ELSEVIER

Information Processing Letters 63 (1997) 283-286

Information Processing Letters

When is a pair of matrices mortal? [1]

Vincent D. Blondel [a,*], John N. Tsitsiklis [b,2]

[a] *Institute of Mathematics, University of Liège, Avenue des Tilleuls 15, B-4000 Liège, Belgium*

[b] *Laboratory for Information and Decision Systems, Massachusetts Institute of Technology, Cambridge, MA 02139, USA*

Received 16 July 1995
Communicated by L. Kott

Abstract

A set of matrices over the integers is said to be *k-mortal* (with k positive integer) if the zero matrix can be expressed as a product of length k of matrices in the set. The set is said to be *mortal* if it is k-mortal for some finite k. We show that the problem of deciding whether a pair of 48 × 48 integer matrices is mortal is undecidable, and that the problem of deciding, for a given k, whether a pair of matrices is k-mortal is NP-complete. © 1997 Elsevier Science B.V.

Keywords: Theory of computation; Computational complexity; Decidability; Matrix theory; Post's correspondence problem

In order to prove our first result we shall need *Post's correspondence problem* which is as follows:

Instance: A set of pairs of words $\{(U_i, V_i) \mid i = 1, \ldots, n\}$ over a finite alphabet.

Question: Does there exist a non-empty sequence of indices $i_1, i_2, \ldots, i_k$ where $1 \leqslant i_j \leqslant n$, such that $U_{i_1} U_{i_2} \cdots U_{i_k} = V_{i_1} V_{i_2} \cdots V_{i_k}$?

This problem is trivially decidable for one letter alphabets but is undecidable when the alphabet contains more than one letter (for a proof of this classical result see, e.g., [2]).

A set of real matrices Σ is said to be *mortal* if there exists a finite product of matrices in Σ that is equal to the zero matrix. In [8] Paterson uses Post's correspondence problem to show that the problem of deciding whether a given finite set of 3 × 3 integer matrices is mortal is undecidable (the case of 2 × 2 integer matrices is open, see [4] for a discussion of this case). Let n_p be any number of pairs of words for which Post's correspondence problem is undecidable. In Theorem 1, we use Paterson's result and a simple matrix argument inspired from a construction appearing in [9], to prove that the mortality of *pairs* of integer matrices of size $n \times n$ is undecidable for $n = 6(n_p + 1)$. In a recent contribution Matiyasevich and Sénizergues [5] have shown that Post's correspondence problem is already undecidable when there are seven pairs of words (the previous bound was nine, see [6]). Combined with our result, this shows that the mortality of pairs of 48 × 48 integer matrices is undecidable.

Theorem 1. *Let n_p be any number of pairs of words for which Post's correspondence problem is undecidable. Then, the mortality of two integer matrices of size $n \times n$ is undecidable for $n = 6(n_p + 1)$.*

[*] Corresponding author. Email: vblondel@ulg.ac.be.

[1] This work was completed while Blondel was visiting Tsitsiklis at MIT and was supported by the ARO under grant DAAL-03-92-G-0115 and by the NATO under grant CRG 961115.

[2] Email: jnt@mit.edu.

PII S0020-0190(97)00123-3

Proof. Let $\{B_1,\ldots,B_m\}$ be a set of $n \times n$ integer matrices. Define two $nm \times nm$ matrices by $A = \operatorname{diag}(B_1,\ldots,B_m)$ (i.e., A is block-diagonal with blocks $B_1,\ldots,B_m$ in that order) and

$$T = \begin{pmatrix} 0 & I_{n(m-1)} \\ I_n & 0 \end{pmatrix},$$

where I_r is the $r \times r$ identity matrix. Notice that $T^m = I_{nm}$ and $A_k := T^{k-1}AT^{m-(k-1)} = T^{k-1}AT^{-(k-1)} = \operatorname{diag}(B_k,\ldots,B_m,B_1,\ldots,B_{k-1})$ for $k = 1,\ldots,m$.

We claim that $\{B_1,\ldots,B_m\}$ is mortal if and only if $\{A,T\}$ is.

In order to prove our claim suppose first that $B_{i_1}\cdots B_{i_q} = 0$ for some $i_j \in \{1,\ldots,m\}$. Then, the first block of the block-diagonal matrix $A_{i_1}\cdots A_{i_q}$ is equal to zero. But then

$$P := \prod_{k=0}^{m-1} T^k(A_{i_1}\cdots A_{i_q})T^{m-k} = 0,$$

and since this product can be written as a product of matrices in $\{A,T\}$ the first implication is proved.

Suppose now that $P := T^{t_1}A^{a_1}T^{t_2}A^{a_2}\cdots T^{t_q}A^{a_q}T^{t_{q+1}} = 0$ for some integers t_i, a_i and assume without loss of generality that $0 \leqslant t_i \leqslant m-1$. We clearly have

$$\begin{aligned} P &= T^{t_1}A^{a_1}T^{m-t_1}T^{t_1+t_2-m}A^{a_2}\cdots T^{t_q}A^{a_q}T^{t_{q+1}} \\ &= (A_{t_1+1})^{a_1}T^{t_1+t_2-m}A^{a_2}\cdots T^{t_q}A^{a_q}T^{t_{q+1}}. \end{aligned}$$

By recursion we are lead to

$$T = (A_{p_1})^{a_1}\cdots(A_{p_q})^{a_q}T^{t_*} = 0$$

for some $t_* \geqslant 0$ and $1 \leqslant p_i \leqslant m$ $(i = 1,\ldots,q)$. The matrices A_k are block diagonal and the second implication is therefore proved.

Mortality of the $nm \times nm$ matrices A and T is thus equivalent to that of the m $n \times n$ matrices $\{B_1,\ldots,B_m\}$. It is shown in [8] that the latter problem is undecidable for 3×3 integer matrices. The proof given by Paterson uses a reduction from Post's correspondence problem with n_p pairs of words to mortality of $2(n_p+1)$ 3×3 integer matrices. By our construction we are lead to two matrices of size $6(n_p+1) \times 6(n_p+1)$ and the proof is therefore complete. □

Remarks. (1) The number of matrices involved in Paterson's proof can be reduced to $(4+n_p)$ by using the modified Post's correspondence problem (see [2]). Therefore, the mortality of two integer matrices of size $n \times n$ is undecidable for $n = 3(n_p+4)$ where n_p is any number of pairs of words for which Post's correspondence problem is undecidable. For $n_p = 7$ this shows undecidability of the mortality of pairs of 33×33 integer matrices. This improvement was brought to our attention by M. Branicky [1].

(2) When the entries of the matrices are nonnegative, then mortality becomes decidable but computationally intractable (NP-complete). We make a comment on this after Theorem 2.

Using a reduction from the classical SAT problem [3] we now show that the a priori bounded version of mortality is NP-complete. (Notice that it is trivially decidable.) Our proof is partly inspired from a reduction technique used in [7] and is similar to the proof of the main result in [10].

k-MORTALITY OF A PAIR OF MATRICES
Instance: $k \geqslant 1$ (encoded in unary), $A_0, A_1 \in \mathbb{Z}^{n\times n}$.
Problem: Do there exist $i_j \in \{0,1\}$ for $j = 1,\ldots,k$ such that $A_{i_1}\cdots A_{i_k} = 0$?

Theorem 2. *k-*MORTALITY OF A PAIR OF MATRICES *is* NP*-complete.*

Proof. k-MORTALITY OF A PAIR OF MATRICES clearly belongs to NP; this is because "yes" instances have a certificate $i_1,\ldots,i_k$ that can be checked by means of $k-1$ multiplication of the $n \times n$ matrices $A_{i_1},\ldots,A_{i_k}$. Since k is encoded in unary, the certificate checking algorithm runs in time polynomial in k and n. Thus, it suffices to exhibit a reduction from SAT.

Starting from an instance of SAT with n variables $x_1,\ldots,x_n$ and m clauses $C_1,\ldots,C_m$, we construct two directed graphs G_0 and G_1. The graphs have identical nodes but have different edges. Besides the start node s, there is a node u_{ij} associated to each clause C_i and variable x_j, a 0th node u_{0j} associated to each variable x_j, and a $(n+1)$th node $u_{i(n+1)}$ associated to each clause C_i. Edges are constructed as follows: For $i = 1,\ldots,m$ and $j = 1,\ldots,n$ there is

- an edge $(u_{ij}, u_{i(j+1)})$ in both G_0 and G_1 if the variable x_j does not appear in clause C_i,

- an edge (u_{ij}, u_{0j}) in G_0 and an edge $(u_{ij}, u_{i(j+1)})$ in G_1 if the variable x_j appears in clause C_i negatively,
- an edge (u_{ij}, u_{0j}) in G_1 and an edge $(u_{ij}, u_{i(j+1)})$ in G_0 if the variable x_j appears in clause C_i positively.

For $i = 1, \ldots, m$ there are edges (s, u_{i1}) and edges $(u_{i(n+1)}, s)$ in both graphs. Finally, the graphs have edges $(u_{0j}, u_{0(j+1)})$ for $j = 1, \ldots, n-1$. There are no edges leaving from u_{0n}.

Let r denote the total number of nodes ($r = (n+1)(m+1)$). We construct two $r \times r$ matrices A_0 and A_1. Associated to the graph G_0 (respectively, G_1) is the $r \times r$ adjacency matrix A_0 (respectively, A_1) whose (i, j)th entry is equal to 1 if there is an edge from node j to node i in G_0 (respectively G_1), and is equal to zero otherwise. (Thus, the jth column is associated with edges that leave node j.) Let $k = (n+1)(n+3)$. We claim that the set $\{A_0, A_1\}$ is k-mortal iff the instance of SAT is satisfiable. Since all transformations are performed in polynomial time, this claim will establish the theorem.

To any given node α we associate a column-vector $x(\alpha)$ of dimension r whose entries are all zero with the exception of the entry corresponding to the node α which is equal to one. We need two observations for proving our claim.

(1) Let a partition of the nodes be given by $P_{n+2} = \{s\}$, $P_{n+1} = \{u_{i1} \mid i = 1, \ldots, m\}$, $P_n = \{u_{01}, u_{i2} \mid i = 1, \ldots, m\}$, …, $P_2 = \{u_{0(n-1)}, u_{in} \mid i = 1, \ldots, m\}$ and $P_1 = \{u_{0n}, u_{i(n+1)} \mid i = 1, \ldots, m\}$. We use l_α to denote the index of the partition to which the node α belongs. Any edge (from G_0 or G_1) leaving from a node of partition P_h goes to a node of partition P_{h-1}. Furthermore, the edges leaving from partition P_1 go back to partition P_{n+2}. Thus, any path in G_0 and G_1 that starts from node α either gets to the node u_{0n}, from which there is no outgoing edge, or it visits node s after l_α steps. In matrix terms this implies the following. Let α be an arbitrary node and let l_α be its associated partition index. If h is a positive integer equal to l_α modulo $(n+2)$ and A is a product of h factors in $\{A_0, A_1\}$, then

$$Ax(\alpha) = \mu x(s) \tag{1}$$

for some nonnegative scalar μ.

(2) Let $q_1, \ldots, q_n \in \{0, 1\}$ be a truth assignment of the boolean variables x_j and consider the product $A_{q_n} \cdots A_{q_1}$. The vector $A_{q_n} \cdots A_{q_1} x(u_{i1})$ is equal to $x(u_{0n})$ if the clause C_i is satisfied and is equal to $x(u_{i(n+1)})$ otherwise. Let A_* be any of A_0 or A_1. There are no edges leaving from u_{0n} and there are edges from s to u_{i1} for $i = 1, \ldots, m$. Thus we have $A_* x(u_{0n}) = 0$ and $A_* x(s) = \sum_{i=1}^m x(u_{i1})$. From this we conclude

$$\begin{aligned} A_* A_{q_n} \cdots A_{q_1} A_* x(s) &= A_* A_{q_n} \cdots A_{q_1} \sum_{i=1}^m x(u_{i1}) \\ &= A_* \sum_{i=1}^m A_{q_n} \cdots A_{q_1} x(u_{i1}) = \lambda x(s), \end{aligned} \tag{2}$$

where λ is equal to the number of clauses that are *not* satisfied by the given truth assignment.

With these two observations we now prove the claim. Assume that the instance of SAT is satisfied by the assignment $x_i = q_i$ for $q_1, \ldots, q_n \in \{0, 1\}$ and define A by $A = A_* A_{q_n} \cdots A_{q_1} A_*$ with A_* any of A_0 or A_1. Since all clauses are satisfied, Eq. (2) gives $Ax(s) = 0$. Using Eq. (1), we infer

$$(A_* A)^{(n+1)} x(\alpha) = 0,$$

for all α. Since $\mathbb{R}^r$ is spanned by $x(\alpha)$ when α ranges over the nodes, we conclude that

$$(A_* A)^{(n+1)} = 0$$

and the set $\{A_0, A_1\}$ is k-mortal for $k = (n+1)(n+3)$.

For the reverse implication, assume that the instance of SAT is not satisfiable and consider any product of $n+2$ factors $A_{q_0} \cdots A_{q_{n+1}}$. Since the instance is not satisfiable, we infer from Eq. (2) that

$$A_{q_0} \cdots A_{q_{n+1}} x(s) \geqslant x(s). \tag{3}$$

Let A be an arbitrary product of k matrices. A^{n+2} is a product of $(n+2)k$ matrices and Eq. (3) gives $A^{n+2} x(s) \geqslant x(s)$, hence $A \neq 0$. Since A was arbitrary the proof is complete. □

Remarks. (1) In Theorem 2 we assume k to be encoded in unary. The reason for this is that the certificate checking algorithm runs in time polynomial in k and n. If k was encoded in a non-unary base, the certificate checking algorithm would run in time exponential in the size of k and the proof of the membership in NP would fail. Thus, when k is encoded in non-unary decimal expansion, k-mortality of a pair of matrices becomes NP-hard.

(2) The proof of Theorem 2 involves only boolean matrices (i.e., matrices with entries in $\{0,1\}$). Thus, the theorem remains valid in the special case where we restrict all matrices in the given family to have $\{0,1\}$ (or nonnegative) entries.

(3) As already mentioned in a remark after Theorem 1, we claim that the mortality of a pair of matrices that have nonnegative entries is decidable, and is NP-complete. Our argument is as follows. The mortality of any set of matrices with nonnegative entries is equivalent to the mortality of the associated set of boolean matrices whose entries are put to zero (respectively, one) when the corresponding entry in the initial matrix is equal to zero (respectively, positive). Because there are at most 2^{n^2} boolean matrices of dimension $n \times n$, any elements of the semigroup generated by a pair of boolean matrices can be written as a product whose length is less than 2^{n^2}. Mortality can thus be checked by simple enumeration.

By a small adaptation of the proof of Theorem 2 one can show that mortality of a pair of matrices with nonnegative entries is NP-complete. As before, the proof involves only boolean matrices and thus the problem remains NP-complete when the given matrices are boolean.

(4) Using a reduction similar to the one used in the proof of Theorem 2, we can establish that the problem of deciding the stability of all products of a given pair of matrices is NP-hard. This, together with other results on the exact and approximate computation of the generalized spectral radius of a set of matrices, is given in [10].

References

[1] M. Branicky, Personal communication, May 1996.

[2] J.E. Hopcroft and J.D. Ullman, *Formal Languages and Their Relation to Automata* (Addison-Wesley, Reading, MA, 1969).

[3] M.R. Garey and D.S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness* (Freeman and Co., New York, 1979).

[4] M. Krom and M. Krom, Recursive solvability of problems with matrices, *Z. Math. Logik Grundlag. Math.* 35 (1989) 437-442.

[5] Y. Matiyasevich and G. Sénizergues, Decision problem for semi-Thue systems with a few rules, Preprint, 1996.

[6] J.J. Pansiot, A note on Post's correspondence problem, *Inform. Process. Lett.* 12 (1981) 233.

[7] C.H. Papadimitriou and J.N. Tsitsiklis, The complexity of Markov decision processes, *Math. Oper. Res.* 12 (1987) 441-450.

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

[9] O. Toker, On the algorithmic unsolvability of some stability problems for discrete event systems, in: *Proc. IFAC World Congress* (1996) 353-358.

[10] J.N. Tsitsiklis and V.D. Blondel, Spectral quantities associated to pairs of matrices are hard - when not impossible - to compute and to approximate, Tech. Rept. LIDS-P-2325, Laboratory for Information and Decision Systems, M.I.T., Cambridge, MA, 1996; also in: *Math. Control Signals Systems*, to appear.