

The Mortality Problem for Matrices of Low Dimensions

O. Bournez¹ and M. Branicky²

¹LORIA, INRIA Lorraine, Campus Scientifique BP 239,
54506 Vandoeuvre les Nancy, France
bournez@loria.fr

²Electrical Engineering and Computer Science Department,
Case Western Reserve University,
Cleveland, OH 44106-7221, USA
branicky@alum.mit.edu

Abstract. In this paper we discuss the existence of an algorithm to decide if a given set of 2×2 matrices is mortal. A set $F = \{A_1, \dots, A_m\}$ of square matrices is said to be *mortal* if there exist an integer $k \geq 1$ and some integers $i_1, i_2, \dots, i_k \in \{1, \dots, m\}$ with $A_{i_1} A_{i_2} \cdots A_{i_k} = 0$. We survey this problem and propose some new extensions. We prove the problem to be BSS-undecidable for real matrices and Turing-decidable for two rational matrices. We relate the problem for rational matrices to the entry-equivalence problem, to the zero-in-the-corner problem, and to the reachability problem for piecewise-affine functions. Finally, we state some NP-completeness results.

1. Introduction

Several undecidability results are known about problems involving matrices [6], [14]. For example, given a finite set F of matrices with integer entries, it is undecidable whether the semi-group generated by M contains a matrix having a zero in the right upper corner [17], is free [11], [8], or contains the zero matrix [20]. These problems have been proved to be undecidable when restricted to 3×3 matrices. However, for both of them, the question of their decidability or undecidability when restricted to 2×2 matrices remains open [6].

In this paper we focus on the decidability of the latter problem. A set $F = \{A_1, \dots, A_m\}$ of $d \times d$ matrices is said to be *mortal* if there exist an integer $k \geq 1$ and some integers $i_1, i_2, \dots, i_k \in \{1, \dots, m\}$ with $A_{i_1} A_{i_2} \cdots A_{i_k} = 0$. Therefore, we focus on the following decision problem denoted by $\text{MORT}_{\mathbb{Q}}(2)$.

Open Problem 1.

- Instance: a finite set F of 2×2 matrices with rational entries.
- Question: is F mortal?

The decidability of problem $\text{MORT}_{\mathbb{Q}}(2)$ remains unknown despite much interest (see [15] and [16] for some references and discussions).

The question of the decidability of $\text{MORT}_{\mathbb{Q}}(2)$ was first mentioned as an open problem in [22] and was formulated as follows: “Find an algorithm, which given a finite set H of non-singular linear transformations of the complex plane and lines L and M through the origin, determines whether some product from H maps L onto M .”

There are at least two motivations to study the mortality problem. First, deciding whether a given set of 2×2 matrices is mortal is equivalent to deciding whether a switched linear system is controllable. In particular, given a system of the form $x(t+1) = A(t, u)x(t)$, where for all t the set of possible values of $A(t, u)$ is a finite set F of $d \times d$ matrices, the question of mortality of F corresponds to the controllability (to the origin) of such a system (see [3]).

Second, proving that $\text{MORT}_{\mathbb{Q}}(2)$ is decidable or undecidable would really clarify computational-complexity issues for discrete-time and hybrid dynamical systems (see [12] and [9]). For example, the reachability problem for piecewise-affine dynamical systems has been proven undecidable for two-dimensional systems, but is open and related to the mortality problem (see Section 4.3) for one-dimensional systems [12].

Observe that if $\text{MORT}_{\mathbb{Q}}(2)$ turned out to be undecidable, it would surely give a way, which would extend the results of [1], [12], [19], and [24], to simulate a Turing machine by a dynamical system of low dimension. Indeed, most of the undecidability results known up to this date rely on simulations of Turing machines.

This paper aims at giving a global picture of the mortality problem. To do so, we also talk about the generalization of the problem to matrices with real entries. When $K \in \{\mathbb{R}, \mathbb{Q}\}$, the problem $\text{MORT}_K(d)$ (resp. $\text{MORT}_K(d, m)$) denotes the following decision problem:

- Instance: a finite set F of $d \times d$ matrices with entries in K (resp. a set F of m $d \times d$ matrices with entries in K).
- Question: is F mortal?

The main contributions of the paper are:

- An undecidability result, already in the case of only two 2×2 matrices, for $K = \mathbb{R}$ in the Blum–Shub–Smale model (BSS-model) of computation [5].
- A decidability result for two 2×2 matrices, in the case $K = \mathbb{Q}$ for the Turing model of computation.
For arbitrary $|F| = m$, the question remains open.
- Reducibility relations between the mortality problem and other problems in the literature.

2. Links between Dimension and Number of Matrices

Paterson proved in [20] that the mortality problem restricted to 3×3 matrices is not decidable.

Theorem 1 [20]. $\text{MORT}_{\mathbb{Q}}(3)$ is recursively unsolvable.

More precisely, Paterson proved in [20] that if the Post Correspondence Problem (PCP) is undecidable with p rules, then $\text{MORT}_{\mathbb{Q}}(3, 2p + 2)$ is undecidable. Using the Modified Post Correspondence Problem (MPCP) instead of PCP, we improve this result.

Proposition 1. Suppose that PCP is undecidable with p rules. Then decision problem $\text{MORT}_{\mathbb{Q}}(3, p + 2)$ is undecidable.

Proof. PCP is the decision problem “given a finite set of pairs of words $\{\langle U_i, V_i \rangle \mid i = 1, \dots, p\}$, determine if there exists a sequence of indexes i_1, i_2, \dots, i_k in $\{1, 2, \dots, p\}$ with $U_{i_1}U_{i_2} \cdots U_{i_k} = V_{i_1}V_{i_2} \cdots V_{i_k}$ ”.

The arguments of Paterson in [20] prove that, to any instance $\{\langle U_i, V_i \rangle \mid i = 1, \dots, p\}$ of PCP, can be associated a finite set

$$F = \{S, T, W(U_j, V_j), W'(U_j, V_j) \mid j = 1, \dots, p\}$$

of integer matrices, which satisfy

1. F is mortal if and only if there exists some integers i_1, i_2, \dots, i_k with $SW'(U_{i_1}, V_{i_1})W(U_{i_2}, V_{i_2}) \cdots W(U_{i_k}, V_{i_k})T = 0$;
2. this latter case holds if and only if $U_{i_1}U_{i_2} \cdots U_{i_k} = V_{i_1}V_{i_2} \cdots V_{i_k}$.

We replace PCP by MPCP [10] to obtain our result. The difference between PCP and MPCP is that in the latter the first index i_1 must be equal to 1. Namely, MPCP is the decision problem “given a finite set of pairs of words $\{\langle U_i, V_i \rangle \mid i = 1, \dots, p\}$, determine if there exists a sequence of indexes i_2, \dots, i_k in $\{1, 2, \dots, p\}$ with $U_1U_{i_2} \cdots U_{i_k} = V_1V_{i_2} \cdots V_{i_k}$ ”.

Since any instance of PCP can be solved by p calls to MPCP, the undecidability of PCP with p rules implies the undecidability of MPCP with p rules.

It only remains to prove that MPCP with p rules reduces to $\text{MORT}_{\mathbb{Q}}(3, p + 2)$. Since in MPCP the first index i_1 is 1, the set of matrices

$$F = \{T, SW'_{U_1, V_1}, W_{U_j, V_j} \mid j = 1, \dots, p\}$$

is mortal if and only if there exist some integers i_2, \dots, i_k with

$$SW'(U_1, V_1)W(U_{i_2}, V_{i_2}) \cdots W(U_{i_k}, V_{i_k})T = 0.$$

By condition 2 above, this holds if and only if $\{\langle U_i, V_i \rangle \mid i = 1, \dots, p\}$ is a positive instance of MPCP. \square

The following result is proved in [2] and [6].

Lemma 1 [2], [6]. *For all $n \geq 2$, $m \geq 1$, $\text{MORT}_{\mathbb{Q}}(d, m)$ undecidable implies $\text{MORT}_{\mathbb{Q}}(dm, 2)$ undecidable.*

The minimal number p of rules for which PCP is undecidable is not known, but p is an integer between 3 and 7 (see [18]).

Hence, from Proposition 1, the following can be stated.

Corollary 1.

- *Decision problem $\text{MORT}_{\mathbb{Q}}(3, 9)$ is undecidable.*
- *Decision problem $\text{MORT}_{\mathbb{Q}}(27, 2)$ is undecidable.*

3. On the Decidability of $\text{MORT}(2, 2)$

We now come back to the decidability of the mortality problem for two-dimensional matrices. We prove first that $\text{MORT}_{\mathbb{R}}(2, 2)$ is BSS-undecidable. Then we prove that $\text{MORT}_{\mathbb{Q}}(2, 2)$ is Turing-decidable.

We make use of the following lemma several times.

Lemma 2. *A finite set $F = \{A_1, \dots, A_m\}$ of 2×2 matrices is mortal if and only if there exist an integer k and integers $i_1, \dots, i_k \in \{1, \dots, m\}$ with $A_{i_1} \cdots A_{i_k} = 0$, and*

1. $\text{rank}(A_{i_j}) = 2$ for $1 < j < k$,
2. $\text{rank}(A_{i_j}) < 2$ for $j \in \{1, k\}$.

Proof. Only the direct sense requires a proof. Assume that F is mortal. Then there exists a null product $A_{i_1} \cdots A_{i_k} = 0$ where k is minimal. Assume $k \geq 2$, because otherwise the assertion is immediate. The matrices A_{i_1} and A_{i_k} of this product are singular because otherwise a null-product with fewer matrices could be obtained by multiplying $A_{i_1} \cdots A_{i_k}$ by their inverse(s).

Let $j \geq 2$ be the smallest integer with $\text{rank}(A_{i_j}) < 2$. Since we have $A_{i_1} \cdots A_{i_k} = 0$, matrix $A_{i_1} \cdots A_{i_{j-1}}$ sends the image I of matrix $A_{i_j} \cdots A_{i_k}$ to 0. Now, I is also equal to the image of A_{i_j} and is of dimension 1. Indeed, first, I is clearly included in the image of A_{i_j} . Second, by definition of k , I cannot be of dimension 0, and, third, the dimension of the image of A_{i_j} is at most 1 because $\text{rank}(A_{i_j}) < 2$. We obtain $A_{i_1} \cdots A_{i_{j-1}} A_{i_j} = 0$. This implies $j = k$, and the direct sense of the lemma. \square

3.1. BSS-Undecidability of $\text{MORT}_{\mathbb{R}}(2, 2)$

Talking about the decidability or undecidability of $\text{MORT}_{\mathbb{R}}(2)$ requires one to talk about machines that manipulate real numbers.

One approach is to use the machine model studied in recursive analysis (e.g., see [26]). However, this model does not meet our needs because one cannot decide whether a real number is equal to zero in this model [26].

Another approach is to use the Turing machine model for real numbers proposed by Blum et al. in [4] and [5]. Roughly speaking, a BSS-machine¹ is an extended Random Access Machine [10] that treats real numbers as basic entities; namely a BSS-machine contains an unbounded number of real registers x_1, \dots, x_n, \dots , each of which can hold one real number in unbounded precision. Moreover, a BSS-machine contains a finite number of built-in constants $\lambda_1, \dots, \lambda_m$. Its program is made of arithmetic operations between its real registers of type $x_i := x_j \# x_k$, for $\# \in \{+, -, *, /\}$, or of type $x_i := \lambda_j$, or of tests of type $x_i \# x_j$ with $\# \in \{>, \geq, <, \leq, =, \neq\}$. Let $\mathbb{R}^\infty = \bigcup_{i \in \mathbb{N}} \mathbb{R}^i$. An input $x \in \mathbb{R}^\infty$ is of type $x = (x_1, \dots, x_i)$ for some i . The input is said to be *accepted* by the machine if the program of the machine eventually halts when started with its real registers set to $(x_1, \dots, x_i, 0, \dots, 0, \dots)$. A language $L \subset \mathbb{R}^\infty$ is said to be *BSS-recursively enumerable* if it consists of the accepted inputs of some BSS-machine. The language L is said to be *BSS-recursive* if, in addition, its complement is BSS-recursively enumerable.

In other words, BSS-recursive sets are those that can be decided using only arithmetical operations and tests. The reader should refer to [4] and [5] for more formal descriptions. We assume that the reader is familiar with the BSS-model in the rest of this paper.

We first recall a lemma proved in [5]. A set $S \subset \mathbb{R}^n$ is said to be a *basic semi-algebraic set* if $S = \{(x_1, \dots, x_n) \mid p_1(x_1, \dots, x_n) > 0 \wedge \dots \wedge p_{n_1}(x_1, \dots, x_n) > 0 \wedge p'_{n_2}(x_1, \dots, x_n) = 0 \wedge \dots \wedge p'_{n_2}(x_1, \dots, x_n) = 0\}$ for some n -variable polynomials $p_1, p_2, \dots, p_{n_1}, p'_{n_2}, \dots, p'_{n_2}$. A *semi-algebraic set* is a finite union of basic semi-algebraic sets.

Lemma 3. *Let $L \subset \mathbb{R}^\infty$ be a BSS-recursively enumerable set. Then L is a denumerable union of semi-algebraic sets.*

Sketch of Proof. Write $L = \bigcup_{t \in \mathbb{N}} \text{ACC}_t$, where ACC_t is the subset of the inputs that are accepted by the machine at time t . Each subset ACC_t is a semi-algebraic set. See [5] for the formal details. \square

The remaining arguments of this subsection are inspired from [13]. (In fact, there seems to be a close relation between mortality and stability. See [13].)

We start with the following preliminary result.

Lemma 4. *Let $a, b, \lambda \in \mathbb{R}$ be some real numbers with $a^2 + b^2 \neq 0$ and $\lambda \neq 0$. Let θ be an argument of complex number $a + ib$. The pair of matrices $F(a, b, \lambda) = \{A_1, A_2\}$ with*

$$A_1 = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}, \quad A_2 = \begin{pmatrix} -\lambda & 1 \\ 0 & 0 \end{pmatrix}$$

is mortal if and only if there exists an integer $n \in \mathbb{N}$ with $\lambda = \tan(n\theta)$.

¹ The BSS-model is not a realizable computation concept but is of mathematical interest for studying computations on the reals.

Proof. From Lemma 2 we know that $F(a, b, \lambda)$ is mortal if and only if there exists an integer $n \in \mathbb{N}$ with $A_2 A_1^n A_2 = 0$. This holds if and only if there exists an n th power of A_1 which sends the image of A_2 to its kernel. Since $\text{Im}(A_2) = \langle (1, 0) \rangle$, $\text{Ker}(A_2) = \langle (1, \lambda) \rangle$, and since A_1 is the composition of a homothety and a rotation of angle θ , this is true if and only if there exists an integer $n \in \mathbb{N}$ with $\lambda = \tan(n\theta)$. \square

The following observations are easy.

Lemma 5. *Let θ be a real number. Let $E(\theta)$ be the subset of \mathbb{R} defined by*

$$E(\theta) = \{\lambda \mid \text{there exists an integer } n \in \mathbb{N} \text{ with } \lambda = \tan(n\theta)\}.$$

1. $E(\theta)$ is a dense subset of \mathbb{R} if and only if $\theta/\pi \notin \mathbb{Q}$.
2. There exist two rational numbers $a, b \in \mathbb{Q}$ such that any argument θ of complex number $a + ib$ satisfies $\theta/\pi \notin \mathbb{Q}$. Indeed, take for example $a = 1$ and $b = 2$ (see Lemma 6).
3. When $\theta/\pi \notin \mathbb{Q}$, the complement $E^c(\theta)$ of $E(\theta)$ in \mathbb{R} has an uncountable number of connected components; actually, every point of $E^c(\theta)$ is its own connected component.

We can now prove that $\text{MORT}_{\mathbb{R}}(2, 2)$ is BSS-undecidable. Observe that the arguments are close to the ones in [13]. We, however, deal with a different problem and with a modified family of matrices.

Theorem 2. $\text{MORT}_{\mathbb{R}}(2, 2)$ is BSS-recursively enumerable but is not BSS-recursive.

Proof. Building a BSS-machine that semi-recognizes $\text{MORT}_{\mathbb{R}}(2, 2)$ is easy. Therefore the problem is BSS-recursively enumerable.

Representing the matrices by their coefficients, the space of the instances of problem $\text{MORT}_{\mathbb{R}}(2, 2)$ is \mathbb{R}^8 . Denote by $\text{POS} \subset \mathbb{R}^8$ (resp. by $\text{NEG} \subset \mathbb{R}^8$) the subset of the positive (resp. negative) instances of the problem. Using Lemma 3, we only need to prove that NEG is not a countable union of semi-algebraic sets.

Let $a, b \in \mathbb{Q}$ with $a + ib = \rho e^{i\theta}$, $\theta/\pi \notin \mathbb{Q}$ as in Lemma 5. Let $\gamma: \mathbb{R} \rightarrow \mathbb{R}^8$ be the function that sends $\lambda \in \mathbb{R}$ to the pair of matrices $F(a, b, \lambda)$. By definition of γ , the image $\text{Im } \gamma$ of γ is an algebraic subset of \mathbb{R}^8 and γ realizes a homeomorphism between \mathbb{R} and $\text{Im } \gamma$. By Lemma 4, we know that $\gamma^{-1}(\text{POS}) = E(\theta)$ and $\gamma^{-1}(\text{NEG}) = E^c(\theta)$. Since γ is a homeomorphism, $E^c(\theta)$ and $\gamma(E^c(\theta)) = \text{NEG} \cap \text{Im } \gamma$ must have the same number of connected components. That is, by part 3 of Lemma 5, they must have an uncountable number of connected components.

Assume, by contradiction, that we can write $\text{NEG} = \bigcup_{i \in \mathbb{N}} S_i$ where each S_i is a semi-algebraic subset. We would have $\text{NEG} \cap \text{Im } \gamma = \bigcup_{i \in \mathbb{N}} (\text{Im } \gamma \cap S_i)$. Each of the $(\text{Im } \gamma \cap S_i)$ must be a semi-algebraic subset as the result of the intersection between an algebraic set and a semi-algebraic set. Since a semi-algebraic set has a finite number of connected components, $\text{NEG} \cap \text{Im } \gamma$ must have a countable number of connected components. This leads to a contradiction. \square

We obtain the following immediately.

Corollary 2.

- For $n \geq 2, m \geq 2$, the problem $\text{MORT}_{\mathbb{R}}(n, m)$ is BSS-recursively enumerable but not BSS-recursive.
- $\text{MORT}_{\mathbb{R}}(2)$ is BSS-recursively enumerable but not BSS-recursive.

However, observe that it is easy to extract the following fact from the proofs of the next section.

Theorem 3. *Problem $\text{MORT}_{\mathbb{R}}(2, 2)$ restricted to matrices with real eigenvalues is BSS-recursive.*

We discuss the results of Theorem 2 and Corollary 2. Deciding whether a set of matrices is mortal using *only arithmetical operations* is not possible. However, it does not mean that the problem cannot be decided by an algorithm which uses non-arithmetical operations or which uses arguments about the semi-ring K of the entries for $K \neq \mathbb{R}$.

Actually, using number-theoretical arguments, we prove in the next subsection that the decision problem $\text{MORT}_{\mathbb{Q}}(2, 2)$ is Turing-decidable.

3.2. *Turing-Decidability of $\text{MORT}_{\mathbb{Q}}(2, 2)$*

The decidability of $\text{MORT}_{\mathbb{Q}}(2, 2)$ has already been claimed [6], [21]. However, the proofs were either wrong or incomplete. More precisely, in [6] the result is claimed without proof. In [21] the result is claimed but the proof is wrong. Indeed, the proof of [21] presents an algorithm to decide $\text{MORT}_{\mathbb{Q}}(2, 2)$ which uses only arithmetical operations, and this precisely contradicts² Theorem 2. We present a full proof herein.

From the previous section we know that to prove the decidability of $\text{MORT}_{\mathbb{Q}}(2, 2)$, we need the use of number-theoretical arguments. The arguments³ we use are based on the following result extracted from [23].

Lemma 6 [23].

- *The following decision problem is decidable.*
 - *Instance: rational numbers $p, q \in [-1, 1]$.*
 - *Question: does there exist $\theta \in \mathbb{R}$ and an integer $n \in \mathbb{N}$ with $\cos(\theta) = p$ and $\cos(n\theta) = q$?*
- *When $p \notin \{0, \frac{1}{2}, 1\}$ there are at most a finite number of such n and those n can be computed effectively.*

² Concretely, the cases studied in the proof [21] do not cover all the cases. In particular, the proof forgets the case of rational matrices with complex eigenvalues.

³ Not present in [21]. Of course, those arguments could always be patched to the (missing) cases of the proof of [21], but we prefer presenting a complete, independent, and correction/patch-free proof.

Proof. For completeness we provide the proof, which is almost cut-and-paste from [23].

Write $p = r/s, q = u/v$ where r, s, u, v are integers such that $\gcd(r, s) = \gcd(u, v) = 1$. The decidability of the problem when $p = 0, p = \frac{1}{2}$, or $p = 1$ is trivial, since in that case the sequence $n \rightarrow \cos(n\theta)$ assumes only a computable finite number of values that can be tested against q . Suppose $p \notin \{0, \frac{1}{2}, 1\}$. The function $\cos(n\theta)$ is a polynomial in $\cos(\theta)$ with integer coefficients. If this polynomial is written $\cos(n\theta) = p_n(r/s)$, then $s^n p_n(r/s)$ is some integer c_n which satisfies

$$2rc_{n+1} - s^2c_n = c_{n+2}, \quad (1)$$

with $c_1 = r$ and $c_2 = 2r^2 - s^2$; indeed, if we denote $a_n = \sin(nx)$ and $b_n = \cos(nx)$, this recurrence comes from $a_{n+1} = a_1b_n + b_1a_n, b_{n+1} = b_1b_n - a_1a_n, \dots$

Suppose that s is not a power of 2. Write $s = 2^a b, v = 2^{a'} b'$ with $b > 1, b' \geq 1$ odd. We are searching for an integer n such that $c_n/(2^{an}b^n) = u/(2^{a'}b')$. We claim $\gcd(c_n, b^n) = 1$ for all $n \in \mathbb{N}$. Indeed, if some odd integer d divides s and c_n simultaneously, then, since $\gcd(r, s) = 1$, the assertions $d|c_{n-1}, d|c_{n-2}, \dots, d|c_2$ imply $d|r^2$, which implies $d = 1$. As a consequence, an integer candidate n must satisfy $b' = b^n$. There are at most a finite number of such n and those n are computable.

Suppose now that s is a power of 2. Write $s = 2^k, k > 1$ (remember that we supposed $r/s \neq \frac{1}{2}$). Write every c_n as $c_n = 2^{\lambda_n} v_n$ where v_n is an odd integer. Recurrence (1) becomes

$$2^{\lambda_{n+1}+1} r v_{n+1} - 2^{\lambda_n+2k} v_n = 2^{\lambda_{n+2}} v_{n+2}. \quad (2)$$

We prove first that there exists an integer n with $\lambda_n + 1 < 2k + \lambda_{n-1}$. Indeed, if it were false, we would always have $\lambda_n + 1 \geq 2k + \lambda_{n-1}$, so that $\lambda_n + 1 \geq 2(n-1)k + \lambda_1$ would hold for all n . Since $|\cos(n\theta)| < 1$, we have $kn \geq \lambda_n$ which implies $kn \geq 2(n-1)k + \lambda_1 - 1$ for all $n \in \mathbb{N}$. Clearly this is impossible.

Let n_0 be the smallest integer such that $\lambda_{n_0+1} + 1 < 2k + \lambda_{n_0}$. Integer n_0 can be computed effectively by testing this condition for increasing n . We have $\lambda_{n_0+2} = \lambda_{n_0+1} + 1$. Indeed, from (1) we must have $rv_{n_0+1} - 2^{\lambda_{n_0}+2k-\lambda_{n_0+1}-1} v_{n_0} = 2^{\lambda_{n_0+2}-\lambda_{n_0+1}-1} v_{n_0+2}$. Considering parity of both sides, this can happen only if $\lambda_{n_0+2} = \lambda_{n_0+1} + 1$.

Since that implies $\lambda_{n_0+2} + 1 = \lambda_{n_0+1} + 2 < \lambda_{n_0+1} + 2k$, we can repeat the argument, and get by induction that for all integers $h \geq 0, \lambda_{n_0+2+h} = \lambda_{n_0+1+h} + 1$ holds. Hence, for each positive integer h , we must have $\lambda_{n_0+h} = \lambda_{n_0} + h$.

Now, return to the existence of an integer n with $\cos(n\theta) = u/v$. For $\cos(\theta)$ having denominator $2^k, v$ must be a power of 2. Suppose $v = 2^m$. It may happen that there exists a solution for $n \leq n_0$. For $n > n_0$, a solution $n = n_0 + h$ must satisfy $\cos((n_0 + h)\theta) = v_{n_0+h} 2^{\lambda_{n_0}+h} / 2^{k(n_0+h)} = u/2^m$, hence $k(n_0+h) - \lambda_{n_0} - h = m$, or $h = (m + \lambda_{n_0} - kn_0)/(k-1)$. That is, the only integer n candidate exceeding n_0 is $n_0 + (m + \lambda_{n_0} - kn_0)/(k-1)$. Hence, there are at most $n_0 + 2$ integer candidates n that could satisfy $\cos(n\theta) = u/v$, and those candidates are computable. \square

With this we now obtain the following.

Theorem 4. $\text{MORT}_{\mathbb{Q}}(2, 2)$ is decidable.

Proof. Let $F = \{A_1, A_2\}$ be an instance of the problem. Suppose without loss of generality that the rank of A_2 is greater than the rank of A_1 . If A_1 is of rank 2, then the two matrices are non-singular and F is non-mortal by Lemma 2. If A_1 is of rank 0, then F is mortal. If the two matrices have rank 1, by Lemma 2, it suffices to test whether one of the products $A_1^2, A_1A_2, A_2A_1, A_2^2$ is null.

There remains only the case where A_2 is non-singular and A_1 is of rank 1. By Lemma 2, F is mortal if and only if there exists an integer $n \in \mathbb{N}$ with

$$A_1A_2^nA_1 = 0. \quad (3)$$

We want to check this relation algebraically using the Jordan forms of the matrices A_1 and A_2 . Write

$$A_1 = P_1^{-1}J_1P_1, \quad A_2 = P_2^{-1}J_2P_2,$$

$$J_1 = \begin{pmatrix} \kappa & 0 \\ 0 & 0 \end{pmatrix},$$

and

$$J_2 = \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$$

with P_1 and P_2 non-singular. Eigenvalue κ is equal to the trace of rational matrix A_1 , and, hence, is a rational number. Eigenvalues λ and μ are the (possibly complex) roots of the characteristic polynomial of rational matrix A_2 .

Equation (3) becomes

$$P_1^{-1}J_1P_1P_2^{-1}J_2^nP_2P_1^{-1}J_1P_1 = 0$$

or, since P_1 is non-singular,

$$J_1PJ_2^nP^{-1}J_1 = 0,$$

where

$$P = P_1P_2^{-1} = \begin{pmatrix} p & q \\ r & s \end{pmatrix}.$$

Now, after substituting P, P^{-1} , and J , the problem is equivalent to testing whether there exists an integer $n \in \mathbb{N}$ with

- $ps\lambda^n - qr\mu^n = 0$, when J_2 is of the first form; or
- $(ps - qr)\lambda^n - rpn = 0$, when J_2 is of the second form.

Suppose that J_2 is of the second form. Eigenvalue λ is rational because λ is equal to the trace of rational matrix A_2 divided by 2. Coefficients κ , p , q , r , and s are computable rational numbers which can easily be expressed in terms of the coefficients of the matrices A_1 and A_2 from previous considerations. Testing whether there exists an integer n with $(ps - qr)\lambda^n - rpn = 0$ is easy in that case. Indeed, the equation $(ps - qr)\lambda^x - rpx = 0$ over real variable x clearly has a unique real solution x^* in that case; any numerical method⁴ can return an approximation to precision $\frac{1}{2}$ of x^* , namely a rational number x_{app} with $|x_{\text{app}} - x^*| < \frac{1}{2}$; testing whether $(ps - qr)\lambda^n - rpn = 0$ has a solution is then equivalent to testing this equation with $n = \lfloor x_{\text{app}} \rfloor$.

Suppose that J_2 is of the first form. We want to test the existence of an integer n with $ps\lambda^n - qr\mu^n = 0$. Observe that $\lambda \neq 0$, $\mu \neq 0$ since A_2 is of rank 2. λ , μ , and the coefficients p , q , r , s can be complex numbers but are computable elements of $\mathbb{Q}(\lambda)$. That is, they are of the form $a + \lambda b$ for some rational numbers $a, b \in \mathbb{Q}$ computable from the rational coefficients of the matrices A_1 and A_2 . By computing in $\mathbb{Q}(\lambda)$, the cases $ps = 0$ or $qr = 0$ are trivial. Suppose now $ps \neq 0$ and $qr \neq 0$. The problem is equivalent to testing whether there exists an integer n with $(\lambda/\mu)^n = (pq)/(rs)$. We must have $|\lambda/\mu|^n = |pq|/|rs|$. When $|\lambda/\mu| \neq 1$, n must be equal to $|pq|/(|rs| \log |\lambda/\mu|)$; we only need to use any numerical algorithm for approximating this real quantity x^* by some rational number x_{app} with $|x_{\text{app}} - x^*| < \frac{1}{2}$, and test the equation for integer $n = \lfloor x_{\text{app}} \rfloor$. When $|\lambda/\mu| = 1$ and λ and μ are real numbers, we have necessarily that $\lambda = \mu$ or $\lambda = -\mu$. In both cases, by computing in $\mathbb{Q}(\lambda)$ the problem is trivial. When $|\lambda/\mu| = 1$ and $|pq|/|rs| \neq 1$ the problem has no solution.

There remains only the case where λ and μ are two conjugated complex roots and $(pq)/(rs)$ is a complex number of modulus 1. In that case λ is a complex number with rational real part because λ is a root of the characteristic polynomial of matrix A_2 with rational coefficients. Therefore, complex numbers λ/μ and $(pq)/(rs)$ of type $a + \lambda b$ with computable $a, b \in \mathbb{Q}$ must also have rational computable real parts. If θ denotes an argument of complex number λ/μ of modulus 1, an integer n solution must satisfy $\cos(n\theta) = r'$ where r' is the real part of $(pq)/(rs)$. When the real part p' of λ/μ is equal to $\frac{1}{2}$, $n \mapsto (\lambda/\mu)^n$ is a periodic sequence of period 6, and it suffices to check $(\lambda/\mu)^n = (pq)/(rs)$ for $n = 0, 1, \dots, 5$. Cases $p' = 0$ and $p' = 1$ can be dealt with similarly. Now, when $p' \notin \{0, \frac{1}{2}\}$, by Lemma 6, there are at most a finite number of integers n satisfying $\cos(n\theta) = r'$ and those integers are computable. It suffices to check if equation $(\lambda/\mu)^n = (pq)/(rs)$ holds for those integers. \square

We have just proved that $\text{MORT}_{\mathbb{Q}}(2, 2)$ is Turing-decidable. We do not know whether $\text{MORT}_{\mathbb{Q}}(2, 3)$ is decidable. So our knowledge of the decidability of $\text{MORT}_{\mathbb{Q}}(2)$ stops at the previous theorem. However, our proof of the BSS-undecidability of the problem shows that the problem is more a number-theoretic problem than a simple computability problem.

In the next section we show that $\text{MORT}_{\mathbb{Q}}(2)$ can be related to other open problems in the literature.

As pointed out by an anonymous referee, the previous theorem can also be proved in

⁴ For example, Newton's method.

a much more compact (but not self-contained) way using the results of [25]. Let A_0, A_1 be two 2×2 matrices with rational entries. To the word $w = w_1 w_2 \cdots w_n \in \{0, 1\}^*$ we associate the matrix $A_w = A_{w_1} A_{w_2} \cdots A_{w_n}$. The language $Z(A_0, A_1)$ is the set of words w for which $A_w = 0$. Theorem 4 says that given two 2×2 matrices A_0, A_1 with rational entries, one can effectively test if $Z(A_0, A_1)$ is empty. This could also be seen as a consequence of the following stronger claim: given two 2×2 matrices A_0, A_1 with rational entries, one can effectively compute the language $Z(A_0, A_1)$.

Indeed, if both matrices are of rank 2, then $Z(A_0, A_1)$ is empty. If $\text{rank}(A_0) = 0$ the problem is trivial, so assume $\text{rank}(A_0) = 1$. Then $A_0 = bc^T$ where b and c are non-zero column vectors with rational entries. By Lemma 2, if there exists a mortal product, then $A_0 A_1^k A_0 = 0$ for some integer k . This condition is equivalent to $c^T A_1^k b = 0$. Let $\gamma_k = c^T A_1^k b$; the sequence γ_k is a linear recursive sequence of order 2. Vereshchagin [25] proves that there exists an algorithm for finding a semi-linear definition of the set of zeros of any linear recursive sequence of order ≤ 3 from a definition of the sequence. That implies that the set of indices k for which $\gamma_k = 0$ can be computed effectively. The language Z is equal to the set of words uvw where u and w are arbitrary words, and v is a word of the form $01111 \cdots 11110$ where the number of 1's is any k for which $\gamma_k = 0$.

4. Relations to Other Problems in the Literature

In this section we prove that $\text{MORT}_{\mathbb{Q}}(2)$ is equivalent to the entry-equivalence problem studied in [15], to the zero-in-the-corner problem studied in [17] and [6], and can be linked to the problems studied in [12].

When C is a matrix, $C_{i,j}$ denotes the entry in its i th row and j th column.

4.1. The Entry-Equivalence Problem

Here is a variation of Theorem 2 of [15] (unlike Theorem 2 of [15], we do not suppose F to be composed of only non-singular matrices).

Lemma 7. *Let F be a finite set of 2×2 matrices. There exists an integer k and some integers i_1, \dots, i_k such that $A_{i_1} \cdots A_{i_k}$ is a matrix C satisfying $C_{2,1} = C_{2,2}$ if and only if the finite set F' composed of the matrices of F and of the matrix*

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

is mortal.

Proof. First observe that $HCH = 0$ holds if and only if $C_{2,1} = C_{2,2}$. That proves the direct sense.

Conversely, by Lemma 2, if F is mortal there exist i_1, \dots, i_k with $A_{i_1} \cdots A_{i_k} = 0$, $A_{i_j} \neq H$ for $1 < j < k$, and $\text{rank}(A_{i_j}) < 2$ for $j \in \{1, k\}$. If $A_{i_1} = A_{i_k} = H$ the remark of the previous paragraph implies that $C = A_{i_2} \cdots A_{i_{k-1}}$ satisfies $C_{2,1} = C_{2,2}$.

If $A_{i_1} \neq H$ and $A_{i_k} \neq H$, then $A_{i_1} \cdots A_{i_k}$ is a product of matrices from F equal to the null-matrix, and the null-matrix O satisfies $O_{2,1} = O_{2,2}$. Now, for the remaining cases, observe that equation $HC = 0$ (resp. $CH = 0$) implies $C_{2,1} = C_{2,2}$. \square

We can now extend a result of [15].

Theorem 5 (Entry-Equivalence). *Let $K \in \{\mathbb{R}, \mathbb{Q}\}$. Problem $\text{MORT}_K(2)$ is equivalent to the following decision problem:*

- *Instance: a finite set $F = \{A_1, \dots, A_m\}$ of 2×2 matrices with entries in K .*
- *Question: does there exist an integer k and some integers i_1, \dots, i_k such that $A_{i_1} \cdots A_{i_k}$ is a matrix C satisfying $C_{2,1} = C_{2,2}$?*

and to the following decision problem:

- *Instance: a finite set $F = \{A_1, \dots, A_m\}$ of non-singular 2×2 matrices with entries in K .*
- *Question: does there exist an integer k and some integers i_1, \dots, i_k such that $A_{i_1} \cdots A_{i_k}$ is a matrix C satisfying $C_{2,1} = C_{2,2}$?*

Proof. Clearly the second problem reduces to the first. The first problem reduces to the mortality problem for 2×2 matrices by Lemma 7 and a reduction from the mortality problem for 2×2 matrices to the second problem is given in [15]. \square

As a corollary to our results, we obtain that the above-mentioned problems are not decidable over \mathbb{R} , and open and equivalent over \mathbb{Q} .

4.2. The Zero-in-the-Corner Problem

It is known that the problem of deciding whether the semi-group generated by a finite set of 3×3 non-singular matrices contains an element with a zero in the right upper corner is undecidable [6], [17]. However, the decidability of the problem for 2×2 matrices is left open [6].

Nevertheless, this problem can be related to the mortality problem by the next theorem.

Theorem 6 (Zero-in-the-Corner). *Let $K \in \{\mathbb{R}, \mathbb{Q}\}$. Problem $\text{MORT}_K(2)$ is equivalent to the following decision problem:*

- *Instance: a finite set $F = \{A_1, \dots, A_m\}$ of 2×2 matrices with entries in K .*
- *Question: does there exist an integer k and some integers i_1, \dots, i_k such that $A_{i_1} \cdots A_{i_k}$ is a matrix C satisfying $C_{1,1} = 0$?*

and to the following decision problem:

- *Instance: a finite set $F = \{A_1, \dots, A_m\}$ of non-singular 2×2 matrices with entries in K .*
- *Question: does there exist an integer k and some integers i_1, \dots, i_k such that $A_{i_1} \cdots A_{i_k}$ is a matrix C satisfying $C_{1,1} = 0$?*

Proof. Denote

$$P = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

Observing that for every matrix C , matrix $C' = PCP^{-1}$ satisfies $C'_{1,1} = 0$ if and only if $C_{2,1} = C_{2,2}$, the above problems are equivalent to the equivalent problems of Theorem 5 by conjugations by matrix P . \square

As a corollary to our results, we obtain that the above-mentioned problems are not decidable over \mathbb{R} , and open and equivalent over \mathbb{Q} .

4.3. Restriction to Lower-Triangular Matrices

It was proposed in [15] to restrict the previous problems to lower-triangular matrices. Indeed, [20] also proves that the entry-equivalence problem is undecidable for lower-triangular 3×3 matrices with rational entries.

Problem $\text{MORT}_{\mathbb{Q}}(2)$ restricted to lower-triangular matrices is trivially decidable [15]. Indeed, a finite set F of lower-triangular matrices is mortal if and only if there exist two matrices A, B in F with $A_{1,1} = 0$ and $B_{2,2} = 0$. The zero-in-the-corner problem also becomes trivial when restricted to lower-triangular matrices.

However, the answer to the following question is not known.

Open Problem 2 (Lower Triangular-Matrices). Is the following decision problem decidable?

- *Instance:* a finite set $F = \{A_1, \dots, A_m\}$ of non-singular lower-triangular 2×2 matrices with rational entries.
- *Question:* does there exist an integer k and some integers i_1, \dots, i_k such that $A_{i_1} \cdots A_{i_k}$ is a matrix C satisfying $C_{2,1} = C_{2,2}$?

We prove that this problem can be related to a non-deterministic version of the open problem mentioned in [12].

Theorem 7. *Open Problem 2 is equivalent to the decidability of the following decision problem:*

- *Instance:* a finite set $F = \{f_1, \dots, f_m\}$ of non-constant rational affine functions of dimension 1 (i.e., a set of functions of type $f_i: x \mapsto a_i x + b_i$, $a_i, b_i \in \mathbb{Q}$, $a_i \neq 0$).
- *Question:* does there exist a composition $f_{i_1} \circ f_{i_2} \circ \dots \circ f_{i_k}$ of these functions that maps point 0 to point 1?

Proof. Call this problem the *composition problem*. Suppose that a finite set $F = \{A_1, \dots, A_m\}$ of non-singular lower-triangular matrices is given. Without loss of generality, we can suppose $A_{2,2} = 1$ for each matrix $A \in F$. Indeed, each matrix $A \in F$ must

satisfy $A_{2,2} \neq 0$ to be non-singular, and replacing each matrix A by matrix $A/A_{2,2}$ in F does not change the mortality of set F .

Open Problem 2 reduces to the instance $F' = \{f_1, \dots, f_m\}$ of the composition problem where $f_i: x \mapsto (A_i)_{1,1}x + (A_i)_{2,1}$. Indeed, any product $C = A_{i_1} \cdots A_{i_k}$ of lower-triangular matrices with $(A_{i_j})_{2,2} = 1$ satisfies $C_{2,2} = 1$ and $C_{2,1} = f_{i_1} \circ f_{i_2} \cdots \circ f_{i_k}(0)$.

Conversely the composition problem reduces to Open Problem 2. When a finite set $F = \{f_1, \dots, f_m\}$ of non-constant affine rational functions is given, $f_i: x \mapsto a_i x + b_i$, it suffices to consider $F' = \{A_1, \dots, A_m\}$ with

$$A_i = \begin{pmatrix} a_i & 0 \\ b_i & 1 \end{pmatrix}$$

and to observe that any product $C = A_{i_1} \cdots A_{i_k}$ of matrices of this form satisfies $C_{2,2} = 1$ and $C_{2,1} = f_{i_1} \circ f_{i_2} \cdots \circ f_{i_k}(0)$. \square

4.4. NP-Completeness Results

4.4.1. K -Length Mortality. A set $F = \{A_1, \dots, A_m\}$ of $d \times d$ matrices is said to be K -length mortal if there exist an integer $k \leq K$ and some integers $i_1, i_2, \dots, i_k \in \{1, \dots, m\}$ with $A_{i_1} A_{i_2} \cdots A_{i_k} = 0$.

Theorem 8. *Given a set F of m 3×3 matrices with rational entries and an integer $K \leq 1 + m/2$, the decision problem “Is F K -length-mortal?” is NP-hard.*

Proof. Via the reduction of [20] (or the proof of Proposition 1) and the NP-completeness of Bounded PCP [7]. \square

Observe that [2] proves that this result remains true whenever the matrices are assumed to have entries in $\{0, 1\}$.

4.4.2. Mortality without Repetition. When repetitions of matrices are not allowed, the problem also becomes clearly decidable. A multi-set $F = \{A_1, \dots, A_m\}$ of $d \times d$ matrices is said to be *mortal without repetition* if there exist integers $k \geq 1$ and some integers $i_1, i_2, \dots, i_k \in \{1, \dots, m\}$ such that $A_{i_1} A_{i_2} \cdots A_{i_k} = 0$ and $i_{j_1} \neq i_{j_2}$ for all $j_1 \neq j_2$.

Theorem 9. *Given a finite multi-set F of m 2×2 matrices, and an integer K , the decision problem “Is F K -length-mortal without repetition?” is NP-hard in the strong sense.*

The proof uses a reduction from subset product [7]. We restate this problem here.

Proposition 2 (Subset Product (Yao)). *Given a finite set A , a size $s(a) \in \mathbb{N}^+$ for each $a \in A$, and a positive integer B , the decision problem “Is there a subset $A' \subset A$ such that the product of the sizes of the elements in A' is exactly B ?” is NP-complete in the strong sense.*

Proof of Theorem 9. Given an instance of subset product with $|A| = n$, define $n + 3$ matrices as follows:

$$\begin{pmatrix} 1 & 0 \\ 0 & s(a) \end{pmatrix} \text{ for } a \in A, \quad \begin{pmatrix} 1 & 0 \\ B & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 0 & -1 \end{pmatrix}.$$

Note that we have repeated the last matrix, since we are required to use it twice. Denote the last matrix by H . Check that for all 2×2 matrices A , $HAH = 0$ if and only if $A_{2,1} = A_{2,2}$. Hence, by Lemma 2, this set of matrices is mortal without repetition with length $4 \leq k \leq n + 3$ steps if and only if the subset product has a solution in $1 \leq k - 3 \leq n$ steps. \square

Acknowledgments

We thank Eduardo Sontag for having pointed out reference [13]. We also thank the anonymous referees for valuable comments and improvements concerning the results of this paper.

References

- [1] E. Asarin, O. Maler, and A. Pnueli. Reachability analysis of dynamical systems having piecewise-constant derivatives. *Theoretical Computer Science*, 138(1):35–65, February 1995.
- [2] V. D. Blondel and J. N. Tsitsiklis. When is a pair of matrices mortal? *Information Processing Letters*, 63(5):283–286, September 1997.
- [3] V. D. Blondel and J. N. Tsitsiklis. Complexity of stability and controllability of elementary hybrid systems. *Automatica*, 35(3):473–489, 1999.
- [4] L. Blum, F. Cucker, M. Shub, and S. Smale. *Complexity and Real Computation*. Springer-Verlag, New York, 1998.
- [5] L. Blum, M. Shub, and S. Smale. On a theory of computation and complexity over the real numbers; NP completeness, recursive functions and universal machines. *Bulletin of the American Mathematical Society*, 21(1):1–46, July 1989.
- [6] J. Cassaigne and J. Karhumäki. Examples of undecidable problems for 2-generator matrix semigroups. *Theoretical Computer Science*, 204(1):29–34, September 1998.
- [7] M. R. Garey and D. S. Johnson. *Computers and Intractability*. Freeman, San Francisco, CA, 1979.
- [8] T. Harju and J. Karhumäki. Morphisms. In G. Rozenberg and A. Salomaa, eds., *Handbook of Formal Languages*, Volume 1, pp. 439–510. Springer-Verlag, Berlin, 1997.
- [9] T. A. Henzinger, P. W. Kopke, A. Puri, and P. Varaiya. What’s decidable about hybrid automata? *Journal of Computer and System Sciences*, 57(1):94–124, August 1998.
- [10] J. E. Hopcroft and J. D. Ullman. *Introduction to Automata Theory, Languages, and Computation*. Addison-Wesley, Reading, MA, 1979.
- [11] D. A. Klarner, J. C. Birget, and W. Satterfield. On the undecidability of the freeness of integer matrix semigroups. *International Journal of Algebra and Computation*, 1:223–226, 1991.
- [12] P. Koiran, M. Cosnard, and M. Garzon. Computability with low-dimensional dynamical systems. *Theoretical Computer Science*, 132(1–2):113–128, September 1994.
- [13] V. S. Kozyakin. Algebraic unsolvability of problems of absolute stability of desynchronized systems. *Scientific-Industrial Organization of Automatic Control Systems*, 6:41–47, 1990.
- [14] M. Krom. An unsolvable problem with products of matrices. *Mathematical System Theory*, 14:335–337, 1981.
- [15] M. Krom and M. Krom. Recursive solvability of problems with matrices. *Zeitschrift für Mathematische Logik und Grundlagen der Mathematik*, 35:437–442, 1989.

- [16] M. Krom and M. Krom. More on mortality. *American Mathematical Monthly*, 97:37–38, 1990.
- [17] Z. Manna. *Mathematical Theory of Computation*. McGraw-Hill, New York, 1974.
- [18] Y. Matiyasevich and G. Sénizergues. Decision problems for semi-Thue systems with a few rules. In *Proceedings, 11th Annual IEEE Symposium on Logic in Computer Science*, pages 523–531. IEEE Computer Society Press, New York, 1996. An extended version can be found on the web page <http://dept-info.labri.u-bordeaux.fr/~ges/publis.rewriting.html>.
- [19] C. Moore. Unpredictability and undecidability in dynamical systems. *Physical Review Letters*, 64(20):2354–2357, May 1990.
- [20] M. S. Paterson. Unsolvability in 3×3 matrices. *Studies in Applied Mathematics*, XLIX(1):105–107, March 1970.
- [21] Y. Saouter. The mortality of a pair of 2×2 matrices is decidable. Technical Report RR-2842, Institut National de Recherche en Informatique et en Automatique, 1996.
- [22] P. Schultz. Mortality of 2×2 matrices. *American Mathematical Monthly*, 84(2):463–464, 1977. Correction, 85:263, 1978.
- [23] H. S. Shank. The rational case of a matrix problem of Harrison. *Discrete Mathematics*, 28:207–212, 1979.
- [24] H. T. Siegelmann and E. D. Sontag. On the computational power of neural nets. *Journal of Computer and System Sciences*, 50(1):132–150, February 1995.
- [25] N. Vereshchagin. Occurrence of zero in a linear recursive sequence. *Mathematical Notes*, 38:609–615, 1985. Translation from *Matematicheskie Zametki* 38(2):609–615, 1985.
- [26] K. Weihrauch. A simple introduction to computable analysis. Technical Report 171–2/1995, Fernuniversität Gesamthochschule in Hagen, Fachbereich Informatik, Hagen, 1995.

Received March 22, 2001, and in revised form November 21, 2001. Online publication March 25, 2002.