On the Identity Problem for Unitriangular Matrices of Dimension Four

Ruiwen Dong

University of Oxford

October 2022

An old decidability problem

Markov (1940s): is the following decidable?

Input: Set of square matrices $\mathcal{G} = \{A_1, \ldots, A_K\}$, target matrix T.
Output: Is there a sequence $B_1, B_2, \ldots, B_m \in \mathcal{G}$, s.t. $B_1 B_2 \cdots B_m = T$?

An old decidability problem

Markov (1940s): is the following decidable?

Input: Set of square matrices $\mathcal{G} = \{A_1, \ldots, A_K\}$, target matrix T.
Output: Is there a sequence $B_1, B_2, \ldots, B_m \in \mathcal{G}$, s.t. $B_1 B_2 \cdots B_m = T$?

Markov (1940s) : undecidable in $\mathbb{Z}^{6\times 6}$.

An old decidability problem

Markov (1940s): is the following decidable?

Input: Set of square matrices $\mathcal{G} = \{A_1, \ldots, A_K\}$, target matrix T.
Output: Is there a sequence $B_1, B_2, \ldots, B_m \in \mathcal{G}$, s.t. $B_1 B_2 \cdots B_m = T$?

Markov (1940s) : undecidable in $\mathbb{Z}^{6\times 6}$.
Michailova (1960s): undecidable in $\mathrm{SL}(4, \mathbb{Z})$.

An old decidability problem

Markov (1940s): is the following decidable?

Input: Set of square matrices $\mathcal{G} = \{A_1, \ldots, A_K\}$, target matrix T.
Output: Is there a sequence $B_1, B_2, \ldots, B_m \in \mathcal{G}$, s.t. $B_1 B_2 \cdots B_m = T$?

Markov (1940s) : undecidable in $\mathbb{Z}^{6\times 6}$.
Michailova (1960s): undecidable in $\mathrm{SL}(4, \mathbb{Z})$.

Specialization: is the following decidable?

Input: Set of element $\mathcal{G} = \{A_1, \ldots, A_K\}$ in a group G.
Output: Is there a sequence $B_1, B_2, \ldots, B_m \in \mathcal{G}$, s.t. $B_1 B_2 \cdots B_m = I$?

An old decidability problem

Markov (1940s): is the following decidable?

Input: Set of square matrices $\mathcal{G} = \{A_1, \ldots, A_K\}$, target matrix T.
Output: Is there a sequence $B_1, B_2, \ldots, B_m \in \mathcal{G}$, s.t. $B_1 B_2 \cdots B_m = T$?

Markov (1940s) : undecidable in $\mathbb{Z}^{6\times 6}$.
Michailova (1960s): undecidable in $\mathrm{SL}(4, \mathbb{Z})$.

Specialization: is the following decidable?

Input: Set of element $\mathcal{G} = \{A_1, \ldots, A_K\}$ in a group G.
Output: Is there a sequence $B_1, B_2, \ldots, B_m \in \mathcal{G}$, s.t. $B_1 B_2 \cdots B_m = I$?

Bell, Potapov (2000s) : undecidable in $\mathrm{SL}(4, \mathbb{Z})$.

the Identity Problem and the Membership Problem

Definition (Identity Problem)

Given a finite set of square matrices $\mathcal{G} = \{A_1, \ldots, A_k\}$, decide whether the (multiplicative) semigroup $\langle \mathcal{G} \rangle$ generated by $A_1, \ldots, A_k$ contains I.

Definition (Membership Problem)

Given a finite set of square matrices $\mathcal{G} = \{A_1, \ldots, A_k\}$ and a matrix A, decide whether the semigroup $\langle \mathcal{G} \rangle$ generated by $A_1, \ldots, A_k$ contains A.

the Identity Problem and the Membership Problem

Definition (Identity Problem)

Given a finite set of square matrices $\mathcal{G} = \{A_1, \ldots, A_k\}$, decide whether the (multiplicative) semigroup $\langle \mathcal{G} \rangle$ generated by $A_1, \ldots, A_k$ contains I.

Definition (Membership Problem)

Given a finite set of square matrices $\mathcal{G} = \{A_1, \ldots, A_k\}$ and a matrix A, decide whether the semigroup $\langle \mathcal{G} \rangle$ generated by $A_1, \ldots, A_k$ contains A.

Known results.

group types	Membership Prob. $T \in \langle \mathcal{G} \rangle$?	Identity Prob. $I \in \langle \mathcal{G} \rangle$?
Commutative	NP-complete	PTIME
$\mathrm{SL}(2, \mathbb{Z})$	Decidable	NP-complete
$\mathrm{SL}(3, \mathbb{Z})$	?	?
$\mathrm{SL}(4, \mathbb{Z})$	Undecidable	Undecidable

$\mathrm{UT}(n, \mathbb{Z})$

Definition ($\mathrm{UT}(n, \mathbb{Z})$)

Define $\mathrm{UT}(n, \mathbb{Z})$ to be the group of $n \times n$ upper triangular integer matrices with ones on the diagonal.

$$\begin{pmatrix} 1 & * & \cdots & * \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \cdots & 0 & 1 \end{pmatrix}$$

$\mathrm{UT}(n, \mathbb{Z})$

Definition ($\mathrm{UT}(n, \mathbb{Z})$)

Define $\mathrm{UT}(n, \mathbb{Z})$ to be the group of $n \times n$ upper triangular integer matrices with ones on the diagonal.

$$\begin{pmatrix} 1 & * & \cdots & * \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \cdots & 0 & 1 \end{pmatrix}$$

Known results.

group types	Group Mem. $T \in \langle \mathcal{G} \rangle_{grp}$?	Semigroup Mem. $T \in \langle \mathcal{G} \rangle$?	Identity Prob. $I \in \langle \mathcal{G} \rangle$?
$\mathrm{UT}(3, \mathbb{Z})$	Decidable	Decidable	PTIME
$\mathrm{UT}(4, \mathbb{Z})$	Decidable	?	PTIME
$\mathrm{UT}(11, \mathbb{Z})$	Decidable	?	PTIME
$\mathrm{UT}(n, \mathbb{Z})$	Decidable	Undecidable	?

Two layers of $\mathrm{UT}(4, \mathbb{Z})$

First layer: Multiplication acts additively on the superdiagonal.

$$\begin{pmatrix} 1 & a_1 & * & * \\ 0 & 1 & b_1 & * \\ 0 & 0 & 1 & c_1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & a_2 & * & * \\ 0 & 1 & b_2 & * \\ 0 & 0 & 1 & c_2 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a_1 + a_2 & * & * \\ 0 & 1 & b_1 + b_2 & * \\ 0 & 0 & 1 & c_1 + c_2 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Second layer: If superdiagonal vanishes, multiplication acts additively.

$$\begin{pmatrix} 1 & 0 & d_1 & f_1 \\ 0 & 1 & 0 & e_1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & 0 & d_2 & f_2 \\ 0 & 1 & 0 & e_2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & d_1 + d_2 & f_1 + f_2 \\ 0 & 1 & 0 & e_1 + e_2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Structure of $\mathrm{UT}(4, \mathbb{Z})$

Short exact sequence:

$$\{I\} \longrightarrow \mathbb{Z}^3 \longrightarrow \mathrm{UT}(4,\mathbb{Z}) \xrightarrow{\varphi} \mathbb{Z}^3 \longrightarrow \{I\}$$

$$\varphi : \begin{pmatrix} 1 & a & d & f \\ 0 & 1 & b & e \\ 0 & 0 & 1 & c \\ 0 & 0 & 0 & 1 \end{pmatrix} \longmapsto (a, b, c)$$

$$\mathrm{U}_1 = \ker\varphi = \left\{ \begin{pmatrix} 1 & 0 & d & f \\ 0 & 1 & 0 & e \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \middle| d, e, f \in \mathbb{Z} \right\} \cong \mathbb{Z}^3$$

U_1 is abelian.

Identity Problem in $\mathsf{UT}(4,\mathbb{Z})$

$$\{I\} \longrightarrow \mathbb{Z}^3 \longrightarrow \mathsf{UT}(4,\mathbb{Z}) \xrightarrow{\varphi} \mathbb{Z}^3 \longrightarrow \{I\}$$

$$\varphi : \begin{pmatrix} 1 & a & d & f \\ 0 & 1 & b & e \\ 0 & 0 & 1 & c \\ 0 & 0 & 0 & 1 \end{pmatrix} \longmapsto (a,b,c)$$

$$\mathsf{U}_1 = \ker\varphi \cong \mathbb{Z}^3.$$

The following are equivalent:

1. $B_1 B_2 \cdots B_m \in \mathsf{U}_1$.
2. $\varphi(B_1) + \varphi(B_2) + \cdots + \varphi(B_m) = \mathbf{0}$.

General idea: Given $\mathcal{G} = \{A_1, \ldots, A_k\}$, characterize $\mathsf{U}_1 \cap \langle \mathcal{G} \rangle$.

Identity Problem in $\mathrm{UT}(4, \mathbb{Z})$: Example

To reach I, we must first reach U_1. $\mathcal{G} = \{A_1, A_2, A_3, A_4\}$.

$$A_1 = \begin{pmatrix} 1 & 1 & 2 & 2 \\ 0 & 1 & 1 & 3 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}, A_2 = \begin{pmatrix} 1 & -1 & 4 & -2 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

$$A_3 = \begin{pmatrix} 1 & 0 & -2 & 0 \\ 0 & 1 & -1 & 3 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, A_4 = \begin{pmatrix} 1 & 0 & 7 & 5 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

Is $I \in \langle \mathcal{G} \rangle$?

Identity Problem in $\mathrm{UT}(4, \mathbb{Z})$: Example

To reach I, we must first reach U_1. $\mathcal{G} = \{A_1, A_2, A_3, A_4\}$.

$$A_1 = \begin{pmatrix} 1 & 1 & 2 & 2 \\ 0 & 1 & 1 & 3 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}, A_2 = \begin{pmatrix} 1 & -1 & 4 & -2 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

$$A_3 = \begin{pmatrix} 1 & 0 & -2 & 0 \\ 0 & 1 & -1 & 3 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, A_4 = \begin{pmatrix} 1 & 0 & 7 & 5 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

Is $I \in \langle \mathcal{G} \rangle$?

$$A_1 A_2 A_3 A_4 = \begin{pmatrix} 1 & 0 & 11 & 2 \\ 0 & 1 & 0 & 8 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \in \mathrm{U}_1 \cap \langle \mathcal{G} \rangle$$

First layer cleared.

Identity Problem in $\mathrm{UT}(4,\mathbb{Z})$: Example

$$A_1 A_2 A_3 A_4 = \begin{pmatrix} 1 & 0 & 11 & 2 \\ 0 & 1 & 0 & 8 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \in \mathrm{U}_1 \cap \langle \mathcal{G} \rangle$$

$$A_2^{100} A_3^{100} A_1^{100} A_4^{100} = \begin{pmatrix} 1 & 0 & 6050 & 77350 \\ 0 & 1 & 0 & -4250 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \in \mathrm{U}_1 \cap \langle \mathcal{G} \rangle$$

$$A_2^{100} A_1^{100} A_3^{100} A_4^{100} = \begin{pmatrix} 1 & 0 & -3950 & 127350 \\ 0 & 1 & 0 & 5750 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \in \mathrm{U}_1 \cap \langle \mathcal{G} \rangle$$

$$A_4^{100} A_3^{100} A_2^{100} A_1^{100} = \begin{pmatrix} 1 & 0 & -3950 & -287650 \\ 0 & 1 & 0 & -4250 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \in \mathrm{U}_1 \cap \langle \mathcal{G} \rangle$$

Identity Problem in $\mathrm{UT}(4,\mathbb{Z})$

$$\begin{pmatrix}1&0&11&2\\0&1&0&8\\0&0&1&0\\0&0&0&1\end{pmatrix}^{1880000}\begin{pmatrix}1&0&6050&77350\\0&1&0&-4250\\0&0&1&0\\0&0&0&1\end{pmatrix}^{14443}\times$$
$$\begin{pmatrix}1&0&-3950&127350\\0&1&0&5750\\0&0&1&0\\0&0&0&1\end{pmatrix}^{16261}\begin{pmatrix}1&0&-3950&-287650\\0&1&0&-4250\\0&0&1&0\\0&0&0&1\end{pmatrix}^{11096}$$
$$=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix} \qquad (1)$$

Second layer cleared. So $I\in\langle\mathcal{G}\rangle$.

General approach

Step 1: Clear first layer using Linear Programming.
We have $B_1 B_2 \cdots B_m \in \mathsf{U}_1$.

Step 2: Clear second layer using permutation and powers of $B_1 B_2 \cdots B_m$.
For all $\sigma \in \mathsf{S}_m, t \in \mathbb{Z}_{>0}$, $B^t_{\sigma(1)} B^t_{\sigma(2)} \cdots B^t_{\sigma(m)} \in \mathsf{U}_1$.

Key: finding a characterization of the cone (in second layer) generated by the matrices $B^t_{\sigma(1)} B^t_{\sigma(2)} \cdots B^t_{\sigma(m)}$, when t, σ vary.

Identity Problem in $\mathrm{UT}(4, \mathbb{Z})$

$$B_{\sigma(1)}^{t} B_{\sigma(2)}^{t} \cdots B_{\sigma(m)}^{t} \xrightarrow{t \to \infty} \begin{pmatrix} 1 & 0 & t^2 D_\sigma & t^3 F_\sigma \\ 0 & 1 & 0 & t^2 E_\sigma \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

where $D_\sigma, E_\sigma, F_\sigma$ are polynomials in $\varphi(B_i), i = 1, \ldots, m$.

Identity Problem in $\mathrm{UT}(4, \mathbb{Z})$

$$B^t_{\sigma(1)} B^t_{\sigma(2)} \cdots B^t_{\sigma(m)} \xrightarrow{t \to \infty} \begin{pmatrix} 1 & 0 & t^2 D_\sigma & t^3 F_\sigma \\ 0 & 1 & 0 & t^2 E_\sigma \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

where $D_\sigma, E_\sigma, F_\sigma$ are polynomials in $\varphi(B_i), i = 1, \ldots, m$.

Example: write $\varphi(B_i) = (a_i, b_i, c_i), i = 1, \ldots, m$,

$$F_\sigma = \sum_{i<j<k} a_{\sigma(i)} b_{\sigma(j)} c_{\sigma(k)} + \frac{1}{2} \sum_{i<j} (a_{\sigma(i)} b_{\sigma(i)} c_{\sigma(j)} + a_{\sigma(i)} b_{\sigma(j)} c_{\sigma(j)}) + \frac{1}{6} \sum_{i=1}^{m} a_i b_i c_i,$$

Key theorem

Idea: $B^t_{\sigma(1)} B^t_{\sigma(2)} \cdots B^t_{\sigma(m)}$ asymptotically approaches $(t^2 D_\sigma, t^2 E_\sigma, t^3 F_\sigma)$.

Observation: $D_\sigma, E_\sigma, F_\sigma$ are polynomials in $a_i, b_i, c_i, i = 1, \ldots, m$. Where $\varphi(B_i) = (a_i, b_i, c_i)$.

Theorem

1. *If $\langle \varphi(B_1), \ldots, \varphi(B_m) \rangle$ has dimension 3, then $\langle (t^2 D_\sigma, t^2 E_\sigma, t^3 F_\sigma) \mid t \in \mathbb{Z}_{>0}, \sigma \in \mathsf{S}_m \rangle$ has dimension 3.*
2. *If $\langle \varphi(B_1), \ldots, \varphi(B_m) \rangle$ has dimension 2, and not orthogonal to any axis, then $\langle (t^2 D_\sigma, t^2 E_\sigma, t^3 F_\sigma) \mid t \in \mathbb{Z}_{>0}, \sigma \in \mathsf{S}_m \rangle$ has dimension 2 and contains the f-axis.*
3. *If $\langle \varphi(B_1), \ldots, \varphi(B_m) \rangle$ has dimension 2, and is orthogonal to some axis, then $\forall \sigma, F_\sigma = 0$, and $\dim \langle (D_\sigma, E_\sigma) \mid \sigma \in \mathsf{S}_m \rangle = 2$.*
4. *If $\langle \varphi(B_1), \ldots, \varphi(B_m) \rangle$ has dimension 1, then $\forall \sigma, D_\sigma = E_\sigma = F_\sigma = 0$.*

In short: $\varphi(\mathcal{G})$ determines (asymptotically) the shape of $\mathsf{U}_1 \cap \langle \mathcal{G} \rangle$.

Proof of the theorem: **computational algebraic geometry**.

Extensions

1. Identity Problem in $\mathsf{UT}(11, \mathbb{Q})$.
2. Identity Problem in nilpotent groups of class ≤ 10.
3. Identity Problem in $\mathsf{T}(2, \mathbb{Q})$.
4. Other problems in nilpotent groups (semigroup intersection etc.)

Extensions

1. Identity Problem in $\mathsf{UT}(11, \mathbb{Q})$.
2. Identity Problem in nilpotent groups of class ≤ 10.
3. Identity Problem in $\mathsf{T}(2, \mathbb{Q})$.
4. Other problems in nilpotent groups (semigroup intersection etc.)
5. Membership Problem in $\mathsf{UT}(4, \mathbb{Z})$?
6. Identity Problem in metabelian groups? $\mathbb{Z} \wr \mathbb{Z}$? solvable groups?