The Membership Problem in matrix semigroups

Pavel Semukhin

Department of Computer Science
University of Oxford

WDCM, 21 July, 2020

A semigroup is a structure $(M, \cdot)$ such that

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \text{for all} \quad a, b, c \in M.$$

Semigroups and Monoids

A semigroup is a structure $(M, \cdot)$ such that

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \text{for all} \quad a, b, c \in M.$$

A semigroup $(M, \cdot)$ is a monoid if there exists $e \in M$ such that

$$a \cdot e = e \cdot a \quad \text{for all} \quad a \in M.$$

Semigroups and Monoids

A semigroup is a structure $(M, \cdot)$ such that

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \text{for all} \quad a, b, c \in M.$$

A semigroup $(M, \cdot)$ is a monoid if there exists $e \in M$ such that

$$a \cdot e = e \cdot a \quad \text{for all} \quad a \in M.$$

We will assume that all groups, semigroups and monoids in this talk have **computable** presentations.

Rational subsets

Let M be a monoid. Then $\mathrm{Rat}(M)$, the family of rational sets of M, is the **smallest** family such that:

- $\mathrm{Rat}(M)$ contains all finite subsets of M.
- If $K, L \in \mathrm{Rat}(M)$, then $K \cup L \in \mathrm{Rat}(M)$ and $KL \in \mathrm{Rat}(M)$.
- If $L \in \mathrm{Rat}(M)$, then $L^* \in \mathrm{Rat}(M)$.

Here $KL = \{u \cdot v \mid u \in K,\ v \in L\}$ and $L^* = \bigcup_{n \geq 0} L^n$ is the submonoid generated by L.

Rational subsets

Let M be a monoid. Then $\mathrm{Rat}(M)$, the family of rational sets of M, is the **smallest** family such that:

- $\mathrm{Rat}(M)$ contains all finite subsets of M.
- If $K, L \in \mathrm{Rat}(M)$, then $K \cup L \in \mathrm{Rat}(M)$ and $KL \in \mathrm{Rat}(M)$.
- If $L \in \mathrm{Rat}(M)$, then $L^* \in \mathrm{Rat}(M)$.

Here $KL = \{u \cdot v \mid u \in K,\ v \in L\}$ and $L^* = \bigcup_{n \geq 0} L^n$ is the submonoid generated by L.

Equivalently, $L \in \mathrm{Rat}(M)$ if L accepted by NFA whose transitions are labelled by elements of M.

Rational subsets

Let M be a monoid. Then $\mathrm{Rat}(M)$, the family of rational sets of M, is the **smallest** family such that:

- $\mathrm{Rat}(M)$ contains all finite subsets of M.
- If $K, L \in \mathrm{Rat}(M)$, then $K \cup L \in \mathrm{Rat}(M)$ and $KL \in \mathrm{Rat}(M)$.
- If $L \in \mathrm{Rat}(M)$, then $L^* \in \mathrm{Rat}(M)$.

Here $KL = \{u \cdot v \mid u \in K,\ v \in L\}$ and $L^* = \bigcup_{n \geq 0} L^n$ is the submonoid generated by L.

Equivalently, $L \in \mathrm{Rat}(M)$ if L accepted by NFA whose transitions are labelled by elements of M.

Example

Any f.g. submonoid or subsemigroup of M is a rational set.

Membership Problems

The Membership problem for rational subsets of M

Input:	Rational subset $R \subseteq M$ and $g \in M$.
Question:	Does $g \in R$?

Membership Problems

The Membership problem for rational subsets of M

Input: Rational subset $R \subseteq M$ and $g \in M$.
Question: Does $g \in R$?

The Semigroup Membership problem for M

Input: Finite subset $F \subseteq M$ and $g \in M$.
Question: Does g belong to the semigroup generated by F?

Membership Problems

The Membership problem for rational subsets of M

Input: Rational subset $R \subseteq M$ and $g \in M$.
Question: Does $g \in R$?

The Semigroup Membership problem for M

Input: Finite subset $F \subseteq M$ and $g \in M$.
Question: Does g belong to the semigroup generated by F?

If M is a **group**.

The Group Membership problem for M

Input: Finite subset $F \subseteq M$ and $g \in M$.
Question: Does g belong to the group generated by F?

The Membership problem for rational subsets is **decidable**

$$\Downarrow$$

The Semigroup Membership problem is **decidable**

Membership Problems

The Membership problem for rational subsets is **decidable**

$$\Downarrow$$

The Semigroup Membership problem is **decidable**

$$\Downarrow$$

The Group Membership problem is **decidable**

Then g belongs to the group generated by $F = \{f_1, \ldots, f_n\}$
iff g belongs to the semigroup generated by $F \cup F^{-1}$,
where $F^{-1} = \{f_1^{-1}, \ldots, f_n^{-1}\}$.

Known results

$$\mathrm{SL}(n,\mathbb{Z}) = \{A \in \mathbb{Z}^{n\times n} \ : \ \det(A) = 1\}$$

$\mathrm{PSL}(2,\mathbb{Z}) = \mathrm{SL}(2,\mathbb{Z})/\{\pm I\}$, i.e. identify A and $-A$

Known results

$$\mathrm{SL}(n,\mathbb{Z}) = \{A \in \mathbb{Z}^{n\times n} \ : \ \det(A) = 1\}$$
$$\mathrm{PSL}(2,\mathbb{Z}) = \mathrm{SL}(2,\mathbb{Z})/\{\pm I\}, \text{ i.e. identify } A \text{ and } -A$$

Theorem (Gurevich and Schupp, 2007)

The **Group** *Membership problem for* $\mathrm{PSL}(2,\mathbb{Z})$ *is decidable in polynomial time.*

$$\mathrm{SL}(n,\mathbb{Z}) = \{A \in \mathbb{Z}^{n\times n} \ : \ \det(A) = 1\}$$
$$\mathrm{PSL}(2,\mathbb{Z}) = \mathrm{SL}(2,\mathbb{Z})/\{\pm I\}, \text{ i.e. identify } A \text{ and } -A$$

Theorem (Gurevich and Schupp, 2007)

*The **Group** Membership problem for $\mathrm{PSL}(2,\mathbb{Z})$ is decidable in polynomial time.*

Theorem (Bell, Hirvensalo and Potapov, 2017)

*The **Semigroup** Membership problem for $\mathrm{PSL}(2,\mathbb{Z})$ is NP-complete.*

Effective Boolean algebras

Example

Let Σ be a finite alphabet and Σ^* be the free monoid generated by Σ. Then

$$\mathrm{Rat}(\Sigma^*) = \text{regular subsets of } \Sigma^*.$$

In this case, $\mathrm{Rat}(\Sigma^*)$ forms an **effective** Boolean algebra.

Example

Let Σ be a finite alphabet and Σ^* be the free monoid generated by Σ. Then

$$\mathrm{Rat}(\Sigma^*) = \text{regular subsets of } \Sigma^*.$$

In this case, $\mathrm{Rat}(\Sigma^*)$ forms an **effective** Boolean algebra.

In general, $\mathrm{Rat}(M)$ is closed under union but not under complement and intersection.

Effective Boolean algebras

Example

Let Σ be a finite alphabet and Σ^* be the free monoid generated by Σ. Then

$$\mathrm{Rat}(\Sigma^*) = \text{regular subsets of } \Sigma^*.$$

In this case, $\mathrm{Rat}(\Sigma^*)$ forms an **effective** Boolean algebra.

In general, $\mathrm{Rat}(M)$ is closed under union but not under complement and intersection.

For any monoid M, it is decidable whether $L = \emptyset$ for $L \in \mathrm{Rat}(M)$.

Effective Boolean algebras

$\mathrm{Rat}(G)$ forms an effective Boolean algebra if

1. G is a f.g. free group. [Benois, 1969]

Effective Boolean algebras

$\mathrm{Rat}(G)$ forms an effective Boolean algebra if

1. G is a f.g. free group. [Benois, 1969]
2. G is a f.g. virtually free group. [Silva, 2002]

Effective Boolean algebras

$\mathrm{Rat}(G)$ forms an effective Boolean algebra if

1. G is a f.g. free group. [Benois, 1969]
2. G is a f.g. virtually free group. [Silva, 2002]

The Membership problem for rational subsets of f.g. virtually free groups is decidable.

Effective Boolean algebras

$\mathrm{Rat}(G)$ forms an effective Boolean algebra if

1. G is a f.g. free group. [Benois, 1969]
2. G is a f.g. virtually free group. [Silva, 2002]

The Membership problem for rational subsets of f.g. virtually free groups is decidable.

In particular, this problem is decidable for the group

$$\mathrm{GL}(2,\mathbb{Z}) = \{A \in \mathbb{Z}^{2\times 2} \ : \ \det(A) = \pm 1\}$$

The matrices $\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$ generate a free subgroup of $\mathrm{GL}(2,\mathbb{Z})$ of index 24.

Commuting matrices

Theorem (Babai, Beals, Cai, Ivanyos and Luks, 1996)

The Membership problem is decidable in PTIME for **commuting** *matrices in any dimension (over the field of algebraic numbers).*

Undecidability results

- The Semigroup Membership problem is undecidable in $\mathbb{Z}^{6\times 6}$. [Markov, 1951]

Undecidability results

- The Semigroup Membership problem is undecidable in $\mathbb{Z}^{6\times 6}$. [Markov, 1951]
- The Group Membership problem is undecidable in $F_2 \times F_2$. [Mihailova, 1958]

Undecidability results

- The Semigroup Membership problem is undecidable in $\mathbb{Z}^{6\times 6}$. [Markov, 1951]
- The Group Membership problem is undecidable in $F_2 \times F_2$. [Mihailova, 1958]
- The Group Membership problem is undecidable in $\mathrm{SL}(4,\mathbb{Z})$.

Undecidability results

- The Semigroup Membership problem is undecidable in $\mathbb{Z}^{6\times 6}$. [Markov, 1951]
- The Group Membership problem is undecidable in $F_2 \times F_2$. [Mihailova, 1958]
- The Group Membership problem is undecidable in $\mathrm{SL}(4,\mathbb{Z})$.
- The Semigroup Membership problem is undecidable in $\mathbb{Z}^{3\times 3}$. [Paterson, 1970]

Undecidability results

- The Semigroup Membership problem is undecidable in $\mathbb{Z}^{6\times 6}$. [Markov, 1951]
- The Group Membership problem is undecidable in $F_2 \times F_2$. [Mihailova, 1958]
- The Group Membership problem is undecidable in $\mathrm{SL}(4, \mathbb{Z})$.
- The Semigroup Membership problem is undecidable in $\mathbb{Z}^{3\times 3}$. [Paterson, 1970]

It is an open question whether (any) Membership problem is decidable in $\mathrm{SL}(3, \mathbb{Z})$.

2×2 integer matrices

Theorem (Semukhin and Potapov, 2017)

The Semigroup Membership problem is decidable for 2×2 integer matrices with nonzero determinant.

2×2 integer matrices

Theorem (Semukhin and Potapov, 2017)

The Semigroup Membership problem is decidable for 2×2 integer matrices with nonzero determinant.

Theorem (Semukhin and Potapov, 2017)

The Semigroup Membership problem is decidable for 2×2 integer matrices with determinant $0, \pm 1$.

2×2 integer matrices

Theorem (Semukhin and Potapov, 2017)

The Semigroup Membership problem is decidable for 2×2 integer matrices with nonzero determinant.

Theorem (Semukhin and Potapov, 2017)

The Semigroup Membership problem is decidable for 2×2 integer matrices with determinant $0, \pm 1$.

Open questions:

- Is the Semigroup Membership for all 2×2 integer matrices.
- Is the Membership problem decidable for

$$\mathrm{GL}(2, \mathbb{Q}) = \{A \in \mathbb{Q}^{2\times 2} \ : \ \det(A) \neq 0\}$$

Theorem (Diekert, S. and Potapov, 2020)

Let G be a f.g. group $\mathrm{GL}(2,\mathbb{Z}) < G \leq \mathrm{GL}(2,\mathbb{Q})$.
Then there are two mutually exclusive cases:

Theorem (Diekert, S. and Potapov, 2020)

Let G be a f.g. group $\mathrm{GL}(2, \mathbb{Z}) < G \leq \mathrm{GL}(2, \mathbb{Q})$.
Then there are two mutually exclusive cases:

1. *G is isomorphic to $\mathrm{GL}(2, \mathbb{Z}) \times \mathbb{Z}^k$ for some $k \geq 1$;*

Baumslag-Solitar group $\mathrm{BS}(1,q) = \langle a, t \mid tat^{-1} = a^q \rangle$

Theorem (Diekert, S. and Potapov, 2020)

Let G be a f.g. group $\mathrm{GL}(2,\mathbb{Z}) < G \leq \mathrm{GL}(2,\mathbb{Q})$. Then there are two mutually exclusive cases:

1. *G is isomorphic to $\mathrm{GL}(2,\mathbb{Z}) \times \mathbb{Z}^k$ for some $k \geq 1$;*
2. *G contains a subgroup which is an extension of infinite index of $\mathrm{BS}(1,q)$ for some $q \geq 2$.*

Baumslag-Solitar group $\mathrm{BS}(1,q) = \langle a, t \mid tat^{-1} = a^q \rangle$

Theorem (Diekert, S. and Potapov, 2020)

Let G be a f.g. group $\mathrm{GL}(2,\mathbb{Z}) < G \leq \mathrm{GL}(2,\mathbb{Q})$.
Then there are two mutually exclusive cases:

1. *G is isomorphic to $\mathrm{GL}(2,\mathbb{Z}) \times \mathbb{Z}^k$ for some $k \geq 1$;*
2. *G contains a subgroup which is an extension of infinite index of $\mathrm{BS}(1,q)$ for some $q \geq 2$.*

Theorem (Lohrey and Steinberg, 2008)

The Membership problem is decidable for $\mathrm{GL}(2,\mathbb{Z}) \times \mathbb{Z}^k$.

Baumslag-Solitar group $\mathrm{BS}(1,q) = \langle a, t \mid tat^{-1} = a^q \rangle$

Theorem (Diekert, S. and Potapov, 2020)

Let G be a f.g. group $\mathrm{GL}(2,\mathbb{Z}) < G \leq \mathrm{GL}(2,\mathbb{Q})$. Then there are two mutually exclusive cases:

1. *G is isomorphic to $\mathrm{GL}(2,\mathbb{Z}) \times \mathbb{Z}^k$ for some $k \geq 1$;*
2. *G contains a subgroup which is an extension of infinite index of $\mathrm{BS}(1,q)$ for some $q \geq 2$.*

Theorem (Lohrey and Steinberg, 2008)

The Membership problem is decidable for $\mathrm{GL}(2,\mathbb{Z}) \times \mathbb{Z}^k$.

Theorem (Romanovskii, 1974)

The Group Membership problem is decidable for metabelian groups, in particular for $\mathrm{BS}(1,q)$.

Baumslag-Solitar group $\mathrm{BS}(1,q) = \langle a, t \mid tat^{-1} = a^q \rangle$

Theorem (Diekert, S. and Potapov, 2020)

Let G be a f.g. group $\mathrm{GL}(2,\mathbb{Z}) < G \leq \mathrm{GL}(2,\mathbb{Q})$. Then there are two mutually exclusive cases:

1. *G is isomorphic to $\mathrm{GL}(2,\mathbb{Z}) \times \mathbb{Z}^k$ for some $k \geq 1$;*
2. *G contains a subgroup which is an extension of infinite index of $\mathrm{BS}(1,q)$ for some $q \geq 2$.*

Theorem (Cadilhac, Chistikov and Zetzsche, 2020)

The Membership problem for rational subsets of $\mathrm{BS}(1,q)$ is PSPACE-complete.

Baumslag-Solitar group $\mathrm{BS}(1,q) = \langle a, t \mid tat^{-1} = a^q \rangle$

Theorem (Diekert, S. and Potapov, 2020)

Let G be a f.g. group $\mathrm{GL}(2,\mathbb{Z}) < G \leq \mathrm{GL}(2,\mathbb{Q})$.
Then there are two mutually exclusive cases:

1. *G is isomorphic to $\mathrm{GL}(2,\mathbb{Z}) \times \mathbb{Z}^k$ for some $k \geq 1$;*
2. *G contains a subgroup which is an extension of infinite index of $\mathrm{BS}(1,q)$ for some $q \geq 2$.*

Theorem (Cadilhac, Chistikov and Zetzsche, 2020)

The Membership problem for rational subsets of $\mathrm{BS}(1,q)$ is PSPACE-complete.

Open problem: is the Semigroup Membership decidable for infinite extensions of $\mathrm{BS}(1,q)$?

Heisenberg group

The Heisenberg group $\mathrm{H}(3, \mathbb{Z})$ is a natural subgroup of $\mathrm{SL}(3, \mathbb{Z})$ that consists of the matrices of the form

$$\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \qquad \text{where } a, b, c \in \mathbb{Z}.$$

Heisenberg group

The Heisenberg group $\mathrm{H}(3,\mathbb{Z})$ is a natural subgroup of $\mathrm{SL}(3,\mathbb{Z})$ that consists of the matrices of the form

$$\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \qquad \text{where } a, b, c \in \mathbb{Z}.$$

$\mathrm{H}(3,\mathbb{Z})$ is 2-step nilpotent group. Hence the Group Membership problem for $\mathrm{H}(3,\mathbb{Z})$ is decidable by

Theorem (Mostowski, 1966)

The Group Membership is decidable for f.g. nilpotent groups.

Heisenberg group

The Heisenberg group $\mathrm{H}(3,\mathbb{Z})$ is a natural subgroup of $\mathrm{SL}(3,\mathbb{Z})$ that consists of the matrices of the form

$$\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \qquad \text{where } a, b, c \in \mathbb{Z}.$$

$\mathrm{H}(3,\mathbb{Z})$ is 2-step nilpotent group. Hence the Group Membership problem for $\mathrm{H}(3,\mathbb{Z})$ is decidable by

Theorem (Mostowski, 1966)

The Group Membership is decidable for f.g. nilpotent groups.

Theorem (Colcombet, Ouaknine, S. and Worrell, 2019)

The Semigroup Membership problem in $\mathrm{H}(3,\mathbb{Z})$ is decidable.

Heisenberg group

Theorem (König, Lohrey and Zetzsche, 2015)

The Knapsack problem in $\mathrm{H}(3, \mathbb{Z})$ *is decidable, that is, given* $A_1, \dots A_k, A \in \mathrm{H}(3, \mathbb{Z})$, *does there exist* $n_1, \dots n_k \in \mathbb{N}$ *such that*

$$A_1^{n_1} \cdots A_k^{n_k} = A.$$

Theorem (König, Lohrey and Zetzsche, 2015)

The Knapsack problem in $\mathrm{H}(3, \mathbb{Z})$ *is decidable, that is, given* $A_1, \ldots A_k, A \in \mathrm{H}(3, \mathbb{Z})$, *does there exist* $n_1, \ldots n_k \in \mathbb{N}$ *such that*

$$A_1^{n_1} \cdots A_k^{n_k} = A.$$

Proof idea

Reduce the Knapsack problem to the Hilbert's 10th problem for a quadratic Diophantine equation, which is decidable by a result of Grunewald and Segal, 2004.

Heisenberg group

Theorem (König, Lohrey and Zetzsche, 2015)

The Knapsack problem in $\mathrm{H}(3,\mathbb{Z})$ *is decidable, that is, given* $A_1, \dots A_k, A \in \mathrm{H}(3,\mathbb{Z})$, *does there exist* $n_1, \dots n_k \in \mathbb{N}$ *such that*

$$A_1^{n_1} \cdots A_k^{n_k} = A.$$

- Is the Membership problem for rational subsets of $\mathrm{H}(3,\mathbb{Z})$ decidable?
- Is the Semigroup Membership problem for $\mathrm{H}(3,\mathbb{Z}) \times \mathrm{H}(3,\mathbb{Z})$ decidable?

Theorem (König, Lohrey and Zetzsche, 2015)

The Knapsack problem in $\mathrm{H}(3,\mathbb{Z})$ *is decidable, that is, given* $A_1,\dots A_k, A \in \mathrm{H}(3,\mathbb{Z})$*, does there exist* $n_1,\dots n_k \in \mathbb{N}$ *such that*

$$A_1^{n_1}\cdots A_k^{n_k} = A.$$

- Is the Membership problem for rational subsets of $\mathrm{H}(3,\mathbb{Z})$ decidable?
- Is the Semigroup Membership problem for $\mathrm{H}(3,\mathbb{Z}) \times \mathrm{H}(3,\mathbb{Z})$ decidable?

$\exists n$ such that the **Knapsack** and the **Semigroup** Membership problems are undecidable in $\mathrm{H}(3,\mathbb{Z})^n$.

Theorem (König, Lohrey and Zetzsche, 2015)

The Knapsack problem in $\mathrm{H}(3,\mathbb{Z})$ *is decidable, that is, given* $A_1,\dots A_k, A \in \mathrm{H}(3,\mathbb{Z})$, *does there exist* $n_1,\dots n_k \in \mathbb{N}$ *such that*

$$A_1^{n_1}\cdots A_k^{n_k} = A.$$

- Is the Membership problem for rational subsets of $\mathrm{H}(3,\mathbb{Z})$ decidable?
- Is the Semigroup Membership problem for $\mathrm{H}(3,\mathbb{Z}) \times \mathrm{H}(3,\mathbb{Z})$ decidable?

$\exists n$ such that the **Knapsack** and the **Semigroup** Membership problems are undecidable in $\mathrm{H}(3,\mathbb{Z})^n$.

The **Group** Membership is decidable in $\mathrm{H}(3,\mathbb{Z})^n$ for all $n \geq 1$.

The Knapsack problem for the zero matrix

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

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

The Knapsack problem for the zero matrix

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

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

Bell, Halava, Harju, Karhumäki and Potapov, 2008

By an encoding of Hilbert's 10th problem, it was shown that the above problem is undecidable for integer matrices of large dimension and large n.

ABC problem

Given three square matrices A, B and C, decide whether there exists $m, n, \ell \in \mathbb{N}$ such that

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

ABC problem

Given three square matrices A, B and C, decide whether there exists $m, n, \ell \in \mathbb{N}$ such that

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

The ABC problem is algorithmically equivalent to the well-known Skolem problem for linear recurrence sequences.

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 $a_1, \ldots, a_k$ such that for all $n \geq k$

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

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 $a_1, \ldots, a_k$ such that for all $n \geq k$

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

Fibonacci sequence

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

Linear Recurrence Sequences and Skolem's problem

The Skolem problem

Given a LRS $(u_n)_{n=0}^{\infty}$, decide whether there is n such that $u_n = 0$.

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

The Skolem problem is decidable

- *for LRS of depth 3 over algebraic numbers;*
- *for LRS of depth 4 over real algebraic numbers.*

Linear Recurrence Sequences and Skolem's problem

The Skolem problem

Given a LRS $(u_n)_{n=0}^{\infty}$, decide whether there is n such that $u_n = 0$.

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

The Skolem problem is decidable

- *for LRS of depth 3 over algebraic numbers;*
- *for LRS of depth 4 over real algebraic numbers.*

Both proofs rely on Baker's theorem about linear forms in logarithms of algebraic numbers.

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

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

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

Theorem (Bell, S. and Potapov, 2019)

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

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

Theorem (Bell, S. and Potapov, 2019)

The ABC problem for $k \times k$ matrices 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 3×3 matrices over algebraic numbers and for matrices of size 4×4 over real algebraic numbers.

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

Theorem (Bell, S. and Potapov, 2019)

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

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

Theorem (Bell, S. and Potapov, 2019)

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

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

Theorem (Bell, S. and Potapov, 2019)

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

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

$$S = \{p_1^{k_1} \cdots p_n^{k_n} \ : \ k_1, \ldots, k_n \in \mathbb{Z}\}.$$

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

Theorem (Bell, S. and Potapov, 2019)

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

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

$$S = \{p_1^{k_1} \cdots p_n^{k_n} \; : \; k_1, \ldots, k_n \in \mathbb{Z}\}.$$

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 (Bell, S. and Potapov, 2019)

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

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

$$S = \{p_1^{k_1} \cdots p_n^{k_n} \ : \ k_1, \ldots, k_n \in \mathbb{Z}\}.$$

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 (Bell, S. and Potapov, 2019)

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

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

$$S = \{p_1^{k_1} \cdots p_n^{k_n} \ : \ k_1, \ldots, k_n \in \mathbb{Z}\}.$$

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.

Open problems

- Is the Membership problem decidable in $\mathrm{GL}(2, \mathbb{Q})$?
- Is the Semigroup Membership problem decidable in $\mathbb{Z}^{2\times 2}$?
- Is the Knapsack problem decidable in $\mathbb{Z}^{2\times 2}$?
- Is the Membership problem for rational subsets decidable in the Heisenberg group $\mathrm{H}(3, \mathbb{Z})$?
- Is the Membership problem decidable in $\mathrm{SL}(3, \mathbb{Z})$?

Open problems

- Is the Membership problem decidable in $\mathrm{GL}(2, \mathbb{Q})$?
- Is the Semigroup Membership problem decidable in $\mathbb{Z}^{2\times 2}$?
- Is the Knapsack problem decidable in $\mathbb{Z}^{2\times 2}$?
- Is the Membership problem for rational subsets decidable in the Heisenberg group $\mathrm{H}(3, \mathbb{Z})$?
- Is the Membership problem decidable in $\mathrm{SL}(3, \mathbb{Z})$?

THANK YOU