# The Identity Problem in the special affine group of $\mathbb{Z}^2$

Ruiwen Dong

University of Oxford

June 2023

# An old decidability problem

Markov (1940s): is (semigroup) **Membership Problem** 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 (semigroup) **Membership Problem** 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. $B_1 B_2 \cdots B_m = T$?
i.e. whether $T \in \langle \mathcal{G} \rangle$?

# An old decidability problem

Markov (1940s): is (semigroup) **Membership Problem** 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. $B_1 B_2 \cdots B_m = T$?
i.e. whether $T \in \langle \mathcal{G} \rangle$?

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

# An old decidability problem

Markov (1940s): is (semigroup) **Membership Problem** 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. $B_1 B_2 \cdots B_m = T$?
i.e. whether $T \in \langle \mathcal{G} \rangle$?

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

---

# An old decidability problem

Markov (1940s): is (semigroup) **Membership Problem** 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. $B_1 B_2 \cdots B_m = T$?
i.e. whether $T \in \langle \mathcal{G} \rangle$?

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

---

Special case: is the **Identity Problem** decidable?

**Input:** Set of square matrices $\mathcal{G} = \{A_1, \ldots, A_K\}$.
**Output:** Is there a sequence $B_1, B_2, \ldots, B_m \in \mathcal{G}$, s.t. $B_1 B_2 \cdots B_m = I$?
i.e. whether $I \in \langle \mathcal{G} \rangle$?

# An old decidability problem

Markov (1940s): is (semigroup) **Membership Problem** 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. $B_1 B_2 \cdots B_m = T$?
i.e. whether $T \in \langle \mathcal{G} \rangle$?

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

---

Special case: is the **Identity Problem** decidable?

**Input:** Set of square matrices $\mathcal{G} = \{A_1, \ldots, A_K\}$.
**Output:** Is there a sequence $B_1, B_2, \ldots, B_m \in \mathcal{G}$, s.t. $B_1 B_2 \cdots B_m = I$?
i.e. whether $I \in \langle \mathcal{G} \rangle$?

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

**Known results.**

$\mathsf{SL}(n, \mathbb{Z})$ : the group of $n \times n$ integer matrices of determinant one.

| group type | Membership: $T \in \langle \mathcal{G} \rangle$? | Identity Prob: $I \in \langle \mathcal{G} \rangle$? |
|---|---|---|
| $\mathsf{SL}(2, \mathbb{Z})$ | NP-complete [BHP23] | NP-complete [BHP17] |
| $\mathsf{SL}(3, \mathbb{Z})$ | ? | ? |
| $\mathsf{SL}(4, \mathbb{Z})$ | Undecidable | Undecidable |

**Known results.**

$\mathrm{SL}(n, \mathbb{Z})$ : the group of $n \times n$ integer matrices of determinant one.

| group type | Membership: $T \in \langle \mathcal{G} \rangle$? | Identity Prob: $I \in \langle \mathcal{G} \rangle$? |
|---|---|---|
| $\mathrm{SL}(2, \mathbb{Z})$ | NP-complete [BHP23] | NP-complete [BHP17] |
| $\mathrm{SL}(3, \mathbb{Z})$ | ? | ? |
| $\mathrm{SL}(4, \mathbb{Z})$ | Undecidable | Undecidable |

* There exist groups where Membership Problem is undecidable but Identity Problem is decidable.

# Special Affine group

| group type | Membership: $T \in \langle \mathcal{G} \rangle$? | Identity Prob: $I \in \langle \mathcal{G} \rangle$? |
|---|---|---|
| $\mathrm{SL}(2, \mathbb{Z})$ | NP-complete | NP-complete |
| $\mathrm{SL}(3, \mathbb{Z})$ | ? | ? |
| $\mathrm{SL}(4, \mathbb{Z})$ | Undecidable | Undecidable |

# Special Affine group

| group type | Membership: $T \in \langle \mathcal{G} \rangle$? | Identity Prob: $I \in \langle \mathcal{G} \rangle$? |
|---|---|---|
| $\mathrm{SL}(2,\mathbb{Z})$ | NP-complete | NP-complete |
| $\mathrm{SL}(3,\mathbb{Z})$ | ? | ? |
| $\mathrm{SL}(4,\mathbb{Z})$ | Undecidable | Undecidable |

$\mathrm{SA}(2,\mathbb{Z})$ : the Special Affine group

$$\left\{ M = \begin{pmatrix} * & * & * \\ * & * & * \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; \det(M) = 1 \right\}$$

# Special Affine group

| group type | Membership: $T \in \langle \mathcal{G} \rangle$? | Identity Prob: $I \in \langle \mathcal{G} \rangle$? |
|---|---|---|
| $\mathsf{SL}(2,\mathbb{Z})$ | NP-complete | NP-complete |
| $\mathsf{SL}(3,\mathbb{Z})$ | ? | ? |
| $\mathsf{SL}(4,\mathbb{Z})$ | Undecidable | Undecidable |

$\mathsf{SA}(2,\mathbb{Z})$ : the Special Affine group

$$\left\{ M = \begin{pmatrix} * & * & * \\ * & * & * \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; \det(M) = 1 \right\} \leq \mathsf{SL}(3,\mathbb{Z})$$

# Special Affine group

| group type | Membership: $T \in \langle \mathcal{G} \rangle$? | Identity Prob: $I \in \langle \mathcal{G} \rangle$? |
|---|---|---|
| $\mathrm{SL}(2,\mathbb{Z})$ | NP-complete | NP-complete |
| $\mathrm{SL}(3,\mathbb{Z})$ | ? | ? |
| $\mathrm{SL}(4,\mathbb{Z})$ | Undecidable | Undecidable |

$\mathrm{SA}(2,\mathbb{Z})$ : the Special Affine group

$$\mathrm{SL}(2,\mathbb{Z}) \leq \left\{ M = \begin{pmatrix} * & * & * \\ * & * & * \\ 0 & 0 & 1 \end{pmatrix} \middle| \det(M) = 1 \right\} \leq \mathrm{SL}(3,\mathbb{Z})$$

# Special Affine group

| group type | Membership: $T \in \langle \mathcal{G} \rangle$? | Identity Prob: $I \in \langle \mathcal{G} \rangle$? |
|---|---|---|
| $\mathrm{SL}(2, \mathbb{Z})$ | NP-complete | NP-complete |
| $\mathrm{SL}(3, \mathbb{Z})$ | ? | ? |
| $\mathrm{SL}(4, \mathbb{Z})$ | Undecidable | Undecidable |

$\mathrm{SA}(2, \mathbb{Z})$ : the Special Affine group

$$\mathrm{SL}(2,\mathbb{Z}) \leq \left\{ M = \begin{pmatrix} * & * & * \\ * & * & * \\ 0 & 0 & 1 \end{pmatrix} \middle| \det(M) = 1 \right\} \leq \mathrm{SL}(3, \mathbb{Z})$$

Elements of $\mathrm{SA}(2, \mathbb{Z})$ are $(A, \boldsymbol{a}) := \begin{pmatrix} A & \boldsymbol{a} \\ 0 & 1 \end{pmatrix}, A \in \mathrm{SL}(2, \mathbb{Z}), \boldsymbol{a} \in \mathbb{Z}^2$.

# Special Affine group

| group type | Membership: $T \in \langle \mathcal{G} \rangle$? | Identity Prob: $I \in \langle \mathcal{G} \rangle$? |
|---|---|---|
| $\mathrm{SL}(2,\mathbb{Z})$ | NP-complete | NP-complete |
| $\mathrm{SL}(3,\mathbb{Z})$ | ? | ? |
| $\mathrm{SL}(4,\mathbb{Z})$ | Undecidable | Undecidable |

$\mathrm{SA}(2,\mathbb{Z})$ : the Special Affine group

$$\mathrm{SL}(2,\mathbb{Z}) \leq \left\{ M = \begin{pmatrix} * & * & * \\ * & * & * \\ 0 & 0 & 1 \end{pmatrix} \middle| \det(M) = 1 \right\} \leq \mathrm{SL}(3,\mathbb{Z})$$

Elements of $\mathrm{SA}(2,\mathbb{Z})$ are $(A, \boldsymbol{a}) := \begin{pmatrix} A & \boldsymbol{a} \\ 0 & 1 \end{pmatrix}, A \in \mathrm{SL}(2,\mathbb{Z}), \boldsymbol{a} \in \mathbb{Z}^2$.

Group law: $(A, \boldsymbol{a})(B, \boldsymbol{b}) = (AB, A\boldsymbol{b} + \boldsymbol{a})$.

# Main result

| group type | Membership: $T \in \langle \mathcal{G} \rangle$? | Identity Prob: $I \in \langle \mathcal{G} \rangle$? |
|---|---|---|
| $\mathsf{SL}(2, \mathbb{Z})$ | NP-complete | NP-complete |
| $\mathsf{SA}(2, \mathbb{Z})$ | ? | NP-complete |
| $\mathsf{SL}(3, \mathbb{Z})$ | ? | ? |
| $\mathsf{SL}(4, \mathbb{Z})$ | Undecidable | Undecidable |

# Identity Problem. Step 1: the matrix part

Elements of $\mathsf{SA}(2, \mathbb{Z})$ are $(A, \boldsymbol{a})$. Group law $(A, \boldsymbol{a})(B, \boldsymbol{b}) = (AB, A\boldsymbol{b} + \boldsymbol{a})$.

# Identity Problem. Step 1: the matrix part

Elements of $\mathsf{SA}(2, \mathbb{Z})$ are $(A, \boldsymbol{a})$. Group law $(A, \boldsymbol{a})(B, \boldsymbol{b}) = (AB, A\boldsymbol{b} + \boldsymbol{a})$.

Let $\mathcal{G} = \{(A_1, \boldsymbol{a}_1), \ldots, (A_K, \boldsymbol{a}_K)\}$. **Goal:** decide whether $(I, \mathbf{0}) \in \langle \mathcal{G} \rangle$.

# Identity Problem. Step 1: the matrix part

Elements of $\mathrm{SA}(2,\mathbb{Z})$ are $(A, \boldsymbol{a})$. Group law $(A, \boldsymbol{a})(B, \boldsymbol{b}) = (AB, A\boldsymbol{b} + \boldsymbol{a})$.

Let $\mathcal{G} = \{(A_1, \boldsymbol{a}_1), \ldots, (A_K, \boldsymbol{a}_K)\}$. **Goal:** decide whether $(I, \mathbf{0}) \in \langle \mathcal{G} \rangle$.

**Step 1:** for $s = 1, \ldots, K$, check if $A_s^{-1} \in \langle A_1, \ldots, A_K \rangle$.

# Identity Problem. Step 1: the matrix part

Elements of $\mathrm{SA}(2, \mathbb{Z})$ are $(A, \boldsymbol{a})$. Group law $(A, \boldsymbol{a})(B, \boldsymbol{b}) = (AB, A\boldsymbol{b} + \boldsymbol{a})$.

Let $\mathcal{G} = \{(A_1, \boldsymbol{a}_1), \ldots, (A_K, \boldsymbol{a}_K)\}$. **Goal:** decide whether $(I, \boldsymbol{0}) \in \langle \mathcal{G} \rangle$.

**Step 1:** for $s = 1, \ldots, K$, check if $A_s^{-1} \in \langle A_1, \ldots, A_K \rangle$.
If $A_s^{-1} \notin \langle A_1, \ldots, A_K \rangle$, then

$$(A_i, \boldsymbol{a}_i) \cdots (A_s, \boldsymbol{a}_s) \cdots (A_{i'}, \boldsymbol{a}_{i'}) \neq (I, \boldsymbol{0}).$$

So we can delete $(A_s, \boldsymbol{a}_s)$ from $\mathcal{G}$.

# Identity Problem. Step 1: the matrix part

Elements of $\mathrm{SA}(2, \mathbb{Z})$ are $(A, \boldsymbol{a})$. Group law $(A, \boldsymbol{a})(B, \boldsymbol{b}) = (AB, A\boldsymbol{b} + \boldsymbol{a})$.

Let $\mathcal{G} = \{(A_1, \boldsymbol{a}_1), \ldots, (A_K, \boldsymbol{a}_K)\}$. **Goal:** decide whether $(I, \mathbf{0}) \in \langle \mathcal{G} \rangle$.

**Step 1:** for $s = 1, \ldots, K$, check if $A_s^{-1} \in \langle A_1, \ldots, A_K \rangle$.
If $A_s^{-1} \notin \langle A_1, \ldots, A_K \rangle$, then

$$(A_i, \boldsymbol{a}_i) \cdots (A_s, \boldsymbol{a}_s) \cdots (A_{i'}, \boldsymbol{a}_{i'}) \neq (I, \mathbf{0}).$$

So we can delete $(A_s, \boldsymbol{a}_s)$ from $\mathcal{G}$.

**Theorem (Bell, Hirvensalo, Potapov)**

*It is decidable in NP whether* $A_s^{-1} \in \langle A_1, \ldots, A_K \rangle$.

# Identity Problem. Step 1: the matrix part

Elements of $\mathrm{SA}(2,\mathbb{Z})$ are $(A, \boldsymbol{a})$. Group law $(A, \boldsymbol{a})(B, \boldsymbol{b}) = (AB, A\boldsymbol{b} + \boldsymbol{a})$.

Let $\mathcal{G} = \{(A_1, \boldsymbol{a}_1), \ldots, (A_K, \boldsymbol{a}_K)\}$. **Goal:** decide whether $(I, \mathbf{0}) \in \langle \mathcal{G} \rangle$.

**Step 1:** for $s = 1, \ldots, K$, check if $A_s^{-1} \in \langle A_1, \ldots, A_K \rangle$.
If $A_s^{-1} \notin \langle A_1, \ldots, A_K \rangle$, then

$$(A_i, \boldsymbol{a}_i) \cdots (A_s, \boldsymbol{a}_s) \cdots (A_{i'}, \boldsymbol{a}_{i'}) \neq (I, \mathbf{0}).$$

So we can delete $(A_s, \boldsymbol{a}_s)$ from $\mathcal{G}$.

**Theorem (Bell, Hirvensalo, Potapov)**

*It is decidable in NP whether $A_s^{-1} \in \langle A_1, \ldots, A_K \rangle$.*

We can perform Step 1 iteratively, until $A_s^{-1} \in \langle A_1, \ldots, A_K \rangle$ for all $s$.
So the semigroup $\langle A_1, \ldots, A_K \rangle$ becomes a group.

# Step 2: dichotomy on the matrix part

$$\mathcal{G} = \{(A_1, \boldsymbol{a}_1), \ldots, (A_K, \boldsymbol{a}_K)\}.$$

Additionally, $H = \langle A_1, \ldots, A_K \rangle \leq \mathrm{SL}(2, \mathbb{Z})$ is a group.

# Step 2: dichotomy on the matrix part

$$\mathcal{G} = \{(A_1, \boldsymbol{a}_1), \dots, (A_K, \boldsymbol{a}_K)\}.$$

Additionally, $H = \langle A_1, \dots, A_K \rangle \leq \mathrm{SL}(2, \mathbb{Z})$ is a group.

**Theorem (Tits alternative)**

*Let $H$ be a subgroup of $\mathrm{SL}(n, \mathbb{Z})$. Then*

1. *either $H$ contains a non-abelian free subgroup,*
2. *or $H$ contains a solvable subgroup of finite index.*

# Step 2: dichotomy on the matrix part

$$\mathcal{G} = \{(A_1, \boldsymbol{a}_1), \ldots, (A_K, \boldsymbol{a}_K)\}.$$

Additionally, $H = \langle A_1, \ldots, A_K \rangle \leq \mathrm{SL}(2, \mathbb{Z})$ is a group.

**Theorem (Tits alternative)**

*Let $H$ be a subgroup of $\mathrm{SL}(n, \mathbb{Z})$. Then*

1. *either $H$ contains a non-abelian free subgroup,*
2. *or $H$ contains a solvable subgroup of finite index.*

In $\mathrm{SL}(2, \mathbb{Z})$ this means:

1. either $H$ contains two matrices $A, B$ that are not simultaneously triangularizable,
2. or $H$ contains a finite-index subgroup that is isomorphic to $\mathbb{Z}$ or $\{I\}$.

# Step 2: dichotomy on the matrix part

$$\mathcal{G} = \{(A_1, \boldsymbol{a}_1), \ldots, (A_K, \boldsymbol{a}_K)\}.$$

Additionally, $H = \langle A_1, \ldots, A_K \rangle \leq \mathrm{SL}(2, \mathbb{Z})$ is a group.

**Theorem (Tits alternative)**

*Let $H$ be a subgroup of $\mathrm{SL}(n, \mathbb{Z})$. Then*

1. *either $H$ contains a non-abelian free subgroup,*
2. *or $H$ contains a solvable subgroup of finite index.*

In $\mathrm{SL}(2, \mathbb{Z})$ this means:

1. either $H$ contains two matrices $A, B$ that are not simultaneously triangularizable,
2. or $H$ contains a finite-index subgroup that is isomorphic to $\mathbb{Z}$ or $\{I\}$.

Furthermore, the two cases can be distinguished in PTIME (Beals 1999).

# Step 3: first case of the dichotomy

$$\mathcal{G} = \{(A_1, \boldsymbol{a}_1), \ldots, (A_K, \boldsymbol{a}_K)\}.$$

# Step 3: first case of the dichotomy

$$\mathcal{G} = \{(A_1, \boldsymbol{a}_1), \ldots, (A_K, \boldsymbol{a}_K)\}.$$

**Proposition**

*Suppose* $\langle A_1, \ldots, A_K \rangle \leq \mathrm{SL}(2, \mathbb{Z})$ *is a group containing two matrices* $A, B$ *that are not simultaneously triangularizable, then* $(I, \mathbf{0}) \in \langle \mathcal{G} \rangle$*.*

# Step 3: first case of the dichotomy

$$\mathcal{G} = \{(A_1, \boldsymbol{a}_1), \ldots, (A_K, \boldsymbol{a}_K)\}.$$

**Proposition**

*Suppose* $\langle A_1, \ldots, A_K \rangle \leq \mathrm{SL}(2, \mathbb{Z})$ *is a group containing two matrices* $A, B$ *that are not simultaneously triangularizable, then* $(I, \mathbf{0}) \in \langle \mathcal{G} \rangle$*.*

**Proof idea:**

Since $\langle A_1, \ldots, A_K \rangle$ is a group containing $A$ and $B$, it also contains some $Y$ such that $AYB = I$. In particular $\langle \mathcal{G} \rangle$ contains some elements $(A, \boldsymbol{a}), (Y, \boldsymbol{y}), (B, \boldsymbol{b})$ such that $(A, \boldsymbol{a})(Y, \boldsymbol{y})(B, \boldsymbol{b}) = (I, \boldsymbol{x})$ for some $\boldsymbol{x} \in \mathbb{Z}^2$.

# Step 3: first case of the dichotomy

$$\mathcal{G} = \{(A_1, \boldsymbol{a}_1), \dots, (A_K, \boldsymbol{a}_K)\}.$$

**Proposition**

*Suppose* $\langle A_1, \dots, A_K \rangle \leq \mathrm{SL}(2, \mathbb{Z})$ *is a group containing two matrices* $A, B$ *that are not simultaneously triangularizable, then* $(I, \mathbf{0}) \in \langle \mathcal{G} \rangle$*.*

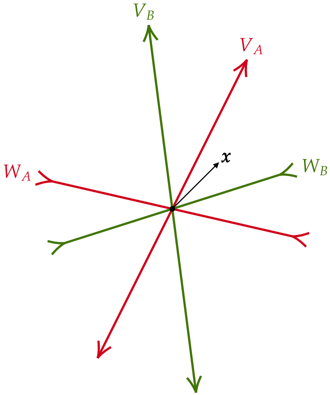
**Proof idea:**

Since $\langle A_1, \dots, A_K \rangle$ is a group containing $A$ and $B$, it also contains some $Y$ such that $AYB = I$. In particular $\langle \mathcal{G} \rangle$ contains some elements $(A, \boldsymbol{a}), (Y, \boldsymbol{y}), (B, \boldsymbol{b})$ such that $(A, \boldsymbol{a})(Y, \boldsymbol{y})(B, \boldsymbol{b}) = (I, \boldsymbol{x})$ for some $\boldsymbol{x} \in \mathbb{Z}^2$.

But $\boldsymbol{x}$ might not be $\mathbf{0}$. So we need to "pump" the word $(A, \boldsymbol{a})(Y, \boldsymbol{y})(B, \boldsymbol{b})$ to change $\boldsymbol{x}$.

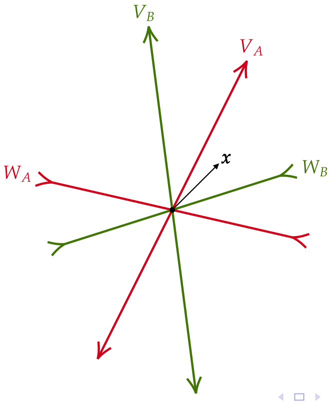
# Step 3: getting 0 in the vector part

Suppose $A$ has eigenspaces $V_A, W_A$, and $B$ has eigenspaces $V_B, W_B$, since $A$ and $B$ are not simultaneously triangularizable, we can suppose $V_A, W_A, V_B, W_B$ pairwise distinct.



# Step 3: getting 0 in the vector part

We have $(A, \boldsymbol{a}), (Y, \boldsymbol{y}), (B, \boldsymbol{b}) \in \langle \mathcal{G} \rangle$ s.t. $(A, \boldsymbol{a})(Y, \boldsymbol{y})(B, \boldsymbol{b}) = (I, \boldsymbol{x})$.

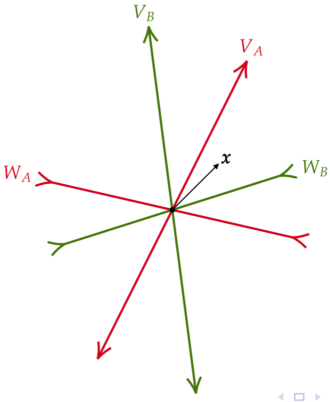


# Step 3: getting 0 in the vector part

We have $(A, \boldsymbol{a}), (Y, \boldsymbol{y}), (B, \boldsymbol{b}) \in \langle \mathcal{G} \rangle$ s.t. $(A, \boldsymbol{a})(Y, \boldsymbol{y})(B, \boldsymbol{b}) = (I, \boldsymbol{x})$.

Consider

$$\underbrace{(A, \boldsymbol{a})(Y, \boldsymbol{y})(A, \boldsymbol{a})(Y, \boldsymbol{y}) \cdots (A, \boldsymbol{a})(Y, \boldsymbol{y})}_{m \text{ times}}(B, \boldsymbol{b})^m = (I, \boldsymbol{x}_1) \in \langle \mathcal{G} \rangle$$



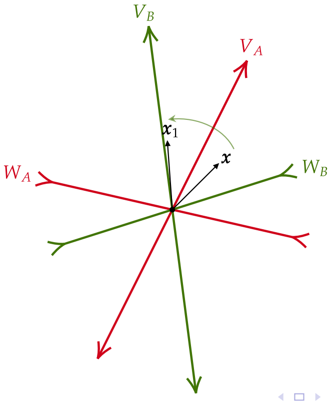
# Step 3: getting 0 in the vector part

We have $(A, \boldsymbol{a}), (Y, \boldsymbol{y}), (B, \boldsymbol{b}) \in \langle \mathcal{G} \rangle$ s.t. $(A, \boldsymbol{a})(Y, \boldsymbol{y})(B, \boldsymbol{b}) = (I, \boldsymbol{x})$.

Consider

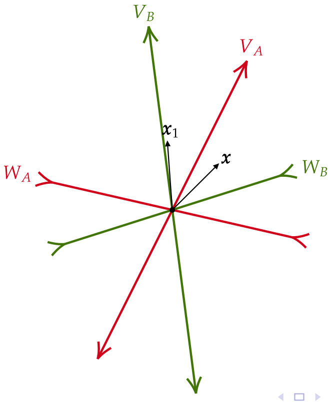
$$\underbrace{(A, \boldsymbol{a})(Y, \boldsymbol{y})(A, \boldsymbol{a})(Y, \boldsymbol{y}) \cdots (A, \boldsymbol{a})(Y, \boldsymbol{y})}_{m \text{ times}}(B, \boldsymbol{b})^m = (I, \boldsymbol{x}_1) \in \langle \mathcal{G} \rangle$$

When $m \to \infty$, the vector $\boldsymbol{x}_1$ tends towards $V_B$.



# Step 3: getting 0 in the vector part

We have $(A, \boldsymbol{a}), (Y_1, \boldsymbol{y}_1), (B, \boldsymbol{b}) \in \langle \mathcal{G} \rangle$ s.t. $(A, \boldsymbol{a})(Y_1, \boldsymbol{y})(B, \boldsymbol{b}) = (I, \boldsymbol{x}_1)$.

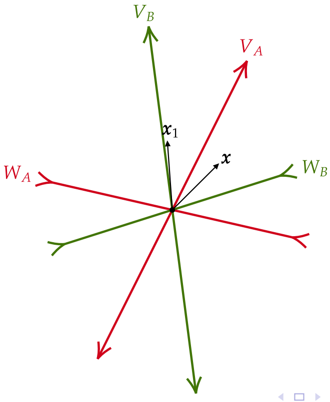


# Step 3: getting 0 in the vector part

We have $(A, \boldsymbol{a}), (Y_1, \boldsymbol{y}_1), (B, \boldsymbol{b}) \in \langle \mathcal{G} \rangle$ s.t. $(A, \boldsymbol{a})(Y_1, \boldsymbol{y})(B, \boldsymbol{b}) = (I, \boldsymbol{x}_1)$.

Consider

$$(A, \boldsymbol{a}) \underbrace{(Y_1, \boldsymbol{y}_1)(B, \boldsymbol{b}) \cdots (Y_1, \boldsymbol{y}_1)(B, \boldsymbol{b})}_{m \text{ times}} (A, \boldsymbol{a})^m (Y_1, \boldsymbol{y}_1)(B, \boldsymbol{b}) = (I, \boldsymbol{x}_2) \in \langle \mathcal{G} \rangle$$



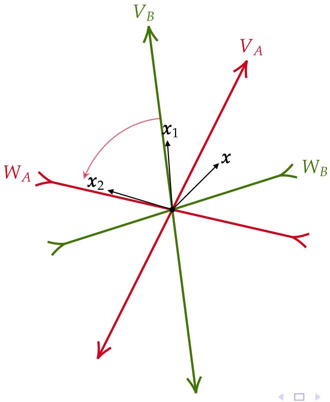
## Step 3: getting 0 in the vector part

We have $(A, \boldsymbol{a}), (Y_1, \boldsymbol{y}_1), (B, \boldsymbol{b}) \in \langle \mathcal{G} \rangle$ s.t. $(A, \boldsymbol{a})(Y_1, \boldsymbol{y}_1)(B, \boldsymbol{b}) = (I, \boldsymbol{x}_1)$.

Consider

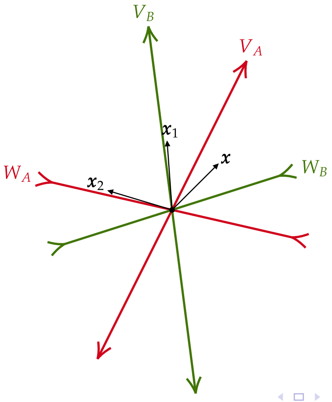
$$(A, \boldsymbol{a}) \underbrace{(Y_1, \boldsymbol{y}_1)(B, \boldsymbol{b}) \cdots (Y_1, \boldsymbol{y}_1)(B, \boldsymbol{b})}_{m \text{ times}} (A, \boldsymbol{a})^m (Y_1, \boldsymbol{y}_1)(B, \boldsymbol{b}) = (I, \boldsymbol{x}_2) \in \langle \mathcal{G} \rangle$$

When $m \to \infty$, the vector $\boldsymbol{x}_2$ tends towards $W_A$.



# Step 3: getting 0 in the vector part

We have $(A, \boldsymbol{a}), (Y_2, \boldsymbol{y}_2), (B, \boldsymbol{b}) \in \langle \mathcal{G} \rangle$ s.t. $(A, \boldsymbol{a})(Y_2, \boldsymbol{y}_2)(B, \boldsymbol{b}) = (I, \boldsymbol{x}_2)$.

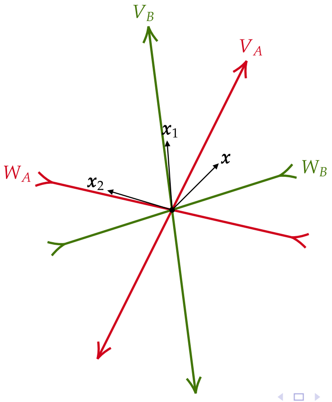


# Step 3: getting 0 in the vector part

We have $(A, \boldsymbol{a}), (Y_2, \boldsymbol{y}_2), (B, \boldsymbol{b}) \in \langle \mathcal{G} \rangle$ s.t. $(A, \boldsymbol{a})(Y_2, \boldsymbol{y}_2)(B, \boldsymbol{b}) = (I, \boldsymbol{x}_2)$.

Consider

$$(A, \boldsymbol{a})(Y_2, \boldsymbol{y}_2)(B, \boldsymbol{b})^m \underbrace{(Y_2, \boldsymbol{y}_2)(A, \boldsymbol{a}) \cdots (Y_2, \boldsymbol{y}_2)(A, \boldsymbol{a})}_{m \text{ times}}(B, \boldsymbol{b}) = (I, \boldsymbol{x}_3) \in \langle \mathcal{G} \rangle$$



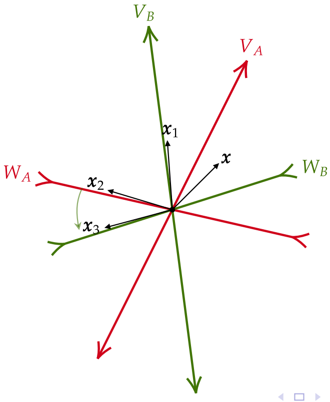
## Step 3: getting 0 in the vector part

We have $(A, \boldsymbol{a}), (Y_2, \boldsymbol{y}_2), (B, \boldsymbol{b}) \in \langle \mathcal{G} \rangle$ s.t. $(A, \boldsymbol{a})(Y_2, \boldsymbol{y}_2)(B, \boldsymbol{b}) = (I, \boldsymbol{x}_2)$.

Consider

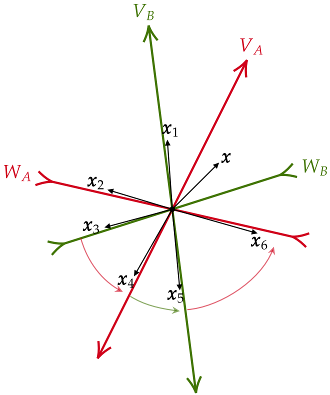
$$(A, \boldsymbol{a})(Y_2, \boldsymbol{y}_2)(B, \boldsymbol{b})^m \underbrace{(Y_2, \boldsymbol{y}_2)(A, \boldsymbol{a}) \cdots (Y_2, \boldsymbol{y}_2)(A, \boldsymbol{a})}_{m \text{ times}}(B, \boldsymbol{b}) = (I, \boldsymbol{x}_3) \in \langle \mathcal{G} \rangle$$

When $m \to \infty$, the vector $\boldsymbol{x}_3$ tends towards $W_B$.



# Step 3: getting 0 in the vector part

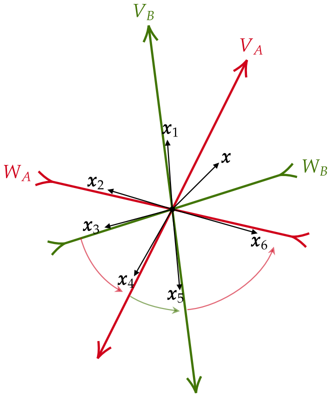
Continue like this, we obtain $(I, \boldsymbol{x}_1), (I, \boldsymbol{x}_2), \dots, (I, \boldsymbol{x}_6) \in \langle \mathcal{G} \rangle$.



# Step 3: getting 0 in the vector part

Continue like this, we obtain $(I, \boldsymbol{x}_1), (I, \boldsymbol{x}_2), \ldots, (I, \boldsymbol{x}_6) \in \langle \mathcal{G} \rangle$.

There exist **positive** integers $n_1, \ldots, n_6$ such that $n_1\boldsymbol{x}_1 + \cdots n_6\boldsymbol{x}_6 = \boldsymbol{0}$.



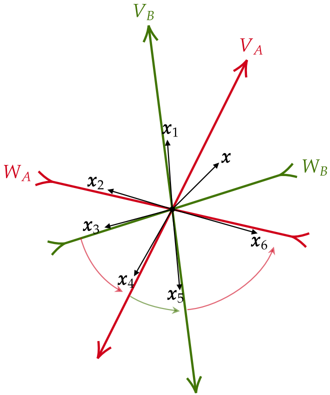
# Step 3: getting 0 in the vector part

Continue like this, we obtain $(I, \boldsymbol{x}_1), (I, \boldsymbol{x}_2), \ldots, (I, \boldsymbol{x}_6) \in \langle \mathcal{G} \rangle$.

There exist **positive** integers $n_1, \ldots, n_6$ such that $n_1 \boldsymbol{x}_1 + \cdots n_6 \boldsymbol{x}_6 = \mathbf{0}$.

Therefore

$$(I, \mathbf{0}) = (I, \boldsymbol{x}_1)^{n_1} (I, \boldsymbol{x}_2)^{n_2} \cdots (I, \boldsymbol{x}_6)^{n_6} \in \langle \mathcal{G} \rangle.$$



# Step 4: second case of dichotomy

$$\mathcal{G} = \{(A_1, \boldsymbol{a}_1), \ldots, (A_K, \boldsymbol{a}_K)\}.$$

We have proved the first case of the dichotomy:

**Proposition**

*Suppose* $\langle A_1, \ldots, A_K \rangle \leq \mathrm{SL}(2, \mathbb{Z})$ *is a group containing two matrices* $A, B$ *that are not simultaneously triangularizable, then* $(I, \mathbf{0}) \in \langle \mathcal{G} \rangle$.

# Step 4: second case of dichotomy

$$\mathcal{G} = \{(A_1, \boldsymbol{a}_1), \ldots, (A_K, \boldsymbol{a}_K)\}.$$

We have proved the first case of the dichotomy:

**Proposition**

*Suppose* $\langle A_1, \ldots, A_K \rangle \leq \mathrm{SL}(2, \mathbb{Z})$ *is a group containing two matrices* $A, B$ *that are not simultaneously triangularizable, then* $(I, \mathbf{0}) \in \langle \mathcal{G} \rangle$.

We can also prove the second case of the dichotomy:

**Proposition**

*Suppose* $\langle A_1, \ldots, A_K \rangle$ *is a group containing a finite-index subgroup that is isomorphic to* $\mathbb{Z}$ *or* $\{I\}$*. Then it is decidable in PTIME whether or not* $(I, \mathbf{0}) \in \langle \mathcal{G} \rangle$.

# Identity Problem in $\mathsf{SA}(2, \mathbb{Z})$: recap

Let $\mathcal{G} = \{(A_1, \boldsymbol{a}_1), \ldots, (A_K, \boldsymbol{a}_K)\}$, we want to decide if $(I, \mathbf{0}) \in \langle \mathcal{G} \rangle$.

We defined $H = \langle A_1, \ldots, A_K \rangle$.

# Identity Problem in $\mathsf{SA}(2,\mathbb{Z})$: recap

Let $\mathcal{G} = \{(A_1, \boldsymbol{a}_1), \ldots, (A_K, \boldsymbol{a}_K)\}$, we want to decide if $(I, \mathbf{0}) \in \langle \mathcal{G} \rangle$.

We defined $H = \langle A_1, \ldots, A_K \rangle$.

Step 1: narrowing down to the case where $H$ is a group is done in NP.
Step 2: distinguishing dichotomy is in PTIME.
Step 3: first dichotomy case, always true.
Step 4: second dichotomy case, complexity is PTIME.

In total, complexity is in NP.

# Identity Problem in $\mathrm{SA}(2, \mathbb{Z})$: recap

Let $\mathcal{G} = \{(A_1, \boldsymbol{a}_1), \ldots, (A_K, \boldsymbol{a}_K)\}$, we want to decide if $(I, \mathbf{0}) \in \langle \mathcal{G} \rangle$.

We defined $H = \langle A_1, \ldots, A_K \rangle$.

Step 1: narrowing down to the case where $H$ is a group is done in NP.
Step 2: distinguishing dichotomy is in PTIME.
Step 3: first dichotomy case, always true.
Step 4: second dichotomy case, complexity is PTIME.

In total, complexity is in NP.

NP-hardness comes from the NP-hardness in $\mathrm{SL}(2, \mathbb{Z}) \leq \mathrm{SA}(2, \mathbb{Z})$.

# Identity Problem in $\mathrm{SA}(2,\mathbb{Z})$: recap

Let $\mathcal{G} = \{(A_1, \boldsymbol{a}_1), \dots, (A_K, \boldsymbol{a}_K)\}$, we want to decide if $(I, \mathbf{0}) \in \langle \mathcal{G} \rangle$.

We defined $H = \langle A_1, \dots, A_K \rangle$.

Step 1: narrowing down to the case where $H$ is a group is done in NP.
Step 2: distinguishing dichotomy is in PTIME.
Step 3: first dichotomy case, always true.
Step 4: second dichotomy case, complexity is PTIME.

In total, complexity is in NP.

NP-hardness comes from the NP-hardness in $\mathrm{SL}(2,\mathbb{Z}) \leq \mathrm{SA}(2,\mathbb{Z})$.

**Theorem**

*The Identity Problem in* $\mathrm{SA}(2,\mathbb{Z})$ *is NP-complete.*

# Identity Problem in $\mathrm{SA}(2, \mathbb{Z})$: recap

Let $\mathcal{G} = \{(A_1, \boldsymbol{a}_1), \ldots, (A_K, \boldsymbol{a}_K)\}$, we want to decide if $(I, \mathbf{0}) \in \langle \mathcal{G} \rangle$.

We defined $H = \langle A_1, \ldots, A_K \rangle$.

Step 1: narrowing down to the case where $H$ is a group is done in NP.
Step 2: distinguishing dichotomy is in PTIME.
Step 3: first dichotomy case, always true.
Step 4: second dichotomy case, complexity is PTIME.

In total, complexity is in NP.

NP-hardness comes from the NP-hardness in $\mathrm{SL}(2, \mathbb{Z}) \leq \mathrm{SA}(2, \mathbb{Z})$.

**Theorem**

*The Identity Problem in* $\mathrm{SA}(2, \mathbb{Z})$ *is NP-complete.*

**Open Problem**

*Is Membership Problem in* $\mathrm{SA}(2, \mathbb{Z})$ *decidable?*