# Membership problem for $2 \times 2$ integer matrices

Pavel Semukhin

joint work with Igor Potapov

Department of Computer Science, University of Liverpool

24 July, 2017

This work was supported by EPSRC grant "Reachability problems for words, matrices and maps" (EP/M00077X/1)

# Definitions

## Membership problem

Let $M$ be an $n \times n$ matrix and $F = \{M_1, \ldots, M_k\}$ be a finite collection of $n \times n$ matrices. Determine whether $M \in \langle F \rangle$, that is, whether

$$M = M_{i_1} M_{i_2} \cdots M_{i_t}$$

for some sequence of matrices $M_{i_1}, M_{i_2}, \ldots, M_{i_t} \in F$.

# Known results

- Membership problem is algorithmically undecidable for $3 \times 3$ matrices over integers, even if we assume that $M$ is the zero matrix. [Paterson, 1970]

# Known results

- Membership problem is algorithmically undecidable for $3 \times 3$ matrices over integers, even if we assume that $M$ is the zero matrix. [Paterson, 1970]
- Membership problem is decidable in PTIME for commuting matrices (over algebraic numbers) [Babai, et. al., 1996]

# Known results

- Membership problem is algorithmically undecidable for $3 \times 3$ matrices over integers, even if we assume that $M$ is the zero matrix. [Paterson, 1970]
- Membership problem is decidable in PTIME for commuting matrices (over algebraic numbers) [Babai, et. al., 1996]
- The Membership problem is decidable for matrices from $\mathrm{GL}(2, \mathbb{Z})$, where $\mathrm{GL}(2, \mathbb{Z})$ is a group of $2 \times 2$ integer matrices with determinant $\pm 1$. [C. Choffrut and J. Karhumäki, 2005]

# Known results

- Membership problem is algorithmically undecidable for $3 \times 3$ matrices over integers, even if we assume that $M$ is the zero matrix. [Paterson, 1970]
- Membership problem is decidable in PTIME for commuting matrices (over algebraic numbers) [Babai, et. al., 1996]
- The Membership problem is decidable for matrices from $\mathrm{GL}(2, \mathbb{Z})$, where $\mathrm{GL}(2, \mathbb{Z})$ is a group of $2 \times 2$ integer matrices with determinant $\pm 1$. [C. Choffrut and J. Karhumäki, 2005]
- It is a long standing open question whether the Membership problem is decidable for $2 \times 2$ matrices (even over integers).

# Main result

A matrix is nonsingular if it has a nonzero determinant.

A matrix is nonsingular if it has a nonzero determinant.

**Main result**

Given a finite collection $F$ of nonsingular matrices from $\mathbb{Z}^{2\times 2}$ and a nonsingular matrix $M \in \mathbb{Z}^{2\times 2}$, it is decidable whether $M \in \langle F \rangle$.

Let $F = \{M_1, \ldots, M_k\} \cup \{N_1, \ldots, N_r\}$,
where $\det(M_i) \neq \pm 1$ and $N_i \in \mathrm{GL}(2, \mathbb{Z})$.

Let $\mathcal{S} = \langle N_1, \ldots, N_r \rangle$ be the semigroup which is generated by the matrices from $F$ which belong to $\mathrm{GL}(2, \mathbb{Z})$.

Let $F = \{M_1, \ldots, M_k\} \cup \{N_1, \ldots, N_r\}$,
where $\det(M_i) \neq \pm 1$ and $N_i \in \mathrm{GL}(2, \mathbb{Z})$.

Let $\mathcal{S} = \langle N_1, \ldots, N_r \rangle$ be the semigroup which is generated by the matrices from $F$ which belong to $\mathrm{GL}(2, \mathbb{Z})$.

$M \in \langle F \rangle$ iff there exist $i_1, \ldots, i_t \in \{1, \ldots, k\}$ and matrices $A_1, \ldots, A_t, A_{t+1} \in \mathcal{S}$ such that

$$M = A_1 M_{i_1} A_2 M_{i_2} \cdots A_t M_{i_t} A_{t+1}.$$

Let $F = \{M_1, \ldots, M_k\} \cup \{N_1, \ldots, N_r\}$,
where $\det(M_i) \neq \pm 1$ and $N_i \in \mathrm{GL}(2, \mathbb{Z})$.

Let $\mathcal{S} = \langle N_1, \ldots, N_r \rangle$ be the semigroup which is generated by the matrices from $F$ which belong to $\mathrm{GL}(2, \mathbb{Z})$.

$M \in \langle F \rangle$ iff there exist $i_1, \ldots, i_t \in \{1, \ldots, k\}$ and matrices $A_1, \ldots, A_t, A_{t+1} \in \mathcal{S}$ such that

$$M = A_1 M_{i_1} A_2 M_{i_2} \cdots A_t M_{i_t} A_{t+1}.$$

The value of $t$ is bounded: since $|\det(M_i)| \geq 2$, we have that $t \leq \log_2 |\det(M)|$.

So, to decide whether $M \in \langle F \rangle$ we go through all sequences $i_1, \ldots, i_t \in \{1, \ldots, k\}$ of length up to $\log_2 |\det(M)|$ and for each such sequence check whether there are matrices $A_1, \ldots, A_t, A_{t+1} \in \mathcal{S}$ such that

$$M = A_1 M_{i_1} A_2 M_{i_2} \cdots A_t M_{i_t} A_{t+1}.$$

So, to decide whether $M \in \langle F \rangle$ we go through all sequences $i_1, \ldots, i_t \in \{1, \ldots, k\}$ of length up to $\log_2 |\det(M)|$ and for each such sequence check whether there are matrices $A_1, \ldots, A_t, A_{t+1} \in \mathcal{S}$ such that

$$M = A_1 M_{i_1} A_2 M_{i_2} \cdots A_t M_{i_t} A_{t+1}.$$

**Theorem**

*Given a nonsingular matrices $M$ and $M_1, \ldots, M_t$ and a finitely generated semigroup $\mathcal{S} \subseteq \mathrm{GL}(2, \mathbb{Z})$, it is decidable whether there are matrices $A_1, \ldots, A_t, A_{t+1} \in \mathcal{S}$ such that*

$$M = A_1 M_1 A_2 M_2 \cdots A_t M_t A_{t+1}.$$

# Proof sketch: The base case

The proof is by induction on $t$.

# Proof sketch: The base case

The proof is by induction on $t$.

The base case $t = 1$: $\quad M = A_1 M_1 A_2$.

# Proof sketch: The base case

The proof is by induction on $t$.

The base case $t = 1$: $\quad M = A_1 M_1 A_2$.

**Theorem (Smith Normal Form)**

*For any matrix $A \in \mathbb{Z}^{2\times 2}$, there are matrices $E, F$ from $\mathrm{GL}(2,\mathbb{Z})$ such that $A = E \begin{bmatrix} m & 0 \\ 0 & nm \end{bmatrix} F$ for some $n, m \in \mathbb{N}$.*

*The numbers $n$ and $m$ are uniquely defined by $A$. The diagonal matrix $D = \begin{bmatrix} m & 0 \\ 0 & nm \end{bmatrix}$ is called the Smith normal form of $A$.*

# Proof sketch: The base case

If $M = A_1 M_1 A_2$, then $M$ and $M_1$ must have the same Smith normal form $D$ because $A_1, A_2 \in \mathrm{GL}(2, \mathbb{Z})$.

# Proof sketch: The base case

If $M = A_1 M_1 A_2$, then $M$ and $M_1$ must have the same Smith normal form $D$ because $A_1, A_2 \in \mathrm{GL}(2, \mathbb{Z})$.

The base case $t = 1$: $\qquad M = A_1 M_1 A_2$.

# Proof sketch: The base case

If $M = A_1 M_1 A_2$, then $M$ and $M_1$ must have the same Smith normal form $D$ because $A_1, A_2 \in \mathrm{GL}(2, \mathbb{Z})$.

The base case $t = 1$: $\quad D = A_1 D A_2$, where $D = \begin{bmatrix} 1 & 0 \\ 0 & n \end{bmatrix}$.

# Proof sketch: The base case

If $M = A_1 M_1 A_2$, then $M$ and $M_1$ must have the same Smith normal form $D$ because $A_1, A_2 \in \mathrm{GL}(2, \mathbb{Z})$.

The base case $t = 1$: $\quad D = A_1 D A_2$, where $D = \begin{bmatrix} 1 & 0 \\ 0 & n \end{bmatrix}$.

**Theorem**

*Given a matrix* $D = \begin{bmatrix} 1 & 0 \\ 0 & n \end{bmatrix}$ *and a finitely generated semigroup* $\mathcal{S} \subseteq \mathrm{GL}(2, \mathbb{Z})$*, it is decidable whether there are matrices* $A_1, A_2 \in \mathcal{S}$ *such that*

$$D = A_1 D A_2.$$

# Proof sketch: The base case

$D = \begin{bmatrix} 1 & 0 \\ 0 & n \end{bmatrix}$. The equation $D = A_1 D A_2$ is equivalent to

$$A_2^{-1} = D^{-1} A_1 D = A_1^D.$$

# Proof sketch: The base case

$D = \begin{bmatrix} 1 & 0 \\ 0 & n \end{bmatrix}$. The equation $D = A_1 D A_2$ is equivalent to

$$A_2^{-1} = D^{-1} A_1 D = A_1^D.$$

Let $A_1 = \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix}$ and $A_2 = \begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix}$, then we have

$$\begin{bmatrix} b_4 & -b_2 \\ -b_3 & b_1 \end{bmatrix} = \begin{bmatrix} a_1 & n a_2 \\ \frac{1}{n} a_3 & a_4 \end{bmatrix}$$

# Proof sketch: The base case

$D = \begin{bmatrix} 1 & 0 \\ 0 & n \end{bmatrix}$. The equation $D = A_1 D A_2$ is equivalent to

$$A_2^{-1} = D^{-1} A_1 D = A_1^D.$$

Let $A_1 = \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix}$ and $A_2 = \begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix}$, then we have

$$\begin{bmatrix} b_4 & -b_2 \\ -b_3 & b_1 \end{bmatrix} = \begin{bmatrix} a_1 & na_2 \\ \frac{1}{n} a_3 & a_4 \end{bmatrix}$$

If the above equation has a solution, then $n$ divides $a_3$.

# Proof sketch: The base case

$D = \begin{bmatrix} 1 & 0 \\ 0 & n \end{bmatrix}$. The equation $D = A_1 D A_2$ is equivalent to

$$A_2^{-1} = D^{-1} A_1 D = A_1^D.$$

Let $A_1 = \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix}$ and $A_2 = \begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix}$, then we have

$$\begin{bmatrix} b_4 & -b_2 \\ -b_3 & b_1 \end{bmatrix} = \begin{bmatrix} a_1 & n a_2 \\ \frac{1}{n} a_3 & a_4 \end{bmatrix}$$

If the above equation has a solution, then $n$ divides $a_3$.

Let $H = \left\{ \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \in \mathrm{GL}(2, \mathbb{Z}) \ : \ n \text{ divides } a_3 \right\}$.

Thus $A \in H$ if and only if $A^D \in \mathrm{GL}(2, \mathbb{Z})$.

# Proof sketch: The base case

**Proposition**

$H$ is a subgroup of $\mathrm{GL}(2, \mathbb{Z})$ of finite index (at most $n^2$).

# Proof sketch: The base case

**Proposition**

$H$ is a subgroup of $\mathrm{GL}(2,\mathbb{Z})$ of finite index (at most $n^2$).

A right coset of $H$ in $\mathrm{GL}(2,\mathbb{Z})$ is a subset

$$HU = \{AU \; : \; A \in H\},$$

where $U \in \mathrm{GL}(2,\mathbb{Z})$.

# Proof sketch: The base case

**Proposition**

$H$ is a subgroup of $\mathrm{GL}(2,\mathbb{Z})$ of finite index (at most $n^2$).

A right coset of $H$ in $\mathrm{GL}(2,\mathbb{Z})$ is a subset

$$HU = \{AU \ : \ A \in H\},$$

where $U \in \mathrm{GL}(2,\mathbb{Z})$.

The index is $H$ in $\mathrm{GL}(2,\mathbb{Z})$ is the number of right cosets of $H$.

The group $\mathrm{GL}(2, \mathbb{Z})$ is generated by the matrices $S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$, $R = \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}$ and $N = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.

# Presentation of matrices by words

The group $\mathrm{GL}(2,\mathbb{Z})$ is generated by the matrices
$S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$, $R = \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}$ and $N = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.

So any matrix $A \in \mathrm{GL}(2,\mathbb{Z})$ is represented by a word in the alphabet $\Sigma = \{S, R, N\}$.

# Presentation of matrices by words

The group $\mathrm{GL}(2,\mathbb{Z})$ is generated by the matrices $S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$, $R = \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}$ and $N = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.

So any matrix $A \in \mathrm{GL}(2,\mathbb{Z})$ is represented by a word in the alphabet $\Sigma = \{S, R, N\}$.

This presentation is not unique because $S^2 = R^3 = -I$.

# Presentation of matrices by words

The group $\mathrm{GL}(2,\mathbb{Z})$ is generated by the matrices
$S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$, $R = \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}$ and $N = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.

So any matrix $A \in \mathrm{GL}(2,\mathbb{Z})$ is represented by a word in the alphabet $\Sigma = \{S, R, N\}$.
This presentation is not unique because $S^2 = R^3 = -I$.

However, for every $M \in \mathrm{GL}(2,\mathbb{Z})$ there is a unique canonical word $w \in \{S, R, N\}^*$ which represents $M$.

A word $w$ is canonical if it does not contain subwords $SS$ and $RRR$ and $N$ appears only in the first position of $w$.

# Regular subsets

A subset $\mathcal{S}$ of $\mathrm{GL}(2,\mathbb{Z})$ is regular if there is a regular language $L$ in the alphabet $\Sigma = \{S, R, N\}$ such that

- Every word $w \in L$ represents a matrix from the subset $\mathcal{S}$.
- For any $A \in \mathcal{S}$, there is at least one $w \in L$ such that $w$ represents $A$.

# Regular subsets

A subset $\mathcal{S}$ of $\mathrm{GL}(2, \mathbb{Z})$ is regular if there is a regular language $L$ in the alphabet $\Sigma = \{S, R, N\}$ such that

- Every word $w \in L$ represents a matrix from the subset $\mathcal{S}$.
- For any $A \in \mathcal{S}$, there is at least one $w \in L$ such that $w$ represents $A$.

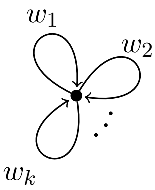
A semigroup $\mathcal{S} = \langle M_1, \ldots, M_k \rangle$ is defined by the regular expression $(w_1 + \cdots + w_k)^*$, where $w_1, \ldots, w_k$ are words that represent the matrices $M_1, \ldots, M_k$.

# Regular subsets

A subset $\mathcal{S}$ of $\mathrm{GL}(2,\mathbb{Z})$ is regular if there is a regular language $L$ in the alphabet $\Sigma = \{S, R, N\}$ such that

- Every word $w \in L$ represents a matrix from the subset $\mathcal{S}$.
- For any $A \in \mathcal{S}$, there is at least one $w \in L$ such that $w$ represents $A$.

A semigroup $\mathcal{S} = \langle M_1, \ldots, M_k \rangle$ is defined by the regular expression $(w_1 + \cdots + w_k)^*$, where $w_1, \ldots, w_k$ are words that represent the matrices $M_1, \ldots, M_k$.



**Theorem**

*The set $L = \{w \;:\; w$ represents a matrix from $H\}$ is regular.*

# $H = \{A \in \mathrm{GL}(2,\mathbb{Z}) \ : \ A^D \in \mathrm{GL}(2,\mathbb{Z})\}$

**Theorem**

*The set $L = \{w \ : \ w$ represents a matrix from $H\}$ is regular.*

- Let $U_0 = I, U_1, \ldots, U_s$ be representatives of the right cosets of $H$ in $\mathrm{GL}(2,\mathbb{Z})$.

# $H = \{A \in \mathrm{GL}(2,\mathbb{Z}) \ : \ A^D \in \mathrm{GL}(2,\mathbb{Z})\}$

**Theorem**

*The set $L = \{w \ : \ w$ represents a matrix from $H\}$ is regular.*

- Let $U_0 = I, U_1, \ldots, U_s$ be representatives of the right cosets of $H$ in $\mathrm{GL}(2,\mathbb{Z})$.
- Then the automaton $\mathcal{A}$ that recognizes $L$ has the states $Q = \{U_0, U_1, \ldots, U_s\}$, where $U_0$ is both the initial and the final state of $\mathcal{A}$.

**Theorem**

*The set $L = \{w \ : \ w$ represents a matrix from $H\}$ is regular.*

- Let $U_0 = I, U_1, \ldots, U_s$ be representatives of the right cosets of $H$ in $\mathrm{GL}(2,\mathbb{Z})$.
- Then the automaton $\mathcal{A}$ that recognizes $L$ has the states $Q = \{U_0, U_1, \ldots, U_s\}$, where $U_0$ is both the initial and the final state of $\mathcal{A}$.
- $\mathcal{A}$ has a transition $U_i \xrightarrow{R} U_j$ iff $U_i R U_j^{-1} \in H$.
  And similarly for $S$- and $N$-transitions.

# Example of an automaton for $H$

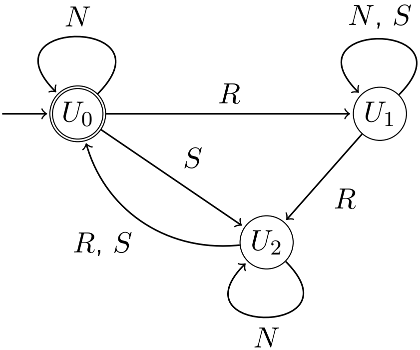
Let $D = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$. Then $H$ has index 3 in $\mathrm{GL}(2, \mathbb{Z})$ and representatives of the right cosets of $H$ in $\mathrm{GL}(2, \mathbb{Z})$ are

$$U_0 = I, \quad U_1 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \text{ and } U_2 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

# Example of an automaton for $H$

Let $D = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$. Then $H$ has index 3 in $\mathrm{GL}(2,\mathbb{Z})$ and representatives of the right cosets of $H$ in $\mathrm{GL}(2,\mathbb{Z})$ are

$$U_0 = I, \quad U_1 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \text{ and } U_2 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$




$$U_0 R U_1^{-1} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \in H.$$

So, $\mathcal{A}$ has a transition $U_0 \xrightarrow{R} U_1$.

# Base case $D = A_1 D A_2$

Let $\mathcal{M}$ be an automaton that recognizes the semigroup $\mathcal{S}$. We will construct an automaton $\mathrm{Inv}(\mathcal{M})$ that recognizes $\mathcal{S}^{-1}$ and an automaton $\mathcal{F}(\mathcal{M})$ that recognizes the following subset of $\mathrm{GL}(2, \mathbb{Z})$

$$\mathcal{S}^D = \{A^D \ : \ A \in \mathcal{S} \text{ and } A \in H\},$$

where $H = \{A \in \mathrm{GL}(2, \mathbb{Z}) \ : \ A^D \in \mathrm{GL}(2, \mathbb{Z})\}$.

## Base case $D = A_1 D A_2$

Let $\mathcal{M}$ be an automaton that recognizes the semigroup $\mathcal{S}$. We will construct an automaton $\mathrm{Inv}(\mathcal{M})$ that recognizes $\mathcal{S}^{-1}$ and an automaton $\mathcal{F}(\mathcal{M})$ that recognizes the following subset of $\mathrm{GL}(2,\mathbb{Z})$

$$\mathcal{S}^D = \{A^D \ : \ A \in \mathcal{S} \text{ and } A \in H\},$$

where $H = \{A \in \mathrm{GL}(2,\mathbb{Z}) \ : \ A^D \in \mathrm{GL}(2,\mathbb{Z})\}$.

Then the equation $A_2^{-1} = A_1^D$ has a solution $A_1, A_2 \in \mathcal{S}$ iff

$$L(\mathrm{Inv}(\mathcal{M})) \cap L(\mathcal{F}(\mathcal{M})) \neq \emptyset.$$

Let $\mathcal{M}$ be an automaton that recognizes the semigroup $\mathcal{S}$. We will construct an automaton $\mathrm{Inv}(\mathcal{M})$ that recognizes $\mathcal{S}^{-1}$ and an automaton $\mathcal{F}(\mathcal{M})$ that recognizes the following subset of $\mathrm{GL}(2,\mathbb{Z})$

$$\mathcal{S}^D = \{A^D \ : \ A \in \mathcal{S} \text{ and } A \in H\},$$

where $H = \{A \in \mathrm{GL}(2,\mathbb{Z}) \ : \ A^D \in \mathrm{GL}(2,\mathbb{Z})\}$.

Then the equation $A_2^{-1} = A_1^D$ has a solution $A_1, A_2 \in \mathcal{S}$ iff

$$L(\mathrm{Can}(\mathrm{Inv}(\mathcal{M}))) \cap L(\mathrm{Can}(\mathcal{F}(\mathcal{M}))) \neq \emptyset.$$

$\mathrm{Can}(\mathcal{M})$ recognizes the same subset of $\mathrm{GL}(2,\mathbb{Z})$ as $\mathcal{M}$ but accepts only canonical words.

# Construction of $\mathrm{Can}(\mathcal{M})$

To construct $\mathrm{Can}(\mathcal{M})$ we add the following transitions to $\mathcal{M}$:

# Construction of $\mathrm{Can}(\mathcal{M})$

To construct $\mathrm{Can}(\mathcal{M})$ we add the following transitions to $\mathcal{M}$:

- If $q_1$ and $q_2$ are two states of $\mathcal{M}$ which are connected by a path with label $RRR$ or $SS$, then we add a transition with label $(-I)$ from $q_1$ to $q_2$.

# Construction of $\mathrm{Can}(\mathcal{M})$

To construct $\mathrm{Can}(\mathcal{M})$ we add the following transitions to $\mathcal{M}$:

- If $q_1$ and $q_2$ are two states of $\mathcal{M}$ which are connected by a path with label $RRR$ or $SS$, then we add a transition with label $(-I)$ from $q_1$ to $q_2$.
- If $q_1$ and $q_2$ are two states of $\mathcal{M}$ which are connected by a path with label $(-I)(-I)$ or $\epsilon\epsilon$, then we add an $\epsilon$-transition from $q_1$ to $q_2$.

# Construction of $\mathrm{Can}(\mathcal{M})$

To construct $\mathrm{Can}(\mathcal{M})$ we add the following transitions to $\mathcal{M}$:

- If $q_1$ and $q_2$ are two states of $\mathcal{M}$ which are connected by a path with label $RRR$ or $SS$, then we add a transition with label $(-I)$ from $q_1$ to $q_2$.
- If $q_1$ and $q_2$ are two states of $\mathcal{M}$ which are connected by a path with label $(-I)(-I)$ or $\epsilon\epsilon$, then we add an $\epsilon$-transition from $q_1$ to $q_2$.
- Repeat this process until no new transitions can be added.

# Construction of $\mathrm{Can}(\mathcal{M})$

To construct $\mathrm{Can}(\mathcal{M})$ we add the following transitions to $\mathcal{M}$:

- If $q_1$ and $q_2$ are two states of $\mathcal{M}$ which are connected by a path with label $RRR$ or $SS$, then we add a transition with label $(-I)$ from $q_1$ to $q_2$.
- If $q_1$ and $q_2$ are two states of $\mathcal{M}$ which are connected by a path with label $(-I)(-I)$ or $\epsilon\epsilon$, then we add an $\epsilon$-transition from $q_1$ to $q_2$.
- Repeat this process until no new transitions can be added.

We also add special transitions in order to move $N$ to the beginning of the words.

# Construction of $\mathrm{Can}(\mathcal{M})$

To construct $\mathrm{Can}(\mathcal{M})$ we add the following transitions to $\mathcal{M}$:

- If $q_1$ and $q_2$ are two states of $\mathcal{M}$ which are connected by a path with label $RRR$ or $SS$, then we add a transition with label $(-I)$ from $q_1$ to $q_2$.
- If $q_1$ and $q_2$ are two states of $\mathcal{M}$ which are connected by a path with label $(-I)(-I)$ or $\epsilon\epsilon$, then we add an $\epsilon$-transition from $q_1$ to $q_2$.
- Repeat this process until no new transitions can be added.

We also add special transitions in order to move $N$ to the beginning of the words.

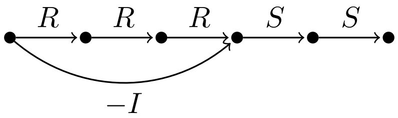
$$\bullet \xrightarrow{R} \bullet \xrightarrow{R} \bullet \xrightarrow{R} \bullet \xrightarrow{S} \bullet \xrightarrow{S} \bullet$$

# Construction of $\mathrm{Can}(\mathcal{M})$

To construct $\mathrm{Can}(\mathcal{M})$ we add the following transitions to $\mathcal{M}$:

- If $q_1$ and $q_2$ are two states of $\mathcal{M}$ which are connected by a path with label $RRR$ or $SS$, then we add a transition with label $(-I)$ from $q_1$ to $q_2$.
- If $q_1$ and $q_2$ are two states of $\mathcal{M}$ which are connected by a path with label $(-I)(-I)$ or $\epsilon\epsilon$, then we add an $\epsilon$-transition from $q_1$ to $q_2$.
- Repeat this process until no new transitions can be added.

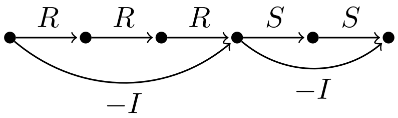
We also add special transitions in order to move $N$ to the beginning of the words.



To construct $\mathrm{Can}(\mathcal{M})$ we add the following transitions to $\mathcal{M}$:

- If $q_1$ and $q_2$ are two states of $\mathcal{M}$ which are connected by a path with label $RRR$ or $SS$, then we add a transition with label $(-I)$ from $q_1$ to $q_2$.
- If $q_1$ and $q_2$ are two states of $\mathcal{M}$ which are connected by a path with label $(-I)(-I)$ or $\epsilon\epsilon$, then we add an $\epsilon$-transition from $q_1$ to $q_2$.
- Repeat this process until no new transitions can be added.

We also add special transitions in order to move $N$ to the beginning of the words.

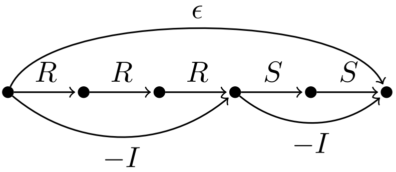


# Construction of $\mathrm{Can}(\mathcal{M})$

To construct $\mathrm{Can}(\mathcal{M})$ we add the following transitions to $\mathcal{M}$:

- If $q_1$ and $q_2$ are two states of $\mathcal{M}$ which are connected by a path with label $RRR$ or $SS$, then we add a transition with label $(-I)$ from $q_1$ to $q_2$.
- If $q_1$ and $q_2$ are two states of $\mathcal{M}$ which are connected by a path with label $(-I)(-I)$ or $\epsilon\epsilon$, then we add an $\epsilon$-transition from $q_1$ to $q_2$.
- Repeat this process until no new transitions can be added.

We also add special transitions in order to move $N$ to the beginning of the words.



We need to build $\mathcal{F}(\mathcal{M})$ that recognizes the set

$$\mathcal{S}^D = \{A^D \ : \ A \in \mathcal{S} \text{ and } A \in H\},$$

where $H = \{A \in \mathrm{GL}(2,\mathbb{Z}) \ : \ A^D \in \mathrm{GL}(2,\mathbb{Z})\}$.

We need to build $\mathcal{F}(\mathcal{M})$ that recognizes the set

$$\mathcal{S}^D = \{A^D \ : \ A \in \mathcal{S} \text{ and } A \in H\},$$

where $H = \{A \in \mathrm{GL}(2, \mathbb{Z}) \ : \ A^D \in \mathrm{GL}(2, \mathbb{Z})\}$.

The construction of $\mathcal{F}(\mathcal{M})$ is based on the following property: if $A = SRS$, then $A^D = S^D R^D S^D$.

We need to build $\mathcal{F}(\mathcal{M})$ that recognizes the set

$$\mathcal{S}^D = \{A^D \ : \ A \in \mathcal{S} \text{ and } A \in H\},$$

where $H = \{A \in \mathrm{GL}(2,\mathbb{Z}) \ : \ A^D \in \mathrm{GL}(2,\mathbb{Z})\}$.

The construction of $\mathcal{F}(\mathcal{M})$ is based on the following property: if $A = SRS$, then $A^D = S^D R^D S^D$.

The idea is to replace every transition $q_i \xrightarrow{R} q_j$ of $\mathcal{M}$ by a path labelled by a word $w$ such that $w$ represents the matrix $R^D$. And do the same for $S$- and $N$-transitions.

We need to build $\mathcal{F}(\mathcal{M})$ that recognizes the set

$$\mathcal{S}^D = \{A^D \ : \ A \in \mathcal{S} \text{ and } A \in H\},$$

where $H = \{A \in \mathrm{GL}(2,\mathbb{Z}) \ : \ A^D \in \mathrm{GL}(2,\mathbb{Z})\}$.

The construction of $\mathcal{F}(\mathcal{M})$ is based on the following property: if $A = SRS$, then $A^D = S^D R^D S^D$.

The idea is to replace every transition $q_i \xrightarrow{R} q_j$ of $\mathcal{M}$ by a path labelled by a word $w$ such that $w$ represents the matrix $R^D$. And do the same for $S$- and $N$-transitions.

However, $S^D$ and $R^D$ have fractional coefficients. So they don't belong to $\mathrm{GL}(2,\mathbb{Z})$ and cannot be presented by words.

$$\text{If } D = \begin{bmatrix} 1 & 0 \\ 0 & n \end{bmatrix}, \text{ then } \ S^D = \begin{bmatrix} 0 & -1 \\ \frac{1}{n} & 0 \end{bmatrix} \ \text{ and } \ R^D = \begin{bmatrix} 0 & -1 \\ \frac{1}{n} & 1 \end{bmatrix}$$

We need to build $\mathcal{F}(\mathcal{M})$ that recognizes the set

$$\mathcal{S}^D = \{A^D \ : \ A \in \mathcal{S} \text{ and } A \in H\},$$

where $H = \{A \in \mathrm{GL}(2, \mathbb{Z}) \ : \ A^D \in \mathrm{GL}(2, \mathbb{Z})\}$.

We need to build $\mathcal{F}(\mathcal{M})$ that recognizes the set

$$\mathcal{S}^D = \{A^D \;:\; A \in \mathcal{S} \text{ and } A \in H\},$$

where $H = \{A \in \mathrm{GL}(2,\mathbb{Z}) \;:\; A^D \in \mathrm{GL}(2,\mathbb{Z})\}$.

Let $\mathcal{A}$ be the automaton which recognizes $H$.
Recall that $\mathcal{A}$ has the states $\{U_0, U_1, \ldots, U_s\}$.

We need to build $\mathcal{F}(\mathcal{M})$ that recognizes the set

$$\mathcal{S}^D = \{A^D \ : \ A \in \mathcal{S} \text{ and } A \in H\},$$

where $H = \{A \in \mathrm{GL}(2, \mathbb{Z}) \ : \ A^D \in \mathrm{GL}(2, \mathbb{Z})\}$.

Let $\mathcal{A}$ be the automaton which recognizes $H$.
Recall that $\mathcal{A}$ has the states $\{U_0, U_1, \ldots, U_s\}$.
Suppose the automaton $\mathcal{M}$ has the states $\{q_0, \ldots, q_r\}$.

We need to build $\mathcal{F}(\mathcal{M})$ that recognizes the set

$$\mathcal{S}^D = \{A^D \ : \ A \in \mathcal{S} \text{ and } A \in H\},$$

where $H = \{A \in \mathrm{GL}(2, \mathbb{Z}) \ : \ A^D \in \mathrm{GL}(2, \mathbb{Z})\}$.

Let $\mathcal{A}$ be the automaton which recognizes $H$.
Recall that $\mathcal{A}$ has the states $\{U_0, U_1, \ldots, U_s\}$.
Suppose the automaton $\mathcal{M}$ has the states $\{q_0, \ldots, q_r\}$.

To construct $\mathcal{F}(\mathcal{M})$ we first construct the Cartesian product $\mathcal{M} \times \mathcal{A}$ which recognizes the intersection $L(\mathcal{M}) \cap L(\mathcal{A})$.

We need to build $\mathcal{F}(\mathcal{M})$ that recognizes the set

$$\mathcal{S}^D = \{A^D \ : \ A \in \mathcal{S} \text{ and } A \in H\},$$

where $H = \{A \in \mathrm{GL}(2,\mathbb{Z}) \ : \ A^D \in \mathrm{GL}(2,\mathbb{Z})\}$.

Let $\mathcal{A}$ be the automaton which recognizes $H$.
Recall that $\mathcal{A}$ has the states $\{U_0, U_1, \ldots, U_s\}$.
Suppose the automaton $\mathcal{M}$ has the states $\{q_0, \ldots, q_r\}$.

To construct $\mathcal{F}(\mathcal{M})$ we first construct the Cartesian product $\mathcal{M} \times \mathcal{A}$ which recognizes the intersection $L(\mathcal{M}) \cap L(\mathcal{A})$.

Then we replace every transition $(q_i, U_j) \xrightarrow{R} (q_l, U_m)$ of $\mathcal{M} \times \mathcal{A}$ with a path

$$(q_i, U_j) \xrightarrow{\sigma_1} p_1 \xrightarrow{\sigma_2} p_2 \to \cdots \to p_{k-1} \xrightarrow{\sigma_k} (q_l, U_m),$$

where $p_1, p_2, \ldots, p_{k-1}$ are new states and the word $w = \sigma_1\sigma_2 \ldots \sigma_k$ represents the matrix $(U_j R U_m^{-1})^D$.

We need to build $\mathcal{F}(\mathcal{M})$ that recognizes the set

$$\mathcal{S}^D = \{A^D \ : \ A \in \mathcal{S} \text{ and } A \in H\},$$

where $H = \{A \in \mathrm{GL}(2,\mathbb{Z}) \ : \ A^D \in \mathrm{GL}(2,\mathbb{Z})\}$.

Let $\mathcal{A}$ be the automaton which recognizes $H$.
Recall that $\mathcal{A}$ has the states $\{U_0, U_1, \ldots, U_s\}$.
Suppose the automaton $\mathcal{M}$ has the states $\{q_0, \ldots, q_r\}$.

To construct $\mathcal{F}(\mathcal{M})$ we first construct the Cartesian product $\mathcal{M} \times \mathcal{A}$ which recognizes the intersection $L(\mathcal{M}) \cap L(\mathcal{A})$.

Then we replace every transition $(q_i, U_j) \xrightarrow{R} (q_l, U_m)$ of $\mathcal{M} \times \mathcal{A}$ with a path

$$(q_i, U_j) \xrightarrow{\sigma_1} p_1 \xrightarrow{\sigma_2} p_2 \to \cdots \to p_{k-1} \xrightarrow{\sigma_k} (q_l, U_m),$$

where $p_1, p_2, \ldots, p_{k-1}$ are new states and the word $w = \sigma_1\sigma_2\ldots\sigma_k$ represents the matrix $(U_j R U_m^{-1})^D$.
Do the same for $S$- and $N$-transitions.

Then we replace every transition $(q_i, U_j) \xrightarrow{R} (q_l, U_m)$ of $\mathcal{M} \times \mathcal{A}$ with a path

$$(q_i, U_j) \xrightarrow{\sigma_1} p_1 \xrightarrow{\sigma_2} p_2 \to \cdots \to p_{k-1} \xrightarrow{\sigma_k} (q_l, U_m),$$

where $p_1, p_2, \ldots, p_{k-1}$ are new states and the word $w = \sigma_1\sigma_2 \ldots \sigma_k$ represents the matrix $(U_j R U_m^{-1})^D$.

Then we replace every transition $(q_i, U_j) \xrightarrow{R} (q_l, U_m)$ of $\mathcal{M} \times \mathcal{A}$ with a path

$$(q_i, U_j) \xrightarrow{\sigma_1} p_1 \xrightarrow{\sigma_2} p_2 \to \cdots \to p_{k-1} \xrightarrow{\sigma_k} (q_l, U_m),$$

where $p_1, p_2, \ldots, p_{k-1}$ are new states and the word $w = \sigma_1\sigma_2\ldots\sigma_k$ represents the matrix $(U_j R U_m^{-1})^D$.

If $(q_i, U_j) \xrightarrow{R} (q_l, U_m)$ is a transition of $\mathcal{M} \times \mathcal{A}$, then $\mathcal{A}$ has a transition $U_j \xrightarrow{R} U_m$.

Then we replace every transition $(q_i, U_j) \xrightarrow{R} (q_l, U_m)$ of $\mathcal{M} \times \mathcal{A}$ with a path

$$(q_i, U_j) \xrightarrow{\sigma_1} p_1 \xrightarrow{\sigma_2} p_2 \to \cdots \to p_{k-1} \xrightarrow{\sigma_k} (q_l, U_m),$$

where $p_1, p_2, \ldots, p_{k-1}$ are new states and the word $w = \sigma_1\sigma_2 \ldots \sigma_k$ represents the matrix $(U_j R U_m^{-1})^D$.

If $(q_i, U_j) \xrightarrow{R} (q_l, U_m)$ is a transition of $\mathcal{M} \times \mathcal{A}$, then $\mathcal{A}$ has a transition $U_j \xrightarrow{R} U_m$.

By definition of $\mathcal{A}$ this implies that $U_j R U_m^{-1} \in H$.

Then we replace every transition $(q_i, U_j) \xrightarrow{R} (q_l, U_m)$ of $\mathcal{M} \times \mathcal{A}$ with a path

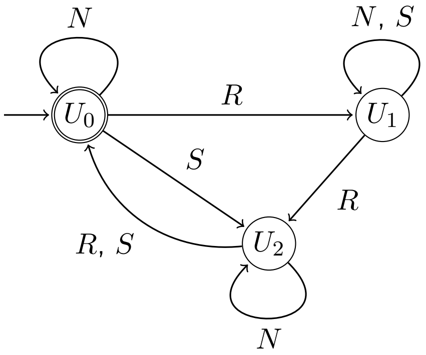
$$(q_i, U_j) \xrightarrow{\sigma_1} p_1 \xrightarrow{\sigma_2} p_2 \to \cdots \to p_{k-1} \xrightarrow{\sigma_k} (q_l, U_m),$$

where $p_1, p_2, \ldots, p_{k-1}$ are new states and the word $w = \sigma_1 \sigma_2 \ldots \sigma_k$ represents the matrix $(U_j R U_m^{-1})^D$.

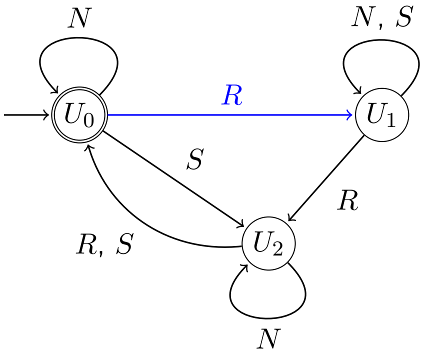
If $(q_i, U_j) \xrightarrow{R} (q_l, U_m)$ is a transition of $\mathcal{M} \times \mathcal{A}$, then $\mathcal{A}$ has a transition $U_j \xrightarrow{R} U_m$.

By definition of $\mathcal{A}$ this implies that $U_j R U_m^{-1} \in H$.

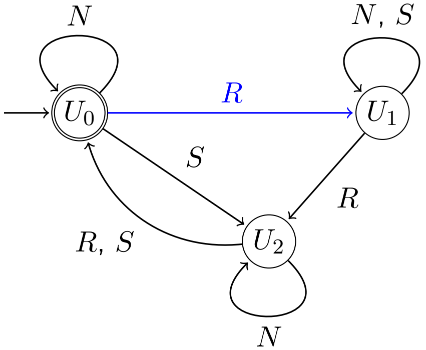
Hence $(U_j R U_m^{-1})^D$ belongs to $\mathrm{GL}(2, \mathbb{Z})$, and we can find a word $w$ that represents $(U_j R U_m^{-1})^D$.




Let $D = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$.

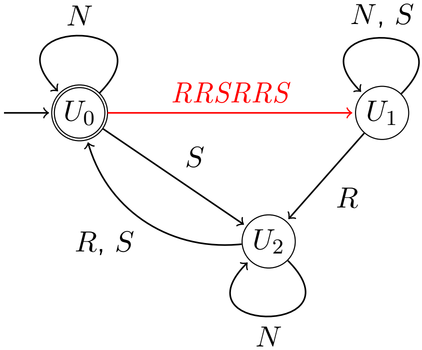



Let $D = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$.



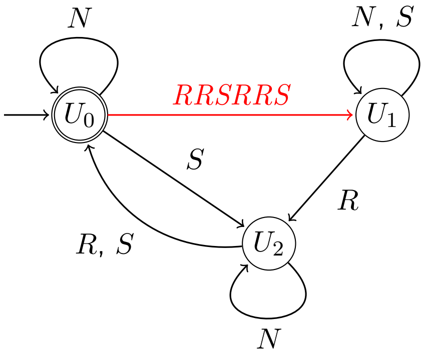

Let $D = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$.

$$(U_0 {\color{blue}R} U_1^{-1})^D = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}^D = \begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix} = {\color{red}RRSRRS}.$$

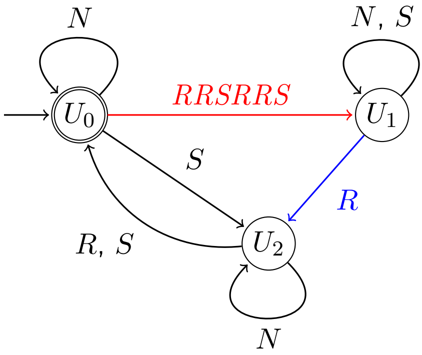



Let $D = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$.

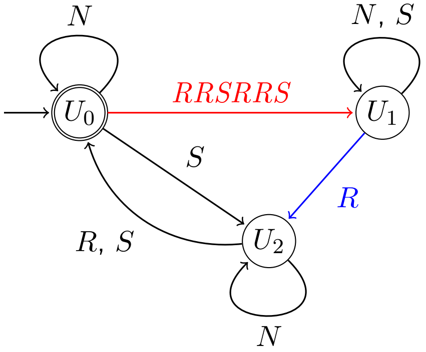
$$(U_0 R U_1^{-1})^D = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}^D = \begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix} = RRSRRS.$$




Let $D = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$.

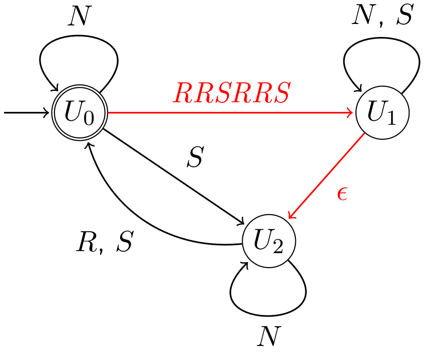



Let $D = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$.




Let $D = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$.

$$(U_1 R U_2^{-1})^D = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}^D = I.$$




Let $D = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$.

$$(U_1 R U_2^{-1})^D = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}^D = I.$$

Suppose $A = SRS$ belongs to $\mathcal{S} \cap H$. Then there is an accepting run of $SRS$ in the automaton $\mathcal{A}$ that recognizes $H$

$$U_0 \xrightarrow{S} U_1 \xrightarrow{R} U_2 \xrightarrow{S} U_0, \qquad U_0 = I$$

Suppose $A = SRS$ belongs to $\mathcal{S} \cap H$. Then there is an accepting run of $SRS$ in the automaton $\mathcal{A}$ that recognizes $H$

$$U_0 \xrightarrow{S} U_1 \xrightarrow{R} U_2 \xrightarrow{S} U_0, \qquad U_0 = I$$

The matrices $U_0 S U_1^{-1}$, $U_1 R U_2^{-1}$, $U_2 S U_0^{-1}$ belong to $H$.

Suppose $A = SRS$ belongs to $\mathcal{S} \cap H$. Then there is an accepting run of $SRS$ in the automaton $\mathcal{A}$ that recognizes $H$

$$U_0 \xrightarrow{S} U_1 \xrightarrow{R} U_2 \xrightarrow{S} U_0, \qquad U_0 = I$$

The matrices $U_0 S U_1^{-1}$, $U_1 R U_2^{-1}$, $U_2 S U_0^{-1}$ belong to $H$.

Rewrite $A = SRS = (U_0 S U_1^{-1})(U_1 R U_2^{-1})(U_2 S U_0^{-1})$.

Suppose $A = SRS$ belongs to $\mathcal{S} \cap H$. Then there is an accepting run of $SRS$ in the automaton $\mathcal{A}$ that recognizes $H$

$$U_0 \xrightarrow{S} U_1 \xrightarrow{R} U_2 \xrightarrow{S} U_0, \qquad U_0 = I$$

The matrices $U_0 S U_1^{-1}$, $U_1 R U_2^{-1}$, $U_2 S U_0^{-1}$ belong to $H$.

Rewrite $A = SRS = (U_0 S U_1^{-1})(U_1 R U_2^{-1})(U_2 S U_0^{-1})$.

Then $A^D = (U_0 S U_1^{-1})^D (U_1 R U_2^{-1})^D (U_2 S U_0^{-1})^D$.

Suppose $A = SRS$ belongs to $\mathcal{S} \cap H$. Then there is an accepting run of $SRS$ in the automaton $\mathcal{A}$ that recognizes $H$

$$U_0 \xrightarrow{S} U_1 \xrightarrow{R} U_2 \xrightarrow{S} U_0, \qquad U_0 = I$$

The matrices $U_0 S U_1^{-1}$, $U_1 R U_2^{-1}$, $U_2 S U_0^{-1}$ belong to $H$.

Rewrite $A = SRS = (U_0 S U_1^{-1})(U_1 R U_2^{-1})(U_2 S U_0^{-1})$.

Then $A^D = \underbrace{(U_0 S U_1^{-1})^D}_{w_1} \underbrace{(U_1 R U_2^{-1})^D}_{w_2} \underbrace{(U_2 S U_0^{-1})^D}_{w_3}$.

Let $w_1$, $w_2$ and $w_3$ be words that represent the matrices $(U_0 S U_1^{-1})^D$, $(U_1 R U_2^{-1})^D$ and $(U_2 S U_0^{-1})^D$.

Suppose $A = SRS$ belongs to $\mathcal{S} \cap H$. Then there is an accepting run of $SRS$ in the automaton $\mathcal{A}$ that recognizes $H$

$$U_0 \xrightarrow{S} U_1 \xrightarrow{R} U_2 \xrightarrow{S} U_0, \qquad U_0 = I$$

The matrices $U_0 S U_1^{-1}$, $U_1 R U_2^{-1}$, $U_2 S U_0^{-1}$ belong to $H$.

Rewrite $A = SRS = (U_0 S U_1^{-1})(U_1 R U_2^{-1})(U_2 S U_0^{-1})$.

Then $A^D = \underbrace{(U_0 S U_1^{-1})^D}_{w_1} \underbrace{(U_1 R U_2^{-1})^D}_{w_2} \underbrace{(U_2 S U_0^{-1})^D}_{w_3}$.

Let $w_1$, $w_2$ and $w_3$ be words that represent the matrices $(U_0 S U_1^{-1})^D$, $(U_1 R U_2^{-1})^D$ and $(U_2 S U_0^{-1})^D$.

Then $\mathcal{F}(\mathcal{M})$ has an accepting path of the form

$$(q_0, U_0) \xrightarrow{w_1} (q_1, U_1) \xrightarrow{w_2} (q_2, U_2) \xrightarrow{w_3} (q_3, U_0)$$

Suppose $A = SRS$ belongs to $\mathcal{S} \cap H$. Then there is an accepting run of $SRS$ in the automaton $\mathcal{A}$ that recognizes $H$

$$U_0 \xrightarrow{S} U_1 \xrightarrow{R} U_2 \xrightarrow{S} U_0, \qquad U_0 = I$$

The matrices $U_0 S U_1^{-1}$, $U_1 R U_2^{-1}$, $U_2 S U_0^{-1}$ belong to $H$.

Rewrite $A = SRS = (U_0 S U_1^{-1})(U_1 R U_2^{-1})(U_2 S U_0^{-1})$.

Then $A^D = \underbrace{(U_0 S U_1^{-1})^D}_{w_1} \underbrace{(U_1 R U_2^{-1})^D}_{w_2} \underbrace{(U_2 S U_0^{-1})^D}_{w_3}$.

Let $w_1$, $w_2$ and $w_3$ be words that represent the matrices $(U_0 S U_1^{-1})^D$, $(U_1 R U_2^{-1})^D$ and $(U_2 S U_0^{-1})^D$.

Then $\mathcal{F}(\mathcal{M})$ has an accepting path of the form

$$(q_0, U_0) \xrightarrow{w_1} (q_1, U_1) \xrightarrow{w_2} (q_2, U_2) \xrightarrow{w_3} (q_3, U_0)$$

where $q_0 \xrightarrow{S} q_1 \xrightarrow{R} q_2 \xrightarrow{S} q_3$ is an accepting run of $\mathcal{M}$ on $SRS$.

# Main steps of the proof

# Main steps of the proof

- We use Smith normal form theorem to reduce $M = A_1 M_1 A_2$ to $D = A_1 D A_2$, where $D = \begin{bmatrix} 1 & 0 \\ 0 & n \end{bmatrix}$.

# Main steps of the proof

- We use Smith normal form theorem to reduce $M = A_1 M_1 A_2$ to $D = A_1 D A_2$, where $D = \begin{bmatrix} 1 & 0 \\ 0 & n \end{bmatrix}$.
- Rewrite $D = A_1 D A_2$ as $A_2^{-1} = A_1^D$ and note that $A_1 \in H = \{A \in \mathrm{GL}(2, \mathbb{Z}) \ : \ A^D \in \mathrm{GL}(2, \mathbb{Z})\}$

# Main steps of the proof

- We use Smith normal form theorem to reduce $M = A_1 M_1 A_2$ to $D = A_1 D A_2$, where $D = \begin{bmatrix} 1 & 0 \\ 0 & n \end{bmatrix}$.
- Rewrite $D = A_1 D A_2$ as $A_2^{-1} = A_1^D$ and note that $A_1 \in H = \{A \in \mathrm{GL}(2,\mathbb{Z}) \ : \ A^D \in \mathrm{GL}(2,\mathbb{Z})\}$
- $H$ is a subgroup of $\mathrm{GL}(2,\mathbb{Z})$ of finite index, and there is an automaton $\mathcal{A}$ that recognizes $H$.

# Main steps of the proof

- We use Smith normal form theorem to reduce $M = A_1 M_1 A_2$ to $D = A_1 D A_2$, where $D = \begin{bmatrix} 1 & 0 \\ 0 & n \end{bmatrix}$.
- Rewrite $D = A_1 D A_2$ as $A_2^{-1} = A_1^D$ and note that $A_1 \in H = \{A \in \mathrm{GL}(2, \mathbb{Z}) \ : \ A^D \in \mathrm{GL}(2, \mathbb{Z})\}$
- $H$ is a subgroup of $\mathrm{GL}(2, \mathbb{Z})$ of finite index, and there is an automaton $\mathcal{A}$ that recognizes $H$.
- Construction of $\mathrm{Can}(\mathcal{A})$.

# Main steps of the proof

- We use Smith normal form theorem to reduce $M = A_1 M_1 A_2$ to $D = A_1 D A_2$, where $D = \begin{bmatrix} 1 & 0 \\ 0 & n \end{bmatrix}$.
- Rewrite $D = A_1 D A_2$ as $A_2^{-1} = A_1^D$ and note that $A_1 \in H = \{A \in \mathrm{GL}(2,\mathbb{Z}) \ : \ A^D \in \mathrm{GL}(2,\mathbb{Z})\}$
- $H$ is a subgroup of $\mathrm{GL}(2,\mathbb{Z})$ of finite index, and there is an automaton $\mathcal{A}$ that recognizes $H$.
- Construction of $\mathrm{Can}(\mathcal{A})$.
- Construction of $\mathcal{F}(\mathcal{M})$ that recognizes $\mathcal{S}^D = \{A^D \ : \ A \in \mathcal{S}$ and $A \in H\}$.

# Main steps of the proof

- We use Smith normal form theorem to reduce $M = A_1 M_1 A_2$ to $D = A_1 D A_2$, where $D = \begin{bmatrix} 1 & 0 \\ 0 & n \end{bmatrix}$.
- Rewrite $D = A_1 D A_2$ as $A_2^{-1} = A_1^D$ and note that $A_1 \in H = \{A \in \mathrm{GL}(2,\mathbb{Z}) \ : \ A^D \in \mathrm{GL}(2,\mathbb{Z})\}$
- $H$ is a subgroup of $\mathrm{GL}(2,\mathbb{Z})$ of finite index, and there is an automaton $\mathcal{A}$ that recognizes $H$.
- Construction of $\mathrm{Can}(\mathcal{A})$.
- Construction of $\mathcal{F}(\mathcal{M})$ that recognizes $\mathcal{S}^D = \{A^D \ : \ A \in \mathcal{S}$ and $A \in H\}$.
- The equation $A_2^{-1} = A_1^D$ has a solution $A_1, A_2 \in \mathcal{S}$ iff

$$L(\mathrm{Can}(\mathrm{Inv}(\mathcal{M}))) \cap L(\mathrm{Can}(\mathcal{F}(\mathcal{M}))) \neq \emptyset.$$

# Construction of $\mathcal{F}(\mathcal{M})$

Recall that $\mathcal{M}$ recognizes $\mathcal{S}$, and $\mathcal{A}$ recognizes $H$.
To construct $\mathcal{F}(\mathcal{M})$:

Recall that $\mathcal{M}$ recognizes $\mathcal{S}$, and $\mathcal{A}$ recognizes $H$.
To construct $\mathcal{F}(\mathcal{M})$:

- First, construct the product $\mathcal{M} \times \mathcal{A}$ for $L(\mathcal{M}) \cap L(\mathcal{A})$.

Recall that $\mathcal{M}$ recognizes $\mathcal{S}$, and $\mathcal{A}$ recognizes $H$.
To construct $\mathcal{F}(\mathcal{M})$:

- First, construct the product $\mathcal{M} \times \mathcal{A}$ for $L(\mathcal{M}) \cap L(\mathcal{A})$.
- Use $\mathcal{A}$ to rewrite any word accepted by $\mathcal{A}$ as

$$SRS = (U_0 S U_1^{-1})(U_1 R U_2^{-1})(U_2 S U_0^{-1})$$

where $U_0 \xrightarrow{S} U_1 \xrightarrow{R} U_2 \xrightarrow{S} U_0$ is an accepting run of $\mathcal{A}$.

## Construction of $\mathcal{F}(\mathcal{M})$

Recall that $\mathcal{M}$ recognizes $\mathcal{S}$, and $\mathcal{A}$ recognizes $H$.
To construct $\mathcal{F}(\mathcal{M})$:

- First, construct the product $\mathcal{M} \times \mathcal{A}$ for $L(\mathcal{M}) \cap L(\mathcal{A})$.
- Use $\mathcal{A}$ to rewrite any word accepted by $\mathcal{A}$ as

$$SRS = (U_0 S U_1^{-1})(U_1 R U_2^{-1})(U_2 S U_0^{-1})$$

  where $U_0 \xrightarrow{S} U_1 \xrightarrow{R} U_2 \xrightarrow{S} U_0$ is an accepting run of $\mathcal{A}$.
- Express $(SRS)^D = (U_0 S U_1^{-1})^D (U_1 R U_2^{-1})^D (U_2 S U_0^{-1})^D$

# Construction of $\mathcal{F}(\mathcal{M})$

Recall that $\mathcal{M}$ recognizes $\mathcal{S}$, and $\mathcal{A}$ recognizes $H$.
To construct $\mathcal{F}(\mathcal{M})$:

- First, construct the product $\mathcal{M} \times \mathcal{A}$ for $L(\mathcal{M}) \cap L(\mathcal{A})$.
- Use $\mathcal{A}$ to rewrite any word accepted by $\mathcal{A}$ as

$$SRS = (U_0 S U_1^{-1})(U_1 R U_2^{-1})(U_2 S U_0^{-1})$$

  where $U_0 \xrightarrow{S} U_1 \xrightarrow{R} U_2 \xrightarrow{S} U_0$ is an accepting run of $\mathcal{A}$.
- Express $(SRS)^D = (U_0 S U_1^{-1})^D (U_1 R U_2^{-1})^D (U_2 S U_0^{-1})^D$
- Replace transitions of $\mathcal{M} \times \mathcal{A}$ with new paths:

# Construction of $\mathcal{F}(\mathcal{M})$

Recall that $\mathcal{M}$ recognizes $\mathcal{S}$, and $\mathcal{A}$ recognizes $H$.
To construct $\mathcal{F}(\mathcal{M})$:

- First, construct the product $\mathcal{M} \times \mathcal{A}$ for $L(\mathcal{M}) \cap L(\mathcal{A})$.
- Use $\mathcal{A}$ to rewrite any word accepted by $\mathcal{A}$ as

$$SRS = (U_0 S U_1^{-1})(U_1 R U_2^{-1})(U_2 S U_0^{-1})$$

  where $U_0 \xrightarrow{S} U_1 \xrightarrow{R} U_2 \xrightarrow{S} U_0$ is an accepting run of $\mathcal{A}$.
- Express $(SRS)^D = (U_0 S U_1^{-1})^D (U_1 R U_2^{-1})^D (U_2 S U_0^{-1})^D$
- Replace transitions of $\mathcal{M} \times \mathcal{A}$ with new paths: every transition $(q_i, U_j) \xrightarrow{R} (q_l, U_m)$ is replaced by a path with label $w$, where $w$ represents the matrix $(U_j R U_m^{-1})^D$.