Mortality problem for bounded languages and linear recurrence sequences

Pavel Semukhin

joint work with P. Bell and I. Potapov

Department of Computer Science, University of Oxford

Reachability Problems, 25 September, 2018

Membership problem

Input: A finite collection of matrices $M_1, \ldots, M_n$ and M.

Membership problem

Input: A finite collection of matrices $M_1, \ldots, M_n$ and M.

Question: Does M belong to $\langle M_1, \ldots, M_n \rangle$, that is, does there exist a sequence of indices $i_1, \ldots, i_k \in \{1, \ldots, n\}$ such that

$$M = M_{i_1} M_{i_2} \cdots M_{i_k}?$$

Membership problem

Input: A finite collection of matrices $M_1, \ldots, M_n$ and M.

Question: Does M belong to $\langle M_1, \ldots, M_n \rangle$, that is, does there exist a sequence of indices $i_1, \ldots, i_k \in \{1, \ldots, n\}$ such that

$$M = M_{i_1} M_{i_2} \cdots M_{i_k}?$$

Mortality problem

Input: A finite collection of matrices $M_1, \ldots, M_n$.

Question: Does $\mathbf{O}$ belong to $\langle M_1, \ldots, M_n \rangle$?

Known results

- Mortality problem (and hence the membership problem) is algorithmically undecidable for 3×3 integer matrices. [Paterson, 1970]

Known results

- Mortality problem (and hence the membership problem) is algorithmically undecidable for 3×3 integer matrices. [Paterson, 1970]
- Membership problem is decidable in PTIME for commuting matrices (over algebraic numbers) [Babai, et al., 1996]

Known results

- Mortality problem (and hence the membership problem) is algorithmically undecidable for 3×3 integer matrices. [Paterson, 1970]
- Membership problem is decidable in PTIME for commuting matrices (over algebraic numbers) [Babai, et al., 1996]

It is a long standing open question whether the membership problem is decidable for 2×2 matrices (even over integers).

Known results

- The membership problem is decidable for 2×2 integer matrices with determinant ± 1.
  [C. Choffrut and J. Karhumäki, 2005]

Known results

- The membership problem is decidable for 2×2 integer matrices with determinant ± 1.
  [C. Choffrut and J. Karhumäki, 2005]
- The membership problem is decidable for 2×2 nonsingular integer matrices.
  [P. Semukhin and I. Potapov, 2017]

Known results

- The membership problem is decidable for 2×2 integer matrices with determinant ± 1.
  [C. Choffrut and J. Karhumäki, 2005]
- The membership problem is decidable for 2×2 nonsingular integer matrices.
  [P. Semukhin and I. Potapov, 2017]
- The membership problem is decidable for 2×2 integer matrices with determinant $0, \pm 1$.
  [P. Semukhin and I. Potapov, 2017]

Known results

- The membership problem is decidable for 2×2 integer matrices with determinant ± 1.
  [C. Choffrut and J. Karhumäki, 2005]

- The membership problem is decidable for 2×2 nonsingular integer matrices.
  [P. Semukhin and I. Potapov, 2017]

- The membership problem is decidable for 2×2 integer matrices with determinant $0, \pm 1$.
  [P. Semukhin and I. Potapov, 2017]

It is an open question whether the Membership or Mortality problem is decidable for all 2×2 integer matrices.

Mortality Problem for bounded languages

Given matrices $A_1, \ldots, A_n$, decide whether there exist $k_1, \ldots, k_n \in \mathbb{N}$ such that

$$A_1^{k_1} A_2^{k_2} \cdots A_n^{k_n} = \mathbf{O}$$

Mortality Problem for bounded languages

Given matrices $A_1, \ldots, A_n$, decide whether there exist $k_1, \ldots, k_n \in \mathbb{N}$ such that

$$A_1^{k_1} A_2^{k_2} \cdots A_n^{k_n} = \mathbf{O}$$

By an encoding of Hilbert's tenth problem, it was shown that there exist n and d such that the above problem is undecidable for n matrices of size $d \times d$ with integer coefficients.
[P. Bell, et al., 2008]

Linear Recurrence Sequences and Skolem's Problem

$(u_n)_{n=0}^{\infty}$ is called a linear recurrence sequence (LRS) of depth k if there exist constants $a_1, \ldots, a_k$ (with $a_k \neq 0$) such that for all $n \geq 0$

$$u_{n+k} = a_1 u_{n+k-1} + a_2 u_{n+k-2} + \cdots + a_k u_n$$

Linear Recurrence Sequences and Skolem's Problem

$(u_n)_{n=0}^{\infty}$ is called a linear recurrence sequence (LRS) of depth k if there exist constants $a_1, \ldots, a_k$ (with $a_k \neq 0$) such that for all $n \geq 0$

$$u_{n+k} = a_1 u_{n+k-1} + a_2 u_{n+k-2} + \cdots + a_k u_n$$

Fibonacci sequence

The sequence $0, 1, 1, 2, 3, 5, 8, 13, \ldots$ satisfies the recurrence relation $u_{n+2} = u_{n+1} + u_n$.

Linear Recurrence Sequences and Skolem's Problem

$(u_n)_{n=0}^{\infty}$ is called a linear recurrence sequence (LRS) of depth k if there exist constants $a_1, \ldots, a_k$ (with $a_k \neq 0$) such that for all $n \geq 0$

$$u_{n+k} = a_1 u_{n+k-1} + a_2 u_{n+k-2} + \cdots + a_k u_n$$

Fibonacci sequence

The sequence $0, 1, 1, 2, 3, 5, 8, 13, \ldots$ satisfies the recurrence relation $u_{n+2} = u_{n+1} + u_n$.

$\mathcal{Z}(u_n) = \{n \in \mathbb{N} \ : \ u_n = 0\}$ is called the zero set of $(u_n)_{n=0}^{\infty}$.

Linear Recurrence Sequences and Skolem's Problem

$(u_n)_{n=0}^{\infty}$ is called a linear recurrence sequence (LRS) of depth k if there exist constants $a_1, \ldots, a_k$ (with $a_k \neq 0$) such that for all $n \geq 0$

$$u_{n+k} = a_1 u_{n+k-1} + a_2 u_{n+k-2} + \cdots + a_k u_n$$

Fibonacci sequence

The sequence $0, 1, 1, 2, 3, 5, 8, 13, \ldots$ satisfies the recurrence relation $u_{n+2} = u_{n+1} + u_n$.

$\mathcal{Z}(u_n) = \{n \in \mathbb{N} \ : \ u_n = 0\}$ is called the zero set of $(u_n)_{n=0}^{\infty}$.

Skolem's Problem

Given a LRS $(u_n)_{n=0}^{\infty}$, decide whether $\mathcal{Z}(u_n)$ is non-empty.

Linear Recurrence Sequences and Skolem's Problem

Theorem (Mignotte, Shorey, Tijdeman'84 and Vereshchagin'85)

The Skolem Problem is decidable for LRS of depth 3 over algebraic numbers and for LRS of depth 4 over real algebraic numbers.

Theorem (Mignotte, Shorey, Tijdeman'84 and Vereshchagin'85)

The Skolem Problem is decidable for LRS of depth 3 over algebraic numbers and for LRS of depth 4 over real algebraic numbers.

Theorem (Skolem-Mahler-Lech)

For any LRS $(u_n)_{n=0}^{\infty}$ over algebraic numbers, its zero set $\mathcal{Z}(u_n)$ is semilinear, that is,

$$\mathcal{Z}(u_n) = F \cup \{b_1 + m\mathbb{N}\} \cup \cdots \cup \{b_t + m\mathbb{N}\}$$

where F is a finite set and $b_1, \ldots, b_t, m \in \mathbb{N}$. Moreover $b_1, \ldots, b_t$ and m can be computed from a presentation of $(u_n)_{n=0}^{\infty}$.

Mortality Problem over bounded languages

ABC problem: given three square matrices A, B and C, decide whether there exists $m, n, \ell \in \mathbb{N}$ such that $A^m B^n C^\ell = \mathbf{O}$.

Mortality Problem over bounded languages

ABC problem: given three square matrices A, B and C, decide whether there exists $m, n, \ell \in \mathbb{N}$ such that $A^m B^n C^\ell = \mathbf{O}$.

Let $\mathcal{F}$ denote one of the following fields: $\mathbb{Q}$ (rational numbers), $\mathbf{A}$ (algebraic numbers) $\mathbf{A}_\mathbb{R}$ (real algebraic numbers).

Mortality Problem over bounded languages

ABC problem: given three square matrices A, B and C, decide whether there exists $m, n, \ell \in \mathbb{N}$ such that $A^m B^n C^\ell = \mathbf{O}$.

Let $\mathcal{F}$ denote one of the following fields: $\mathbb{Q}$ (rational numbers), $\mathbf{A}$ (algebraic numbers) $\mathbf{A}_{\mathbb{R}}$ (real algebraic numbers).

Theorem

The ABC problem for matrices of size $k \times k$ with coefficients from $\mathcal{F}$ is equivalent to the Skolem problem for LRS of depth k over $\mathcal{F}$.

Mortality Problem over bounded languages

ABC problem: given three square matrices A, B and C, decide whether there exists $m, n, \ell \in \mathbb{N}$ such that $A^m B^n C^\ell = \mathbf{O}$.

Let $\mathcal{F}$ denote one of the following fields: $\mathbb{Q}$ (rational numbers), $\mathbf{A}$ (algebraic numbers) $\mathbf{A}_\mathbb{R}$ (real algebraic numbers).

Theorem

The ABC problem for matrices of size $k \times k$ with coefficients from $\mathcal{F}$ is equivalent to the Skolem problem for LRS of depth k over $\mathcal{F}$.

Corollary

The ABC problem is decidable for 2×2 and 3×3 matrices over algebraic numbers and for matrices of size 4×4 over real algebraic numbers.

ABC problem: $A^m B^n C^\ell = \mathbf{O}$

The following are equivalent:

- $(u_n)_{n=0}^{\infty}$ is a LRS of depth k
- There is a $k \times k$ matrix B and k-dimensional vector $\mathbf{v}$ and $\mathbf{w}$ such that $\forall n \geq 0 \qquad u_n = \mathbf{v}^\top B^n \mathbf{w}$.

ABC problem: $A^m B^n C^\ell = \mathbf{O}$

The following are equivalent:

- $(u_n)_{n=0}^{\infty}$ is a LRS of depth k
- There is a $k \times k$ matrix B and k-dimensional vector $\mathbf{v}$ and $\mathbf{w}$ such that $\forall n \geq 0 \qquad u_n = \mathbf{v}^\top B^n \mathbf{w}$.

Proposition

If $A^m B^n C^\ell = \mathbf{O}$ for some $m, n, \ell \in \mathbb{N}$, then $AB^nC = \mathbf{O}$.

ABC problem: $A^m B^n C^\ell = \mathbf{O}$

The following are equivalent:

- $(u_n)_{n=0}^{\infty}$ is a LRS of depth k
- There is a $k \times k$ matrix B and k-dimensional vector $\mathbf{v}$ and $\mathbf{w}$ such that $\forall n \geq 0 \qquad u_n = \mathbf{v}^\top B^n \mathbf{w}$.

Proposition

If $A^m B^n C^\ell = \mathbf{O}$ for some $m, n, \ell \in \mathbb{N}$, then $AB^nC = \mathbf{O}$.

True only if the JNF of A and B do not contain nilpotent Jordan blocks of the form $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$

ABC problem

Theorem

Let $\mathcal{U} = \{(m, n, \ell) \in \mathbb{N}^3 \ : \ A^m B^n C^\ell = \mathbf{O}\}$.

ABC problem

Theorem

Let $\mathcal{U} = \{(m, n, \ell) \in \mathbb{N}^3 \;:\; A^m B^n C^\ell = \mathbf{O}\}$.

If the JNF of A and C do not contain nilpotent Jordan blocks, then $\mathcal{U} = \mathbb{N} \times S \times \mathbb{N}$, where S is a semilinear set.

ABC problem

Theorem

Let $\mathcal{U} = \{(m, n, \ell) \in \mathbb{N}^3 \ : \ A^m B^n C^\ell = \mathbf{O}\}$.

If the JNF of A *and* C *do not contain nilpotent Jordan blocks, then* $\mathcal{U} = \mathbb{N} \times S \times \mathbb{N}$, *where* S *is a semilinear set.*

In general,

$$\mathcal{U} = \bigcup_{i=1}^{N} S_1^i \times S_2^i \times S_3^i$$

where S_j^i are semilinear sets.

ABCD problem

ABCD problem: decide if there exist $k, m, n, \ell \in \mathbb{N}$ such that

$$A^k B^m C^n D^\ell = \mathbf{O}$$

ABCD problem: decide if there exist $k, m, n, \ell \in \mathbb{N}$ such that

$$A^k B^m C^n D^\ell = \mathbf{O}$$

Non-semilinear solutions

$$\begin{pmatrix} 1 & -1 \\ 0 & 0 \end{pmatrix}^k \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}^m \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}^\ell = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

This equation holds iff $n = 2^m$ and $k, \ell \in \mathbb{N}$ are arbitrary.

ABCD problem: $A^k B^m C^n D^\ell = \mathbf{O}$

Theorem

ABCD problem is decidable for 2×2 rational upper-triangular matrices.

ABCD problem: $A^k B^m C^n D^\ell = \mathbf{O}$

Theorem

ABCD problem is decidable for 2×2 rational upper-triangular matrices.

Our proof relies of the following result: Let $T = \{p_1, \dots, p_t\}$ be a finite collection of primes.

ABCD problem: $A^k B^m C^n D^\ell = \mathbf{O}$

Theorem

ABCD problem is decidable for 2×2 rational upper-triangular matrices.

Our proof relies of the following result: Let $T = \{p_1, \ldots, p_t\}$ be a finite collection of primes.

Let S be the set of rational numbers that can be expressed as products of primes from T (with positive or negative powers).

ABCD problem: $A^k B^m C^n D^\ell = \mathbf{O}$

Theorem

ABCD problem is decidable for 2×2 rational upper-triangular matrices.

Our proof relies of the following result: Let $T = \{p_1, \ldots, p_t\}$ be a finite collection of primes.

Let S be the set of rational numbers that can be expressed as products of primes from T (with positive or negative powers). Consider the equation

$$x + y = 1 \quad \text{where } x, y \in S$$

ABCD problem: $A^k B^m C^n D^\ell = \mathbf{O}$

Theorem

ABCD problem is decidable for 2×2 rational upper-triangular matrices.

Our proof relies of the following result: Let $T = \{p_1, \ldots, p_t\}$ be a finite collection of primes.

Let S be the set of rational numbers that can be expressed as products of primes from T (with positive or negative powers). Consider the equation

$$x + y = 1 \quad \text{where } x, y \in S$$

This equation has only finitely many solutions which can be algorithmically found.

ABCD problem: $A^k B^m C^n D^\ell = \mathbf{O}$

Theorem

ABCD problem is decidable for 2×2 rational upper-triangular matrices.

Our proof relies of the following result: Let $T = \{p_1, \ldots, p_t\}$ be a finite collection of primes.

Let S be the set of rational numbers that can be expressed as products of primes from T (with positive or negative powers). Consider the equation

$$x + y = 1 \quad \text{where } x, y \in S$$

This equation has only finitely many solutions which can be algorithmically found.

This result relies on Baker's theorem about linear forms in logarithms of algebraic numbers.

Summary

- The ABC problem is decidable for 2×2 and 3×3 matrices over algebraic numbers.

Summary

- The ABC problem is decidable for 2×2 and 3×3 matrices over algebraic numbers.
- The ABC problem is decidable for 4×4 matrices over real algebraic numbers.

Summary

- The ABC problem is decidable for 2×2 and 3×3 matrices over algebraic numbers.
- The ABC problem is decidable for 4×4 matrices over real algebraic numbers.
- The ABCD problem is decidable for 2×2 upper-triangular rational matrices.

Summary

- The ABC problem is decidable for 2×2 and 3×3 matrices over algebraic numbers.
- The ABC problem is decidable for 4×4 matrices over real algebraic numbers.
- The ABCD problem is decidable for 2×2 upper-triangular rational matrices.
- $\mathcal{U} = \{(m, n, \ell) \in \mathbb{N}^3 \ : \ A^m B^n C^\ell = \mathbf{O}\}$ is a finite union of direct products of semilinear sets.

Summary

- The ABC problem is decidable for 2×2 and 3×3 matrices over algebraic numbers.
- The ABC problem is decidable for 4×4 matrices over real algebraic numbers.
- The ABCD problem is decidable for 2×2 upper-triangular rational matrices.
- $\mathcal{U} = \{(m, n, \ell) \in \mathbb{N}^3 \ : \ A^m B^n C^\ell = \mathbf{O}\}$ is a finite union of direct products of semilinear sets.

THANK YOU!