The Identity Problem for nilpotent groups of bounded class

Ruiwen Dong

Saarland University

January 2024

Membership Problems

Markov (1940s): is *Semigroup Membership* decidable?

Definition (Semigroup Membership)

Input: Set of square matrices $S = \{A_1, \ldots, A_K\}$, target matrix T.
Output: Is there a sequence $A_{i_1}, A_{i_2}, \ldots, A_{i_m} \in S$, s.t. $A_{i_1} A_{i_2} \cdots A_{i_m} = T$?

Membership Problems

Markov (1940s): is *Semigroup Membership* decidable?

Definition (Semigroup Membership)

Input: Set of square matrices $S = \{A_1, \ldots, A_K\}$, target matrix T.
Output: Is there a sequence $A_{i_1}, A_{i_2}, \ldots, A_{i_m} \in S$, s.t. $A_{i_1} A_{i_2} \cdots A_{i_m} = T$?

Theorem (Mikhailova 1966)

Semigroup Membership is undecidable, even when $S \subseteq \mathrm{SL}(4, \mathbb{Z})$.

Membership Problems

Markov (1940s): is *Semigroup Membership* decidable?

Definition (Semigroup Membership)

Input: Set of square matrices $S = \{A_1, \dots, A_K\}$, target matrix T.
Output: Is there a sequence $A_{i_1}, A_{i_2}, \dots, A_{i_m} \in S$, s.t. $A_{i_1} A_{i_2} \cdots A_{i_m} = T$?

Theorem (Mikhailova 1966)

Semigroup Membership is undecidable, even when $S \subseteq \mathrm{SL}(4, \mathbb{Z})$.

Choffrut, Karhumäki (2000s): is *Identity Problem* decidable?

Definition (Identity Problem)

Input: Set of square matrices $S = \{A_1, \dots, A_K\}$.
Output: Is there a sequence $A_{i_1}, A_{i_2}, \dots, A_{i_m} \in S$, s.t. $A_{i_1} A_{i_2} \cdots A_{i_m} = I$ (the identity matrix)?

Markov (1940s): is *Semigroup Membership* decidable?

Definition (Semigroup Membership)

Input: Set of square matrices $S = \{A_1, \dots, A_K\}$, target matrix T.
Output: Is there a sequence $A_{i_1}, A_{i_2}, \dots, A_{i_m} \in S$, s.t. $A_{i_1} A_{i_2} \cdots A_{i_m} = T$?

Theorem (Mikhailova 1966)

Semigroup Membership is undecidable, even when $S \subseteq \mathrm{SL}(4, \mathbb{Z})$.

Choffrut, Karhumäki (2000s): is *Identity Problem* decidable?

Definition (Identity Problem)

Input: Set of square matrices $S = \{A_1, \dots, A_K\}$.
Output: Is there a sequence $A_{i_1}, A_{i_2}, \dots, A_{i_m} \in S$, s.t. $A_{i_1} A_{i_2} \cdots A_{i_m} = I$ (the identity matrix)?

Theorem (Bell, Potapov 2010)

Identity Problem is undecidable, even when $S \subseteq \mathrm{SL}(4, \mathbb{Z})$.

Membership Problems has been proven to be decidable in groups with additional structures:

Theorem (Babai et al. 1996)

Semigroup Membership is decidable (and NP) for commutative matrices.
Identity Problem is decidable (and PTIME) for commutative matrices.

"proof": suppose we work with $(\mathbb{Z}^n, +)$ instead of multiplication of commutative matrices. Suppose $S = \{a_1, \ldots, a_K\} \subset \mathbb{Z}^n$ and $t \in \mathbb{Z}^n$.

Membership Problems has been proven to be decidable in groups with additional structures:

Theorem (Babai et al. 1996)

Semigroup Membership is decidable (and NP) for commutative matrices.
Identity Problem is decidable (and PTIME) for commutative matrices.

"proof": suppose we work with $(\mathbb{Z}^n, +)$ instead of multiplication of commutative matrices. Suppose $S = \{a_1, \ldots, a_K\} \subset \mathbb{Z}^n$ and $t \in \mathbb{Z}^n$.

t is in semigroup generated by $S \iff$ there exist $n_1, \ldots, n_K \in \mathbb{N}$, such that $n_1 \cdot a_1 + \cdots + n_K \cdot a_K = t$.

Membership Problems has been proven to be decidable in groups with additional structures:

Theorem (Babai et al. 1996)

Semigroup Membership is decidable (and NP) for commutative matrices.
Identity Problem is decidable (and PTIME) for commutative matrices.

"proof": suppose we work with $(\mathbb{Z}^n, +)$ instead of multiplication of commutative matrices. Suppose $S = \{a_1, \dots, a_K\} \subset \mathbb{Z}^n$ and $t \in \mathbb{Z}^n$.

t is in semigroup generated by $S \iff$ there exist $n_1, \dots, n_K \in \mathbb{N}$, such that $n_1 \cdot a_1 + \cdots + n_K \cdot a_K = t$.

Solving linear equations over $\mathbb{N}$: NP (integer programming).

Membership Problems has been proven to be decidable in groups with additional structures:

Theorem (Babai et al. 1996)

Semigroup Membership is decidable (and NP) for commutative matrices.
Identity Problem is decidable (and PTIME) for commutative matrices.

"proof": suppose we work with $(\mathbb{Z}^n, +)$ instead of multiplication of commutative matrices. Suppose $S = \{a_1, \ldots, a_K\} \subset \mathbb{Z}^n$ and $t \in \mathbb{Z}^n$.

t is in semigroup generated by $S \iff$ there exist $n_1, \ldots, n_K \in \mathbb{N}$, such that $n_1 \cdot a_1 + \cdots + n_K \cdot a_K = t$.

Solving linear equations over $\mathbb{N}$: NP (integer programming).

---

e is in semigroup generated by $S \iff$ there exist $n_1, \ldots, n_K \in \mathbb{N}$, not all zero, such that $n_1 \cdot a_1 + \cdots + n_K \cdot a_K = 0^n$.

Membership Problems has been proven to be decidable in groups with additional structures:

Theorem (Babai et al. 1996)

Semigroup Membership is decidable (and NP) for commutative matrices.
Identity Problem is decidable (and PTIME) for commutative matrices.

"proof": suppose we work with $(\mathbb{Z}^n, +)$ instead of multiplication of commutative matrices. Suppose $S = \{a_1, \ldots, a_K\} \subset \mathbb{Z}^n$ and $t \in \mathbb{Z}^n$.

t is in semigroup generated by $S \iff$ there exist $n_1, \ldots, n_K \in \mathbb{N}$, such that $n_1 \cdot a_1 + \cdots + n_K \cdot a_K = t$.

Solving linear equations over $\mathbb{N}$: NP (integer programming).

---

e is in semigroup generated by $S \iff$ there exist $n_1, \ldots, n_K \in \mathbb{N}$, not all zero, such that $n_1 \cdot a_1 + \cdots + n_K \cdot a_K = 0^n$. $\iff$ there exist $n_1, \ldots, n_K \in \mathbb{Q}_{\geq 0}$, not all zero, such that $n_1 \cdot a_1 + \cdots + n_K \cdot a_K = 0^n$.

Membership Problems has been proven to be decidable in groups with additional structures:

Theorem (Babai et al. 1996)

Semigroup Membership is decidable (and NP) for commutative matrices.
Identity Problem is decidable (and PTIME) for commutative matrices.

"proof": suppose we work with $(\mathbb{Z}^n, +)$ instead of multiplication of commutative matrices. Suppose $S = \{a_1, \ldots, a_K\} \subset \mathbb{Z}^n$ and $t \in \mathbb{Z}^n$.

t is in semigroup generated by $S \iff$ there exist $n_1, \ldots, n_K \in \mathbb{N}$, such that $n_1 \cdot a_1 + \cdots + n_K \cdot a_K = t$.

Solving linear equations over $\mathbb{N}$: NP (integer programming).

---

e is in semigroup generated by $S \iff$ there exist $n_1, \ldots, n_K \in \mathbb{N}$, not all zero, such that $n_1 \cdot a_1 + \cdots + n_K \cdot a_K = 0^n$. $\iff$ there exist $n_1, \ldots, n_K \in \mathbb{Q}_{\geq 0}$, not all zero, such that $n_1 \cdot a_1 + \cdots + n_K \cdot a_K = 0^n$.

Solving linear equations over $\mathbb{Q}_{\geq 0}$: PTIME (linear programming).

Beyond commutative groups

commutative groups $\subsetneq$ **nilpotent groups** $\subsetneq$ solvable groups $\subsetneq$ all groups

Beyond commutative groups

commutative groups $\subsetneq$ **nilpotent groups** $\subsetneq$ solvable groups $\subsetneq$ all 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.

commutative groups $\subsetneq$ **nilpotent groups** $\subsetneq$ solvable groups $\subsetneq$ all 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

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

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

commutative groups $\subsetneq$ **nilpotent groups** $\subsetneq$ solvable groups $\subsetneq$ all 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

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

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

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

Semigroup Membership and Identity Problem in nilpotent groups

Theorem (Roman'kov 2022)

There exists a finitely generated class-2 nilpotent group, namely $\mathsf{UT}(3,\mathbb{Z})^{10000}$*, where Semigroup Membership is undecidable.*

Theorem (Roman'kov 2022)

There exists a finitely generated class-2 nilpotent group, namely $\mathsf{UT}(3, \mathbb{Z})^{10000}$, *where Semigroup Membership is undecidable.*

Proof idea: embed polynomial equations over $\mathbb{Z}$, undecidable (Hilbert's 10th Problem).

Theorem (Roman'kov 2022)

There exists a finitely generated class-2 nilpotent group, namely $\mathsf{UT}(3,\mathbb{Z})^{10000}$, *where Semigroup Membership is undecidable.*

Proof idea: embed polynomial equations over $\mathbb{Z}$, undecidable (Hilbert's 10th Problem).

Theorem (D. 2024)

Identity Problem is decidable (and PTIME) in all finitely generated nilpotent groups of class d, $d \leq 10$.

Theorem (Roman'kov 2022)

There exists a finitely generated class-2 nilpotent group, namely $\mathsf{UT}(3,\mathbb{Z})^{10000}$, *where Semigroup Membership is undecidable.*

Proof idea: embed polynomial equations over $\mathbb{Z}$, undecidable (Hilbert's 10th Problem).

Theorem (D. 2024)

Identity Problem is decidable (and PTIME) in all finitely generated nilpotent groups of class d, $d \leq 10$.

In particular, this means that Identity Problem is decidable (and PTIME) in $\mathsf{UT}(3,\mathbb{Z})^{10000}$, or even $\mathsf{UT}(11,\mathbb{Z})^{10000}$.

Theorem (Roman'kov 2022)

There exists a finitely generated class-2 nilpotent group, namely $\mathrm{UT}(3, \mathbb{Z})^{10000}$, *where Semigroup Membership is undecidable.*

Proof idea: embed polynomial equations over $\mathbb{Z}$, undecidable (Hilbert's 10th Problem).

Theorem (D. 2024)

Identity Problem is decidable (and PTIME) in all finitely generated nilpotent groups of class d, $d \leq 10$.

In particular, this means that Identity Problem is decidable (and PTIME) in $\mathrm{UT}(3, \mathbb{Z})^{10000}$, or even $\mathrm{UT}(11, \mathbb{Z})^{10000}$.

Theorem (D. 2024)

For each $d > 10$, *subject to a conjecture* P_d, *the Identity Problem is decidable (and PTIME) in all finitely generated nilpotent groups of class* d.
For each d, *the conjecture* P_d *can be verified by computer algebra software in case it is true.*

Theorem (D. 2024)

Identity Problem is decidable (and PTIME) in all finitely generated nilpotent groups of class d, $d \leq 10$.

Identity Problem in nilpotent groups: main idea

Theorem (D. 2024)

Identity Problem is decidable (and PTIME) in all finitely generated nilpotent groups of class d, $d \leq 10$.

Denote by $\langle S \rangle_{semigrp}$ the semigroup generated by S.

Lemma (Very easy lemma)

We have $I \in \langle S \rangle_{semigrp}$ if and only if there exists a non-empty subset $H \subseteq S$, such that the semigroup $\langle H \rangle_{semigrp}$ is a group.

Identity Problem in nilpotent groups: main idea

Theorem (D. 2024)

Identity Problem is decidable (and PTIME) in all finitely generated nilpotent groups of class d, $d \leq 10$.

Denote by $\langle S \rangle_{semigrp}$ the semigroup generated by S.

Lemma (Very easy lemma)

We have $I \in \langle S \rangle_{semigrp}$ if and only if there exists a non-empty subset $H \subseteq S$, such that the semigroup $\langle H \rangle_{semigrp}$ is a group.

Recall that $[G, G]$ denotes the (normal) subgroup of G generated by $ghg^{-1}h^{-1}$, $g, h \in G$. In particular, the quotient group $G/[G, G]$ is abelian.

Proposition (Very difficult proposition)

For $d \leq 10$, let G be a class-d nilpotent group. Let S be the generators of G as a group, then $\langle S \rangle_{semigrp} = G$ if and only if $\langle S[G, G] \rangle_{semigrp} = G/[G, G]$.

Let's illustrate with $G := \mathrm{UT}(4, \mathbb{Z})$.

$$G = \left\{ \begin{pmatrix} 1 & * & * & * \\ 0 & 1 & * & * \\ 0 & 0 & 1 & * \\ 0 & 0 & 0 & 1 \end{pmatrix} \middle| * \in \mathbb{Z} \right\}, \quad [G, G] = \left\{ \begin{pmatrix} 1 & 0 & * & * \\ 0 & 1 & 0 & * \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \middle| * \in \mathbb{Z} \right\}$$

$G/[G, G] \cong \mathbb{Z}^3$: multiplication acts additively on the superdiagonal.

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

$[G, G]$ itself is also abelian:

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

Proposition (Very difficult proposition)

For $d \leq 10$, let G be a class-d nilpotent group. Let S be the generators of G as a group, then $\langle S \rangle_{semigrp} = G$ if and only if $\langle S[G, G] \rangle_{semigrp} = G/[G, G]$.

Proposition (Very difficult proposition)

For $d \leq 10$, let G be a class-d nilpotent group. Let S be the generators of G as a group, then $\langle S \rangle_{semigrp} = G$ if and only if $\langle S[G,G] \rangle_{semigrp} = G/[G,G]$.

Suppose $S = \{A_1, A_2, A_3, A_4\}$,

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

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

S generates G as a group.

Proposition (Very difficult proposition)

For $d \leq 10$, let G be a class-d nilpotent group. Let S be the generators of G as a group, then $\langle S \rangle_{semigrp} = G$ if and only if $\langle S[G, G] \rangle_{semigrp} = G/[G, G]$.

Suppose $S = \{A_1, A_2, A_3, A_4\}$,

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

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

S generates G as a group. What is $\langle S[G, G] \rangle_{semigrp}$?

$$S[G, G] = \{A_1[G, G], \dots, A_4[G, G]\} = \left\{ \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ -1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ -1 \end{pmatrix} \right\}.$$

So indeed $\langle S[G, G] \rangle_{semigrp} = \mathbb{Z}^3 = G/[G, G]$.

Since $\langle S[G, G] \rangle_{semigrp} = G/[G, G]$, the proposition claims that $\langle S \rangle_{semigrp} = G$.
We will prove $\langle S \rangle_{semigrp} = G$ for this example.

Since $\langle S[G,G]\rangle_{semigrp} = G/[G,G]$, the proposition claims that $\langle S\rangle_{semigrp} = G$.
We will prove $\langle S\rangle_{semigrp} = G$ for this example.
Since $\langle S[G,G]\rangle_{semigrp} = G/[G,G]$, we have $\langle S\rangle_{semigrp} \cap [G,G] \neq \emptyset$.

$$A_1A_2A_3A_4 = \begin{pmatrix} 1 & 0 & 11 & 2 \\ 0 & 1 & 0 & 8 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \in \langle S\rangle \cap [G,G],$$

$$A_2^{100}A_3^{100}A_1^{100}A_4^{100} = \begin{pmatrix} 1 & 0 & 6050 & 77350 \\ 0 & 1 & 0 & -4250 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \in \langle S\rangle \cap [G,G],$$

$$A_2^{100}A_1^{100}A_3^{100}A_4^{100} = \begin{pmatrix} 1 & 0 & -3950 & 127350 \\ 0 & 1 & 0 & 5750 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \in \langle S\rangle \cap [G,G],$$

$$A_4^{100}A_3^{100}A_2^{100}A_1^{100} = \begin{pmatrix} 1 & 0 & -3950 & -287650 \\ 0 & 1 & 0 & -4250 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \in \langle S\rangle \cap [G,G].$$

$$
\begin{pmatrix} 1 & 0 & 11 & 2 \\ 0 & 1 & 0 & 8 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}^{1880000}
\begin{pmatrix} 1 & 0 & 6050 & 77350 \\ 0 & 1 & 0 & -4250 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}^{14443} \times
$$

$$
\begin{pmatrix} 1 & 0 & -3950 & 127350 \\ 0 & 1 & 0 & 5750 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}^{16261}
\begin{pmatrix} 1 & 0 & -3950 & -287650 \\ 0 & 1 & 0 & -4250 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}^{11096}
$$

$$
= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{1}
$$

Therefore
$(A_1A_2A_3A_4)^{1880000}\left(A_2^{100}A_3^{100}A_1^{100}A_4^{100}\right)^{14443}\cdots\left(A_4^{100}A_3^{100}A_2^{100}A_1^{100}\right)^{11096} = I.$

Consequently, $A_1^{-1}, \dots, A_4^{-1} \in \langle A_1, A_2, A_3, A_4\rangle_{semigroup}$. i.e. $\langle S\rangle_{semigrp} = G$.

The general case

In general, we might not be able to find **positive** powers (1880000, 14443 etc.) to cancel elements in $\langle S \rangle \cap [G, G]$. Therefore, we need to prove that such cancellations always exist.

The general case

In general, we might not be able to find **positive** powers (1880000, 14443 etc.) to cancel elements in $\langle S \rangle \cap [G, G]$. Therefore, we need to prove that such cancellations always exist.

One can take the **logarithm** of a matrix in $\mathrm{UT}(n, \mathbb{Z})$:

$$\log : A \mapsto \sum_{k=1}^{n} \frac{(-1)^{k-1}}{k} (A - I)^k.$$

In particular, $\log I = 0$.

In general, we might not be able to find **positive** powers (1880000, 14443 etc.) to cancel elements in $\langle S \rangle \cap [G, G]$. Therefore, we need to prove that such cancellations always exist.

One can take the **logarithm** of a matrix in $\mathrm{UT}(n, \mathbb{Z})$:

$$\log : A \mapsto \sum_{k=1}^{n} \frac{(-1)^{k-1}}{k} (A - I)^k.$$

In particular, $\log I = 0$.

Theorem (Baker-Campbell-Hausdorff formula)

Let $B_1, \ldots, B_m \in \mathrm{UT}(n, \mathbb{Z})$, *then*

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

where $H_k, k = 2, 3, \ldots,$ *are expressions with explicitly computable forms.*

The general case

In general, we might not be able to find **positive** powers (1880000, 14443 etc.) to cancel elements in $\langle S \rangle \cap [G, G]$. Therefore, we need to prove that such cancellations always exist.

One can take the **logarithm** of a matrix in $\mathrm{UT}(n, \mathbb{Z})$:

$$\log : A \mapsto \sum_{k=1}^{n} \frac{(-1)^{k-1}}{k} (A - I)^k.$$

In particular, $\log I = 0$.

Theorem (Baker-Campbell-Hausdorff formula)

Let $B_1, \dots, B_m \in \mathrm{UT}(n, \mathbb{Z})$*, then*

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

where $H_k, k = 2, 3, \dots,$ *are expressions with explicitly computable forms.*

To find cancellation for elements of $\langle S \rangle \cap [G, G]$: cancel $H_2, H_3, \dots, H_d$ one by one.

We use computer algebra software to find the explicit cancellation pattern for $H_k, k = 2, 3, \cdots$. (These are **fixed** expressions!)

Identity Problem in nilpotent groups

Theorem (D. 2024)

Identity Problem is decidable (and PTIME) in all finitely generated nilpotent groups of class-d, $d \leq 10$.

Theorem (D. 2024)

For each $d > 10$, subject to a conjecture P_d, the Identity Problem is decidable (and PTIME) in all finitely generated nilpotent groups of class-d.
For each d, the conjecture P_d can be verified by computer algebra software in case it is true.

In particular, the conjecture P_d concerns the existence of cancellation for the term H_d, which we were able to verify up to $d \leq 10$.