On reachability problems for low dimensional matrix semigroups

Pavel Semukhin

joint work with T. Colcombet, J. Ouaknine and J. Worrell

Department of Computer Science, University of Oxford

RP 2019, Brussels

The Membership problem

Input: A finite collection $\mathcal{G}$ of $n \times n$ matrices and a "target" matrix M.

Question: Does M belong to $\langle \mathcal{G} \rangle$

The Membership problem

Input: A finite collection $\mathcal{G}$ of $n \times n$ matrices and a "target" matrix M.

Question: Does M belong to $\langle \mathcal{G} \rangle$, that is, does there exist a sequence of matrices $M_1, M_2, \ldots, M_k \in \mathcal{G}$ such that

$$M = M_1 M_2 \cdots M_k$$

The Membership problem

Input: A finite collection $\mathcal{G}$ of $n \times n$ matrices and a "target" matrix M.

Question: Does M belong to $\langle \mathcal{G} \rangle$, that is, does there exist a sequence of matrices $M_1, M_2, \ldots, M_k \in \mathcal{G}$ such that

$$M = M_1 M_2 \cdots M_k$$

The Membership problem is called:

- the Mortality problem if the target M is the zero matrix,
- the Identity problem if the target M is the identity matrix.

Known results

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

Known results

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

Known results

Let $\mathrm{SL}(2,\mathbb{Z}) = \{A \in \mathbb{Z}^{2\times 2} \; : \; \det(A) = 1\}$.

- The Mortality problem (and hence the Membership problem) is undecidable for 3×3 integer matrices. [Paterson, 1970]
- The membership problem is decidable for commuting matrices over algebraic numbers [Babai, et. al., 1996]
- The Membership problem is decidable in $\mathrm{SL}(2,\mathbb{Z})$. [P. Silva, 2002; Choffrut and Karhumäki, 2005]

Known results

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

Known results

- The Membership problem is decidable for 2×2 nonsingular integer matrices. [Semukhin and Potapov, 2017]
- The Identity problem is undecidable in $\mathrm{SL}(4, \mathbb{Z})$. [Bell and Potapov, 2010]

Known results

- The Membership problem is decidable for 2×2 nonsingular integer matrices. [Semukhin and Potapov, 2017]
- The Identity problem is undecidable in $\mathrm{SL}(4, \mathbb{Z})$. [Bell and Potapov, 2010]
- It is an open question whether the Membership (or the Identity) problem is decidable in $\mathrm{SL}(3, \mathbb{Z})$.

Known results

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

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

Known results

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

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

The Identity problem in $\mathrm{H}(3,\mathbb{Z})$ is decidable in PTIME.
[Ko, Niskanen, Potapov, 2018]

Known results

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

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

The Identity problem in $\mathrm{H}(3,\mathbb{Z})$ is decidable in PTIME. [Ko, Niskanen, Potapov, 2018]

In fact, this result holds in $\mathrm{H}(3,\mathbb{Q})$.

Theorem

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

Theorem

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

- The Membership problem in $\mathrm{H}(3, \mathbb{Q})$ is reducible to $\mathrm{H}(3, \mathbb{Z})$.

Theorem

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

- The Membership problem in $\mathrm{H}(3,\mathbb{Q})$ is reducible to $\mathrm{H}(3,\mathbb{Z})$.
- For $M = \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}$ define $\varphi(M) = (a, b)$.

Theorem

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

- The Membership problem in $\mathrm{H}(3,\mathbb{Q})$ is reducible to $\mathrm{H}(3,\mathbb{Z})$.
- For $M = \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}$ define $\varphi(M) = (a, b)$.
- $\varphi : \mathrm{H}(3,\mathbb{Z}) \to \mathbb{Z} \times \mathbb{Z}$ is a homomorphism, that is,

$$\varphi(M_1 M_2) = \varphi(M_1) + \varphi(M_2).$$

Suppose $\mathcal{G} = \{M_1, \ldots, M_k\} \subseteq \mathrm{H}(3, \mathbb{Z})$ is the given set of generators and $M \in \mathrm{H}(3, \mathbb{Z})$.

Suppose $\mathcal{G} = \{M_1, \ldots, M_k\} \subseteq \mathrm{H}(3, \mathbb{Z})$ is the given set of generators and $M \in \mathrm{H}(3, \mathbb{Z})$.

We partition $\mathcal{G} = \mathcal{G}_+ \cup \mathcal{G}_0$ and compute a bound K such that:

- Any $M_i \in \mathcal{G}_+$ can be used at most K times in any product of generators from $\mathcal{G}$ that is equal to M.

Suppose $\mathcal{G} = \{M_1, \ldots, M_k\} \subseteq \mathrm{H}(3, \mathbb{Z})$ is the given set of generators and $M \in \mathrm{H}(3, \mathbb{Z})$.

We partition $\mathcal{G} = \mathcal{G}_+ \cup \mathcal{G}_0$ and compute a bound K such that:

- Any $M_i \in \mathcal{G}_+$ can be used at most K times in any product of generators from $\mathcal{G}$ that is equal to M.
- There is a sequence $A_1, \ldots, A_m \in \mathcal{G}_0$ such that

$$\varphi(A_1 \cdots A_m) = (0, 0).$$

Suppose $\mathcal{G} = \{M_1, \ldots, M_k\} \subseteq \mathrm{H}(3, \mathbb{Z})$ is the given set of generators and $M \in \mathrm{H}(3, \mathbb{Z})$.

We partition $\mathcal{G} = \mathcal{G}_+ \cup \mathcal{G}_0$ and compute a bound K such that:

- Any $M_i \in \mathcal{G}_+$ can be used at most K times in any product of generators from $\mathcal{G}$ that is equal to M.
- There is a sequence $A_1, \ldots, A_m \in \mathcal{G}_0$ such that

$$\varphi(A_1 \cdots A_m) = (0, 0).$$

In this case there is no bound on how many times a matrix from $\mathcal{G}_0$ can appear in a product which is equal to M.

Let $\mathcal{G} = \{M_1, \ldots, M_k\}$ and suppose that for $i = 1, \ldots, k$

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

Let $\mathcal{G} = \{M_1, \ldots, M_k\}$ and suppose that for $i = 1, \ldots, k$

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

Define the cone

$$C = \mathrm{Cone}\{\varphi(M_1), \ldots, \varphi(M_k)\} = \{(a_1, b_1), \ldots, (a_k, b_k)\}.$$

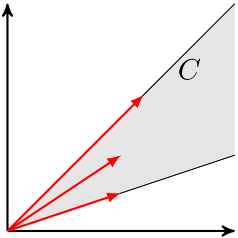

Figure: C is a pointed cone

In this case $\mathcal{G}_+ = \mathcal{G}$ and $\mathcal{G}_0 = \emptyset$.

Every matrix from $\mathcal{G} = \mathcal{G}_+$ can be used at most K times to reach the target M.

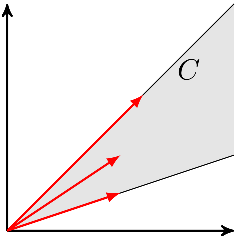

Figure: C is a pointed cone

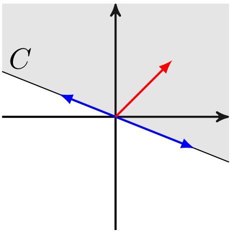

Figure: C is a half-plane

In this case $\mathcal{G}_+ = \mathcal{G}$ and $\mathcal{G}_0 = \emptyset$.

Every matrix from $\mathcal{G} = \mathcal{G}_+$ can be used at most K times to reach the target M.

In this case the matrices from $\mathcal{G}_0$ commute.

The problem can be reduced to a system of linear Diophantine equations.

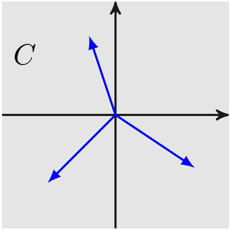

Figure: C is the whole plane: $\mathcal{G}_0 = \mathcal{G}$, $\mathcal{G}_+ = \emptyset$.

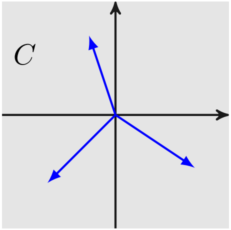

Figure: C is the whole plane: $\mathcal{G}_0 = \mathcal{G}$, $\mathcal{G}_+ = \emptyset$.

Using the fact that there are non-commuting matrices in $\mathcal{G}_0$ we can show that there is an integer $m > 0$ such that

$$\begin{pmatrix} 1 & 0 & m \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 & -m \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{are in } \langle \mathcal{G}_0 \rangle.$$

Hence $M = \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \in \langle \mathcal{G} \rangle$ iff

$$\begin{pmatrix} 1 & a & d \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \in \langle \mathcal{G} \rangle \quad \text{for some } d \equiv c \pmod{m}.$$

Hence $M = \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \in \langle \mathcal{G} \rangle$ iff

$$\begin{pmatrix} 1 & a & d \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \in \langle \mathcal{G} \rangle \quad \text{for some } d \equiv c \pmod{m}.$$

This is because

$$\begin{pmatrix} 1 & a & d \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & \pm m \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a & d \pm m \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}$$

Hence $M = \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \in \langle \mathcal{G} \rangle$ iff

$$\begin{pmatrix} 1 & a & d \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \in \langle \mathcal{G} \rangle \quad \text{for some } d \equiv c \pmod{m}.$$

This is because

$$\begin{pmatrix} 1 & a & d \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & \pm m \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a & d \pm m \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}$$

To check whether $\mathcal{G}$ contains such a matrix we will use a register automaton $\mathcal{A}$.

- The alphabet of $\mathcal{A}$ is $\mathcal{G} = \{M_1, \ldots, M_k\}$.

- The alphabet of $\mathcal{A}$ is $\mathcal{G} = \{M_1, \ldots, M_k\}$.
- The states of $\mathcal{A}$ are triples (s, t, u) such that $s, t, u \in \{0, \ldots, m-1\}$, and $(0, 0, 0)$ is the initial state.

- The alphabet of $\mathcal{A}$ is $\mathcal{G} = \{M_1, \ldots, M_k\}$.
- The states of $\mathcal{A}$ are triples (s, t, u) such that $s, t, u \in \{0, \ldots, m-1\}$, and $(0, 0, 0)$ is the initial state.
- $\mathcal{A}$ has two integer registers that are initially zeros.

- The alphabet of $\mathcal{A}$ is $\mathcal{G} = \{M_1, \ldots, M_k\}$.
- The states of $\mathcal{A}$ are triples (s, t, u) such that $s, t, u \in \{0, \ldots, m-1\}$, and $(0, 0, 0)$ is the initial state.
- $\mathcal{A}$ has two integer registers that are initially zeros.
- The transitions of $\mathcal{A}$ are defined in such a way that after reading a word

$$M_{i_1} \cdots M_{i_k} = \begin{pmatrix} 1 & a' & c' \\ 0 & 1 & b' \\ 0 & 0 & 1 \end{pmatrix}$$

the automaton moves to the state

$$(a',\ b',\ c') \qquad (\mathrm{mod}\ m)$$

- The alphabet of $\mathcal{A}$ is $\mathcal{G} = \{M_1, \ldots, M_k\}$.
- The states of $\mathcal{A}$ are triples (s, t, u) such that $s, t, u \in \{0, \ldots, m-1\}$, and $(0, 0, 0)$ is the initial state.
- $\mathcal{A}$ has two integer registers that are initially zeros.
- The transitions of $\mathcal{A}$ are defined in such a way that after reading a word

$$M_{i_1} \cdots M_{i_k} = \begin{pmatrix} 1 & a' & c' \\ 0 & 1 & b' \\ 0 & 0 & 1 \end{pmatrix}$$

the automaton moves to the state

$$(a',\ b',\ c') \pmod m$$

and the value of the registers becomes equal to (a', b').

- The final state is

$$(a,\ b,\ c) \pmod m$$

where $M = \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}$

- The final state is

$$(a,\ b,\ c) \pmod{m}$$

where $M = \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}$

Hence if the registers of $\mathcal{A}$ can reach the value (a, b) at the final state, then there is a product

$$M_{i_1} \cdots M_{i_k} = \begin{pmatrix} 1 & a & d \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \text{ for some } d \equiv c \pmod{m}.$$

- The final state is

$$(a,\ b,\ c) \qquad (\text{mod } m)$$

where $M = \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}$

Hence if the registers of $\mathcal{A}$ can reach the value (a, b) at the final state, then there is a product

$$M_{i_1} \cdots M_{i_k} = \begin{pmatrix} 1 & a & d \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \text{ for some } d \equiv c \pmod{m}.$$

Recall that this is equivalent to $M \in \langle \mathcal{G} \rangle$.

- After reading any M_i, the resisters of $\mathcal{A}$ are updated by constant values, namely, by (a_i, b_i).

- After reading any M_i, the resisters of $\mathcal{A}$ are updated by constant values, namely, by (a_i, b_i).
- $\mathcal{A}$ does not have zero checks, and the registers can be positive or negative.

- After reading any M_i, the resisters of $\mathcal{A}$ are updated by constant values, namely, by (a_i, b_i).
- $\mathcal{A}$ does not have zero checks, and the registers can be positive or negative.
- For such automata the set of register values reachable at any given state is effectively semilinear.

- After reading any M_i, the resisters of $\mathcal{A}$ are updated by constant values, namely, by (a_i, b_i).
- $\mathcal{A}$ does not have zero checks, and the registers can be positive or negative.
- For such automata the set of register values reachable at any given state is effectively semilinear.
- So we can decide whether (a, b) can be reached at the final state of $\mathcal{A}$, and hence decide whether $M \in \langle \mathcal{G} \rangle$.

- After reading any M_i, the resisters of $\mathcal{A}$ are updated by constant values, namely, by (a_i, b_i).
- $\mathcal{A}$ does not have zero checks, and the registers can be positive or negative.
- For such automata the set of register values reachable at any given state is effectively semilinear.
- So we can decide whether (a, b) can be reached at the final state of $\mathcal{A}$, and hence decide whether $M \in \langle \mathcal{G} \rangle$.

THANK YOU!