's problem is decidable for  $2 \times 2$  matrices. The proof we present is based on ideas of J. Cassaigne [Cas].

In the eighth chapter we will prove that it is decidable, whether there is infinite number of zeros in the right upper corner in the powers of one matrix. This proof, due to [Han], is elementary, but not simple and it uses the theory of rational series. The proof is based on so called Skolem's theorem. Results of rational series in that chapter is from [BeR].

We shall summarize the results of this work in the tenth chapter where a table of decidable and undecidable matrix problems is presented.

## 2 Preliminaries

#### 2.1 Basics

We shall denote the set of natural numbers by  $\mathbb{N}$ . It is assumed troughout this paper that zero is in  $\mathbb{N}$ , i.e.  $\mathbb{N} = \{0, 1, 2, ...\}$ . The sets of integers, rational numbers, real numbers and complex numbers are denoted by  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$  and  $\mathbb{C}$ , respectively.

#### 2.2 Semigroups and monoids

Let S be a set. A pair  $(S, \cdot)$  is called a *semigroup*, if  $\cdot$  is a binary operation such that, for all a, b and c in S,

$$a \cdot b \in S$$
 and  $(a \cdot b) \cdot c = a \cdot (b \cdot c).$ 

In other words  $\cdot$  is an associative operation in S. Usually the operation  $\cdot$  is called a *product* and the semigroup  $(S, \cdot)$  is denoted simply by S.

Semigroup S is called a *monoid*, if it has a *neutral* or *identity element*, i.e. there exists an element 1 in S such that for all a in S,

 $1 \cdot a = a \cdot 1 = a.$ 

Form now on, we denote  $ab = a \cdot b$  if no misunderstanding is possible.

A semigroup S is said to be *freely generated* and it is *free* if there exists subset X of S such that every element of S has a unique factorization over X, i.e. every element of S can be uniquely expressed as a product of elements of X. In this case the set X is called the *free generating set*.

A monoid M is said to be *free*, if  $M \setminus \{1\}$  is a free semigroup.

#### 2.3 Matrix semigroups and monoids

In this work we consider square matrices over integers, and in this section we shall recall some basic notations and properties of these matrices. As a general reference for matrix theory we give F.P. Gantmacher's book The Theory of Matrices [Gan].

The set of  $n \times n$  matrices over integers is denoted by  $\mathbb{Z}^{n \times n}$ , and n is called the *dimension*. Sometimes  $\mathbb{Z}$  is replaced by  $\mathbb{N}$  or by some other *semiring*. Recall that K is a semiring, if it has two operations, + and  $\cdot$ , satisfying the following properties:

- (i) (K, +) is a commutative monoid with 0 as its neutral element.
- (ii)  $(K \setminus \{0\}, \cdot)$  is a monoid with 1 as its neutral element.
- (iii) For all a, b, c in K, a(b+c) = ab + ac and (b+c)a = ba + ca.
- (iv) For all a in K, 0a = a0 = 0.

Let A be a matrix in  $K^{m \times n}$ . We denote the coefficient in the *i*'th row and on the *j*'th column of matrix A by  $A_{ij}$ , and, consequently, a matrix A is defined to be  $(A_{ij})_{m \times n}$ .

It is clear that  $(\mathbb{Z}^{n \times n}, \cdot)$  forms a monoid, where  $\cdot$  is the usual multiplication of matrices, i.e. if A and B are in  $\mathbb{Z}^{n \times n}$ , then

$$(A \cdot B)_{ij} = (AB)_{ij} = \sum_{k=1}^{n} A_{ik} B_{kj},$$

and the identity element is the *identity matrix* I (or  $I_n$ ),

$$I = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}_{n \times n}$$

We will denote this monoid by  $M_n(\mathbb{Z})$ . The above can be extended to other semirings than  $\mathbb{Z}$ , and the matrix monoid of  $n \times n$  matrices over semiring Kis denoted by  $M_n(K)$ .

We call a matrix P in  $M_n(\mathbb{N})$  a *permutation matrix*, if it is derived from  $I_n$  by mixing the rows (or columns) by some permutation. Clearly, if P is a permutation matrix, then each row and each column has 1 in exactly one position and in the other positions there are 0's. We denote

$$\delta_{ij} = \begin{cases} 1, & \text{if } i = j, \\ 0, & \text{otherwise.} \end{cases}$$

Clearly  $I_{ij} = \delta_{ij}$ , and if  $\pi$  is a permutation on the set  $\{1, \ldots, n\}$ , then P, for which  $P_{ij} = \delta_{i,\pi(j)}$ , is a permutation matrix. It is also easy to see that  $P^{-1} = \delta_{\pi(i),j}$ .

For a square matrix  $A = (A_{ij})_{n \times n}$  define the *determinant* of A by

$$\det(A) = \begin{vmatrix} A_{11} & A_{12} & \dots & A_{1n} \\ A_{21} & A_{22} & \dots & A_{2n} \\ \dots & \dots & \dots \\ A_{n1} & A_{n2} & \dots & A_{nn} \end{vmatrix}$$

$$= \sum_{\alpha} \operatorname{sign}(j_1, j_2, \dots, j_n) A_{1j_1} A_{2j_2} \cdots A_{nj_n},$$
(2.1)

where  $\alpha$  runs through the permutations on  $\{1, 2, ..., n\}$ ,  $\alpha = (j_1, j_2, ..., j_n)$ , and sign $(j_1, ..., j_n)$  is the *sign* of the permutation  $\alpha$ ,

$$\operatorname{sign}(j_1, j_2, \dots, j_n) = (-1)^{t(\alpha)},$$

where  $t(\alpha)$  is the number of inversions in  $\alpha$ , i.e the number of cases where  $j_l > j_k$  and l < k. Recall that in a permutation  $(j_1, \ldots, j_n)$  all  $j_i$ 's are different.

There are also some other methods than the sum (2.1) to calculate the determinant, but we will use the one in the definition.

Let A be an element of  $M_n(\mathbb{Q})$ . If det  $A \neq 0$ , we say that A is *invertible*, and it has the unique *inverse matrix*  $A^{-1}$  in  $M_n(\mathbb{Q})$  such that  $AA^{-1} = A^{-1}A = I$ . Note that if A is an element of  $\mathbb{Z}^{n \times n}$  and det $(A) \neq 0$ , then the inverse matrix of A is not necessarily an element of  $\mathbb{Z}^{n \times n}$ , but it is an element of  $\mathbb{Q}^{n \times n}$ .

The eigenvalue  $\lambda$  in  $\mathbb{C}$  and eigenvector  $\mathbf{x}$  in  $\mathbb{C}^n$ ,  $\mathbf{x} \neq (0, \ldots, 0)$ , of a matrix A in  $M_n(\mathbb{C})$  satisfy the condition

$$A\mathbf{x} = \lambda \mathbf{x},\tag{2.2}$$

where  $\mathbb{C}^n$  denotes as usual the *n* dimensional vector space over the complex numbers. The vector **x** can be understood also as an  $n \times 1$  matrix.

From the equation (2.2) it follows that the eigenvalue  $\lambda$  of A satisfies the equation

$$\det(A - \lambda I) = 0.$$

This equation is called the *characteristic equation* of the matrix A. The left hand side of this equation is so called *characteristic polynomial*, which is denoted by

$$c_A(\lambda) = (-1)^n (\lambda^n - c_1 \lambda^{n-1} + \cdots + (-1)^n c_n).$$

This polynomial has degree n, if A is in  $\mathbb{C}^{n \times n}$ , and the coefficients  $c_i$  are in  $\mathbb{C}$ . If  $\lambda'$  is an eigenvalue of A, we know that  $c_A(\lambda') = 0$ . Therefore, if we let the eigenvalues of A be  $\lambda_i$ ,  $i = 1, \ldots, n$ , it follows that

$$c_A(\lambda) = (-1)^n (\lambda - \lambda_1) (\lambda - \lambda_2) \cdots (\lambda - \lambda_n),$$

where the  $\lambda_i$ 's need not be different. Now we see that

$$c_n = \prod_{i=1}^n \lambda_i = c(0) = \det(A)$$
 and  $c_1 = \sum_{i=1}^n \lambda_i$ .

We call the sum of  $\lambda_i$ 's the *trace* of the matrix A, and denote it by tr(A).

Let p be a polynomial with coefficients in  $\mathbb{C}$ ,  $p(x) = c_1 x^k + c_2 x^{k-1} + \cdots + c_1$ . Then for a matrix A in  $M_n(\mathbb{Z})$  we define

$$p(A) = c_1 A^k + c_2 A^{k-1} + \dots + c_1 I.$$

Next we present the so called *Cayley–Hamilton* theorem. We do not present a proof here, a detailed proof can be found for example from [Gan].

**Theorem 2.1.** Let A be a square matrix and let  $c_A$  be its characteristic polynomial. Then

$$c_A(A) = 0,$$

where  $0 = (0)_{n \times n}$  is the zero matrix.

Note that since we are able to compute the determinant of a square matrix, we are also able to compute the characteristic polynomial of a square matrix.

We end this section with a notation for the *transpose matrix*  $A^T$  of A,  $(A^T)_{ij} = A_{ji}$ .

#### 2.4 Decidability and undecidability

Let P be a well-defined decision problem, i.e. a set of instances each of which either has or does not have a certain property. We say that the problem Pis *decidable*, if there exists an algorithm, which for every correct input or an instance of P terminates and gives an answer "yes", if the input has the required property and answers "no" otherwise. If no such algorithm exists, then P is called *undecidable*. To prove that the problem P is decidable, we must find an algorithm which decides P, or show that such an algorithm exists.

The usual method to prove the undecidability of a problem P is to reduce some already known undecidable problem Q to P. This means that, we transform effectively an arbitrary instance q of Q to some instance p of P, so that the condition "p has the property of P" is equivalent with the condition "q has the property of Q". It follows that if the problem P is decidable, then the instances q of the problem Q can be solved and therefore the problem Q is decidable, which leads to a contradiction. We shall use a classical undecidable problem, the *Post Correspondence Problem* or one of its modifications, in such reductions. These undecidable problems are introduced later in this chapter.

#### 2.5 Word monoids and morphisms

Let  $\Sigma$  be a finite set of symbols. We call  $\Sigma$  an *alphabet* and its elements are called *letters*. A finite sequence of letters is called a *word*. Denote by  $\Sigma^+$  the set of all words over  $\Sigma$ . The set  $\Sigma^+$  is a semigroup, the *word semigroup*, when the binary operation  $\cdot$  is defined as the *concatenation* of words, which means that, if  $w_1 = a_1 \dots a_n$  and  $w_2 = b_1 \dots b_m$  are in  $\Sigma^+$ , then

$$w_1 \cdot w_2 = a_1 \dots a_n b_1 \dots b_m.$$

The result of the catenation is clearly in  $\Sigma^+$  and it is an associative operation.

Let  $\epsilon$  be the *empty word* and  $\Sigma^* = \Sigma^+ \cup {\epsilon}$ . Clearly  $\Sigma^*$  is a free monoid generated by  $\Sigma$  and  $\epsilon$  is its identity element.

A subset of a word monoid is called a *language*.

Next we define a few properties of words. Let  $w = a_1 \dots a_n$  be a word in  $\Sigma^+$ , so  $a_i$  is in  $\Sigma$  for all  $1 \leq i \leq n$ . The *length* of the word w is n, and we denote it by |w| = n.

A word u in  $\Sigma^*$  is called a *prefix* of the word w, if there exists a word v in  $\Sigma^*$  such that w = uv. Then the word v is called a *suffix* of w.

A mapping h from a monoid  $M_1$  to a monoid  $M_2$  is called a *morphism* if, for all u and v in  $M_1$ , h satisfies the condition

$$h(uv) = h(u)h(v).$$

Note that in the right hand side of this equation the operation is the operation of the monoid  $M_2$ .

#### 2.6 The Post Correspondence Problem

We shall next study the *Post Correspondence Problem*, PCP for short, introduced by E. Post [Pos] in 1946.

Let h and g be two morphisms from  $\Sigma^*$  into  $\Delta^*$ . The equality set of h and g is the set

$$E(h,g) = \{ w \in \Sigma^+ \mid h(w) = g(w) \}$$

The Post Correspondence Problem asks to decide for a given pair (h, g) whether or not  $E(h, g) = \emptyset$ . Elements in E(h, g) are called *solutions* of the instance (h, g) of PCP.

This version of PCP is not the original version of the problem, but equivalent and more useful to our purposes.

The size of an instance (h, g) of PCP is defined to be the cardinality of the alphabet  $\Sigma$ . We denote by PCP(n) the subproblem of PCP for instances of size at most n.

The undecidability of PCP is a classical result in formal language theory, and it was first proved by Post in [Pos] in the general case, i.e. there does not exist any algorithm for solving all instances of PCP. It is also known that if  $n \leq 2$ , then PCP(n) is decidable, and if  $n \geq 7$  then it is undecidable. The proof of the undecidability of PCP(7) can be found from [MSe] and the proof of the decidability of PCP(n), for  $n \leq 2$ , can be found, for example, from [HaK]. For n greater than 2 and smaller than 7 the decidability status is open.

#### 2.7 The Mixed Modification of PCP

There exists many modifications of the Post Correspondence Problem, which have been proved to be undecidable. We shall next introduce one of these that is later used in the Chapter 4.

The mixed modification of PCP, MMPCP for short, asks to determine for two given morphisms  $h, g: \Sigma^* \to \Delta^*$  whether there exists a word  $w = a_1 \dots a_k$ with  $a_i$  in  $\Sigma$  and  $k \geq 1$ , such that

$$h_1(a_1)h_2(a_2)\dots h_k(a_k) = g_1(a_1)g_2(a_2)\dots g_k(a_k),$$
 (2.3)

where, for each i,  $h_i$  and  $g_i$  are in  $\{h, g\}$  and, for some j,  $h_j \neq g_j$ . The word w satisfying the equation (2.3) is called a *solution* of the instance (h, g) of MMPCP.

We show that MMPCP is undecidable. The proof is from [CHK], cf. also [HaK].

#### **Theorem 2.2.** *MMPCP is undecidable.*

*Proof.* We use the method, mentioned earlier in this chapter, to prove the undecidability. This requires to reduce PCP to MMPCP, that is, to transform an instance of PCP to that of MMPCP such that both of these have a solution simultaneously.

Let (h, g) be an instance of PCP and assume that  $h, g : \Sigma^* \to \Delta^*$  and that c, d and e are new letters not in  $\Sigma \cup \Delta$ . Further, let mappings  $l, r : \Delta^* \to (\Delta \cup \{d\})^*$  be morphisms defined as l(a) = da and r(a) = ad for all a in  $\Delta$ . Finally, for each a in  $\Delta$  we define two morphisms  $h_a, g_a : (\Sigma \cup \{d, e\})^* \to (\Delta \cup \{c, d, e\})^*$  by setting

$$h_a(x) = l(h(x)), \qquad g_a(x) = r(g(x)) \qquad \text{for all } x \in \Sigma,$$
  

$$h_a(d) = cl(h(a)), \qquad g_a(d) = cdr(g(a)),$$
  

$$h_a(e) = de, \qquad g_a(e) = e.$$

Next we show that the instance (h, g) of PCP has a solution aw, w in  $\Sigma^*$ , if and only if the instance  $(h_a, g_a)$  of PCP has a solution dwe. This follows from the equations

$$h_a(dwe) = cl(h(a))l(h(w))de = cl(h(aw))de$$

and

$$g_a(dwe) = cdr(g(a))r(g(w))e = cdr(g(aw))e.$$

Now, since the pair  $(h_a, g_a)$  can only have solutions of the form dwe, we conclude that it is undecidable whether for given morphisms  $h, g: \Sigma^* \to \Delta^*$  the instance  $(h_a, g_a)$  of PCP has a solution.

Finally we show that the pair  $(h_a, g_a)$ , as an instance of PCP, has a solution if and only if the same pair has a solution as an instance of MMPCP. To simplify notation we denote  $h = h_a$  and  $g = g_a$ .

If (h, g) has a solution as an instance of PCP, then it has a solution also as an instance of MMPCP, therefore the implication in one direction is clear. So assume that the pair (h, g) has a solution as an instance of MMPCP and let  $w = a_1 \dots a_k$  be a solution of minimal length. We claim that then also h(w) = g(w), i.e. w is a solution of instance (h, g) of PCP.

In notations of (2.3), the minimality of w implies that  $h_1 \neq g_1$  and  $h_k \neq g_k$ , so by the definitions of h and g,  $a_1 = d$  and  $a_k = e$ . We see also that  $a_i$ 

is not d or e if i = 2, ..., k - 1, because otherwise there would be a shorter solution than w. We may assume, by symmetry, that  $h_1 = h$  and  $g_1 = g$  and we will show that  $h_i = h$  and  $g_i = g$  for all i = 1, ..., k.

Assume the contrary. Then there must be the smallest t such that  $g_t = h$  or  $h_t = g$ . Consider the first alternative. Then we have

$$g(a_1 \dots a_{t-1})h(a_t) \in cd(\Sigma d)^+ (d\Sigma)^+,$$

and so there is a prefix in the right hand side of (2.3) that ends with dd. But no prefix of the left hand side of (2.3) matches with this prefix, because if  $h_i \neq g$  for all *i*, then  $h_1(a_1) \dots h_k(a_k) \in c(d\Sigma)^+$ , and if  $h_i = g$  for some *i*, then there is a prefix which is in  $c(d\Sigma)^+\Sigma$ . Therefore we do not get two *d*'s without having two consecutive letters of  $\Sigma$  first. This is a contradiction.

In the second alternative, similarly, we get that

$$h(a_1 \dots a_{t-1})g(a_t) \in c(d\Sigma)^+(\Sigma d)^+,$$

i.e. the left hand side of (2.3) has a prefix that ends with two consecutive letters of  $\Sigma$ . But no prefix of the right hand side of (2.3) matches with this prefix, because  $g(a_1) \dots g(a_k) \in cd(\Sigma d)^+$ , and if, for some  $i, g_i = h$ , then there is a prefix which is in  $cd(\Sigma d)^+(d\Sigma)^+$ . Therefore we cannot have two consecutive letters of  $\Sigma$  without having a factor dd first. This contradiction proves the claim.

We shall use MMPCP in the proof of the undecidability of the freeness of matrix monoids, for which it suits very well.

## **3** Mortality of Matrix Monoids

Let S be a given finitely generated submonoid of  $n \times n$  matrices from  $\mathbb{Z}^{n \times n}$ . 'Given' here means that we are given a finite generator set of S. In this section we consider the *mortality problem*, which is defined next.

**Problem 1.** Determine whether the zero matrix belongs to S. In other words, determine whether there exists a sequence of matrices  $M_1, M_2, \ldots, M_k$  in S such that  $M_1 M_2 \cdots M_k = 0$ .

#### 3.1 The undecidability of the mortality problem

We prove that the mortality problem is undecidable for  $3 \times 3$  matrices. This result was first proved by M.S. Paterson in 1970 [Pat]. He used clever coding techniques to make a reduction to PCP. We use the same method, but our proof itself is simpler, althought the idea remains the same.

The basic idea of the proof is to reduce an instance of PCP to the mortality problem. Let  $\Gamma$  be an alphabet. We use an injective morphism from  $\Gamma^* \times \Gamma^*$  into  $\mathbb{N}^{3\times 3}$  to represent a pair of words in the multiplicative monoid of matrices. Then, of course, the product of matrices representing pairs (u, v)and (u', v') represents pair the (uu', vv').

First we define notions needed in the proof. Let  $\Gamma = \{a_1, a_2, ..., a_n\}$  and define a function  $\sigma : \Gamma^* \to \mathbb{N}$  by

$$\sigma(a_{i_1}a_{i_2}...a_{i_k}) = \sum_{j=1}^k i_j n^{k-j}$$
 and  $\sigma(\epsilon) = 0.$ 

We see that, for each word w, the function  $\sigma$  gives the value which w represents as an *n*-adic number, and because each natural number has a unique *n*-adic representation,  $\sigma$  must be injective. We also note that, for all u and v in  $\Gamma^*$ ,

$$\sigma(uv) = n^{|v|}\sigma(u) + \sigma(v). \tag{3.1}$$

Next define a mapping  $\beta: \Gamma^* \to \mathbb{N}^{2 \times 2}$  by

$$\beta(a_i) = \begin{pmatrix} n & 0\\ i & 1 \end{pmatrix},$$

for all i = 1, 2, ..., n. Now if  $i, j \in \{1, ..., n\}$ , we get that

$$\beta(a_i)\beta(a_j) = \begin{pmatrix} n & 0\\ i & 1 \end{pmatrix} \begin{pmatrix} n & 0\\ j & 1 \end{pmatrix}$$
$$= \begin{pmatrix} n^2 & 0\\ ni+j & 1 \end{pmatrix} = \begin{pmatrix} n^{|a_ia_j|} & 0\\ \sigma(a_ia_j) & 1 \end{pmatrix}.$$

Clearly this can be extended for all  $w \in \Gamma^*$ , and therefore

$$\beta(w) = \begin{pmatrix} n^{|w|} & 0\\ \sigma(w) & 1 \end{pmatrix}$$

•

This can be proved by induction. We note that  $\beta$  is a morphism from  $\Gamma^*$  into  $\mathbb{N}^{2\times 2}$ , since if u and v are in  $\Gamma^*$ , then

$$\beta(u)\beta(v) = \begin{pmatrix} n^{|u|} & 0\\ \sigma(u) & 1 \end{pmatrix} = \begin{pmatrix} n^{|v|} & 0\\ \sigma(v) & 1 \end{pmatrix} = \begin{pmatrix} n^{|u|}n^{|v|} & 0\\ \sigma(u)n^{|v|} + \sigma(v) & 1 \end{pmatrix} = \begin{pmatrix} n^{|uv|} & 0\\ \sigma(uv) & 1 \end{pmatrix} = \beta(uv)$$

 $\beta$  is also injective, because  $\sigma$  is injective and  $\sigma(w)$  is the (2, 1)-entry of the matrix  $\beta(w)$ .

Next we define a monoid morphism  $\gamma : \Gamma^* \times \Gamma^* \to \mathbb{N}^{3\times 3}$ , where two copies of  $\beta$  is applied simultaneously in  $3 \times 3$  matrices,

$$\gamma(u,v) = \begin{pmatrix} n^{|u|} & 0 & 0\\ 0 & n^{|v|} & 0\\ \sigma(u) & \sigma(v) & 1 \end{pmatrix}.$$
 (3.2)

The fact that  $\gamma$  is a morphism follows from the fact that  $\beta$  is a morphism. The morphism  $\gamma$  is also *doubly injective*, which means that, if  $\gamma(u_1, v_1)_{31} = \gamma(u_2, v_2)_{31}$ , then  $u_1 = u_2$ , and if  $\gamma(u_1, v_1)_{32} = \gamma(u_2, v_2)_{32}$ , then  $v_1 = v_2$ . Notice also that for the empty word  $\epsilon$  we have  $\gamma(\epsilon, \epsilon) = I_3$ .

We are now ready to prove the undecidability result.

**Theorem 3.1.** The mortality problem is undecidable for  $3 \times 3$ -matrices with integer entries.

*Proof.* First define matrix A,

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

Let Y be the set of matrices

$$W(p,q,r,s) = \begin{pmatrix} p & 0 & 0\\ 0 & r & 0\\ q & s & 1 \end{pmatrix}, \text{ where } p,r > 0, q, s \ge 0,$$

and p, q, s and r are integers. If B and C are in Y, say

$$B = W(p_1, q_1, r_1, s_1)$$
 and  $C = W(p_2, q_2, r_2, s_2),$ 

then

$$BC = \begin{pmatrix} p_1 p_2 & 0 & 0\\ 0 & r_1 r_2 & 0\\ q_1 p_2 + q_2 & s_1 r_2 + s_2 & 1 \end{pmatrix} = W(p_1 p_2, q_1 p_2 + q_2, r_1 r_2, s_1 r_2 + s_2),$$

then clearly BC is in Y. Since also I is in Y, Y is a monoid.

Let L be a finitely generated submonoid of Y and S be the matrix monoid generated by  $\{A\} \cup L$ .

We notice that  $A^2 = A$ , i.e. A is an *idempotent*, and that for all W(p,q,r,s) in L,

$$AW(p,q,r,s)A = (p+q-s)A.$$
 (3.3)

Next we show that

$$0 \in S \iff \exists W \in L : AWA = 0. \tag{3.4}$$

The reverse implication is trivial, because if AWA = 0 for some  $W \in L$ , then  $0 \in S$ .

Assume now that  $0 \in S$ . Since  $0 \notin L$  and for all  $k \geq 1$ ,  $A^k = A$ , there must be product

$$AW_1 A W_2 A \cdots A W_t A = 0 \tag{3.5}$$

for some  $t \ge 1$  and  $W_j \in L$ , for all j = 1, ..., t. If we assume that t > 1 and that t is minimal, then, because A is an idempotent, we have

$$AW_1A \cdot AW_2A \cdots AW_tA = 0.$$

Now by equation (3.3) we get that, for some integer m,

$$mAW_2A\cdots AW_tA=0.$$

Now we have two cases; if m = 0, then  $AW_1A = 0$ , and if  $m \neq 0$ , then t is not a minimal. Both of these cases lead to a contradiction with the minimality of t and therefore there exists W in L, such that AWA = 0.

Next we reduce an instance of PCP to the mortality problem using mapping  $\gamma$  from  $\Gamma^* \times \Gamma^*$  into  $\mathbb{N}^{3\times 3}$  as defined in (3.2). Assume that  $\Gamma = \{a_1, a_2, a_3\}$ , so that n = 3. Let (h, g) be an instance of PCP, where  $h, g : \Sigma^* \to \Delta^*$  and  $\Delta = \{a_2, a_3\}$ . Define the matrices

$$W_a = \gamma(h(a), g(a)) \quad \text{and} \quad W'_a = \gamma(h(a), a_1 g(a)) \tag{3.6}$$

for all  $a \in \Sigma$ . Clearly, these matrices  $W_a$  and  $W'_a$  are in Y. Let L be the set of all matrices  $W_a$  and  $W'_a$ , where  $a \in \Sigma$ . Consider now a matrix monoid S generated by  $\{A\} \cup L$ . By the claim (3.4), S is mortal if and only if there is a matrix W generated by matrices of L such that AWA = 0. From the definition (3.6), and from the properties of the morphism  $\gamma$ , it follows that W is of the form

$$W = \begin{pmatrix} 3^{|u|} & 0 & 0\\ 0 & 3^{|v|} & 0\\ \sigma(u) & \sigma(v) & 1 \end{pmatrix},$$

where u is in  $\Delta^*$  and v in  $\Gamma^*$ . By (3.3) we have to analyse the condition

$$3^{|u|} + \sigma(u) - \sigma(v) = 0.$$

This is, by the property (3.1) of  $\sigma$ , equivalent to the equation  $v = a_1 u$ . Because  $u = h(w) \in \Delta^*$  and  $a_1 \notin \Delta$ , we must have

$$W = W'_{w_1} W_{w_2} \cdots W_{w_n}$$

where  $w_i$ 's are in  $\Sigma$  and  $w = w_1 \cdots w_n$ . This is equivalent to the condition

$$v = a_1 g(w) = a_1 h(w).$$

Therefore S is mortal if and only if the instance (h, g) of PCP has a solution, and this proves the claim.

This proof works also for  $n \times n$  matrices where n > 3. We just add zero columns to the right hand side and zero rows to the bottom of all matrices in the proof of Theorem 3.1 to get  $n \times n$  matrices. The products of these new matrices depend only on product of original  $3 \times 3$  matrices.

**Corollary 3.1.** The mortality problem is undecidable for  $n \times n$  matrices with integer entries and  $n \geq 3$ .

As mentioned before, the idea of the proof of Theorem 3.1 is the same as in the original proof by Paterson. We used only one special matrix A when Paterson had two of them. Also, by the choice of this A, we managed to simplify some details in the proof.

As mentioned before the PCP(7) is proved to be undecidable in [MSe]. Therefore the size of the alphabet  $\Sigma$  in the proof can be set to be seven and therefore we need 15 matrices in that proof.

#### 3.2 The mortality of semigroups with two generators

In this section we consider the mortality problem in the case, where the semigroup is generated by only two matrices with integer entries. We shall show that this problem is undecidable. The proof is based on Theorem 3.1 and on a simple trick to represent a matrix semigroup with k generators of dimension n in a semigroup with only two generators of dimension nk. The proof of the following theorem is from [CKa].

**Theorem 3.2.** Given two square matrices A and B with integer entries, it is undecidable whether the semigroup generated by  $\{A, B\}$  contains the zero matrix.

*Proof.* By Theorem 3.1 we know that the presence of the zero matrix is undecidable for a semigroup T generated by  $M_1, \ldots, M_k$  with dimension n = 3, where k = 15. We shall construct two matrices A and B of dimension nk such that the semigroup S generated by  $\{A, B\}$  contains the zero matrix if and only if T contains it. Since an algorithm to decide this property for S could then be turned into an algorithm for any finitely generated semigroup, also for T, this shows that the problem is undecidable.

The construction is quite simple. A and B are defined with  $n \times n$  blocks, using the matrices  $M_i$ , the  $n \times n$  identity I and the  $n \times n$  zero. A is a block diagonal and B is a permutation matrix:

$$A = \begin{pmatrix} M_1 & 0 & \cdots & 0 \\ 0 & M_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & M_k \end{pmatrix} \text{ and } B = \begin{pmatrix} 0 & 0 & \cdots & 0 & I \\ I & 0 & 0 & \cdots & 0 \\ 0 & I & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & I & 0 \end{pmatrix}$$

It is quite clear that  $B^{-1} = B^{k-1} = B^T$  and that  $B^k = I_{nk}$ . We shall prove next that for any index  $1 \le i \le k$ , the element  $C_i = B^{k-i+1}AB^{i-1}$  is a block diagonal like A, but with the blocks circularly permuted, namely its diagonal is  $M_i, M_{i+1}, \ldots, M_k, M_1, \ldots, M_{i-1}$ . The proof is by induction on i.

First, if i = 1, then  $C_1 = B^{k-1+1}AB^{1-1} = B^kAI = IAI = A$ .

Assume now that there exists i such that the claim holds for all  $t, 1 \leq t \leq i < n$ . Then  $C_{i+1} = B^{k-(i+1)+1}AB^{i+1-1} = B^{-1}C_iB$ , and

$$B^{-1}C_{i}B = B^{T} \begin{pmatrix} 0 & 0 & \cdots & 0 & M_{i} \\ M_{i+1} & 0 & 0 & \cdots & 0 \\ 0 & M_{i+2} & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & M_{i-1} & 0 \end{pmatrix}$$
$$= \begin{pmatrix} M_{i+1} & 0 & \cdots & 0 \\ 0 & M_{i+2} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & M_{i} \end{pmatrix}.$$

So  $C_{i+1}$  is of the required form.

Using the relation  $B^k = I_{nk}$ , any element of the semigroup S can be written in the form  $B^tC_{i_1}C_{i_2}\cdots C_{i_m}$  with  $m \ge 0$ . Therefore, if we assume that the zero matrix is in S, we have  $C_{i_1}C_{i_2}\cdots C_{i_m} = 0$ , since Bis invertible. Now the left upper block of the product  $C_{i_1}C_{i_2}\cdots C_{i_m}$  is  $0 = M_{i_1}M_{i_2}\cdots M_{i_m}$ , which means that the zero matrix is in T. Conversely, assume that T contains the zero matrix and that  $M_{i_1}M_{i_2}\cdots M_{i_m} = 0$ . Let  $D_j = C_{i_1-j+1}C_{i_2-j+1}\cdots C_{i_m-j+1}$  for  $1 \le j \le k$ , where the indices are taken modulo k. The matrix  $D_j$  is block diagonal and its j'th diagonal block is  $M_{i_1}M_{i_2}\cdots M_{i_m} = 0$ . Therefore, the product  $D_1D_2\cdots D_k$ , which is an element of S, is the zero matrix.

It follows from the previous theorem that the mortality problem is undecidable for semigroups generated by two matrices, if the dimension of the matrices is at least  $3 \cdot 15 = 45$ .

We shall return to the question of the mortality of semigroups generated by two matrices in the Chapter 7, where this problem is shown to be decidable for  $2 \times 2$  matrices.

## 3.3 The existence of the zero element in matrix semigroups

In the two previous sections we considered the existence of the zero matrix in a finitely generated matrix semigroup. In this section we consider the existence of the zero element in a matrix semigroup, i.e. the existence of an element x in a semigroup S such that, for all a in S, xa = ax = x. Clearly, if a matrix semigroup S contains the zero matrix, then it has also a zero element.

We shall show in this section that also the existence of the zero element is an undecidable property. We begin with an easy semigroup theoretical lemma.

**Lemma 3.1.** The zero element in a semigroup is unique.

*Proof.* Let  $(S, \cdot)$  be a semigroup and to the contrary that S contains two zero elements, say  $x_1$  and  $x_2$ . Then by the definition of a zero element  $x_1 = x_1 \cdot x_2 = x_2$ .

Next theorem is obvious after the previous lemma.

**Theorem 3.3.** For  $n \ge 3$ , it is undecidable whether a given finitely generated matrix semigroup of  $n \times n$  matrices with integer entries contains the zero element.

*Proof.* Assume that the matrices  $M_1, \ldots, M_k$  are the given generator matrices of the semigroup. Assume to the contrary that it is decidable whether S contains a zero element. Then we can also decide whether the zero matrix is in S. This follows, since if there does not exist a zero element in S, then the zero matrix is not in S either, and if there exists a zero element, we check all the elements in S until we find it. The checking is easy to do, since X is a zero element if and only if

$$M_1X = \cdots = M_kX = X = XM_1 = \cdots = XM_k.$$

Now when we find the zero element, we check if it is the zero matrix or not. Hence, indeed, we can decide whether S contains the zero matrix, a contradiction with Theorem 3.1.

#### 3.4 The mortality problem in dimension two

It is clear that for  $1 \times 1$  matrices the mortality problem is decidable. The only possibility to have the zero matrix in S is that it is one of the generators.

What can we say about the problem for  $2 \times 2$  matrices  $\Gamma$  Not much, because it is not known whether the mortality problem is decidable or undecidable for  $2 \times 2$  matrices in the case, where we have more than two generators. As we mentioned before, it can be proved decidable in two generator case. This proof is presented in Chapter 7.

One thing we can say is that if the mortality problem for  $2 \times 2$  matrices with arbitrary many generators is undecidable, then it must be proved with some other techniques than the undecidability for  $3 \times 3$  matrices, because that proof was based on the injective morphism from  $\Sigma^* \times \Sigma^*$  into  $\mathbb{N}^{3\times 3}$ , and there is no such morphism into  $\mathbb{N}^{2\times 2}$ . We shall now prove this fact, but before that, we prove a lemma concerning the commutation of certain special  $2 \times 2$ matrices.

**Lemma 3.2.** Let A be an upper triangular  $2 \times 2$  matrix over  $\mathbb{C}$ .

1) If  $A = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$ , where  $b \neq 0$ , then for all matrices  $B \in \mathbb{C}^{2 \times 2}$ , AB = BA if and only if  $B = \begin{pmatrix} e & f \\ 0 & e \end{pmatrix}$ . 2) If  $A = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$ , where  $a \neq d$ , then for all  $B \in \mathbb{C}^{2 \times 2}$ , AB = BA if and only if  $B = \begin{pmatrix} e & 0 \\ 0 & h \end{pmatrix}$ .

*Proof.* 1) Assume that  $B = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$  and that AB = BA. These imply that  $(AB)_{11} = ae + bg = ae = (BA)_{11}$  and therefore g = 0. Now we see that  $(AB)_{12} = af + bh = eb + fa = (BA)_{12}$ , so h = e. Clearly also  $(AB)_{21} = 0 = (BA)_{21}$  and  $(AB)_{22} = ae = (BA)_{22}$ . This shows that if B commutes with A it is of the required form, and conversily.

2) Assume that  $B = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$  and that AB = BA. Then  $(AB)_{12} = af = fd = (BA)_{11}$ , and since  $a \neq d$ , it follows that f = 0. Also  $(AB)_{21} = dg = ga = (BA)_{21}$ , so g = 0 and we are done, since the other direction is obvious.

The reason we need the previous lemma is that we use in the next proof the existence of so called *Jordan normal form* of square matrices. The Jordan normal form J of a matrix A in  $\mathbb{Z}^{n \times n}$  is an upper triangular matrix, which is *similar* to A, that is, there exists an invertible matrix P in  $\mathbb{C}^{n \times n}$  such that,  $A = PJP^{-1}$ . The diagonal of J consists of the eigenvalues of A.

For a matrix A in  $\mathbb{Z}^{2\times 2}$ , the Jordan normal form has two possibilities:

- 1) If A has two different eigenvalues, say  $\lambda$  and  $\mu$ , then  $J = \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$ .
- 2) If A has only one eigenvalue, say  $\lambda$ , then then  $J = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$  or

$$J = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}.$$

For the proof of these facts we refer to [Gan].

The next theorem shows that there is no injective morphism from  $\Sigma^* \times \Sigma^*$ into  $\mathbb{C}^{2\times 2}$ . Actually we need this property only for morphisms into  $\mathbb{N}^{2\times 2}$ , but we use  $\mathbb{C}^{2\times 2}$  here, because in the proof we need the Jordan normal form of matrices, which is in  $\mathbb{C}^{2\times 2}$ , since the eigenvalues are in  $\mathbb{C}$ .

Now we are ready for the theorem, the proof of it being from [CHK].

**Theorem 3.4.** There is no injective morphism

$$\phi: \Sigma^* \times \Sigma^* \to \mathbb{C}^{2 \times 2}$$

for any alphabet  $\Sigma$  with at least two elements.

*Proof.* It is sufficient to prove the theorem in the case where  $\Sigma = \{0, 1\}$ . In this case the monoid  $S = \Sigma^* \times \Sigma^*$  has a generating set

$$L = \{ (0, \epsilon), (1, \epsilon), (\epsilon, 0), (\epsilon, 1), (\epsilon, \epsilon) \},\$$

where  $\epsilon$  is the empty word. To simplify the notations we set  $a = (0, \epsilon)$ ,  $b = (1, \epsilon)$ ,  $c = (\epsilon, 0)$ ,  $d = (\epsilon, 1)$  and  $e = (\epsilon, \epsilon)$ .

Assume to the contrary that there is an injective morphism  $\phi$  from S into  $\mathbb{C}^{2\times 2}$ , and let  $A = \phi(a)$ ,  $B = \phi(b)$ ,  $C = \phi(c)$ ,  $D = \phi(d)$ , and  $E = \phi(e)$ . Since the conjugation by an invertible matrix does not influence the injectivity, we can suppose that A is in the Jordan normal form.

Suppose that A has two different eigenvalues. Then  $A = \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$ , and the matrices commuting with A are exactly the diagonal matrices by Lemma 3.2. Therefore C and D must be diagonal, since ac = ca and ad = da in

S. It follows that also matrices C and D commute, which contradicts the injectivity, since c and d do not commute in S.

If A has only one eigenvalue, then  $A = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$  or  $A = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$ . The first case is impossible, because then  $A = \lambda I$  commutes with all matrices, especially with B, but b and a do not commute in S. In the second case A would commute only with the matrices of the form  $\begin{pmatrix} x & y \\ 0 & x \end{pmatrix}$  by Lemma 3.2, and they commute with each others, which yields a contradiction as above.

The mortality of  $2 \times 2$  matrices is also connected to other branches of mathematics, cf. [Sch].

We end this chapter by showing that the mortality problem is decidable for the  $2 \times 2$  upper triangular matrices. This special case is not very important and it does not say anything about the general case.

**Theorem 3.5.** Let L be a set of  $2 \times 2$  upper triangular matrices with integer entries. Then the zero matrix belongs to the semigroup generated by L if and only if there are matrices A and B in L such that

$$A_{11} = 0$$
 and  $B_{22} = 0$ .

*Proof.* Let A and B be  $2 \times 2$  upper triangular matrices,

$$A = \begin{pmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{pmatrix}$$
 and  $B = \begin{pmatrix} b_{11} & b_{12} \\ 0 & b_{22} \end{pmatrix}$ .

Then

$$AB = \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} + a_{12}b_{22} \\ 0 & a_{22}b_{22} \end{pmatrix}.$$

We see that the product is also an upper triangular matrix. To get zeros to the diagonal, necessarily either  $a_{11}$  or  $b_{11}$  equals with the zero and either  $a_{22}$  or  $b_{22}$  equals with the zero. So we have four cases, but, by symmetry, it is enough to consider only two of those. First, if  $a_{11} = a_{22} = 0$ , then AA = 0. The second case is that  $a_{11} = b_{22} = 0$ , and then AB = 0. Both directions of the equivalence follow from this.

## 4 Freeness of Matrix Semigroups

In this chapter we concentrate on the freeness property of semigroups which is one of the fundamental properties of semigroups and monoids.

Recall that a semigroup S is said to be free if there exists a subset X of S such that every element of S has a unique factorization over X, i.e. every element of S can be uniquely expressed as a product of elements of X. The results in this chapter also concern monoids, because a monoid M is said to be free if  $M \setminus \{1\}$  is a free semigroup.

Next we define the freeness problem for square matrices.

**Problem 2.** Determine whether a given finitely generated semigroup of  $n \times n$  matrices with non-negative integer entries is free?

As in the case of the mortality problem, we first prove that this problem is undecidable for  $3 \times 3$  matrices, and therefore also for all  $n \times n$  matrices, where  $n \geq 3$ . After that we consider the case of  $2 \times 2$  matrices.

In the final section of this chapter we prove that it is undecidable, whether two matrix semigroups have an equal element.

#### 4.1 The undecidability of the freeness

We shall now prove that the freeness problem is undecidable for  $3 \times 3$  matrices. This result was first proved by Klarner, Birget and Satterfield [KBS] in 1990, but we will present a proof which was developed by J. Cassaigne, T. Harju and J. Karhumäki [CHK]. This proof is shorter and also gives a better bound for the number of matrices.

The proof uses the same techniques than the proof of the mortality problem, but instead of an instance of PCP we will reduce an instance of MMPCP to this problem.

Assume that  $\Sigma$  is an alphabet,  $\Sigma = \{a_1, \ldots, a_n\}$ , and let function  $\sigma$ :  $\Sigma^* \to \mathbb{N}$  correspond a value of word as an *n*-adic representation as in the mortality chapter. We now define a mapping  $\gamma_1 : \Sigma^* \times \Sigma^* \to \mathbb{N}^{3 \times 3}$  by setting

$$\gamma_1(u,v) = (\gamma(u,v))^T = \begin{pmatrix} n^{|u|} & 0 & \sigma(u) \\ 0 & n^{|v|} & \sigma(v) \\ 0 & 0 & 1 \end{pmatrix},$$

where  $\gamma$  is the injective morphism defined in Section 3.1. Clearly also  $\gamma_1$  is a doubly injective morphism.

**Theorem 4.1.** It is undecidable whether a semigroup generated by finite set of upper-triangular  $3 \times 3$  matrices of non-negative integers is free.

*Proof.* Let (h, g) be an instance of MMPCP. Of course, we may assume that h and g are morphism from  $\Sigma^*$  into  $\Sigma^*$  i.e. they are endomorphisms. Next define the set

$$M = \{\gamma_1(a, h(a)), \gamma_1(a, g(a)) \mid a \in \Sigma\}$$

and let S be the semigroup generated by M.

Let  $\alpha_{i_1}, \ldots, \alpha_{i_p}, \beta_{j_1}, \ldots, \beta_{j_q}$  be in M,  $\alpha_{i_t} = \gamma_1(a_{i_t}, h_{i_t}(a_{i_t}))$  and  $\beta_{j_s} = \gamma_1(b_{j_s}, g_{j_s}(b_{j_s}))$ , with  $h_{i_t}$  and  $g_{j_s}$  in  $\{h, g\}$  and  $a_{i_t}$  and  $b_{j_s}$  in  $\Sigma$ , for  $t = 1, \ldots, p$  and  $s = 1, \ldots, q$ . Then, by the definition of  $\gamma_1$  (and  $\gamma$ ), we have:

$$\alpha_{i_1} \dots \alpha_{i_p} = \beta_{j_1} \dots \beta_{j_q}$$
 in S

if and only if

$$(\alpha_{i_1} \dots \alpha_{i_p})_{1,3} = (\beta_{j_1} \dots \beta_{j_q})_{1,3}$$
 and  $(\alpha_{i_1} \dots \alpha_{i_p})_{2,3} = (\beta_{j_1} \dots \beta_{j_q})_{2,3}$ 

But this is equivalent to

$$a_{i_1} \dots a_{i_p} = b_{j_1} \dots b_{j_q}$$
 and  $h_{i_1}(a_{i_1}) \dots h_{i_p}(a_{i_p}) = g_{j_1}(b_{j_1}) \dots g_{j_q}(b_{j_q})$ 

by the uniqueness of the n-adic representations.

We have proved that S is nonfree if and only if the instance (h, g) of MMPCP has a solution. Hence the nonfreeness, and so also the freeness, is an undecidable property.

We could have used also the morphism  $\gamma$  itself in the above proof but we prefered to formulate the result for upper triangular matrices. This is the first reason that this proof is better than the proof of Klarner, Birget and Satterfield [KBS]. The second reason is that they needed 29 matrices when we needed only 18, assuming that in the PCP we consider instances over 7 letter domain alphabet, as can be done, cf. [MSe] - in the undecidability proof of the MMPCP we added two letters to this alphabet.

The next corollary is clear by extending the matrices in the above proof in an obvious way.

**Corollary 4.1.** The freeness problem is undecidable for  $n \times n$  upper triangular matrices with non-negative integer entries for any  $n \geq 3$ .

#### 4.2 The freeness problem in dimension two

As in the case of the mortality problem, it is not known whether the freeness problem is decidable or undecidable in the case of  $2 \times 2$ -matrices. But, again, we know that if it is undecidable, it cannot be proved using a construction similar to the one used for  $3 \times 3$ -matrices. This is due to Theorem 3.4.

In the theory of semigroups, it is known that every finitely generated free semigroup is isomorphic to some free word semigroup  $\Sigma_k^+$ , where k is the number of letters in the alphabet  $\Sigma$ . It is also known that every free semigroup  $\Sigma_k^+$  can be embedded into the semigroup of 2 × 2-matrices over nonnegative integer, i.e. into  $\mathbb{N}^{2\times 2}$ . Such embeddings can be done in many different ways. For example, if  $\Sigma_k = \{a_0, a_1, \ldots, a_{k-1}\}$ , then the morphism defined by

$$a_i \mapsto \begin{pmatrix} k & i \\ 0 & 1 \end{pmatrix}$$

is one such embedding. Another one is the embedding  $\beta$  defined in the chapter considering the mortality problem, Chapter 3.

It is known that it is decidable whether a finite set of words is a free generating set, i.e. whether a semigroup generated by a finite set of words is free, cf. [BeP]. Therefore it is natural to ask, whether the freeness problem is decidable for the  $2 \times 2$  matrices over nonnegative integers. This problem seems to be very difficult. Indeed, in [CHK] Cassaigne, Harju and Karhumäki considered a restricted case, where the semigroup is generated by two upper triangular  $2 \times 2$  matrices over  $\mathbb{Q}$ , but even in this case, no general method for deciding the freeness was found.

#### 4.3 Common elements in semigroups

In this section we consider the existence of a common element in two matrix semigroups.

**Problem 3.** Given two finitely generated subsemigroups of  $M_n(\mathbb{Z})$ , say M and N, determine whether there exists a matrix X, which is both in M and in N.

Here 'given' means again that we are given the generators of M and N.

The existence of a common element is actually an independent problem and it is not connected to the freeness problem, but we present it here, since in the proof of the undecidability we use the same mapping  $\gamma_1$  as defined earlier in this chapter.

M. Krom considered a variant of this problem in [Kro]. He asked, whether there exists a matrix X in both M and N such that X is a product of equally many generators of both M and N. We shall prove that the problem of equal element is undecidable, if  $n \geq 3$ , and the proof we present suits also for the variant of Krom.

**Theorem 4.2.** It is undecidable whether two finitely generated subsemigroups of  $M_3(\mathbb{Z})$  have a common element.

*Proof.* Let (h, g) be an instance of PCP, where h and g are morphism from  $\Sigma^*$  into  $\Delta^*$ . Assume that  $\Delta \subseteq \Sigma$  and let  $\gamma_1$  be the morphism defined in Section 4.1. Now let  $S_H$  and  $S_G$  be two semigroups generated by the matrices  $H_a = \gamma_1(a, h(a))$  and  $G_a = \gamma_1(a, g(a))$  for all a in  $\Sigma$ , respectively.

Since  $\gamma_1$  is doubly injective, we get that

$$H_{a_1}\cdots H_{a_k}=G_{b_1}\cdots G_{b_t}$$

if and only if

$$a_1 \dots a_k = b_1 \dots b_t$$
 and  $h(a_1) \dots h(a_k) = g(b_1) \dots g(b_t)$ .

Therefore the claim follows from the undecidability of the PCP.

Clearly this proof works for the variant of Krom, since in the proof neccessarily k = t.

## 5 Finiteness of Matrix Semigroups

We are given a finitely generated subsemigroup S of  $\mathbb{N}^{n \times n}$ , i.e. we are given the generator matrices of S. In this chapter we consider the problem which asks:

**Problem 4.** Determine whether the semigroup S is finite or not?

We show that this problem is decidable by showing that, if S is finite, then an upper bound of the cardinality of S can be computed.

Natural extensions of the finiteness problem are the ones considering semigroups of matrices over the rational numbers  $\mathbb{Q}$  and, in general, over any field. Also these extensions can be proved to be decidable, cf. [MaS].

Our proofs and notions are from the article [MaS] by A. Mandel and I. Simon in 1977. At the end of this chapter we mention also some other results which give better upper bounds than the bound proved here.

#### 5.1 The decidability of the finiteness

As mentioned above, we shall show that there exists an upper bound for the cardinality of a finite subsemigroup of  $\mathbb{N}^{n \times n}$ , which depends on n and on the number of generators of the semigroup. The proof we present is a combinatorial one. First we need some new definitions.

Let S be a semigroup. An element a of S is called a *torsion* (or periodic), if  $a^p = a^q$  for some natural numbers p < q. If every element of S is a torsion, then S is a *torsion semigroup* (or a periodic semigroup).

Note that a matrix A from  $M(\mathbb{N})$  is torsion if and only if there exists a natural number m, such that  $(A^r)_{ij} \leq m$  for all r.

We need also the next theorem, which is a classical result of Ramsey [Ram].

**Theorem 5.1.** Given natural numbers m, n and k such that  $m \ge 2$  and  $n \ge k \ge 1$ , then there exist a natural number R(m, n, k) such that for every set X of cardinality at least R(m, n, k) and every partition of k element subsets of X into m blocks, there exists a subset Y of X, with the cardinality n, such that all k element subsets of Y belong to the same block.

Ramsey's theorem has many equivalent formulations and there exists a branch in combinatorics, namely The Ramsey Theory, which is based on this theorem, cf. [GRS].

Next we define a graph representation of a matrix in  $M_n(\mathbb{N})$ . For a given A in  $M_n(\mathbb{N})$ , we define a graph  $G_A$  to have a vertex set  $V = \mathbf{n} = \{1, \ldots, n\}$  and an edge set E, such that, there is a directed edge from i to j in E with label  $A_{ij}$ , whenever  $A_{ij} \neq 0$ . For an edge e, we denote its label by  $\rho(e)$ . For a walk  $T = (i_0, e_1, i_1, \ldots, e_r, i_r)$  in  $G_A$ , where  $i_j$ 's are vertices, and  $e_i$  is an edge from  $i_{j-1}$  to  $i_j$ , we define the label  $\rho(T)$  to be  $\prod_{j=1}^r \rho(e_j)$ . We say that the length of T is r.

The next lemma follows from the above definitions.

**Lemma 5.1.** Assume that A is in  $M_n(\mathbb{N})$ . For all r in  $\mathbb{N}$ ,  $(A^r)_{ij}$  is the sum of the labels of the length r walks from i to j in  $G_A$ .

*Proof.* We prove this by induction on r.

If r = 1, then this is clear by the definition of  $G_A$ .

Assume that for some  $k \geq 1$ , the claim holds, whenever  $r \leq k$ . This means that for all *i* and *j*,  $(A^r)_{ij}$  is the sum of the labels of all walks from *i* to *j* of length *r*. Now

$$(A^{k+1})_{ij} = (A \cdot A^k)_{ij} = \sum_{h=1}^k A_{ih}(A^k)_{hj},$$

which is the sum of all labels of walks of length k + 1 from i to j.

Before our next lemma we define one more property of graphs. Let G be a directed graph, G = (V, E), where V is the set of vertices and E is the set of directed edges. Then a subgraph H of G,  $H = (V_H, E_H)$ , where  $V_H \subseteq V$ and  $E_H \subseteq E$ , is called a *strong component of* G, if for all i and j in  $V_H$ , there is a directed path (or walk) from i to j and from j to i.

**Lemma 5.2.** Let A be a matrix in  $M_n(\mathbb{N})$ . Then the following statements are equivalent:

(a) A is a torsion.

(b)  $G_A$  contains neither a directed cycle with label at least 2, nor two directed cycles which are connected by a path.

(c) There exists a permutation matrix P such that  $P^{-1}AP$  has the block form

$$\begin{pmatrix} B_{11} & B_{12} & B_{13} \\ 0 & B_{22} & B_{23} \\ 0 & 0 & B_{33} \end{pmatrix},$$
(5.1)

where some blocks might be empty,  $B_{11}$  and  $B_{33}$  are upper triangular with zeros on the diagonals, and  $B_{22}$  is a permutation matrix.

*Proof.* To show that (a) implies (b), let A be in  $M_n(\mathbb{N})$  and let  $G_A$  be its graph representation. Assume that  $G_A$  contains a cycle T with  $\rho(T) \geq 2$ , and assume also that i is a vertex in T. Denote by l the length of T; clearly  $l \geq 1$ . By Lemma 5.1,  $(A^{lr})_{ii} \geq \rho(T)^r \geq 2^r$ , and hence A is not a torsion.

Assume now that  $G_A$  has two distinct cycles  $T_1$  and  $T_2$  through vertices i and j, respectively, and that there is a path  $T_3$  from i to j. Let  $l_k$  be the length of  $T_k$  for k = 1, 2, 3. Consider the walks of the form  $T_1^{m_1 l_2} T_3 T_2^{m_2 l_1}$ . The length of such a walk is clearly  $(m_1 + m_2)l_1l_2 + l_3$ . If  $m = m_1 + m_2$ , then for all m in  $\mathbb{N}$  we have at least m different paths from i to j of length  $ml_1l_2 + l_3$ , because there is m different ways to express m as a sum  $m_1 + m_2$ . Therefore by Lemma 5.1,  $(A^{ml_1 l_2 + l_3})_{ij} \geq m$ , and so A is not a torsion.

Next we show that (b) implies (c). We say that a strong component of the graph  $G_A$  is trivial if it contains no edges. Consider the following partition of the vertex set of  $G_A$ :

 $V_2 = \{i \in \mathbf{n} \mid i \text{ belongs to a nontrivial strong component of } G_A\},$   $V_1 = \{i \in \mathbf{n} \setminus V_2 \mid \text{there exists a path from } i \text{ to some vertex in } V_2\},$  $V_3 = \mathbf{n} \setminus (V_1 \cup V_2).$ 

Let  $G_k$  denote the subgraph of  $G_A$  induced by  $V_k$  for k = 1, 2, 3, i.e.  $G_k$ consists of all vertices of  $V_k$  and all edges between the vertices of  $V_k$ . Because the vertices that are in some cycle of  $G_A$  belong to  $V_2$ , it follows that  $G_1$  and  $G_3$  are acyclic. Therefore we are able to define total orders  $\leq_1$  and  $\leq_3$  on  $V_1$  and  $V_3$ , respectively, such that if there is a edge from i to j in  $G_k$ , then  $i \leq_k j$ . Now there exists a permutation  $\pi$  of  $\mathbf{n}$ , such that

$$\forall i, j \in V_k, i \neq j : \quad \pi(i) < \pi(j) \iff i <_k j \quad \text{for } k = 1, 3, \tag{5.2}$$

$$\forall i \in V_k, j \in V_l : k < l \implies \pi(i) < \pi(j).$$
(5.3)

Such a permutation can be constructed in such a way that  $\mathbf{n}$  is first divided into three parts according to (5.3), and then the permutation is defined using (5.2).

Let P to be the permutation matrix defined by  $P_{ij} = \delta_{i,\pi(j)}$ . Then the matrix  $P^{-1}AP$  satisfies the condition  $(P^{-1}AP)_{ij} = A_{\pi(i),\pi(j)}$ , since the multiplication by  $P^{-1} = \delta_{\pi(i),j}$  from the left permutes the rows of A according to  $\pi$ , i.e.  $(P^{-1}A)_{ij} = A_{\pi(i),j}$ , and the multiplication by P from the right permutes the columns of  $A_{\pi(i)j}$  according to  $\pi$ . Let  $B_{ij}$  denote the restriction of the matrix  $P^{-1}AP$  to  $\pi(V_i) \times \pi(V_j)$ . Because no vertices of  $V_3$  is connected

to  $V_1$  or  $V_2$  (by definition), it follows from (5.3) that  $B_{31}$  and  $B_{32}$  are zero matrices. Also  $B_{21}$  is zero, because there exists no path from the vertices of  $V_2$  to the vertices of  $V_1$ , only vice versa. Further since no element in  $V_1 \cup V_3$ belongs to any nontrivial strong component of  $G_A$ , it follows that  $B_{11}$  and  $B_{33}$  have zeros on the diagonals: from (5.2) it also follows that they are upper triangular. Conditions (b) imply that the strong components of  $G_A$  are cycles with label 1, and because no two distinct cycles are joined by a path, there are no edges, such that i and j belong to different strong components and there is a an edge from i to j in  $G_A$ . Therefore  $B_{22}$  is a permutation matrix.

Finally we show that (c) implies (a). Clearly, for a permutation matrix P there exists a natural number r such that  $P^r = I$ . Let r be such a natural number that  $B_{22}^r = I$  and  $r \ge n$ . Now we have

$$(P^{-1}AP)^r = P^{-1}A^r P = \begin{pmatrix} 0 & B'_{12} & B'_{13} \\ 0 & I & B'_{23} \\ 0 & 0 & 0 \end{pmatrix},$$

because  $B_{11}$  and  $B_{33}$  are upper triangular with zeros on the diagonals; so  $B_{11}^n = B_{33}^n = 0$ . Hence

$$(P^{-1}AP)^{2r} = P^{-1}A^{2r}P = P^{-1}\begin{pmatrix} 0 & B'_{12} & B'_{12}B'_{23} \\ 0 & I & B'_{23} \\ 0 & 0 & 0 \end{pmatrix}P$$
$$(P^{-1}AP)^{3r} = P^{-1}A^{3r}P = P^{-1}\begin{pmatrix} 0 & B'_{12} & B'_{12}B'_{23} \\ 0 & I & B'_{23} \\ 0 & 0 & 0 \end{pmatrix}P.$$

Therefore  $A^{2r} = A^{3r}$ , i.e. A is a torsion.

As corollaries of the previous lemma we prove two lemmas, but first we must set a few new definitions. Define a semiring  $\mathbb{N}_2 = \{0, 1, 2\} \subseteq \mathbb{N}$  with the operations  $a \oplus b = \min\{a + b, 2\}$  and  $a \odot b = \min\{ab, 2\}$ . Let  $\Psi : M_n(\mathbb{N}) \to$  $M_n(\mathbb{N}_2)$  be the monoid morphism given by  $\Psi(A)_{ij} = \min\{A_{ij}, 2\}$  and let  $\iota$ denote the set inclusion  $\iota : M_n(\mathbb{N}_2) \to M_n(\mathbb{N})$ .

Note that, for a matrix A in  $M_n(\mathbb{N})$ ,  $G_{\Psi(A)}$  has exactly the same edges than  $G_A$ , and if  $G_A$  has a cycle with a label at least 2, then so does  $G_{\Psi(A)}$ , since in  $G_A$ , necessarily one of the edges on this cycle has a label at least 2, and in  $G_{\Psi(A)}$  this label is exactly 2. Similarly, if  $G_{\Psi(A)}$  contains a cycle with a label 2, (the product of labels of a path is  $\odot$ ), then  $G_A$  contains a cycle with a label at least 2. Therefore, the graph  $G_A$  satisfies the condition (b) of Lemma 5.2 if and only if the graph  $G_{\Psi(A)}$  satisfies it. We shall use these considerations as the final conclusion in the proof of the next lemma.

**Lemma 5.3.** Let A and B be matrices of  $M_n(\mathbb{N})$  such that  $\Psi(A) = \Psi(B)$ . Then A is a torsion if and only if B is a torsion.

*Proof.* Because  $\Psi(A) = \Psi(B)$ , graphs  $G_{\Psi(A)}$  and  $G_{\Psi(B)}$  are equal. Therefore, if  $G_A$  satisfies Condition (b) of Lemma 5.2, so does  $G_B$ .

Recall that an element a of a semiring is called *idempotent*, if  $a^2 = a$ . The next lemma shows how the torsions of the monoid  $M_n(\mathbb{N})$  are connected to the idempotents of the monoid  $M_n(\mathbb{N}_2)$ .

**Lemma 5.4.** If  $A \in M_n(\mathbb{N})$  is a torsion and  $\Psi(A)$  is an idempotent, then  $A^2 = A^3$ , and there exists a permutation matrix P such that  $P^{-1}AP$  has a block form

$$\begin{pmatrix} 0 & C & D \\ 0 & I & E \\ 0 & 0 & 0 \end{pmatrix}, (5.4)$$

where I is an identity matrix.

*Proof.* Let P be a permutation matrix such that  $P^{-1}AP$  has the form (5.1) of Lemma 5.2. Since  $\Psi(A)$  is idempotent in  $M_n(\mathbb{N}_2)$  and  $\Psi$  is a morphism,

$$\Psi((P^{-1}AP)^2) = \Psi(P^{-1}A^2P) = \Psi(P^{-1}AP).$$

Now since  $B_{11}$  and  $B_{33}$  are upper triangular with zeros on the diagonals,  $B_{11}$ and  $B_{33}$  must be zero matrices. Indeed, if they are not zero matrices, then on each power the number of zero entries grows. Since  $B_{22}$  is a permutation matrix and therefore invertible, from  $B_{22}^2 = B_{22}$  it follows that  $B_{22} = I$ . Hence  $P^{-1}AP$  is of the form (5.4). Now

$$(P^{-1}AP)^{2} = P^{-1}A^{2}P = P^{-1}\begin{pmatrix} 0 & C & CE\\ 0 & I & E\\ 0 & 0 & 0 \end{pmatrix}P,$$
$$(P^{-1}AP)^{3} = P^{-1}A^{3}P = P^{-1}\begin{pmatrix} 0 & C & CE\\ 0 & I & E\\ 0 & 0 & 0 \end{pmatrix}P.$$

So we have that  $P^{-1}A^2P = P^{-1}A^3P$ , and by multiplying this equation by P from the left and by  $P^{-1}$  from the right we get that  $A^2 = A^3$ .

We are ready for the main theorem of this section. It shows that if a finitely generated subsemigroup S of  $M_n(\mathbb{N})$  is finite, then we can state an upper bound for cardinality of S.

**Theorem 5.2.** Let S be a subsemigroup of  $M_n(\mathbb{N})$ , generated by k of its elements. The following statement are equivalent:

- (a) S is finite.
- (b) For all  $A \in \Psi(S)$ , if A is idempotent then  $\iota(A)^2 = \iota(A)^3$ .
- (c)  $|S| \leq g(n,k)$  where g is a function depending only on n and k.

*Proof.* First we show that (a) implies (b). Since S is finite, it is torsion. Let A in  $\Psi(S)$  be idempotent and let B in S be such that  $\Psi(B) = A$ . Since  $A = \Psi(\iota(A))$ , it follows that  $\Psi(B) = \Psi(\iota(A))$ . Since B is a torsion, by Lemma 5.3, so is  $\iota(A)$ , and by Lemma 5.4, since A is idempotent,  $\iota(A)^2 = \iota(A)^3$ .

Second we show that (b) implies (c). Let  $m = 3^{n^2} = |M_n(\mathbb{N}_2)|$ , p = R(m, 4, 2) and  $g(n, k) = \sum_{i=0}^{p-1} k^i$ . Without loss of generality we may assume that S is a monoid. Since S is generated by k of its elements, there is an epimorphism, i.e. a surjective morphism,  $\chi : X^* \to S$ , where  $X^*$  is the free word monoid generated by an alphabet X of cardinality k. We continue by proving the next claim.

**Claim.** If x in  $X^*$  is a word of length  $|x| \ge p$ , then there exists another word y in  $X^*$ , with |y| < |x|, such that  $\chi(x) = \chi(y)$ .

Proof of the Claim. Let r = |x| and let  $x = x_1 x_2 \dots x_r$ , with  $x_i$ 's in X. Let us partition the 2-subsets of  $\{1, \dots, r\}$  into m blocks  $\{Q_A \mid A \in M_n(\mathbb{N}_2)\}$ ; by letting

$$Q_A = \{\{i, j\} \mid i < j \text{ and } \Psi(\chi(x_i x_{i+1} \dots x_j)) = A\}.$$

Since  $r \ge p$ , there exists, by Theorem 5.1, a set  $Y = \{i_1, i_2, i_3, i_4\}$ , with  $1 \le i_1 < i_2 < i_3 < i_4 \le r$ , such that all 2-subsets of Y belong to the same block, say  $Q_A$ . Let  $y_k = x_{i_k} \dots x_{i_{k+1}-1}$  for k = 1, 2, 3, and let u and v in  $X^*$  be such that  $x = uy_1y_2y_3v$ . Denote the composition  $(\Psi \circ \chi)$  by  $\xi$ . Since  $\{i_1, i_2\}, \{i_2, i_3\}, \{i_1, i_3\}$  and  $\{i_3, i_4\}$  are in  $Q_A$ , we have

$$A = \xi(y_1) = \xi(y_2) = \xi(y_1y_2) = \xi(y_3).$$
(5.5)

Now, because  $\xi$  is a morphism (since  $\Psi$  and  $\chi$  are), we have that  $A = \xi(y_1y_2) = \xi(y_1)\xi(y_2) = A^2$ , i.e. A is an idempotent in  $\Psi(S)$ . By our assumption (b), this implies that  $\iota(A)^2 = \iota(A)^3$ , and by Lemma 5.4, there exists a permutation matrix P such that  $P^{-1}\iota(A)P$  has a block form (5.4). Since P and  $P^{-1}$  are permutation matrices, it is clear that  $\Psi(P) = P$  and

 $\Psi(P^{-1}) = P^{-1}$ , and it follows from (5.5) that  $P^{-1}\iota(A)P = \Psi(P^{-1}\chi(y_k)P)$ , for k = 1, 2, 3. Hence by the definition of  $\Psi$  and  $\iota$ ,  $P^{-1}\chi(y_k)P$  has the block form

$$\begin{pmatrix} 0 & C_k & D_k \\ 0 & I & E_k \\ 0 & 0 & 0 \end{pmatrix}$$

This implies that

$$(P^{-1}\chi(y_1)P)(P^{-1}\chi(y_2)P)(P^{-1}\chi(y_3)P) = \begin{pmatrix} 0 & C_1 & C_1E_2 \\ 0 & I & E_2 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & C_3 & D_3 \\ 0 & I & E_3 \\ 0 & 0 & 0 \end{pmatrix}$$
$$= \begin{pmatrix} 0 & C_1 & C_1E_3 \\ 0 & I & E_3 \\ 0 & 0 & 0 \end{pmatrix} = (P^{-1}\chi(y_1)P)(P^{-1}\chi(y_3)P).$$

Now  $P^{-1}\chi(y_1y_2y_3)P = P^{-1}\chi(y_1y_3)P$ , i.e.  $\chi(y_1y_2y_3) = \chi(y_1y_3)$ . Thus,  $\chi(x) = \chi(uy_1y_3v)$  and this completes the proof of the Claim, since  $|y_2| > 0$ .

It follows that  $\chi(x) = \chi(z)$  for some word z in  $X^*$ , such that |z| < p; hence  $|S| \leq g(n, k)$ .

It is clear that (c) implies (a).

In our proof we had p = R(m, 4, 2), but these Ramsey numbers are very large. We mention that A. Weber and H. Seidl proved in [WeS] that the number R(m, 4, 2) can be replaced by the number  $\lceil e^2 \cdot n! \rceil - 1$ , where e is the natural base of logarithms. Their proof is based on the theory of automata, and it is different from the one we presented. Weber and Seidl also mention in the appendix of [WeS] that it can be decided in time  $O(n^6 \cdot |H|)$ , whether a subsemigroup of  $M_n(\mathbb{N})$  generated by the set H is finite. There exists also many other papers concerning this upper bound and the exact algorithm, for example by G. Jacob, [Ja1] and [Ja2], and by some of the authors already mentioned in this chapter.

**Corollary 5.1.** It is decidable whether a given finitely generated subsemigroup of  $M_n(\mathbb{N})$  is finite.

*Proof.* The previous theorem shows that we have to find only g(n,k) + 1 different matrices from S to see that S is infinite. If we cannot find that many different matrices, then S is finite.

Mandel and Simon also proved in [MaS], that there is an upper bound for the cardinality of the finite subsemigroups of  $M_n(\mathbb{Q})$  and of  $M_n(F)$ , where F is an arbitrary field.

The next two theorems are corollaries of the result of Mandel and Simon for  $M_n(\mathbb{Q})$ .

**Theorem 5.3.** It is decidable whether a semigroup generated by one integer matrix is free.

*Proof.* We can decide whether the semigroup generated by a given matrix is finite or not, and if the semigroup is finite, then it is not free, and otherwise it is free.  $\Box$ 

**Theorem 5.4.** It is decidable whether some power of a given integer matrix is zero, i.e. the mortality problem for the semigroup generated by one matrix is decidable.

*Proof.* We can decide whether the matrix semigroup generated by this matrix is finite or not, and if it is, we check if one of these matrices is zero.  $\Box$ 

The same conclusion holds for the decidability of the existence of the identity matrix as a power of given matrix. It is also decidable.

## 6 Zero in the Right Upper Corner

The problem considered in this chapter is called the *zero in the right upper corner*.

**Problem 5.** For a given finite subset of  $\mathbb{Z}^{n \times n}$ , determine whether there exists an M in the semigroup generated by these matrices such that  $M_{1n} = 0$ .

In the first section we shall show that if  $n \geq 3$ , then the problem is undecidable. The method we use is the usual coding of pairs of words into  $3 \times 3$  matrices. First we have to recall and introduce few notions and functions.

In the latter part of this chapter we consider the above problem in the case where we have only two generators. We shall prove that also in this case the problem is undecidable, when the dimension of the matrices is large enough.

# 6.1 The undecidability of the zero in the right upper corner

We begin with some definitions for the proof. Let  $\Gamma = \{a_1, a_2, ..., a_n\}$  be an alphabet and let function  $\sigma$  be as in Chapter 2, i.e.  $\sigma : \Gamma^* \to \mathbb{N}$  such that

$$\sigma(a_{i_1}a_{i_2}...a_{i_k}) = \sum_{j=1}^k i_j n^{k-j} \text{ and } \sigma(1) = 0.$$

We recall that  $\sigma$  is injective, and that for all u, v in  $\Gamma^*$ 

$$\sigma(uv) = \sigma(v) + n^{|v|}\sigma(u).$$
(6.1)

Assume now that n = 2, i.e.  $\Gamma = \{a_1, a_2\}$ , and define a mapping  $\gamma_2 : \Gamma^* \times \Gamma^* \to \mathbb{Z}^{3 \times 3}$  by

$$\gamma_2(u,v) = \begin{pmatrix} 1 & \sigma(v) & \sigma(u) - \sigma(v) \\ 0 & 2^{|v|} & 2^{|u|} - 2^{|v|} \\ 0 & 0 & 2^{|u|} \end{pmatrix}.$$

This mapping is clearly injective, because  $\sigma$  is injective, and it is also a

morphism, since for all  $u_1, u_2, v_1, v_2$  in  $\Gamma^*$ ,

$$\begin{split} &\gamma_{2}(u_{1},v_{1})\gamma_{2}(u_{2},v_{2}) \\ &= \begin{pmatrix} 1 & \sigma(v_{1}) & \sigma(u_{1}) - \sigma(v_{1}) \\ 0 & 2^{|v_{1}|} & 2^{|u_{1}|} - 2^{|v_{1}|} \\ 0 & 0 & 2^{|u_{1}|} \end{pmatrix} \begin{pmatrix} 1 & \sigma(v_{2}) & \sigma(u_{2}) - \sigma(v_{2}) \\ 0 & 2^{|v_{2}|} & 2^{|u_{2}|} - 2^{|v_{2}|} \\ 0 & 0 & 2^{|u_{2}|} \end{pmatrix} \\ &= \begin{pmatrix} 1 & \sigma(v_{2}) + \sigma(v_{1})2^{|v_{1}|} & \sigma(u_{2}) - \sigma(v_{2}) + \sigma(v_{1})(2^{|u_{2}|} - 2^{|v_{2}|}) \\ & + 2^{|u_{2}|}(\sigma(u_{1}) - \sigma(v_{1})) \\ 0 & 2^{|v_{1}|}2^{|v_{2}|} & 2^{|v_{1}|}(2^{|u_{2}|} - 2^{|v_{2}|}) + 2^{|u_{2}|}(2^{|u_{1}|} - 2^{|v_{1}|}) \\ 0 & 0 & 2^{|u_{1}|}2^{|u_{2}|} \end{pmatrix} \\ \stackrel{(6.1)}{=} \begin{pmatrix} 1 & \sigma(v_{1}v_{2}) & \sigma(u_{1}u_{2}) - \sigma(v_{1}v_{2}) \\ 0 & 2^{|v_{1}v_{2}|} & 2^{|u_{1}u_{2}|} - 2^{|v_{1}v_{2}|} \\ 0 & 0 & 2^{|u_{1}u_{2}|} \end{pmatrix} = \gamma_{2}(u_{1}u_{2}, v_{1}v_{2}). \end{split}$$

The next theorem is attributed to R.W. Floyd in [Man].

**Theorem 6.1.** It is undecidable whether a finitely generated subsemigroup of  $M_3(\mathbb{Z})$  contains a matrix M with  $M_{13} = 0$ .

*Proof.* Let (h, g) be an instance of PCP, let h and g be morphisms from  $\Sigma^*$  into  $\Gamma^*$ , and define the matrices  $M_a = \gamma_2(h(a), g(a))$  for all a in  $\Sigma$ . Then, because  $\gamma_2$  is morphism, for a matrix  $M = M_{a_1}M_{a_2}\cdots M_{a_m}$ ,

 $M_{13} = 0$ 

if and only if

$$\sigma(h(a_1)h(a_2)...h(a_m)) = \sigma(g(a_1)g(a_2)...g(a_m)),$$

i.e.  $\sigma(h(w)) = \sigma(g(w))$ , where  $w = a_1 a_2 \dots a_m$ . Now, because  $\sigma$  is injective, we get that  $M_{13} = 0$  if and only if h(w) = g(w), and the claim follows from the undecidability of PCP.

Note that in the proof we needed 7 generators, since, as remarked before, PCP(7) is undecidable.

Because we may add zero columns to the left and zero rows to the bottom of the matrices in the previous proof, we get the next corollary.

**Corollary 6.1.** If  $n \ge 3$ , it is undecidable whether a finitely generated subsemigroup of  $M_n(\mathbb{Z})$  contains a matrix M with  $M_{1n} = 0$ .

The decidability of the existence of the zero in the right upper corner for  $2 \times 2$  matrices is an open question. We note again, that if it is undecidable, it must be proved with some other method than the one used in the proof of the previous theorem.

#### 6.2 The two generator case

In Chapter 3 we considered the mortality problem in the case, where the semigroup is generated by two matrices. We used the construction from matrices  $M_1, \ldots, M_k$  with dimension n into two matrices A and B with dimension nk such that

,

$$A = \begin{pmatrix} M_1 & 0 & \cdots & 0 \\ 0 & M_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & M_n \end{pmatrix} \text{ and } B = \begin{pmatrix} 0 & 0 & \cdots & 0 & I \\ I & 0 & 0 & \cdots & 0 \\ 0 & I & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & I & 0 \end{pmatrix}$$

We cannot apply these matrices to the problem of the zero in the right upper corner, but we shall use them as blocks in the matrices with dimension nk+3. First we define two vectors of dimension n, namely

$$X = \begin{pmatrix} 1 & 0 & \dots & 0 \end{pmatrix} \text{ and } Y = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix},$$

so XMY is the entry in the right upper corner of M in  $\mathbb{Z}^{n \times n}$ . Next define two vectors of dimension nk,

$$U = \begin{pmatrix} X & \dots & X \end{pmatrix}$$
 and  $V = \begin{pmatrix} Y \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ .

Now we define the matrices A' and B' with dimension nk + 3 to be

$$A' = \begin{pmatrix} 0 & 1 & U & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & A & V \\ 0 & 0 & 0 & 0 \end{pmatrix} \text{ and } B' = \begin{pmatrix} 0 & 1 & U & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & B & V \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Note the difference in the second diagonal entry.

The proof of the next theorem is from [CKa].

**Theorem 6.2.** It is undecidable whether the semigroup generated by  $\{A', B'\}$  has an element such that it has a zero in the right upper corner.

*Proof.* Let S be the semigroup generated by  $\{A, B\}$ , S' be the semigroup generated by  $\{A', B'\}$ , and T be the semigroup generated by  $\{M_1, \ldots, M_k\}$ . Let C' be an element of S'. Then

$$C' = \begin{pmatrix} 0 & * & * & * \\ 0 & \lambda & 0 & * \\ 0 & 0 & C & * \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

where \*'s represent the unimportant values, C is an element of S, and  $\lambda$  is 1, if C' is power of B', and 0 otherwise.

Consider any element of S' other than the generators A' and B'. It can be written in the form PC'Q, where P and Q are equal to A' or B',

$$P = \begin{pmatrix} 0 & 1 & U & 1 \\ 0 & * & 0 & 1 \\ 0 & 0 & * & V \\ 0 & 0 & 0 & 0 \end{pmatrix} \text{ and } Q = \begin{pmatrix} 0 & 1 & U & 1 \\ 0 & * & 0 & 1 \\ 0 & 0 & * & V \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

and C' is an element of S'. The product expands to

$$PC'Q = \begin{pmatrix} 0 & * & * & \lambda + UCV \\ 0 & * & 0 & * \\ 0 & 0 & * & * \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

where the right upper corner entry is  $\lambda + UCV$ . If C' is a power of B', then C is a power of B and  $\lambda = 1$  and UCV = 0, hence the right upper entry of PC'Q is 1. Otherwise,  $\lambda = 0$  and if we divide C to  $n \times n$  blocks  $N_{ij}$ , where  $1 \leq i, j \leq k$ , then  $UCV = \sum_{i=1}^{k} XN_{i1}Y$ . As in the proof of Theorem 3.2, we can write  $C = B^{t}C_{i_{1}}C_{i_{2}}\cdots C_{i_{m}}$ , where  $C_{i_{j}} = B^{k-i_{j}+1}AB^{i_{j}-1}$ , where  $1 \leq i_{j} \leq k$ . The initial  $B^{t}$  permutes the lines only, so the  $N_{i1}$ 's are also, in a different order, the elements of the first block column of  $C_{i_{1}}C_{i_{2}}\cdots C_{i_{m}}$ , and one of them is  $M = M_{i_{1}}M_{i_{2}}\cdots M_{i_{m}}$  and the k-1 others are zero blocks. Therefore the right upper corner entry of PC'Q is XMY, i.e. the right upper corner entry of M, which can be any element of T. If we now define the matrices  $M_{i}$  to be the matrices of the proof of Theorem 6.1, we get that for S' the existence of the zero in the right upper corner is undecidable, since it is undecidable for T.

Notice that dimension of A' and B' is nk+3 and, by the proof of Theorem 6.1, we may set n = 3 and k = 7. Therefore we get that the problem of the zero in the right upper corner is undecidable in two generator semigroups, when the dimension of these matrices is at least 24. This is an obvious corollary of the previous theorem.

## 7 Skolem's Problem

In this and next chapters we consider the so called *Skolem's problem*, which we define next. It is related to the problem of the zero in the right upper corner in a way that in Skolem's problem we consider semigroups generated by one matrix.

**Problem 6.** Let M be a given matrix from  $M_n(\mathbb{Z})$ . Determine whether there exist a power k such that  $(M^k)_{1n} = 0$ ?

It is not known whether the Skolem's problem is decidable or not, when  $n \geq 3$ . We shall prove the decidability for case of dimension two in the first section and the main result of the next chapter is that it is decidable, whether there exists infinitely many powers k such that  $(M^k)_{1n} = 0$ .

In the proof of the decidability of the Skolem's problem in dimension two we shall use Theorem 7.1 which suits for deciding the existence of the zero in any entry of the powers of a given  $2 \times 2$  matrix, and the decidability of the Skolem's problem is a corollary of that theorem. That theorem gives us also a way to prove the decidability of the mortality problem in the case, when the semigroup is generated by two  $2 \times 2$  matrices. This proof is presented in the second section of this chapter.

#### 7.1 Skolem's problem in dimension two

We are now going to prove that the Skolem's problem is decidable in the case of  $2 \times 2$  matrices. To prove this we need certain properties of sequences.

Let  $(u_n)_{n=1}^{\infty}$  be an integer sequence, defined by constants  $u_0 = c_0$ ,  $u_1 = c_1$ and a formula

$$u_n + a_1 u_{n-1} + a_2 u_{n-2} = 0, (7.1)$$

where  $a_i$ 's are in  $\mathbb{Q}$ . Let  $\alpha$  and  $\beta$  are the roots of the equation

$$y^2 + a_1 y + a_2 = 0. (7.2)$$

The next lemma has an elementary combinatorial proof, which we give for the sake of completeness. **Lemma 7.1.** Let  $(u_n)_{n=0}^{\infty}$  be as above. Then we have two cases, namely: (i) If  $\alpha \neq \beta$ , then there exists constants a and b such that

$$u_n = a\alpha^n + b\beta^n$$

for all n in  $\mathbb{N}$ .

(ii) If  $\alpha = \beta$ , then there exists constants c and d such that

$$u_n = (cn+d)\alpha^n$$

*Proof.* (i): If the claim holds, then by the equalities  $a + b = c_0$  and  $a\alpha + b\beta = c_1$ , we have

$$a = \frac{c_1 - c_0 \beta}{\alpha - \beta}$$
 and  $b = \frac{c_1 - c_0 \alpha}{\beta - \alpha}$ 

We assume that a and b are as above and prove the claim (i) by induction.

Clearly, when n = 0, 1 the claim holds. Assume that it holds for all  $n \le k + 1$ , where  $k \ge 0$ . Then by the assumption (7.1)

$$u_{k+2} = -a_1 u_{k+1} - a_2 u_k = -a_1 (a\alpha^{k+1} + b\beta^{k+1}) - a_2 (a\alpha^k + b\beta^k)$$
  
=  $-a\alpha^k (a_1\alpha + a_2) - b\beta^k (a_1\beta + a_2) = a\alpha^{k+2} + b\beta^{k+1},$ 

where the last equation follows from the fact that  $\alpha$  and  $\beta$  are roots of the equation (7.2), and therefore  $-\beta^2 = a_1\beta + a_2$  and  $-\alpha^2 = a_1\alpha + a_2$ .

(ii): Like in the previous case, if the claim holds, then we have that  $d = c_0$  and  $c = (c_1 - c_0 \alpha)/\alpha$ . We prove the claim (ii) by induction.

If n = 0, 1, then the claim holds. Assume that claim holds for all  $n \le k+1$ , where  $k \ge 0$ . Then by the assumption (7.1)

$$u_{k+2} = -a_1(c(k+1) + d)\alpha^{k+1} - a_2(ck+d)\alpha^k$$
  
=  $\alpha^k(-a_1c(k+1)\alpha - a_1d\alpha - a_2ck - a_2d)$   
=  $\alpha^k(ck(-a_1\alpha - a_2) + d(-a_1\alpha - a_2) - a_1c\alpha)$   
=  $\alpha^k(ck\alpha^2 + d\alpha^2 - (-2\alpha)c\alpha) = (c(k+2) + d)\alpha^{k+2}$ 

since  $\alpha$  is a root of equation (7.2) and  $t^2 + a_1t + a_2 = (t - \alpha)^2$ , we have  $a_1 = -2\alpha$ .

Let p be a prime number. We define the p-adic valuation  $v_p$  over  $\mathbb{Q}$  by  $v_p(0) = \infty$  and  $v_p(q) = n$ , where  $q = p^n \frac{a}{b}$  with a and b in  $\mathbb{Z}$  and p divides neither a nor b.

It is clear by the definition of  $v_p$  that  $v_p(a+b) \ge \inf\{v_p(a), v_p(b)\}$ . And if a and b are integers, we can prove a stronger result for  $v_p(a+b)$  as stated in the next lemma. **Lemma 7.2.** Let a and b be two integers and p a prime number. If  $v_p(a) < v_p(b)$ , then  $v_p(a+b) = v_p(a)$ .

Proof. Assume that  $v_p(a) = n$  and  $v_p(b) = k$ , with n < k. Then  $a + b = p^n(a_1 + b_1)$ , where  $v_p(a_1) = 0$  and  $v_p(b_1) > 1$ . Clearly  $v_p(a + b) \ge n$ , and if  $v_p(a+b) > n$ , then  $a_1+b_1 \equiv 0 \pmod{p}$  and therefore  $a_1 \equiv -b_1 \equiv 0 \pmod{p}$ , and we have a contradiction. Now  $v_p(a+b) = n = v_p(a)$ .

Now we are ready for the main theorem of this section. The proof is modelled after the ideas of J.Cassaigne [Cas].

**Theorem 7.1.** Let A be a  $2 \times 2$  matrix over integers and assume that u and v are integer vectors of dimension 2. Then it is decidable whether  $uA^nv^T = 0$  for some n > 0.

*Proof.* Let t = tr(A) and d = det(A). By Section 2.3 we know that the characteristic polynomial of A is  $c_A(\lambda) = \lambda^2 - t\lambda + d$ . Also by Section 2.3 we know that  $c_A(A) = A^2 - tA + dI = 0$ , so we see that

$$A^2 = tA - dI. ag{7.3}$$

Consider the sequence  $(x_n)_{n\geq 0} = uA^n v^T$ . By multiplying the equation (7.3) by  $uA^n$  from the left and by  $v^T$  from the right we get  $x_{n+2} = tx_{n+1} - dx_n$ . We see that  $x_n$  is defined by  $x_0$  and  $x_1$ , and if both of these are zero, then for all  $n, x_n = 0$ . We assume that this is not the case.

Consider next the equation (7.2) for the sequence  $x_n$ , i.e. the equation

$$y^2 - ty + d = 0. (7.4)$$

We know that the roots of this equation are of the form  $y = \frac{t \pm \sqrt{t^2 - 4d}}{2}$ . Let  $\Delta = t^2 - 4d$ . We divide the proof into three cases:

1)  $\Delta = 0$ . Then by the case (ii) of Lemma 7.1,  $x_n = (\frac{t}{2})^n (cn+d)$ , where c and d are in  $\mathbb{Q}$ , and they are fixed by  $x_0$  and  $x_1$ . Now if t = 0, then  $(x_n)_{n\geq 0}$  has infinitely many zeros, and if  $t \neq 0$  and  $-\frac{d}{c}$  in  $\mathbb{N}$ , then  $(x_n)_{n\geq 0}$  has exactly one zero. Otherwise  $(x_n)_{n\geq 0}$  has no zeros.

2)  $\Delta > 0$ . If t = 0, then

$$x_n = \begin{cases} (-d)^{\frac{n}{2}} x_0, & \text{if } n \text{ is even,} \\ (-d)^{\lfloor \frac{n}{2} \rfloor} x_1, & \text{if } n \text{ is odd.} \end{cases}$$
(7.5)

If  $x_0$  or  $x_1$  is zero, then  $(x_n)_{n\geq 0}$  has infinitely many zeros. Otherwise it has no zeros.

If  $t \neq 0$ , then we have case (i) in Lemma 7.1, i.e.

$$x_n = a\alpha^n + b\beta^n,$$

where  $\alpha$  and  $\beta$  (in  $\mathbb{R}$ ) are the roots of the equation (7.4) and a and b are in

$$\mathbb{Q}\left[\sqrt{\Delta}\right] = \left\{u + v\sqrt{\Delta} \mid u, v \in \mathbb{Q}\right\} \subseteq \mathbb{R}$$

by the proof of Lemma 7.1. They can be effectively computed by the same proof. Assume that  $\alpha > \beta$ . Now  $x_n = 0$  if and only if  $(\frac{\alpha}{\beta})^n = -\frac{b}{a}$ . As  $|\frac{\alpha}{\beta}| > 1$ , a bound on n can be found and we are able to check whether  $(x_n)_{n\geq 0}$  has a zero or not.

3)  $\Delta < 0$ . If t = 0, we have the case (7.5), and it is easy to verify whether  $x_n = 0$  for some n. We assume that  $t \neq 0$ . We know that d > 0 and we shall prove first that  $x_n = O(d^{\frac{n}{2}})$ , which means that there exist constants c and  $n_0$  such that for all  $n \geq n_0$ ,  $x_n \leq c \cdot d^{\frac{n}{2}}$ . Since  $\Delta < 0$ , it follows by the case (i) of Lemma 7.1 that, for some constants a and b,

$$x_n = a\left(\frac{t+\sqrt{t^2-4d}}{2}\right)^n + b\left(\frac{t-\sqrt{t^2-4d}}{2}\right)^n.$$

Now we get that

$$\begin{aligned} |x_n| &= \left| a \left( \frac{t + \sqrt{t^2 - 4d}}{2} \right)^n + b \left( \frac{t - \sqrt{t^2 - 4d}}{2} \right)^n \right| \\ &\leq \left| a \left( \frac{t + \sqrt{t^2 - 4d}}{2} \right)^n \right| + \left| b \left( \frac{t - \sqrt{t^2 - 4d}}{2} \right)^n \right| \\ &\leq \frac{|a|}{2^n} |t + \sqrt{t^2 - 4d}|^n + \frac{|b|}{2^n} |t - \sqrt{t^2 - 4d}|^n \\ &= \frac{|a|}{2^n} |t + i\sqrt{4d - t^2}|^n + \frac{|b|}{2^n} |t - i\sqrt{4d - t^2}|^n \\ &= \frac{|a|}{2^n} \sqrt{t^2 + 4d - t^2}^n + \frac{|b|}{2^n} \sqrt{t^2 + 4d - t^2}^n \\ &= \frac{|a|}{2^n} \sqrt{4d}^n + \frac{|b|}{2^n} \sqrt{4d}^n = |a| d^{\frac{n}{2}} + |b| d^{\frac{n}{2}} = d^{\frac{n}{2}} (|a| + |b|), \end{aligned}$$

and therefore  $x_n \le (|a| + |b|)d^{\frac{n}{2}} \le O(d^{\frac{n}{2}}).$ 

Assume that p is a prime number such that p divides t and  $p^2$  divides d. Then  $p^{n-1}$  divides  $x_n$ , and by setting  $t' = \frac{t}{p}$  and  $d' = \frac{d}{p^2}$ , we can define an integer sequence  $(x'_n)_{n\geq 0}$  such that  $x'_0 = x_0$ ,  $x'_1 = x_1$  and for  $n \geq 2$ ,

$$x'_{n} = t'x'_{n_{1}} - d'x'_{n-2} = \frac{x_{n}}{p^{n-1}}$$

Clearly  $x'_n = 0$  if and only if  $x_n = 0$  and therefore we may consider the sequence  $(x'_n)_{n\geq 0}$  instead of  $(x_n)_{n\geq 0}$ . So we may assume that there is no such prime p that p divides t and  $p^2$  divides d.

Let u be the greatest common divisor of t and d, we denote, as usual, u = gcd(t, d) > 0, and t = uv, d = uw for some integers v and w. By the above assumption about prime factors of t and d, gcd(u, w) = gcd(v, w) = 1.

Assume that p is a prime factor of u. Then, again by induction, we can prove that  $v_p(x_n) \ge [\frac{n}{2}]$ . Also  $v_p(x_2) \ge \inf\{v_p(tx_1), v_p(dx_0)\} \ge 1$  and the induction step is

$$v_p(x_{n+1}) \ge \inf\{v_p(uvx_n), v_p(uwx_{n-1})\} \ge 1 + [\frac{n-1}{2}] = [\frac{n+1}{2}].$$

This means that  $u^{\left[\frac{n}{2}\right]}$  divides  $x_n$  for all  $n \geq 2$ .

Assume now that for all prime factors p of w, and for all n,  $v_p(x_{n+1}) - v_p(x_n) \ge v_p(w)$ . This implies that  $x_n \ne 0$  for all n. Also since  $v_p(w) \ge 1$ , it implies that  $w^n$  divides  $x_n$ . Now, since gcd(u, w) = 1, we know that  $u^{[\frac{n}{2}]}w^n$  divides  $x_n$ . Therefore

$$u^{\left[\frac{n}{2}\right]}w^n \le x_n = O(d^{\frac{n}{2}})$$

and because d = uw > 0, necessarily w = 1. Now  $\Delta = (uv)^2 - 4u < 0$ , so we get that  $uv^2 < 4$ , and |v| = 1 and  $u \in \{1, 2, 3\}$ . Since d = u, we see that  $d \in \{1, 2, 3\}$ , and t = d or t = -d. All these cases lead to an equation  $x_{n+12} = d^6x_n$ , which can be verified by simple calculations. For example, if d = t = 3, then  $x_{n+2} = 3x_{n+1} - 3x_n$ . We prove the equation by induction. First, for n = 0

$$\begin{aligned} x_{12} &= 3x_{11} - 3x_{10} = 9x_{10} - 9x_9 - 3x_{10} = 6x_{10} - 9x_9 = 18x_9 - 18x_8 - 9x_9 \\ &= 9x_9 - 18x_8 = 9x_8 - 27x_7 = -27x_6 = -81x_5 + 81x_4 \\ &= -162x_4 + 243x_3 = -243x_3 + 486x_2 = -243x_2 + 729x_1 = 729x_0 \\ &= 3^6x_0, \end{aligned}$$

and similarly for n = 1, we get that  $x_{13} = 3^6 x_1$ . The induction step is for  $n \ge 2$ 

$$\begin{aligned} x_{(n+1)+12} &= 3x_{n+12} - 3x_{(n-1)+12} = 3 \cdot 3^6 x_n - 3 \cdot 3^6 x_{n-1} \\ &= 3^6 (3x_n - 3x_{n-1}) = 3^6 x_{n+1}. \end{aligned}$$

This proves the case d = t = 3, and the other cases can be proved similarly.

We can easily verify whether  $x_{n+12} = d^6 x_n$  and  $t = \pm d$ . If this is not the case, then for some prime factor p of w and some n,  $v_p(x_{n+1}) - v_p(x_n) < v_p(w)$ . Now  $v_p(x_{n+1}) < v_p(x_n) + v_p(w) = v_p(uwx_n)$ , so by Lemma 7.2

$$v_p(x_{n+2}) = v_p(uvx_{n+1} + uwx_n) = v_p(x_{n+1}).$$

By induction we prove that

$$v_p(x_m) = v_p(x_{n+1}) < \infty$$
 for all  $m \ge n+1$ . (7.6)

Assume that for some m, (7.6) holds for all  $k, m \ge k \ge n+1$ 

$$v_p(x_{m+1}) = v_p(uvx_m + uwx_{m-1}) = \inf\{v_p(x_{n+1}), 1 + v_p(x_{n+1})\} = v_p(x_{n+1}).$$

Clearly the only possible zero is  $x_n$  where  $v_p(x_{n+1}) - v_p(x_n) < v_p(w)$  for the first time. So we check whether this  $x_n = 0$ .

Note that p and n are not known at first, but we can compute the values  $v_p(x_{n+1}) - v_p(x_n)$  for all prime factors p of w until p and n are found. There is no explicit bound for this loop of computation; it terminates always, since we evaluate this loop for all prime factors p of w at the same time. The loop terminates, when the first pair p and n is found and then the only possibility for the zero in  $(x_n)_{n>0}$  is found. We check that one, and we are done.

We have proved that there is a method in all cases of  $\Delta$  to solve whether there is  $n \ge 0$  such that  $uA^n v = 0$ .

**Corollary 7.1.** Skolem's problem is decidable for  $2 \times 2$  matrices over integers.

*Proof.* If we set u = (1,0) and v = (0,1) in Theorem 7.1, then the product  $uA^nv^T$  equals  $(A^n)_{22}$ .

#### 7.2 Skolem's problem and the mortality problem

We shall now return to the mortality problem. We restrict to the case when we are given two  $2 \times 2$  matrices over integers. We shall prove that this case is decidable. The proof is based on Theorem 7.1.

First we consider some properties of  $2 \times 2$  matrices over integers. Let A and B be elements of  $\mathbb{Z}^{n \times n}$ . We recall that  $\det(AB) = \det(A) \det(B)$  and that if A is *singular*, i.e.  $\det(A) = 0$ , we know that the rows and the columns of A are *linearly dependent* vectors. Set  $B = \{v_1, \ldots, v_k\}$  of vectors from  $\mathbb{Z}^n$  is linearly dependent if the exists integers  $c_1, \ldots, c_k$  such that

$$c_1 v_1 = c_2 v_2 + c_3 v_3 + \dots + c_k v_k$$

and at least for one  $i, c_i \neq 0$ . Otherwise B is called *linearly independent*.

The number of linearly independent rows in A is called the *rank* of A and denoted by rank(A). It can be proved that the number of linearly independent columns is also rank(A). Note that the rank of a matrix is also the dimension of the vectors space generated by the rows or the columns of the matrix.

Let A be  $in\mathbb{Z}^{n\times n}$ . It is known that A can be presented in the form

$$A = \sum_{i=1}^{\operatorname{rank}(A)} a_i^T b_i$$

where  $a_i$  and  $b_i$  are vectors in  $\mathbb{Z}^n$  for  $i = 1, ..., \operatorname{rank}(A)$ . Clearly, if  $\operatorname{rank}(A) = 1$ , then there exists vectors a and b in  $\mathbb{Z}^n$  such that  $A = a^T b$ .

**Lemma 7.3.** Let A, B and C three matrices with rank 1 from  $\mathbb{Z}^{n \times n}$ . If ABC = 0, then either AB or BC is zero.

*Proof.* Assume that  $A = a^T b$ ,  $B = c^T d$  and  $C = e^T f$ . If one of these matrices is zero, then the claim obviously holds, so we may assume that this is not the case. It follows that

$$ABC = a^T b c^T d e^T f = (b c^T) (d e^T) a^T f,$$

where  $bc^T$  and  $de^T$  is are integers. If now ABC = 0, then clearly either  $bc^T$  or  $de^T$  is zero. Since

$$AB = a^T b c^T d = (b c^T) a^T d$$

and

$$BC = c^T de^T f = (de^T)c^T f,$$

the claim follows.

**Theorem 7.2.** Given two  $2 \times 2$  matrices over integers, say A and B, it is decidable whether the zero matrix is in the semigroup generated by  $\{A, B\}$ .

*Proof.* Assume that A and B are non-zero, otherwise we are done. As we mentioned earlier, det(AB) = det(A) det(B) and det(0) = 0, so if A and B are both invertible, then the zero matrix is not in the semigroup S generated by  $\{A, B\}$ . It also follows that if the zero is in S, then at least one of these matrices is singular, i.e. has determinant equal to zero.

Assume that either A or B is singular. Then by Lemma 7.3, in the minimal-length zero product of S, the singular element can occur only as the first and the last factor. We have two possible cases:

 $\Box$ 

1) If A and B are both singular, then we have to check only the products AB, BA,  $B^2$  and  $A^2$ .

2) If A is invertible and B is singular, then B can be written in form  $B = x^T y$ , where x and y are vectors in  $\mathbb{Z}^2$ . Now

$$BA^kB = x^T y A^k x^T y = (y A^k x^T) x^T y = 0$$

if and only if

$$yA^kx^T = 0,$$

and by Theorem 7.1 this is decidable.

We shall next show that the decidability status of the Skolem's problem is equivalent with the decidability status of the certain instance of the mortality problem. The decidability status of a problem is either decidable, undecidable or unknown.

The theorem in this section is based on Lemma 7.3 and on next lemma.

**Lemma 7.4.** Let A be an element of  $\mathbb{Z}^{n \times n}$ , u and v be in  $\mathbb{Z}^n$ . There exists matrix M in  $\mathbb{Z}^{(n+2)\times(n+2)}$  such that for all integers  $k \geq 1$ 

$$uA^{k}v^{T} = (1, 0, \dots, 0)M^{k}(0, \dots, 0, 1)^{T}.$$
(7.7)

*Proof.* Define M as block form

$$M = \begin{pmatrix} 0 & uA^2 & uAv^T \\ 0 & A & v^T \\ 0 & 0 & 0 \end{pmatrix}.$$

The right hand side of the equation (7.7) clearly is the right upper corner element of  $M^k$ . We shall prove by induction that

$$M^{k} = \begin{pmatrix} 0 & uA^{k+1} & uA^{k}v^{T} \\ 0 & A^{k} & A^{k-1}v^{T} \\ 0 & 0 & 0 \end{pmatrix}$$
(7.8)

for all integers  $k \geq 1$ .

First, for k = 1 (7.8) is obvious by the definition. Assume now that (7.8) holds for all  $k \leq j, j > 1$ . So

$$M^{j+1} = M^{j}M = \begin{pmatrix} 0 & uA^{j+1} & uA^{j}v^{T} \\ 0 & A^{j} & A^{j-1}v^{T} \\ 0 & 0 & 0 \end{pmatrix} M = \begin{pmatrix} 0 & uA^{j+2} & uA^{j+1}v^{T} \\ 0 & A^{j+1} & A^{j}v^{T} \\ 0 & 0 & 0 \end{pmatrix}.$$

This proves the lemma.

Now we are ready for the next theorem.

**Theorem 7.3.** Let I be an instance of the mortality problem such that we are given matrices  $M_1, \ldots, M_t$  and A in  $\mathbb{Z}^{n \times n}$  and  $\operatorname{rank}(M_i) = 1$  for all  $i = 1, \ldots, t$ . The decidability status of instance I is equivalent with decidability status of Skolem's problem for matrix with dimension n + 2.

Proof. By Lemma 7.3 in I it is enough to study products  $M_iM_j$  and  $M_iA^kM_j$ ,  $i, j = 1, \ldots, t$  and  $k \ge 1$ . The products of the second form are actually of the form  $uA^kv^T$ , since rank  $M_i = 1$  for all  $i = 1, \ldots, t$ , and by Lemma 7.4 these are equivalent with the Skolem's problem for matrices with dimension n+2.

We have proved that there is a certain relation between the mortality problem and the Skolem's problem. Note that the decidability status of instances I of the mortality problem is unknown.

### 7.3 Skolem's problem for matrices over natural numbers

If we restrict in Skolem's problem to square matrices over natural numbers, we have a simple decidable special case. It follows from the fact that if M is in  $M_n(\mathbb{N})$ , then in  $M^k$  we are only interested in whether  $(M^k)_{1n}$  is positive or zero.

Let  $\mathbb{B}$  be the boolean semiring,  $\mathbb{B} = \{0, 1\}$ , where the operations are the usual product and addition of integers except that 1 + 1 = 1.

Assume that A is in  $M_n(\mathbb{N})$  and define a mapping  $\psi : M_n(\mathbb{N}) \to M_n(\mathbb{B})$ by

$$\psi(A)_{ij} = \begin{cases} 0, & \text{if } A_{ij} = 0, \\ 1, & \text{otherwise.} \end{cases}$$

We end this chapter with a simple theorem.

**Theorem 7.4.** Let A be in  $M_n(\mathbb{N})$ . It is decidable whether  $(A^k)_{1n} = 0$  for some  $k \geq 1$ .

*Proof.* Assume that B is in  $M_n(\mathbb{B})$  and that  $B = \psi(A)$ . Clearly  $(B^k)_{1n} = 0$  if and only if  $(A^k)_{1n}$ . There are  $2^{n^2}$  elements in  $M_n(\mathbb{B})$ , and we can compute  $B^k$  for all k, and stop if  $(B^k)_{1n} = 0$  or if  $B^k = B^h$  for some h < k. This procedure terminates, since the number of elements in  $M_n(\mathbb{B})$  is finite.  $\Box$ 

## 8 An Infinite Number of Zeros in Skolem's Problem

In this chapter we will show that it is decidable for a given matrix M from  $M_n(\mathbb{Z})$  whether there exist infinitely many k's such that  $(M^k)_{1n} = 0$ . The proof uses the theory of rational series so we begin with the basics of these series.

Our presentation on rational series follows the book *Rational Series and Their Languages* by J. Berstel and C. Reutenauer [BeR].

#### 8.1 Rational series

Let X be a finite, nonempty alphabet and denote the empty word by  $\epsilon$ . Recall that  $X^*$  is a monoid, the product is the concatenation of two words and with neutral element  $\epsilon$ .

Let K be a semiring and X an alphabet. A *formal series* (or formal power series) S is a function

$$X^* \to K.$$

The image of word w under S is denoted by (S, w) and is called the *coefficient* of w in S. The image of  $X^*$  under S is denoted by  $\Im(S)$ . The support of S is the language

$$supp(S) = \{ w \in X^* \mid (S, w) \neq 0 \}.$$

The set of formal series over X with coefficients in K is denoted by  $K\langle\langle X\rangle\rangle$ .

Let S and T be two formal series in  $K\langle\langle X\rangle\rangle$ . Then their sum is given by

$$(S + T, w) = (S, w) + (T, w)$$

and their product by

$$(ST, w) = \sum_{uv=w} (S, u)(T, v).$$

Note that here the sum is always finite. We note also that  $K\langle\langle X\rangle\rangle$  is a semiring under these operations. The identity element with respect to the product is the series 1 defined by

$$(1,w) = \begin{cases} 1_K & \text{if } w = \epsilon, \\ 0_K & \text{otherwise,} \end{cases}$$

and the identity element with respect to the sum is the series 0 defined by  $(0, w) = 0_K$ .

We also define two external operations of K in  $K\langle\langle X\rangle\rangle$ . Assume that a is in K and S in  $K\langle\langle X\rangle\rangle$ , then the series aS and Sa are defined by

$$(aS, w) = a(S, w)$$
 and  $(Sa, w) = (S, w)a$ .

A formal series with a finite support is called a *polynomial*. The set of polynomials is denoted by  $K\langle X \rangle$ .

If  $X = \{x\}$ , i.e. X is a unary alphabet, then we have the usual sets of formal power series  $K\langle\langle x \rangle\rangle = K[[x]]$  and of polynomials K[x]

A formal series S can also be written in the sum form  $S = \sum a_w w$ , where w is in  $X^*$  and  $a_w$  is the coefficient of w in K, i.e.  $(S, w) = a_w$ .

**Example 1.** Let  $X = \{x, y, z\}$  and consider the formal series in  $\mathbb{Z}\langle\langle X \rangle\rangle$  defined by S = xy + xxyz + 2zx. We get, for example, that (S, xy) = 1, (S, zx) = 2 and (S, xx) = 0.

A family of formal series, say  $(S_i)_{i \in I}$  is called *locally finite*, if, for every word w in  $X^*$ , there exists only a finite number of indices i in I such that  $(S_i, w) \neq 0$ .

A formal series S in  $K\langle\langle X\rangle\rangle$  is called *proper* if the coefficient of the empty word vanishes, that is  $(S, \epsilon) = 0$ .

Let S be proper formal series. Then the family  $(S^n)_{n\geq 0}$  is locally finite, since for any word w, if |w| > n, then  $(S^n, w) = 0$ . The sum of this family is denoted by  $S^*$ ,

$$S^* = \sum_{n \ge 0} S^n$$

and it is called the the *star* of S. Similarly we define the *plus* of S,  $S^+ = \sum_{n>1} S^n$ . Clearly  $S^0 = 1$ , and it can be proved that the equations

$$S^* = 1 + S^+$$
 and  $S^+ = SS^* = S^*S$ 

hold for proper formal series.

The rational operations in  $K\langle\langle X\rangle\rangle$  are the sum, the product, the two external products of K in  $K\langle\langle X\rangle\rangle$  and the star operation. The subset of  $K\langle\langle X\rangle\rangle$  is called rationally closed, if it is closed under the rational operations. The smallest rationally closed subset of  $K\langle\langle X\rangle\rangle$  containing a subset E of  $K\langle\langle X\rangle\rangle$  is called the rational closure of E.

A formal series is called *rational* if it is an element of the rational closure of  $K\langle X\rangle$ , i.e. it can be defined using the polynomials  $K\langle X\rangle$  and the rational operations.

**Example 2.** Denote by  $\hat{X}$  the formal series  $\sum_{x \in X} x$ .  $\hat{X}$  is proper, since  $(\hat{X}, 1) = 0$ , and rational, since it is a polynomial. The series

$$\hat{X}^* = \sum_{n \ge 0} \hat{X}^n = \sum_{w \in X^*} w.$$

is also rational.

We denote  $K^{m \times n}$ , as usual, the set of the  $m \times n$  matrices over K.

A formal series  $S \in K\langle\langle X \rangle\rangle$  is called *recognizable* if there exists an integer  $n \geq 1$ , and a morphism of monoids  $\mu : X^* \to K^{n \times n}$ , into the multiplicative structure of  $K^{n \times n}$ , and two matrices (or vectors)  $\tau \in K^{n \times 1}$  and  $\rho \in K^{1 \times n}$  such that for all words w,

$$(S, w) = \tau \mu(w)\rho.$$

The triple  $(\tau, \mu, \rho)$  is called a *linear representation* of S with *dimension* n.

A linear representation of a rational series S is called *reduced*, if its dimension is minimum among all linear representations of S.

Note that if we define  $\tau$  and  $\rho$  as vectors in  $K^n$ , then

$$(S,w) = \tau \mu(w) \rho^T$$

The next theorem is fundamental in the theory of rational series. It was first proved by Kleene in 1956 for languages that are those series with coefficients in the Boolean semiring. It was later extended by Schützenberger [Scb] to arbitrary semirings.

**Theorem 8.1.** A formal series is recognizable if and only if it is rational.

The proof by Schützenberger uses some properties of K-modules and it is quite long, and omitted here.

It is clear by the definition of recognizable series that we can transform our problem of matrices into rational series quite nicely.

From now on we shall fix the alphabet to be  $X = \{x\}$ . We denote the formal series S over X by

$$S = \sum_{n \ge 0} a_n x^n = \sum a_n x^n.$$

A rational series is called *regular*, if it has a linear representations  $(\tau, \mu, \rho)$  such that  $\mu(x)$  is an invertible matrix.

There are also other ways to define regular series. It can be proved that for a regular series S, any reduced linear representation  $(\tau, \mu, \rho)$  has invertible  $\mu(x)$ .

Assume that  $K = \mathbb{Z}$  and that S is a rational series in  $\mathbb{Z}[[x]]$  having a linear representation  $(\tau, \mu, \rho)$ , and moreover that the characteristic polynomial of the matrix  $\mu(x)$  in  $\mathbb{Z}^{k \times k}$  is  $c(\lambda)$ . Then

$$c(\lambda) = (-1)^k (\lambda^k + c_1 \lambda^{k-1} + \dots + c_k),$$

where  $c_i$ 's are in  $\mathbb{Z}$  and k is the dimension of the linear representation  $(\tau, \mu, \rho)$ . By the Cayley-Hamilton theorem we know that

$$c(\mu(x)) = \mu(x^k) + c_1\mu(x^{k-1}) + \dots + c_kI = 0.$$

If we multiply this equation from the left by  $\tau \mu(x^n)$   $(n \in \mathbb{N})$  and from the right by  $\rho$ , we get

$$a_{n+k} + c_1 a_{n+k-1} + \dots + c_k a_n = 0.$$
(8.1)

The equation

$$a_{n+h} + \beta_1 a_{n+h-1} + \dots + \beta_h a_n = 0,$$

for  $n \ge 0$ , satisfied by rational series  $S = \sum a_n x^n$  in  $\mathbb{Z}[[x]]$  is called a *linear* recurrence relation. A linear recurrence relation is called *proper*, if  $\beta_h \ne 0$ .

Note that having a linear recurrence relation, every  $a_n$  for  $n \ge h$  can be computed if we know the elements  $a_0, a_1, \ldots, a_{h-1}$  of the series S. These h first elements are called the *starting conditions*.

Next lemma gives a method to calculate a regular linear representation from a proper linear recurrence relation. **Lemma 8.1.** If rational series  $S \in \mathbb{Z}[[x]]$  satisfies a proper linear recurrence relation, then it is has a regular linear representation  $(\tau_1, \mu_1, \rho_1)$ , i.e. a linear representation satisfying det $(\mu_1(x)) \neq 0$ .

*Proof.* Let

$$a_{n+h} - \beta_1 a_{n+h-1} - \dots - \beta_h a_n = 0$$

be a proper linear recurrence relation of S and assume that  $a_j$ 's,  $0 \le j < h$ , are the starting conditions. Let

$$\tau_1 = (1, 0, \dots, 0), \quad \mu_1(x) = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & \dots & 1 \\ \beta_h & \dots & \dots & \beta_1 \end{pmatrix}, \quad \rho_1 = \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{h-1} \end{pmatrix}.$$

The matrix  $\mu_1(x)$  is called the *companion matrix*. It is easy to see that  $\det(\mu_1(x)) = \pm \beta_h \neq 0$ . Now  $\tau_1 \mu_1(x^j)$  gives the first row of matrix  $\mu_1(x^j)$ . If  $0 \leq j \leq h-1$ , then the first row of  $\mu_1(x^j)$  has 1 in the j'th entry and all the others are 0. Therefore  $\tau_1 \mu_1(x^j)\rho_1 = a_j$ , if  $0 \leq j \leq h-1$ .

To prove that  $a_n = \tau_1 \mu(x^n) \rho_1$  for all  $n \ge 0$ , we use the method mentioned before the lemma, i.e. we calculate the characteristic polynomial of  $\mu_1(x)$  to get a linear recurrence relation. So we calculate

$$\det(\mu_1(x) - \lambda I) = \begin{vmatrix} -\lambda & 1 & 0 & \cdots & 0\\ 0 & -\lambda & 1 & \cdots & 0\\ \vdots & \ddots & \ddots & \ddots & \vdots\\ \vdots & \ddots & 0 & -\lambda & 1\\ \beta_h & \dots & \beta_1 - \lambda \end{vmatrix}$$
$$= \sum_{i=1}^h (-1)^{i-1} \beta_i (-\lambda)^{h-i} + (-\lambda)^h,$$

where the last equality follows from the definition of the determinant in Section 2.3:

$$\det((A_{ij})_{n\times n}) = \sum_{\alpha} \operatorname{sign}(j_1, j_2, \dots, j_n) A_{1j_1} A_{2j_2} \cdots A_{nj_n},$$

where  $\alpha$  represents a permutation of the set  $\{1, \ldots, n\}$ , and from the fact that only permutations with non-zero product are of the form  $(1, \ldots, i-1, i+1)$ 

 $1, \ldots, h, i$ ). These permutations have i - 1 inversions, and the signs of these permutations are  $(-1)^{i-1}$ . The last term  $(-\lambda)^h$  follows from the permutation  $(h, 1, \ldots, h-1)$  and from the element  $\beta_1 - \lambda$  in the product. Now

$$\det(\mu_1(x) - \lambda I) = (-1)^h \left( \sum_{i=1}^h (-1)^{i-1-i} \beta_i \lambda^{h-1} + \lambda^h \right)$$
  
=  $(-1)^h (\lambda - \beta_1 \lambda^{h-1} - \dots - \beta_h).$ 

Thus the rational series with linear representation  $(\tau_1, \mu_1, \rho_1)$  satisfies the same linear recurrence relation than S. Therefore they are equal.

Note that one way to define the regular rational series is to use the fact that they satisfy a proper linear recurrence relation.

#### 8.2 Skolem's theorem

In this section we prove an important theorem concerning the zeros in rational series over  $\{x\}$  with coefficients in  $\mathbb{Z}$ , namely a theorem proved by Skolem in 1934.

**Theorem 8.2.** Let  $S = \sum a_n x^n$  be a rational series with coefficients in  $\mathbb{Z}$ . Then the set

$$\{n \in \mathbb{N} \mid a_n = 0\}$$

is a union of a finite set and of a finite number of arithmetic progressions.

The proof we give here is based on the proof by G. Hansel in [Han], cf. also [BeR]. Hansel proved the theorem for rational series with coefficients in the fields of characteristic 0. His first step was to prove the claim for regular rational series with coefficients in  $\mathbb{Z}$ . We use that proof up to that point, and then present a proof for all rational series with coefficients in  $\mathbb{Z}$ . The proof requires several definitions and lemmas.

A set A of natural numbers is called *purely periodic*, if there exists a natural number N and integers  $k_1, k_2, \ldots, k_r \in \{0, 1, \ldots, N-1\}$  such that

$$A = \{k_i + nN \mid n \in \mathbb{N}, \quad 1 \le i \le r\}.$$

The integer N is called a *period* of A. A *quasiperiodic* set of period N is a subset of  $\mathbb{N}$  that is a union of a finite set and a purely periodic set of period N.

**Lemma 8.2.** The intersection of a family of quasiperiodic sets of period N is a quasiperiodic set of period N.

*Proof.* Let  $(A_i)_{i \in I}$  be a family of quasiperiodic sets, all having period N. For all  $j \in \{0, 1, \ldots, N-1\}$  and for all i in I, the set  $(j + nN) \cap A_i$  is either finite or equal to (j + nN). Clearly the same holds for  $(j + nN) \cap (\bigcap_{i \in I} A_i)$  and therefore the intersection  $\cap A_i$  is quasiperiodic.

Assume that  $S = \sum a_n x^n$  is a rational series. We denote the set  $\{n \in \mathbb{N} \mid a_n = 0\}$  by  $\operatorname{ann}(S)$ , and it is called the *annihilator* of S. Clearly the annihilator is the complement of the support defined in the previous section.

Let  $v_p$  be the *p*-adic valuation defined in the previous chapter. Our next Lemma states an inequality, which we shall use later. Recall first that

$$v_p(q_1\cdots q_n) = \sum_{i=1}^n v_p(q_i)$$

and

$$v_p(q_1 + \dots + q_n) \ge \inf\{v_p(q_1), \dots, v_p(q_n)\},\$$

where  $q_i$ 's are in  $\mathbb{Q}$ .

**Lemma 8.3.** If p is a prime number and n a natural number, then

$$v_p\left(\frac{p^n}{n!}\right) \ge n\frac{p-2}{p-1}.$$

*Proof.* First, since  $\lfloor n/p \rfloor$  of the numbers  $1, \ldots, n$  are dividable by  $p, \lfloor n/p^2 \rfloor$  are dividable by  $p^2$  and so on, we have that

$$v_p(n!) \le \lfloor n/p \rfloor + \lfloor n/p^2 \rfloor + \ldots + \lfloor n/p^k \rfloor + \ldots$$
$$\le n/p + n/p^2 + \ldots + n/p^k + \ldots \le n/(p-1).$$

Therefore,

$$v_p\left(\frac{p^n}{n!}\right) = n - v_p(n!) \ge n - \frac{n}{p-1} = n\frac{p-2}{p-1}.$$

Consider next an arbitrary polynomial  $P(x) = a_0 + a_1 x + \ldots + a_n x^n$  in  $\mathbb{Q}[x]$ . For any integer  $k \ge 0$ , let

$$\omega_k(P) = \inf\{v_p(a_j) \mid j \ge k\}.$$

Clearly,

$$\omega_0(P) \leq \omega_1(P) \leq \ldots \leq \omega_k(P) \leq \ldots$$

and for k > n,

$$\omega_k(P) = \infty.$$

Note also that  $v_p(P(t)) \ge \inf\{v_p(a_0), v_p(a_1t), \ldots, v_p(a_nt^n)\}$  for any integer t, and therefore

$$v_p(P(t)) \ge \omega_0(P). \tag{8.2}$$

**Lemma 8.4.** Let P and Q be two polynomials with rational coefficients such that

$$P(x) = (x - t)Q(x)$$

for some  $t \in \mathbb{Z}$ . Then for all  $k \in \mathbb{N}$ 

$$\omega_{k+1}(P) \le \omega_k(Q).$$

*Proof.* Assume that

$$Q(x) = a_0 + a_1 x + \dots + a_n x^n,$$
  

$$P(x) = b_0 + b_1 x + \dots + b_{n+1} x^{n+1}.$$

Then  $b_{j+1} = a_j - ta_{j+1}$ , for  $0 \le j \le n-1$ , and  $b_{n+1} = a_n$ , and therefore for  $j = 0, \ldots, n$ 

$$a_j = b_{j+1} + tb_{j+2} + \dots + t^{n-j}b_{n+1}$$

It follows that  $v_p(a_j) \ge \omega_{j+1}(P)$  for any j in  $\mathbb{N}$ . Thus, for any given k in  $\mathbb{N}$ , if  $j \ge k$ , then

$$v_p(a_j) \ge \omega_{j+1}(P) \ge \omega_{k+1}(P),$$

and consequently,

$$\omega_k(Q) \ge \omega_{k+1}(P).$$

Our next corollary is a straightforward extension of the previous lemma.

**Corollary 8.1.** Let Q be a polynomial with rational coefficients, and assume that  $t_1, t_2, \ldots, t_k$  are in  $\mathbb{Z}$  and let

$$P(x) = (x - t_1)(x - t_2) \cdots (x - t_k)Q(x).$$

Then  $\omega_k(P) \leq \omega_0(Q)$ .

The main argument in our proof of Skolem's theorem is the following lemma.

**Lemma 8.5.** Let  $(d_n)_{n \in \mathbb{N}}$  be any sequence of integers and let  $(b_n)_{n \in \mathbb{N}}$  be the sequence defined by

$$b_n = \sum_{i=0}^n \binom{n}{i} p^i d_i$$

where p is an odd prime number. If  $b_n = 0$  for infinitely many indices n, then the sequence  $b_n$  vanishes, i.e.  $b_n = 0$  for all n in  $\mathbb{N}$ .

*Proof.* For n in  $\mathbb{N}$ , let

$$R_n(x) = \sum_{i=0}^n d_i p^i \frac{x(x-1)\cdots(x-i+1)}{i!}.$$

Then for t in  $\mathbb{N}$ ,

$$R_n(t) = \sum_{i=0}^n d_i p^i \frac{t(t-1)\cdots(t-i+1)}{i!} = \sum_{i=0}^n d_i p^i \frac{t!}{i!(t-i)!}$$
$$= \sum_{i=0}^n \binom{t}{i} p^i d_i$$

and since  $\binom{t}{i} = 0$  for i > t, it follows that

$$b_t = R_t(t) = R_n(t) \quad \text{for } n \ge t.$$
(8.3)

Next, we show that for all  $k, n \ge 0$ ,

$$\omega_k(R_n) \ge k \frac{p-2}{p-1}$$

For this we write  $R_n(x) = \sum_{i=0}^n c_i^{(n)} x^k$ . Clearly each  $c_k^{(n)}$  is a linear combination, with integer coefficients, of the numbers  $d_i \frac{p^i}{i!}$ , for indices *i* with  $k \leq i \leq n$ , i.e

$$c_k^{(n)} = a_k d_k \frac{p^k}{k!} + a_{k+1} d_{k+1} \frac{p^{k+1}}{(k+1)!} + \dots + a_n d_n \frac{p^n}{n!},$$

where  $a_j$ 's are integers. Consequently,

$$v_p(c_k^{(n)}) \ge \inf_{k \le i \le n} \left( v_p\left(d_i \frac{p^i}{i!}\right) \right),$$

and so Lemma 8.3 implies that

$$v_p(c_k^{(n)}) \ge \inf_{k \le i \le n} \left(i\frac{p-2}{p-1}\right) \ge k\frac{p-1}{p-2},$$

which in turn shows that

$$\omega_k(R_n(x)) \ge k \frac{p-2}{p-1}.$$
(8.4)

Consider now any coefficient  $b_t$  of the sequence  $(b_n)_{n \in \mathbb{N}}$ . We shall see that, for any integer k,

$$v_p(b_t) \ge k \frac{p-2}{p-1},$$

which means that  $b_t = 0$ . For this, let  $t_1 < t_2 < \cdots < t_k$  be the first k indices with  $b_{t_1} = \cdots = b_{t_k} = 0$ , and let  $n \ge \max\{t, t_k\}$ . By equation (8.3),  $R_n(t_i) = b_{t_i} = 0$  for  $i = 1, \ldots, k$ . Therefore

$$R_n(x) = (x - t_1)(x - t_2) \cdots (x - t_k)Q(x)$$

for some polynomial Q(x) with integer coefficients. By Corollary 8.1 we know that  $\omega_k(R_n) \leq \omega_0(Q)$ . Now  $v_p(R_n(t)) \geq v_p(Q(t))$ , and by the equation (8.2),  $v_p(Q(t)) \geq \omega_0(Q)$ . So we get

$$v_p(R_n(t)) \ge v_p(Q(t)) \ge \omega_0(Q) \ge \omega_k(R_n).$$

Finally, by equation (8.3),  $v_p(b_t) = v_p(R_n(t))$ , and therefore it follows from equation (8.4) that

$$v_p(b_t) \ge k \frac{p-2}{p-1}$$

for all  $k \ge 0$ . This proves the claim.

We shall first prove Theorem 8.2 for regular rational series with coefficients in  $\mathbb{Z}$ .

Recall that, for a prime p,  $\mathbb{Z}_p = \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}$  is the ring, where the usual operations of the semiring  $\mathbb{Z}$  are done modulo p.  $\mathbb{Z}_p$  is a ring, since it is a semiring and furthermore, every element a of  $\mathbb{Z}_p$  has an inverse element  $a^{-1}$  in  $\mathbb{Z}_p$  such that  $a \cdot a^{-1} = 1$ .

**Lemma 8.6.** Let  $S = \sum a_n x_n$  in  $\mathbb{Z}[[x]]$  be a regular rational series and let  $(\tau, \mu, \rho)$  be a linear representation of S of minimal dimension k with integer coefficients. For any odd prime p not dividing det $(\mu(x))$ , the annihilator ann(S) is quasiperiodic of period at most  $p^{k^2}$ .

Proof. Let p be an odd prime not dividing  $\det(\mu(x))$ . Let  $n \mapsto \overline{n}$  be the canonical morphism from  $\mathbb{Z}$  to  $\mathbb{Z}_p$ , i.e.  $\overline{n}$  is in  $\{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}$  and  $n \equiv \overline{n} \pmod{p}$ . Since  $\det(\overline{\mu(x)}) = \overline{\det(\mu(x))} \neq 0$ , the matrix  $\overline{\mu(x)}$  has the inverse matrix in  $M_k(\mathbb{Z}_p)$ , and it can be calculated from the inverse matrix of  $\mu(x)$  in  $M_k(\mathbb{Q})$  by mapping every element to  $\mathbb{Z}_p$ . Now there are  $p^{k^2}$  different elements in  $M_k(\mathbb{Z}_p)$ , therefore there exist some i and j in  $\mathbb{N}, i \neq j$ , such that  $\overline{\mu(x)}^i = \overline{\mu(x)}^j$ . Since  $\overline{\mu(x)}$  has an inverse matrix, it follows that there exists an integer  $N, 0 \leq N \leq p^{k^2}$ , such that

$$\overline{\mu(x^N)} = \overline{I}.$$

This means that for the original matrix  $\mu(x)$ , there exists a matrix M with integer coefficients such that

$$\mu(x^N) = I + pM.$$

Consider a fixed integer  $j \in \{0, 1, ..., N-1\}$ , and define series

$$b_n = a_{j+nN},\tag{8.5}$$

where  $n \ge 0$ . Then

$$b_n = \tau \mu(x^{j+nN})\rho = \tau \mu(x^j)(I+pM)^n \rho = \sum_{i=0}^n \binom{n}{i} p^i \tau \mu(x^j) M^i \rho$$

 $\operatorname{since}$ 

$$(I + pM)^n = \sum_{i=0}^n \binom{n}{i} (pM)^i I^{n-i} = \sum_{i=0}^n \binom{n}{i} p^i M^i.$$

By setting  $d_i = \tau \mu(x^j) M^i \rho$ , we obtain

$$b_n = \sum_{i=0}^n \binom{n}{i} p^i d_i.$$

Now by Lemma 8.5, the sequence  $b_n$  either vanishes or contains only finitely many vanishing terms. Thus the annihilator of S is a union of finite and purely periodic sets by definition (8.5) of series  $b_n$ . Therefore  $\operatorname{ann}(S)$  is quasiperiodic.

Proof of Theorem 8.2. Let  $(\tau, \mu, \rho)$  be a linear representation of  $S = \sum a_n x^n$ in  $\mathbb{Z}[[x]]$ . If det $(\mu(x)) \neq 0$ , by Lemma 8.6, ann(S) is quasiperiodic. So we can assume that det $(\mu(x)) = 0$ .

Let  $c(\lambda)$  be the characteristic polynomial of  $\mu(x)$ ,

$$c(\lambda) = (-1)^k (\lambda^k + c_1 \lambda^{k-1} + \dots + c_k).$$

As mentioned in the previous section, the equation

$$a_{n+k} + c_1 a_{n+k-1} + \dots + c_k a_n = 0, (8.6)$$

where  $n \ge 0$ , is a linear recurrence relation satisfied by S.

Since  $c(0) = \det(\mu(x))$ , by definition of the characteristic polynomial, necessarily  $c_k = 0$ , and we may write equation (8.6) in the form

$$a_{n+k} + c_1 a_{n+k-1} + \dots + c_m a_{n+k-m} = 0$$

where  $0 \le m < k$  and  $c_m \ne 0$ . Let  $T = \sum e_n x^n$  be the rational series defined by the (proper) linear recurrence relation

$$e_{n+h} + c_1 e_{n+h-1} + \dots + c_m e_n = 0,$$

for  $n \ge 0$ , and let the starting conditions be

$$e_0 = a_{k-m}, e_1 = a_{k-m+1}, \dots, e_{h-1} = a_{k-1}$$

Now T has a linear representation  $(\tau_1, \mu_1, \rho_1)$  of Lemma 8.1, and  $det(\mu_1) = \pm c_m$  and T is regular, and so by Lemma 8.6, ann(T) is quasiperiodic. The annihilator of S is not necessarily quasiperiodic, but since

$$\operatorname{ann}(S) = \{i \mid 0 \le i < k - m, \quad a_i = 0\} \cup (\operatorname{ann}(T) + (k - m)),$$

where  $\operatorname{ann}(T) + (k - m)$  denotes the addition of (k - m) to all elements of  $\operatorname{ann}(T)$ , the annihilator of S is clearly a union of a finite set and of a finite number of arithmetic progressions.

From the proof of Skolem's theorem we obtain a corollary for the rational series over rational numbers.

**Corollary 8.2.** Let  $S = \sum a_n x^n$  be a rational series with coefficients in  $\mathbb{Q}$ . Then the set

$$\{n \in \mathbb{N} \mid a_n = 0\}$$

is a union of a finite set and of a finite number of arithmetic progressions.

Proof. Let  $(\tau, \mu, \rho)$  be a linear representation of  $S = \sum a_n x^n \in \mathbb{Q}[[x]]$ , and let q be the common multiple of the denominators of coefficients in  $\tau$ ,  $\mu$ and  $\rho$ . Then  $(q\tau, q\mu, q\rho)$  is a linear representation of rational series S' with coefficients in  $\mathbb{Z}$ . Now  $S' = \sum q^{n+2}a_n x^n$ , and therefore  $\operatorname{ann}(S) = \operatorname{ann}(S')$ .  $\Box$ 

As mentioned earlier the idea of the proof in this section is due to G. Hansel. This proof, as we saw, is elementary, but not short. Skolem's original proof and its extensions by Mahler to rational series with coefficients in algebraic number fields, and by Lech to fields of characteristic 0, were much more difficult using p-adic analysis. The last extension to rational series with coefficients in a field of characteristic 0 is referred to as Skolem–Mahler–Lech theorem.

The proofs in this section were also constructive. This is very nice from our point of view, since we are looking for an algorithm to decide whether square a matrix M has infinitely many powers k such that  $(M^k)_{1n} = 0$ .

#### 8.3 Decidability of the infinite number of zeros

We end this chapter with a theorem the proof of which is based on the constructive ideas in previous section.

**Theorem 8.3.** Given a square matrix M in  $M_n(\mathbb{Z})$ , it is decidable whether there exists an infinite number of natural numbers k such that  $(M^k)_{1n} = 0$ , i.e.  $M^k$  has zero in the right upper corner.

*Proof.* We construct a rational series  $S = \sum a_k x^k$ , where  $a_k = (M^k)_{1n}$ . Clearly this has an linear representation  $(\tau, \mu, \rho)$ , where

$$\tau = (1, 0, \dots, 0) \in \mathbb{Z}^{1 \times n}, \quad \mu(x) = M \text{ and } \rho = (0, \dots, 0, 1)^T \in \mathbb{Z}^{n \times 1}.$$

First we decide whether  $\mu(x)$  is invertible or not, i.e. whether the linear representation  $(\tau, \mu, \rho)$  is regular. If not, we consider the regular rational series T defined in the proof of Skolem's theorem.

Now we have a regular series to consider, and we can use the proof of Lemma 8.5. By this proof we can compute the period N, and we then divide the rational series considered into series  $(b_n)_{n\geq 0}$ . We obtain N series, and from the proof we also get linear representations satisfied by these series. So we can compute linear recurrence relations satisfied by these series from the characteristic polynomials of their linear representations. Finally we know that these series  $(b_n)_{n\geq 0}$  either vanish or have only finitely many nonzero elements. If some of these series vanish then there is infinitely many n such that  $(M^k)_{1n} = 0$ , otherwise none.

## 9 Summary

We have considered many simply formulated problems in matrix theory. Some of them are proved to be decidable and some undecidable, but many problems are also left open. For instance, the freeness and the mortality problem for  $2 \times 2$  matrices and Skolem's problem for  $n \times n$  matrices, where  $n \geq 3$ , were such.

We have also seen that the Post Correspondence Problem is very useful in the proofs of the undecidability results in the matrix theory. Actually all undecidability results were based on the undecidability of PCP. They also used the same method, coding of two independent words to matrices, a method that was first used by Paterson.

We also notice that the proofs for the decidable cases are complicated, and need some backround from other branches of mathematics. We used combinatorics, graph theory and theory of rational series in these proofs.

We shall now present the results proved in this work in the form of a table. The entries are vectors of two parameters (n, k), where n is the dimension of matrices and k the number of matrices. We restrict to the cases, where matrices are over integers. Numbers n and k in the table present arbitrary values of these parameters and Skolem's problem is included in the problem of the zero in the right upper corner.

Problem	Decidable	Undecidable
Mortality	(2,2), (n,1)	$(\geq 3, 15), (\geq 45, 2)$
Freeness	(n,1)	$(\geq 3, 18)$
Finiteness	(n,k)	
Zero in the right upper corner	$(\leq 2, 1)$	$(\geq 3,7), (\geq 24,2)$
Common element		$(\geq 3,7)$

Table: Summary of decidable and undecidable matrix problems.

## References

- [BeP] J. Berstel and D. Perrin, Theory of Codes. Academic Press, 1986.
- [BeR] J. Berstel and C. Reutenauer, Rational Series and Their Languages, Springer-Verlag, 1984.
- [Cas] J. Cassaigne, personal communication.
- [CHK] J. Cassaigne, T. Harju and J. Karhumäki, On the decidability of the freeness of matrix semigroups, TUCS Technical Report No 56.
- [CKa] J. Cassaigne and J. Karhumäki, Examples of undecidable problems for 2-generator matrix semigroups, TUCS Technical Report No 57.
- [Gan] F. R. Gantmacher, The Theory of Matrices, Vol. I. Chelsea Publishing Company, New York, 1959.
- [GRS] R. Graham, R Rothschild and J. Spencer, Ramsey Theory, John Wiley & Sons, 1990.
- [HaK] T. Harju and J. Karhumäki, Morphisms, In G. Rozenberg and A. Salomaa, editors, Handbook of Formal Languages, Springer Verlag, 1997.
- [Han] G. Hansel, Une démonstration simple du théorème de Skolem-Mahler-Lech, Theoret. Comput. Sci. 43 (1986), 1-10.
- [Ja1] G. Jacob, La finitude des representations lineaires des semi-groupes est decidable, J. Algebra 52 (1978), 437-459.
- [Ja2] G. Jacob, Un algorithme calculant le cardinal, fini ou infini, des demi groups de matrices, Theoret. Comput. Sci. 5 (1977).
- [KBS] D.A. Klarner, J.-C. Birget and W. Satterfield, On the undecidability of the freeness of the integer matrix semigroups, Int. J. Algebra Comp. 1 (1991), 223-226.
- [Kro] M. Krom, An unsolvable problem with product of matrices, Math. System Theory 14 (1981), 335-337.
- [MaS] A. Mandel and I. Simon, On finite semigroups of matrices, Theoret. Comput. Sci. 5 (1977), 101-111.
- [Man] Z. Manna, Mathematical Theory of Computations, McGraw-Hill, 1974.

- [MSe] Y. Matiyasevich and G. Senizerques, Decision problems for semi Thue systems with a few rules. Manuscript, 1996.
- [Pat] M.S. Paterson, Unsolvability in  $3 \times 3$  matrices, Studies in Appl. Math. **49** (1970), 105-107.
- [Pos] E. Post, A variant of a recursively unsolvable problem, Bulletin of Amer. Math. Soc. 52 (1946), 264-268.
- [Ram] F.P. Ramsey, On a problem of formal logic, Proc. London Math. Soc. 2nd Ser. 30 (1930), 264-286.
- [Sch] P. Schultz, Mortality of 2×2 matrices, Amer. Math. Monthly 84 (1977), 463-464.
- [Scb] M.P. Schützenberger, On the definition of a family of automata, Information and Control 4 (1961), 245-270.
- [WeS] A. Weber and H. Seidl, On finitely generated monoids of matrices with entries in N, RAIRO Inform. Theor., 25 (1991), 19-38.

Turku Centre for Computer Science Lemminkäisenkatu 14 FIN-20520 Turku Finland

http://www.tucs.abo.fi



University of Turku • Department of Mathematical Sciences



Åbo Akademi University

- Department of Computer Science
- Institute for Advanced Management Systems Research



Turku School of Economics and Business Administration • Institute of Information Systems Science