Semigroup Algorithmic Problems in Metabelian Groups

Ruiwen Dong

Saarland University

June 2024

We consider the following decision problem:

Definition (Identity Problem)

Input: A set of square matrices $S = \{A_1, \ldots, A_K\}$.
Question: Is there $m \geq 1$ and a sequence $A_{i_1}, A_{i_2}, \ldots, A_{i_m} \in S$, such that $A_{i_1} A_{i_2} \cdots A_{i_m} = I$?

In other words, whether the semigroup $\langle S \rangle$ generated by S contains the neutral element I?

We consider the following decision problem:

Definition (Identity Problem)

Input: A set of square matrices $S = \{A_1, \dots, A_K\}$.
Question: Is there $m \geq 1$ and a sequence $A_{i_1}, A_{i_2}, \dots, A_{i_m} \in S$, such that $A_{i_1} A_{i_2} \cdots A_{i_m} = I$?

In other words, whether the semigroup $\langle S \rangle$ generated by S contains the neutral element I?

Theorem (Bell, Potapov 2010)

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

Identity Problem

We consider the following decision problem:

Definition (Identity Problem)

Input: A set of square matrices $S = \{A_1, \ldots, A_K\}$.
Question: Is there $m \geq 1$ and a sequence $A_{i_1}, A_{i_2}, \ldots, A_{i_m} \in S$, such that $A_{i_1} A_{i_2} \cdots A_{i_m} = I$?

In other words, whether the semigroup $\langle S \rangle$ generated by S contains the neutral element I?

Theorem (Bell, Potapov 2010)

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

Theorem (Ko, Niskanen, Potapov 2017)

Identity Problem is undecidable, even when $S \subseteq \mathrm{SL}(3, \mathbb{Q})$.

We consider the following decision problem:

Definition (Identity Problem)

Input: A set of square matrices $S = \{A_1, \ldots, A_K\}$.
Question: Is there $m \geq 1$ and a sequence $A_{i_1}, A_{i_2}, \ldots, A_{i_m} \in S$, such that $A_{i_1} A_{i_2} \cdots A_{i_m} = I$?

In other words, whether the semigroup $\langle S \rangle$ generated by S contains the neutral element I?

Theorem (Bell, Potapov 2010)

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

Theorem (Ko, Niskanen, Potapov 2017)

Identity Problem is undecidable, even when $S \subseteq \mathrm{SL}(3, \mathbb{Q})$.

Theorem (Bell, Hirvensalo, Potapov 2017)

Identity Problem is decidable (NP-complete) when $S \subseteq \mathrm{SL}(2, \mathbb{Z})$.

Identity Problem for commuting matrices

Theorem (Babai et al. 1996)

Identity Problem is decidable (in PTIME) when the matrices in S commute.

Theorem (Babai et al. 1996)

Identity Problem is decidable (in PTIME) when the matrices in S commute.

"proof": we work with $(\mathbb{Z}^d, +)$ instead of (matrices, multiplication).
Let $S = \{(a_{11}, \dots, a_{1d})^\top, \dots, (a_{K1}, \dots, a_{Kd})^\top\} \subset \mathbb{Z}^d$.
We want to decide whether $(0, \dots, 0)^\top \in \langle S \rangle$.

Theorem (Babai et al. 1996)

Identity Problem is decidable (in PTIME) when the matrices in S commute.

"proof": we work with $(\mathbb{Z}^d, +)$ instead of (matrices, multiplication).
Let $S = \{(a_{11}, \dots, a_{1d})^\top, \dots, (a_{K1}, \dots, a_{Kd})^\top\} \subset \mathbb{Z}^d$.
We want to decide whether $(0, \dots, 0)^\top \in \langle S \rangle$.

The semigroup $\langle S \rangle$ generated by S is

$$\left\{ n_1 \cdot \begin{pmatrix} a_{11} \\ a_{12} \\ \vdots \\ a_{1d} \end{pmatrix} + \cdots + n_K \cdot \begin{pmatrix} a_{K1} \\ a_{K2} \\ \vdots \\ a_{Kd} \end{pmatrix} \;\middle|\; n_1, n_2, \dots, n_K \in \mathbb{N}, \text{not all zero} \right\}$$

Identity Problem for commuting matrices

Theorem (Babai et al. 1996)

Identity Problem is decidable (in PTIME) when the matrices in S commute.

"proof": we work with $(\mathbb{Z}^d, +)$ instead of (matrices, multiplication).
Let $S = \{(a_{11}, \ldots, a_{1d})^\top, \ldots, (a_{K1}, \ldots, a_{Kd})^\top\} \subset \mathbb{Z}^d$.
We want to decide whether $(0, \ldots, 0)^\top \in \langle S \rangle$.

The semigroup $\langle S \rangle$ generated by S is

$$\left\{ n_1 \cdot \begin{pmatrix} a_{11} \\ a_{12} \\ \vdots \\ a_{1d} \end{pmatrix} + \cdots + n_K \cdot \begin{pmatrix} a_{K1} \\ a_{K2} \\ \vdots \\ a_{Kd} \end{pmatrix} \;\middle|\; n_1, n_2, \ldots, n_K \in \mathbb{N}, \text{not all zero} \right\}$$

So $\langle S \rangle$ contains the neutral element $(0, \ldots, 0)^\top$ if and only if

$$\begin{aligned} n_1 a_{11} + \cdots + n_K a_{K1} &= 0 \\ &\vdots \\ n_1 a_{1d} + \cdots + n_K a_{Kd} &= 0 \end{aligned}$$

has non-trivial solutions $n_1, n_2, \ldots, n_K \in \mathbb{N}$;

Identity Problem for commuting matrices

Theorem (Babai et al. 1996)

Identity Problem is decidable (in PTIME) when the matrices in S commute.

"proof": we work with $(\mathbb{Z}^d, +)$ instead of (matrices, multiplication).
Let $S = \{(a_{11}, \ldots, a_{1d})^\top, \ldots, (a_{K1}, \ldots, a_{Kd})^\top\} \subset \mathbb{Z}^d$.
We want to decide whether $(0, \ldots, 0)^\top \in \langle S \rangle$.

The semigroup $\langle S \rangle$ generated by S is

$$\left\{ n_1 \cdot \begin{pmatrix} a_{11} \\ a_{12} \\ \vdots \\ a_{1d} \end{pmatrix} + \cdots + n_K \cdot \begin{pmatrix} a_{K1} \\ a_{K2} \\ \vdots \\ a_{Kd} \end{pmatrix} \;\middle|\; n_1, n_2, \ldots, n_K \in \mathbb{N}, \text{not all zero} \right\}$$

So $\langle S \rangle$ contains the neutral element $(0, \ldots, 0)^\top$ if and only if

$$\begin{aligned} n_1 a_{11} + \cdots + n_K a_{K1} &= 0 \\ &\vdots \\ n_1 a_{1d} + \cdots + n_K a_{Kd} &= 0 \end{aligned}$$

has non-trivial solutions $n_1, n_2, \ldots, n_K \in \mathbb{N}$; if and only if it has non-trivial solutions over $\mathbb{Q}_{\geq 0}$. (Linear programming, PTIME)

Theorem (Babai et al. 1996)

Identity Problem is decidable (in PTIME) in abelian matrix groups.

Theorem (Babai et al. 1996)

Identity Problem is decidable (in PTIME) in abelian matrix groups.

Our main result:

Theorem (D. 2024)

Identity Problem is decidable in metabelian matrix groups.

Theorem (Babai et al. 1996)

Identity Problem is decidable (in PTIME) in abelian matrix groups.

Our main result:

Theorem (D. 2024)

Identity Problem is decidable in metabelian matrix groups.

Definition (Metabelian groups)

A group G is called metabelian if it has a normal subgroup A, such that both A and the quotient G/A are abelian.

Metabelian groups

G is metabelian if it has a normal subgroup A, s.t. both A and G/A are abelian.

Examples of metabelian groups

- All finite groups of size at most 23.

Metabelian groups

G is <u>metabelian</u> if it has a normal subgroup A, s.t. both A and G/A are abelian.

Examples of metabelian groups

- All finite groups of size at most 23.
- The Heisenberg group over any field $\mathbb{K}$:

$$\mathrm{H}_3(\mathbb{K}) := \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \middle| \; a, b, c \in \mathbb{K} \right\}.$$

G is metabelian if it has a normal subgroup A, s.t. both A and G/A are abelian.

Examples of metabelian groups

- All finite groups of size at most 23.
- The Heisenberg group over any field $\mathbb{K}$:

$$\mathrm{H}_3(\mathbb{K}) := \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \middle| \, a, b, c \in \mathbb{K} \right\}.$$

- The group of 2×2 upper-triangular matrices over any field $\mathbb{K}$:

$$\mathrm{T}(2, \mathbb{K}) := \left\{ \begin{pmatrix} a & c \\ 0 & b \end{pmatrix} \middle| \, a, b, c \in \mathbb{K}, ab \neq 0 \right\}.$$

G is metabelian if it has a normal subgroup A, s.t. both A and G/A are abelian.

Examples of metabelian groups

- All finite groups of size at most 23.
- The Heisenberg group over any field $\mathbb{K}$:

$$\mathrm{H}_3(\mathbb{K}) := \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \middle| \, a, b, c \in \mathbb{K} \right\}.$$

- The group of 2×2 upper-triangular matrices over any field $\mathbb{K}$:

$$\mathrm{T}(2, \mathbb{K}) := \left\{ \begin{pmatrix} a & c \\ 0 & b \end{pmatrix} \middle| \, a, b, c \in \mathbb{K}, ab \neq 0 \right\}.$$

- The **wreath product**

$$\mathbb{Z} \wr \mathbb{Z}^d := \left\{ \begin{pmatrix} X_1^{z_1} X_2^{z_2} \cdots X_d^{z_d} & f \\ 0 & 1 \end{pmatrix} \middle| \, z_1, \ldots, z_d \in \mathbb{Z}, f \in \underbrace{\mathbb{Z}[X_1^{\pm}, \ldots, X_d^{\pm}]}_{\text{Laurent polynomial}} \right\}.$$

Theorem (Magnus, Baumslag)

Any finitely generated metabelian group can be written as a quotient G/H, where G, H are subgroups of $\mathbb{Z} \wr \mathbb{Z}^d$.

$$\mathbb{Z} \wr \mathbb{Z}^d := \left\{ \begin{pmatrix} X_1^{z_1} X_2^{z_2} \cdots X_d^{z_d} & f \\ 0 & 1 \end{pmatrix} \middle| \ z_1, \dots, z_d \in \mathbb{Z}, \underbrace{f \in \mathbb{Z}[X_1^{\pm}, \dots, X_d^{\pm}]}_{\text{Laurent polynomial}} \right\}.$$

Theorem (Magnus, Baumslag)

Any finitely generated metabelian group can be written as a quotient G/H, where G, H are subgroups of $\mathbb{Z} \wr \mathbb{Z}^d$.

$$\mathbb{Z} \wr \mathbb{Z}^d := \left\{ \begin{pmatrix} X_1^{z_1} X_2^{z_2} \cdots X_d^{z_d} & f \\ 0 & 1 \end{pmatrix} \middle| \; z_1, \dots, z_d \in \mathbb{Z}, \underbrace{f \in \mathbb{Z}[X_1^{\pm}, \dots, X_d^{\pm}]}_{\text{Laurent polynomial}} \right\}.$$

Proposition (Dong 2024)

Identity Problem in metabelian groups reduces to solving systems of homogeneous linear equations over $\underbrace{\mathbb{N}[X_1^{\pm}, \dots, X_d^{\pm}]}_{\substack{\textit{Laurent polynomials} \\ \textit{with positive coefficients}}}$*, with possible degree constraints.*

Example of such systems

Does the following system of equations

$$f_1 \cdot (X_1^2 X_2 - 1) + \cdots + f_K \cdot (X_1^{-3} + 2X_2 + 1) = 0,$$
$$f_1 \cdot (3X_1 + X_2^{-3}) + \cdots + f_K \cdot (-2X_1^{-3} X_2 - 5) = 0,$$

have non-trivial solutions (with positive coefficients) $f_1, \ldots, f_K \in \mathbb{N}[X_1^{\pm}, X_2^{\pm}]$, satisfying the following degree constraints?

$$\deg_{(3,2)} f_1 \geq \deg_{(3,2)} f_K,$$
$$\deg_{(a,2)} f_1 > \deg_{(a,2)} f_K, \quad \text{for all } 0 < a < 3.$$

weighted degree: $\deg_{(a_1,a_2)} X_1^{b_1} X_2^{b_2} = a_1 b_1 + a_2 b_2$.

Polynomials with positive coefficients

How to decide where a solution exists?

How to decide where a solution exists?

Example 1

Does the following equation have solutions over $\mathbb{N}[X^{\pm}]^*$?

$$(X-2)\cdot f_1 + (4-X)\cdot f_2 + (X-1)\cdot f_3 = 0.$$

Polynomials with positive coefficients

How to decide where a solution exists?

Example 1

Does the following equation have solutions over $\mathbb{N}[X^{\pm}]^*$?

$$(X - 2) \cdot f_1 + (4 - X) \cdot f_2 + (X - 1) \cdot f_3 = 0.$$

No, evaluate $X := 3$, then $f_1(3) + f_2(3) + 2 \cdot f_3(3) = 0$.

How to decide where a solution exists?

Example 1

Does the following equation have solutions over $\mathbb{N}[X^{\pm}]^*$?

$$(X-2)\cdot f_1 + (4-X)\cdot f_2 + (X-1)\cdot f_3 = 0.$$

No, evaluate $X := 3$, then $f_1(3) + f_2(3) + 2\cdot f_3(3) = 0$.

Example 2

Does the following equation have solutions over $\mathbb{N}[X^{\pm}]^*$, such that $\deg(f_1) > \deg(f_2) > \deg(f_3)$?

$$(X-2)\cdot f_1 + (3-X)\cdot f_2 + (1-X)f_3 = 0.$$

How to decide where a solution exists?

Example 1

Does the following equation have solutions over $\mathbb{N}[X^{\pm}]^*$?

$$(X-2)\cdot f_1 + (4-X)\cdot f_2 + (X-1)\cdot f_3 = 0.$$

No, evaluate $X := 3$, then $f_1(3) + f_2(3) + 2\cdot f_3(3) = 0$.

Example 2

Does the following equation have solutions over $\mathbb{N}[X^{\pm}]^*$, such that $\deg(f_1) > \deg(f_2) > \deg(f_3)$?

$$(X-2)\cdot f_1 + (3-X)\cdot f_2 + (1-X)f_3 = 0.$$

No, otherwise degree of $(X-2)\cdot f_1$ would be bigger than $(3-X)\cdot f_2 + (1-X)f_3$.

Proposition (D. 2024)

A system of homogeneous linear equations over $\mathbb{N}[X_1^{\pm}, \ldots, X_d^{\pm}]$, with possible degree constraints, has solutions if and only if there is no contradictions of any of the two types: (i) evaluation at positive reals, (ii) degree (i.e. evaluation at infinity).

Proposition (D. 2024)

A system of homogeneous linear equations over $\mathbb{N}[X_1^{\pm}, \ldots, X_d^{\pm}]$, with possible degree constraints, has solutions if and only if there is no contradictions of any of the two types: (i) evaluation at positive reals, (ii) degree (i.e. evaluation at infinity).

Proof: real algebraic geometry (Positivstellensatz-type arguments) and tropical geometry (gluing Newton polytopes).

Proposition (D. 2024)

A system of homogeneous linear equations over $\mathbb{N}[X_1^{\pm}, \ldots, X_d^{\pm}]$, with possible degree constraints, has solutions if and only if there is no contradictions of any of the two types: (i) evaluation at positive reals, (ii) degree (i.e. evaluation at infinity).

Proof: real algebraic geometry (Positivstellensatz-type arguments) and tropical geometry (gluing Newton polytopes).

We then use a "parallel double procedure" to decide existence of solutions:

Procedure A: enumerate tuples in $\mathbb{N}[X_1^{\pm}, \ldots, X_d^{\pm}]$ and check if is solution.
Procedure B: enumerate a dense set of evaluations and check if is contradiction.

Decidability of Identity Problem in metabelian groups: proof overview

Identity Problem in metabelian groups

$\downarrow$ reduce using group theory theorem of Magnus and Baumslag

Identity Problem in quotient of $\mathbb{Z} \wr \mathbb{Z}^d$

$\downarrow$ reduce using Key technical proposition (whose proof uses convex polytopes and graph theory)

solving systems of homogeneous linear equations over $\mathbb{N}[X_1^{\pm}, \ldots, X_d^{\pm}]$

$\downarrow$ solve using real algebraic geometry and tropical geometry

decidable