The Identity Problem in $\mathbb{Z} \wr \mathbb{Z}$ is decidable

Ruiwen Dong

University of Oxford

July 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 $T \in \langle \mathcal{G} \rangle$? ($\langle \mathcal{G} \rangle$ denotes the semigroup generated by $\mathcal{G}$)

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 $T \in \langle \mathcal{G} \rangle$? ($\langle \mathcal{G} \rangle$ denotes the semigroup generated by $\mathcal{G}$)

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 $T \in \langle \mathcal{G} \rangle$? ($\langle \mathcal{G} \rangle$ denotes the semigroup generated by $\mathcal{G}$)

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 (semigroup) **Membership Problem** decidable?

Input: Set of square matrices $\mathcal{G} = \{A_1, \dots, A_K\}$, target matrix T.
Output: Is there a sequence $B_1, B_2, \dots, B_m \in \mathcal{G}$, s.t. $B_1 B_2 \cdots B_m = T$?
i.e. whether $T \in \langle \mathcal{G} \rangle$? ($\langle \mathcal{G} \rangle$ denotes the semigroup generated by $\mathcal{G}$)

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

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

Input: Set of square matrices $\mathcal{G} = \{A_1, \dots, A_K\}$.
Output: Is there a sequence $B_1, B_2, \dots, B_m \in \mathcal{G}$, 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 $T \in \langle \mathcal{G} \rangle$? ($\langle \mathcal{G} \rangle$ denotes the semigroup generated by $\mathcal{G}$)

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

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 $\mathrm{SL}(4, \mathbb{Z})$.

the Identity Problem and the Membership Problem

Known results.

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

Group	Membership Prob. $T \in \langle \mathcal{G} \rangle$?	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

Known results.

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

Group	Membership Prob. $T \in \langle \mathcal{G} \rangle$?	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

Membership and Identity Problem might not have the same difficulty:

$\mathbb{Z}^n$	NP-complete	PTIME

the Identity Problem and the Membership Problem

Known results.

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

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

Membership and Identity Problem might not have the same difficulty:

$\mathbb{Z}^n$	NP-complete	PTIME

or decidability:

$\mathbb{Z} \wr \mathbb{Z}$	Undecidable (ICALP 2013)	Decidable (ICALP 2023)

Known results.

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

Group	Membership Prob. $T \in \langle \mathcal{G} \rangle$?	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

Membership and Identity Problem might not have the same difficulty:

$\mathbb{Z}^n$	NP-complete	PTIME

or decidability:

$\mathbb{Z} \wr \mathbb{Z}$	Undecidable (ICALP 2013)	Decidable (ICALP 2023)

"$\wr$" is the **wreath product**, important in decomposing finite automata (Krohn-Rhodes theorem), constructing symmetry groups, etc.

What is $\mathbb{Z} \wr \mathbb{Z}$? Its elements

First interpretation: as the set of matrices

$$\mathbb{Z} \wr \mathbb{Z} := \left\{ \begin{pmatrix} X^{b} & y \\ 0 & 1 \end{pmatrix} \;\middle|\; y \in \mathbb{Z}[X, X^{-1}], b \in \mathbb{Z} \right\}.$$

What is $\mathbb{Z} \wr \mathbb{Z}$? Its elements

First interpretation: as the set of matrices

$$\mathbb{Z} \wr \mathbb{Z} := \left\{ \begin{pmatrix} X^{b} & y \\ 0 & 1 \end{pmatrix} \middle| \; y \in \mathbb{Z}[X, X^{-1}], b \in \mathbb{Z} \right\}.$$

Second interpretation: as a “cheap” Turing machine.

Each element of $\mathbb{Z} \wr \mathbb{Z}$ is a configuration

$\cdots$	a_{-2}	a_{-1}	a_0	a_1	a_2	$\cdots$
			$\uparrow$		$\downarrow$	

where $\cdots a_{-2}, a_{-1}, a_0, a_1, a_2 \cdots \in \mathbb{Z}$.

The arrow $\uparrow$ is placed at 0. The arrow $\downarrow$ is placed at some integer b.

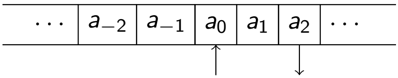
What is $\mathbb{Z} \wr \mathbb{Z}$? Its elements

First interpretation: as the set of matrices

$$\mathbb{Z} \wr \mathbb{Z} := \left\{ \begin{pmatrix} X^{b} & y \\ 0 & 1 \end{pmatrix} \;\middle|\; y \in \mathbb{Z}[X, X^{-1}], b \in \mathbb{Z} \right\}.$$

Second interpretation: as a “cheap” Turing machine.

Each element of $\mathbb{Z} \wr \mathbb{Z}$ is a configuration



where $\cdots a_{-2}, a_{-1}, a_0, a_1, a_2 \cdots \in \mathbb{Z}$.

The arrow $\uparrow$ is placed at 0. The arrow $\downarrow$ is placed at some integer b.

Let $y := \cdots + a_{-1}X^{-1} + a_0 + a_1 X + a_2 X^2 + \cdots$, then the configuration represents the element $\begin{pmatrix} X^{b} & y \\ 0 & 1 \end{pmatrix}$.

What is $\mathbb{Z} \wr \mathbb{Z}$? the group law

First interpretation: as matrix multiplication

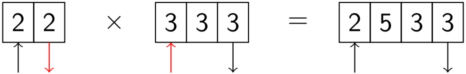
$$\begin{pmatrix} X & 2+2X \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X^2 & 3+3X+3X^2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} X^3 & 2+5X+3X^2+3X^3 \\ 0 & 1 \end{pmatrix}$$

What is $\mathbb{Z} \wr \mathbb{Z}$? the group law

First interpretation: as matrix multiplication

$$\begin{pmatrix} X & 2+2X \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X^2 & 3+3X+3X^2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} X^3 & 2+5X+3X^2+3X^3 \\ 0 & 1 \end{pmatrix}$$

Second interpretation: align $\downarrow$ of first element and $\uparrow$ of second element, then add all cells.

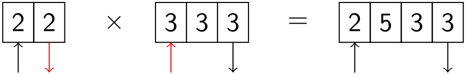


What is $\mathbb{Z} \wr \mathbb{Z}$? the group law

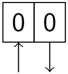
First interpretation: as matrix multiplication

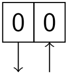
$$\begin{pmatrix} X & 2+2X \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X^2 & 3+3X+3X^2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} X^3 & 2+5X+3X^2+3X^3 \\ 0 & 1 \end{pmatrix}$$

Second interpretation: align $\downarrow$ of first element and $\uparrow$ of second element, then add all cells.

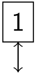


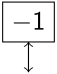
Each element is an "instruction".

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

$=$ "move right", $\begin{pmatrix} X^{-1} & 0 \\ 0 & 1 \end{pmatrix} =$ 

$=$ "move left".

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

$=$ "increase counter", $\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} =$ 

$=$ "decrease counter".

What is $\mathbb{Z} \wr \mathbb{Z}$? Membership and Identity Problem

Given a finite set of elements

$$\mathcal{G} = \left\{ \begin{pmatrix} X^{a_1} & y_1 \\ 0 & 1 \end{pmatrix}, \cdots, \begin{pmatrix} X^{a_K} & y_K \\ 0 & 1 \end{pmatrix} \right\}.$$

What is $\mathbb{Z} \wr \mathbb{Z}$? Membership and Identity Problem

Given a finite set of elements

$$\mathcal{G} = \left\{ \begin{pmatrix} X^{a_1} & y_1 \\ 0 & 1 \end{pmatrix}, \cdots, \begin{pmatrix} X^{a_K} & y_K \\ 0 & 1 \end{pmatrix} \right\}.$$

Membership Problem: whether $\begin{pmatrix} X^{a} & y \\ 0 & 1 \end{pmatrix} \in \langle \mathcal{G} \rangle$?

Identity Problem: whether $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \langle \mathcal{G} \rangle$?

What is $\mathbb{Z} \wr \mathbb{Z}$? Membership and Identity Problem

Given a finite set of elements

$$\mathcal{G} = \left\{ \begin{pmatrix} X^{a_1} & y_1 \\ 0 & 1 \end{pmatrix}, \ldots, \begin{pmatrix} X^{a_K} & y_K \\ 0 & 1 \end{pmatrix} \right\}.$$

Membership Problem: whether $\begin{pmatrix} X^{a} & y \\ 0 & 1 \end{pmatrix} \in \langle \mathcal{G} \rangle$?

Identity Problem: whether $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \langle \mathcal{G} \rangle$?

As a machine: given a finite number of instructions $\mathcal{G} = \{A_1, \ldots, A_K\}$.

What is $\mathbb{Z} \wr \mathbb{Z}$? Membership and Identity Problem

Given a finite set of elements

$$\mathcal{G} = \left\{ \begin{pmatrix} X^{a_1} & y_1 \\ 0 & 1 \end{pmatrix}, \dots, \begin{pmatrix} X^{a_K} & y_K \\ 0 & 1 \end{pmatrix} \right\}.$$

Membership Problem: whether $\begin{pmatrix} X^a & y \\ 0 & 1 \end{pmatrix} \in \langle \mathcal{G} \rangle$?

Identity Problem: whether $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \langle \mathcal{G} \rangle$?

As a machine: given a finite number of instructions $\mathcal{G} = \{A_1, \dots, A_K\}$.

Membership Problem: can we reach a certain configuration?

Identity Problem: can we reach the initial configuration (can we loop)?

What is $\mathbb{Z} \wr \mathbb{Z}$? Membership and Identity Problem

Given a finite set of elements

$$\mathcal{G} = \left\{ \begin{pmatrix} X^{a_1} & y_1 \\ 0 & 1 \end{pmatrix}, \dots, \begin{pmatrix} X^{a_K} & y_K \\ 0 & 1 \end{pmatrix} \right\}.$$

Membership Problem: whether $\begin{pmatrix} X^{a} & y \\ 0 & 1 \end{pmatrix} \in \langle \mathcal{G} \rangle$?

Identity Problem: whether $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \langle \mathcal{G} \rangle$?

As a machine: given a finite number of instructions $\mathcal{G} = \{A_1, \dots, A_K\}$.

Membership Problem: can we reach a certain configuration?

Identity Problem: can we reach the initial configuration (can we loop)?

Theorem (Lohrey, Steinberg, Zetzsche 2013)

Membership Problem in $\mathbb{Z} \wr \mathbb{Z}$ is undecidable.

Theorem

The Identity Problem in $\mathbb{Z} \wr \mathbb{Z}$ is decidable.

The Identity Problem in $\mathbb{Z} \wr \mathbb{Z}$: a special case

As an example, consider a set of *three* elements

$$\mathcal{G} = \left\{ \begin{pmatrix} X & y_1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & y_2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} X^{-1} & y_3 \\ 0 & 1 \end{pmatrix} \right\},$$

The Identity Problem in $\mathbb{Z} \wr \mathbb{Z}$: a special case

As an example, consider a set of *three* elements

$$\mathcal{G} = \left\{ \begin{pmatrix} X & y_1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & y_2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} X^{-1} & y_3 \\ 0 & 1 \end{pmatrix} \right\},$$

Given three instructions A_1, A_2, A_3, where

- A_1 is "move right one step, change nearby counters according to y_1",
- A_2 is "don't move, change nearby counters according to y_2",
- A_3 is "move left one step, change nearby counters according to y_3".

Identity Problem: can we reach the initial configuration using A_1, A_2, A_3?

The special case: path of the run

Consider a sequence that might reach I:

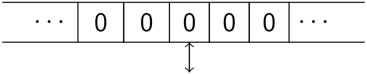
$$\begin{pmatrix} X & y_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X & y_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & y_2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X^{-1} & y_3 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X^{-1} & y_3 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$$

The special case: path of the run

Consider a sequence that might reach I:

$$\begin{pmatrix} X & y_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X & y_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & y_2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X^{-1} & y_3 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X^{-1} & y_3 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$$

The corresponding run:

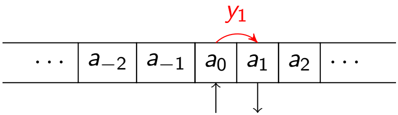


The special case: path of the run

Consider a sequence that might reach I:

$$\begin{pmatrix} X & y_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X & y_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & y_2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X^{-1} & y_3 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X^{-1} & y_3 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$$

The corresponding run:



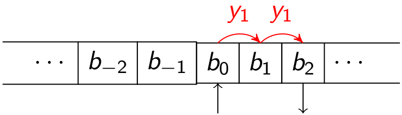
Where $y_1 = \cdots + a_{-2}X^{-2} + a_{-1}X^{-1} + a_0 + a_1 X + a_2 X^2 + \cdots$.

The special case: path of the run

Consider a sequence that might reach I:

$$\begin{pmatrix} X & y_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X & y_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & y_2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X^{-1} & y_3 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X^{-1} & y_3 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$$

The corresponding run:



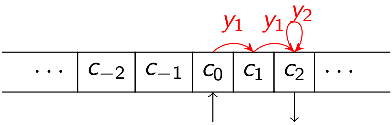
Where $y_1 + X \cdot y_1 = \cdots + b_{-2}X^{-2} + b_{-1}X^{-1} + b_0 + b_1 X + b_2 X^2 + \cdots$.

The special case: path of the run

Consider a sequence that might reach I:

$$\begin{pmatrix} X & y_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X & y_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & y_2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X^{-1} & y_3 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X^{-1} & y_3 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$$

The corresponding run:

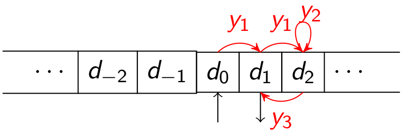


The special case: path of the run

Consider a sequence that might reach I:

$$\begin{pmatrix} X & y_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X & y_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & y_2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X^{-1} & y_3 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X^{-1} & y_3 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$$

The corresponding run:

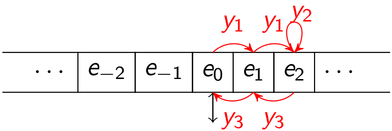


The special case: path of the run

Consider a sequence that might reach I:

$$\begin{pmatrix} X & y_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X & y_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & y_2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X^{-1} & y_3 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X^{-1} & y_3 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$$

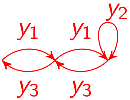
The corresponding run:



The special case: path of the run

Consider a sequence that might reach I:

$$\begin{pmatrix} X & y_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X & y_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & y_2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X^{-1} & y_3 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X^{-1} & y_3 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$$

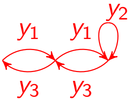
The corresponding run: 

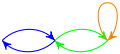
.

The special case: path of the run

Consider a sequence that might reach I:

$$\begin{pmatrix} X & y_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X & y_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & y_2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X^{-1} & y_3 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X^{-1} & y_3 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$$

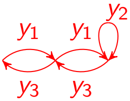
The corresponding run: 

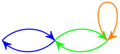
. Decompose into tiles: 

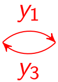
The special case: path of the run

Consider a sequence that might reach I:

$$\begin{pmatrix} X & y_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X & y_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & y_2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X^{-1} & y_3 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X^{-1} & y_3 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$$

The corresponding run: 

. Decompose into tiles: 

It can be decomposed into two tiles of 

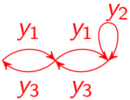
and one tile of 

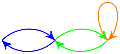
.

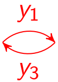
The special case: path of the run

Consider a sequence that might reach I:

$$\begin{pmatrix} X & y_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X & y_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & y_2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X^{-1} & y_3 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X^{-1} & y_3 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$$

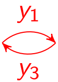
The corresponding run: 

. Decompose into tiles: 

It can be decomposed into two tiles of 

and one tile of 

.

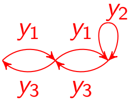
The **effect** of tile 

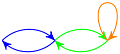
is p_{13} where $\begin{pmatrix} 1 & p_{13} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} X & y_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X^{-1} & y_3 \\ 0 & 1 \end{pmatrix}$.

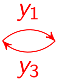
The special case: path of the run

Consider a sequence that might reach I:

$$\begin{pmatrix} X & y_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X & y_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & y_2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X^{-1} & y_3 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X^{-1} & y_3 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$$

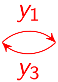
The corresponding run: 

. Decompose into tiles: 

It can be decomposed into two tiles of 

and one tile of 

.

The **effect** of tile 

is p_{13} where $\begin{pmatrix} 1 & p_{13} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} X & y_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X^{-1} & y_3 \\ 0 & 1 \end{pmatrix}$.

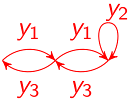
The **effect** of tile 

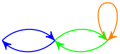
is $p_2 := y_2$

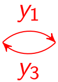
The special case: path of the run

Consider a sequence that might reach I:

$$\begin{pmatrix} X & y_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X & y_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & y_2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X^{-1} & y_3 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X^{-1} & y_3 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$$

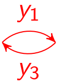
The corresponding run: 

. Decompose into tiles: 

It can be decomposed into two tiles of 

and one tile of 

.

The **effect** of tile 

is p_{13} where $\begin{pmatrix} 1 & p_{13} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} X & y_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} X^{-1} & y_3 \\ 0 & 1 \end{pmatrix}$.

The **effect** of tile 

is $p_2 := y_2$

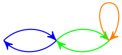
Total effect: $* = (1 + X)p_{13} + X^2 p_2$.

Runs vs Polynomials

The effect of each (cyclic) run is described by a linear combination

$$* = f_{13} p_{13} + f_2 p_2.$$

For example:



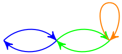
$$\longrightarrow \quad * = (1 + X) p_{13} + X^2 p_2.$$

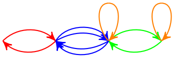
Runs vs Polynomials

The effect of each (cyclic) run is described by a linear combination

$$* = f_{13} p_{13} + f_2 p_2.$$

For example:

 $\longrightarrow$ $* = (1 + X)p_{13} + X^2 p_2.$

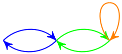
 $\longrightarrow$ $* = (X^{-1} + 2 + X)p_{13} + (X + X^2)p_2.$

Runs vs Polynomials

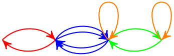
The effect of each (cyclic) run is described by a linear combination

$$* = f_{13} p_{13} + f_2 p_2.$$

For example:



$\longleftrightarrow \quad * = (1 + X) p_{13} + X^2 p_2.$



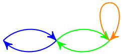
$\longleftrightarrow \quad * = \underbrace{(X^{-1} + 2 + X)}_{\in \mathbb{N}[X^{\pm}]} p_{13} + \underbrace{(X + X^2)}_{\in \mathbb{N}[X^{\pm}]} p_2.$

Runs vs Polynomials

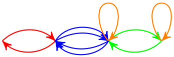
The effect of each (cyclic) run is described by a linear combination

$$* = f_{13} p_{13} + f_2 p_2.$$

For example:



$$\longleftrightarrow \quad * = (1 + X) p_{13} + X^2 p_2.$$



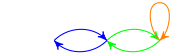
$$\longleftrightarrow \quad * = \underbrace{\left(X^{-1} + 2 + X\right)}_{\in \mathbb{N}[X^{\pm}]} p_{13} + \underbrace{\left(X + X^2\right)}_{\in \mathbb{N}[X^{\pm}]} p_2.$$

Cyclic runs $\overset{?}{\longleftrightarrow}$ $* \in \mathbb{N}[X^{\pm}] \cdot p_{13} + \mathbb{N}[X^{\pm}] \cdot p_2$

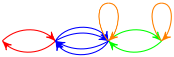
The effect of each (cyclic) run is described by a linear combination

$$* = f_{13} p_{13} + f_2 p_2.$$

For example:



$$\longleftrightarrow \quad * = (1 + X) p_{13} + X^2 p_2.$$



$$\longleftrightarrow \quad * = \underbrace{\left(X^{-1} + 2 + X\right)}_{\in \mathbb{N}[X^{\pm}]} p_{13} + \underbrace{\left(X + X^2\right)}_{\in \mathbb{N}[X^{\pm}]} p_2.$$

Cyclic runs $\overset{?}{\longleftrightarrow}$ $* \in \mathbb{N}[X^{\pm}] \cdot p_{13} + \mathbb{N}[X^{\pm}] \cdot p_2$

Failure:

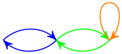
$$\longleftrightarrow \quad * = (X^{-1} + 1) p_{13} + X^2 p_2.$$

Runs vs Polynomials

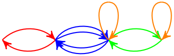
The effect of each (cyclic) run is described by a linear combination

$$* = f_{13} p_{13} + f_2 p_2.$$

For example:



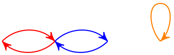
$$\longleftrightarrow \quad * = (1 + X) p_{13} + X^2 p_2.$$



$$\longleftrightarrow \quad * = \underbrace{\left(X^{-1} + 2 + X\right)}_{\in \mathbb{N}[X^{\pm}]} p_{13} + \underbrace{\left(X + X^2\right)}_{\in \mathbb{N}[X^{\pm}]} p_2.$$

Cyclic runs $\overset{?}{\longleftrightarrow}$ $* \in \mathbb{N}[X^{\pm}] \cdot p_{13} + \mathbb{N}[X^{\pm}] \cdot p_2$

Failure:



$$\longleftrightarrow \quad * = (X^{-1} + 1) p_{13} + X^2 p_2.$$

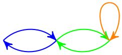
Not connected

Runs vs Polynomials

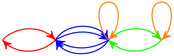
The effect of each (cyclic) run is described by a linear combination

$$* = f_{13} p_{13} + f_2 p_2.$$

For example:



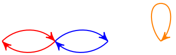
$$\longleftrightarrow \quad * = (1 + X) p_{13} + X^2 p_2.$$



$$\longleftrightarrow \quad * = \underbrace{\left(X^{-1} + 2 + X\right)}_{\in \mathbb{N}[X^{\pm}]} p_{13} + \underbrace{\left(X + X^2\right)}_{\in \mathbb{N}[X^{\pm}]} p_2.$$

$$\text{Cyclic runs} \quad \overset{?}{\longleftrightarrow} \quad * \in \mathbb{N}[X^{\pm}] \cdot p_{13} + \mathbb{N}[X^{\pm}] \cdot p_2$$

Failure:



$$\longleftrightarrow \quad * = (X^{-1} + 1) p_{13} + X^2 p_2.$$

Not connected: **degree** of $f_2 = X^2$ is too big compared to $f_{13} = X^{-1} + 1$

Identity Problem vs linear equations over $\mathbb{N}[X^{\pm}]$

Proposition

There exists a run whose effect is $* = 0$*, if and only if the equation* $0 = f_{13}p_{13} + f_2p_2$ *admits non-zero solutions* $f_{13}, f_2 \in \mathbb{N}[X^{\pm}]^*$ *satisfying* **"degree constraints"**.

Identity Problem vs linear equations over $\mathbb{N}[X^{\pm}]$

Proposition

There exists a run whose effect is $* = 0$*, if and only if the equation* $0 = f_{13}p_{13} + f_2p_2$ *admits non-zero solutions* $f_{13}, f_2 \in \mathbb{N}[X^{\pm}]^*$ *satisfying* **"degree constraints"**.

"degree constraints": $\deg_+(f_2) < \deg_+(f_{13}), \deg_-(f_2) \geq \deg_-(f_{13})$.

Identity Problem vs linear equations over $\mathbb{N}[X^{\pm}]$

Proposition

There exists a run whose effect is $* = 0$*, if and only if the equation* $0 = f_{13}p_{13} + f_2 p_2$ *admits non-zero solutions* $f_{13}, f_2 \in \mathbb{N}[X^{\pm}]^*$ *satisfying* **"degree constraints"**.

"degree constraints": $\deg_+(f_2) < \deg_+(f_{13}), \deg_-(f_2) \geq \deg_-(f_{13})$.

Identity Problem $\Longleftrightarrow$ existence of run with effect $* = 0$.

Identity Problem vs linear equations over $\mathbb{N}[X^{\pm}]$

Proposition

There exists a run whose effect is $* = 0$, if and only if the equation $0 = f_{13}p_{13} + f_2p_2$ admits non-zero solutions $f_{13}, f_2 \in \mathbb{N}[X^{\pm}]^*$ satisfying **"degree constraints"**.

"degree constraints": $\deg_+(f_2) < \deg_+(f_{13}), \deg_-(f_2) \geq \deg_-(f_{13})$.

Identity Problem $\iff$ existence of run with effect $* = 0$.

This not only works for the current example (where we can only move one cell). In general:

Theorem

The Identity Problem in $\mathbb{Z} \wr \mathbb{Z}$ reduces to solving a **system** *of* **homogeneous** *linear equations over $\mathbb{N}[X^{\pm}]^*$, with additional "degree constraints".*

Local-global principle

Does $0 = f_{13} \cdot (2X^2 - 1) + f_2 \cdot (X + 2)$ have solution $f_{13}, f_2 \in \mathbb{N}[X^{\pm}]^*$?

Local-global principle

Does $0 = f_{13} \cdot (2X^2 - 1) + f_2 \cdot (X + 2)$ have solution $f_{13}, f_2 \in \mathbb{N}[X^{\pm}]^*$?

No! Evaluate $X = 1$, then $0 = f_{13}(1) + 3f_2(1)$. No solution over $\mathbb{N}^*$.

Local-global principle

Does $0 = f_{13} \cdot (2X^2 - 1) + f_2 \cdot (X + 2)$ have solution $f_{13}, f_2 \in \mathbb{N}[X^{\pm}]^*$?

No! Evaluate $X = 1$, then $0 = f_{13}(1) + 3f_2(1)$. No solution over $\mathbb{N}^*$.

Such a "certificate" always exists if no solution over $\mathbb{N}[X^{\pm}]^*$:

Theorem (Generalization of Einsiedler, Mouat, Tuncel (2003))

Let $\mathcal{M}$ be an $\mathbb{Z}[X^{\pm}]$-submodule of $\mathbb{Z}[X^{\pm}]^K$. Then there exists $\boldsymbol{f} \in \mathcal{M} \cap (\mathbb{N}[X^{\pm}]^*)^K$ satisfying "degree constraints" if and only if the following are satisfied:

1. *For every $r \in \mathbb{R}_{>0}$, there exists $\boldsymbol{f}_r \in \mathcal{M}$ such that $\boldsymbol{f}_r(r) \in \mathbb{R}^K_{>0}$.*
2. *For $v \in \{+, -\}$, there exists $\boldsymbol{f}_v \in \mathcal{M}$ such that $\mathrm{lt}_v(\boldsymbol{f}_v) \in (\mathbb{N}^*)^K$ satisfies "degree constraints".*

Local-global principle

Does $0 = f_{13} \cdot (2X^2 - 1) + f_2 \cdot (X + 2)$ have solution $f_{13}, f_2 \in \mathbb{N}[X^{\pm}]^*$?

No! Evaluate $X = 1$, then $0 = f_{13}(1) + 3f_2(1)$. No solution over $\mathbb{N}^*$.

Such a "certificate" always exists if no solution over $\mathbb{N}[X^{\pm}]^*$:

Theorem (Generalization of Einsiedler, Mouat, Tuncel (2003))

Let $\mathcal{M}$ be an $\mathbb{Z}[X^{\pm}]$-submodule of $\mathbb{Z}[X^{\pm}]^K$. Then there exists $\boldsymbol{f} \in \mathcal{M} \cap (\mathbb{N}[X^{\pm}]^*)^K$ satisfying "degree constraints" if and only if the following are satisfied:

1. *For every $r \in \mathbb{R}_{>0}$, there exists $\boldsymbol{f}_r \in \mathcal{M}$ such that $\boldsymbol{f}_r(r) \in \mathbb{R}^K_{>0}$.*
2. *For $v \in \{+, -\}$, there exists $\boldsymbol{f}_v \in \mathcal{M}$ such that $\mathrm{lt}_v(\boldsymbol{f}_v) \in (\mathbb{N}^*)^K$ satisfies "degree constraints".*

Therefore, instead of searching for solutions, we search for "certificates". This can be done using the first order theory of $\mathbb{R}$. Decidable (Tarski).

Local-global principle

Does $0 = f_{13} \cdot (2X^2 - 1) + f_2 \cdot (X + 2)$ have solution $f_{13}, f_2 \in \mathbb{N}[X^{\pm}]^*$?

No! Evaluate $X = 1$, then $0 = f_{13}(1) + 3f_2(1)$. No solution over $\mathbb{N}^*$.

Such a "certificate" always exists if no solution over $\mathbb{N}[X^{\pm}]^*$:

Theorem (Generalization of Einsiedler, Mouat, Tuncel (2003))

Let $\mathcal{M}$ be an $\mathbb{Z}[X^{\pm}]$-submodule of $\mathbb{Z}[X^{\pm}]^K$. Then there exists $\boldsymbol{f} \in \mathcal{M} \cap (\mathbb{N}[X^{\pm}]^*)^K$ satisfying "degree constraints" if and only if the following are satisfied:

1. *For every $r \in \mathbb{R}_{>0}$, there exists $\boldsymbol{f}_r \in \mathcal{M}$ such that $\boldsymbol{f}_r(r) \in \mathbb{R}^K_{>0}$.*
2. *For $v \in \{+, -\}$, there exists $\boldsymbol{f}_v \in \mathcal{M}$ such that $\operatorname{lt}_v(\boldsymbol{f}_v) \in (\mathbb{N}^*)^K$ satisfies "degree constraints".*

Therefore, instead of searching for solutions, we search for "certificates". This can be done using the first order theory of $\mathbb{R}$. Decidable (Tarski).

Theorem

The Identity Problem in $\mathbb{Z} \wr \mathbb{Z}$ is decidable.