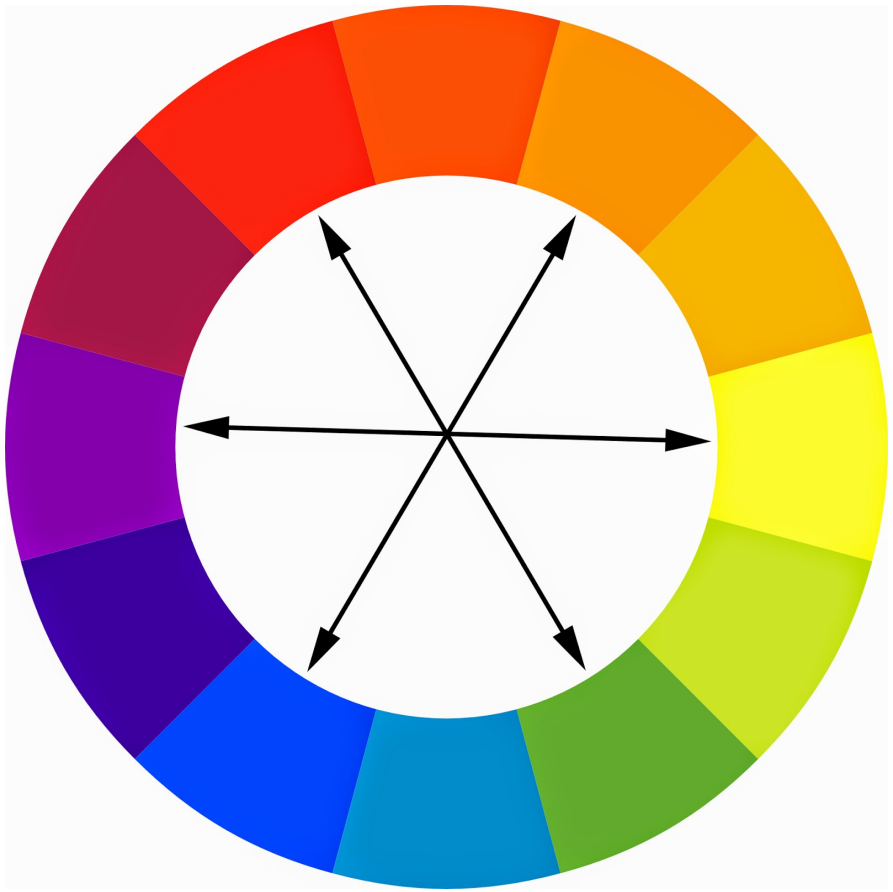
A different way of simulating Turing machines with matrices

Reino Niskanen

School of Computer Science and Mathematics, Liverpool John Moores University, UK

SAMSA'25



Decision problems in matrix semigroup

- Let $S \subseteq \mathbb{K}^{d \times d}$ be a finite set of matrices.
- $\langle S \rangle$ is the semigroup containing all possible matrix products.

A myriad of decision problems.

Decision problems in matrix semigroup

- Let $S \subseteq \mathbb{K}^{d \times d}$ be a finite set of matrices.
- $\langle S \rangle$ is the semigroup containing all possible matrix products.

A myriad of decision problems.

- Membership Problem: Given matrix M. Does $M \in \langle S \rangle$ hold?

Decision problems in matrix semigroup

- Let $S \subseteq \mathbb{K}^{d \times d}$ be a finite set of matrices.
- $\langle S \rangle$ is the semigroup containing all possible matrix products.

A myriad of decision problems.

- Membership Problem: Given matrix M. Does $M \in \langle S \rangle$ hold?
- Identity Problem: Let I be the identity matrix. Does $I \in \langle S \rangle$ hold?

Decision problems in matrix semigroup

- Let $S \subseteq \mathbb{K}^{d \times d}$ be a finite set of matrices.
- $\langle S \rangle$ is the semigroup containing all possible matrix products.

A myriad of decision problems.

- Membership Problem: Given matrix M. Does $M \in \langle S \rangle$ hold?
- Identity Problem: Let I be the identity matrix. Does $I \in \langle S \rangle$ hold?
- Mortality Problem: Let O be the zero matrix. Does $O \in \langle S \rangle$ hold?

Decision problems in matrix semigroup

- Let $S \subseteq \mathbb{K}^{d \times d}$ be a finite set of matrices.
- $\langle S \rangle$ is the semigroup containing all possible matrix products.

A myriad of decision problems.

- Membership Problem: Given matrix M. Does $M \in \langle S \rangle$ hold?
- Identity Problem: Let I be the identity matrix. Does $I \in \langle S \rangle$ hold?
- Mortality Problem: Let O be the zero matrix. Does $O \in \langle S \rangle$ hold?
- Vector Reachability Problem: Let $\boldsymbol{u}, \boldsymbol{v}$ be two vectors. Does there exist $M \in \langle S \rangle$ such that $\boldsymbol{u} = M\boldsymbol{v}$?

Decision problems in matrix semigroup

- Let $S \subseteq \mathbb{K}^{d \times d}$ be a finite set of matrices.
- $\langle S \rangle$ is the semigroup containing all possible matrix products.

A myriad of decision problems.

- Membership Problem: Given matrix M. Does $M \in \langle S \rangle$ hold?
- Identity Problem: Let I be the identity matrix. Does $I \in \langle S \rangle$ hold?
- Mortality Problem: Let O be the zero matrix. Does $O \in \langle S \rangle$ hold?
- Vector Reachability Problem: Let $\boldsymbol{u}, \boldsymbol{v}$ be two vectors. Does there exist $M \in \langle S \rangle$ such that $\boldsymbol{u} = M\boldsymbol{v}$?
- Freeness Problem: Is $\langle S \rangle$ free, i.e., is there a matrix $M \in \langle S \rangle$ that can be generated in two different ways?

Restricting parameters

The general problems tend to be undecidable.

Restricting parameters

The general problems tend to be undecidable.

Consider instead restrictions to:

- dimensions of matrices (e.g., at most 2);
- number of generators (e.g., 2 generators);
- number systems used (e.g., natural numbers);
- types of matrices (e.g., upper triangular);

Isn't this too restrictive?

Freeness Problem

Let $S \subseteq \mathbb{K}^{d \times d}$ be a finite set of matrices. Is $\langle S \rangle$ free, i.e., is there a matrix $M \in \langle S \rangle$ that can be generated in two different ways?

Isn't this too restrictive?

Freeness Problem

Let $S \subseteq \mathbb{K}^{d \times d}$ be a finite set of matrices. Is $\langle S \rangle$ free, i.e., is there a matrix $M \in \langle S \rangle$ that can be generated in two different ways?

Restricted Freeness Instance

Is the semigroup generated by $A = \left(\begin{smallmatrix} 2 & 0 \\ 0 & 3 \end{smallmatrix}\right)$ and $B = \left(\begin{smallmatrix} 3 & 5 \\ 0 & 5 \end{smallmatrix}\right)$ free?

Isn't this too restrictive?

Freeness Problem

Let $S \subseteq \mathbb{K}^{d \times d}$ be a finite set of matrices. Is $\langle S \rangle$ free, i.e., is there a matrix $M \in \langle S \rangle$ that can be generated in two different ways?

Restricted Freeness Instance

Is the semigroup generated by $A = \left(\begin{smallmatrix} 2 & 0 \\ 0 & 3 \end{smallmatrix}\right)$ and $B = \left(\begin{smallmatrix} 3 & 5 \\ 0 & 5 \end{smallmatrix}\right)$ free?

Stated as an open problem in 1999.

Isn't this too restrictive?

Freeness Problem

Let $S \subseteq \mathbb{K}^{d \times d}$ be a finite set of matrices. Is $\langle S \rangle$ free, i.e., is there a matrix $M \in \langle S \rangle$ that can be generated in two different ways?

Restricted Freeness Instance

Is the semigroup generated by $A = \left(\begin{smallmatrix} 2 & 0 \\ 0 & 3 \end{smallmatrix}\right)$ and $B = \left(\begin{smallmatrix} 3 & 5 \\ 0 & 5 \end{smallmatrix}\right)$ free?

Stated as an open problem in 1999.

Two independent solutions in 2009.

Isn't this too restrictive?

Freeness Problem

Let $S \subseteq \mathbb{K}^{d \times d}$ be a finite set of matrices. Is $\langle S \rangle$ free, i.e., is there a matrix $M \in \langle S \rangle$ that can be generated in two different ways?

Restricted Freeness Instance

Is the semigroup generated by $A = \left(\begin{smallmatrix} 2 & 0 \\ 0 & 3 \end{smallmatrix}\right)$ and $B = \left(\begin{smallmatrix} 3 & 5 \\ 0 & 5 \end{smallmatrix}\right)$ free?

Stated as an open problem in 1999.

Two independent solutions in 2009.

$$AB^{10}A^2BA^2BA^{10} = B^2A^6B^2A^2BABABA^2B^2A^2BAB^2$$

with no shorter relations.

The landscape

dim. \ $\mathbb{K}$	$\mathbb{N}$	$\mathbb{Z}$	$\mathbb{Q}$
2			
3			
4			

Key: an undecidable problem, a decidable problem, * a restricted variant of a problem

The landscape

dim. \ $\mathbb{K}$	$\mathbb{N}$	$\mathbb{Z}$	$\mathbb{Q}$
2			
3	Freeness	Membership, Mortality, VRP	
4		Identity	

Key: an undecidable problem, a decidable problem, * a restricted variant of a problem

The landscape

dim. \ $\mathbb{K}$	$\mathbb{N}$	$\mathbb{Z}$	$\mathbb{Q}$
2		Membership*, Mortality*, Identity, VRP*, Freeness*	
3	Freeness	Membership, Mortality, VRP	
4		Identity	

Key: an undecidable problem, a decidable problem, * a restricted variant of a problem

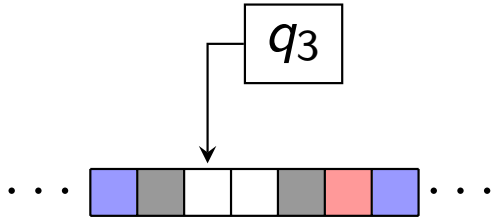
The landscape

dim. \ $\mathbb{K}$	$\mathbb{N}$	$\mathbb{Z}$	$\mathbb{Q}$
2	Freeness?	Membership*, Mortality*, Identity, VRP*, Freeness*	
3	Freeness	Membership, Mortality, VRP, Identity?	
4		Identity	

Key: an undecidable problem, a decidable problem, * a restricted variant of a problem

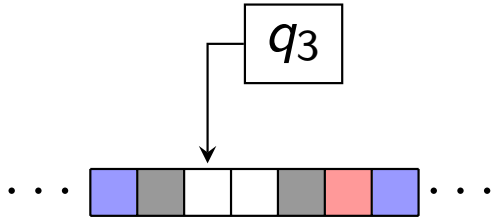
Towards the undecidability

- Turing machines have an undecidable halting problem: $(u, (q, a), v) \rightarrow^* (\varepsilon, (q_h, \star), \varepsilon)$?



Towards the undecidability

- Turing machines have an undecidable halting problem: $(u, (q, a), v) \to^* (\varepsilon, (q_h, \star), \varepsilon)$?

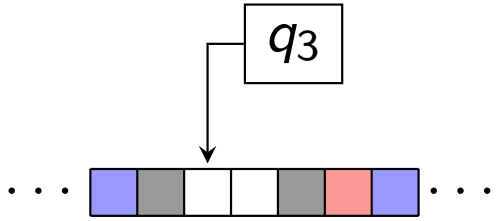


Post Correspondence Problem (Post'46)

Given two morphisms $g, h : A^* \to B^*$. Does there exist a word $w \in A^*$ such that $g(w) = h(w)$?

Towards the undecidability

- Turing machines have an undecidable halting problem: $(u, (q, a), v) \rightarrow^* (\varepsilon, (q_h, \star), \varepsilon)$?



Post Correspondence Problem (Post'46)

Given two morphisms $g, h : A^* \rightarrow B^*$. Does there exist a word $w \in A^*$ such that $g(w) = h(w)$?

A computation of a Turing-complete model can be simulated with two morphisms.

$$\frac{g(w)}{h(w)} = \frac{}{\#conf_0}\,\frac{\#}{\#}\,\frac{conf_0}{conf_1}\frac{\#}{\#}\frac{conf_1}{conf_2}\frac{\#}{\#}\cdots\frac{\#}{\#}\frac{conf_{halt}\#}{}$$

Constructed in such way that words are equal if and only if the machine halts.

Application of the PCP

- The next aim is to find an embedding $\{1,2\}^* \times \{1,2\}^* \hookrightarrow \mathbb{K}^{d \times d}$

Embedding pairs of words

- Define $\sigma : \{1,2\}^* \to \mathbb{N}$: For a word $w_1 w_2 \cdots w_k \in \{1,2\}^*$, $\sigma(w_1 w_2 \cdots w_k) = 3^{k-1} w_1 + 3^{k-2} w_2 + \ldots + 3^0 w_k$.

Embedding pairs of words

- Define $\sigma : \{1,2\}^* \to \mathbb{N}$: For a word $w_1 w_2 \cdots w_k \in \{1,2\}^*$, $\sigma(w_1 w_2 \cdots w_k) = 3^{k-1} w_1 + 3^{k-2} w_2 + \ldots + 3^0 w_k$.
- This is a base 3 representation of a binary word.
- Now $\sigma(uv) = 3^{|v|}\sigma(u) + \sigma(v)$, for all $u, v \in \{1,2\}^*$.

Embedding pairs of words

- Define $\sigma : \{1,2\}^* \to \mathbb{N}$: For a word $w_1 w_2 \cdots w_k \in \{1,2\}^*$, $\sigma(w_1 w_2 \cdots w_k) = 3^{k-1} w_1 + 3^{k-2} w_2 + \ldots + 3^0 w_k$.
- This is a base 3 representation of a binary word.
- Now $\sigma(uv) = 3^{|v|}\sigma(u) + \sigma(v)$, for all $u, v \in \{1,2\}^*$.
- Define $\gamma : \{1,2\}^* \times \{1,2\}^* \to \mathbb{N}^{3\times 3}$ be the mapping

$$\gamma(u,v) = \begin{pmatrix} 3^{|u|} & 0 & 0 \\ 0 & 3^{|v|} & 0 \\ \sigma(u) & \sigma(v) & 1 \end{pmatrix}.$$

Embedding pairs of words

- Define $\sigma : \{1,2\}^* \to \mathbb{N}$: For a word $w_1 w_2 \cdots w_k \in \{1,2\}^*$, $\sigma(w_1 w_2 \cdots w_k) = 3^{k-1} w_1 + 3^{k-2} w_2 + \ldots + 3^0 w_k$.
- This is a base 3 representation of a binary word.
- Now $\sigma(uv) = 3^{|v|}\sigma(u) + \sigma(v)$, for all $u, v \in \{1,2\}^*$.
- Define $\gamma : \{1,2\}^* \times \{1,2\}^* \to \mathbb{N}^{3\times 3}$ be the mapping

$$\gamma(u,v) = \begin{pmatrix} 3^{|u|} & 0 & 0 \\ 0 & 3^{|v|} & 0 \\ \sigma(u) & \sigma(v) & 1 \end{pmatrix}.$$

- This is a morphism and one can define such matrix $\gamma(g(a), h(a))$ for each letter a of the PCP instance.

What if embedding doesn't exist?

- In 1999, Cassaigne, Harju and Karhumäki showed that there is no injective morphism from $\{a, b\}^* \times \{a, b\}^*$ into $\mathbb{C}^{2\times 2}$.

What if embedding doesn't exist?

- In 1999, Cassaigne, Harju and Karhumäki showed that there is no injective morphism from $\{a, b\}^* \times \{a, b\}^*$ into $\mathbb{C}^{2\times 2}$.
- Suggests decidability as virtually all undecidability results rely on such an embedding.

What if embedding doesn't exist?

- In 1999, Cassaigne, Harju and Karhumäki showed that there is no injective morphism from $\{a, b\}^* \times \{a, b\}^*$ into $\mathbb{C}^{2\times 2}$.
- Suggests decidability as virtually all undecidability results rely on such an embedding.
- Does not mean that the decidability will be straightforward.

Embedding into 3×3 matrices

Theorem (Ko, Niskanen, Potapov'18)

There is no embedding from $\{a, b\}^* \times \{a, b\}^*$ into $SL(3, \mathbb{Z})$.

Embedding into 3×3 matrices

Theorem (Ko, Niskanen, Potapov'18)

There is no embedding from $\{a, b\}^* \times \{a, b\}^*$ into $SL(3, \mathbb{Z})$.

Proof idea:

- $\{a, b\}^* \times \{a, b\}^*$ has relations like $(a, \varepsilon)(\varepsilon, a) = (\varepsilon, a)(a, \varepsilon)$ and $(a, \varepsilon)(b, \varepsilon) \neq (b, \varepsilon)(a, \varepsilon)$.
- For a hypothetical embedding γ, $\gamma(a, \varepsilon)\gamma(\varepsilon, a) = \gamma(\varepsilon, a)\gamma(a, \varepsilon)$ etc.
- Solving these equations shows that any assignment $\gamma(a, \varepsilon) = M \in SL(3, \mathbb{Z})$ contradicts some relation.

Other impossible embeddings

2nd component \ 1st component	binary semigroup	unary free group	binary free group
$\emptyset$			$U(n, \mathbb{C})$
binary semigroup	$\mathbb{C}^{2\times 2}$, $\mathrm{SL}(3, \mathbb{Z})$	$\mathbb{Z}^{2\times 2}$	$\mathbb{Z}^{3\times 3}$
unary free group			$\mathbb{Z}^{2\times 2}$
binary free group			$\mathbb{Z}^{3\times 3}$

The identity problem

The identity problem

Let $S \subseteq \mathbb{K}^{d \times d}$ be a finite set of matrices and let I be the identity matrix. Does $I \in \langle S \rangle$ hold?

- Remains open for three-dimensional matrices.
- Known to be decidable for two-dimensional matrices.
- Known to be undecidable for four-dimensional matrices.

The identity problem

The identity problem

Let $S \subseteq \mathbb{K}^{d \times d}$ be a finite set of matrices and let I be the identity matrix. Does $I \in \langle S \rangle$ hold?

- Remains open for three-dimensional matrices.
- Known to be decidable for two-dimensional matrices.
- Known to be undecidable for four-dimensional matrices.
  - Uses $f : \mathrm{FG}(\Sigma_2) \hookrightarrow \mathbb{Z}^{2 \times 2}$ as blocks in a 4-by-4 matrix.

The identity problem

The identity problem

Let $S \subseteq \mathbb{K}^{d \times d}$ be a finite set of matrices and let I be the identity matrix. Does $I \in \langle S \rangle$ hold?

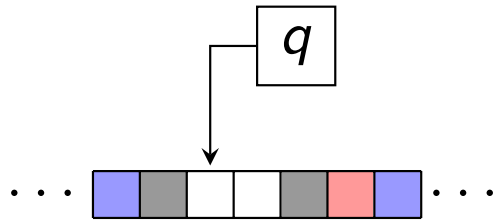
- Remains open for three-dimensional matrices.
- Known to be decidable for two-dimensional matrices.
- Known to be undecidable for four-dimensional matrices.
  - Uses $f : \mathrm{FG}(\Sigma_2) \hookrightarrow \mathbb{Z}^{2\times 2}$ as blocks in a 4-by-4 matrix.
  - Now, $\gamma(u, v) = \begin{pmatrix} f(u) & \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right) \\ \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right) & f(v) \end{pmatrix}$ can be used to simulate a computation of the PCP.

Another way?

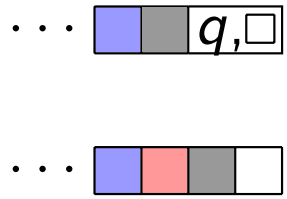
- Typically building sequences of words is encoded into the model.
- The whole computation is stored.
- For this addition dimensions are required.

Simulating directly

TM:

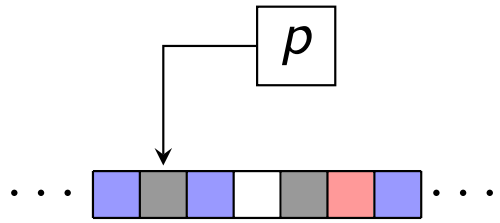


Simulation:

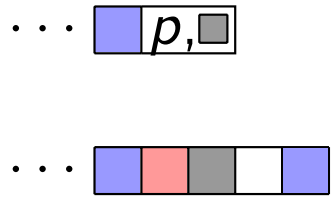


Simulating directly

TM:

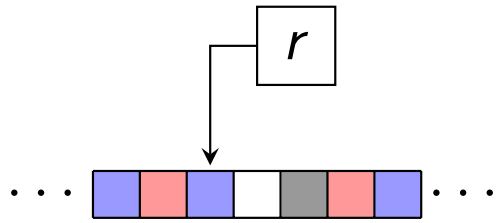


Simulation:

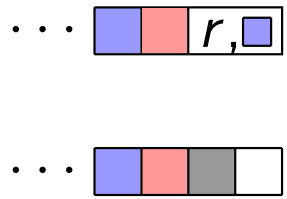


Simulating directly

TM:



Simulation:



Simulating directly

- Let $\mathcal{M}$ be a TM.
- Map a configuration $(u, (q, a), v)$ to a pair of words $(u(q, a), v^R)$, where (q, a) is treated as a single letter.

Simulating directly

- Let $\mathcal{M}$ be a TM.
- Map a configuration $(u, (q, a), v)$ to a pair of words $(u(q, a), v^R)$, where (q, a) is treated as a single letter.
- Define $\gamma : \{a_1, \ldots, a_m\}^* \times \{a_1, \ldots, a_m\}^* \to \mathbb{N}^{3\times 3}$ be the mapping

$$\gamma(u, v^R) = \begin{pmatrix} n^{|u|} & 0 & 0 \\ 0 & n^{|v|} & 0 \\ \sigma(u) & \sigma(v^R) & 1 \end{pmatrix},$$

where σ is a base n ($n \gg m$) representation of a word.

Simulating directly

- Let $\mathcal{M}$ be a TM.
- Map a configuration $(u, (q, a), v)$ to a pair of words $(u(q, a), v^R)$, where (q, a) is treated as a single letter.
- Define $\gamma : \{a_1, \ldots, a_m\}^* \times \{a_1, \ldots, a_m\}^* \to \mathbb{N}^{3\times 3}$ be the mapping

$$\gamma(u, v^R) = \begin{pmatrix} n^{|u|} & 0 & 0 \\ 0 & n^{|v|} & 0 \\ \sigma(u) & \sigma(v^R) & 1 \end{pmatrix},$$

  where σ is a base n ($n \gg m$) representation of a word.
- Each letter a_j is mapped to $\prod_{\substack{i=1 \\ i\neq j}}^{m} p_i$, where p_i are prime numbers.

Simulating directly

- Let $\mathcal{M}$ be a TM.
- Map a configuration $(u, (q, a), v)$ to a pair of words $(u(q, a), v^R)$, where (q, a) is treated as a single letter.
- Define $\gamma : \{a_1, \ldots, a_m\}^* \times \{a_1, \ldots, a_m\}^* \to \mathbb{N}^{3\times 3}$ be the mapping

$$\gamma(u, v^R) = \begin{pmatrix} n^{|u|} & 0 & 0 \\ 0 & n^{|v|} & 0 \\ \sigma(u) & \sigma(v^R) & 1 \end{pmatrix},$$

  where σ is a base n ($n \gg m$) representation of a word.
- Each letter a_j is mapped to $\prod_{\substack{i=1 \\ i\neq j}}^{m} p_i$, where p_i are prime numbers.
- For each transition of the TM define matrices that update $n^{|u|}, n^{|v|}, \sigma(u)$ and $\sigma(v^R)$ appropriately.

Observations

- A TM configuration is integral (even over naturals);
  but matrices are not.

Observations

- A TM configuration is integral (even over naturals);
  but matrices are not.
- Multiplying by a "correct" matrix keeps the result integral;
  but "incorrect" does not guarantee a non-integer matrix.

How to deal with errors?

Allow to test for rationality.

- Disallows applying transitions with the wrong source, $\boxed{p,\blacksquare}$, when the configuration is $\boxed{q,\blacksquare}$ when the head is moving left.
- Allows to go to a state with an incorrect letter being read ($\boxed{p,\blacksquare}$ instead of $\boxed{p,\blacksquare}$) when the head is moving left.

How to deal with errors?

Allow to test for rationality.

- Disallows applying transitions with the wrong source, $\boxed{p,\blacksquare}$, when the configuration is $\boxed{q,\blacksquare}$ when the head is moving left.
- Allows to go to a state with an incorrect letter being read ($\boxed{p,\blacksquare}$ instead of $\boxed{p,\blacksquare}$) when the head is moving left.
- Moving over this location is no longer possible.
- The encoding ensures that it cannot be corrected.

Differences from the standard embedding

- Simulation is more direct.
- Absolute values of entries are not strictly increasing.

Differences from the standard embedding

- Simulation is more direct.
- Absolute values of entries are not strictly increasing.

Theorem (Halava, Niskanen'24)

The identity problem with rational tests is undecidable for $\mathbb{Q}^{3\times 3}$ *matrices.*

Differences from the standard embedding

- Simulation is more direct.
- Absolute values of entries are not strictly increasing.

Theorem (Halava, Niskanen'24)

The identity problem with rational tests is undecidable for $\mathbb{Q}^{3\times 3}$ *matrices.*

- Sometimes a choice of embedding matters.
- Knowing whether an embedding exists or not can be used as a guide.
- Question: Where else can this be applied?

Thank you for your attention!