JANUARY 1996

LIDS-P-2314
Submitted to Information
Processing Letters

When is a pair of matrices mortal? *

Vincent D. Blondel[†] John N. Tsitsiklis[‡]

January 4, 1996

Abstract

A set of matrices over the integers is said to be *length-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 length-k-mortal for some finite k. We show that the problem of deciding whether a pair of 33×33 integer matrices is mortal is undecidable, and that the problem of deciding, for a given k, whether a pair of matrices is length-k-mortal is NP-complete.

Keywords

Theory of Computation, Computational Complexity, Decidability, Matrix theory.

In [5] 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 2×2 case is open, see [2] for a discussion). We use Paterson's result and a simple matrix argument (inspired from a construction appearing in [6]) to prove undecidability of the mortality of *pairs* of 33×33 integer matrices.

MORTALITY OF A PAIR OF 33×33 MATRICES

Instance: $A_0, A_1 \in \mathbf{Z}^{33\times 33}$.

Problem: Does there exist a finite product of A_0 and A_1 that is equal to the zero matrix?

Theorem 1 MORTALITY OF A PAIR OF 33×33 MATRICES is undecidable.

*This work was completed while Blondel was visiting Tsitsiklis at MIT and was supported by the ARO under grant DAAL-03-92-G-0115.

[†] Institute of Mathematics, University of Liège, Avenue des Tilleuls 15, B-4000 Liège, Belgium; email: blondel@math.ulg.ac.be

[‡] Laboratory for Information and Decision Systems, Massachusetts Institute of Technology, Cambridge, MA 02139, USA; email: jnt@mit.edu

Proof

Let $\{B_1, \cdots, B_m\}$ be a set of $n \times n$ integer matrices. Define two $nm \times nm$ matrices by $A = \mathrm{diag}(B_1, \cdots, B_m)$ (i.e., A is block-diagonal with blocks $B_1, \cdots, B_m$ 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 $A_k := T^{k-1} A T^{m-(k-1)} = T^{k-1} A T^{-(k-1)} = \mathrm{diag}(B_k, \cdots, B_m, B_1, \cdots, B_{k-1})$ for $k = 1, \cdots, m$.

We claim that $\{B_1, \cdots, B_m\}$ 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 $i_j \in \{1, \cdots, m\}$. 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 $P := T^{t_1} A^{a_1} T^{t_2} \cdots T^{t_q} A^{a_q} T^{t_{q+1}} = 0$ for some t_i, a_i and assume without loss of generality that $0 \leq t_i \leq m - 1$. We clearly have

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

By recursion we are thus lead to

$$T = (A_{t_1+1})^{a_1} \cdots (A_{t_q+1})^{a_q} T^{t_*} = 0$$

for some $t_* \geq 0$. The matrices A_k are block diagonal and the second implication is therefore proved.

The mortality of the $nm \times nm$ matrices A and T is thus equivalent to that of the m $n \times n$ matrices $\{B_1, \cdots, B_m\}$. It is shown in Paterson [5] that the latter problem is undecidable for integer matrices when $n = 3$. The proof given by Paterson uses a reduction from Post's correspondence problem. It is shown in [3] that Post's correspondence problem remains undecidable when the number of pairs of words is equal to nine. This leads to eleven 3×3 integer matrices in Paterson's proof and our proof is therefore complete. □

Using a reduction from the classical SAT problem [1] we now show that the a priori bounded version of MORTALITY OF A PAIR OF MATRICES is NP-complete. (Notice that it is trivially decidable.) Our proof is partly inspired from a reduction technique used in

[4] and is similar to the proof of the main result in [7].

K-MORTALITY OF A PAIR OF MATRICES

Instance: $k \geq 1$ (encoded in unary), $A_0, A_1 \in \mathbf{Z}^{n \times n}$.

Problem: Do there exist $i_j \in \{0,1\}$ for $j = 1, \cdots, k$ 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 $x_1, \cdots, x_n$ and m clauses $C_1, \cdots, C_m$, 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 a_{ij} associated to each clause C_i and variable x_j, a 0-th node a_{0j} associated to each variable x_j, and a $(n+1)$-th node $a_{i(n+1)}$ associated to each clause C_i. Edges are constructed as follows: For $i = 1, \cdots, m$ and $j = 1, \cdots, n$ there is

- an edge $(a_{ij}, a_{i(j+1)})$ in both G_0 and G_1 if the variable x_j does not appear in clause C_i;
- an edge (a_{ij}, a_{0j}) in G_0 and an edge $(a_{ij}, a_{i(j+1)})$ in G_1 if the variable x_j appears in clause C_i negatively;
- an edge (a_{ij}, a_{0j}) in G_1 and an edge $(a_{ij}, a_{i(j+1)})$ in G_0 if the variable x_j appears in clause C_i positively.

For $i = 1, \cdots, m$ there are edges (s, a_{i1}) and edges $(a_{i(n+1)}, s)$ in both graphs. Finally, the graphs have edges $(a_{0j}, a_{0(j+1)})$ for $j = 1, \cdots, n-1$. There are no edges leaving a_{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 j-th 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 length-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 $P_0 = \{s\}$, $P_1 = \{a_{i1} : i = 1, \cdots, m\}$, $P_2 = \{a_{01}, a_{i2} : i = 1, \cdots, m\}, \cdots, P_n = \{a_{0(n-1)}, a_{in} : i = 1, \cdots, m\}$ and $P_{n+1} = \{a_{0n}, a_{i(n+1)} : i = 1, \cdots, m\}$, then, 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_{n+1} go back to P_0. Thus, any path in the graphs G_0 and G_1 either gets to the node a_{0n} from which there is no outgoing edge, or it visits node s after $\ell(\alpha)$ steps, where $0 \leq \ell(\alpha) \leq n+1$. In matrix terms this implies the following. If A is a product of h factors in $\{A_0, A_1\}$ where h is a nonnegative integer equal to $\ell(\alpha)$ modulo $n+2$, then

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

for some nonnegative scalar μ.

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

$$A_* A_{q_n} \cdots A_{q_1} A_* x(s) = A_* A_{q_n} \cdots A_{q_1} \sum_{i=1}^{m} x(a_{i1}) = A_* \sum_{i=1}^{m} A_{q_n} \cdots A_{q_1} x(a_{i1}) = \lambda x(s). \tag{2}$$

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

With these two observations we now the claim. Assume that the instance of SAT is satisfied by the assignment $x_i = q_i$ for $q_1, \cdots, q_n \in \{0, 1\}$ 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 $\mathbf{R}^r$ 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 length-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

$$A_{q0} \cdots A_{q_{n+1}} x(s) \geq x(s). \tag{3}$$

Let A be an arbitrary product of k matrices. A^{n+2} is a product of $(n+2)k$ matrices and Eq. (3) gives $A^{n+2}x(s) \geq x(s)$, 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 0-1 entries). 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. If we constrain the entries of the matrices in MORTALITY OF A PAIR OF 33×33 MATRICES to have nonnegative entries, then the problem becomes decidable.

   MORTALITY OF A PAIR OF MATRICES WITH NONNEGATIVE ENTRIES

   Instance: $A_0, A_1 \in \mathbf{N}^{n \times n}$.

   Problem: Does there exist a finite product of A_0 and A_1 that is equal to the zero matrix?

   We claim that MORTALITY OF A PAIR OF MATRICES WITH NONNEGATIVE ENTRIES is decidable, and is in fact 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.

References

[1] Garey M. R. and Johnson D. S., Computers and Intractability: A Guide to the Theory of NP-completeness, Freeman and Co., New York, 1979.

[2] Krom M. and M. Krom, Recursive solvability of problems with matrices, Zeitschr. f. math. Logik und Grundlagen d. Math., 35, pp. 437-442, 1989.

[3] Pansiot J. J., A note on Post's correspondence problem, Information Processing Letters, 12, pp. 233, 1981.

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

[5] Paterson M. S., Unsolvability in 3 × 3 matrices, Studies in Appl. Math., 49, pp. 105-107, 1970.

[6] Toker O., On the algorithmic unsolvability of some stability problems for discrete systems, preprint, 1995.

[7] Tsitsiklis J. N. and V. D. Blondel, It is hard to approximate the spectral radius of a pair of matrices, preprint, 1995.