On the mortality problem: from multiplicative matrix equations to linear recurrence sequences and beyond

Paul C. Bell[a,*], Igor Potapov[b,1], Pavel Semukhin[c]

[a] *Department of Computer Science, Byrom Street, Liverpool John Moores University, Liverpool, L3-3AF, UK, p.c.bell@ljmu.ac.uk*

[b] *Department of Computer Science, Ashton Building, Ashton Street, University of Liverpool, Liverpool, L69-3BX, UK, potapov@liverpool.ac.uk*

[c] *Department of Computer Science, Wolfson Building, Parks Road, University of Oxford, Oxford, OX1 3QD, UK, pavel.semukhin@cs.ox.ac.uk*

Abstract

We consider the following variant of the mortality problem: given $k \times k$ matrices $A_1, A_2, \ldots, A_t$, do there exist t nonnegative integers $m_1, m_2, \ldots, m_t$ such that the product $A_1^{m_1} A_2^{m_2} \cdots A_t^{m_t}$ is equal to the zero matrix? It is known that this problem is decidable when $t \leq 2$ for matrices over algebraic numbers but becomes undecidable for sufficiently large t and k, even for integral matrices.

In this paper, we prove the first decidability results for $t > 2$. We show as one of our central results that for $t = 3$ this problem in any dimension is Turing equivalent to the well-known Skolem problem for linear recurrence sequences. Our proof relies on the primary decomposition theorem for matrices. Up to now, this result has not been used to prove decidability results about matrix semigroups. As a corollary we obtain that the above problem is decidable for $t = 3$ and $k \leq 3$ for matrices over algebraic numbers and for $t = 3$ and $k = 4$ for matrices over real algebraic numbers. Another consequence is that the set of triples (m_1, m_2, m_3) for which the equation $A_1^{m_1} A_2^{m_2} A_3^{m_3}$ equals the zero matrix is equal to a finite union of direct products of semilinear sets.

For $t = 4$ we show that the solution set can be non-semilinear, and thus it seems unlikely that there is a direct connection to the Skolem problem. However we prove that the problem is still decidable for upper-triangular 2×2 rational matrices by employing powerful tools from transcendence theory such as Baker's theorem and S-unit equations.

Keywords: Linear recurrence sequences, Skolem's problem, mortality problem, matrix equations, primary decomposition theorem, Baker's theorem

*Corresponding author.

[1] Funding: Partially supported by EPSRC grants EP/R018472/1 and EP/M00077X/1.

1. Introduction

A large number of naturally-defined matrix problems are still unanswered, despite the long history of matrix theory. Some of these questions have recently drawn renewed interest in the context of the analysis of digital processes, verification problems, and links with several fundamental questions in mathematics [11, 7, 39, 41, 40, 37, 18, 14, 15, 38, 6, 45, 28].

One of these challenging problems is the *mortality problem* of whether the zero matrix belongs to a finitely generated matrix semigroup. It plays a central role in many questions from control theory and software verification [48, 10, 8, 38, 2]. The mortality problem has been known to be undecidable for matrices in $\mathbb{Z}^{3\times 3}$ since 1970 [43]. The current undecidability bounds for the $M(d, k \times k)$ problem (i.e., the mortality problem for semigroups generated by d matrices of size $k \times k$) are $M(6, 3 \times 3)$, $M(4, 5 \times 5)$, $M(3, 9 \times 9)$ and $M(2, 15 \times 15)$; see [13]. It is also known that the problem is NP-hard for 2×2 integer matrices [5] and is decidable for 2×2 integer matrices with determinant $0, \pm 1$ [36]. In the case of finite matrix semigroups of any dimension the mortality problem is known to be PSPACE-complete [27].

In this paper, we study a very natural variant of the mortality problem when matrices must appear in a fixed order (i.e., under bounded language constraint): *Given $k \times k$ matrices $A_1, A_2, \ldots, A_t$ over a ring $\mathcal{F}$, do there exist $m_1, m_2, \ldots, m_t \in \mathbb{N}$ such that $A_1^{m_1} A_2^{m_2} \ldots A_t^{m_t} = \mathbf{O}_{k,k}$, where $\mathbf{O}_{k,k}$ is $k \times k$ zero matrix?*

In general (i.e., replacing $\mathbf{O}_{k,k}$ by other matrices) this problem is known as the solvability of multiplicative matrix equations and has been studied for many decades. In its simplest form, when $k = 1$, the problem was studied by Harrison in 1969 [22] as a reformulation of the "accessibility problem" for linear sequential machines. The case $t = 1$ was solved in polynomial time in a celebrated paper by Kannan and Lipton in 1980 [26]. The case $t = 2$, i.e., $A^x B^y = C$ where A, B and C are commuting matrices, was solved by Cai, Lipton and Zalcstein in 1994 [12]. Later, in 1996, the solvability of matrix equations over commuting matrices was solved in polynomial time in [1] and in 2010 it was shown in [4] that $A^x B^y = C$ is decidable for non-commuting matrices of any dimension with algebraic coefficients by a reduction to the commutative case from [1]. However, it was also shown in [4] that the solvability of multiplicative matrix equations for sufficiently large natural numbers t and k is, in general, undecidable, by an encoding of *Hilbert's tenth problem* and in particular for the mortality problem with bounded language constraint. In 2015 it was also shown that the undecidability result holds for such equations with unitriangular matrices [33] and also in the case of specific equations with nonnegative matrices [24].

The decidability of matrix equations for non-commuting matrices is only known as corollaries of either recent decidability results for solving membership problem in 2×2 matrix semigroups [45, 46] or in the case of quite restricted classes of matrices, e.g., matrices from the Heisenberg group [28, 29] or row-monomial matrices over commutative semigroups [32]. In the other direction, progress has been made for matrix-exponential equations, but again in the case

of commuting matrices [38].

In this paper, we prove the first decidability results for the above problem when $t = 3$ and $t = 4$. We will call these problems the ABC-Z and ABCD-Z problems, respectively. More precisely, we will show that the ABC-Z problem in any dimension is Turing equivalent to the Skolem problem (also known as Skolem-Pisot problem) which asks whether a given linear recurrence sequence ever attains the value zero. Our proof relies on the primary decomposition theorem for matrices (Theorem 2). Up to now, this result has not been used to prove decidability results about matrix semigroups. As a corollary, we obtain that the ABC-Z problem is decidable for 2×2 and 3×3 matrices over algebraic numbers and also for 4×4 matrices over real algebraic numbers. Another consequence of the above equivalence is that the set of triples (m, n, ℓ) that satisfy the equation $A^m B^n C^\ell = \mathbf{O}_{k\times k}$ can be expressed as a finite union of direct products of semilinear sets.

In contrast to the ABC-Z problem, we show that the solution set of the ABCD-Z problem can be non-semilinear. This indicates that the ABCD-Z problem is unlikely to be related to Skolem's problem. However we will show that the ABCD-Z problem is decidable for upper-triangular 2×2 rational matrices. The proof of this result relies on powerful tools from transcendence theory such as Baker's theorem for linear forms in logarithms, S-unit equations from algebraic number theory, and the Frobenius rank inequality from matrix analysis. More precisely, we will reduce the ABCD-Z equation for upper-triangular 2×2 rational matrices to an equation of the form $ax+by+cz = 0$, where x, y, z are S-units, and then use an upper bound on the solutions of this equation (as in Theorem 5). On the other hand, if we try to generalize this result to arbitrary 2×2 rational matrices or to upper-triangular matrices of higher dimension, then we end up with an equation that contain a sum of four or more S-units. No effective upper bounds on the solutions of such equations are known. These generalizations thus seem to lie beyond the reach of current mathematical knowledge.

2. Preliminaries

We denote by $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{C}$ the sets of natural, integer, rational and complex numbers, respectively (where $\mathbb{N} = \{0, 1, \ldots\}$). We let $\mathbf{A}$ denote the set of algebraic numbers and $\mathbf{A}_\mathbb{R}$ denote the set of real algebraic numbers.

For a prime number p we define a valuation $v_p(x)$ for nonzero $x \in \mathbb{Q}$ as follows: if $x = p^k \frac{m}{n}$, where $k, m, n \in \mathbb{Z}$ and p does not divide m or n, then $v_p(x) = v_p(p^k \frac{m}{n}) = k$.

Throughout this paper $\mathcal{F}$ will denote either the ring of integers $\mathbb{Z}$ or one of the fields $\mathbb{Q}$, $\mathbf{A}$, $\mathbf{A}_\mathbb{R}$ or $\mathbb{C}$. We will use the notation $\mathcal{F}^{n\times m}$ for the set of $n \times m$ matrices over $\mathcal{F}$.

We denote by $\mathbf{e}_i$ the i'th standard basis vector of some dimension (which will be clear from the context). Let $\mathbf{O}_{n,m}$ be the zero matrix of size $n \times m$, $\mathbf{I}_n$ be the identity matrix of size $n \times n$, and $\mathbf{0}_n$ be the zero column vector of length n. Given a finite set of matrices $\mathcal{G} \subseteq \mathcal{F}^{n\times n}$, we denote by $\langle \mathcal{G} \rangle$ the multiplicative semigroup generated by $\mathcal{G}$.

If $A \in \mathcal{F}^{m\times m}$ and $B \in \mathcal{F}^{n\times n}$, then we define the direct sum of A and B as $A \oplus B = \left[\begin{array}{c|c} A & \mathbf{O}_{m,n} \\ \hline \mathbf{O}_{n,m} & B \end{array}\right]$. Let $C \in \mathcal{F}^{k\times k}$ be a square matrix. We write $\det(C)$ for the determinant of C. We call C singular if $\det(C) = 0$; otherwise it is said to be invertible (or non-singular). Matrices A and B from $\mathcal{F}^{k\times k}$ are called *similar* if there exists an invertible $k \times k$ matrix S (perhaps over a larger field containing $\mathcal{F}$) such that $A = SBS^{-1}$. In this case, S is said to be a similarity matrix transforming A to B.

We will also require the following inequality regarding ranks of matrices, known as the *Frobenius rank inequality*. As usual, the rank of a matrix A, denoted $\mathsf{Rk}(A)$, is defined as the dimension of the subspace spanned by its columns. See [25] for further details and a proof of the Frobenius rank inequality.

Theorem 1 (Frobenius rank inequality)**.** *Let $A, B, C \in \mathcal{F}^{k\times k}$. Then*

$$\mathsf{Rk}(AB) + \mathsf{Rk}(BC) \leq \mathsf{Rk}(ABC) + \mathsf{Rk}(B)$$

In the proof of our first main result about the ABC-Z problem we will make use of the primary decomposition theorem for matrices. The minimal polynomial of a matrix $A \in \mathcal{F}^{n\times n}$, denoted m_A, is defined as the monic polynomial of minimal degree such that $m_A(A) = \mathbf{O}_{n,n}$.

Theorem 2 (Primary decomposition theorem [23])**.** *Let A be a matrix from $\mathcal{F}^{n\times n}$, where $\mathcal{F}$ is a field. Let $m_A(x)$ be the minimal polynomial for A such that*

$$m_A(x) = p_1(x)^{r_1} \cdots p_k(x)^{r_k},$$

where the $p_i(x)$ are distinct irreducible monic polynomials over $\mathcal{F}$ and the r_i are positive integers. Let W_i be the null space of $p_i(A)^{r_i}$ and let S_i be a basis for W_i. Then

(1) *$S_1 \cup \cdots \cup S_k$ is a basis for $\mathcal{F}^n$ and $\mathcal{F}^n = W_1 \oplus \cdots \oplus W_k$,*
(2) *each W_i is invariant under A, that is, $A\mathbf{x} \in W_i$ for any $\mathbf{x} \in W_i$,*
(3) *let S be a matrix whose columns are equal to the basis vectors from $S_1 \cup \cdots \cup S_k$; then*

$$S^{-1}AS = A_1 \oplus \cdots \oplus A_k,$$

where each A_i is a matrix over $\mathcal{F}$ of the size $|S_i| \times |S_i|$, and the minimal polynomial of A_i is equal to $p_i(x)^{r_i}$.

We will also need the following two propositions.

Proposition 3. *If $p(x)$ is a polynomial over a field $\mathcal{F}$, where $\mathcal{F}$ is either $\mathbb{Q}$, $\mathbf{A}$ or $\mathbf{A}_{\mathbb{R}}$, then the primary decomposition of $p(x)$ can be algorithmically computed.*

Proof. If $\mathcal{F} = \mathbb{Q}$, then one can use the LLL algorithm [31] to find the primary decomposition in polynomial time.

If $\mathcal{F} = \mathbf{A}$, then one can use well-known algorithms to compute standard representations of the roots of $p(x)$ in polynomial time [3, 16, 42, 44]. Let

$\lambda_1, \ldots, \lambda_k$ be distinct roots of $p(x)$ with multiplicities $m_1, \ldots, m_k$, respectively. In this case the primary decomposition of $p(x)$ is equal to

$$p(x) = (x - \lambda_1)^{m_1} \cdots (x - \lambda_k)^{m_k}.$$

If $\mathcal{F} = \mathbf{A}_{\mathbb{R}}$, then again one can compute standard representations of the roots of $p(x)$ in $\mathbf{A}$ in polynomial time. Let $\lambda_1, \ldots, \lambda_i$ be real roots of $p(x)$ with multiplicities $m_1, \ldots, m_i$ and let $\mu_1, \overline{\mu}_1, \ldots, \mu_j, \overline{\mu}_j$ be pairs of complex conjugate roots of $p(x)$ with multiplicities $n_1, \ldots, n_j$, respectively. Then the primary decomposition of $p(x)$ over $\mathbf{A}_{\mathbb{R}}$ is equal to

$$p(x) = (x - \lambda_1)^{m_1} \cdots (x - \lambda_i)^{m_i} p_1(x)^{n_1} \cdots p_j(x)^{n_j},$$

where $p_s(x) = (x - \mu_s)(x - \overline{\mu}_s) = x^2 - 2\,\mathrm{Re}(\mu_s)x + |\mu_s|^2$ for $s = 1, \ldots, j$. □

Proposition 4. *Let $A \in \mathcal{F}^{n \times n}$ and $m_A(x)$ be the minimal polynomial of A. Then A is invertible if and only if $m_A(x)$ has a nonzero free coefficient, i.e., $m_A(x)$ is not divisible by x.*

Proof. Suppose that A is invertible but $m_A(x) = xm'(x)$ for some polynomial $m'(x)$. Then

$$\mathbf{O}_{n,n} = m_A(A) = A \cdot m'(A).$$

Multiplying the above equation by A^{-1} we obtain $m'(A) = \mathbf{O}_{n,n}$, which contradicts the assumption that $m_A(x)$ is the minimal polynomial for A.

On the other hand, it x does not divide $m_A(x)$, then $m_A(x) = xm'(x) + a$ for some $m'(x)$ and a nonzero constant a. Then

$$\mathbf{O}_{n,n} = m_A(A) = A \cdot m'(A) + a\mathbf{I}_n.$$

From this equation we conclude that A is invertible, and $A^{-1} = -\frac{1}{a}m'(A)$. □

Our proof of the decidability of the ABCD-Z problem for 2×2 upper-triangular rational matrices relies on the following result, which is proved using Baker's theorem on linear forms in logarithms (see Corollary 4 in [17] and also [19]).

Theorem 5. *Let $S = \{p_1, \ldots, p_s\}$ be a finite collection of prime numbers and let a, b, c be relatively prime nonzero integers, that is,* $\gcd(a, b, c) = 1$.

If x, y, z are relatively prime nonzero integers composed of primes from S that satisfy the equation $ax + by + cz = 0$, then

$$\max\{|x|, |y|, |z|\} < \exp(s^{Cs} P^{4/3} \log A)$$

for some constant C, where $P = \max\{p_1, \ldots, p_s\}$ and $A = \max\{|a|, |b|, |c|, 3\}$.

Remark 6. *Rational numbers whose numerator and denominator are divisible only by the primes from S are called* S-units.

3. Linear recurrence sequences and semilinear sets

There is a long history in computer science and mathematics of studying sequences of numbers defined by some recurrence relation, where the next value in the sequence depends upon some 'finite memory' of previous values in the sequence. Possibly the simplest, and certainly the most well known of these, is the *Fibonacci sequence*. This sequence is defined by the linear recurrence $F(n) = F(n-1) + F(n-2)$ with $F(1) = 1$ and $F(0) = 0$ being given as the *initial conditions*. We may generalise the Fibonacci sequence to define a *linear recurrence sequence*, which find application in many areas of mathematics and other sciences and for which many questions remain open. Let $\mathcal{F}$ be a ring; a sequence $(u_n)_{n=0}^{\infty}$ is called a *linear recurrence sequence* (1-LRS) if it satisfies a relation of the form:

$$u_n = a_{k-1}u_{n-1} + \cdots + a_1 u_{n-k+1} + a_0 u_{n-k},$$

for any $n \geq k$, where each $a_0, a_1, \ldots, a_{k-1} \in \mathcal{F}$ are fixed coefficients[2]. Such a sequence $(u_n)_{n=0}^{\infty}$ is said to be of depth k if it satisfies no shorter linear recurrence relation (for any $k' < k$). We call the initial k values of the sequence $u_0, u_1, \ldots, u_{k-1}$ the initial conditions of the 1-LRS. Given the initial conditions and coefficients of a 1-LRS, every element is uniquely determined.

The *zero set* of a 1-LRS is defined as follows: $\mathcal{Z}(u_n) = \{j \in \mathbb{N} \mid u_j = 0\}$.

There are various questions that one may ask regarding $\mathcal{Z}(u_n)$. One notable example relates to the famous "Skolem problem" which is stated in the following way:

Problem 7 (Skolem's problem)**.** *Given the coefficients and initial conditions of a depth k 1-LRS $(u_n)_{n=0}^{\infty}$, determine if $\mathcal{Z}(u_n)$ is the empty set.*

Skolem's problem has a long and rich history; see [20] for a good survey. We note here that the problem remains open despite properties of zero sets having been studied even since 1934 [47]. It is known that Skolem's problem is at least NP-hard [9] and that it is decidable for depth 3 over $\mathbf{A}$ and for depth 4 over $\mathbf{A}_{\mathbb{R}}$; see [48] and [35][3]. Other interesting questions are related to the structure of $\mathcal{Z}(u_n)$. We remind the reader the definition of semilinear sets.

Definition 8 (Semilinear set)**.** *A set $S \subseteq \mathbb{N}$ is called* semilinear *if it is the union of a finite set and finitely many arithmetic progressions.*

A seminal result regarding 1-LRSs is that there zero sets are semilinear.

[2] In the literature, such a sequence is ordinarily called an LRS; we use the nomenclature 1-LRS since we will study a multidimensional variant of this concept. Also, 1-LRS are usually considered over integers, but in the present paper we will consider such sequences over algebraic numbers.

[3] A proof of decidability for depth 5 was claimed in [20], although there is possibly a gap in the proof [39].

Theorem 9 (Skolem, Mahler, Lech [34, 47, 30, 20, 21])**.** *The zero set of a 1-LRS over $\mathbb{C}$ (or more generally over any field of characteristic 0) is semilinear.*

In particular, if $(u_n)_{n=0}^{\infty}$ is a 1-LRS whose coefficients and initial conditions are algebraic numbers, then one can algorithmically find a number $L \in \mathbb{N}$ such that for every $i = 0, \ldots, L-1$, if we let $u_m^i = u_{i+mL}$, then

(1) *the sequence $(u_m^i)_{m=0}^{\infty}$ is a 1-LRS of the same depth as $(u_n)_{n=0}^{\infty}$, and*
(2) *either $\mathcal{Z}(u_m^i) = \mathbb{N}$ or $\mathcal{Z}(u_m^i)$ is finite.*

Note that in the above theorem we can decide whether $\mathcal{Z}(u_m^i)$ is finite or $\mathcal{Z}(u_m^i) = \mathbb{N}$ because $\mathcal{Z}(u_m^i) = \mathbb{N}$ if and only if $u_0^i = \cdots = u_{k-1}^i = 0$, where k is the depth of $(u_m^i)_{m=0}^{\infty}$.

We will also consider a stronger version of the Skolem problem.

Problem 10 (Strong Skolem Problem)**.** *Given the coefficients and initial conditions of a 1-LRS $(u_n)_{n=0}^{\infty}$ over $\mathbf{A}$, find a description of the set $\mathcal{Z}(u_n)$. That is, find a finite set F such that $\mathcal{Z}(u_n) = F$ if $\mathcal{Z}(u_n)$ is finite or, if $\mathcal{Z}(u_n)$ is infinite, find a finite set F, a constant $L \in \mathbb{N}$ and numbers $i_1, \ldots, i_t \in \{0, \ldots, L-1\}$ such that*

$$\mathcal{Z}(u_n) = F \cup \{i_1 + mL : m \in \mathbb{N}\} \cup \cdots \cup \{i_t + mL : m \in \mathbb{N}\}.$$

Using the Skolem-Mahler-Lech theorem we can prove an equivalence between the strong version of the Skolem problem and the standard version[4].

Theorem 11. *Skolem's problem of depth k over $\mathbf{A}$ is Turing equivalent to the strong Skolem problem of the same depth.*

Proof. Obviously, Skolem's problem is reducible to the strong Skolem problem. We now show a reduction in the other direction.

Let $(u_n)_{n=0}^{\infty}$ be a depth-k 1-LRS over $\mathbf{A}$. By Theorem 9, we can algorithmically find a number L such that, for every $i = 0, \ldots, L-1$, the sequence $u_m^i = u_{i+mL}$ is a 1-LRS of depth k which is either everywhere zero, that is, $\mathcal{Z}(u_m^i) = \mathbb{N}$ or $\mathcal{Z}(u_m^i)$ is finite. Recall that we can decide whether $\mathcal{Z}(u_m^i)$ is equal to $\mathbb{N}$ by considering the first k terms of $(u_m^i)_{m=0}^{\infty}$.

By definition, we have $\mathcal{Z}(u_n) = \bigcup_{i=0}^{L-1} \{i + L \cdot \mathcal{Z}(u_m^i)\}$. So, if $\mathcal{Z}(u_m^i) = \mathbb{N}$, then $\{i + L \cdot \mathcal{Z}(u_m^i)\} = \{i + mL : m \in \mathbb{N}\}$, and if $\mathcal{Z}(u_m^i)$ is finite, then so is $\{i + L \cdot \mathcal{Z}(u_m^i)\}$.

To finish the proof we need to show how to compute $\mathcal{Z}(u_m^i)$, and hence $\{i + L \cdot \mathcal{Z}(u_m^i)\}$, when it is finite. For this we will use an oracle for the Skolem problem. Let m' be the smallest number such that $\mathcal{Z}(u_{m+m'}^i)$ is empty. Such an m' exists because $\mathcal{Z}(u_m^i)$ is finite. Furthermore, $(u_{m+m'})_{m=0}^{\infty}$ is a 1-LRS of depth k for any m'. So, we ask the oracle for the Skolem problem to decide

[4]This result was announced in [48] without a proof, probably with a similar construction in mind.

whether $\mathcal{Z}(u^i_{m+m'}) = \emptyset$ for each $m' \in \mathbb{N}$ starting from 0 until we find one for which $\mathcal{Z}(u^i_{m+m'})$ is empty. Note that we do not have any bound on m' because we do not even know the size of $\mathcal{Z}(u^i_m)$. All we know is that $\mathcal{Z}(u^i_m)$ is finite, and hence the above algorithm will eventually terminate. Since $\mathcal{Z}(u^i_m)$ is a subset of $\{0, \ldots, m'\}$, then we can compute it by checking whether $u^i_m = 0$ for $m = 0, \ldots, m'$. □

Linear recurrence sequences can also be represented using matrices [20]:

Lemma 12. *Let $\mathcal{F}$ be a ring; for a sequence $(u_n)_{n=0}^{\infty}$ over $\mathcal{F}$ the following are equivalent:*

(1) *$(u_n)_{n=0}^{\infty}$ is a 1-LRS of depth k.*
(2) *There are vectors $\mathbf{u}, \mathbf{v} \in \mathcal{F}^k$ and a matrix $M \in \mathcal{F}^{k\times k}$ such that $u_n = \mathbf{u}^T M^n \mathbf{v}$ for $n \in \mathbb{N}$.*

Moreover, for any matrix $M \in \mathcal{F}^{k\times k}$, the sequence $u_n = (M^n)_{[1,k]}$ is a 1-LRS of depth at most k. On the other hand, if $(u_n)_{n=0}^{\infty}$ is a 1-LRS of depth k, then there is a matrix $M \in \mathcal{F}^{(k+1)\times(k+1)}$ such that $u_n = (M^n)_{[1,k+1]}$ for all $n \in \mathbb{N}$.

Lemma 12 motivates the following definition of n-dimensional Linear Recurrence Sequences (n-LRSs) which as we show later are related to the mortality problem for bounded languages.

Definition 13 (n-LRS)**.** *A multidimensional sequence $u_{m_1,m_2,\ldots,m_n}$ is called an n-LRS of depth k over $\mathcal{F}$ if there exist two vectors $\mathbf{u}, \mathbf{v} \in \mathcal{F}^k$ and matrices $M_1, M_2, \ldots, M_n \in \mathcal{F}^{k\times k}$ such that*

$$u_{m_1,m_2,\ldots,m_n} = \mathbf{u}^T M_1^{m_1} M_2^{m_2} \cdots M_n^{m_n} \mathbf{v}.$$

4. The mortality problem for bounded languages

We remind the reader of the definition of the mortality problem for bounded languages.

Problem 14 (Mortality for bounded languages)**.** *Given $k\times k$ matrices $A_1, \ldots, A_t$ over a ring $\mathcal{F}$, do there exist $m_1, m_2, \ldots, m_t \in \mathbb{N}$ such that*

$$A_1^{m_1} A_2^{m_2} \ldots A_t^{m_t} = \mathbf{O}_{k,k}?$$

Recall that for $t = 3$ and $t = 4$ this problem is called the ABC-Z and ABCD-Z problem, respectively. Our first main result is that the ABC-Z problem is computationally equivalent to the Skolem problem for 1-LRS. Our reduction holds in any dimension and over the same number field which means that any new decidability results for the Skolem problem will automatically extend the decidability of ABC-Z equations and can immediately lead to new decidability results for equations in dimensions 2, 3 and 4. For the proof we will need the following technical lemma.

Lemma 15. *Let $\mathcal{F}$ be a field, and suppose $A, B, C \in \mathcal{F}^{k\times k}$ are matrices of the form*

$$A = \left[\begin{array}{c|c} A_{s,s} & \mathbf{O}_{s,k-s} \\ \hline \mathbf{O}_{k-s,s} & \mathbf{O}_{k-s,k-s} \end{array}\right],\ B = \left[\begin{array}{c|c} B_{s,t} & X_{s,k-t} \\ \hline Y_{k-s,t} & Z_{k-s,k-t} \end{array}\right],\ C = \left[\begin{array}{c|c} C_{t,t} & \mathbf{O}_{t,k-t} \\ \hline \mathbf{O}_{k-t,t} & \mathbf{O}_{k-t,k-t} \end{array}\right]$$

for some $s, t \le k$, where $A_{s,s}$, $B_{s,t}$, $X_{s,k-t}$, $Y_{k-s,t}$, $Z_{k-s,k-t}$ and $C_{t,t}$ are matrices over $\mathcal{F}$ whose dimensions are indicated by their subscripts (in particular, $A = A_{s,s} \oplus \mathbf{O}_{k-s,k-s}$ and $C = C_{t,t} \oplus \mathbf{O}_{k-t,k-t}$). If $A_{s,s}$ and $C_{t,t}$ are invertible matrices, then the equation $ABC = \mathbf{O}_{k,k}$ is equivalent to $B_{s,t} = \mathbf{O}_{s,t}$.

Proof. It is not hard to check that

$$AB = \left[\begin{array}{c|c} A_{s,s} & \mathbf{O}_{s,k-s} \\ \hline \mathbf{O}_{k-s,s} & \mathbf{O}_{k-s,k-s} \end{array}\right] \cdot \left[\begin{array}{c|c} B_{s,t} & X_{s,k-t} \\ \hline Y_{k-s,t} & Z_{k-s,k-t} \end{array}\right] = \left[\begin{array}{c|c} A_{s,s}B_{s,t} & A_{s,s}X_{s,k-t} \\ \hline \mathbf{O}_{k-s,t} & \mathbf{O}_{k-s,k-t} \end{array}\right],$$

and hence

$$(AB)C = \left[\begin{array}{c|c} A_{s,s}B_{s,t} & A_{s,s}X_{s,k-t} \\ \hline \mathbf{O}_{k-s,t} & \mathbf{O}_{k-s,k-t} \end{array}\right] \cdot \left[\begin{array}{c|c} C_{t,t} & \mathbf{O}_{t,k-t} \\ \hline \mathbf{O}_{k-t,t} & \mathbf{O}_{k-t,k-t} \end{array}\right] = \left[\begin{array}{c|c} A_{s,s}B_{s,t}C_{t,t} & \mathbf{O}_{s,k-t} \\ \hline \mathbf{O}_{k-s,t} & \mathbf{O}_{k-s,k-t} \end{array}\right].$$

So, if $B_{s,t} = \mathbf{O}_{s,t}$, then $ABC = \mathbf{O}_{k,k}$. Conversely, if $ABC = \mathbf{O}_{k,k}$, then $A_{s,s}B_{s,t}C_{t,t} = \mathbf{O}_{s,t}$. Using the fact that $A_{s,s}$ and $C_{t,t}$ are invertible matrices, we can multiply the equation $A_{s,s}B_{s,t}C_{t,t} = \mathbf{O}_{s,t}$ by $A_{s,s}^{-1}$ on the left and by $C_{t,t}^{-1}$ on the right to obtain that $B_{s,t} = \mathbf{O}_{s,t}$. □

The next lemma is similar to Lemma 15 and can also be proved by directly multiplying the matrices.

Lemma 16. *(1) Suppose $A, B \in \mathcal{F}^{k\times k}$ are matrices of the following form*

$$A = \left[\begin{array}{c|c} A_{s,s} & \mathbf{O}_{s,k-s} \\ \hline \mathbf{O}_{k-s,s} & \mathbf{O}_{k-s,k-s} \end{array}\right] = A_{s,s} \oplus \mathbf{O}_{k-s,k-s} \quad \textit{and} \quad B = \left[\begin{array}{c} B_{s,k} \\ \hline X_{k-s,k} \end{array}\right],$$

for some $s \le k$. If $A_{s,s}$ is invertible, then $AB = \mathbf{O}_{k,k}$ is equivalent to $B_{s,k} = \mathbf{O}_{s,k}$.

(2) Suppose $A, B \in \mathcal{F}^{k\times k}$ are matrices of the following form

$$A = \left[\begin{array}{c|c} A_{k,t} & Y_{k,k-t} \end{array}\right] \quad \textit{and} \quad B = \left[\begin{array}{c|c} B_{t,t} & \mathbf{O}_{t,k-t} \\ \hline \mathbf{O}_{k-t,t} & \mathbf{O}_{k-t,k-t} \end{array}\right] = B_{t,t} \oplus \mathbf{O}_{k-t,k-t},$$

for some $t \le k$. If $B_{t,t}$ is invertible, then $AB = \mathbf{O}_{k,k}$ is equivalent to $A_{k,t} = \mathbf{O}_{k,t}$.

As in Lemma 15, in the above equations $A_{s,s}$, $B_{s,k}$, $X_{k-s,k}$, $A_{k,t}$, $Y_{k,k-t}$ and $B_{t,t}$ are matrices over $\mathcal{F}$ whose dimensions are indicated by their subscripts.

Theorem 17. *Let $\mathcal{F}$ be the ring of integers $\mathbb{Z}$ or one of the fields $\mathbb{Q}$, $\mathbf{A}$ or $\mathbf{A}_{\mathbb{R}}$. Then the ABC-Z problem for matrices from $\mathcal{F}^{k\times k}$ is Turing equivalent to the Skolem problem of depth k over $\mathcal{F}$.*

Proof. First, we show a reduction from the ABC-Z problem to the Skolem problem.

Clearly, the ABC-Z problem over $\mathbb{Z}$ is equivalent to the ABC-Z problem over $\mathbb{Q}$ (by multiplying the matrices A, B, C by a suitable integer number). It is also not hard to see that the Skolem problem for 1-LRS over $\mathbb{Q}$ is equivalent to the Skolem problem over $\mathbb{Z}$ for 1-LRS of the same depth. Indeed, by Lemma 12 we can express any 1-LRS $(u_n)_{n=0}^{\infty}$ over $\mathbb{Q}$ as $u_n = \mathbf{u}^T M^n \mathbf{v}$ for some rational vectors $\mathbf{u}$ and $\mathbf{v}$ and a rational matrix M. If we multiply $\mathbf{u}$, $\mathbf{v}$ and M by a suitable natural number t, then $(t^{n+2}u_n)_{n=0}^{\infty}$ will be an integer 1-LRS, which has the same zero set as $(u_n)_{n=0}^{\infty}$. Hence, without loss of generality, we will assume that $\mathcal{F}$ is one of the fields $\mathbb{Q}$, $\mathbf{A}$ or $\mathbf{A}_{\mathbb{R}}$.

Consider an instance of the ABC-Z problem $A^m B^n C^\ell = \mathbf{O}_{k,k}$, where $A, B, C \in \mathcal{F}^{k,k}$. Let $\chi_A(x)$ be the characteristic polynomial of A. By Proposition 3, we can find a primary decomposition $\chi_A(x) = p_1(x)^{m_1} \cdots p_t(x)^{m_t}$, where $p_1(x), \ldots, p_t(x)$ are distinct irreducible monic polynomials. From this decomposition we can find the minimal polynomial $m_A(x)$ of A because $m_A(x)$ is a factor of $\chi_A(x)$, and we can check all divisors of $\chi_A(x)$ to find $m_A(x)$.

Let $m_A(x) = p_1(x)^{r_1} \cdots p_u(x)^{r_u}$, where $p_1(x), \ldots, p_u(x)$ are distinct irreducible monic polynomials. Now we apply the primary decomposition theorem (Theorem 2) to A. Let S_i be a basis for the null space of $p_i(A)^{r_i}$, which can be found, e.g., using Gaussian elimination. Let S be a matrix whose columns are the vectors of the basis $S_1 \cup \cdots \cup S_u$. Then

$$S^{-1}AS = A_1 \oplus \cdots \oplus A_u,$$

where the minimal polynomial of A_i is $p_i(A)^{r_i}$ for $i = 1, \ldots, u$. Similarly, we can compute a primary decomposition $m_C(x) = q_1(x)^{s_1} \cdots q_v(x)^{s_v}$ of the minimal polynomial for C, where $q_1(x), \ldots, q_v(x)$ are distinct irreducible monic polynomials, and a matrix T such that

$$T^{-1}CT = C_1 \oplus \cdots \oplus C_v,$$

where the minimal polynomial of C_i is $q_i(C)^{s_i}$ for $i = 1, \ldots, v$.

Note that if $p(x)$ is an irreducible monic polynomial, then either $p(x) = x$ or x does not divide $p(x)$. So, among the polynomials $p_1(x), \ldots, p_u(x)$ in the primary decomposition of $m_A(x)$ at most one is equal to x, and the same holds for the polynomials $q_1(x), \ldots, q_v(x)$ in the primary decomposition of $m_C(x)$.

Suppose we have, for example, that $p_u(x) = x$. In this case $m_A(x) = p_1(x)^{r_1} \cdots p_{u-1}(x)^{r_{u-1}} x^{r_u}$, and $S^{-1}AS = A_1 \oplus \cdots \oplus A_{u-1} \oplus A_u$, where the minimal polynomial of A_u is x^{r_u}, and hence A_u is a nilpotent matrix of index r_u. Recall that, for $i = 1, \ldots, u-1$, the polynomial $p_i(x)$ is not divisible by x, and thus neither is $p_i(x)^{r_i}$, which is the minimal polynomial for A_i. Hence, by Proposition 4, A_i is invertible. Let $A_{\text{inv}} = A_1 \oplus \cdots \oplus A_{u-1}$ and $A_{\text{nil}} = A_u$. Then we obtain

$$S^{-1}AS = A_{\text{inv}} \oplus A_{\text{nil}}, \tag{1}$$

where A_{inv} is invertible, and A_{nil} is nilpotent. If $p_i(x) = x$ for some $i < u$, then we need in addition to permute some rows and columns of matrix S to obtain

one that gives us Equation (1) above. If none of the $p_i(x)$ is equal to x, then we assume that A_{nil} is the empty matrix of size 0×0.

The same reasoning can be applied to matrix C, that is, we can compute an invertible matrix C_{inv}, a nilpotent (or empty) matrix C_{nil}, and an invertible matrix T such that

$$T^{-1}CT = C_{\text{inv}} \oplus C_{\text{nil}}.$$

Note that the indices of the nilpotent matrices A_{nil} and C_{nil} are at most k, and hence A_{nil}^k and C_{nil}^k are zero (or empty) matrices.

Our goal is to find all triples $(m, n, \ell) \in \mathbb{N}^3$ for which $A^m B^n C^\ell = \mathbf{O}_{k,k}$. In order to do this we will consider four cases: (1) $m \geq k$ and $\ell \geq k$, (2) $m < k$ and $\ell < k$, (3) $m \geq k$ and $\ell < k$, and (4) $m < k$ and $\ell \geq k$.

Before dealing with each of these cases, we note that the equation $A^m B^n C^\ell = \mathbf{O}_{k,k}$ is equivalent to

$$\begin{aligned} S(A_{\text{inv}}^m \oplus A_{\text{nil}}^m)S^{-1}B^nT(C_{\text{inv}}^\ell \oplus C_{\text{nil}}^\ell)T^{-1} = \mathbf{O}_{k,k} \quad \text{or to} \\ (A_{\text{inv}}^m \oplus A_{\text{nil}}^m)S^{-1}B^nT(C_{\text{inv}}^\ell \oplus C_{\text{nil}}^\ell) = \mathbf{O}_{k,k} \end{aligned}$$

because S and T are invertible matrices.

Now suppose A_{inv} has size $s \times s$, and C_{inv} has size $t \times t$ for some $s, t \leq k$.

Case 1: $m \geq k$ and $\ell \geq k$. Since $m, \ell \geq k$, we have $A_{\text{nil}}^m = \mathbf{O}_{k-s,k-s}$ and $C_{\text{nil}}^\ell = \mathbf{O}_{k-t,k-t}$, and hence the equation $A^m B^n C^\ell = \mathbf{O}_{k,k}$ is equivalent to

$$(A_{\text{inv}}^m \oplus \mathbf{O}_{k-s,k-s})S^{-1}B^nT(C_{\text{inv}}^\ell \oplus \mathbf{O}_{k-t,k-t}) = \mathbf{O}_{k,k}. \tag{2}$$

Suppose the matrix $S^{-1}B^nT$ has a form $S^{-1}B^nT = \left[\begin{array}{c|c} B_{s,t} & X_{s,k-t} \\ \hline Y_{k-s,t} & Z_{k-s,k-t} \end{array}\right]$. Since A_{inv}^m and C_{inv}^ℓ are invertible matrices, Lemma 15 implies that Equation (2) is equivalent to $B_{s,t} = \mathbf{O}_{s,t}$. Therefore, we obtain the following equivalence: $A^m B^n C^\ell = \mathbf{O}_{k,k}$ if and only if

$$s_n^{i,j} = (\mathbf{e}_i^\top S^{-1})B^n(T\mathbf{e}_j) = 0 \quad \text{for all } i = 1, \ldots, s \text{ and } j = 1, \ldots, t. \tag{3}$$

By Lemma 12, the sequence $(s_n^{i,j})_{n=0}^\infty$ is a 1-LRS of order k over $\mathcal{F}$. As in the proof of Theorem 11, we can use an oracle for the Skolem problem for 1-LRS of depth k over $\mathcal{F}$ to compute the descriptions of the semilinear sets $\mathcal{Z}(s_n^{i,j})$. Hence we can compute a description of the intersection $Z_1 = \bigcap_{\substack{i=1,\ldots,s \\ j=1,\ldots,t}} \mathcal{Z}(s_n^{i,j})$, which is also a semilinear set. An important observation is that the set Z_1 does not depend on m and ℓ.

Case 2: $m < k$ and $\ell < k$. Fix some $m < k$ and $\ell < k$. For this particular choice of m and ℓ, the equation $A^m B^n C^\ell = \mathbf{O}_{k,k}$ is equivalent to

$$s_n^{i,j} = (\mathbf{e}_i^\top A^m)B^n(C^\ell \mathbf{e}_j) = 0 \quad \text{for all } i = 1, \ldots, k \text{ and } j = 1, \ldots, k.$$

Again, by Lemma 12, the sequence $(s_n^{i,j})_{n=0}^\infty$ is a 1-LRS of order k over $\mathcal{F}$, and we can use an oracle for the Skolem problem for 1-LRS of depth k over $\mathcal{F}$

to compute the descriptions of the semilinear sets $\mathcal{Z}(s_n^{i,j})$. Therefore, we can compute a description of the intersection $Z_2(m,\ell) = \bigcap_{\substack{i=1,\ldots,k\\ j=1,\ldots,k}} \mathcal{Z}(s_n^{i,j})$ which is equal to all values of n for which $A^m B^n C^\ell = \mathbf{O}_{k,k}$ holds for fixed $m, \ell < k$.

Case 3: $m \geq k$ and $\ell < k$. To solve this case we will combine ideas from cases (1) and (2). Fix some $\ell < k$ and let m be any integer such that $m \geq k$. Then $A_{\text{nil}}^m = \mathbf{O}_{k-s,k-s}$, and the equation $A^m B^n C^\ell = \mathbf{O}_{k,k}$ is equivalent to

$$(A_{\text{inv}}^m \oplus \mathbf{O}_{k-s,k-s}) S^{-1} B^n C^\ell = \mathbf{O}_{k,k}. \tag{4}$$

Suppose the matrix $S^{-1}B^nC^\ell$ has a form $S^{-1}B^nC^\ell = \left[\frac{B_{s,k}}{X_{k-s,k}}\right]$. Since A_{inv}^m is invertible, Lemma 16 implies that Equation (4) is equivalent to $B_{s,k} = \mathbf{O}_{s,k}$. Therefore, Equation (4) is equivalent to

$$s_n^{i,j} = (\mathbf{e}_i^\top S^{-1}) B^n (C^\ell \mathbf{e}_j) = 0 \quad \text{for all } i = 1, \ldots, s \text{ and } j = 1, \ldots, k.$$

As in the previous two cases, we can use an oracle for the Skolem problem for 1-LRS of depth k over $\mathcal{F}$ to compute the descriptions of the semilinear sets $\mathcal{Z}(s_n^{i,j})$ and of the intersection $Z_3(\ell) = \bigcap_{\substack{i=1,\ldots,s\\ j=1,\ldots,k}} \mathcal{Z}(s_n^{i,j})$. $Z_3(\ell)$ is the set of all n for which $A^m B^n C^\ell = \mathbf{O}_{k,k}$ holds for a fixed $\ell < k$ and for any $m \geq k$.

Case 4: $m < k$ and $\ell \geq k$. Fix some $m < k$ and let ℓ be any integer such that $\ell \geq k$. Using the same ideas as in Case 3 we can use an oracle for the Skolem problem to compute a description of a semilinear set $Z_4(m)$ which is equal to all values of n for which $A^m B^n C^\ell = \mathbf{O}_{k,k}$ holds for a fixed $m < k$ and for any $\ell \geq k$.

Combining all the above cases together, we conclude that the set of all triples $(m,n,\ell) \in \mathbb{N}^3$ that satisfy the equation $A^m B^n C^\ell = \mathbf{O}_{k,k}$ is equal to the following union

$$\{(m,n,\ell) : n \in Z_1 \text{ and } m,\ell \geq k\} \bigcup \bigcup_{m,\ell<k} \{(m,n,\ell) : n \in Z_2(m,\ell)\} \bigcup$$
$$\bigcup_{\ell<k} \{(m,n,\ell) : n \in Z_3(\ell) \text{ and } m \geq k\} \bigcup \bigcup_{m<k} \{(m,n,\ell) : n \in Z_4(m) \text{ and } \ell \geq k\}. \tag{5}$$

Having a description for the above set, we can decide whether is it empty or not, that is, whether there exist $m,n,\ell \in \mathbb{N}$ such that $A^m B^n C^\ell = \mathbf{O}_{k,k}$.

We now show the reduction in the other direction. Let $(u_n)_{n=0}^\infty$ be a 1-LRS that satisfies a relation

$$u_n = a_{k-1}u_{n-1} + \cdots + a_1 u_{n-k+1} + a_0 u_{n-k},$$

where $a_0 \neq 0$. Let A, B and C be the following matrices of size $k \times k$:

$$A = \begin{pmatrix} u_{k-1} & \cdots & u_1 & u_0 \\ 0 & \cdots & 0 & 0 \\ 0 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & 0 \end{pmatrix}, \; B = \begin{pmatrix} a_{k-1} & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_2 & 0 & \cdots & 1 & 0 \\ a_1 & 0 & \cdots & 0 & 1 \\ a_0 & 0 & \cdots & 0 & 0 \end{pmatrix}, \; C = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}.$$

A straightforward computation shows that the product $A^m B^n C^\ell$ is equal to a matrix where all entries equal zero except for the entry in the upper-right corner which is equal to $u_{k-1}^{m-1} u_n$. So, if $u_{k-1} \neq 0$, then we have the following implications: (1) if $A^m B^n C^\ell = \mathbf{O}_{k,k}$ for some $m, n, \ell \in \mathbb{N}$ with $m, \ell \geq 1$, then $u_n = 0$; and (2) if $u_n = 0$, then the equation $A^m B^n C^\ell = \mathbf{O}_{k,k}$ holds for any $m, \ell \geq 1$.

The general case can be reduced to the case when $u_{k-1} \neq 0$ by shifting the original sequence by at most k positions. In other words, instead of $(u_n)_{n=0}^\infty$ we can consider a sequence $(u_{n+t})_{n=0}^\infty$ for some $0 < t < k$. It can be seen that a 1-LRS of depth k is identically zero if and only if it contains k consecutive zeros. Hence if $(u_n)_{n=0}^\infty$ is not identically zero, then we can find $t < k$ such that the sequence $(u_{n+t})_{n=0}^\infty$ satisfies the condition that $u_{k-1+t} \neq 0$. □

Corollary 18. *The set of triples (m, n, ℓ) that satisfy an equation $A^m B^n C^\ell = \mathbf{O}_{k,k}$ is equal to a finite union of direct products of semilinear sets.*

Proof. The corollary follows from Equation (5) above that describes all triples (m, n, ℓ) that satisfy the equation $A^m B^n C^\ell = \mathbf{O}_{k,k}$. By construction and the Skolem-Mahler-Lech theorem, the sets Z_1, $Z_2(m, \ell)$, $Z_3(\ell)$ and $Z_4(m)$ are semilinear. In Equation (5) we take direct product of these sets either with singleton sets or with sets of the form $\mathbb{N}_k = \{n \in \mathbb{N} : n \geq k\}$, which are also semilinear sets, and then take a finite union of such products. In other words, Equation (5) can be rewritten as follows

$$\mathbb{N}_k \times Z_1 \times \mathbb{N}_k \bigcup \bigcup_{m,\ell<k} \{m\} \times Z_2(m, \ell) \times \{\ell\} \bigcup$$
$$\bigcup_{\ell<k} \mathbb{N}_k \times Z_3(\ell) \times \{\ell\} \bigcup \bigcup_{m<k} \{m\} \times Z_4(m) \times \mathbb{N}_k.$$

The main corollary of Theorem 17 is the following result. □

Corollary 19. *The ABC-Z problem is decidable for 3×3 matrices over algebraic numbers and for 4×4 matrices over real algebraic numbers.*

Proof. By Theorem 17, the ABC-Z problem for 3×3 matrices over $\mathbf{A}$ is equivalent to the Skolem problem of depth 3 over $\mathbf{A}$, and the ABC-Z problem 4×4 matrices over $\mathbf{A}_\mathbb{R}$ is equivalent to the Skolem problem of depth 4 over $\mathbf{A}_\mathbb{R}$. Now the corollary follows from the fact that the Skolem problem is decidable for linear recurrence sequences of depth 3 over $\mathbf{A}$ and of depth 4 over $\mathbf{A}_\mathbb{R}$ [48, 35]. □

The next theorem is a generalisation of Theorem 17 to an arbitrary number of matrices.

Theorem 20. *Let $\mathcal{F}$ be the ring of integers $\mathbb{Z}$ or one of the fields $\mathbb{Q}$, $\mathbf{A}$ or $\mathbf{A}_{\mathbb{R}}$. Then the mortality problem for bounded languages (Problem 14) over $\mathcal{F}$ for $t+2$ matrices is reducible to the following problem: given matrices $A_1, \ldots, A_t$ from $\mathcal{F}^{k\times k}$ and vectors $\mathbf{u}_i$, $\mathbf{v}_i$ from $\mathcal{F}^k$, where $i = 1, \ldots, r$,do there exists $m_1, \ldots, m_t \in \mathbb{N}$ such that $s^i_{m_1,\ldots,m_t} = 0$ for all $i = 1, \ldots, r$, where*

$$s^i_{m_1,\ldots,m_t} = \mathbf{u}_i^\top A_1^{m_1} \ldots A_t^{m_t} \mathbf{v}_i.$$

Proof. Consider an instance of the mortality problem for bounded languages with $t+2$ matrices

$$A_0^{m_0} A_1^{m_1} \cdots A_t^{m_t} A_{t+1}^{m_{t+1}} = \mathbf{O}_{k,k}.$$

The proof of the reduction is similar to the proof of Theorem 17 for the equation $A^m B^n C^\ell = \mathbf{O}_{k,k}$. However note that in Theorem 17 we proved a stronger result in the sense that in Equation (5) we gave a description of all the triples (m, n, ℓ) that satisfy $A^m B^n C^\ell = \mathbf{O}_{k,k}$. If we simply want to know whether there *exists* one such triple, then we only need to consider Case 1 from the proof of Theorem 17, because if the equation $A^m B^n C^\ell = \mathbf{O}_{k,k}$ has a solution, then it has one in which $m \geq k$ and $\ell \geq k$.

So, we replicate the proof of Case 1 where in place of matrices A and C we consider A_0 and A_{t+1}. By doing this we obtain a system of equations similar to Equation (3), where in place of B^n we will have the product $A_1^{m_1} \cdots A_t^{m_t}$. This gives us the desired reduction.

The key difference between this theorem and Theorem 17 is that for $t = 1$ the system of equations (3) for 1-LRSs s^i_n can be reduced to the Skolem problem using Theorem 11 and the Skolem-Mahler-Lech theorem (Theorem 9). For $t > 1$, the solution set of the equation

$$\mathbf{u}^\top A_1^{m_1} \cdots A_t^{m_t} \mathbf{v} = 0$$

is not semilinear (see, e.g., Proposition 28), and we do not have an analog of Theorem 11 or the Skolem-Mahler-Lech theorem in this case. So, we cannot solve a system of such equations using an oracle for a single equation of this form. □

5. The ABCD-Z problem in dimension two

Recall that the ABCD-Z problem in dimension two asks whether there exist natural numbers $k, m, n, \ell \in \mathbb{N}$ such that

$$A^k B^m C^n D^\ell = \mathbf{O}_{2,2}. \tag{6}$$

In this section we will show that this problem is decidable for 2×2 upper-triangular matrices with rational coefficients. In the proof we will use the following simple lemmas which show how to diagonalise and compute powers of an upper-triangular 2×2 matrix.

Lemma 21. *Consider an upper triangular matrix* $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ *such that* $a \neq c$. *Then*

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} 1 & -\frac{b}{a-c} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \begin{pmatrix} 1 & \frac{b}{a-c} \\ 0 & 1 \end{pmatrix}.$$

Lemma 22. *Consider matrices of the form* $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ *and* $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$, *such that* $a \neq c$, *and any* $k \in \mathbb{N}$. *Then we see that*

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}^k = \begin{pmatrix} a^k & b\dfrac{a^k - c^k}{a - c} \\ 0 & c^k \end{pmatrix} \text{ and } \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}^k = \begin{pmatrix} a^k & kba^{k-1} \\ 0 & a^k \end{pmatrix}.$$

Theorem 23. *The ABCD-Z problem is decidable for* 2×2 *upper-triangular matrices over rational numbers.*

Proof. First, note that if one of the matrices A, B, C or D is nilpotent, then Equation (6) obviously has a solution. So from now on we assume that none of A, B, C or D is nilpotent. Furthermore, if A or D is invertible, then the ABCD-Z problem reduces to the ABC-Z problem for rational matrices of dimension two that is decidable by Theorem 17. So, without loss of generality, we will assume that both A and D are singular matrices.

Now suppose we are given an instance of the ABCD-Z problem which satisfies the above-mentioned requirements. We will show that if Equation (6) has a solution, then it has a solution with $k = \ell = 1$. Indeed, assume Equation (6) has a solution, and let (k, m, n, ℓ) be a solution of minimal length, where the length of a solution is the sum $k+m+n+\ell$. Using Theorem 17 we can exclude the case when $k = 0$ or $\ell = 0$ since in this case our problem is just an instance of the ABC-Z for 2×2 matrices. So we will assume that in the above solution $k, \ell \geq 1$.

By the Frobenius rank inequality (Theorem 1), we have that:

$$\mathsf{Rk}(A^k B^m C^n D^{\ell-1}) + \mathsf{Rk}(A^{k-1} B^m C^n D^{\ell}) \leq \mathsf{Rk}(A^{k-1} B^m C^n D^{\ell-1}).$$

This follows since $\mathsf{Rk}(A^k B^m C^n D^{\ell}) = \mathsf{Rk}(\mathbf{O}_{2,2}) = 0$. In the above inequality, notice that neither $A^k B^m C^n D^{\ell-1}$ nor $A^{k-1} B^m C^n D^{\ell}$ is the zero matrix by the assumption that the solution has minimal length. Hence the ranks of the matrices on the left hand side are at least 1. Therefore, $\mathsf{Rk}(A^{k-1} B^m C^n D^{\ell-1}) = 2$. Since we assumed that A and D are singular, it is necessary that $k = \ell = 1$. Also notice that if $\mathsf{Rk}(B) = 1$ or $\mathsf{Rk}(C) = 1$, then we must have $m = 0$ or $n = 0$, respectively. Again these cases can be excluded by Theorem 17.

Thus, using the Frobenius rank inequality and the assumption that the solution is of minimal length, we reduced the ABCD-Z problem to an equation of the form:

$$AB^m C^n D = \mathbf{O}_{2,2},$$

where $\mathsf{Rk}(A) = \mathsf{Rk}(D) = 1$ and $\mathsf{Rk}(B) = \mathsf{Rk}(C) = 2$.

We assumed that A and D have rank one but are not nilpotent. This means that they have one zero and one nonzero element on the diagonal, in particular, they satisfy the condition of Lemma 21. Hence we can find invertible rational matrices S_A and S_D such that

$$A = S_A^{-1} \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} S_A \quad \text{and} \quad D = S_D^{-1} \begin{pmatrix} d & 0 \\ 0 & 0 \end{pmatrix} S_D,$$

where a, d are nonzero rational numbers. Applying Lemma 15 with matrix $S_A B^m C^n S_D^{-1}$ in place of B, we conclude that $AB^mC^nD = \mathbf{O}_{2,2}$ holds if and only if the $(1,1)$-entry of $S_A B^m C^n S_D^{-1}$ equals zero. In other words, the equation $AB^mC^nD = \mathbf{O}_{2,2}$ is equivalent to $s_{m,n} = \mathbf{u}^\top B^m C^n \mathbf{v} = 0$, where $\mathbf{u}^\top = \mathbf{e}_1^\top S_A$ and $\mathbf{v} = S_D^{-1}\mathbf{e}_1$ are vectors with rational coefficients.

We will consider three cases: (1) both B and C have distinct eigenvalues, (2) both B and C have a single eigenvalue of multiplicity 2 and (3) one matrix has distinct eigenvalues and the other has a single eigenvalue of multiplicity 2.

Case (1): B and C have distinct eigenvalues, that is, $B = \begin{pmatrix} b_1 & b_3 \\ 0 & b_2 \end{pmatrix}$ and $C = \begin{pmatrix} c_1 & c_3 \\ 0 & c_2 \end{pmatrix}$, where $b_1 \neq b_2$ and $c_1 \neq c_2$. By Lemma 22 we have

$$B^m = \begin{pmatrix} b_1^m & b_3 \dfrac{b_1^m - b_2^m}{b_1 - b_2} \\ 0 & b_2^m \end{pmatrix} \quad \text{and} \quad C^n = \begin{pmatrix} c_1^n & c_3 \dfrac{c_1^n - c_2^n}{c_1 - c_2} \\ 0 & c_2^n \end{pmatrix}$$

Multiplying these matrices we obtain:

$$\begin{aligned} B^m C^n &= \begin{pmatrix} b_1^m & b_3 \dfrac{b_1^m - b_2^m}{b_1 - b_2} \\ 0 & b_2^m \end{pmatrix} \begin{pmatrix} c_1^n & c_3 \dfrac{c_1^n - c_2^n}{c_1 - c_2} \\ 0 & c_2^n \end{pmatrix} \\ &= \begin{pmatrix} b_1^m c_1^n & b_3 \dfrac{b_1^m c_2^n - b_2^m c_2^n}{b_1 - b_2} + c_3 \dfrac{b_1^m c_1^n - b_1^m c_2^n}{c_1 - c_2} \\ 0 & b_2^m c_2^n \end{pmatrix} \end{aligned}$$

From this formula one can see that the entries of B^mC^n are linear combinations of $b_1^m c_1^n$, $b_1^m c_2^n$ and $b_2^m c_2^n$ with rational coefficients. Notice that the term $b_2^m c_1^n$ does not appear in the entries of B^mC^n. Since $\mathbf{u}$ and $\mathbf{v}$ are rational vectors we conclude that

$$s_{m,n} = \mathbf{u}^\top B^m C^n \mathbf{v} = \alpha b_1^m c_1^n + \beta b_1^m c_2^n + \gamma b_2^m c_2^n,$$

where $\alpha, \beta, \gamma \in \mathbb{Q}$. Multiplying the equation $s_{m,n} = \alpha b_1^m c_1^n + \beta b_1^m c_2^n + \gamma b_2^m c_2^n = 0$ by the product of denominators of α, β, γ and b_1, b_2, c_1, c_2 we can rewrite it in the following form

$$as^m r^n + bs^m t^n + cq^m t^n = 0$$

where a, b, c, q, r, s, t are integers and a, b, c are relatively prime. Recall that we want to find out if there exist $m, n \in \mathbb{N}$ that satisfy the above exponential

Diophantine equation. If one of the coefficients a, b, c is zero, then this problem is easy to solve. For instance, if $b = 0$ then the above equation is equivalent to $as^m r^n = -cq^m t^n$. This equality holds if and only if $as^m r^n$ and $-cq^m t^n$ have the same sign and $v_p(as^m r^n) = v_p(-cq^m t^n)$ for every prime divisor p of a, c, s, r, q or t. Each of these conditions can be expressed as a linear Diophantine equation. For instance, the sign of $as^m r^n$ or $-cq^m t^n$ depends on the parity of m and n. So, the requirement that $as^m r^n$ and $-cq^m t^n$ have the same sign can be written as a linear congruence equation in m and n modulo 2, which in turn can be expressed as a linear Diophantine equation. Since a system of linear Diophantine equations can be effectively solved, we can find out whether there exist m and n that satisfy $as^m r^n = -cq^m t^n$.

Now suppose that a, b, c are relatively prime nonzero integers. Let T be all primes that appear in s, r, q or t. Theorem 5 gives an upper bound on nonzero relatively prime integers x, y, z that are composed of the primes from T and satisfy the equation $ax + by + cz = 0$. Therefore, we can algorithmically compute the following set

$$\mathcal{U} = \{(x, y, z) \ : \ ax + by + cz = 0, \ x, y, z \neq 0 \text{ and } \gcd(x, y, z) = 1\}.$$

Next for each triple $(x, y, z) \in \mathcal{U}$ we want to find out if there exist $m, n \in \mathbb{N}$ such that

$$(s^m r^n, s^m t^n, q^m t^n) = (xg, yg, zg) \tag{7}$$

for some $g \in \mathbb{N}$ that is composed of the primes from T. It can be seen that Equation (7) holds if and only if for every $p \in T$

$$v_p(s^m r^n) - v_p(x) = v_p(s^m t^n) - v_p(y) = v_p(q^m t^n) - v_p(z)$$

and $s^m r^n, s^m t^n, q^m t^n$ have the same signs as x, y, z, respectively. Since these conditions can be expressed as a system of linear Diophantine equations, we can algorithmically find if there are $m, n \in \mathbb{N}$ that satisfy Equation (7). If such m and n exist for at least one triple $(x, y, z) \in \mathcal{U}$, then the original equation $s_{m,n} = 0$ has a solution. Otherwise, the equation $s_{m,n} = 0$ does not have a solution.

Case (2): both B and C have a single eigenvalue of multiplicity 2, that is, $B = \begin{pmatrix} b_1 & b_2 \\ 0 & b_1 \end{pmatrix}$ and $C = \begin{pmatrix} c_1 & c_2 \\ 0 & c_1 \end{pmatrix}$. By Lemma 22 we have

$$B^m = \begin{pmatrix} b_1^m & m b_2 b_1^{m-1} \\ 0 & b_1^m \end{pmatrix} \quad \text{and} \quad C^n = \begin{pmatrix} c_1^n & n c_2 c_1^{n-1} \\ 0 & c_1^n \end{pmatrix}.$$

Multiplying these matrices we obtain:

$$B^m C^n = \begin{pmatrix} b_1^m & m b_2 b_1^{m-1} \\ 0 & b_1^m \end{pmatrix} \begin{pmatrix} c_1^n & n c_2 c_1^{n-1} \\ 0 & c_1^n \end{pmatrix} = \begin{pmatrix} b_1^m c_1^n & m b_2 b_1^{m-1} c_1^n + n c_2 b_1^m c_1^{n-1} \\ 0 & b_1^m c_1^n \end{pmatrix}.$$

Note that the entries of $B^m C^n$ are equal to linear combinations of $b_1^m c_1^n$, $m b_1^{m-1} c_1^n$ and $n b_1^m c_1^{n-1}$ with rational coefficients. Therefore,

$$s_{m,n} = \mathbf{u}^\top B^m C^n \mathbf{v} = \alpha b_1^m c_1^n + \beta m b_1^{m-1} c_1^n + \gamma n b_1^m c_1^{n-1} = b_1^{m-1} c_1^{n-1} (\alpha b_1 c_1 + m \beta c_1 + n \gamma b_1)$$

where $\alpha, \beta, \gamma \in \mathbb{Q}$. Hence $s_{m,n} = 0$ is equivalent to the linear Diophantine equation

$$\alpha b_1 c_1 + m\beta c_1 + n\gamma b_1 = 0,$$

which can be easily solved.

Case (3): one matrix has distinct eigenvalues and the other has a single eigenvalue of multiplicity 2. We consider only the case when B has distinct eigenvalues and C has a single eigenvalue because the other case is similar.

Suppose $B = \begin{pmatrix} b_1 & b_3 \\ 0 & b_2 \end{pmatrix}$, where $b_1 \neq b_2$, and $C = \begin{pmatrix} c_1 & c_2 \\ 0 & c_1 \end{pmatrix}$. By Lemma 22 we have

$$B^m = \begin{pmatrix} b_1^m & b_3 \dfrac{b_1^m - b_2^m}{b_1 - b_2} \\ 0 & b_2^m \end{pmatrix} \quad \text{and} \quad C^n = \begin{pmatrix} c_1^n & nc_2c_1^{n-1} \\ 0 & c_1^n \end{pmatrix}.$$

Multiplying these matrices we obtain:

$$\begin{aligned} B^m C^n &= \begin{pmatrix} b_1^m & b_3 \dfrac{b_1^m - b_2^m}{b_1 - b_2} \\ 0 & b_2^m \end{pmatrix} \begin{pmatrix} c_1^n & nc_2c_1^{n-1} \\ 0 & c_1^n \end{pmatrix} \\ &= \begin{pmatrix} b_1^m c_1^n & b_3 \dfrac{b_1^m c_1^n - b_2^m c_1^n}{b_1 - b_2} + nc_2 b_1^m c_1^{n-1} \\ 0 & b_2^m c_1^n \end{pmatrix}. \end{aligned}$$

Note that the entries of $B^m C^n$ are equal to linear combinations of $b_1^m c_1^n$, $b_2^m c_1^n$ and $nb_1^m c_1^{n-1}$ with rational coefficients. Therefore,

$$s_{m,n} = \mathbf{u}^\top B^m C^n \mathbf{v} = \alpha b_1^m c_1^n + \beta b_2^m c_1^n + \gamma n b_1^m c_1^{n-1} = b_1^m c_1^{n-1}(\alpha c_1 + \beta c_1 \Big(\frac{b_2}{b_1}\Big)^m + \gamma n)$$

where $\alpha, \beta, \gamma \in \mathbb{Q}$. Hence $s_{m,n} = 0$ is equivalent to

$$\alpha c_1 + \beta c_1 \Big(\frac{b_2}{b_1}\Big)^m + \gamma n = 0.$$

If $\beta = 0$ then the solution is trivial. If $\beta \neq 0$, then after multiplying the above equation by the product of denominators of α, β, γ and c_1 we can rewrite it as

$$c\frac{s^m}{t^m} = a + bn,$$

where $a, b, c, s, t \in \mathbb{Z}$, $t > 0$, $\gcd(s, t) = 1$ and $\dfrac{s}{t} = \dfrac{b_2}{b_1}$. If $t > 1$, then it is not hard to see that the left hand side can be integer only for finitely many values of m, which can be effectively found, and for each of these values of m one can check if there exists corresponding $n \in \mathbb{N}$. If $t = 1$, then the above equation reduces to

$$cs^m \equiv a \pmod{b}.$$

This equation can also be algorithmically solved. For instance, one can start computing the values $cs^m \pmod b$ for $m = 0, 1, 2, \ldots$. Since there are only $b-1$ different residues modulo b, this sequence will be eventually periodic, and so we can decide whether $cs^m \pmod b$ is equal to $a \pmod b$ for some m and in fact find all such m. □

Remark 24. *Regarding the previous proof, it is interesting to note that in Cases (1) and (2) the solutions (m, n) of the equation $s_{m,n} = 0$ are described by linear Diophantine equations, and only in Case (3) we have a linear-exponential equation. This agrees with an example from Proposition 28, in which matrix A has a single eigenvalue 1 of multiplicity 2 and matrix B has distinct eigenvalues 1 and 2.*

Remark 25. *In the above argument we used Theorem 5 to obtain a bound on the solutions of the equation $as^m r^n + bs^m t^n + cq^m t^n = 0$, which is a special type of an S-unit equation. This leaves open an interesting question of whether any S-unit equation can be encoded into the ABCD-Z problem.*

The obvious question is how hard would it be to solve n-LRSs, or in general multiplicative matrix equations, in low dimensions. In fact we can show that the Skolem problem for n-LRSs of depth 2 is NP-hard. It is not direct but an easy corollary following the hardness proof of the mortality problem for 2×2 matrices [5].

Theorem 26 ([5])**.** *The mortality problem for integer matrices of dimension two is NP-hard.*

Corollary 27. *Determining if the zero set of an n-LRS of depth 2 is empty is NP-hard.*

Proof. A minor adaptation of a proof technique from [5] is required in order to prove this result, which we sketch here for completion.

Let $P = \{p_1, p_2, \ldots, p_k\} \subseteq \mathbb{N}$ and $x \in \mathbb{N}$ denote an instance of the subset sum problem; thus it is NP-hard to determine if there exists a subset $P' \subseteq P$ such that $\sum_{j \in P'} j = x$.

Let $\Sigma = \{1, 2, \ldots, 2k+2, a, b\}$ denote an alphabet forming a free group (i.e., with no non-trivial identities). We form a set of words W over Σ as follows:

$$
W = \begin{array}{ll}
\{1a^{p_1}2^{-1}, & 1 \cdot 2^{-1}, \\
2a^{p_2}3^{-1}, & 2 \cdot 3^{-1}, \\
\vdots & \vdots \\
ka^{p_k}(k+1)^{-1}, & k(k+1)^{-1}, \\
(k+1)a^{-x}(k+2)^{-1}, & \\
(k+2)b^{p_1}(k+3)^{-1}, & (k+2)(k+3)^{-1}, \\
(k+3)b^{p_2}(k+4)^{-1}, & (k+3)(k+4)^{-1}, \\
\vdots & \vdots \\
(2k+1)b^{p_k}(2k+2)^{-1}, & (2k+1)(2k+2)^{-1}, \\
(2k+2)b^{-x}1^{-1}\} \subseteq \Sigma^* &
\end{array}
$$

In [5], a morphism $\varphi : W^* \to \mathbb{Z}^{2\times 2}$ is given such that for any $w = w_1 w_2 \cdots w_j \in W^j$ then the matrix $\varphi(w)$ has a representation of size polynomial in j and the largest element of P (Lemma 7 of [5]), and for every $X \in \{\varphi(w_j)|w_j \in \Sigma^*\}$ then $X_{1,2} \neq 0$ unless $X = I_2$, i.e., the only element with a top right element which is 0 is the 2×2 identity matrix. Further, it was shown that $I_2 \in W^+$ if and only if the instance of the subset sum problem P has a solution. This can be readily seen from the structure of W, where the only way to cancel the 'border letters' of the form i or i^{-1} on the left and right of each word, is if a product sequentially uses exactly one word from each row with each row selected once.

In such a product, the border letters and a and b letters will cancel if and only if there exists a subset $P' \subseteq P$ such that

$$a^{\sum_{j\in P'} j} a^{-x} = b^{\sum_{j\in P'} j} b^{-x} = \varepsilon.$$

Let $\mathbf{u} = (1,0)^T$ and $\mathbf{v} = (0,1)^T$, and then if there exists some

$$M \in \varphi(w_1)^{j_1}\varphi(w_2)^{j_2}\cdots\varphi(w_{4k+2})^{j_{4k+2}} \quad | \quad j_1, j_2, \ldots, j_{4k+2} \geq 0$$

such that $M_{1,2} = 0$, then $\mathbf{u}^\top M \mathbf{v} = 0$ (by construction each $j_i \in \{0,1\}$). Since only the identity matrix has an upper-right element equal to 0 in $\langle\{\varphi(w_i)|w_i \in W\}\rangle$, and the representation size of $\varphi(w_1)^{j_1}\varphi(w_2)^{j_2}\cdots\varphi(w_{4k+2})^{j_{4k+2}}$ is polynomial in the representation size of P, then it is NP-hard to determine if there exists a 0 for this n-LRS (where $n = 4k+2$).

In fact we can reduce the size of the LRS as we now outline. In [5] it was necessary to encode the instance P 'twice', once using letters 'a' and once using letters 'b' (corresponding to the first $2k+1$ and last $2k+1$ elements of W respectively). This was for a technical reason since we formed a semigroup of matrices $\langle\{\varphi(w_1), \ldots, \varphi(w_{4k+2})\}\rangle$ with no implied ordering on the sequence of matrices in any product. When defining an n-LRS however, we have a strict ordering of the matrices and therefore determining whether the following $(2k+1)$-LRS has a zero is NP-hard:

$$\mathbf{u}^\top \varphi(w_1)^{j_1}\varphi(w_2)^{j_2}\cdots\varphi(w_{2k+1})\mathbf{v},$$

where we redefine $w_{2k+1} = (k+1)a^{-x}1^{-1}$ rather than $(k+1)a^{-x}(k+2)^{-1}$. □

Another interesting observation is that the zero set of a 2-LRS is not necessarily semilinear, in contrast to the situation for 1-LRSs, which indicates that the Skolem problem for 2-LRSs is likely to be significantly harder than the Skolem problem for 1-LRSs even for sequences of small depth.

Proposition 28. *There exists a 2-LRS of depth 2 for which the zero set is not semilinear.*

Proof. Let $u = (0,1)^T, v = (1,-1)^T$, $A = \begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}$ and $B = \begin{pmatrix}1 & 0\\ 0 & 2\end{pmatrix}$. Define

$$s_{n,m} = u^T A^n B^m v = (0,1)\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}^n \begin{pmatrix}1 & 0\\ 0 & 2\end{pmatrix}^m \begin{pmatrix}1\\ -1\end{pmatrix} = n - 2^m.$$

Then $s_{n,m} = 0$ if and only if $n = 2^m$. Clearly, the zero set is not semilinear. □

6. Acknowledgements

We thank Prof. James Worrell for useful discussions, particularly related to S-unit equations. We also thank the referees for their helpful comments and suggestions.

References

[1] L. Babai, R. Beals, J.-Y. Cai, G. Ivanyos, and E. M. Luks. Multiplicative equations over commuting matrices. In *Proc. of the Seventh Annual ACM-SIAM Symposium on Discrete Algorithms (SODA'96)*, pages 498–507. Society for Industrial and Applied Mathematics, 1996.

[2] C. Baier, S. Kiefer, J. Klein, S. Klüppelholz, D. Müller, and J. Worrell. Markov chains and unambiguous Büchi automata. In *Computer Aided Verification (CAV'16)*, volume 9779 of *LNCS*, pages 23–42. Springer, 2016.

[3] S. Basu, R. Pollack, and M.-F. Roy. *Algorithms in real algebraic geometry*, volume 10 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, second edition, 2006.

[4] P. C. Bell, V. Halava, T. Harju, J. Karhumäki, and I. Potapov. Matrix equations and Hilbert's tenth problem. *International Journal of Algebra and Computation*, 18:1231–1241, 2008.

[5] P. C. Bell, M. Hirvensalo, and I. Potapov. Mortality for 2×2 matrices is NP-hard. In *Mathematical Foundations of Computer Science (MFCS'12)*, volume 7464 of *LNCS*, pages 148–159. Springer, 2012.

[6] P. C. Bell, M. Hirvensalo, and I. Potapov. The identity problem for matrix semigroups in $\mathrm{SL}_2(\mathbb{Z})$ is NP-complete. In *Proceedings of the Annual ACM-SIAM Symposium on Discrete Algorithms (SODA'17)*, pages 187–206. Society for Industrial and Applied Mathematics, 2017.

[7] V. Blondel, E. Jeandel, P. Koiran, and N. Portier. Decidable and undecidable problems about quantum automata. *SIAM Journal on Computing*, 34:6:1464–1473, 2005.

[8] V. D. Blondel, O. Bournez, P. Koiran, C. Papadimitriou, and J. N. Tsitsiklis. Deciding stability and mortality of piecewise affine dynamical systems. *Theoretical Computer Science*, 255(1-2):687–696, 2001.

[9] V. D. Blondel and N. Portier. The presence of a zero in an integer linear recurrent sequence is NP-hard to decide. *Linear Algebra and its Applications*, 351-352:91–98, 2002.

[10] V. D. Blondel and J. N. Tsitsiklis. Complexity of stability and controllability of elementary hybrid systems. *Automatica*, 35:479–489, 1999.

[11] J.-Y. Cai, W. H. J. Fuchs, D. Kozen, and Z. Liu. Efficient average-case algorithms for the modular group. In *35th Annual Symposium on Foundations of Computer Science (FOCS'94)*, pages 143–152. IEEE, 1994.

[12] J.-Y. Cai, R. J. Lipton, and Y. Zalcstein. The complexity of the membership problem for 2-generated commutative semigroups of rational matrices. In *35th Annual Symposium on Foundations of Computer Science (FOCS'94)*, pages 135–142. IEEE, 1994.

[13] J. Cassaigne, V. Halava, T. Harju, and F. Nicolas. Tighter undecidability bounds for matrix mortality, zero-in-the-corner problems, and more. *CoRR*, abs/1404.0644, 2014.

[14] V. Chonev, J. Ouaknine, and J. Worrell. On the complexity of the orbit problem. *Journal of the ACM*, 63(3):1–18, 2016.

[15] V. Chonev, J. Ouaknine, and J. Worrell. On the Skolem problem for continuous linear dynamical systems. In *43rd International Colloquium on Automata, Languages, and Programming, (ICALP'16)*, volume 55 of *Leibniz International Proceedings in Informatics*, pages 100:1–100:13. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2016.

[16] H. Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[17] J.-H. Evertse, K. Győry, C. L. Stewart, and R. Tijdeman. S-unit equations and their applications. In *New advances in transcendence theory (Durham, 1986)*, pages 110–174. Cambridge Univ. Press, Cambridge, 1988.

[18] E. Galby, J. Ouaknine, and J. Worrell. On matrix powering in low dimensions. In *32nd International Symposium on Theoretical Aspects of Computer Science (STACS'15)*, volume 30 of *Leibniz International Proceedings in Informatics*, pages 329–340. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2015.

[19] K. Győry. On the *abc* conjecture in algebraic number fields. *Acta Arithmetica*, 133(3):281–295, 2008.

[20] V. Halava, T. Harju, M. Hirvensalo, and J. Karhumäki. Skolem's problem - on the border between decidability and undecidability. In *TUCS Technical Report Number 683*, 2005.

[21] G. Hansel. Une démonstration simple du théorème de Skolem-Mahler-Lech. *Theoretical Computer Science*, 43(1):91–98, 1986.

[22] M. A. Harrison. *Lectures on linear sequential machines*. Academic Press, Inc., Orlando, FL, USA, 1969.

[23] K. Hoffman and R. Kunze. *Linear algebra*. Second edition. Prentice-Hall, Inc., Englewood Cliffs, N.J., 1971.

[24] J. Honkala. Products of matrices and recursively enumerable sets. *Journal of Computer and System Sciences*, 81(2):468–472, 2015.

[25] R. Horn and C. Johnson. *Matrix Analysis*. Cambridge University Press, 1990.

[26] R. Kannan and R. J. Lipton. The orbit problem is decidable. In *Proceedings of the Twelfth Annual ACM Symposium on Theory of Computing (STOC'80)*, pages 252–261. Association for Computing Machinery, 1980.

[27] J.-Y. Kao, N. Rampersad, and J. Shallit. On NFAs where all states are final, initial, or both. *Theoretical Computer Science*, 410(47-49):5010–5021, 2009.

[28] S.-K. Ko, R. Niskanen, and I. Potapov. On the identity problem for the special linear group and the Heisenberg group. In *45th International Colloquium on Automata, Languages, and Programming, (ICALP'18)*, volume 107 of *Leibniz International Proceedings in Informatics*, pages 132:1–132:15. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2018.

[29] D. König, M. Lohrey, and G. Zetzsche. Knapsack and subset sum problems in nilpotent, polycyclic, and co-context-free groups. *CoRR*, abs/1507.05145, 2015. URL: `http://arxiv.org/abs/1507.05145`, `arXiv:1507.05145`.

[30] C. Lech. A note on recurring series. *Arkiv för Matematik*, 2(5):417–421, 1953.

[31] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261(4):515–534, 1982.

[32] A. Lisitsa and I. Potapov. Membership and reachability problems for row-monomial transformations. In *Mathematical Foundations of Computer Science 2004*, volume 3153 of *LNCS*, pages 623–634. Springer Berlin Heidelberg, 2004.

[33] M. Lohrey. Rational subsets of unitriangular groups. *International Journal of Algebra and Computation*, 25(1-2):113–122, 2015.

[34] K. Mahler. Eine arithmetische Eigenschaft der Taylor-Koeffizienten rationaler Funktionen. In *Akad. Wet. Amsterdam*, volume 38, pages 50–60. Noord-Hollandsche Uitgevers Mij, 1935.

[35] M. Mignotte, T. N. Shorey, and R. Tijdeman. The distance between terms of an algebraic recurrence sequence. *Journal für die reine und angewandte Mathematik*, 349:63–76, 1984.

[36] C. Nuccio and E. Rodaro. Mortality problem for 2×2 integer matrices. In *34th Conference on Current Trends in Theory and Practice of Computer Science (SOFSEM'08)*, volume 4910 of *LNCS*, pages 400–405. Springer, 2008.

[37] J. Ouaknine, J. Sousa Pinto, and J. Worrell. On termination of integer linear loops. In *Proceedings of the Twenty-Sixth Annual ACM-SIAM Symposium on Discrete Algorithms (SODA'15)*, pages 957–969. Society for Industrial and Applied Mathematics, 2015.

[38] J. Ouaknine, A. Pouly, J. Sousa Pinto, and J. Worrell. Solvability of matrix-exponential equations. In *Proceedings of the 31st Annual ACM/IEEE Symposium on Logic in Computer Science (LICS'16)*, pages 798–806. Association for Computing Machinery, 2016.

[39] J. Ouaknine and J. Worrell. Decision problems for linear recurrence sequences. In *Reachability Problems - 6th International Workshop, (RP'12)*, volume 7550 of *LNCS*, pages 21–28. Springer, 2012.

[40] J. Ouaknine and J. Worrell. On the positivity problem for simple linear recurrence sequences,. In *Automata, Languages, and Programming - 41st International Colloquium, (ICALP'14)*, volume 8573 of *LNCS*, pages 318–329. Springer, 2014.

[41] J. Ouaknine and J. Worrell. Positivity problems for low-order linear recurrence sequences. In *Proceedings of the Twenty-Fifth Annual ACM-SIAM Symposium on Discrete Algorithms, (SODA'14)*, pages 366–379. Society for Industrial and Applied Mathematics, 2014.

[42] V. Y. Pan. Optimal and nearly optimal algorithms for approximating polynomial zeros. *Computers & Mathematics with Applications*, 31(12):97–138, 1996.

[43] M. S. Paterson. Unsolvability in 3×3 matrices. *Studies in Applied Mathematics*, 49(1):105–107, 1970.

[44] J. R. Pinkert. An exact method for finding the roots of a complex polynomial. *ACM Transactions on Mathematical Software*, 2(4):351–363, 1976.

[45] I. Potapov and P. Semukhin. Decidability of the membership problem for 2×2 integer matrices. In *Proceedings of the Twenty-Eighth Annual ACM-SIAM Symposium on Discrete Algorithms, (SODA'17)*, pages 170–186. Society for Industrial and Applied Mathematics, 2017.

[46] I. Potapov and P. Semukhin. Membership problem in GL(2, Z) extended by singular matrices. In *42nd International Symposium on Mathematical Foundations of Computer Science, (MFCS'17)*, volume 83 of *Leibniz International Proceedings in Informatics*, pages 44:1–44:13. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2017.

[47] T. Skolem. Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen und diophantischer Gleichungen. *Skand. Mat. Kongr.*, 8:163–188, 1934.

[48] N. K. Vereshchagin. The problem of the appearance of a zero in a linear recursive sequence. *Matematicheskie Zametki*, 347(2):609–615, 1985.