On the Membership of Invertible Diagonal Matrices

Paul Bell and Igor Potapov*

Department of Computer Science,
University of Liverpool, Chadwick Building,
Peach St, Liverpool L69 7ZF, U.K.,
{pbell,igor}@csc.liv.ac.uk

Abstract. In this paper we consider decidability questions that are related to the membership problem in matrix semigroups. In particular we consider the membership of a particular invertible diagonal matrix in a matrix semigroup and then a scalar matrix, which has a separate geometric interpretation. Both problems have been open for any dimensions and are shown to be undecidable in dimenesion 4 with integral matrices and in dimension 3 with rational matrices by a reduction of the Post Correspondence Problem (PCP). Although the idea of PCP reduction is standard for such problems, we suggest a new coding technique to cover the case of diagonal matrices.

1 Introduction

In this paper we consider decidability questions that are related to the membership problem in matrix semigroups. The membership problem for a semigroup with only one generator ("is a matrix B a power of a matrix A") was known as the "orbit problem" and was shown to be decidable (in polynomial time) by Kannan and Lipton in 1986 [6]. The most natural generalization of the the "orbit problem" is the membership problem for matrix semigroups, given by a list of generators.

Problem 1. **The membership problem.** Let S be a given finitely generated semigroup of $n \times n$ matrices from $\mathbb{Z}^{n \times n}$. Determine whether a matrix M 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 $M_1 \cdot M_2 \cdots M_k = M$.

Paterson [9] showed that the problem is undecidable even for 3×3 integral matrices when he considered a special case of the membership problem for matrix semigroups - the *mortality problem* (determination of whether the zero matrix belongs to a matrix semigroup). It was show in [5] that the mortality problem is undecidable even for a case of two generators where the dimension of the matrices is at least 24.

* Work partially supported by The Nuffield Foundation grant NAL/00684/G.

The current research in this area is focused on long standing open problems in low dimensions such as freeness, membership or vector reachability prolems for 2×2 matrices and on the problems that are open in any dimension, like the membership problem of a unity matrix in a matrix semigroup [1]. A related problem, also open at the moment, asks whether the semigroup S contains a diagonal matrix [2]. In this context, we consider the following problem:

Problem 2. Given a multiplicative semigroup S generated by a finite set of $n \times n$ integer matrices and an invertible diagonal matrix M_{D}. Decide whether the semigroup S contains the matrix M_{D}.

In this paper we show that above problem is undecidable in dimension 4 and in case of rational matrices it is undecidable in dimension 3. As a corollary of the above fact we show that the membership of a scalar invertible matrix is also undecidable for a 3×3 rational matrix semigroup and 4×4 integral matrix semigroup. One of the interpretations for a scalar matrix is geometric scaling that alters the size of an object. So checking the membership of a scalar matrix gives us an answer to the following geometric problem:

Problem 3. **Scaling problem.** Given a finite set of linear transformations and a scalar $k \in \mathbb{N}$. Decide whether it is possible to have a combination of such transformations that enlarges the size of an object k times.

Both Problem 2 and Problem 3 are shown to be undecidable by a reduction of the Post Correspondence Problem (PCP) to the membership problem in an integral matrix semigroup. The idea of PCP reduction is quite common in algorithmic matrix problems [5,9,10], but in this paper we use a different technique. In particular, in the process of coding the words and indices, we design a set of matrices in such a way that only the correct order of matrix products leads to a particular matrix in a semigroup. In other words we design the semigroup generator set as a set of "tiles" that should be connected in the product with appropriate order, otherwise the product preserves some parts that cannot be reduced later.

2 Notations and Definitions

In what follows we use traditional denotations $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Z}^+$ and $\mathbb{Q}$ for the sets of naturals, integers, non-negative integers and rationals, respectively.

A *semigroup* is a pair $(S, \cdot)$, where S is a set and $\cdot$ is an associative binary operation on S. A semigroup $(S, \cdot)$ is generated by a set A of its elements iff every element of S is a finite product $a_{i_1} \cdot a_{i_2} \cdot \ldots \cdot a_{i_k}$ where $a_{i_j} \in A$. The set of $n \times n$ matrices over integers is denoted by $\mathbb{Z}^{n \times n}$. It is clear that the identity element for a semigroup $(\mathbb{Z}^{n \times n}, \cdot)$ is the identity matrix that we denote by E_n (or E). Minor $M^{j_1,\ldots,j_l}_{i_1,\ldots,i_k}$ of a matrix M is just the matrix formed from the selected rows $i_1, \ldots, i_k$ and columns $j_1, \ldots, j_l$

$$\mathbf{M} = \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{pmatrix} \qquad \mathbf{M}^{j1..jl}_{i1..1k} = \begin{pmatrix} a_{i_1,j_1} & \cdots & a_{i_1,j_l} \\ \vdots & \ddots & \vdots \\ a_{i_k,j_1} & \cdots & a_{i_k,j_l} \end{pmatrix}.$$

We denote an empty word by ϵ. The concatenation of two strings w and v is a string obtained by appending the symbols of v to the right end of w, that is, if $w = a_1 a_2 \dots a_n$ and $v = b_1 b_2 \dots b_n$ then the concatenation of w and v, denoted by $w \cdot v$ or wv, is $a_1 a_2 \dots a_n b_1 b_2 \dots b_n$. We denote a word $\underbrace{a \cdot a \cdots a}_{k}$ by a^k. The reverse of a string is obtained by writing the symbols in reverse order; if w is a string as shown above, then its reverse w^{R} is $a_n \dots a_2 a_1$. The inverse of a character a is written a^{-1} and is the unique character such that $a \cdot a^{-1}$ is equal to the identity element. For any word w, we define $\mathrm{suff}_n(w)$ to be the *suffix* of length n from the word w.

We also define a notation for use with words called an *inverse palindrome*. This is a word in which the second half is equal to the reverse and inverse of the first half of the word. For example if w is an inverse palindrome, then it can be written $w = z \cdot (z^R)^{-1}$ for some word z. It is clear that any inverse palindrome is equal to the identity element.

2.1 Two Mappings Between Words and Matrices

Now we introduce two mappings ψ and φ that give us an embedding from words to matrices. Let us consider the mapping ψ between $\{0,1\}^*$ and 2×2 matrices:

$$\psi : \epsilon \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = E \quad \psi : 0 \mapsto \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = M_0 \quad \psi : 1 \mapsto \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} = M_1$$

$$\psi : w_1 \cdot \ldots \cdot w_r \mapsto M_{w_1} \times \ldots \times M_{w_r}.$$

It is a well known fact that the mapping ψ is an isomorphism between $\{0,1\}^*$ and elements of the matrix semigroup generated by 2×2 matrices M_0 and M_1. Since for every matrix with non-zero determinant there is only one unique inverse matrix, we can also define a similar mapping φ. It can be defined using inverse matrices of the semigroup generator. Mapping φ is also an isomorphism between $\{0,1\}^*$ and elements of the matrix semigroup generated by 2×2 matrices $\{M_0^{-1}, M_1^{-1}\}$:

$$\varphi : \epsilon \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = E \quad \varphi : 0 \mapsto \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix} = M_0^{-1} \quad \varphi : 1 \mapsto \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix} = M_1^{-1}$$

$$\varphi : w_1 \cdot \ldots \cdot w_r \mapsto M_{w_1}^{-1} \times \ldots \times M_{w_r}^{-1}.$$

Note that the mappings from $w \in \{0,1\}^+$ to $w^{\mathrm{R}} \in \{0,1\}^+$ and from $\psi(u)$ to $\varphi(u^{\mathrm{R}})$ are bijective. Another very useful property of these mapping is that they can be used to define a free semigroup and group:

Proposition 1. *[4, 11] The semigroup or group generated by the pair of matrices $\psi(0)$, $\psi(1)$ is free.*

Moreover since the semigroup generated by $\{\psi(0), \psi(1)\}$ is free we can express an equality on words in terms of matrix equality:

Lemma 1. *[10] Given two words $u, v \in X^*$, $u = v$ iff $\varphi(u^{\mathrm{R}}) = (\psi(v))^{-1}$.*

From Lemma 1 and the fact that matrices $\psi(w)$ and $\varphi(w)$ have inverse matrices (elements) for any word $w \in \{0,1\}^*$, the following lemma holds:

Lemma 2. *[10] Given a binary alphabet X, a finite sequence of pairs of words in X^*:*

$$(u_1, v_1), \ldots, (u_k, v_k)$$

and a finite sequence of indexes $\{i_j\}$ with $\{i_j \in \{1..k\}\}$. The word $u = u_{i_1} \cdot \ldots \cdot u_{i_n}$ is equal to the word $v = v_{i_1} \cdot \ldots \cdot v_{i_n}$ if and only if

$$\varphi(u^{\mathrm{R}}) \times \psi(v) = E.$$

2.2 Reduced words and their cyclic permutation

Let $\Gamma = \{0, 1, 0^{-1}, 1^{-1}\}$ where $0 \equiv \varphi(0)$, $1 \equiv \varphi(1)$, $0^{-1} \equiv \psi(0)$ and $1^{-1} \equiv \psi(1)$. For any word, u, such that

$$u = y_1 \cdot y_2 \cdots y_n, \quad (y_i \in \Gamma)$$

we say that u is a reduced word if $y_i \neq y_{i+1}^{-1}$, $(1 \leq i < n)$, i.e u does not contain a subword of the type yy^{-1} for any character $y \in \Gamma$.

Let P be the semigroup generated by the matrices $\{\varphi(0), \varphi(1), \psi(0), \psi(1)\}$ shown above, using multiplication as the associative operator. We define an isomorphic mapping, ω, from any element of P to its reduced word in Γ:

$$\omega : X_{2,2} \mapsto \Gamma^* \qquad | \quad X \in P$$

We shall also define $|\omega(X)|$ to be the number of characters in $\omega(X)$ for any matrix X. It is clear that $\omega(E) = \varepsilon$ therefore $|\omega(E)| = 0$. Let $\omega_k(X)$ denote the kth symbol of $\omega(X)$ and $\omega_F(X)$ denote the final symbol of $\omega(X)$.

For any sequence $T = (t_1, t_2, \cdots, t_n)$ we define a k-cyclic permutation (or k-cyclic shift) to be the result of moving all elements to the right k times with elements overflowing from the right being inserted to the left. Thus if we shift this sequence k places to the right we get the sequence $\mathrm{suff}_k(T) \cdot T \cdot (\mathrm{suff}_k(T)^{-1})^R$ where $0 \leq k \leq n$.

3 PCP Encoding

In this section we show the idea of reducing the Post Correspondence Problem to the membership problem for an invertible diagonal matrix. Post's correspondence problem (in short, PCP) is formulated as follows: Given a finite alphabet X and a finite sequence of pairs of words in X^*: $(u_1, v_1), \ldots, (u_k, v_k)$. Is there a finite sequence of indexes $\{i_j\}$ with $\{i_j \in \{1..k\}\}$, such that $u_{i_1} \cdot \ldots \cdot u_{i_m} = v_{i_1} \cdot \ldots \cdot v_{i_m}$? PCP(n) denotes the same problem with a sequence of n pairs. Without loss of generality we assume that the alphabet X is binary.

Let us construct a generator of a matrix semigroup S. For an instance of the PCP with n pairs of words the generator contains $4n + 2$ different matrices.

1. For each pair (u_i, v_i), we will create four matrices:
   - Matrix of type 1: $U_{1,2}^{1,2} = \varphi(u^R), U_{3,4}^{3,4} = \varphi(0^i 1), U_5^5 = 1$
   - Matrix of type 2: $U_{1,2}^{1,2} = \varphi(u^R), U_{3,4}^{3,4} = \varphi(0^i 1), U_5^5 = 2$
   - Matrix of type 3: $V_{1,2}^{1,2} = \psi(v), V_{3,4}^{3,4} = \psi(0^i 1), V_5^5 = 1$
   - Matrix of type 4: $V_{1,2}^{1,2} = \psi(v), V_{3,4}^{3,4} = \psi(0^i 1), V_5^5 = 3$
2. A single matrix, M, where $M_{1,2}^{1,2} = E, M_{3,4}^{3,4} = \varphi(1), M_5^5 = 5$
3. A single matrix, N, where $N_{1,2}^{1,2} = E, N_{3,4}^{3,4} = \psi(1), N_5^5 = 7$

We assign zero to all matrix elements not defined above. Now we state the reduction lemma and give an example of such an encoding below.

Lemma 3. *An instance of PCP has a solution iff the corresponding semigroup S contains the matrix M_D*

$$M_D = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 210 \end{pmatrix}.$$

Example 1. Given an instance of the PCP, $P = (\,(101, 1), (0, 01010)\,)$. We will construct an example of how our coding will represent this problem in a semigroup and what a solution to the problem will look like.

We are given two separate 'tiles' and need to construct a solution to the PCP. We can see that P_1, P_2, P_1 is one such solution. We will have a semigroup generator G of $((4 * n) + 2) = 10$ matrices $G_1, G_2, \ldots, G_{10}$ where:

Matrix Number	Word part	Index Part	Factor part
Matrix 1 :	${G_1}_{1,2}^{1,2} = \varphi(101)$	${G_1}_{3,4}^{3,4} = \varphi(01)$	${G_1}_{5,5}^{5,5} = 1$
Matrix 2 :	${G_2}_{1,2}^{1,2} = \varphi(101)$	${G_2}_{3,4}^{3,4} = \varphi(01)$	${G_2}_{5,5}^{5,5} = 2$
Matrix 3 :	${G_3}_{1,2}^{1,2} = \varphi(0)$	${G_3}_{3,4}^{3,4} = \varphi(001)$	${G_3}_{5,5}^{5,5} = 1$
Matrix 4 :	${G_4}_{1,2}^{1,2} = \varphi(0)$	${G_4}_{3,4}^{3,4} = \varphi(001)$	${G_4}_{5,5}^{5,5} = 2$
Matrix 5 :	${G_5}_{1,2}^{1,2} = \psi(1)$	${G_5}_{3,4}^{3,4} = \psi(01)$	${G_5}_{5,5}^{5,5} = 1$
Matrix 6 :	${G_6}_{1,2}^{1,2} = \psi(1)$	${G_6}_{3,4}^{3,4} = \psi(01)$	${G_6}_{5,5}^{5,5} = 3$
Matrix 7 :	${G_7}_{1,2}^{1,2} = \psi(01010)$	${G_7}_{3,4}^{3,4} = \psi(001)$	${G_7}_{5,5}^{5,5} = 1$
Matrix 8 :	${G_8}_{1,2}^{1,2} = \psi(01010)$	${G_8}_{3,4}^{3,4} = \psi(001)$	${G_8}_{5,5}^{5,5} = 3$
Matrix 9(M) :	${G_9}_{1,2}^{1,2} = E$	${G_9}_{3,4}^{3,4} = \varphi(1)$	${G_9}_{5,5}^{5,5} = 5$
Matrix 10(N) :	${G_{10}}_{1,2}^{1,2} = E$	${G_{10}}_{3,4}^{3,4} = \psi(1)$	${G_{10}}_{5,5}^{5,5} = 7$

As stated before, a sequence from P giving a solution of PCP is 1,2,1 thus we can define the following matrix product $\Omega = G_9 \cdot G_2 \cdot G_3 \cdot G_1 \cdot G_{10} \cdot G_6 \cdot G_7 \cdot G_5$. We will now show this gives the requires form of a matrix.

Consider the word part of the matrix first, $W(\Omega) = E \cdot \varphi(101) \cdot \varphi(0) \cdot \varphi(101) \cdot E \cdot \psi(1) \cdot \psi(01010) \cdot \psi(1) = E$. Now consider the index part, $I(\Omega) = \varphi(1) \cdot \varphi(01) \cdot \varphi(001) \cdot \varphi(01) \cdot \psi(1) \cdot \psi(01) \cdot \psi(001) \cdot \psi(01) = E$. Finally we have the factorization part as a (integer) product, $I(\Omega) = 5 * 2 * 1 * 1 * 7 * 3 * 1 * 1 = 210$. This is indeed a matrix is of the required form and is a solution of the above PCP instance.

In the next section we prove Lemma 3 by showing the correctness of the presented reduction.

3.1 Correctness of the reduction

Let S be a semigroup that is constructed by the above rules for an instance of the PCP problem. We start by showing the word equation coding in minor $M_{1,2}^{1,2}$. Given a sequence of pairs of words in a binary alphabet $A = \{0, 1\}$:

$$(u_1, v_1), \ldots, (u_n, v_n).$$

Let us construct the sequence of pairs of 2×2 matrices using two mappings φ and ψ: $(\varphi(u_1), \psi(v_1)), \ldots, (\varphi(u_n), \psi(v_n))$.

Instead of equation $u = v$ we would like to consider a concatenation of two words $u^R \cdot v$ that is a palindrome in the case where $u = v$. Now we show a matrix interpretation of this concatenation. We associate 2×2 matrix C with a word w of the form $u^R \cdot v$. Initially we can think that C is an identity matrix corresponding to an empty word. The extension of a word w by a new pair of words (u_r, v_r) (i.e. that gives us $w' = u_r^R \cdot w \cdot v_r$) corresponds to the following matrix multiplication

$$C_{w'} = C_{u_r^R \cdot w \cdot v_r} = \varphi(u_r^R) \times C_w \times \psi(v_r) \tag{1}$$

According to Lemma 2 $u = u_{i_1} \cdot \ldots \cdot u_{i_n} = v_{i_1} \cdot \ldots \cdot v_{i_n} = v$ for a finite sequence of indexes $\{i_j\}$ with $\{i_j \in \{1..k\}\}$ if and only if $\varphi(u^R) \times \psi(v)$ is equal to the identity matrix. So the question of the word equality can be reduced to the problem of finding a sequence of pairwise matrix multiplications that gives us the identity matrix. Note that not only an inverse palindrome but also all its cyclic permutations are equal to the identity element.

Lemma 4. *Any k-cyclic permutation of an inverse palindrome of length n is a concatenation of two distinct (i.e. non-overlapping) inverse palindromes when $1 \leq k < n$.*

Proof. We are given a word $w = w_1 \cdot w_2 \cdots w_n$ which is an inverse palindrome (i.e. it can be written as $w = z \cdot (z^R)^{-1}$).

For a k-cyclic shift of w we will get a word of the form:

$$w' = \mathrm{suff}_k(w) \cdot w \cdot (\mathrm{suff}_k(w)^R)^{-1} \qquad | \quad 1 \leq k < n$$

In an inverse palindrome, element w_1 is inverse to w_n and w_2 is inverse to w_{n-1} etc. we can see that any cyclic permutation simply changes the order of the multiplication from left to right (i.e. $w_1 \cdot w_n$ becomes $w_n \cdot w_1$). Each time we shift right, the first sub-word increases by size 2 whilst the sub-word on the right decreases by size 2. Thus any cyclic shift of an inverse palindrome gives either one or two inverse palindromes (depending whether $k = n$).

Now by the definition of an inverse palindrome, each opposite pair from the centre outwards is inverse to each other and thus in any such word all elements cancel to give $w = \epsilon$. For any k-cyclic shift, we get one or two sub words which are inverse palindromes. In terms of matrices, this means all such cyclic permutations produce the identity matrix.

Since we cannot control the order of a matrix product in the semigroup we cannot directly apply the idea of pairwise multiplication. So we show that it is possible to avoid the pairwise matrix multiplications problem by increasing the dimension from 2 to 5 using the idea of relative matrices for index encoding.

The idea is to design such associated "tiles" for the above matrices that they disallow any products that cannot be represented as pairwise multiplications. In particular, a sequence of "tiles" in an incorrect order preserves some parts that cannot be reduced later.

We show now that using two specially designed minors of 5 dimensional matrices, $M_{3,4}^{3,4}$ and M_5^5, we can guarantee such a property. It is easy to see that the minor M_5^5 controls the exact number of appearences of auxiliary matrices and the minimum number of main matrices to avoid an empty word solution. This is achieved by assigning unique prime values to some matrices and by employing the fundamental theorem of arithmetic regarding prime factorization.

We will now prove that the index coding will only result in the identity matrix in the case that the matrix multiplication is of the correct form. The initial conditions of the following lemma are satisfied by the prime factorization in the last diagonal element of each matrix.

Lemma 5. *Let S be a set containing matrices $M = \varphi(1)$, $N = \psi(1)$, $U_i = \varphi(0^i 1)$ and $V_i = \psi(0^i 1)$ where $1 \leq i \leq n$. Let P be a set of matrices where each member of P is the product of at least one U and V matrix and exactly one M and N matrix from set S. The identity matrix is a member of the set P iff it is a cyclic permutation of the following sequence:*

$$M \cdot U_{i_1} \cdot U_{i_2} \cdots U_{i_n} \cdot N \cdot V_{i_n} \cdots V_{i_2} \cdot V_{i_1}$$

Proof. $\Leftarrow$ ¿From the definition of the lemma, we know there is 1 matrix of type M, 1 matrix of type N and at least 1 matrix of type U and V. Thus we will prove by induction that any multiplication of the above forms gives the identity element.

Let us prove the base case, when $n = 1$:

$$M \cdot U_{i_1} \cdot N \cdot V_{i_1} = \varphi(1) \cdot \varphi(0^{i_1} 1) \cdot \psi(1) \cdot \psi(0^{i_1} 1) = E$$

Let us consider a matrix multiplication of the form $U_{n+1} \cdot N \cdot V_{n+1}$:

$$\varphi(0^{n+1} 1) \cdot \psi(1) \cdot \psi(0^{n+1} 1) = \psi(1) = N \tag{1}$$

We now assume the inductive hypothesis that for any n:

$$M \cdot U_{i_1} \cdots U_{i_n} \cdot N \cdot V_{i_n} \cdots V_{i_1} = E$$

But since we showed in (1) that $U_{n+1} \cdot N \cdot V_{n+1} = N$, we can substitute this into the above expression to get the same result for $n+1$. Thus this product gives the identity matrix by the principle of induction.

We now prove that if the above form is equal to the identity matrix, all cyclic permutations are aswell.

We can clearly see that in terms of atomic matrices, the given form of matrix product is an inverse palindrome as defined in lemma 4. This can be seen by looking at an example :

$$M \cdot U_{i_1} \cdot U_{i_2} N \cdot V_{i_2} \cdot V_{i_1} = \varphi(10^{i_1}10^{i_2}1) \cdot \psi(10^{i_2}10^{i_1}1)$$

But as shown in lemma 4, any cyclic permutation of an inverse palindrome is equal to two smaller inverse palindromes (except for the trivial case where we cycle a multiple of the number of matrices and get the original word back). Further, we showed that inverse palindromes are clearly equal to the identity element. Thus any cyclic shift of the above sequence gives the identity matrix.
$\Rightarrow$ We now move to the reverse direction of the proof; proving that all identity elements must be a cyclical permutation of the following form:

$$M \cdot U_{i_1} \cdot U_{i_2} \cdots U_{i_n} \cdot N \cdot V_{i_n} \cdots V_{i_2} \cdot V_{i_1}$$

We have four different matrix “types”. We shall show that these elements cannot produce the identity element in any way other than the above form.

We first consider only U and V matrices in a product. We define a sequence of matrices by $(Y_{i_1}, Y_{i_2}, \cdots, Y_{i_n})$ where $Y_i \in \{U_i, V_i\}$. For any k, $\omega_1(U_k) = 0$ and $\omega_F(U_k) = 1$. Similarly, $\omega_1(V_k) = 0^{-1}$ and $\omega_F(V_k) = 1^{-1}$. Therefore any multiplication of these matrices will not have any consecutive inverse pairs since $1 \cdot 0^{-1} \neq E$ and $1^{-1} \cdot 0 \neq E$. More formally,

$$\left| \omega \left(\prod_{k=1}^{n} Y_{i_k} \right) \right| = \sum_{k=1}^{n} |\omega(Y_{i_k})| \quad , Y_k \in \{U_k, V_k\} \tag{2}$$

We will now prove that if we have a matrix sequence containing any consecutive products $U_i \cdot V_j$ (similarly for $V_j \cdot U_i$), it will never be able to be fully cancelled using just one M and N matrix:

Let $X = U_i \cdot V_j$ where $1 \leq i, j < n$. Given that $X = \varphi(0^i 1) \cdot \psi(0^j 1)$ and $\omega(X) = 0^i 1 (0^{-1})^j 1^{-1}$, we can see $\omega_1(X) = 0$. Since for all $Y \in S$, $\omega_F(Y) = 1$ or 1^{-1}, no matrix can be pre-multiplied to reduce the length of $\omega(X)$. Given that $\omega_F(X) = 1^{-1}$, we can *only* post multiply by M to reduce the length of $\omega(X)$ because $\omega_1(M) = 1$. Therefore $U_i \cdot V_j \cdot M = \varphi(0^i 1) \cdot \psi(0^j)$ and $\omega(U_i \cdot V_j \cdot M) = 0^i 1 (0^{-1})^j$. Again, no matrix can be pre-multiplied, but we can post-multiply by some U_k since only $\omega_1(U) = 0$. We have three cases, where $(k < j)$, $(k = j)$ and $(k > j)$ giving matrices $\varphi(0^i 1) \cdot \psi(0^{j-k}) \cdot \varphi(1)$, $\varphi(0^i 1)$ and $\varphi(0^i 1) \cdot \varphi(0^{k-j} 1)$ respectively. Since ω_F of these three matrices equals 1 it can only cancel with an N matrix. In all cases, there are now either 0 or 0^{-1} symbols on the right of the product. It can be seen however that further multiplications by the remaining U, V matrices will not fully cancel any of these products.

A similar argument holds for $X = V_j \cdot U_i$. Therefore if any matrix sequence contains consecutive elements U_i, V_j or V_j, U_i, its product cannot equal the identity matrix.

We now consider a matrix M in a product. We have four cases to consider.

1. Given $\omega(U_i \cdot M) = 0^i 11$, we see that it cannot be reduced to zero size because only N cancels with the final symbol leaving U_i and (2) shows that using only U and V matrices never gives the identity matrix.
2. $M \cdot U_i$ is of the correct form as shown in the first part of the proof.
3. $V_i \cdot M$ is of the correct form as shown in the first part of the proof.
4. Given $\omega(M \cdot V_i) = 1(0^{-1})^i 1^{-1}$. We cannot post-multiply by any remaining matrix type to reduce the number of matrix elements. We can pre-multiply this product by N but this again leaves only U and V matrices. Pre-multiplying by V_j gives a product: $\omega(V_j \cdot M \cdot V_i) = (0^{-1})^{(j+i)} 1^{-1}$, equal to V_{j+i} which cannot reduce to zero length because the M matrix has been used and only M cancels with the last element.

Since each matrix type has an inverse, the same situation occurs with the N matrix. Therefore any matrix product containing $(U_i \cdot M)$, $(M \cdot V_i)$, $(V_i \cdot N)$ or $(N \cdot U_i)$ will never be able to result in the identity element.

Thus the sequence must of the following form to produce the identity matrix:

$$\cdots V_{i_1} \cdot M \cdot U_{j_1} \cdots U_{j_n} \cdot N \cdot V_{k_m} \cdots V_{k_1} \cdot M \cdot U_{l_1} \cdots U_{l_p} \cdot N \cdot V_{h_q} \cdots$$

This pattern can repeat indefinitely, but since we only have a single M and N matrix:

$$\begin{array}{l} V_{i_m} \cdots V_{i_1} \cdot M \cdot U_{j_1} \cdots U_{j_n} \cdot N \cdot V_{k_p} \cdots V_{k_1} \ |m, p \in \mathbb{Z}^+, n \in \mathbb{N} \\ U_{i_m} \cdots U_{i_1} \cdot N \cdot V_{j_1} \cdots V_{j_n} \cdot M \cdot U_{k_p} \cdots U_{k_1} \ |m, p \in \mathbb{Z}^+, n \in \mathbb{N} \end{array}$$

Since $\varphi(1)$ is only inverse to $\psi(1)$ and each U,V matrix sequence contains exactly one of these matrices, the number of U matrices must equal the number of V matrices, thus $m + p = n$.

For the first equation, let us define two sub-sequences of matrices $\alpha_1 = (V_{i_m}, \cdots, V_{i_1}, M, U_{j_1}, \cdots, U_{j_m})$ and $\alpha_2 = (U_{j_{(n-p+1)}}, \cdots, U_{j_n}, N, V_{k_p}, \cdots, V_{k_1})$.

Assume the first equation is equal to the identity element. Now assume the contrary that $\alpha_1 \neq M$. There is an equal number of U and V matrices and the U matrices follow the M matrix therefore the last matrix in the sequence must be a U matrix. ω_F of any U is always 1. If $\alpha_2 = N$ then it will cancel with this element but leave a non-identity element in α_1(since $\alpha_1 \neq M$). Thus $\alpha_2 \neq N$ and since it has an equal number of U and V matrices and the U matrices preceed all V matrices, the first matrix in the sequence must also be some U matrix. But as shown in (2) the product of U matrices only increases the size of the sequence. The reverse argument also holds if $\alpha_2 \neq N$. Thus the resulting matrix cannot be the identity element unless $\alpha_1 = M$ and $\alpha_2 = N$.

Define $\alpha_1[i]$ to be the i'th element of the sequence. Now we prove that $\alpha_1[(m+1)-k] \cdot \alpha_1[(m+1)+k] = E$ where $(0 \leq k \leq m)$. Let us assume by contradiction that their exists some k where $\alpha_1[(m+1)-k] \cdot \alpha_1[(m+1)+k] \neq E$, i.e. 2 opposite elements who are not inverse to each other. Therefore we have:

$$V_a \cdot M \cdot U_b = \psi(0^a 1) \cdot \varphi(1) \cdot \varphi(0^b 1) \quad | a \neq b$$

If $a > b$ then it will give a matrix $\psi(0^{a-b}) \cdot \varphi(1)$. Since M has been used and N is not in this sequence however, we only have U and V matrices which (2) shows cannot reduce the length of $|\omega(\psi(0^{a-b}) \cdot \varphi(1))|$ (and $|M| = 1$). If $a < b$ then it gives a matrix $\varphi(0^{b-a}1)$ which is equal to $U_{(b-a)}$. Again, since M has been used, there are only U and V matrices left which cannot reduce to M giving a contradiction.

Similarly for α_2 we get opposite matrices produced which gives the same result that all opposite matrices from the central element (N) are inverse.

Thus in the first equation given above, it must be of the form:

$$V_{i_m} \cdots V_{i_1} \cdot M \cdot U_{i_1} \cdots U_{i_m} \cdots U_{i_n} \cdot N \cdot V_{i_n} \cdots V_{i_{n-m+1}}$$

We can clearly see that this is a cyclic permutation of the form given in the first part of the proof and the form of equation 2 is a cyclic permutation of equation 1, thus both must be equal to the identity matrix.

The proof of above lemma ends the proof of reduction from Lemma 3 since the PCP has a solution if and only if the semigroup S contains the matrix M_D. Thus the following Theorem holds:

Theorem 1. *Problem 2 is undecidable in dimension five.*

3.2 Reduction to lower dimensions

Now we can reduce the dimensions used and state some corollaries.

Corollary 1. *Problem 2 is undecidable in dimension* 4.

Proof. The element M_5^5, in our previous construction, is a scalar value and is commutative in all matrices since all other elements along row and column 5 are zero. Therefore we can multiply minor $M_{3,4}^{3,4}$ by M_5^5 and we will still preserve this value across the multiplication without changing the structure of multiplications of $M_{3,4}^{3,4}$.

Corollary 2. *Problem 3 is undecidable for linear transformations defined by a finite set of integral* 4×4 *matrices.*

Proof. In order to prove the undecidablity of Problem 3 we can show that the scalar matrix $M = 210 \cdot E_4$ is undecidable. We use the same idea as we did for Problem 2 with the only difference being that we extend the generator of the semigroup by the following matrix R:

$$\begin{pmatrix} 210 & 0 & 0 & 0 \\ 0 & 210 & 0 & 0 \\ 0 & 0 & 210 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

It is easy to see that the above matrix commutes with all other matrices in the semigroup, since the minor $M_{1,2,3}^{1,2,3}$ is a scalar matrix and M_4^4 is the identity element. On the other hand we cannot use more than one copy of matrix R since the determinant of any matrix from a semigroup that uses more than one copy of R will be more than 210^4. So the matrix $M = 210 \cdot E_4$ is reachable if and only if the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 210 \end{pmatrix}$$

is reachable and does not use R, that in turn is undecidable.

In fact we can prove an even stronger claim that membership of any non-unimodular scalar matrix over rationals is undecidable in dimension four for rational matrix semigroups.

Corollary 3. *Given a semigroup S generated by a finite set of $n \times n$ matrices over rationals and a scalar $k \in \mathbb{Q}$ such that $k \neq 1$. It is undecidable to check whether the scalar matrix $k \cdot E$ belonds to S for any $n \geq 4$.*

Proof. We use Lemma 3 to show the undecidablity of the membership problem for a scalar matrix $k \cdot E_4$ by repeating the proof of Corollary 2 and introducing another matrix R that is now equal to

$$\begin{pmatrix} k & 0 & 0 & 0 \\ 0 & k & 0 & 0 \\ 0 & 0 & k & 0 \\ 0 & 0 & 0 & \frac{k}{210} \end{pmatrix}.$$

We now use the suggestion of an anonymous referee to use our technique with different bijections ψ and φ to get an undecidability result in dimension 3 with rational matrices.

Corollary 4. *The problem of determining if a matrix $210 \cdot E_3$ is a member of a multiplicative semigroup with rational matrices is undecidable in dimension 3*

Proof. We show this result by using a different mapping for ϕ and ψ which form a free semigroup. We change this mapping for the separate minors $M_{1,2}^{1,2}$ and $M_{2,3}^{2,3}$. The mapping is such that the central element M_2^2 is always equal to 1 for all but one of the generators. This allows us to merge the two smaller minors into a single 3*3 matrix.

$$\psi_{M_{1,2}^{1,2}}(0) = \begin{pmatrix} 2 & 0 \\ 1 & 1 \end{pmatrix} \; \psi_{M_{1,2}^{1,2}}(1) = \begin{pmatrix} 2 & 0 \\ 2 & 1 \end{pmatrix} \; \varphi_{M_{1,2}^{1,2}}(0) = \begin{pmatrix} \frac{1}{2} & 0 \\ \frac{-1}{2} & 1 \end{pmatrix} \; \varphi_{M_{1,2}^{1,2}}(1) = \begin{pmatrix} \frac{1}{2} & 0 \\ -1 & 1 \end{pmatrix}$$

$$\psi_{M_{2,3}^{2,3}}(0) = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} \; \psi_{M_{2,3}^{2,3}}(1) = \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix} \; \varphi_{M_{2,3}^{2,3}}(0) = \begin{pmatrix} 1 & \frac{-1}{2} \\ 0 & \frac{1}{2} \end{pmatrix} \; \varphi_{M_{2,3}^{2,3}}(1) = \begin{pmatrix} 1 & -1 \\ 0 & \frac{1}{2} \end{pmatrix}$$

All mappings from ϵ give E_2. We can see that any product of the $M_{1,2}^{1,2}$ mapping matrices will give a 1 in element M_2^2. Similarly, any product of the $M_{2,3}^{2,3}$ mapping matrices will give a 1 in element M_2^2. These matrices also form a free group and we can therefore use them to embed the PCP problem within a 3*3 matrix as before. However, we must now multiply the whole matrix by the scalars 2,3,5,7 that were previously in M_5^5. This means we cannot use this method for an arbitrary scalar matrix but only specific ones (in this case we use the matrix $210 \cdot E$).

4 Conclusion and Some Remarks

In this paper we have proved that the membership problem of a particular invertible diagonal matrix is undecidable for a 4×4 integral matrix semigroup. Then as a corollary of this fact we have shown that the membership of a particular invertible scalar matrix is undecidable in dimension 4 for an integral matrix semigroup and in dimension 3 for rational matrix semigroup. Moreover we have shown that in dimension 4 the membership of any non-unimodular scalar matrix is undecidable for a rational matrix semigroup. The same problems for lower dimensions and the membership problem for an arbitrary diagonal matrix in a matrix semigroup are still open.

Acknowledgements We would like to thank the anonymous referees for their helpful suggestions. Special thanks to the referee who proposed the idea of different bijections that helps to get the undecidability result for dimension 3.

References

1. J.Bestel and J.Karhumäki. Combinatorics on Words - A Tutorial, Bulletin of the EATCS, February 2003, 178 - 228
2. V.Blondel, J.Cassaigne, J.Karhumäki. Problem 10.3. Freeness of multiplicative matrix semigroups. Unsolved Problems in Mathematical Systems and Control Theory, Edited by V.Blondel and A.Megretski, 309-314
3. V. Blondel and J. Tsitsiklis. A survey of computational complexity results in systems and control. Automatica, 36, 2000, 1249-1274
4. R.Graham, D.Knuth, O.Patashnik. Concrete Mathematics. 2nd edition, Addison-Wesley, 1994
5. V.Halava, T.Harju. Mortality in Matrix Semigroups, American Mathematical Monthly, Vol 108 No. 7, (2001) 649-653
6. R.Kannan and R.Lipton. Polynomial-time algorithm for the orbit problem, Journal of the ACM (JACM), Volume 33 , Issue 4, 1986, 808 - 821
7. A.Lisitsa, I.Potapov. Membership and reachability problems for row-monomial transformations. MFCS, 2004, 623-634
8. C.Moore. Unpredictability and Undecidability in Dynamical Systems, *Physical Review Letters*, Vol.64, N. 20, 1990, 2354-2357
9. M.Paterson. Unsolvability in 3×3 matrices. Studies in Applied Mathematics, 49 (1970), 105-107
10. I.Potapov. From Post systems to the reachability problems for matrix semigroups and counter automata. 8th International Conference on Developments in Language Theory (DLT04), LNCS 3340, 345-356
11. http://planetmath.org/encyclopedia/FreeGroup.html