On the Identity Problem in unipotent matrix groups

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 : 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 : undecidable in $\mathbb{Z}^{6\times 6}$.

Michailova (1960s): is the following decidable?

Input: Set of element $\mathcal{G} = \{a_1, \ldots, a_K\}$ in a group G, target element T.
Output: Is T in the subgroup $\langle \mathcal{G} \rangle_{grp}$ generated by $\mathcal{G}$?

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 : undecidable in $\mathbb{Z}^{6\times 6}$.

Michailova (1960s): is the following decidable?

Input: Set of element $\mathcal{G} = \{a_1, \ldots, a_K\}$ in a group G, target element T.
Output: Is T in the subgroup $\langle \mathcal{G} \rangle_{grp}$ generated by $\mathcal{G}$?

Michailova : undecidable in $F_2 \times F_2 \hookrightarrow \mathbb{Z}^{4\times 4}$.

Membership problems

$\langle \mathcal{G} \rangle$: the *semigroup* generated by $\mathcal{G}$. $\langle \mathcal{G} \rangle_{grp}$: the *group* generated by $\mathcal{G}$.
Input: generator set $\mathcal{G} = \{A_1, \ldots, A_K\}$ and target T.

Definition (Semigroup Membership Problem)

Output: $T \in \langle \mathcal{G} \rangle$?

Membership problems

$\langle \mathcal{G} \rangle$: the *semigroup* generated by $\mathcal{G}$. $\langle \mathcal{G} \rangle_{grp}$: the *group* generated by $\mathcal{G}$.
Input: generator set $\mathcal{G} = \{A_1, \ldots, A_K\}$ and target T.

Definition (Semigroup Membership Problem)

Output: $T \in \langle \mathcal{G} \rangle$?

Definition (Group Membership Problem)

Output: $T \in \langle \mathcal{G} \rangle_{grp}$?

Membership problems

$\langle \mathcal{G} \rangle$: the *semigroup* generated by $\mathcal{G}$. $\langle \mathcal{G} \rangle_{grp}$: the *group* generated by $\mathcal{G}$.
Input: generator set $\mathcal{G} = \{A_1, \ldots, A_K\}$ and target T.

Definition (Semigroup Membership Problem)

Output: $T \in \langle \mathcal{G} \rangle$?

Definition (Group Membership Problem)

Output: $T \in \langle \mathcal{G} \rangle_{grp}$?

Semigroup structure / Invertibility-type problems:
Input: generator set $\mathcal{G} = \{A_1, \ldots, A_K\}$.

Definition (Identity Problem)

Output: $I \in \langle \mathcal{G} \rangle$?

Membership problems

$\langle \mathcal{G} \rangle$: the *semigroup* generated by $\mathcal{G}$. $\langle \mathcal{G} \rangle_{grp}$: the *group* generated by $\mathcal{G}$.
Input: generator set $\mathcal{G} = \{A_1, \ldots, A_K\}$ and target T.

Definition (Semigroup Membership Problem)

Output: $T \in \langle \mathcal{G} \rangle$?

Definition (Group Membership Problem)

Output: $T \in \langle \mathcal{G} \rangle_{grp}$?

Semigroup structure / Invertibility-type problems:
Input: generator set $\mathcal{G} = \{A_1, \ldots, A_K\}$.

Definition (Identity Problem)

Output: $I \in \langle \mathcal{G} \rangle$?

Definition (Group Problem)

Output: $\langle \mathcal{G} \rangle = \langle \mathcal{G} \rangle_{grp}$?

Known results

Known results on **matrix groups**.

group types	Group Mem. $T \in \langle \mathcal{G} \rangle_{grp}$?	Semigroup Mem. $T \in \langle \mathcal{G} \rangle$?	Invertibility $I \in \langle \mathcal{G} \rangle$? $\langle \mathcal{G} \rangle = \langle \mathcal{G} \rangle_{grp}$
Commutative	PTIME	NP-complete	PTIME
Nilpotent	Decidable	Undecidable	?
Solvable	Decidable	Undecidable	?
$\mathrm{SL}(2, \mathbb{Z})$	PTIME	Decidable	NP-complete
$\mathrm{SL}(3, \mathbb{Z})$	?	?	?
$\mathrm{SL}(4, \mathbb{Z})$	Undecidable	Undecidable	Undecidable

Known results

Known results on **matrix groups**.

group types	Group Mem. $T \in \langle \mathcal{G} \rangle_{grp}$?	Semigroup Mem. $T \in \langle \mathcal{G} \rangle$?	Invertibility $I \in \langle \mathcal{G} \rangle$? $\langle \mathcal{G} \rangle = \langle \mathcal{G} \rangle_{grp}$?
Commutative	PTIME	NP-complete	PTIME
Nilpotent	Decidable	Undecidable	PTIME for class ≤ 10
Solvable	Decidable	Undecidable	?
$\mathsf{SL}(2, \mathbb{Z})$	PTIME	Decidable	NP-complete
$\mathsf{SL}(3, \mathbb{Z})$	?	?	?
$\mathsf{SL}(4, \mathbb{Z})$	Undecidable	Undecidable	Undecidable

Nilpotent groups

Definition

The **lower central series** of a group G is the sequence of subgroups

$$G = G_1 \geq G_2 \geq G_3 \geq \cdots ,$$

in which $G_k = [G, G_{k-1}]$. ($[G, H]$ is the group generated by $ghg^{-1}h^{-1}, g \in G, h \in H$.)

Nilpotent groups

Definition

The **lower central series** of a group G is the sequence of subgroups

$$G = G_1 \geq G_2 \geq G_3 \geq \cdots,$$

in which $G_k = [G, G_{k-1}]$. ($[G, H]$ is the group generated by $ghg^{-1}h^{-1}, g \in G, h \in H$.)

G is **nilpotent** if $G_{d+1} = \{I\}$ for some d. The smallest such d is the **nilpotency class** of G.

Nilpotent groups

Definition

The **lower central series** of a group G is the sequence of subgroups

$$G = G_1 \geq G_2 \geq G_3 \geq \cdots,$$

in which $G_k = [G, G_{k-1}]$. ($[G, H]$ is the group generated by $ghg^{-1}h^{-1}, g \in G, h \in H$.)

G is **nilpotent** if $G_{d+1} = \{I\}$ for some d. The smallest such d is the **nilpotency class** of G.

Example

$G = \mathrm{UT}(3, \mathbb{Q})$ has nilpotency class two:

$$G_1 = \left\{ \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} \right\} \geq G_2 = \left\{ \begin{pmatrix} 1 & 0 & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\} \geq G_3 = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\}$$

Nilpotent groups

Definition

The **lower central series** of a group G is the sequence of subgroups

$$G = G_1 \geq G_2 \geq G_3 \geq \cdots ,$$

in which $G_k = [G, G_{k-1}]$. ($[G, H]$ is the group generated by $ghg^{-1}h^{-1}, g \in G, h \in H$.)

G is **nilpotent** if $G_{d+1} = \{I\}$ for some d. The smallest such d is the **nilpotency class** of G.

Example

$G = \mathrm{UT}(3, \mathbb{Q})$ has nilpotency class two:

$$G_1 = \left\{ \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} \right\} \geq G_2 = \left\{ \begin{pmatrix} 1 & 0 & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\} \geq G_3 = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\}$$

$\mathrm{UT}(n, \mathbb{Q})$ **has nilpotency class** $n-1$**, so does** $\mathrm{UT}(n, \mathbb{Q})^k$**.**

Embedding in $\mathrm{UT}(n, \mathbb{Q})$

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

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

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

Theorem

Any finitely generated nilpotent group G admits an embedding $G \hookrightarrow A \times \mathrm{UT}(n, \mathbb{Q})$, where A is finite.

Hence: we can focus on $\mathrm{UT}(n, \mathbb{Q})$!

Main results

Theorem

For any group $G \leq \mathrm{UT}(n, \mathbb{Q})$ of nilpotency class ≤ 10, the Identity Problem and the Group Problem in G is decidable in PTIME.

Main results

Theorem

For any group $G \leq \mathrm{UT}(n, \mathbb{Q})$ *of nilpotency class* ≤ 10*, the Identity Problem and the Group Problem in* G *is decidable in PTIME.*

Corollary

The Identity Problem in $\mathrm{UT}(11, \mathbb{Q})^k$ *is decidable in PTIME.*

We can replace $\mathbb{Q}$ by any algebraic number field.

Main results

Theorem

For any group $G \leq \mathrm{UT}(n, \mathbb{Q})$ of nilpotency class ≤ 10, the Identity Problem and the Group Problem in G is decidable in PTIME.

Corollary

The Identity Problem in $\mathrm{UT}(11, \mathbb{Q})^k$ is decidable in PTIME.

We can replace $\mathbb{Q}$ by any algebraic number field.

Corollary

The Identity Problem in any nilpotent group of class ≤ 10 are decidable.

Definition ($\mathfrak{u}(n)$)

Define $\mathfrak{u}(n)$ to be the $\mathbb{Q}$-linear space of n by n upper triangular rational matrices with *zeros* on the diagonal.

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

$$\log : \mathrm{UT}(n, \mathbb{Q}) \to \mathfrak{u}(n), \quad A \mapsto \sum_{k=1}^{n} \frac{(-1)^{k-1}}{k}(A - I)^k$$

and

$$\exp : \mathfrak{u}(n) \to \mathrm{UT}(n, \mathbb{Q}), \quad X \mapsto \sum_{k=0}^{n} \frac{1}{k!} X^k$$

are inverse of one another. In particular, $\log I = 0$ and $\exp(0) = I$.

Lie group - Lie algebra

$$\log : \mathrm{UT}(n, \mathbb{Q}) \to \mathfrak{u}(n)$$

and

$$\exp : \mathfrak{u}(n) \to \mathrm{UT}(n, \mathbb{Q})$$

are inverse of one another.

$$\textbf{group } \mathrm{UT}(n, \mathbb{Q}) \underset{\exp}{\overset{\log}{\rightleftarrows}} \textbf{ linear space } \mathfrak{u}(n).$$

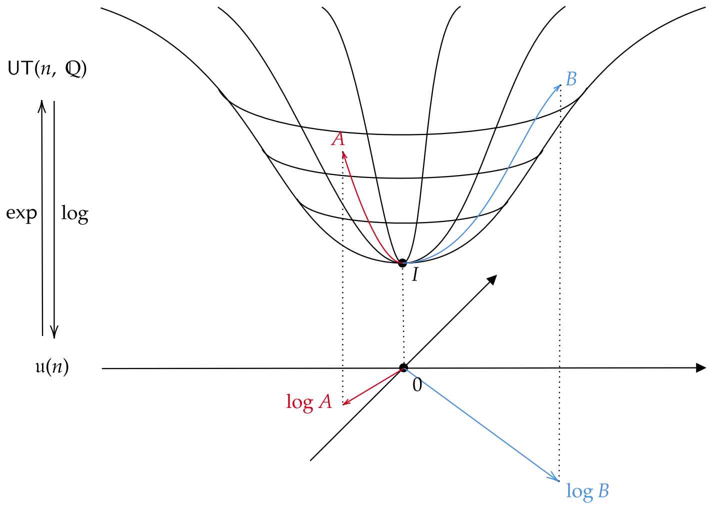
Example

$$\log \begin{pmatrix} 1 & 1 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 3 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix} - \frac{1}{2} \begin{pmatrix} 0 & 1 & 3 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 1 & 2 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix}$$

$$exp \begin{pmatrix} 0 & 1 & 2 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix} = I + \begin{pmatrix} 0 & 1 & 2 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix} + \frac{1}{2} \begin{pmatrix} 0 & 1 & 2 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 1 & 1 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$$

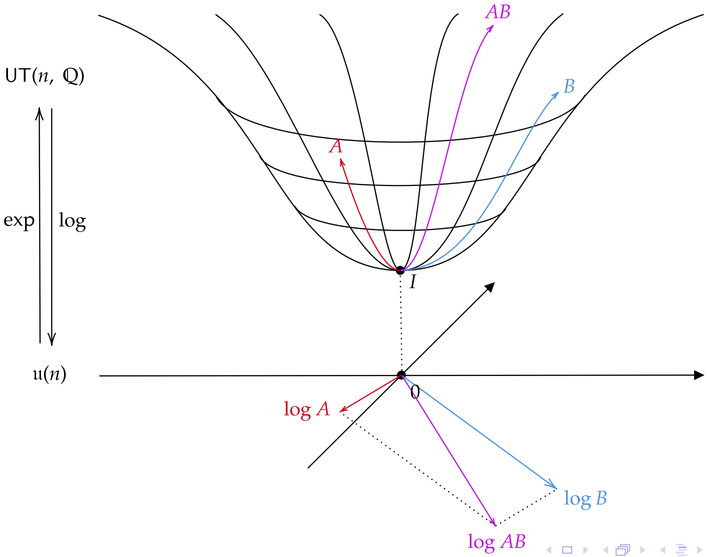
Lie group - Lie algebra : illustration

$$\log\colon \mathsf{UT}(n, \mathbb{Q}) \xrightarrow{\text{“projection”}} \mathfrak{u}(n).$$



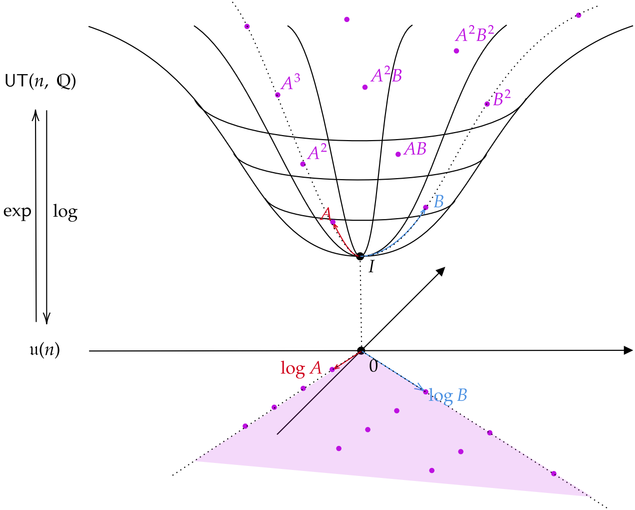
Lie group - Lie algebra : commutative case

When A and B **commute** ($AB = BA$), we have $\log AB = \log A + \log B$.



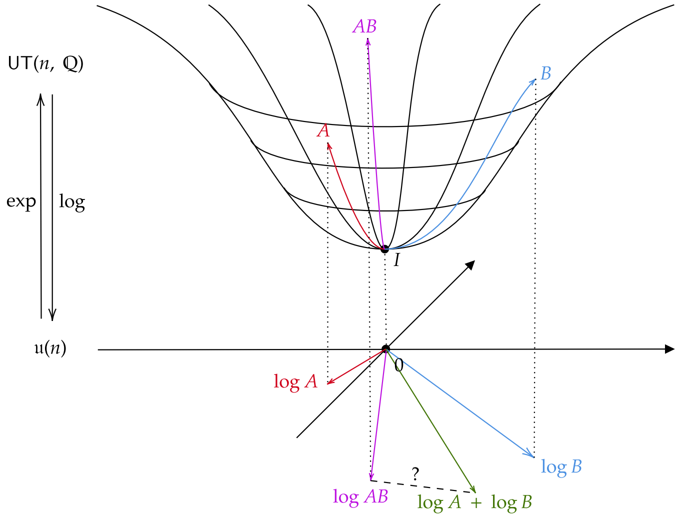
$\log: \text{ group } \xrightarrow{\text{"projection"}} \text{ linear space }.$

$\log: \text{ semigroup } \xrightarrow{\text{"projection"}} \text{ cone }.$



Lie group - Lie algebra : non-commutative case

If A and B do **not** commute ($AB \neq BA$), then $\log AB \neq \log A + \log B$.



Baker-Campbell-Hausdorff formula

$$\begin{aligned}\log(AB) = \log A + \log B + \frac{1}{2}[\log A, \log B] \\ + \frac{1}{12}[\log A, [\log A, \log B]] - \frac{1}{12}[\log B, [\log A, \log B]] + \cdots\end{aligned}$$

where $[X, Y] := XY - YX$ is the **Lie bracket**.

Baker-Campbell-Hausdorff formula

$$\log(AB) = \log A + \log B + \frac{1}{2}[\log A, \log B] + \frac{1}{12}[\log A, [\log A, \log B]] - \frac{1}{12}[\log B, [\log A, \log B]] + \cdots$$

where $[X, Y] := XY - YX$ is the **Lie bracket**.

Some properties of the Lie bracket:

1. Bilinear: $[X_1 + X_2, Y] = [X_1, Y] + [X_2, Y]$.
2. Anticommutative: $[X, Y] = -[Y, X]$.
3. Jacobi Identity: $[X, [Y, Z]] + [Y, [X, Z]] + [Z, [X, Y]] = 0$.

Lie brackets

Definition

Given a set $\mathcal{H} \subseteq \mathfrak{u}(n)$ and $k \geq 2$, define

$$[\mathcal{H}]_k := \left\{ [\ldots[[X_1, X_2], X_3], \ldots, X_k] \;\middle|\; X_1, X_2, \ldots, X_k \in \mathcal{H} \right\}.$$

the set of all "left bracketing" of length k of elements in $\mathcal{H}$.

Lie brackets

Definition

Given a set $\mathcal{H} \subseteq \mathfrak{u}(n)$ and $k \geq 2$, define

$$[\mathcal{H}]_k := \left\{ [\ldots[[X_1, X_2], X_3], \ldots, X_k] \;\middle|\; X_1, X_2, \ldots, X_k \in \mathcal{H} \right\}.$$

the set of all "left bracketing" of length k of elements in $\mathcal{H}$.

Any k-iteration of Lie brackets of elements in $\mathcal{H}$ can be written as a linear combination of elements in $[\mathcal{H}]_k$:

$$\begin{aligned}
[[X_1, X_2], [X_3, X_4]] &\overset{J.I.}{=} -[[X_2, [X_3, X_4]], X_1] - [[[X_3, X_4], X_1], X_2] \\
&\overset{AC}{=} [[[X_3, X_4], X_2], X_1] - [[[X_3, X_4], X_1], X_2].
\end{aligned}$$

Baker-Campbell-Hausdorff formula

Suppose $G \leq \mathrm{UT}(n, \mathbb{Q})$ has nilpotency class d.

$$\log(B_1 \cdots B_m) = \sum_{i=1}^{m} \log B_i + \sum_{k=2}^{d} H_k(\log B_1, \ldots, \log B_m), \tag{1}$$

where $H_k(\log B_1, \ldots, \log B_m), k = 2, 3, \ldots$, can be expressed as $\mathbb{Q}$-linear combinations of elements in $[\{\log B_1, \ldots, \log B_m\}]_k$.

Baker-Campbell-Hausdorff formula

Suppose $G \leq \mathrm{UT}(n, \mathbb{Q})$ has nilpotency class d.

$$\log(B_1 \cdots B_m) = \sum_{i=1}^{m} \log B_i + \sum_{k=2}^{d} H_k(\log B_1, \ldots, \log B_m), \qquad (1)$$

where $H_k(\log B_1, \ldots, \log B_m), k = 2, 3, \ldots$, can be expressed as $\mathbb{Q}$-linear combinations of elements in $[\{\log B_1, \ldots, \log B_m\}]_k$.

Some first terms ($C_i = \log B_i$):

$$H_2(C_1, \ldots, C_m) = \frac{1}{2} \sum_{i<j} [C_i, C_j]$$

$$H_3(C_1, \ldots, C_m) = \sum_{i<j<k} \left(\frac{1}{3}[C_i, [C_j, C_k]] + \frac{1}{6}[[C_i, C_k], C_j] \right) + \frac{1}{12} \sum_{i<j} ([C_i, [C_i, C_j]] + [[C_i, C_j], C_j])$$

Expression for H_k: *Dynkin formula*

Filtered Lie algebra

For any set $\mathcal{H} \subseteq \log G$, denote

$$\mathfrak{L}_{\geq k}(\mathcal{H}) := \left\langle \bigcup_{i \geq k} [\mathcal{H}]_i \right\rangle_{\mathbb{Q}} .$$

the linear space spanned by the set of all "left bracketing" of length **at least** k of elements in $\mathcal{H}$.

Theorem (Mal'cev correspondence)

G has nilpotency class $\leq d$ **iff** $\mathfrak{L}_{\geq d+1}(G) = \{0\}$.

Filtered Lie algebra

For any set $\mathcal{H} \subseteq \log G$, denote

$$\mathfrak{L}_{\geq k}(\mathcal{H}) \coloneqq \left\langle \bigcup_{i \geq k} [\mathcal{H}]_i \right\rangle_{\mathbb{Q}}.$$

the linear space spanned by the set of all "left bracketing" of length **at least** k of elements in $\mathcal{H}$.

Theorem (Mal'cev correspondence)

G has nilpotency class $\leq d$ **iff** $\mathfrak{L}_{\geq d+1}(G) = \{0\}$.

Property: if G has nilpotency class d, then

1. $\mathfrak{L}_{\geq 1}(\mathcal{H}) \supseteq \mathfrak{L}_{\geq 2}(\mathcal{H}) \supseteq \cdots \supseteq \mathfrak{L}_{\geq d+1}(\mathcal{H}) = \{0\}$.
2. $[\mathfrak{L}_{\geq i}(\mathcal{H}), \mathfrak{L}_{\geq j}(\mathcal{H})] \subseteq \mathfrak{L}_{\geq i+j}(\mathcal{H})$.

Filtered Lie algebra

For any set $\mathcal{H} \subseteq \log G$, denote

$$\mathfrak{L}_{\geq k}(\mathcal{H}) := \left\langle \bigcup_{i \geq k} [\mathcal{H}]_i \right\rangle_{\mathbb{Q}}.$$

the linear space spanned by the set of all "left bracketing" of length **at least** k of elements in $\mathcal{H}$.

Theorem (Mal'cev correspondence)

*G has nilpotency class $\leq d$ **iff** $\mathfrak{L}_{\geq d+1}(G) = \{0\}$.*

Property: if G has nilpotency class d, then

1. $\mathfrak{L}_{\geq 1}(\mathcal{H}) \supseteq \mathfrak{L}_{\geq 2}(\mathcal{H}) \supseteq \cdots \supseteq \mathfrak{L}_{\geq d+1}(\mathcal{H}) = \{0\}$.
2. $[\mathfrak{L}_{\geq i}(\mathcal{H}), \mathfrak{L}_{\geq j}(\mathcal{H})] \subseteq \mathfrak{L}_{\geq i+j}(\mathcal{H})$.

In particular:

$$\sum_{k=2}^{n} H_k(\log B_1, \dots, \log B_m) \in \mathfrak{L}_{\geq 2}(\{\log B_1 \cdots \log B_m\})$$

Example

Example

$$\{\log A, \log B\} = \log \mathcal{G} \quad \subseteq \quad \mathfrak{u}(n) = \begin{pmatrix} 0 & * & * & * \\ 0 & 0 & * & * \\ 0 & 0 & 0 & * \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

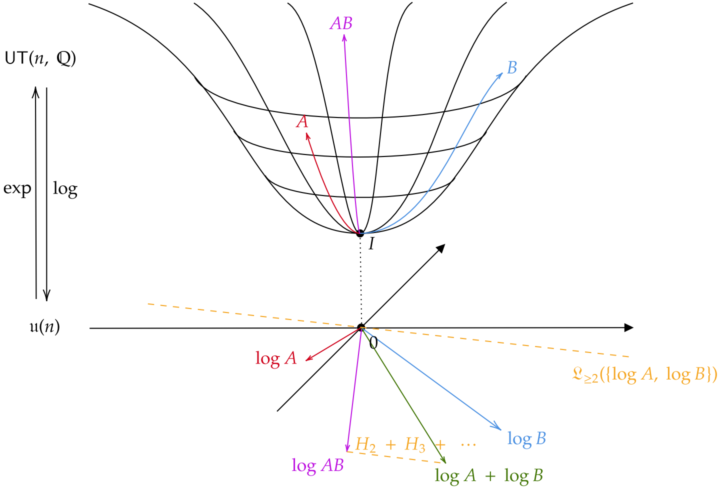
$$H_2(\log A, \log B) \in \mathfrak{L}_2(\log \mathcal{G}) \quad \subseteq \quad \mathfrak{L}_{\geq 2}(\mathfrak{u}(n)) = \begin{pmatrix} 0 & 0 & * & * \\ 0 & 0 & 0 & * \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$H_3(\log A, \log B) \in \mathfrak{L}_3(\log \mathcal{G}) \quad \subseteq \quad \mathfrak{L}_{\geq 3}(\mathfrak{u}(n)) = \begin{pmatrix} 0 & 0 & 0 & * \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$H_4(\log A, \log B) \in \mathfrak{L}_4(\log \mathcal{G}) \quad \subseteq \quad \mathfrak{L}_{\geq 4}(\mathfrak{u}(n)) = \mathbf{0}$$

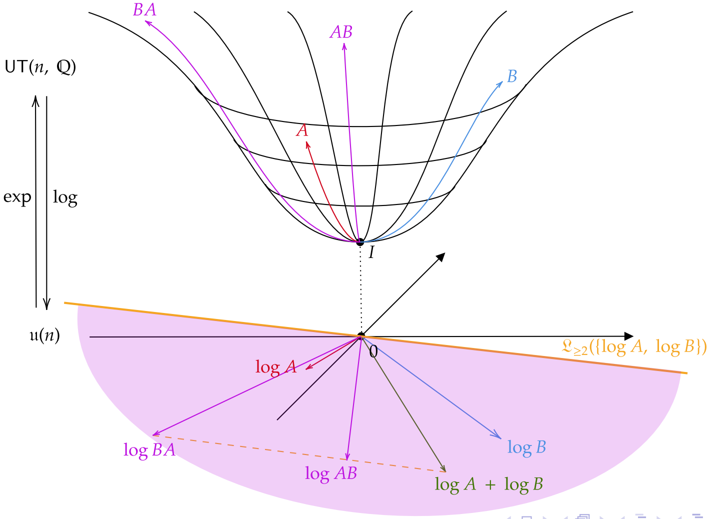
Lie group - Lie algebra : non-commutative case

We have $\log AB \in \log A + \log B + \mathfrak{L}_2(\{\log A, \log B\})$!



Lie group - Lie algebra : non-commutative case

$\log\langle A, B\rangle$ falls in the purple area generated by $\log A$, $\log B$ and $\mathfrak{L}_2(\{\log A, \log B\})$.



Key theorem

$$\log w = \log(B_1 \cdots B_m) = \underbrace{\sum_{i=1}^{K} \ell_i \log A_i}_{\text{linear form in } \boldsymbol{\ell}} + \underbrace{\sum_{k=2}^{d} H_k(\log B_1, \ldots, \log B_m)}_{\in \mathfrak{L}_{\geq 2}(\{\log B_1, \ldots, \log B_m\})}$$

Theorem (Very technical theorem)

Let $\mathcal{G} = \{A_1, \ldots, A_K\}$ *be such that* $\mathfrak{L}_{\geq 11}(\log \mathcal{G}) = \{0\}$.

1. $\langle \mathcal{G} \rangle = \langle \mathcal{G} \rangle_{grp}$ *if and only if there exist strictly positive integers* $\ell_i \in \mathbb{Z}_{>0}$ *for* $i = 1, \ldots, K$, *such that*
$$\sum_{i=1}^{K} \ell_i \log A_i \in \mathfrak{L}_{\geq 2}(\log \mathcal{G}).$$
2. $I \in \langle \mathcal{G} \rangle$ *if and only if there exist a non-empty subset* $\mathcal{H} \subseteq \mathcal{G}$ *and strictly positive integers* $\ell_i \in \mathbb{Z}_{>0}$ *for all* i *with* $A_i \in \mathcal{H}$, *such that*
$$\sum_{A_i \in \mathcal{H}} \ell_i \log A_i \in \mathfrak{L}_{\geq 2}(\log \mathcal{H}).$$

Key theorem

$$\log w = \log(B_1 \cdots B_m) = \underbrace{\sum_{i=1}^{K} \ell_i \log A_i}_{\text{linear form in } \boldsymbol{\ell}} + \underbrace{\sum_{k=2}^{d} H_k(\log B_1, \ldots, \log B_m)}_{\in \mathfrak{L}_{\geq 2}(\{\log B_1, \ldots, \log B_m\})}$$

Theorem (Very technical theorem)

Let $\mathcal{G} = \{A_1, \ldots, A_K\}$ be such that $\mathfrak{L}_{\geq 11}(\log \mathcal{G}) = \{0\}$.

1. $\langle \mathcal{G} \rangle = \langle \mathcal{G} \rangle_{grp}$ *if and only if there exist strictly positive integers* $\ell_i \in \mathbb{Z}_{>0}$ *for* $i = 1, \ldots, K$, *such that*
$$\sum_{i=1}^{K} \ell_i \log A_i \in \mathfrak{L}_{\geq 2}(\log \mathcal{G}).$$
2. $I \in \langle \mathcal{G} \rangle$ *if and only if there exist a non-empty subset* $\mathcal{H} \subseteq \mathcal{G}$ *and strictly positive integers* $\ell_i \in \mathbb{Z}_{>0}$ *for all* i *with* $A_i \in \mathcal{H}$, *such that*
$$\sum_{A_i \in \mathcal{H}} \ell_i \log A_i \in \mathfrak{L}_{\geq 2}(\log \mathcal{H}).$$

Key to the proof: understanding H_k using *Dynkin's formula*.
Tools: Lie algebra + computer algebra software.

$\mathcal{G} = \{A_1, A_2, A_3, A_4\}$.

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

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

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

Identity Problem in $UT(4, \mathbb{Q})$: An example

$\mathcal{G} = \{A_1, A_2, A_3, A_4\}$.

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

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

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

$$\mathfrak{L}_{\geq 1}(\log \mathcal{G}) \subseteq \left\{ \begin{pmatrix} 0 & * & * & * \\ 0 & 0 & * & * \\ 0 & 0 & 0 & * \\ 0 & 0 & 0 & 0 \end{pmatrix} \right\}, \mathfrak{L}_{\geq 2}(\log \mathcal{G}) \subseteq \left\{ \begin{pmatrix} 0 & 0 & * & * \\ 0 & 0 & 0 & * \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \right\}$$

Identity Problem in $\mathrm{UT}(4, \mathbb{Q})$: An example

$$\log A_1 = \begin{pmatrix} 0 & 1 & \frac{3}{2} & -\frac{1}{6} \\ 0 & 0 & 1 & \frac{5}{2} \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \log A_2 = \begin{pmatrix} 0 & -1 & 4 & -\frac{3}{2} \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

$$\log A_3 = \begin{pmatrix} 0 & 0 & -2 & 0 \\ 0 & 0 & -1 & 3 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \log A_4 = \begin{pmatrix} 0 & 0 & 7 & \frac{17}{2} \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

Is $0 \in \log\langle\mathcal{G}\rangle$?

$$\log A_1 = \begin{pmatrix} 0 & 1 & \frac{3}{2} & -\frac{1}{6} \\ 0 & 0 & 1 & \frac{5}{2} \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \log A_2 = \begin{pmatrix} 0 & -1 & 4 & -\frac{3}{2} \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

$$\log A_3 = \begin{pmatrix} 0 & 0 & -2 & 0 \\ 0 & 0 & -1 & 3 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \log A_4 = \begin{pmatrix} 0 & 0 & 7 & \frac{17}{2} \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

Is $0 \in \log\langle\mathcal{G}\rangle$?
Let $\boldsymbol{\ell} = (1,1,1,1)$, then $\sum_{i=1}^{4} \ell_i \log A_i \in \mathfrak{L}_{\geq 2}(\log \mathcal{G})$.

$$\log(A_1 A_2 A_3 A_4) = \sum_{i=1}^{4} \log A_i + H_2(\log A_1, \dots, \log A_4) + H_3(\log A_1, \dots, \log A_4)$$

$$= \begin{pmatrix} 0 & 0 & 11 & 2 \\ 0 & 0 & 0 & 8 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \in \mathfrak{L}_{\geq 2}(\log \mathcal{G})$$

Identity Problem in $\mathsf{UT}(4,\mathbb{Q})$: An example

$$\log A_1' = \log A_1 A_2 A_3 A_4 = \begin{pmatrix} 0 & 0 & 11 & 2 \\ 0 & 0 & 0 & 8 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \in \mathfrak{L}_{\geq 2}(\log \mathcal{G})$$

$$\log A_2' = \log A_2^{100} A_3^{100} A_1^{100} A_4^{100} = \begin{pmatrix} 0 & 0 & 6050 & 77350 \\ 0 & 0 & 0 & -4250 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \in \mathfrak{L}_{\geq 2}(\log \mathcal{G})$$

$$\log A_3' = \log A_2^{100} A_1^{100} A_3^{100} A_4^{100} = \begin{pmatrix} 0 & 0 & -3950 & 127350 \\ 0 & 0 & 0 & 5750 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \in \mathfrak{L}_{\geq 2}(\log \mathcal{G})$$

$$\log A_4' = \log A_4^{100} A_3^{100} A_2^{100} A_1^{100} = \begin{pmatrix} 0 & 0 & -3950 & -287650 \\ 0 & 0 & 0 & -4250 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \in \mathfrak{L}_{\geq 2}(\log \mathcal{G})$$

Observation:

$$\mathfrak{L}_{\geq 2}(\mathfrak{L}_{\geq 2}(\log \mathcal{G})) = \{0\}.$$

Hence

$$[\log A_i', \log A_j'] = 0.$$

$$\begin{aligned}
&\log({A_1'}^{1880000} {A_2'}^{14443} {A_3'}^{16261} {A_4'}^{11096}) \\
=&1880000 \log A_1' + 14443 \log A_2' + 16261 \log A_3' + 11096 \log A_4' \\
=&1880000 \cdot \begin{pmatrix} 0 & 0 & 11 & 2 \\ 0 & 0 & 0 & 8 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} + 14443 \cdot \begin{pmatrix} 0 & 0 & 6050 & 77350 \\ 0 & 0 & 0 & -4250 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \\
&+ 16261 \cdot \begin{pmatrix} 0 & 0 & -3950 & 127350 \\ 0 & 0 & 0 & 5750 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} + 11096 \cdot \begin{pmatrix} 0 & 0 & -3950 & -287650 \\ 0 & 0 & 0 & -4250 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \\
=& \, 0
\end{aligned}$$

So $0 \in \log\langle \mathcal{G} \rangle$, $I \in \langle \mathcal{G} \rangle$.

Takeaway, future work

Takeway:

1. Solving problems in Lie algebra could be easier than solving problems in (semi)groups.
2. Semigroup generated by $\mathcal{G}$ is closely related to the cone generated by $\log \mathcal{G}$.
3. The Identity Problem is easier than the Membership Problem, because it is partially a "local" property.
4. The key to the Identity Problem in $\mathsf{UT}(n, \mathbb{Q})$ is the structure of H_k.

Takeaway, future work

Takeway:

1. Solving problems in Lie algebra could be easier than solving problems in (semi)groups.
2. Semigroup generated by $\mathcal{G}$ is closely related to the cone generated by $\log \mathcal{G}$.
3. The Identity Problem is easier than the Membership Problem, because it is partially a "local" property.
4. The key to the Identity Problem in $\mathsf{UT}(n, \mathbb{Q})$ is the structure of H_k.

Future work:

1. What about polycyclic/solvable groups? (It's doable for $\mathsf{T}(2, \mathbb{Q})$!)
2. Non-solvable groups?
3. Any chance to solve the Membership Problem in low dimensions?